DISTINGUISHABILITY, SYMMETRY, AND ENERGY ESTIMATION: QUANTUM ALGORITHMS AND COMPLEXITY

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Soorya Rethinasamy

May 2025

DISTINGUISHABILITY, SYMMETRY, AND ENERGY ESTIMATION:
QUANTUM ALGORITHMS AND COMPLEXITY

Soorya Rethinasamy, Ph.D.
Cornell University 2025

Quantum computing is a relatively new computing paradigm that seeks to use quantum resources, like superposition and entanglement, to process information in a significantly new way. These resources allow quantum computers to solve certain problems more efficiently than their classical counterparts, with promising applications in cryptography, optimization, and materials science. This thesis investigates the development and implementation of quantum algorithms to solve certain estimation problems in quantum information science and computing. Using variational quantum algorithms and near-term hardware, we investigate three interconnected domains of research: distinguishability estimation, symmetry testing, and nuclear dynamics.

In the first study, we explore the estimation of distinguishability measures, such as trace distance and fidelity, which are crucial for evaluating quantum information processing protocols. We provide novel interpretations of these different measures and study the computational complexity of the algorithms to estimate these measures.

Next, we put forth several symmetry testing algorithms that estimate what we call 'maximum symmetric fidelities.' We study several different symmetry examples, including cyclicity, permutation, and others. A major contribution of this study is the connection of the symmetry testing algorithms to the computational complexity hierarchy. We provide proofs that symmetry testing algorithms are complete for different complexity classes.

In the last study, we explore different qubit encoding techniques for translating nuclear physics problems to quantum computers. We analyze the various trade-offs and show that one encoding outperforms that others in all the relevant metrics.

For all the studies above, we simulate the algorithms in the noiseless and noisy scenarios and show robust convergence for the examples considered.

Biographical Sketch

Soorya Rethinasamy is a fifth-year graduate student in the Applied and Engineering Physics Department at Cornell University. He received his Bachelor of Engineering (Hons.) in Computer Science and his Master of Science (Hons.) in Physics from the Birla Institute of Technology and Science, Pilani. He began his Ph.D. at Louisiana State University in 2021 and transferred to Cornell University in 2022.

During his tenure, he has authored several publications and presented his work at multiple conferences. He has also mentored several high school and undergraduate students in quantum computing, resulting in collaborative research publications.

His research field is the design and analysis of quantum algorithms. He attended the IBM Summer School on quantum error correction and interned at the Global Technology Applied Research Team at JP Morgan Chase.

This document is dedicated to my wife.

Acknowledgements

This thesis, and my graduate school journey as a whole, would not have been possible without the invaluable support of many people, including professional colleagues, friends, and family.

First and foremost, I would like to extend my heartfelt gratitude to my advisor, Dr. Mark M. Wilde, without whom the entire endeavor would have been impossible. His guidance and deep knowledge of the material was invaluable. I would also like to thank my committee members, Dr. Valla Fatemi and Dr. Karan K. Mehta. My sincere thanks also goes to Dr. Kristina D. Launey and Dr. Zoë Holmes.

I would not have made it through graduate school without the constant support from my wife, Lauren Hingle. She has spent many an hour looking at random circuit diagrams and equations on our various whiteboards, all while acting actively interested. Her unlimited patience for my tomfoolery has sustained me through this journey, and I am forever grateful.

Next, I would like to thank my family. This includes my mom, Dr. Thankam S., and dad, R. S. Rethinasamy; my sister, Megha Rethinasamy; my grandfather, P. Subramonian; my uncle, Nataraj Subramonian; my cousins, Karthik Nataraj and Nivedita Nataraj; and my brother-in-law, Christopher Andre de la Porte. Our weekly multi-hour Zoom calls have been quite entertaining and have definitely brought us closer. I would also like to thank the extended Chalo Chalo family for accepting me into their tribe.

The next important group of people are my colleagues. First and foremost, I would like to acknowledge Margarite L. LaBorde. Working alongside her has been my most productive and meaningful collaboration, greatly enriching this thesis. In no particular order, I would like to thank my fellow Cornell graduate students Aby Philip, Vishal Singh, Dhrumil Patel, Hemant Mishra, Theshani Nuradha, and Kaiyuan Ji. My heartfelt gratitude also goes to my LSU friends Stav Haldar, Anshumita Baul, Akhil Bharadwaj, Prerna Agarwal, Karunya Shirali, Pratik Barge,

and Rujuta Vaidya. I would also like to thank my various co-authors who made each project a great experience. Again, in no particular order, the list includes Rochisha Agarwal, Kunal Sharma, Vincent Russo, Hanna Westerheim, Jingxuan Chen, Ivy Luo, Kathie Wang, Ethan Guo, and Alexander Wei.

My final set of personal thanks goes to my friends from back home in India who have been a big part of my journey. Again, in no particular order, I would like to thank Deepak Vasudevan, Gokul Srinivasan, Sneha Kumari, Anvita Srinivas, Abhinav Sundar, Samvida S. Venkatesh, Niranjana Menon, Padma Venkataraman, Aparna Muraleekrishan, Sahili Totale, Ritika Diwan, Tanvi Ahuja, Sneha Khandelwal, and Aiswarya Sasi.

I would also like to acknowledge support from the National Science Foundation under Grant No. 2315398 and Grant No. 1907615, from the Air Force Research Laboratory under agreement no. FA8750-23-2-0031, and from the U.S. Department of Energy under award DE-SC0023694.

Contents

Chapter 1

Introduction and brief history

> *The more important fundamental laws and facts of physical science have all been discovered, and these are now so firmly established that the possibility of their ever being supplanted in consequence of new discoveries is exceedingly remote.*
> – Albert A. Michelson, 1894

> *Anyone who is not shocked by quantum theory has not understood it.*
> – Neils Bohr (Widely attributed; expresses Bohr's views from the 1920s-30s on the strangeness of quantum mechanics.)

The goal of this chapter is to provide an overarching introduction to various ideas and concepts. We begin with a very short journey into the history of quantum mechanics and, more focusedly, quantum computing. This journey will necessarily have to be brief, but I shall try to cover all the relevant landmarks.

The origins of quantum mechanics begin with a light bulb. In 1900, Max Planck was attempting to design a light bulb that emits the maximum amount of energy in the visible spectrum, as opposed to the other regions, like ultraviolet and infrared. To do this, he tried to theoretically model what the energy spectrum of a hot body would look like at different temperatures. Using the strongly established wave theory of light by James Clark Maxwell, he derived a function that looks like Figure 1.1.

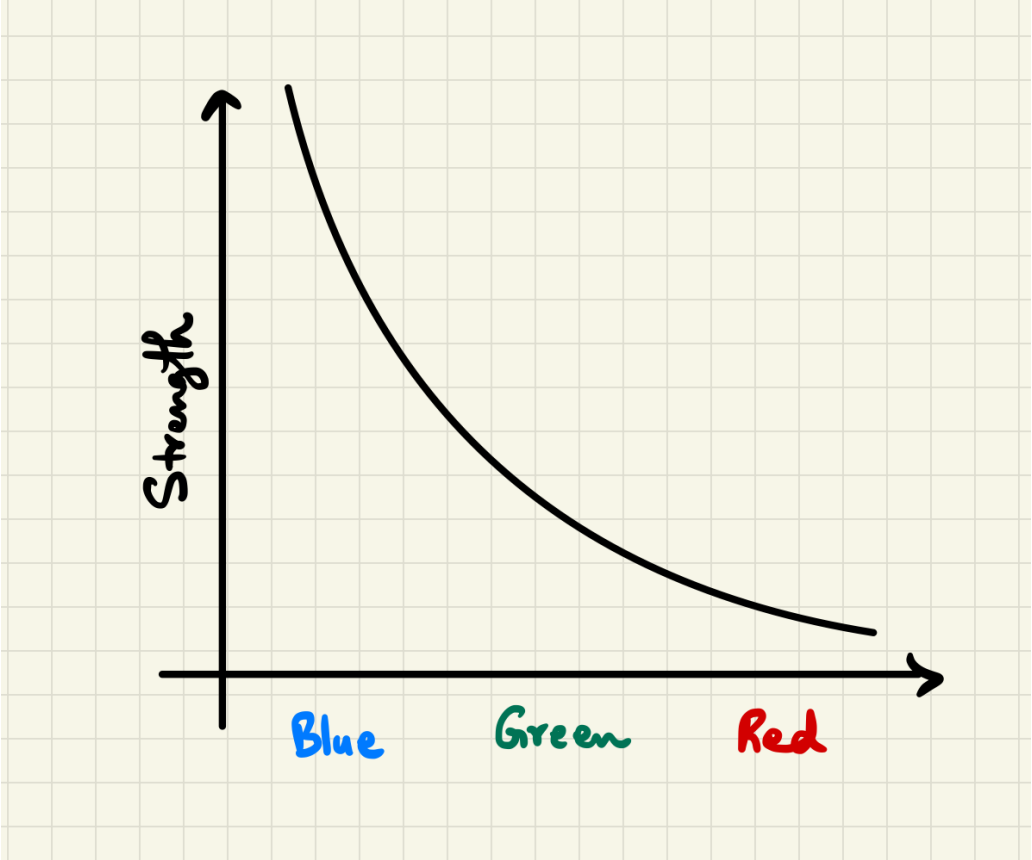


Figure 1.1: Schematic of the spectral radiance function derived by Max Planck and others.

This was called the "ultraviolet catastrophe" because it predicted an unbounded amount of energy that is emitted by a hot body at high frequencies, a prediction that was in stark contrast with the observed data. In an 'act of despair', Max Planck proposed a new model, working backwards from the experimental data. He proposed a theory that light is emitted in packets, called *quanta*, and not continuously. The frequency of the light determines the energy of the packet. The total energy is split into packets of different sizes based on their frequency. The larger the frequency, the more energy it will contain, but there will be a smaller number of such large packets. The two effects compete with each other and lead to a different expected function of energy as a function of frequency, as seen in Figure 1.2. Increasing the temperature increased the overall average frequency, but at large frequencies, the energy density goes to zero, avoiding the catastrophe.

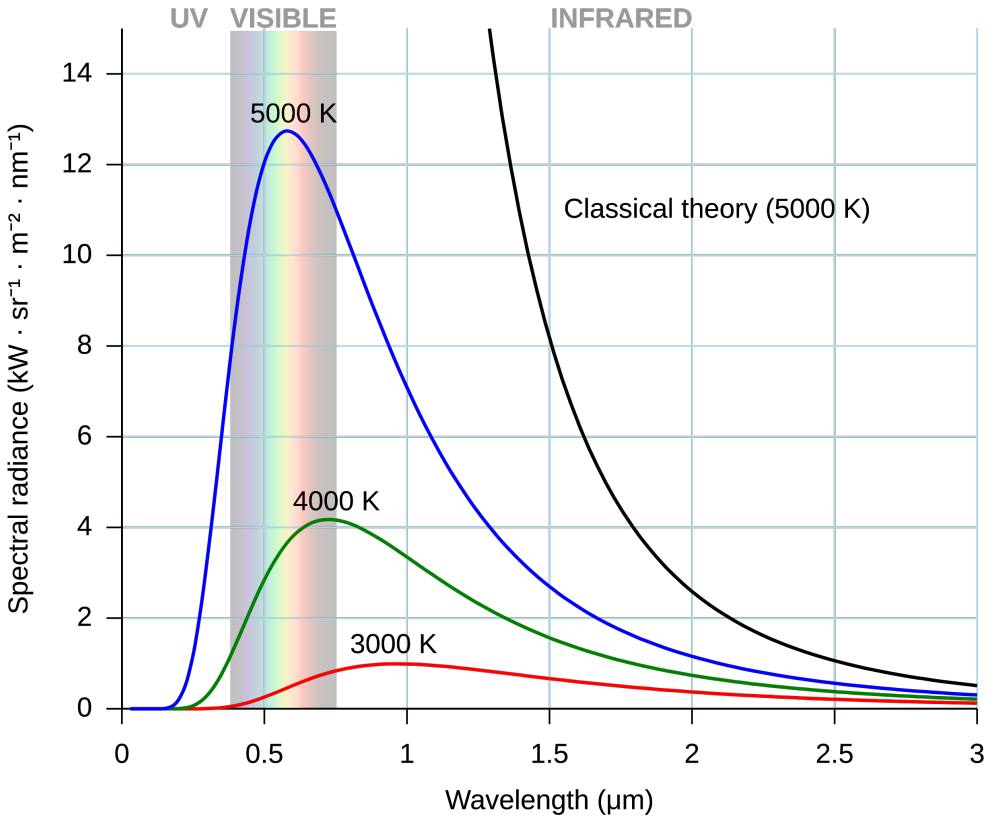


Figure 1.2: Experimentally observed light distribution, in excellent agreement with Max Planck's new theory.

In 1095, Albert Einstein advanced this hypothesis that light comes in packets, showing that it theoretically explains the photoelectric effect. When light was shone on a metal surface, electrons were ejected from it, and the number of electrons can be measured. Classical wave theory predicted that the number of electrons would be proportional to the intensity of the incoming light. However, it was observed that the energy of the ejected electrons was independent of the intensity of light. Furthermore, a minimum frequency of light was required to begin ejecting electrons. All of this was explained by Einstein using the equation

$$E = h\nu, \tag{1.1}$$

where E is the energy of a light packet, ν is its frequency, and h is a fundamental constant, which was named Planck's constant.

So something weird was going on with light. In some experiments, like diffraction and interference, it behaved like a wave. In contrast, in experiments like the photoelectric effect, it behaved as a particle. In 1924, Louis de Broglie proposed a radical idea. If light can behave as both a particle and a wave, maybe matter could also behave as both! He postulated that a matter particle with momentum p has a wavelength

$$\lambda = \frac{h}{p}. \tag{1.2}$$

This hypothesis was tested and confirmed by experiments like Young's double-slit experiment and the Davisson-Germer experiment, which both showed that electrons displayed an interference pattern! To explain the wave nature, Erwin Schrödinger, in 1926, proposed the idea of the *wavefunction*. This was a mathematical object that contains all the information about a system. In addition, he put forth the equation known as Schrödinger's wave equation: for a particle of mass m in a potential $V(x)$, the equation reads

$$i\hbar\frac{\partial}{\partial t}\psi(x,t) = \left(-\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} + V(x)\right)\psi(x,t). \tag{1.3}$$

The wavefunction $\psi(x,t)$ doesn't describe the particle's position directly. The absolute square of the wavefunction $|\psi(x,t)|^2$ is the probability density of finding the particle at position x at time t. Simultaneously, Werner Heisenberg developed a matrix mechanics representation of quantum mechanics, which was later shown to be equivalent to Schrödinger's wave mechanics representation.

Quantum mechanics grew in fame and became the most successful theory ever proposed. However, there were prominent scientists, Einstein included, who were unsatisfied with the implications of quantum theory. For example, quantum theory predicts the existence of entangled states (which we will discuss in detail in the next chapter), where the state of one particle is intimately linked to the state of another, independent of the distance between them.

Einstein famously referred to this as "spooky action at a distance." He, along with Podolsky and Rosen, proposed a thought experiment (now known as the EPR paradox) to argue that quantum mechanics must be incomplete. They predicted that there had to be some local hidden variables determining the outcomes behind the scenes, preserving locality and determinism. To resolve the paradox, John Bell (1964) formulated a test that any local hidden variable theory must satisfy. Quantum mechanics, on the other hand, was shown to violate these condi-

tions. Decades later, experiments confirmed these violations. This was the final nail in the coffin and strongly suggests that nature cannot be both local and real. Thus, quantum theory not only replaced Newtonian certainty with probabilistic outcomes — it also fundamentally changed our notions of reality, causality, information, and *computation*.

In Section 2.4, we delve into the idea of computation and what it means. For now, we think of computation as anything that we can do on anything ranging from a small calculator to a large supercomputer. The underlying principle is that all of these devices are based on classical mechanics. In 1982, Richard Feynman proposed the idea that to simulate quantum systems, a computer based on quantum principles might be more efficient [Fey82]. This led to the development of a universal quantum computer by David Deutsch in 1985 [Deu85]. A universal quantum computer could do anything a classical computer could do, with the 'potential' added advantages of quantum mechanics. In 1994 and 1996, two important algorithms called Shor's algorithm [Sho97] and Grover's algorithm [Gro96b] were proposed to solve the prime fractorization and unstructured search problems more efficiently than the best known classical algorithm for these problems. This was one of the earliest examples of the idea of 'quantum advantage.'

There are multiple different possible realizations of quantum computers that are based on different architectures. Examples include ion traps, neutral atoms, superconducting circuits, and photonics. Different research labs and companies have made significant progress towards universal scalable quantum computers. Note that in this thesis, we will focus on top-level discussions of algorithms and circuits that do not depend on the underlying quantum computer.

With this brief historical context in place, we now turn to the central focus of this thesis. This work is structured around three main pillars: distinguishability, symmetry, and energy estimation. In each of the corresponding chapters, we develop quantum algorithms to estimate relevant quantities and analyze their computational complexity. Furthermore, in each chapter, we formally introduce the concepts required and talk about the impact and applications of the chapter. Where appropriate, we include numerical simulations to illustrate the performance of these algorithms. The source code used for these simulations is available online.

Chapter 2

Mathematical preliminaries

The goal of this chapter is to present a brief introduction to a few different topics that are key to understanding the remainder of this thesis. In Section 2.1, we begin with an introduction to quantum computing and the different objects commonly used in any quantum computation. Following this, in Section 2.2, we talk about distance measures, like trace distance and fidelity. Next, in Section 2.3, we discuss group and representation theory, two seemingly abstract mathematical fields that are extremely relevant to real physical systems. In Section 2.4, we delve into complexity theory, which is all about classifying the difficulty of problems. Lastly, in Section 2.5, we discuss variational quantum algorithms, a paradigm of quantum computing that is more suited to devices available now and forms the basis of all the algorithms in this thesis.

2.1 The language of quantum computing

Quantum mechanics is spoken in the language of linear algebra. It is based on a set of postulates and is considered the most well-tested theory that explains the universe. The postulates of quantum mechanics specify the playground, the evolution, the measurement, and other key pillars to the theory. One important aspect of quantum mechanics that sets it apart from classical mechanics is that it is random. “Quantum mechanics is an inherently probabilistic theory," but what does this statement mean exactly? To satisfactorily answer this question, we first

begin with classical probability.

Consider a coin that may or may not be weighted. Let the probability of getting heads (H) be p. Since the total probability must be 1, the probability of tails (T) must be $1 - p$. For example, consider a coin that always lands with H facing up. This corresponds to $p = 1$, and we call such a coin **H**. Similarly, we define the all-tails coin, with $p = 0$, **T**. A system with two outcomes, like our coin, is called a **bit**.

We now give a geometric interpretation to this idea. Since a single parameter $0 \leq p \leq 1$ represents the coin, we use a one-dimensional vector (say pointing along the z-axis). Define $z = 2p - 1$, and any coin is represented as a vector with base at the origin and the other end at z. The extreme cases **H** and **T** are represented by Figure 2.1.

$$\begin{aligned} \mathbf{H} &\mapsto z = 1, \\ \mathbf{T} &\mapsto z = -1. \end{aligned} \tag{2.1}$$

But what about the points with $-1 < z < 1$? We now show that any biased/weighted coin can be represented as a **mixture** of **H** and **T** and has $-1 < z < 1$. A fair coin, with $p = 0.5$ is represented by an equal mixture, and the corresponding point on the line is the origin $z = 0$.

We now formalize what we mean by a "mixture." A general coin can be represented by

$$\mathbf{C} = p\mathbf{H} + (1 - p)\mathbf{T}, \tag{2.2}$$

which can be thought of as a weighted mixture of the endpoints. This equation is more general, but we can see it in action by substituting for **H** and **T** in terms of z. We see that for any coin

$$\begin{aligned} C &= p\mathbf{H} + (1 - p)\mathbf{T} \\ &\to p(1) + (1 - p)(-1) \\ &= 2p - 1 \\ &= z, \end{aligned} \tag{2.3}$$

as expected. Crucially, setting $p = 0.5$ ($z = 0$) gives the state

$$C_{\text{fair}} = 0.5\mathbf{H} + 0.5\mathbf{T}. \tag{2.4}$$

The coefficients p and $1 - p$ are probabilities themselves and are real numbers. Figure 2.2 shows this one-dimensional representation.

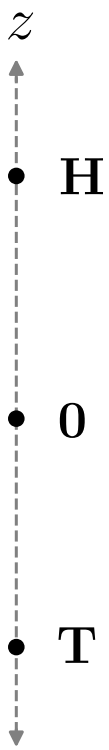


Figure 2.1: One-dimensional system representing a bit or a coin. $z = 1$ represents H, and $z = -1$ represents T, where $z = 2p - 1$.

Here is where we depart from classical probability and step into quantum mechanics. A quantum mechanical two-level system is called a **qubit**. A qubit no longer lives on a one-dimensional line, like a bit. A qubit lives somewhere in or on a sphere of radius one. This sphere is called the **Bloch sphere**. The North Pole is represented by $|H\rangle \equiv |0\rangle$, and the South Pole is represented by $|T\rangle \equiv |1\rangle$. This notation is called the Dirac braket notation, and is the de facto method to mathematically represent quantum states.

States on the surface of the sphere are called pure states, and states within the sphere are called mixed states. For now, we restrict ourselves to just pure states. Just like the surface of the globe, to label any point on the surface of a sphere, we need to specify two parameters, the latitude and longitude.

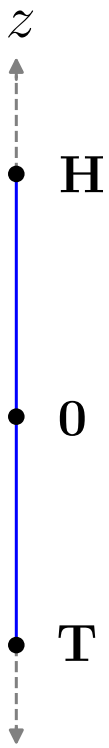


Figure 2.2: A classical bit, plotted as a one-dimensional system. All the points in blue represnt a valid biased coin.

Pure states are complex superpositions of the states $|0\rangle$ and $|1\rangle$. In other words, any pure state $|\psi\rangle$ can be written as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.5}$$

where α and β are complex numbers. Unlike classical bits, qubits need to be measured to figure out what state they are in, and this measurement affects the state of the qubit itself. For example, for the state $|\psi\rangle$ above, the probabilities for measuring (0) and (1) are given by

$$\begin{aligned} p(0) &= |\alpha|^2, \\ p(1) &= |\beta|^2, \end{aligned} \tag{2.6}$$

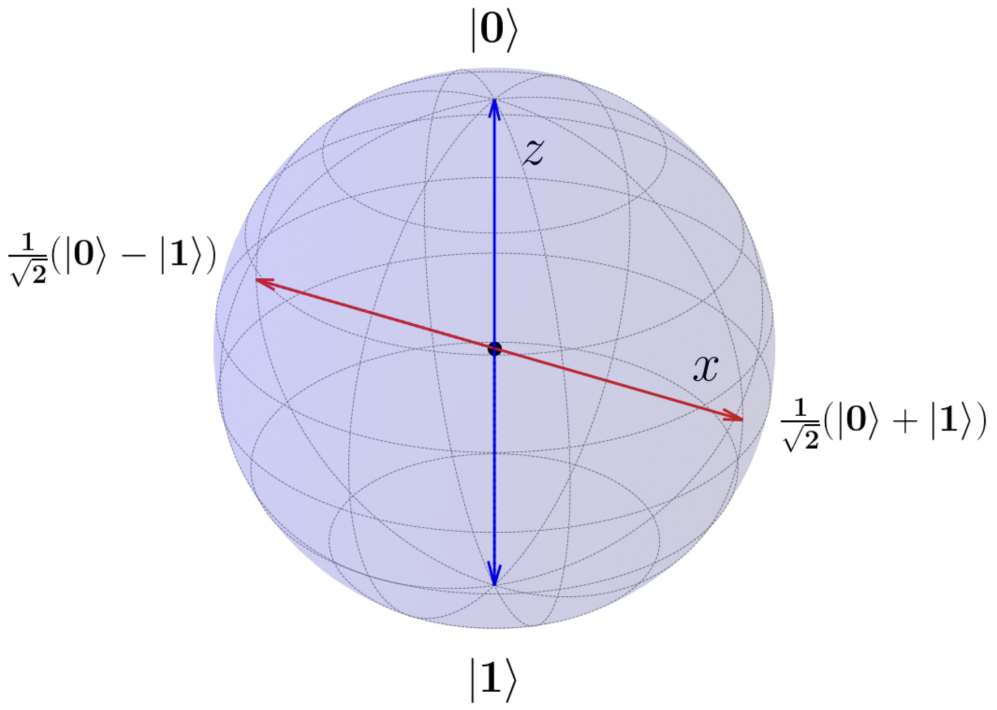


Figure 2.3: Bloch sphere with some special states labelled.

and after the measurement, the state 'collapses' to the state $|0\rangle$ or $|1\rangle$ depending on what outcome occurs. The coefficients α and β are not probabilities, but probability amplitudes.

In the case of the coin, the only relevant question is whether the side up is H or T. There is only 'one' question, which has two possible outcomes. The coin is **either** H **or** T side up. The key operative word here is "or." In sharp contrast, quantum mechanics allows us to ask an interesting variety of questions. For a qubit, one can pick any axis of interest and then measure the qubit along this axis, as opposed to just the z-axis for the classical case. There are still just two outcomes, which one can call 0 and 1, similar to H and T.

Consider the case where the state is given by

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{2.7}$$

When measured along the z-axis, the probabilities for both outcomes 0 and 1 can

be calculated using (2.6) and are both 0.5. This seems very similar to the state of a fair coin (2.4). However, we can now measure along the x-axis! Similar to $|0\rangle$ and $|1\rangle$ being the north and south poles along the z-axis, the corresponding poles along the x-axis turn out to be $|0\rangle_x \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|1\rangle_x \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Thus, the given state $|\psi\rangle$ is just

$$|\psi\rangle = |0\rangle_x \,. \tag{2.8}$$

Thus, measuring along this axis gives us 0 with unit probability! This is clearly different from the case of a fair coin. In this example, we say that the qubit is both 0 **and** 1 at the same time, since we are allowed to ask a different set of questions. Mathematically, we say that the state $|\psi\rangle$ is in a **superposition** of the states $|0\rangle$ and $|1\rangle$.

So what is the difference between a superposition and a mixture? A superposition of states is a "fixed" state in the sense that there exists a measurement that gives one of the outcomes with unit probability. Using the example above, measuring the $|0\rangle_x$ in the x direction gives 0 with unit probability. For other measurement directions, the outcome is not deterministic, like measuring in the z-direction. Unlike a superposition, a mixture of states always gives a non-deterministic outcome distribution. A mixture can be thought of as layering classical randomness on top of the inherent quantum randomness. We will soon see that a mixture of pure states leads to mixed states — states that are within the sphere and no longer on the surface.

Let us look at a concrete example that will help clarify some details. In scenario 1, consider a black box that outputs one of two states – the $|0\rangle$ state with probability 0.5, and the $|1\rangle$ state with probability 0.5. We are to measure the quantum state along the x-axis, and for each 0 we see, we add 1 to the total, and for each 1 we see, we add a -1 to the total. To simplify the calculations, we express $|0\rangle$ and $|1\rangle$ in terms of $|0\rangle_x$ and $|1\rangle_x$.

$$\begin{aligned} |0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_x + |1\rangle_x), \\ |1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_x - |1\rangle_x). \end{aligned} \tag{2.9}$$

The proability of measuring 0, using the law of total probability, is given by

$$p(0) = p(|0\rangle) * p(0\,||0\rangle) + p(|1\rangle) * p(0\,||1\rangle) = 0.25 + 0.25 = 0.5, \tag{2.10}$$

and the proability of measuring 1 is given by

$$p(1) = p(|1\rangle) * p(1\,||0\rangle) + p(|1\rangle) * p(1\,||1\rangle) = 0.25 + 0.25 = 0.5. \tag{2.11}$$

In the two equations above, we use the notation $p(i||j\rangle)$ to mean the probability of getting outcome i if the state is $|j\rangle$. Thus, the expected value is given by

$$\begin{aligned} & p(0) * 1 + p(1) * (-1) \\ & = 0.5 * 1 + 0.5 * (-1) \\ & = 0. \end{aligned} \tag{2.12}$$

In the second scenario, the box spits out the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ with unit probability. We still use the same procedure – measure the quantum state along the x-axis, and for each 0 we see, we add 1 to the total, and for each 1 we see, we add a -1 to the total. In this scenario, the input state is the $|0\rangle_x$ state. Thus, we always get 0 when we measure! Thus, the expected value is given by

$$\begin{aligned} & p(0) * 1 + p(1) * (-1) \\ & = 1 * 1 + 0 * (-1) \\ & = 1. \end{aligned} \tag{2.13}$$

Comparing (2.12) and (2.13), we see that a classical mixture of $|0\rangle$ and $|1\rangle$ and superposition of $|0\rangle$ and $|1\rangle$ are different objects! We leave it to the reader to try the same experiment but measure along the z-axis. In such a setting, the result of the two scenarios would be exactly the same. The ability to measure along the x-axis shows us a clear departure from the classical regime!

With this intuition in place, we now introduce the mathematical machinery of quantum mechanics. Quantum mechanics is built on the theory of linear algebra. Before we proceed, we assume that the reader understands the following non-exhaustive set of concepts – vectors, vector spaces, matrices, bases, inner products, eigenvectors, adjoints, functions of operators, trace of an operator, and tensor products. All of these topics can be found in any textbook on linear algebra, but we recommend [NC10, Section 2.1]. For ease of reference and notation, we summarize some of the notation in Table 2.1.

The postulates of quantum mechanics can be stated in two ways – for pure states and for mixed states. We begin with the pure state version since it is more digestible. However, the mixed state version is more complete, and we will jot them down as well.

Notation	Description
z^*	Complex conjugate of the complex number z.
$\|\psi\rangle$	Vector. Also known as a ket.
$\langle\psi\|$	Vector dual to $\|\psi\rangle$. Also known as a bra.
$\langle\phi\|\psi\rangle$	Inner product between the vectors $\|\phi\rangle$ and $\|\psi\rangle$
$\|\phi\rangle \otimes \|\psi\rangle$	Tensor product of $\|\phi\rangle$ and $\|\psi\rangle$
A^*	Complex conjugate of the A matrix
A^T	Transpose of the A matrix
$A^\dagger$	Hermitian conjugate of the A matrix, $A^\dagger = (A^T)^*$
$\langle\phi\|A\|\psi\rangle$	Inner product between $\|\phi\rangle$ and $A\|\psi\rangle$
$\mathrm{Tr}(A)$	Trace of the matrix A, the sum of the diagonal values

Table 2.1: Basic terms and descriptions. Table from [NC10, Section 2.1].

2.1.1 The postulates of quantum mechanics - pure states

1. Quantum states are unit vectors that belong to a **Hilbert space**. A Hilbert space is a vector space with an inner product defined on it (there are some more conditions, but they rarely appear, and we invite the interested reader to explore the conditions further). The condition that a quantum state $|\psi\rangle$ is a unit vector is represented as

$$\langle\psi|\psi\rangle = 1. \tag{2.14}$$

2. Quantum states evolve from one state to another by application of unitary operators. Unitary operators are operators that act on the underlying Hilbert space with $U^\dagger = U^{-1}$. This property of unitary operators preserves the length of a vector. Mathematically, if a state $|\psi\rangle$ evolves into state $|\phi\rangle$ under the operation of a unitary U, we denote this as

$$|\phi\rangle = U|\psi\rangle, \tag{2.15}$$

and

$$\begin{aligned}\langle\phi|\phi\rangle &= \langle\psi|U^\dagger U|\psi\rangle &(2.16)\\ &= \langle\psi|(U^{-1}U)|\psi\rangle &(2.17)\\ &= \langle\psi|\psi\rangle &(2.18)\\ &= 1. &(2.19)\end{aligned}$$

3. A measurement is a set of operators $\{M_m\}$ that obey the completeness condition —$\sum_m M_m^\dagger M_m = \mathbb{I}$. The different m values represent the different measurement outcomes possible, and M_m is the operator corresponding to the measurement outcome. A quantum measurement is inherently probabilistic, i.e., the particular outcome cannot be known beforehand. Furthermore, once measured, the quantum state collapses to a different state, which we call the post-measurement state. The probability of outcome m is given by

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle, \tag{2.20}$$

and if the outcome m occurs, the post-measurement state is given by

$$|\psi_m\rangle = \frac{1}{\sqrt{p(m)}} M_m |\psi\rangle . \tag{2.21}$$

We note that the completeness relation is just a recasting of the fact that $\sum_m p(m) = 1$.

4. Multiple systems can be thought of as a state in a tensor product Hilbert space. Consider two systems with states $|\psi_1\rangle$ and $|\psi_2\rangle$ that lie in their corresponding Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Then, the overall state of the two systems is given by $|\psi_1\rangle \otimes |\psi_2\rangle$ belonging to the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Let us re-examine the system we defined above – the qubit. A qubit is the smallest quantum mechanical system, and the underlying Hilbert space is a two-dimensional complex vector space $\mathcal{H}$. A qubit is represented by a column vector of two complex numbers

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}. \tag{2.22}$$

We know that there are infinitely many bases for this Hilbert space, but one of particular interest is called the computational basis, and most of quantum computing is expressed in the computational basis. It consists of two basis states we have already seen!

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.23}$$

Thus, any qubit can be written as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle . \tag{2.24}$$

Refer back to Figure 2.3 to see where $|0\rangle$ and $|1\rangle$ lie.

Quantum states evolve using unitary operators. We discuss unitary operators and their properties in Section 2.1.2. Unitary operators correspond to rotations, and this provides the intuition as to why they preserve lengths.

Lastly, we discuss measurements. We already saw an example of measurements along different axes, which we now put in the framework of postulate 3. A measurement along the z-axis is given by the measurement operator set M_z with operators

$$M_z = \{M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}. \tag{2.25}$$

Consider the scenario where we want to measure the quantum state $|0\rangle$ using M_z. The measurement probabilities and the post-measurement states are then

$$\begin{aligned} p(0) &= \langle 0| \left(|0\rangle\langle 0|^\dagger |0\rangle\langle 0|\right) |0\rangle && (2.26)\\ &= 1. && (2.27)\\ |\psi_0\rangle &= |0\rangle\,. && (2.28)\\ p(1) &= \langle 0| \left(|1\rangle\langle 1|^\dagger |1\rangle\langle 1|\right) |0\rangle && (2.29)\\ &= 0. && (2.30)\\ |\psi_1\rangle &= |1\rangle\,. && (2.31)\\ & && (2.32) \end{aligned}$$

This is a special case, and the outcome is always 0. If instead the input state is the $|+\rangle$, the measurement probabilities and the post-measurement states are then

$$\begin{aligned} p(0) &= \langle +| \left(|0\rangle\langle 0|^\dagger |0\rangle\langle 0|\right) |+\rangle && (2.33)\\ &= 0.5. && (2.34)\\ |\psi_0\rangle &= |0\rangle\,. && (2.35)\\ p(1) &= \langle -| \left(|1\rangle\langle 1|^\dagger |1\rangle\langle 1|\right) |-\rangle && (2.36)\\ &= 0.5. && (2.37)\\ |\psi_1\rangle &= |1\rangle\,. && (2.38) \end{aligned}$$

Lastly, we discuss two-qubit states and some two-qubit operators. From Postulate 4, we know that two-qubit states belong to the tensor product Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$. A simple example of a two-qubit state is $|0\rangle_1 \otimes |0\rangle_2$. For the sake of notational simplicity, this state is usually depicted as $|00\rangle$. Another important two-qubit state is the Bell state

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right). \tag{2.39}$$

This state is special in the sense that it is not factorable into two states $|\psi_1\rangle$ and $|\psi_2\rangle$ such that $|\Phi^+\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. To prove this, let $|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$ and let $|\psi_2\rangle = \gamma|0\rangle + \delta|1\rangle$. Using the properties of the tensor product, we see that

$$|\psi_1\rangle \otimes |\psi_2\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle. \tag{2.40}$$

For this state to be equal to $|\Phi^+\rangle$, we need

$$\alpha\gamma = \frac{1}{\sqrt{2}} \tag{2.41}$$

$$\alpha\delta = 0 \tag{2.42}$$

$$\beta\gamma = 0 \tag{2.43}$$

$$\beta\delta = \frac{1}{\sqrt{2}}, \tag{2.44}$$

which is impossible. States of this form, i.e., states that cannot be factored into individual states, are called **entangled** states. Entangled states play a vital role in quantum computing and information, and we will delve more into entangled states in a later section.

2.1.2 Hermitian and unitary operators

In this section, we discuss the properties of Hermitian and unitary operators, since they are of vital importance in quantum computing. Furthermore, we introduce several important Hermitian and unitary operators that appear often in quantum algorithms.

Hermitian matrices are those that are their own Hermitian conjugate, i.e., $H = H^\dagger$. Hermitian matrices have several important properties:

1. The eigenvalues of Hermitian operators are all real.
2. The eigenvectors of a Hermitian operator form a complete orthonormal basis.

Together, these properties allow for a spectral decomposition of any Hermitian operator H in terms of its eigenvalues and eigenvectors:

$$H = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|. \tag{2.45}$$

Furthermore, Hermitian operators can be measured by defining a measurement operator as follows:

$$M_H \coloneqq \{|\psi_i\rangle\langle\psi_i|\}_i. \tag{2.46}$$

An important class of Hermitian operators are the Pauli matrices:

$$X \equiv \sigma_X \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \tag{2.47}$$

$$Y \equiv \sigma_Y \coloneqq \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \tag{2.48}$$

$$Z \equiv \sigma_Z \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.49}$$

As discussed in Postulate 2 in Section 2.1.1, a unitary operator U has the property $UU^\dagger = \mathbb{I}$. Unitary operators preserve the length of vectors. Unitary operators can be generated from Hermitian operators via the matrix exponential

$$U = \exp(-\mathrm{i}H), \tag{2.50}$$

where H is a Hermitian operator. Using the above connection, corresponding to each Pauli matrix is a unitary operator:

$$R_X(\theta) \coloneqq \exp\left(-\mathrm{i}\frac{\theta}{2}X\right), \tag{2.51}$$

$$R_Y(\theta) \coloneqq \exp\left(-\mathrm{i}\frac{\theta}{2}Y\right), \tag{2.52}$$

$$R_Z(\theta) \coloneqq \exp\left(-\mathrm{i}\frac{\theta}{2}Z\right). \tag{2.53}$$

Using properties of the matrix exponential, we can show that

$$R_i(\theta) \coloneqq \exp\left(-\mathrm{i}\frac{\theta}{2}\sigma_i\right) = \cos\left(\frac{\theta}{2}\right)\mathbb{I} - \mathrm{i}\sin\left(\frac{\theta}{2}\right)\sigma_i, \tag{2.54}$$

where $i \in \{X, Y, Z\}$. Furthermore, we can show that its action on a qubit is to rotate it about the specified axis X, Y, Z, giving it its name.

An important example of a unitary operator is the Hadamard operator

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.55}$$

Its action on the computational basis is given by

$$|+\rangle \coloneqq H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{2.56}$$

$$|-\rangle \coloneqq H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{2.57}$$

which we already met as $|0\rangle_x$ and $|1\rangle_x$. These two states (the north and south poles along the x-axis) together form the Hadamard basis.

A common two-qubit gate is the CNOT gate. This gate flips the second qubit if the first qubit is in the state 1. Expanding, the action of the CNOT gate is written as:

$$\begin{aligned} \text{CNOT}_{12}|00\rangle &= |00\rangle \\ \text{CNOT}_{12}|01\rangle &= |01\rangle \\ \text{CNOT}_{12}|10\rangle &= |11\rangle \\ \text{CNOT}_{12}|11\rangle &= |10\rangle, \end{aligned} \tag{2.58}$$

where CNOT_{12} denotes a controlled-NOT gate using qubit 1 as the control and qubit 2 as the target.

2.1.3 The postulates of quantum mechanics - mixed states

In Section 2.1.1, we saw that a pure quantum state is a unit vector in a Hilbert space. If a system is represented by a pure state, we say that we have complete knowledge of the system. The measurement outcomes of any measurement, the evolution of the system, and other properties can be calculated using the pure state vector.

On the other hand, more realistically, a quantum system about which we only have partial knowledge is represented by a mixed state. This partial knowledge could arise from losing a part of a quantum system or some classical probabilistic ensemble, like the box spitting out quantum states in the previous section. The mixed state formalism is a method to combine all these 'uncertainties' about the quantum system into a single package. We will make this idea more concrete in this section.

Let us look back at the example of a box that spits out the quantum state $|\psi_i\rangle$ with some probability p_i. The box is then represented by an **ensemble** of quantum

states $\{(p_i, \psi_i)\}$. Let's say we would like to measure the output of the box using a measurement $\{M_m\}$. The probability of outcome m_j is given by

$$p(m_j) = \sum_i p(m_j|\psi_i) \times p_i \tag{2.59}$$

$$= \sum_i \langle\psi_i|M_j^\dagger M_j|\psi_i\rangle p_i \tag{2.60}$$

$$= \sum_i \mathrm{Tr}[M_j^\dagger M_j|\psi_i\rangle\langle\psi_i|]p_i \tag{2.61}$$

$$= \mathrm{Tr}\left[M_j^\dagger M_j \left(\sum_i p_i|\psi_i\rangle\langle\psi_i|\right)\right]. \tag{2.62}$$

Looking at this final equality, we see that all the information of the ensemble is present in this object within the regular brackets. This leads to a natural definition of the density operator to be the object

$$\rho \coloneqq \sum_i p_i|\psi_i\rangle\langle\psi_i|. \tag{2.63}$$

This is no longer a vector but is a matrix. What about the post-measurement state? If the input state was $|\psi_i\rangle$ and the outcome was m_j, the post-measurement state is

$$\left|\psi_{m_j}^i\right\rangle = \frac{1}{\sqrt{p(m_j|\psi_i)}} M_j \left|\psi_i\right\rangle. \tag{2.64}$$

So if the measurement outcome m_j occurred, we end up with an ensemble

$$\left\{\left(p(\psi_i|m_j), \left|\psi_{m_j}^i\right\rangle\right)\right\}. \tag{2.65}$$

The density matrix corresponding to this ensemble is thus

$$\rho_j = \sum_i p(\psi_i|m_j)|\psi_{m_j}^i\rangle\langle\psi_{m_j}^i| \tag{2.66}$$

$$= \sum_i p(\psi_i|m_j)\frac{1}{p(m_j|\psi_i)} M_j|\psi_i\rangle\langle\psi_i|M_j^\dagger. \tag{2.67}$$

Using the fact that

$$p(\psi_i|m_j) = \frac{p(\psi_i, m_j)}{p(m_j)} = \frac{p(m_j|\psi_i)p_i}{p(m_j)}, \tag{2.68}$$

the output density matrix is thus

$$\rho_j = \frac{1}{p(m_j)} \sum_i M_j |\psi_i\rangle\langle\psi_i| M_j^\dagger \tag{2.69}$$

$$= \frac{M_j \rho M_j^\dagger}{\mathrm{Tr}[M_j^\dagger M_j \rho]}. \tag{2.70}$$

We note that the special case of a pure state $|\psi\rangle$ is represented by a deterministic ensemble of the form $\{(1.0, |\psi\rangle)\}$, and the corresponding density operator is $\rho = |\psi\rangle\langle\psi|$.

The 'revised' postulates of quantum mechanics that include mixed states are as follows:

1. Quantum states are represented by density operators/matrices, which are positive matrices with unit trace. Mathematically, the conditions on a density operator are

$$\rho \geq 0 : \text{Positivity} \tag{2.71}$$

$$\mathrm{Tr}[\rho] = 1 : \text{Unit Trace.} \tag{2.72}$$

2. Quantum states evolve from one state to another by application of unitary operators. Mathematically, if a state ρ evolves into state ω under the operation of a unitary U, we denote this as

$$\omega = U \rho U^\dagger. \tag{2.73}$$

3. A measurement is a set of operators $\{M_m\}$ that obey the completeness condition —$\sum_m M_m^\dagger M_m = \mathbb{I}$. The different m values represent the different measurement outcomes possible, and M_m is the operator corresponding to the measurement outcome. A quantum measurement is inherently probabilistic; i.e., the particular outcome cannot be known beforehand. Furthermore, once measured, the quantum state collapses to a different state, which we call the post-measurement state. The probability of outcome m is given by

$$p(m) = \mathrm{Tr}[M_m^\dagger M_m \rho], \tag{2.74}$$

and if the outcome m occurs, the post-measurement state is given by

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\mathrm{Tr}[M_m^\dagger M_m \rho]}. \tag{2.75}$$

We note that the completeness relation is just a recasting of the fact that $\sum_m p(m) = 1$.

4. Multiple systems can be thought of as a state in a tensor product Hilbert space. Consider two systems with states ρ_1 and ρ_2 that belong to the set of operators that act on their corresponding Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Then, the overall state of the two systems is given by $\rho_1 \otimes \rho_2$, which acts on the tensor product Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Finally, we are in a position to fully investigate the quantum box example from before. The first scenario was a box that spits out one of the two states $\{|0\rangle, |1\rangle\}$, with equal probability, and we measure along the x-axis. With our new knowledge of density matrices, we know that the density matrix for this box is given by

$$\rho = 0.5 \cdot |0\rangle\langle 0| + 0.5 \cdot |1\rangle\langle 1|, \tag{2.76}$$

and the measurement is given by $\{M_0 = |+\rangle\langle +|, M_1 = |-\rangle\langle -|\}$. Thus, the probabilities are

$$\begin{aligned} p(0) &= \mathrm{Tr}[M_0^\dagger M_0 \rho] && (2.77)\\ &= 0.5, && (2.78)\\ p(1) &= \mathrm{Tr}[M_1^\dagger M_1 \rho] && (2.79)\\ &= 0.5, && (2.80) \end{aligned}$$

which agrees with our derivation before. On the other hand, the second scenario has the density matrix $|+\rangle\langle +|$, and the measurement probabilities are

$$\begin{aligned} p(0) &= \mathrm{Tr}[M_0^\dagger M_0 |+\rangle\langle +|] && (2.81)\\ &= 1.0, && (2.82)\\ p(1) &= \mathrm{Tr}[M_1^\dagger M_1 |+\rangle\langle +|] && (2.83)\\ &= 0.0, && (2.84) \end{aligned}$$

again agreeing with our previous derivation.

The state $\pi := \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ is a special qubit state called the maximally mixed state, and in the Bloch sphere it is represented by the center of the sphere. We leave it as an exercise to show that the maximally mixed state can be realized by an equal mixture of any pair of poles on the sphere. An example of this is that

$$\{(0.5, |0\rangle\langle 0|), (0.5, |1\rangle\langle 1|)\} \equiv \pi = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \tag{2.85}$$

$$\{(0.5, |+\rangle\langle +|), (0.5, |-\rangle\langle -|)\} \equiv \pi = \frac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|). \tag{2.86}$$

Thus, both of these ensembles lead to the exact same measurement outcomes and are indistinguishable from each other.

Looking now at Figure 2.4, we now see that pure states are states that are on the surface of the sphere, and the state of the system is perfectly known. On the other hand, mixed states are inside the sphere, and the state is not exactly known, with the extreme case being the maximally mixed state at the center.

Another important characterization of mixed states is in the form of purifications. Any mixed state ρ_A can be expressed as a subsystem of a larger pure state ψ_{RA}. In other words:

$$\rho_A = \mathrm{Tr}_R[|\psi\rangle\langle\psi|]_{RA}. \tag{2.87}$$

This further solidifies the idea that mixed states represent incomplete knowledge of a quantum system.

2.1.4 Studying subsystems

The density matrix allows us to incorporate classical mixtures into the model that we use. However, the biggest advantage of the density matrix model is the study of subsystems. Consider a quantum state ρ_{AB} that is shared by two parties, Alice and Bob. An important question in such a scenario is to find the measurement statistics when Alice, or Bob, measures their share of the quantum state ρ_{AB}.

Concretely, consider the case where Alice measures her share of the system using the measurement operator $M = \{M_m\}$. Thus, the overall measurement is given by

$$M'_m = \{M_m^A \otimes \mathbb{I}^B\}, \tag{2.88}$$

which we argue is the intuitive idea that Alice locally measuring her system does nothing to Bob's system, represented by the identity operator $\mathbb{I}^B$. Thus, the measurement probabilities are given by

$$p(m) = \mathrm{Tr}[(M'_m)^\dagger M'_m \rho_{AB}] \tag{2.89}$$

$$= \mathrm{Tr}[((M_m^A)^\dagger \otimes \mathbb{I}^B)(M_m^A \otimes \mathbb{I}^B)\rho_{AB}]. \tag{2.90}$$

The trace operation, which is the sum of diagonal elements, for a two-system operator X_{AB} is given by

$$\mathrm{Tr}[X_{AB}] = \sum_i \sum_j \langle i|_A \langle j|_B X_{AB} |i\rangle_A |j\rangle_B. \tag{2.91}$$

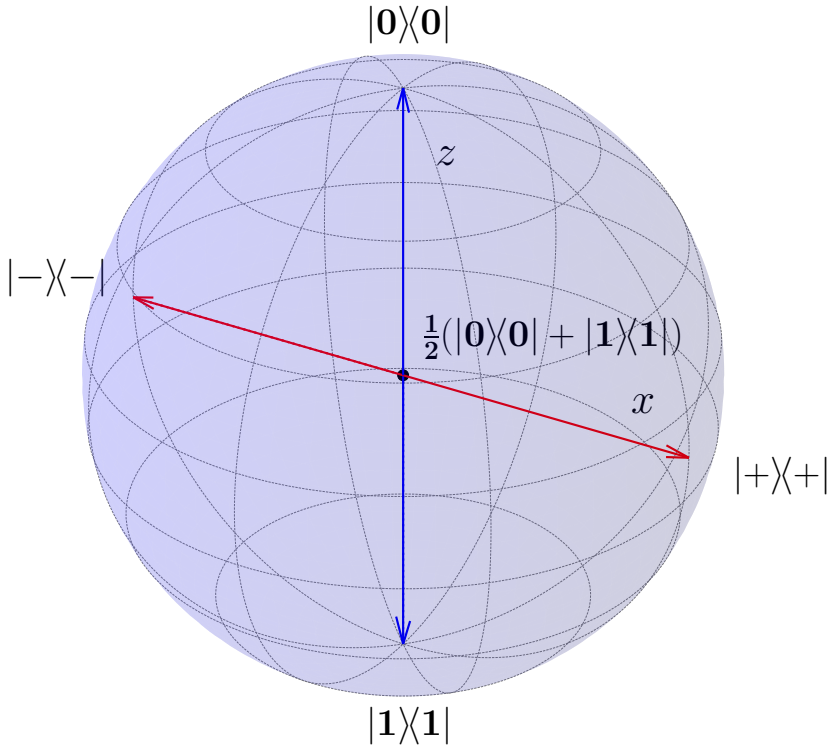


Figure 2.4: Bloch sphere - mixed states.

We now define the partial trace operation with respect to system B to be

$$\mathrm{Tr}_B[X_{AB}] := \sum_j (\mathbb{I}_A \otimes \langle j|_B) X_{AB} (\mathbb{I}_A \otimes |j\rangle_B). \tag{2.92}$$

This is very similar to the usual trace operation, with the main difference being that we only trace over the B index j. Using this new notation, we see that the overall trace can be written as a combination of the two partial traces

$$\mathrm{Tr}[X_{AB}] = \mathrm{Tr}_A[\mathrm{Tr}_B[X_{AB}]]. \tag{2.93}$$

Thus, the probabilities $p(m)$ are given by

$$p(m) = \mathrm{Tr}_A[\mathrm{Tr}_B[((M_m^A)^\dagger \otimes \mathbb{I}^B)(M_m^A \otimes \mathbb{I}^B)\rho_{AB}]] \tag{2.94}$$
$$= \mathrm{Tr}_A[(M_m^A)^\dagger M_m^A \,\mathrm{Tr}_B[\rho_{AB}]], \tag{2.95}$$

where the second equality can be arrived at by using the definition of the partial trace Tr_B. Using this equation as a hint, we define the reduced density matrix ρ_A to be

$$\rho_A \coloneqq \mathrm{Tr}_B[\rho_{AB}], \tag{2.96}$$

and the measurement statistics are given by

$$p(m) = \mathrm{Tr}_A[(M_m^A)^\dagger M_m^A \,\rho_A]. \tag{2.97}$$

This equation only depends on the system in Alice's possession. We argue that the partial trace operation Tr_B gives a description of the state of the qubit in Alice's possession. While this intuition given above is not a direct proof, we encourage the reader to read the entire proof here [NC10, Box 2.6].

Let us look at an interesting example of calculating the reduced operator of the Bell state

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}), \tag{2.98}$$

with the corresponding density operator

$$\Phi_{AB}^+ \coloneqq |\Phi^+\rangle\langle\Phi^+|_{AB} \tag{2.99}$$
$$= \frac{1}{2}[|00\rangle\langle 00|_{AB} + |00\rangle\langle 11|_{AB} + |11\rangle\langle 00|_{AB} + |11\rangle\langle 11|]. \tag{2.100}$$

Since this is a pure state, this means that the overall state is exactly known. Now, let us look at Alice's subsystem, given by $\rho_A \coloneqq \mathrm{Tr}_B[\Phi_{AB}^+]$.

$$\rho_A = \mathrm{Tr}_B[\Phi_{AB}^+] \tag{2.101}$$
$$= \sum_j (\mathbb{I}_A \otimes \langle j|_B)\Phi_{AB}^+(\mathbb{I}_A \otimes |j\rangle_B) \tag{2.102}$$
$$= (\mathbb{I}_A \otimes \langle 0|_B)\Phi_{AB}^+(\mathbb{I}_A \otimes |0\rangle_B) + (\mathbb{I}_A \otimes \langle 1|_B)\Phi_{AB}^+(\mathbb{I}_A \otimes |1\rangle_B) \tag{2.103}$$
$$= \frac{1}{2}(|0\rangle\langle 0|_A + |1\rangle\langle 1|_A) \tag{2.104}$$
$$= \pi_A, \tag{2.105}$$

which is the maximally mixed state! Alice's subsystem is maximally mixed, which means the state of her subsystem is not perfectly known. To reiterate, the full state $|\Phi^+\rangle$ is a pure state and is perfectly known, but her reduced state is maximally mixed and is not known! This is a key signature of quantum entanglement – the global state is known, but the local states are not.

2.1.5 Quantum channels

As seen in previous sections, pure states represent complete knowledge of a system, and mixed states represent incomplete knowledge. Furthermore, any mixed state can be written as an ensemble, or a convex combination of pure states.

In this section, we elevate unitaries using the same idea to **quantum channels**. Unitaries represent 'pure' evolution, and quantum channels represent noisy evolution. For an in-depth analysis of quantum channels, refer to [Wil17]. Quantum channels are all-encompassing, in the sense that state preparation, noisy or noiseless evolution, and measurement can all be represented as quantum channels.

A quantum channel is usually represented by a curly alphabet like $\mathcal{N}_{A\to B}$, with A and B being the input and output Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Sometimes we drop the system labels if it is clear from the context. A general map needs to satisfy several properties to be a valid quantum channel. These properties arise from the condition that when a valid quantum state is inputted, the output must also be a valid quantum state. The conditions are as follows:

1. Linearity - $\mathcal{N}(\alpha\rho + \beta\sigma) = \alpha\mathcal{N}(\rho) + \beta\mathcal{N}(\sigma)$.
2. Trace Preservation - $\mathrm{Tr}[\mathcal{N}(\rho)] = \mathrm{Tr}[\rho]$.
3. Complete Positivity - $(\mathbb{I}_R \otimes \mathcal{N}_A)\rho_{RA} \geq 0$, for all systems R.

Any quantum channel $\mathcal{N}$ can be written in the Kraus representation as follows:

$$\mathcal{N}_{A\to B}(\cdot) \coloneqq \sum_{i=1}^{k} K_i(\cdot)K_i^\dagger, \tag{2.106}$$

with the condition that

$$\sum_{i=1}^{k} K_i^\dagger K_i = \mathbb{I}. \tag{2.107}$$

The special case where $k = 1$ is the channel

$$\mathcal{N}(\rho) = K_1 \rho K_1^\dagger, \tag{2.108}$$

with $K_1^\dagger K_1 = \mathbb{I}$, implying that K_1 is an isometry. Thus, unitary evolution is represented by a quantum channel with a single Kraus operator. This is reminiscent of pure states being represented by ensembles with a single state with unit probability.

The Stinespring dilation theorem states that any quantum channel $\mathcal{N}$ can be thought of as unitary evolution of a larger system. More concretely,

$$\mathcal{N}_A(\rho_A) = \mathrm{Tr}_R[U_{RA}(\rho_A \otimes |0\rangle\langle 0|_R)(U_{RA})^\dagger], \tag{2.109}$$

where U is a unitary operator on the larger Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_R$. This idea is very similar to the purification idea of mixed states from (2.87).

2.1.6 Quantum circuit diagrams

Any quantum computation can be thought of as time-ordered operations involving input states, unitary gates, and final measurements. These algorithms can always be written down and analyzed using long equations using the Dirac braket notation. However, an equivalent but much more intuitive model of computation is quantum circuit diagrams.

Quantum circuit diagrams provide us with a quick, succinct method to represent quantum computations and are similar to classical circuit diagrams that represent classical computation. Let us look at some classic examples to get an idea of how to use quantum circuits.

Consider the preparation of the Bell state, which we saw to be

$$\begin{aligned} \left|\Phi^+\right\rangle &= \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right) \\ &= \mathrm{CNOT}_{12}\, H_1\, |00\rangle_{12}\,. \end{aligned} \tag{2.110}$$

This equation is more easily understood from the circuit diagram in Figure 2.5. Note that the figure has time running from left to right, whereas the equation has time running from right to left.

Another example we have seen before is a measurement in the z-axis of the $|+\rangle$ state. This is represented in Figure 2.6.

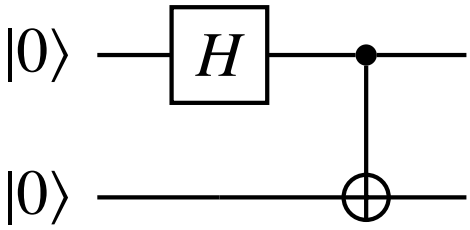


Figure 2.5: Bell-state preparation quantum circuit.

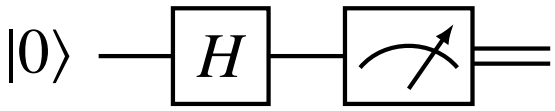


Figure 2.6: Quantum circuit for measuring the $|+\rangle$ state in the z-basis

2.2 Distance measures

In this section, we discuss various distance measures that are commonly used to compare quantum states, channels, and other objects. These measures give us a way to quantify how similar/different two objects are and are often the important metrics for the success of quantum computation. For example, given a protocol to prepare a quantum circuit and a physical realization of the circuit, how different are the outputs?

In this section, we describe and discuss several important measures, which all stem from two base quantities – the fidelity F and the trace distance $\|\cdot\|_1$.

Definition 2.1 [*Normalized Trace Distance*]. *The normalized trace distance between two states ρ and σ is denoted by*

$$\frac{1}{2}\|\rho - \sigma\|_1, \tag{2.111}$$

where $\|X\|_1$ is called the trace norm and is defined as

$$\|X\|_1 \coloneqq \mathrm{Tr}\left[\sqrt{X^\dagger X}\right]. \tag{2.112}$$

The trace distance between two states can be intuitively thought of as how different two states are. This intuition is useful in deriving several properties of the trace distance and the trace norm [Wil17]. We summarize some of the important ones here.

1. **Non-negativity** - $\|X\|_1 \geq 0$ and $\|X\|_1 = 0 \iff X = 0$.
2. **Triangle Inequality** - $\|X + Y\|_1 \leq \|X\|_1 + \|Y\|_1$.
3. **Unitary Invariance** - $\|\rho - \sigma\|_1 = \|U\rho U^\dagger - U\sigma U^\dagger\|_1$. This further proves that unitaries represent 'pure' evolutions, as discussed in Section 2.1.5. The distance of two states cannot change under a unitary operation.
4. **Data Processing** - Given a quantum channel $\mathcal{N}$, $\|\mathcal{N}(\rho) - \mathcal{N}(\sigma)\|_1 \leq \|\rho - \sigma\|_1$. Again, as discussed in Section 2.1.5, quantum channels are noisy evolutions and can only make two states more indistinguishable.

The trace distance has an operational interpretation in terms of a hypothesis-testing game. Say Alice picks one of two states, ρ_0 and ρ_1 with equal probability $p(0) = p(1) = 0.5$. Let X be the random variable associated with this choice. She then gives the chosen state to Bob, who has to perform a measurement $\Lambda = \{\Lambda_0, \Lambda_1\}$ and guess which state was prepared. The output guess is associated with the random variable Y. The success probability, using the total probability theorem and the measurement postulate 3 from 2.1.3, is given by

$$\begin{aligned} p_{\text{succ}}(\Lambda) &= p_{Y|X}(0|0)p_X(0) + p_{Y|X}(1|1)p_X(1) \\ &= \frac{1}{2}\left(\text{Tr}[\Lambda_0\rho_0] + \text{Tr}[\Lambda_1\rho_1]\right). \end{aligned} \tag{2.113}$$

Simplifying, this can be shown to be

$$p_{\text{succ}}(\Lambda) = \frac{1}{2}\left(1 + \text{Tr}[\Lambda_0(\rho_0 - \rho_1)]\right). \tag{2.114}$$

Bob, however, has freedom in choosing the measurement Λ, and thus, the optimal success probability is given by

$$\begin{aligned} p_{\text{succ}} &\coloneqq \max_{\Lambda} p_{\text{succ}}(\Lambda) \\ &= \frac{1}{2}\left(1 + \frac{1}{2}\|\rho_0 - \rho_1\|_1\right), \end{aligned} \tag{2.115}$$

where the last equality is due to another property of the trace distance, which states that the trace distance can be thought of as a probability difference [Wil17, Section 9.1.3]. If two states were the same, then the success probability is exactly 0.5 and Bob's optimal strategy is to pick randomly. However, if the states are perfectly distinguishable, the normalized trace distance has a value of 1, and so does the success probability.

A related quantity is the diamond distance of channels, based on the diamond norm. It measures the distance between two quantum channels and is based on the trace distance. Similar to the game above, consider the scenario where Alice sends a state ρ_A to Bob. Bob then picks one of two channels, $\mathcal{N}_{A\to B}$ or $\mathcal{M}_{A\to B}$, with equal probability and applies it to the state ρ_A. Bob then sends the state back to Alice, who has to decide which channel was used. Using the same reasoning as before, Alice's success probability is

$$\frac{1}{2}\left(1+\frac{1}{2}\|\mathcal{N}_{A\to B}(\rho_A)-\mathcal{M}_{A\to B}(\rho_A)\|_1\right). \tag{2.116}$$

However, Alice has the choice of the input state ρ_A. Furthermore, she can further improve her chances by sending one share of an entangled state. This leads to the definition as follows:

Definition 2.2 [*Normalized Diamond Distance*]. *The diamond distance of two channels $\mathcal{N}_{A\to B}$ and $\mathcal{M}_{A\to B}$ is given by*

$$\|\mathcal{N}_{A\to B}-\mathcal{M}_{A\to B}\|_\diamond := \max_{|\psi\rangle_{RA}} \|\mathcal{N}_{A\to B}(|\psi\rangle\langle\psi|_{RA})-\mathcal{M}_{A\to B}(|\psi\rangle\langle\psi|_{RA})\|_1\,, \tag{2.117}$$

where the size of the reference system R is equal to that of system A.

Next, we define the fidelity of two quantum states and some properties.
Definition 2.3 [*Fidelity*]. *The Uhlmann fidelity of two quantum states ρ_A and σ_A is given by*

$$F(\rho_A,\sigma_A) := \|\sqrt{\rho_A}\sqrt{\sigma_A}\|_1^2. \tag{2.118}$$

The fidelity is intuitively a measure of closeness of states and has the following non-exhaustive list of properties:

1. **Symmetry** - $F(\rho,\sigma)=F(\sigma,\rho)$.
2. **Bounds** - $0\leq F(\rho,\sigma)\leq 1$. The upper bound is met if and only if the states are equal.

3. **Pure states** - For pure states, the fidelity reduces to the overlap $F(\psi, \phi) = |\langle\psi|\phi\rangle|^2$.
4. **Alternate characterization** - The fidelity can be expressed as a maximization over unitaries acting on the purifying subsystem

$$F(\rho_A, \sigma_A) = \max_{U_R} |\langle\phi^\rho|_{RA} U_R \otimes \mathbb{I}_A |\phi^\sigma\rangle_{RA}|^2, \tag{2.119}$$

   where $|\phi^\rho\rangle$ and $|\phi^\sigma\rangle$ are purifications of ρ and σ, respectively.
5. **Unitary Invariance** - $F(\rho, \sigma) = F(U\rho U^\dagger, U\sigma U^\dagger)$. This further proves that unitaries represent 'pure' evolutions, as discussed in Section 2.1.5. The closeness of two states cannot change under a unitary operation.
6. **Data Processing** - Given a quantum channel $\mathcal{N}$, $F(\rho, \sigma) \leq F(\mathcal{N}(\rho), \mathcal{N}(\sigma))$. Again, as discussed in Section 2.1.5, quantum channels are noisy evolutions and can only make two states closer.
7. **Measurement Fidelity** - There is an optimal measurement such that the quantum fidelity is equal to the classical fidelity of the resulting distribution.

$$F(\rho, \sigma) = \min_{\{\Lambda_x\}} \left[\sum_x \sqrt{\mathrm{Tr}[\Lambda_x \rho]\, \mathrm{Tr}[\Lambda_x \sigma]} \right]^2. \tag{2.120}$$

Similar to the diamond distance of channels, we define the channel fidelity here.

Definition 2.4 [*Channel fidelity*]. *The channel fidelity of two channels $\mathcal{N}_{A\to B}$ and $\mathcal{M}_{A\to B}$ is given by*

$$F(\mathcal{N}_{A\to B}, \mathcal{M}_{A\to B}) \coloneqq \min_{|\psi\rangle_{RA}} F(\mathcal{N}_{A\to B}(|\psi_{RA}\rangle\langle\psi_{RA}|), \mathcal{M}_{A\to B}(|\psi_{RA}\rangle\langle\psi_{RA}|)), \tag{2.121}$$

and is a measure of the closeness of two channels.

2.3 Group and representation theory

In the previous sections, we learned the language of quantum mechanics and quantum computing. The key playground was a Hilbert space – an inner product vector space – and the objects living in them, state vectors. In this section, we

study another set of mathematical objects called **groups**. Groups have a different underlying structure as compared to vector spaces. Furthermore, we will explore a brief introduction to representation theory, which will help us connect group theory and our quantum systems.

Before we get into the mathematical prescription of group theory, let us look at an illuminating example. Consider an equilateral triangle with points labelled A, B, and C. We now ask the question – what operations can be done to this triangle such that it is unchanged? For example, rotating it counterclockwise by 120° gives the same triangle with just the points renamed. Let us call this operation r.

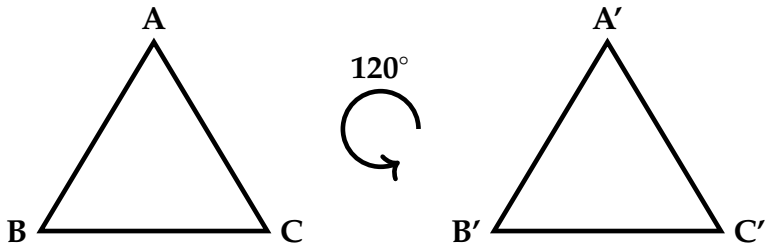


Figure 2.7: Operation r that rotates a triangle counterclockwise by 120°.

Another symmetry of the triangle is flipping it across the vertical dotted line. We call this operation f.

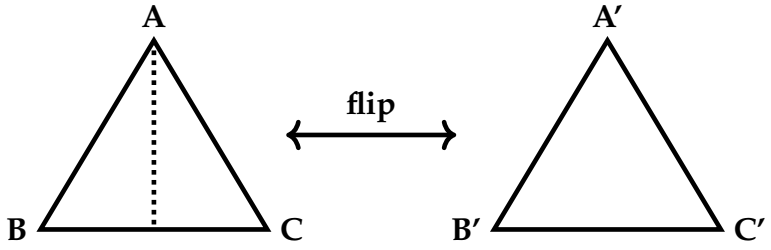


Figure 2.8: Operation f that flips a triangle about its vertical axis.

It turns out that all possible symmetries of the triangle can be expressed as combinations of the two operations f and r. We now list all the operations and the orientation of the points A, B, and C after the operation, starting from the top, then the left, and then the right point. Note that r^2 refers to doing the r operation twice, and rf refers to doing the f operation first followed by the r operation.

1. $e - ABC \to ABC$.

2. $r - ABC \to CAB$.
3. $r^2 - ABC \to BCA$.
4. $f - ABC \to ACB$.
5. $fr - ABC \to CBA$.
6. $fr^2 - ABC \to BAC$.

These six operations $\{e, r, r^2, f, fr, fr^2\}$ are the symmetries of the equilateral triangle. The element e is a special element called the identity element and denotes the 'do nothing' operation. Another interesting fact is that every single operation has a corresponding inverse operation – doing an operation followed by its inverse is the same as doing nothing, i.e., the e operation. For example, the inverse of the r operation is r^2, since $r^2 \circ r = r^3 = e$, since rotating thrice by 120° is the same as not rotating at all. Similarly, the inverse of f is just itself, since $f \circ f = f^2 = e$. Lastly, any combination of these symmetry elements is also a symmetry and thus belongs to the set. For example, consider rfr^2f^2 which can be simplified as

$$\begin{aligned} r^2fr^2f^2 &= r^2fr^2\underline{f^2} \\ &= rr\underline{f}fr^2 \\ &= r\underline{f}r^2r^2 \\ &= f\underline{r^2r^2r^2} \\ &= f, \end{aligned} \tag{2.122}$$

where we use the fact that $rf = fr^2$.

Let us now generalize these ideas to general sets and operations on them. Group theory is the study of a set of objects and an associated operation, called multiplication, that obeys certain properties. A set G, with the binary operation $*$, is a group if the following hold true:

1. Closure - $\forall g_1, g_2 \in G$, $g_1 * g_2 \in G$.
2. Associativity - $\forall g_1, g_2, g_3 \in G$, $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$.
3. Identity - $\forall g \in G$, $g * e = e * g = g$.
4. Inverse - $\forall g \in G$, there exists an inverse g^{-1} such that $g * g^{-1} = e$.

We often suppress the operation $*$ if it is clear from context. While the set of rules seems minimal, they significantly restrict what is considered a group and impose strong conditions and properties. Let us look at one example of such a property.

Theorem 2.1 [*Group Rearrangement Theorem*]. *Let $G = \{g_1, g_2, \ldots, g_k\}$ be a group, and let a be a member of the same group G. Then, the set of elements $H = \{ag_1, ag_2, \ldots, ag_k\}$ are just a rearrangement of the elements in G.*

Proof. First, we show that all the elements of G are in H. Pick an arbitrary element g from G. Consider the following:

$$\begin{aligned} g &= g, \\ &= a(a^{-1}g), \\ &= aa_l, \end{aligned}$$

where $a_l = a^{-1}g$ must belong to G using the closure property. From the definition of H, we see that aa_l is an element in H. Thus, for element $g \in G$, there exists a corresponding element $aa_l \in H$. We also need to show that they map to unique elements, which we do by contradiction. Consider two elements in H, aa_m and aa_n, such that $aa_m = aa_n$. Left multiplying by a^{-1}, we see that $a_m = a_n$, which is not allowed since the elements of G are unique. Thus, left (or right) multiplying the elements of a group with another element amounts to a reordering of the elements. ■

Group theory is the study of theoretical mathematical objects and their relationships with each other. To map them to something more concrete, we turn to representation theory. More specifically, in this work, we restrict ourselves to unitary representation theory, and we use representation theory to mean unitary representation theory. This allows us to study the physical action of groups on physical systems, like qubits.

Representation theory is the study of mapping elements of a group to unitary operations on a Hilbert space such that the rules of the group operation $*$ are obeyed. More concretely, a representation ϕ of a group G on a vector space V is defined as a function $\phi : G \to U(V)$ that preserves the action of the group such that

$$\begin{aligned} \phi(g)\,\phi(h) &= \phi(g * h) \\ \phi(e) &= \mathbb{I}, \end{aligned} \tag{2.123}$$

for all group elements $g, h \in G$. Here $U(V)$ is the set of unitary operators acting on

the vector space V. Let us look at a simple example that helps flesh out some of these ideas.

Consider the simplest non-trivial group called $\mathbb{Z}_2$. This group consists of two elements $\{e, f\}$, such that $ee = e$, $ef = f$, $fe = f$, and $f^2 = e$. We now connect this abstract group to a physical system of interest, the qubit. Consider the following unitary representation ϕ:

$$\phi(e) = \mathbb{I}, \phi(f) = X. \tag{2.124}$$

We know that

$$\begin{aligned}
\phi(e)\phi(f) &= \mathbb{I}X, \\
&= X, \\
&= \phi(f) \\
&= \phi(e * f), \\
\phi(f)\phi(f) &= X \times X, \\
&= I, \\
&= \phi(e) \\
&= \phi(f * f).
\end{aligned}$$

The other two relations, $\phi(e)\phi(e)$ and $\phi(f)\phi(e)$, can be shown similarly. Thus, this function ϕ is a valid unitary representation. Another example is the two-qubit unitary representation $\omega : \mathbb{Z}_2 \to U(\mathcal{H}^2)$ of the group $\mathbb{Z}_2$ with the following mapping:

$$\phi(e) = \mathbb{I}, \phi(f) = \text{CNOT}\,. \tag{2.125}$$

The same properties can be shown for this representation. As discussed earlier, representations give us a way to connect abstract mathematical groups to real quantum systems.

2.4 Complexity theory

Computation is the process of performing calculations or solving problems with a specific set of steps or instructions. Computation is ubiquitous in our world, ranging from small calculators to large-scale supercomputers. The notion of what is computable depends on a specific 'model' of computation. Historically, there have been many models, but Turing machines, described by Alan Turing, have

become the foundational model. While the exact description of a Turing machine is not relevant here, the main takeaway of the model is the Church-Turing thesis, which states that "any real-world computation can be translated into an equivalent computation on a Turing machine." Turing machines capture the essence of computation and became the benchmark using which problems are studied and classified.

Complexity theory builds on this framework of Turing machines to study the efficiency of a particular computation. The idea is to quantify how long (time complexity) and how much memory (space complexity) are required to solve a problem. Before we go ahead, we assume the reader to be familiar with Big-O notation. A short summary can be found in Appendix A. Complexity theory uses the asymptotic growth of the time and space requirements of an algorithm to classify them into classes of problems. All problems within a class can be thought of as having similar complexity or difficulty. Let us look at some interesting examples.

The class of problems **P** (polynomial-time) is the set of problems for which there exists a polynomial-time algorithm that solves the problem. More concretely, this means that there exists an algorithm that solves the problem whose runtime is polynomial in the input size. The polynomial involved can be of any degree. Any example of a **P** problem is sorting a list. Merge sort has a time complexity of $n \log n$, where n is the size of the list.This means that it has polynomial time complexity, since $n \log n = O(n^2)$. Problems in **P** are considered classically efficient problems.

Another important class of problems called **NP** (nondeterministic polynomial-time problems) is the set of problems for which there exists a polynomial-time verification strategy. Intuitively, the class consists of problems that can be efficiently solved when assisted by a powerful 'prover' who provides a 'proof' (solution) that can be efficiently verified. The "subset sum problem" is an example of an **NP** problem – Given a set of numbers, is there a subset that adds up to a specific target value? It is easy to check a possible solution; just add up the entries in that solution and compare. However, finding a solution can be very difficult for large sets.

However, the landscape dramatically changed with the conception of the idea of quantum computers. Turing machines are classical devices and are 'limited' by the laws of classical physics. The model of computation was thus modified to include models that incorporate quantum mechanics. While several models were proposed and shown to be equivalent, the prevalent model is the quantum

circuit model. An excellent review of quantum complexity theory can be found here [BV97, Wat09a]. We now go over a brief overview of the important features of quantum computational complexity theory and the different classes of problems.

Before we go into the important classes, we define two concepts that will be essential – 'hardness' and 'completeness'. A problem is said to be hard for a computational class if it is at least as hard to solve as the hardest problem of the class. A problem is complete for a class if it is hard for the class, and additionally, belongs to the class. A property of complete problems is that every other problem in the class can be efficiently mapped to a complete problem. In other words, the ability to solve a complete problem for a class can be efficiently repurposed to solve any other problem in that class. Therefore, a complete problem indeed completely characterizes the difficulty of the class.

Two different methods exist to show that a problem is hard for a given class. First, we pick another problem that is known to be complete for the class and efficiently map that problem to the problem of interest. Another method is to take the definition of the class itself and show that an arbitrary problem in the class can be efficiently mapped to the problem of interest.

Another important concept needed to fully specify the complexity of a problem is a polynomial-time generated family of circuits. Given a classical description/encoding of a quantum circuit, $x \in S$, where $S \subseteq \{0,1\}^*$ is a set of binary strings, the set of quantum circuits $\{Q_x \mid x \in S\}$ is said to be polynomial-time generated if there exists a Turing machine that takes in as input the string x and outputs an encoding of the quantum circuit Q_x in polynomial time. This particular definition allows us to limit the power of the computational model to circuits that are "polynomially complex" by limiting the process by which such circuits are created.

Lastly, we define promise problems. A promise problem can be thought of as a yes-no rewriting of a general decision problem. More concretely, a promise problem is a pair $L = (L_{\text{yes}}, L_{\text{no}})$, where $L_{\text{yes}}, L_{\text{no}}$ are subsets of all possible inputs such that $L_{\text{yes}} \cap L_{\text{no}} = \emptyset$. The inputs of the two subsets are called yes-instances and no-instances, respectively. For the example of the 'subset sum problem', yes instances are subsets that add up to the specific target value. An algorithm is said to "decide" a promise problem if, given an input from $L_{\text{yes}} \cup L_{\text{no}}$, it can determine to which subset the input belongs.

2.4.1 BQP

The class of bounded-error quantum polynomial time (BQP) promise problems is often referred to as the class of problems efficiently solvable on a quantum computer [NC10, Chapter 4]. The classical analog of BQP is the class of bounded-error probabilistic polynomial time (BPP) problems, which is the class of problems efficiently solvable on a classical computer with access to random bits. A promise problem is a member of BQP if there exists an efficient quantum algorithm solving it in polynomial time with a success probability of at least 2/3.

The formal definition of BQP is as follows. Let $L = (L_{\text{yes}}, L_{\text{no}})$ be a promise problem, $\alpha, \beta : \mathbb{N} \to [0,1]$ arbitrary functions, and p a polynomial function. Then $L \in \text{BQP}_p(\alpha, \beta)$ if there exists a polynomial-time generated family $Q = \{Q_n : n \in \mathbb{N}\}$ of unitary circuits, where each circuit Q_n

- takes $n + p(n)$ input qubits – the first n qubits are used for the input $x \in L$, and the next $p(n)$ input qubits are extra ancilla qubits that the verifier is allowed,
- produces as output one decision qubit labeled by D and $n + p(n) - 1$ garbage qubits labeled by G.

In what follows, we write each Q_n as $Q_{SA\to DG}$, thereby suppressing the dependence on the input length $n = |x|$ and explicitly indicating the systems involved at the input and output of the unitary. In addition, the circuit Q_n has the following properties:

1. Completeness: For all $x \in L_{\text{yes}}$,

$$\begin{aligned} &\Pr[Q \text{ accepts } x] \\ &\quad := \|(\langle 1|_D \otimes I_G) Q_{SA\to DG}(|x\rangle_S \otimes |0\rangle_A)\|_2^2 \\ &\quad \geq \alpha(|x|). \end{aligned} \tag{2.126}$$

2. Soundness: For all $x \in L_{\text{no}}$,

$$\Pr[Q \text{ accepts } x] \leq \beta(|x|), \tag{2.127}$$

where acceptance is defined as obtaining the outcome one upon measuring the decision qubit register D of the state $Q_{SA\to DG}(|x\rangle_S \otimes |0\rangle_A)$. Then $\text{BQP} = \bigcup_p \text{BQP}_p(2/3, 1/3)$, where the union is over every polynomial-bounded function p.

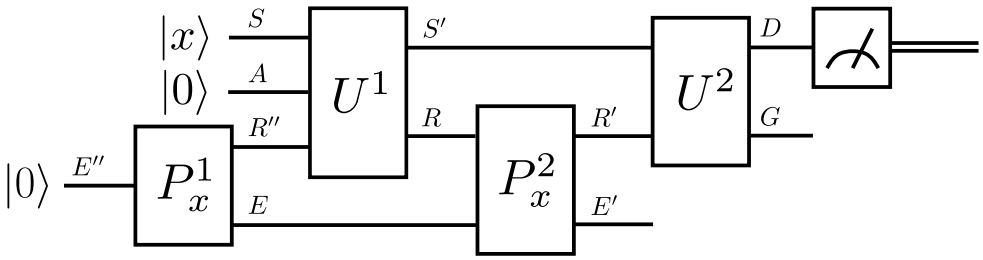


Figure 2.9: A general QIP(3) algorithm. The unitaries P_x^1 and P_x^2 are implemented by an all-powerful prover, and the probability of measuring the decision qubit to be in the state $|1\rangle$ is the acceptance probability of the algorithm.

2.4.2 QIP

Quantum interactive proof systems (QIP) denote a powerful complexity class in quantum computational complexity theory. Indeed, a landmark result of the field is QIP = PSPACE [JJUW10], the set of classical problems that use polynomial space, but unbounded time. The interactive proof system model involves messages between a computationally-bounded verifier and a prover with limitless computational power. These interactions may consist of some number of rounds m, in which case these models can be classified by the number of exchanges as QIP(m). After all the messages have been exchanged, the verifier makes a decision to either accept or reject based on these interactions. Thus, the class QIP refers to all such promise problems that can be framed in this manner.

More formally, the definition both of QIP(m) and QIP are given in [KW00, Wat03] to be as follows: Let $m \in \mathbb{N}$, and let $\alpha, \beta : \mathbb{N} \to [0,1]$ be functions. Then let QIP(m, α, β) denote the class of promise problems L for which there exists an m-message verifier V such that

1. for all $x \in L$, $\exists$ a prover P such that the pair (V, P) accepts with probability at least $\alpha(|x|)$, and,
2. for all $x \notin L$, $\forall$ provers P, the pair (V, P) accepts with probability at most $\beta(|x|)$.

Usually, interactive proof classes are denoted solely by the number of messages exchanged, QIP(m). An important finding for QIP is that QIP = QIP(3), which implies that no further computational power is afforded by increasing the number

of messages exchanged beyond three [KW00]. A general QIP(3) algorithm can be seen in Figure 2.9.

The problem of close images was the first QIP-Complete problem to be proposed [KW00], and it is stated as follows:

Definition 2.5 [*Problem of Close Images*]. *For constants* $0 \leq \beta < \alpha \leq 1$*, the input consists of two polynomial-time computable quantum circuits that agree on the number of output qubits and realize the quantum channels* $\mathcal{N}_1$ *and* $\mathcal{N}_2$*. Decide which of the following holds:*

$$\textit{Yes:} \quad \max_{\rho_1,\rho_2} F(\mathcal{N}_1(\rho_1), \mathcal{N}_2(\rho_2)) \geq \alpha, \tag{2.128}$$

$$\textit{No:} \quad \max_{\rho_1,\rho_2} F(\mathcal{N}_1(\rho_1), \mathcal{N}_2(\rho_2)) \leq \beta, \tag{2.129}$$

where the optimization is over all input states ρ_1 *and* ρ_2*.*

2.4.3 QMA

The quantum Merlin–Arthur (QMA) class is equivalent to QIP(1); that is, this model consists of a single message exchanged between a computationally unbounded prover and a computationally limited verifier.

The definition of QMA can be found in [Wat09a], reproduced here for convenience. Let $L = (L_{\text{yes}}, L_{\text{no}})$ be a promise problem, let p, q be polynomially-bounded functions, and let $\alpha, \beta : \mathbb{N} \to [0,1]$ be functions. Then $L \in \text{QMA}_{p,q}(\alpha,\beta)$ if there exists a polynomial-time generated family of unitary circuits $Q = \{Q_n : n \in \mathbb{N}\}$, where each circuit Q_n

- takes $n + p(n) + q(n)$ input qubits – the first n qubits are used for the input $x \in L$, the next $p(n)$ input qubits are extra ancilla qubits that the verifier is allowed, and the last $q(n)$ qubits are given by the prover,
- produces as output one decision qubit labeled by D and $n + p(n) + q(n) - 1$ garbage qubits labeled by G.

As before, we write Q_n as $Q_{SAP\to DG}$, thereby suppressing the dependence on the input length $n = |x|$ and explicitly indicating the systems involved at the input and output of the unitary. In addition, the circuit Q_n has the following properties:

1. Completeness: For all $x \in L_{\text{yes}}$, there exists a $q(|x|)$-qubit state σ_P such that

$$\begin{aligned} \Pr[Q \text{ accepts } (x, \sigma)] &= \langle 1|_D \operatorname{Tr}_G[\omega_{DG}]|1\rangle_D && (2.130) \\ &\geq \alpha(|x|), && (2.131) \end{aligned}$$

   where

$$\omega_{DG} \coloneqq Q_n(|x\rangle\langle x|_S \otimes |0\rangle\langle 0|_A \otimes \sigma_P)Q_n^\dagger. \tag{2.132}$$

2. Soundness: For all $x \in L_{\text{no}}$ and every $q(|x|)$-qubit state σ_P, the following inequality holds:

$$\Pr[Q \text{ accepts } (x, \sigma)] \leq \beta(|x|). \tag{2.133}$$

Then $\text{QMA} = \bigcup_{p,q} \text{QMA}_{p,q}(2/3, 1/3)$, where the union is over all polynomial-bounded functions p and q.

2.4.4 QMA(2)

QMA(2) is a generalization of QMA with proofs that consist of two systems guaranteed to be separable [KMY01, HM10]. We reproduce the definition of QMA(2) for convenience. Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a promise problem, let p, q, r be polynomially-bounded functions, and let $a, b : \mathbb{N} \to [0, 1]$ be functions. Then $A \in \text{QMA}(2)_{p,q}(a, b)$ if there exists a polynomial-time generated family of circuits $Q = \{Q_n : n \in \mathbb{N}\}$, where each circuit Q_n takes $n + p(n) + q(n) + r(n)$ input qubits and produces one decision qubit D and $n + p(n) + q(n) + r(n) - 1$ garbage qubits G, with the following properties (again, we employ the notation $Q_{SAP_1P_2 \to DG}$ in what follows):

1. Completeness: For all $x \in A_{\text{yes}}$, there exists a $q(|x|)$-qubit state ρ and an $r(|x|)$-qubit state σ such that

$$\begin{aligned} \Pr[Q \text{ accepts } (x, \rho, \sigma)] &= \langle 1|_D \operatorname{Tr}_G[\omega_{DG}]|1\rangle_D \\ &\geq a(|x|), && (2.134) \end{aligned}$$

   where

$$\omega_{DG} \coloneqq Q_{SAP_1P_2 \to DG}(|x\rangle\langle x|_S \otimes |0\rangle\langle 0|_A \otimes \rho_{P_1} \otimes \sigma_{P_2})(Q_{SAP_1P_2 \to DG})^\dagger. \tag{2.135}$$

2. Soundness: For all $x \in A_{\text{no}}$, and every $q(|x|)$-qubit state ρ and $r(|x|)$-qubit state σ, the following inequality holds:

$$\Pr[Q \text{ accepts } (x, \rho, \sigma)] \leq b(|x|). \tag{2.136}$$

Then $\text{QMA}(2) = \bigcup_p \text{QMA}(2)_{p,q}(2/3, 1/3)$, where the union is over all polynomially bounded functions p and q.

2.4.5 QSZK

The complexity class quantum statistical zero-knowledge (QSZK) gives a quantum analog of the classical statistical zero-knowledge class [Wat02b, Wat06], which can be phrased in terms of an interactive proof system.

We reproduce the definition of QSZK here for convenience. Let V be a verifier and P a prover that acts on some input x. Define the mixed state of the verifier and message qubits after j messages to be $\rho_{V,M}(x, j)$. Then the pair (V, P) is a quantum statistical zero-knowledge proof system for a promise problem L if

1. (V, P) is an interactive proof system for L, and
2. there exists a polynomial-time preparable set $\{\sigma_{x,j}\}_j$ of states such that

$$x \in L \Rightarrow \forall j \quad \left\| \sigma_{x,j} - \rho_{V,M}(x, j) \right\|_1 \leq \delta(|x|), \tag{2.137}$$

for some δ such that $\delta(n) < 1/p(n)$ for sufficiently large n and every polynomial p.

The completeness and soundness requirements of this class come from the underlying proof system; for the definition of QSZK, we restrict the completeness and soundness errors to be at most $1/3$.

For this class, as with many class definitions, it can be helpful to look at a QSZK-Complete promise problem. The quantum state distinguishability problem was originally proposed alongside the class definition in [Wat02b], and so it is a natural choice. The problem statement is as follows:

Definition 2.6 [*Quantum State Distinguishability*]. *Let $L = (L_{\text{yes}}, L_{\text{no}})$ be a promise problem, and let α and β be constants satisfying $0 \leq \beta < \alpha \leq 1$. Given two quantum*

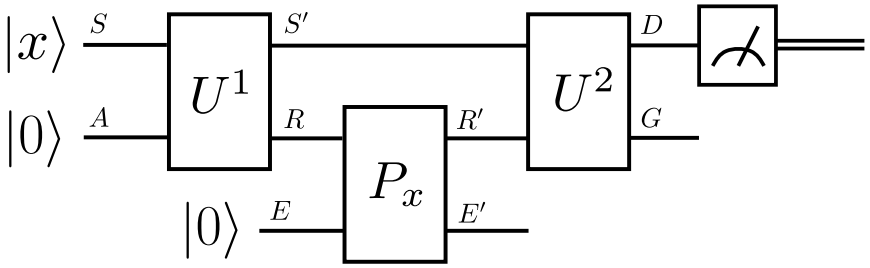


Figure 2.10: A general QIP(2) algorithm. The unitary P_x is implemented by an all-powerful prover, and the probability of measuring the decision qubit to be in the state $|1\rangle$ is the acceptance probability of the algorithm.

circuits Q_0 and Q_1 acting on m qubits each and having k specified output qubits, let ρ_i denote the output mixed state obtained by running Q_i on an input $|0\rangle^{\otimes m}$. Decide whether

$$\textit{Yes:} \quad \frac{1}{2}\|\rho_0 - \rho_1\|_1 \geq \alpha, \tag{2.138}$$

$$\textit{No:} \quad \frac{1}{2}\|\rho_0 - \rho_1\|_1 \leq \beta. \tag{2.139}$$

In [Wat02b], it was shown that (α,β)-Quantum State Distinguishability is QSZK-Complete for $0 \leq \beta < \alpha^2 \leq 1$.

2.4.6 QIP(2)

The complexity class QIP(2) specifically denotes a set of promise problems that include two messages exchanged between the prover and verifier. The formal definition can be inferred from Section 2.4.2 by setting the number of messages to two, i.e., $m = 2$. A general QIP(2) algorithm can be seen in Figure 2.10.

We now reproduce the canonical QIP(2)-Complete problem [Wat02a, HMW14] as follows:

Definition 2.7 [*Problem of Close Image*]. *Given is a circuit to realize a unitary extension $U_{AE'\to BE}$ of a channel $\mathcal{N}_{A\to B}$, such that*

$$\mathcal{N}_{A\to B}(\omega_A) = \mathrm{Tr}_E[U_{AE'\to BE}(\omega_A \otimes |0\rangle\langle 0|_{E'})(U_{AE'\to BE})^\dagger] \tag{2.140}$$

for every input state ω_A, and a circuit to realize a purification of the state ρ_B. Decide which

of the following holds:

$$\textit{Yes:} \quad \max_{\sigma_A} F(\rho_B, \mathcal{N}_{A\to B}(\sigma_A)) \geq \alpha, \tag{2.141}$$

$$\textit{No:} \quad \max_{\sigma_A} F(\rho_B, \mathcal{N}_{A\to B}(\sigma_A)) \leq \beta, \tag{2.142}$$

where the optimization is over every input state σ_A.

Note that the Problem of Close Image is different from the Problem of Close Images (see Definition 2.5). In the former, we bound the fidelity between a channel and a state, whereas in the latter, we bound the fidelity between two channels.

2.4.7 $\mathbf{QIP_{EB}}(2)$

The complexity class $\mathrm{QIP}_{\mathrm{EB}}(2)$ was introduced in [PRRW24] and represents a modification of QIP(2). By inspecting Figure 2.10 and recalling the Stinespring dilation theorem (see, e.g., [Wil17]), we see that the prover's action in a QIP(2) protocol is equivalent to performing a quantum channel that has input system R and output system R' (see also [JUW09, Figure 1]). The idea behind $\mathrm{QIP}_{\mathrm{EB}}(2)$ is that the prover is constrained to performing an entanglement-breaking channel. Such a channel has the following form [HSR03]:

$$\rho \to \sum_x \mathrm{Tr}[\mu_x \rho]\phi_x, \tag{2.143}$$

where $\{\mu_x\}_x$ is a rank-one positive operator-valued measure (i.e., each μ_x is a rank-one positive semi-definite operator and $\sum_x \mu_x = I$) and $\{\phi_x\}_x$ is a set of pure states.

The canonical $\mathrm{QIP}_{\mathrm{EB}}(2)$-Complete problem is as follows [PRRW24, Theorem 11]:

Definition 2.8. *Given circuits to generate a unitary extension of a channel $\mathcal{N}_{G\to S}$ and a purification of a state ρ_S, decide which of the following holds:*

$$\textit{Yes:} \quad \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\varphi^x\}_x,\\ \sum_x p(x)\psi_S^x = \rho_S}} \sum_x p(x) F(\psi_S^x, \mathcal{N}_{G\to S}(\varphi_G^x)) \geq \alpha, \tag{2.144}$$

$$\textit{No:} \quad \max_{\substack{\{(p(x),\psi^x)\}_x,\\ \{\varphi^x\}_x,\\ \sum_x p(x)\psi_S^x = \rho_S}} \sum_x p(x) F(\psi_S^x, \mathcal{N}_{G\to S}(\varphi_G^x)) \leq \beta, \tag{2.145}$$

where the optimization is over every pure-state decomposition of ρ_S, as $\sum_x p(x)\psi_S^x = \rho_S$, and $\{\varphi^x\}_x$ is a set of pure states.

2.4.8 QAM

The quantum Arthur–Merlin (QAM) class was introduced in [MW05], and it can be understood as a variation of QMA in which the verifier and prover are given access to shared randomness in advance. It can also be understood as a restricted version of QIP(2) in which the first message of the verifier is restricted to being a uniformly random classical bitstring. As such, the following containments hold: QMA $\subseteq$ QAM $\subseteq$ QIP(2).

Let us recall its definition here. Let $L = (L_{\text{yes}}, L_{\text{no}})$ be a promise problem, let p, q, r be polynomially-bounded functions, and let $\alpha, \beta : \mathbb{N} \to [0,1]$ be functions. Then $L \in \text{QAM}_{p,q,r}(\alpha,\beta)$ if there exists a polynomial-time generated family of unitary circuits $Q = \left\{Q_{n,y} : n \in \mathbb{N}, y \in \mathcal{Y}\right\}$, where y is a uniformly random bitstring consisting of $r(n)$ bits, so that $\log_2 |\mathcal{Y}| = r(n)$, and each circuit $Q_{n,y}$

- takes $n + p(n) + q(n)$ input qubits – the first n qubits are used for the input $x \in L$, the next $p(n)$ input qubits are extra ancilla qubits that the verifier is allowed, and the last $q(n)$ qubits are given by the prover,
- produces as output one decision qubit labeled by D and $n + p(n) + q(n) - 1$ garbage qubits labeled by G.

We write $Q_{n,y}$ as $Q^y_{SAP\to DG}$, thereby suppressing the dependence on the input length $n = |x|$ and explicitly indicating the systems involved at the input and output of the unitary. We also use the shorthand $Q^y \equiv Q^y_{SAP\to DG}$. In addition, each set $\{Q_{n,y}\}_{y\in\mathcal{Y}}$ of circuits has the following properties:

1. Completeness: For all $x \in L_{\text{yes}}$, there exists a set $\{\sigma^y_P\}_{y\in\mathcal{Y}}$ of $q(|x|)$-qubit states such that

$$\begin{aligned} &\frac{1}{|\mathcal{Y}|}\sum_{y\in\mathcal{Y}} \Pr[Q^y \text{ accepts } (x, \sigma^y)] \\ &= \frac{1}{|\mathcal{Y}|}\sum_{y\in\mathcal{Y}} \langle 1|_D \operatorname{Tr}_G[\omega^y_{DG}]|1\rangle_D \qquad (2.146) \\ &\geq \alpha(|x|), \qquad (2.147) \end{aligned}$$

where

$$\omega_{DG}^{y} := Q^{y}(|x\rangle\langle x|_S \otimes |0\rangle\langle 0|_A \otimes \sigma_P^{y})(Q^{y})^{\dagger}. \tag{2.148}$$

2. Soundness: For all $x \in L_{\text{no}}$, and every set $\{\sigma_P^{y}\}_{y\in\mathcal{Y}}$ of $q(|x|)$-qubit states, the following inequality holds:

$$\frac{1}{|\mathcal{Y}|}\sum_{y\in\mathcal{Y}} \Pr[Q^{y} \text{ accepts } (x, \sigma^{y})] \leq \beta(|x|). \tag{2.149}$$

The acceptance probability

$$\frac{1}{|\mathcal{Y}|}\sum_{y\in\mathcal{Y}} \Pr[Q^{y} \text{ accepts } (x, \sigma^{y})] \tag{2.150}$$

can be understood as the probability of acceptance conditioned on a fixed value of y, which is then averaged over the shared uniform randomness (i.e., here we are applying the law of total probability). Then $\text{QAM} = \bigcup_{p,q,r} \text{QAM}_{p,q,r}(2/3, 1/3)$, where the union is over all polynomial-bounded functions p, q, and r.

2.5 Variational algorithms

Variational algorithms are algorithms that use a hybrid quantum-classical approach to learn some optimal quantum state. As opposed to large quantum circuits that require a large number of high-quality qubits, variational quantum algorithms (VQAs) require a relatively smaller number of qubits, with fewer constraints on their quality. Some part of the workflow is offloaded to a classical computer, reducing the overall quantum load. Since the results of this thesis rely heavily on VQAs, we spend some time developing an intuition of the power, limitations, and future directions of VQAs. Before we delve into the quantum part of VQAs, we first explore the idea of **training parameters to find a best fit**. To do this, we use the pedagogical example of line fitting, or linear regression.

Lienar Regression - Linear regression is the process of finding the best fit line for a given set of data points. Consider we have a set of points as shown in Figure 2.11. The goal is to find the optimal line that fits these points. Each line is **parameterized** by two variables, m and c.

$$y_{m,c}(x) = mx + c. \tag{2.151}$$

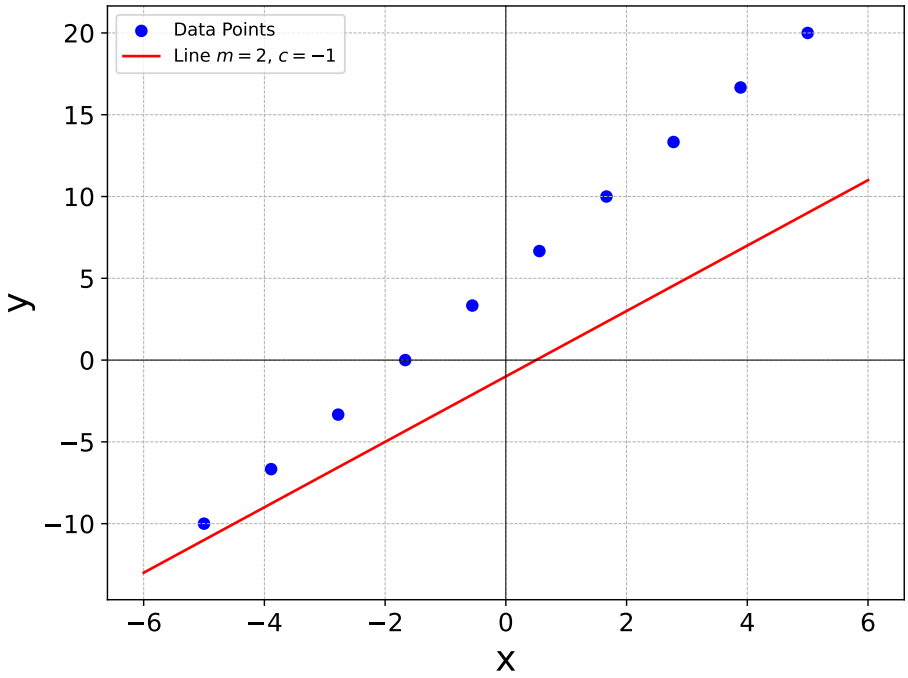


Figure 2.11: Data points in blue and fitted line in red.

From visual inspection of Figure 2.11, we can see that both the slope m and intercept c are too low. This was a simple example with 2D data. For larger dimensions, we need to find a way to learn the optimal parameters. To this end, we define a **loss function** that we minimize. The loss function measures how far the fitted line, defined by m and c, is from the points. In this example, the loss function is the sum of perpendicular lengths squared, as seen in Figure 2.12 (normalized by the number of points). Minimizing the sum of squares of all the dashed green lines, i.e., minimizing the loss function, gives us a method to find the optimal parameters m and c.

How does the minimization procedure work? There are multiple methods to try and minimize the loss function, but here we discuss the simplest – gradient descent. In essence, it involves finding the derivative of the loss function with respect to the parameters and using this information to take a step in the direction that reduces the loss function the most. Let's say that the loss function is given by

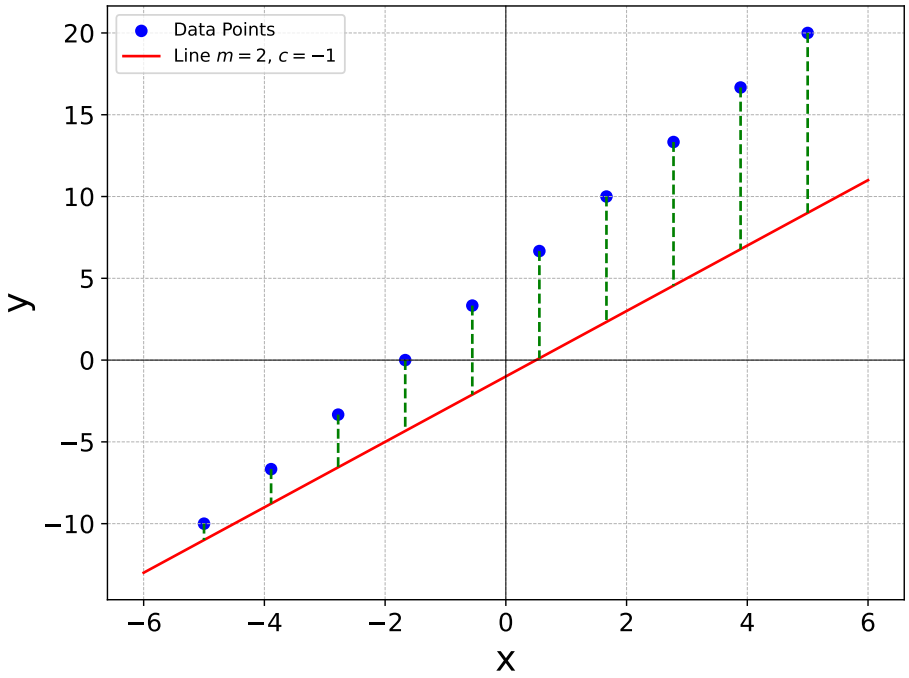


Figure 2.12: Dashed green lines represent the pieces of the loss function.

$\mathcal{L}(m, c)$. If the blue data points are given by $\{(x_i, y_i)\}_i$, then the loss function can be expanded as

$$\mathcal{L}(m, c) = \frac{1}{n} \sum_i (y_i - (mx_i + c))^2. \tag{2.152}$$

Then, the gradient is given by

$$\nabla \mathcal{L} = \frac{\partial \mathcal{L}}{\partial m} \hat{m} + \frac{\partial \mathcal{L}}{\partial c} \hat{c}. \tag{2.153}$$

At $m = 2$ and $c = -1$, the gradient turns out to be

$$\nabla \mathcal{L}(2, -1) \approx (-20, -14). \tag{2.154}$$

The gradient specifies the direction in the space such that moving along that direction will increase the loss function by the maximum amount. Since we seek

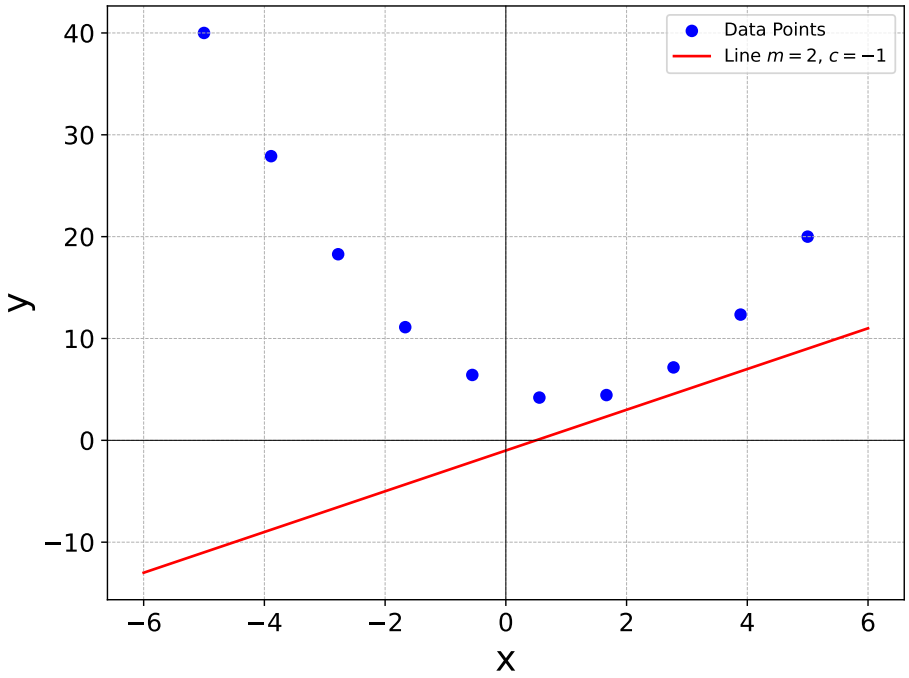


Figure 2.13: An example of a bad-fitting model.

to minimize the loss function, we calculate the new (m, c) as follows:

$$(m_{\text{new}}, c_{\text{new}}) = (m_{\text{old}}, c_{\text{old}}) - \eta \nabla \mathcal{L}(m_{\text{old}}, c_{\text{old}}), \tag{2.155}$$

where the parameter η is called the learning rate. This ensures that we only take a small step and do not overshoot. The fact that the gradient is $(-20, -14)$ confirms that both m and c need to be increased to better approximate the points.

Before moving on, we consider one variation of the above example. Consider the case where the set of points is shown in Figure 2.13. For these points, we can visually see that any possible choice of m and c will be a bad fit for the data. In classical literature, this phenomenon is called underfitting.

The example of linear regression above illustrates several important ideas that we will further explore in the quantum setting.

As discussed, quantum variational algorithms use a hybrid quantum-classical approach to learn an optimal state. The trial state is parameterized using rotation angles and is called an **ansatz**. Different ansatz structures lead to a different set of possible states. An example ansatz can be found in Figure 2.14. After preparing the ansatz state, some observable is estimated. These estimates are sent to a classical computer, and the next set of parameters is chosen.

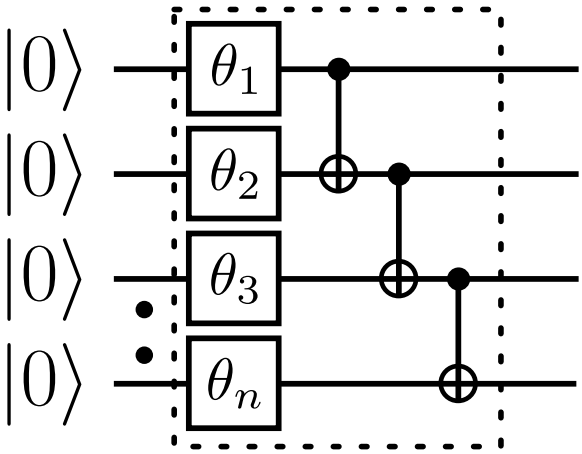


Figure 2.14: An example ansatz on n qubits. The gates within the dotted lines is called a layer and is usually repeated multiple times. The gates θ_i represent the rotation gate $R_y(\theta_i)$.

A typical loss function for a quantum variational algorithm is of the form

$$\mathcal{L}(\vec{\theta}) = \text{Tr}[OU(\vec{\theta})|0\rangle\langle 0|U^\dagger(\vec{\theta})], \tag{2.156}$$

where O is an observable to be measured, $U(\vec{\theta})$ is the ansatz, and $|0\rangle$ is the starting state. Research on variational algorithms has led to several algorithms, and an expansive summary can be found here [CAB+21, BCLK+22] (see also [GRS83] for a review of the variational principle). We now discuss some key factors in a successful variational algorithm.

2.5.1 Expressivity

Let us look at a simple example of learning the optimal rotational parameter to prepare a state. We consider a single qubit starting in the $|0\rangle$ state and acted upon by the parameterized y-rotation gate $R_y(\theta)$ (see Figure 2.15).

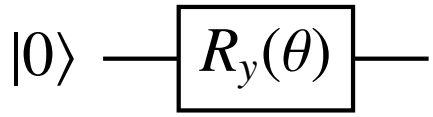


Figure 2.15: Variational state preparation example.

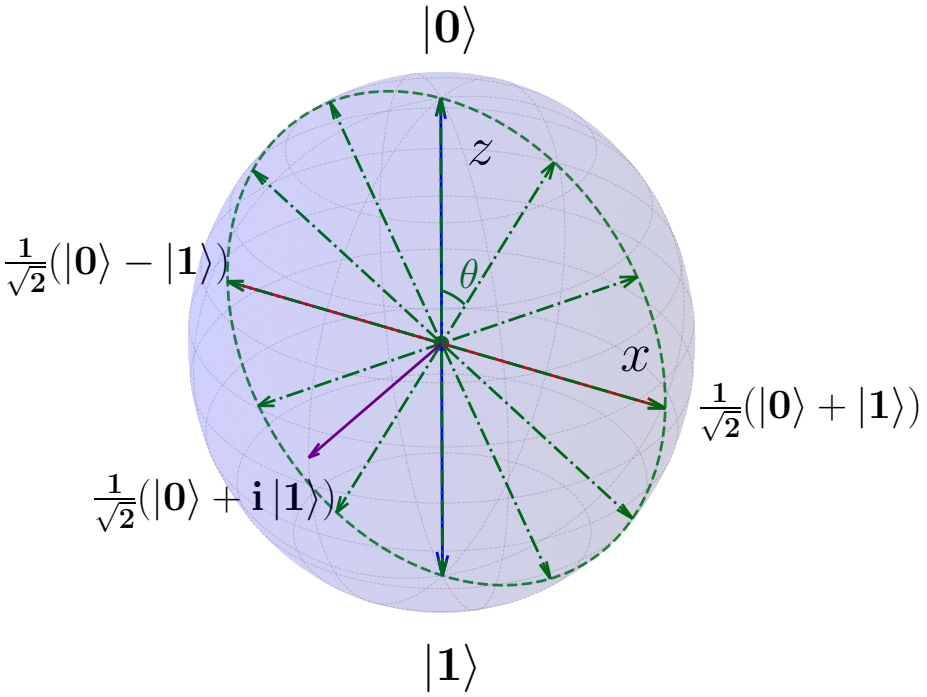


Figure 2.16: Dashed green line all possible states for the circuit in Figure 2.15.

For this small example, we can see all possible states that we can prepare in Figure 2.16. If we define the cost function as the fidelity of the prepared state and the $|+\rangle$ state, we can express this as

$$\begin{aligned}\mathcal{L}(\theta) &= |\langle +|R_y(\theta)|0\rangle|^2, \\ &= \frac{1}{2}\left[\cos(\theta/2) + \sin(\theta/2)\right]^2, \\ &= \frac{1}{2}\left[1 + \sin(\theta)\right].\end{aligned} \tag{2.157}$$

Clearly, for $\theta = \frac{\pi}{2}$, the cost function is maximized, and from Figure 2.16, we see

that this corresponds to the $|+\rangle$ state. This loss function is easy to optimize, as the gradient can be calculated easily and it has only one maximum.

On the other hand, if the loss function is the fidelity of the prepared state with the state $|+;y\rangle$ (labelled in purple), we can expand the loss as follows:

$$\begin{aligned}\mathcal{L}(\theta) &= |\langle +;y|R_y(\theta)|0\rangle|^2, \\ &= \frac{1}{2}\left|\cos(\theta/2) - \mathrm{i}\sin(\theta/2)\right|^2, \\ &= \frac{1}{2}.\end{aligned} \tag{2.158}$$

The loss function is independent of the parameter θ. From the figure, is it clear that the $|+;y\rangle$ state is equidistant from all the states that can be prepared from the given construction. The gradient of this loss is zero, and training is impossible.

Independent of the cost function, this ansatz can clearly only create a subset of all possible one-qubit states. For states not in this subset, the fidelity can never be maximal, with the extreme case being the $|+;y\rangle$ state. A measure of the size of all states that can be created using an ansatz is called the **expressivity** of the ansatz. A highly expressive ansatz is one that can prepare most states in the Hilbert space.

2.5.2 Trainability

Another important property of the combination of an ansatz and the loss function is called trainability. Even if the ansatz is fully expressive, i.e., all states in the Hilbert space of relevance can be prepared using a specific set of parameters, it may be impossible to find this optimal set of parameters. There may be many reasons for loss of trainability, but the common thread among them is the emergence of barren plateaus.

Consider a cost landscape, i.e., the shape of the cost function as a function of all the parameters. Training begins at a random point and uses the gradient information to find a path to the optimal set of parameters. Consider the following two examples of cost landscapes in Figure 2.17.

If the cost landscape looks like the first type, at each point, the gradient value can be estimated easily, and the next set of parameters can be chosen. However, if the cost landscape looks like the second type, it becomes difficult to estimate the

(a) Trainable landscape.

(b) Untrainable landscape.

Figure 2.17: Two different possible cost landscapes: (a) a loss landscape that has features and appreciable gradient values and (b) a barren landscape with low gradient values.

gradient, and thus, the next set of parameters cannot be chosen. Intuitively, we call landscapes of the second kind **barren plateaus**.

In both the statements above, the 'difficulty' of estimating the gradients is described. A more concrete definition of the 'difficulty' is based on the number of shots needed to estimate the gradient accurately. If the gradient of the cost function is small, say exponentially small, then to accurately estimate it, an exponential number of samples are required. Barren plateaus are characterized by exponentially small gradient values, leading to an exponential overhead in training. Thus, barren plateaus pose a significant roadblock to effective quantum variational algorithms.

It turns out the expressivity and trainability of a quantum variational problem are closely connected. A highly expressive ansatz, while probably containing the optimal solution, is more prone to barren plateaus, thus making it untrainable [HSCC22]. We note that in addition to high expressivity, there has been considerable research into other causes, potential solutions, and non-solutions.

The main appealing feature of variational quantum computing was the exploration of an exponential Hilbert space. However, there have been several research works that suggest that this very feature is at the core of the barren plateau issue. Let us consider a simple derivation as to why this must be true. Consider a

general form of the loss function

$$\begin{aligned}\mathcal{L}_\theta(\rho, O) &= \langle U(\boldsymbol{\theta})\rho U^\dagger(\boldsymbol{\theta}), O\rangle \\ &= \langle \rho, U^\dagger(\boldsymbol{\theta}) O U(\boldsymbol{\theta})\rangle. \end{aligned} \tag{2.159}$$

Thus, the loss function is the Hilbert-Schmidt overlap between two vectors in the exponential Hilbert space. Thus, on average, this overlap must be exponentially suppressed.

Thus, solutions to the barren plateau are all based on somehow restricting the size of the explored space to be only polynomially large. These solutions involve shallow circuits, local observables, small dynamical Lie algebras, variable structure ansatzes, etc. A highly recommended comprehensive summary can be found here [LTW+24].

Chapter 3

Distinguishability

The ability to distinguish between things is what gives meaning to knowledge.
—— Isaiah Berlin

This chapter is based on collaborative work with Rochisha Agarwal, Dr. Kunal Sharma, and Dr. Mark M. Wilde [RASW23]. Throughout this section, 'we' refers to all four collaborators.

In quantum information processing, it is essential to quantify the performance of protocols by using distinguishability measures. It is typically the case that there is an ideal state to prepare or an ideal channel to simulate, but in practice, we can only realize approximations, due to experimental error. Two commonly employed distinguishability measures for states are the trace distance [Hel67, Hel69] and the fidelity [Uhl76]. The former has an operational interpretation as the distinguishing advantage in the optimal success probability when trying to distinguish two states that are chosen uniformly at random. The latter has an operational meaning as the maximum probability that a purification of one state could pass a test for being a purification of the other (this is known as Uhlmann's transition probability [Uhl76]). These distinguishability measures have generalizations to quantum channels, in the form of the diamond distance [Kit97] and the fidelity of channels [GLN05]. Each of these measures are generalized by the generalized divergence of states [PV10], and channels [LKDW18]. The operational interpretations of these latter distinguishability measures are similar to the aforementioned ones, but the corresponding protocols involve more steps that are used in the distinguishing process.

Both the trace distance and the fidelity can be computed by means of semi-definite programming [Wat13], so that they can be estimated accurately with a run-time that is polynomial in the dimension of the states. The same is true for the diamond distance [Wat09c], and the fidelity of channels [YF17, KW21]. While this method of estimating these quantities is reasonable for states, and channels, its computational complexity actually increases exponentially with the number of qubits involved, due to the well-known fact that Hilbert-space dimension grows exponentially with the number of qubits.

In this paper, we provide several quantum algorithms for estimating these distinguishability measures. Some of the algorithms rely on interaction with a quantum prover, in which case they are not necessarily efficiently computable even on a quantum computer. In fact, the computational hardness results of [Wat02c, RW05, Wat09d] lend credence to the belief that estimating these quantities reliably is not generally possible in polynomial time on a quantum computer. However, as we show in our paper, by replacing the quantum prover with a parameterized circuit (see [CAB+21, BCLK+22] for reviews of variational algorithms), it is possible in some cases to estimate these quantities reliably. Identifying precise conditions under which a quantum computer can estimate these quantities efficiently is an interesting open question that we leave for future research. Already in [WZC+21], it was shown that estimating the fidelity of two quantum states is possible in quantum polynomial time when one of the states is low rank, and the same is the case for estimating the trace distance under certain promises [WGL+22, WZ23]. See also [CPCC20, CSZW22, TV21] for variational algorithms that estimate fidelity of states and [CSZW22, LLSL21] for variational algorithms to estimate trace distance. It is open to determine precise conditions under which estimation is possible for channel distinguishability measures.

We perform noiseless and noisy simulations of several of the algorithms provided. We find that in the noiseless scenario, all algorithms converge, for the examples considered, to the true known value of the distinguishability measure under consideration. In the noisy simulations, the algorithms converge well, and the parameters obtained exhibit a noise resilience, as put forward in [SKCC20]; i.e., the relevant quantity can be accurately estimated by inputting the parameters learned from the noisy simulator into the noiseless simulator.

Lastly, we discuss the computational complexity of various distance estimation algorithms. We prove that several fidelity and distance estimation algorithms are complete for well-known quantum complexity classes (see Section 2.4 for a brief review of quantum computational complexity theory). In particular, we

prove that estimating the fidelity between two pure states, a mixed state and a pure state, and estimating the Hilbert–Schmidt distance of two mixed states are BQP-complete problems. These aforementioned results follow by demonstrating that there is an efficient quantum algorithm for these tasks and by showing a reduction from an arbitrary BQP algorithm to one for these tasks. Thus, if we believe that there is a separation between the computational power of classical and quantum computers, then these estimation problems are those for which a quantum computer has an advantage. Several BQP-complete promise problems are known, including approximating the Jones polynomial [AJL06], estimating quadratically signed weight enumerators [KL01], estimating diagonal entries of powers of sparse matrices [JW07], a problem related to matrix inversion [HHL09], and deciding whether a pure bipartite state is entangled [GHMW15]. See [Zha12] for a 2012 review of BQP-complete promise problems.

We then prove that the problem of estimating the fidelity between a channel with arbitrary input and a pure state is a QMA-complete promise problem. We show this by constructing an efficient quantum algorithm, augmented by a single all-powerful prover, to solve this problem, and by showing a reduction from an arbitrary QMA problem to one for this task. Lastly, we demonstrate that the problem of estimating the fidelity between a channel with separable input and a pure state is QMA(2)-complete. QMA(2) is the class of problems that can be efficiently solved when augmented by two all-powerful quantum provers who are guaranteed to be unentangled [KMY01, HM10].

In the rest of the paper, we provide details of the algorithms and results mentioned above. In particular, our paper proceeds as follows:

1. The various subsections of Section 3.1 are about estimating the fidelity of states, channels, and strategies. We begin in Section 3.1.1 by establishing two quantum algorithms for estimating the fidelity of pure states, one of which is based on a state overlap test (Algorithm 3.1) and another that employs Bell state preparation and measurement along with a controlled unitary (Algorithm 3.2).
2. In Section 3.1.2, we generalize Algorithm 3.1 to estimate the fidelity of a pure state and a mixed state (see Algorithm 3.3).
3. In Section 3.1.3, we establish several quantum algorithms for estimating the fidelity of two arbitrary states. Algorithm 3.4 generalizes Algorithm 3.2. Algorithm 3.5 generalizes the well-known swap test to the case of arbitrary

states. Algorithm 3.6 is a variational algorithm that employs Bell measurements, as a generalization of the approach in [GECP13, SCC19] for pure states. Algorithm 3.7 is another variational algorithm that attempts to simulate a fidelity-achieving measurement, such as the Fuchs–Caves measurement [FC95], in order to estimate the fidelity.

4. In Section 3.1.4, we generalize Algorithm 3.4 to a quantum algorithm for estimating the fidelity of quantum channels (see Algorithm 3.8). This algorithm involves interaction with competing quantum provers, and interestingly, its acceptance probability is directly related to the fidelity of channels, thus giving the latter an operational meaning. Later, we replace the provers with parameterized circuits and arrive at a method for estimating the fidelity of channels.
5. In Section 3.1.5, we briefly discuss alternative methods for estimating the fidelity of channels, based on the approaches from Section 3.1.3 for estimating the fidelity of states.
6. Section 3.1.6 introduces a method for estimating the maximum output fidelity of two quantum channels, which has an application to generating a fixed point of a quantum channel.
7. In Sections 3.1.7 and 3.1.8, we generalize the whole development above to the case of testing similarity of arbitrary ensembles of states and channels. We find that the acceptance probability of the corresponding algorithms is related to the secrecy measure from [KRS09], which can be understood as a measure of similarity of the states in an ensemble. We then establish generalizations of this measure for an ensemble of channels and remark how this has applications in private quantum reading [BDW18, DBW20].
8. We then move on in Section 3.2 to estimating trace-distance-based measures, for states, and channels. We stress that these various algorithms were already known, and our goal here is to investigate their performance using a variational approach. In Sections 3.2.1, and 3.2.2, Algorithms 3.13, and 3.14 provide methods for estimating the trace distance of states, and the diamond distance of channels, respectively.
9. In Section 3.2.3, we provide two different but related algorithms for estimating the minimum trace distance between two quantum channels. The related approaches employ competing provers to do so.
10. In Section 3.2.4, we generalize the whole development for trace-distance based algorithms to the case of multiple states, and channels.

11. In Section 3.3, we discuss the results of numerical simulations of Algorithms 3.4–3.8, Algorithms 3.13–3.14, and Algorithm 3.17. We use both noiseless and noisy quantum simulators and a variational approach with parameterized circuits.
12. In Section 3.4, we prove that the problems of evaluating the fidelity between two pure states, a pure state and a mixed state, and evaluating the Hilbert–Schmidt distance of two mixed states are BQP-complete (Theorem 3.8, 3.9, 3.10). We then show that the problem of evaluating the fidelity between a channel with arbitrary input and a pure state is QMA-complete (Theorem 3.11). Finally, we demonstrate that the problem of evaluating the fidelity between a channel with separable input and a pure state is QMA(2)-complete (Theorem 3.12).

We finally conclude in Section 3.5 with a summary and some open questions.

3.1 Estimating fidelity

In this section, we propose algorithms for several different fidelity problems.

3.1.1 Estimating fidelity of pure states

We begin by outlining two simple quantum algorithms for estimating fidelity when both states are pure. A standard approach for doing so is to use the swap test [BBD+97, BCWdW01] or Bell measurements [GECP13, SCC19]. The approaches that we discuss below are different from these approaches. The first algorithm is a special case of that proposed in [Wat02c] (see also [CSZW22]), as well as a special case of Algorithm 3.3 presented later. The second algorithm involves a Bell-state preparation and projection, as well as controlled interactions, and it is a special case of Algorithm 3.4 presented later. We list both of these algorithms here for completeness and because later algorithms build upon them.

Suppose that the goal is to estimate the fidelity of pure states ψ^0 and ψ^1, and we are given access to quantum circuits U^0 and U^1 that prepare these states when acting on the all-zeros state. We now detail a first quantum algorithm for estimating

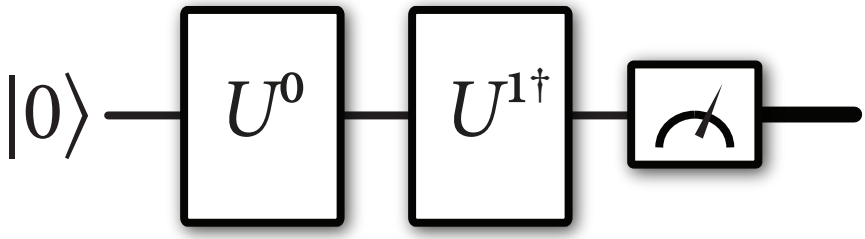


Figure 3.1: This figure depicts Algorithm 3.1 for estimating the fidelity of pure states generated by quantum circuits U^0 and U^1. In this, and all following figures, we use the convention that a bold line represents a classical register.

the fidelity

$$F(\psi^0, \psi^1) := \left|\langle \psi^1 | \psi^0 \rangle\right|^2 . \tag{3.1}$$

Algorithm 3.1 Algorithm schematic for fidelity of pure states.

Input: Quantum circuits U^0 and U^1 that prepare ψ^0 and ψ^1.
Output: Estimate of $F(\psi^0, \psi^1)$.

1: Act with the circuit U^0 on the all-zeros state $|0\rangle$.
2: Act with $U^{1\dagger}$ and perform a measurement of all qubits in the computational basis.
3: Accept if and only if the all-zeros outcome is observed.

Algorithm 3.1 is depicted in Figure 3.1. The acceptance probability of Algorithm 3.1 is precisely equal to $\left|\langle 0|U^{1\dagger}U^0|0\rangle\right|^2$, which by definition is equal to the fidelity in (3.1). In fact, Algorithm 3.1 is a quantum computational implementation of the well known operational interpretation of the fidelity as the probability that the state ψ^0 passes a test for being the state ψ^1.

Our next quantum algorithm for estimating fidelity makes use of a Bell-state preparation and projection. Its acceptance probability is equal to

$$\frac{1}{2}\left(1 + \sqrt{F}(\psi^0, \psi^1)\right) \tag{3.2}$$

and thus gives a way to estimate the fidelity through repetition. It is a variational algorithm that optimizes over a phase ϕ and makes use of the fact that

$$\max_{\phi \in [0,2\pi]} \text{Re}[e^{i\phi} \langle \psi^0 | \psi^1 \rangle] = |\langle \psi^0 | \psi^1 \rangle|. \tag{3.3}$$

This can be seen from the fact that the optimal phase ϕ picked is such that

$$e^{i\phi} = \frac{\langle \psi^1 | \psi^0 \rangle}{|\langle \psi^1 | \psi^0 \rangle|}. \tag{3.4}$$

Let S denote the quantum system in which the states ψ^0 and ψ^1 are prepared.

Algorithm 3.2 Algorithm schematic for fidelity of pure states.

Input: Quantum circuits U^0 and U^1 that prepare ψ^0 and ψ^1.
Output: Estimate of $F(\psi^0, \psi^1)$.

1: Prepare a Bell state

$$|\Phi\rangle_{T'T} := \frac{1}{\sqrt{2}}(|00\rangle_{T'T} + |11\rangle_{T'T}) \tag{3.5}$$

on registers T' and T and prepare system S in the all-zeros state $|0\rangle_S$.

2: Using the circuits U_S^0 and U_S^1, perform the following controlled unitary:

$$\sum_{i \in \{0,1\}} |i\rangle\langle i|_T \otimes U_S^i. \tag{3.6}$$

3: Act with the following unitary on system T':

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}. \tag{3.7}$$

4: Perform a Bell measurement

$$\{\Phi_{T'T}, I_{T'T} - \Phi_{T'T}\} \tag{3.8}$$

on systems T' and T. Accept if and only if the outcome $\Phi_{T'T}$ occurs.

Figure 3.2 depicts Algorithm 3.2. After Step 3 of Algorithm 3.2, the overall state is as follows:

$$\frac{1}{\sqrt{2}} \sum_{j \in \{0,1\}} |jj\rangle_{T'T} e^{ij\phi} |\psi^j\rangle_S, \tag{3.9}$$

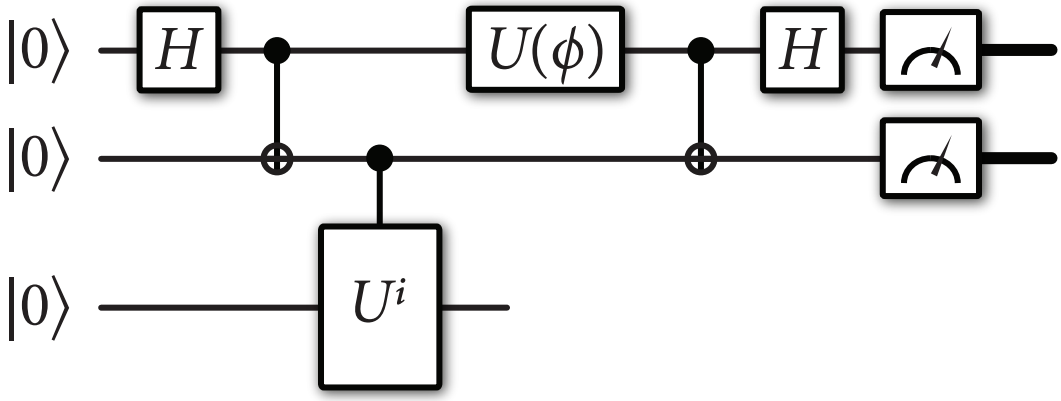


Figure 3.2: This figure depicts Algorithm 3.2 for estimating the fidelity of pure states generated by quantum circuits U^0 and U^1. The third gate with U^i in the box is defined in (3.6).

and the acceptance probability is equal to

$$\left\| \langle \Phi |_{T'T} \left(\frac{1}{\sqrt{2}} \sum_{j \in \{0,1\}} |jj\rangle_{T'T} e^{\mathrm{i}j\phi} |\psi^j\rangle_S \right) \right\|_2^2 = \frac{1}{4} \left\| \sum_{j,k \in \{0,1\}} \langle kk|jj\rangle_{T'T} e^{\mathrm{i}j\phi} |\psi^j\rangle_S \right\|_2^2 \tag{3.10}$$

$$= \frac{1}{4} \left\| \sum_{j \in \{0,1\}} e^{\mathrm{i}j\phi} |\psi^j\rangle_S \right\|_2^2 \tag{3.11}$$

$$= \frac{1}{4} \left(2 + 2\,\mathrm{Re}[e^{\mathrm{i}\phi} \langle \psi^0 | \psi^1 \rangle] \right). \tag{3.12}$$

By choosing the optimal phase ϕ in (3.3), we find that the acceptance probability is equal to the expression in (3.2). Note that, through repetition, we can execute Algorithm 3.2 in a variational way to learn the optimal value of ϕ.

Later on, in Section 3.4, we prove that a promise version of the problem of estimating the fidelity between two pure states is a BQP-complete promise problem.

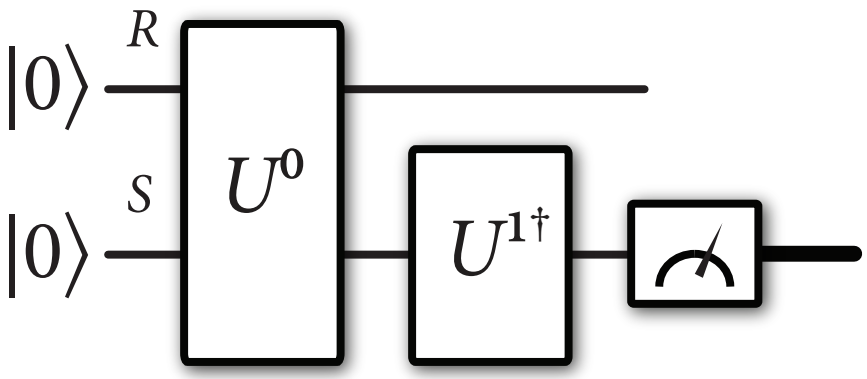


Figure 3.3: This figure depicts Algorithm 3.3 for estimating the fidelity of a mixed state generated by a quantum circuit U^0 and a pure state generated by U^1.

3.1.2 Estimating fidelity when one state is pure and the other is mixed

In this section, we outline a simple quantum algorithm that estimates the fidelity between a mixed state ρ_S and a pure state ψ_S. It is a straightforward generalization of Algorithm 3.1.

Let U^ρ_{RS} be a quantum circuit that generates a purification φ_{RS} of ρ_S when acting on the all-zeros state of systems RS, and let U^ψ_S be a circuit that generates ψ_S when acting on the all-zeros state.

Algorithm 3.3 Algorithm schematic for fidelity of a pure and a mixed state.

Input: Quantum circuits U^ρ and U^ψ that prepare a purification of ρ and ψ, respectively.

Output: Estimate of $F(\psi^0, \psi^1)$.

1: Act on the all-zeros state $|0\rangle_{RS}$ with the circuit U^ρ_{RS}.
2: Act with $U^{\psi\dagger}_S$ on system S and perform a measurement of all qubits of system S in the computational basis.
3: Accept if and only if the all-zeros outcome is observed.

Figure 3.3 depicts Algorithm 3.3. The acceptance probability of Algorithm 3.3 is equal to the fidelity $F(\psi, \rho) = \langle\psi|\rho|\psi\rangle$, which follows because

$$\left\| \langle 0|_S U_S^{\psi\dagger} U_{RS}^{\rho} |0\rangle_{RS} \right\|_2^2 = \mathrm{Tr}[(I_R \otimes |\psi\rangle\langle\psi|_S)\, |\varphi\rangle\langle\varphi|_{RS}] \tag{3.13}$$

$$= \mathrm{Tr}[|\psi\rangle\langle\psi|_S \rho_S] \tag{3.14}$$

$$= \langle\psi|\rho|\psi\rangle. \tag{3.15}$$

We note here that it is not strictly necessary to have access to the reference system R of $|\varphi\rangle_{RS}$ in order to execute Algorithm 3.3. It is only necessary to have some method of generating the reduced state ρ_S.

Later on, in Section 3.4, we prove that a promise version of the problem of estimating the fidelity of a pure state and a mixed state is a BQP-complete promise problem.

3.1.3 Estimating fidelity of arbitrary states

In this section, we outline several quantum algorithms for estimating the fidelity of arbitrary states on a quantum computer, some of which involve an interaction with a quantum prover (more precisely, the algorithms involving interaction with a prover are QSZK algorithms, where QSZK stands for "quantum statistical zero knowledge" [Wat02c, Wat09d]). The algorithms are different from the algorithm proposed in [Wat02c] (as also considered in [CSZW22]), which is based on Uhlmann's formula for fidelity [Uhl76].

Suppose that the goal is to estimate the fidelity of states ρ_S^0 and ρ_S^1, defined as [Uhl76]

$$F(\rho_S^0, \rho_S^1) := \left\| \sqrt{\rho_S^0}\, \sqrt{\rho_S^1} \right\|_1^2, \tag{3.16}$$

where the trace norm of an operator A is defined as $\|A\|_1 := \mathrm{Tr}[\sqrt{A^\dagger A}]$. Suppose also that we are given access to quantum circuits U_{RS}^0 and U_{RS}^1 that prepare purifications ψ_{RS}^0 and ψ_{RS}^1 of ρ_S^0 and ρ_S^1, respectively, when acting on the all-zeros state $|0\rangle_{RS}$. Let us recall Uhlmann's formula for fidelity [Uhl76]:

$$F(\rho_S^0, \rho_S^1) = \max_{|\psi^0\rangle_{RS}, |\psi^1\rangle_{RS}} \left| \langle\psi^1|\psi^0\rangle_{RS} \right|^2, \tag{3.17}$$

where the optimization is over all purifications ψ_{RS}^0 and ψ_{RS}^1 of ρ_S^0 and ρ_S^1, respectively. We note here that the fidelity can be computed by means of a semi-definite

program [Wat13]. Also, the promise version of this problem, involving descriptions of quantum circuits as input, is a QSZK-complete promise problem [Wat02c], where QSZK stands for quantum statistical zero knowledge (see [Wat02c, Wat09d] for details of this complexity class). Thus, it is unlikely that anyone will find a general-purpose efficient quantum algorithm for estimating fidelity (i.e., one that does not involve interaction with an all-powerful prover).

We note that the algorithms in this subsection need the purification of the state of interest to be provided. In scenarios where the purification of a state is not available, there exist variational algorithms to learn the purification [EBS+23, CSZW22].

Controlled unitary and Bell state overlap

We now detail a QSZK algorithm for estimating the following quantity:

$$\frac{1}{2}\left(1 + \sqrt{F}(\rho_S^0, \rho_S^1)\right). \tag{3.18}$$

It is a QSZK algorithm because, in the case that the fidelity $\sqrt{F}(\rho_S^0, \rho_S^1) \approx 1$, the verifier does not learn anything by interacting with the prover (i.e., the verifier only learns that the algorithm accepts with high probability). This algorithm is somewhat similar to the quantum algorithm proposed in [CHM+16], which was used for estimating a quantity known as fidelity of recovery [SW15]. It is also similar to the algorithm described in Figure 3 of [KW00]. It can be understood as a generalization of Algorithm 3.2 from pure states to arbitrary states.

Figure 3.4 depicts Algorithm 3.4.

Theorem 3.1. *The acceptance probability of Algorithm 3.4 is equal to*

$$\frac{1}{2}\left(1 + \sqrt{F}(\rho_S^0, \rho_S^1)\right). \tag{3.22}$$

Proof. The proof can be found in Appendix B.1. ■

Generalized swap test

We now detail another quantum algorithm for estimating the fidelity of arbitrary states, which is a generalization of the well known swap test from

Algorithm 3.4 Algorithm schematic to for fidelity of two mixed states.

Input: Quantum circuits U^0 and U^1 that prepare purification of ρ^0 and ρ^1, respectively.

Output: Estimate of $F(\rho^0, \rho^1)$.

1: The verifier prepares a Bell state

$$|\Phi\rangle_{T'T} := \frac{1}{\sqrt{2}}(|00\rangle_{T'T} + |11\rangle_{T'T}) \tag{3.19}$$

on registers T' and T and prepares systems RS in the all-zeros state $|0\rangle_{RS}$.

2: Using the circuits U^0_{RS} and U^1_{RS}, the verifier performs the following controlled unitary:

$$\sum_{i\in\{0,1\}} |i\rangle\langle i|_T \otimes U^i_{RS}. \tag{3.20}$$

3: The verifier transmits systems T' and R to the prover.

4: The prover prepares a system F in the $|0\rangle_F$ state and acts on systems T', R, and F with a unitary $P_{T'RF\to T''F'}$ to produce the output systems T'' and F', where T'' is a qubit system.

5: The prover sends system T'' to the verifier, who then performs a Bell measurement

$$\{\Phi_{T''T}, I_{T''T} - \Phi_{T''T}\} \tag{3.21}$$

on systems T'' and T. The verifier accepts if and only if the outcome $\Phi_{T''T}$ occurs.

[BBD+97, BCWdW01]. We note that this algorithm was used in [KW00, Figure 3] as part of their proof that QIP = QIP(3). A key difference between Algorithm 3.5 and [KW00, Figure 3] is that Algorithm 3.5 accepts if and only if both qubits at the end are measured to be in the all-zeros state, whereas it is written in [KW00, Figure 3] that their algorithm accepts if and only if the first qubit is measured to be in the zero state.

Figure 3.5 depicts Algorithm 3.5.

Theorem 3.2. *The acceptance probability of Algorithm 3.5 is equal to*

$$\frac{1}{2}\left(1 + F(\rho^0_S, \rho^1_S)\right). \tag{3.25}$$

Proof. The proof can be found in Appendix B.2. ■

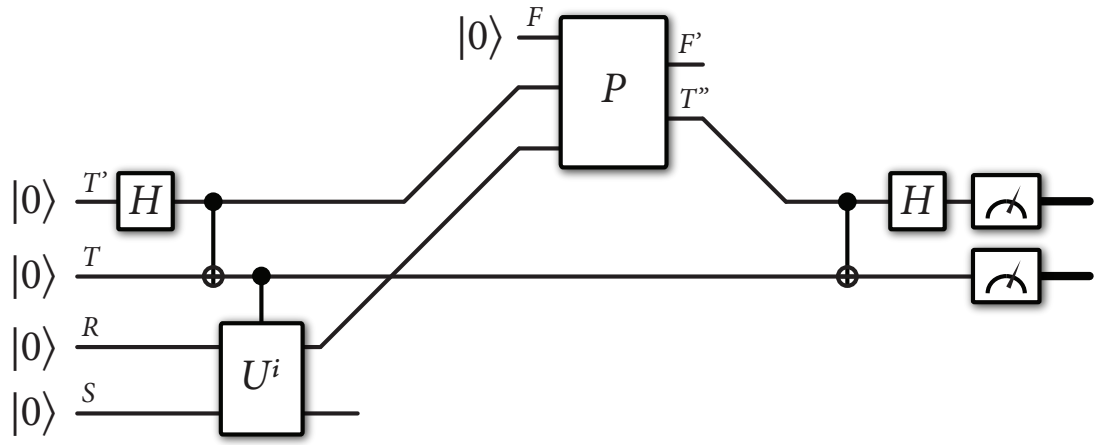


Figure 3.4: This figure depicts Algorithm 3.4 for estimating the fidelity of mixed states generated by quantum circuits U^0_{RS} and U^1_{RS}.

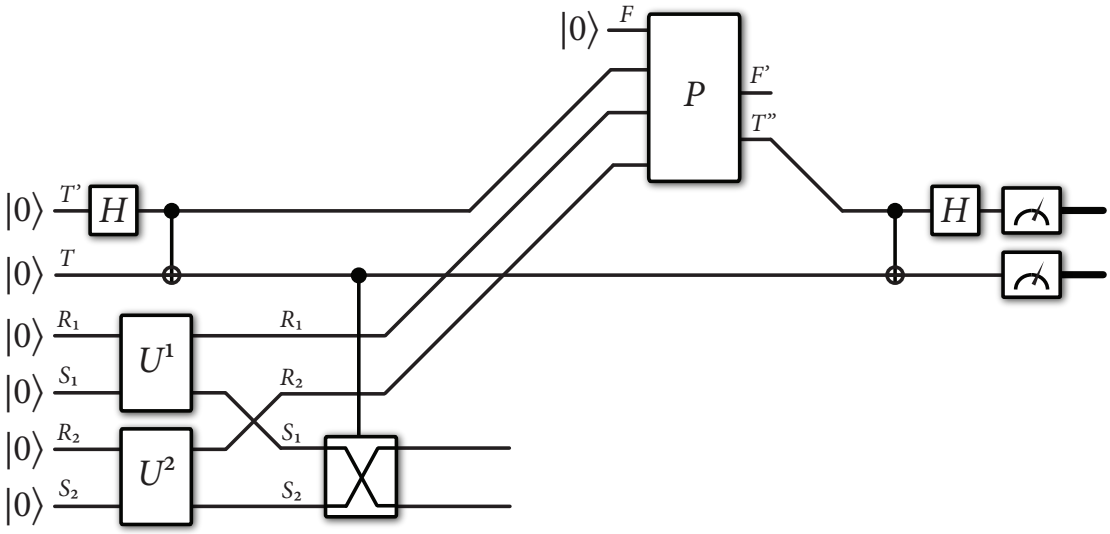


Figure 3.5: This figure depicts Algorithm 3.5 for estimating the fidelity of mixed states generated by quantum circuits U^0_{RS} and U^1_{RS}. Algorithm 3.5 represents a generalization of the well known swap test for estimating the fidelity of pure states.

Algorithm 3.5 Algorithm schematic to for fidelity of two mixed states.

Input: Quantum circuits U^0 and U^1 that prepare purification of ρ^0 and ρ^1, respectively.

Output: Estimate of $F(\rho^0, \rho^1)$.

1: The verifier prepares a Bell state

$$|\Phi\rangle_{T'T} := \frac{1}{\sqrt{2}}(|00\rangle_{T'T} + |11\rangle_{T'T}) \tag{3.23}$$

on registers T' and T and prepares systems $R_1 S_1 R_2 S_2$ in the all-zeros state $|0\rangle_{R_1 S_1 R_2 S_2}$.

2: Using the circuits U^0_{RS} and U^1_{RS}, the verifier acts on $R_1 S_1 R_2 S_2$ to prepare the two pure states $|\psi^{\rho^0}\rangle_{R_1 S_1}$ and $|\psi^{\rho^1}\rangle_{R_2 S_2}$.

3: The verifier performs a controlled SWAP from qubit T to systems S_1 and S_2, which applies the identity if the control qubit is $|0\rangle$ and swaps S_1 with S_2 if the control qubit is $|1\rangle$.

4: The verifier transmits systems T', R_1, and R_2 to the prover.

5: The prover prepares a system F in the $|0\rangle_F$ state and acts on systems T', R_1, R_2, and F with a unitary $P_{T'R_1R_2F\to T''F'}$ to produce the output systems T'' and F', where T'' is a qubit system.

6: The prover sends system T'' to the verifier, who then performs a Bell measurement

$$\{\Phi_{T''T}, I_{T''T} - \Phi_{T''T}\} \tag{3.24}$$

on systems T'' and T. The verifier accepts if and only if the outcome $\Phi_{T''T}$ occurs.

Variational algorithm with Bell measurements

A third method for estimating the fidelity of arbitrary multi-qubit states is a variational algorithm that is based on a generalization of the approach outlined in [GECP13, SCC19]. The approach from [GECP13, SCC19] employs Bell measurements to estimate the expectation of the SWAP observable, which in turn allows for estimating the fidelity of multi-qubit pure states. See also [Bru04].

We begin in this section by recalling the basic idea from [GECP13, SCC19] for estimating fidelity of pure states. Let ψ_S and φ_S be m-qubit pure states of a system S (so that $S = S_1 \cdots S_m$, where each S_i is a qubit system, for $i \in \{1, \ldots, m\}$).

Let $F_{S\tilde{S}}$ denote the unitary swap operator that swaps systems S and $\tilde{S}$, and recall that

$$\mathrm{Tr}[F_{S\tilde{S}}(\psi_S \otimes \varphi_{\tilde{S}})] = |\langle\psi|\varphi\rangle|^2 = F(\psi_S, \varphi_S). \tag{3.26}$$

Consider that

$$F_{S\tilde{S}} = F_{S_1\tilde{S}_1} \otimes F_{S_2\tilde{S}_2} \otimes \cdots \otimes F_{S_m\tilde{S}_m}. \tag{3.27}$$

Now observe that

$$F_{S_i\tilde{S}_i} = \sum_{x,z\in\{0,1\}} (-1)^{x\cdot z} \Phi^{x,z}_{S_i\tilde{S}_i}, \tag{3.28}$$

where the Bell states are defined as

$$|\Phi^{0,0}\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{3.29}$$

$$|\Phi^{0,1}\rangle := \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \tag{3.30}$$

$$|\Phi^{1,0}\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \tag{3.31}$$

$$|\Phi^{1,1}\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{3.32}$$

We then conclude that

$$\begin{aligned}
&F(\psi_S, \varphi_S) \\
&= \mathrm{Tr}\left[\left(\bigotimes_{i=1}^{m} F_{S_i\tilde{S}_i}\right)(\psi_S \otimes \varphi_{\tilde{S}})\right] && (3.33)\\
&= \mathrm{Tr}\left[\left(\bigotimes_{i=1}^{m} \sum_{x_i,z_i\in\{0,1\}} (-1)^{x_i\cdot z_i} \Phi^{x_i,z_i}_{S_i\tilde{S}_i}\right)(\psi_S \otimes \varphi_{\tilde{S}})\right] && (3.34)\\
&= \sum_{\substack{x_1,z_1,\ldots,\\ x_m,z_m\in\{0,1\}}} (-1)^{\vec{x}\cdot\vec{z}}\, \mathrm{Tr}\left[\left(\bigotimes_{i=1}^{m} \Phi^{x_i,z_i}_{S_i\tilde{S}_i}\right)(\psi_S \otimes \varphi_{\tilde{S}})\right], && (3.35)
\end{aligned}$$

where

$$\vec{x}\cdot\vec{z} \equiv \sum_{i=1}^{m} x_i \cdot z_i. \tag{3.36}$$

Thus, the approach of [GECP13, SCC19] is to estimate $F(\psi_S, \varphi_S)$ by repeatedly performing Bell measurements on corresponding qubits of ψ_S and $\varphi_{\tilde{S}}$ followed by classical postprocessing of the outcomes. In particular, for $j \in \{1, \ldots, n\}$, set

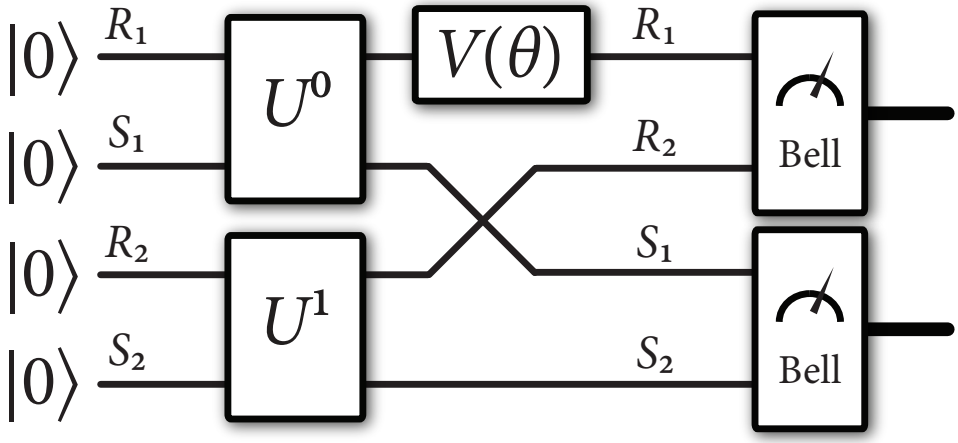


Figure 3.6: This figure depicts Algorithm 3.6 for estimating the fidelity of quantum states generated by quantum circuits U^0_{RS} and U^1_{RS}.

$Y_j = (-1)^{\sum_{i=1}^m x_i \cdot z_i}$, where $x_1, z_1, \ldots, x_m, z_m \in \{0,1\}$ are the outcomes of the Bell measurements on the jth iteration. Then set $\overline{Y^n} := \frac{1}{n}\sum_{j=1}^n Y_j$. By the Hoeffding inequality [Hoe63], for accuracy $\varepsilon \in (0,1)$ and failure probability $\delta \in (0,1)$, we are guaranteed that

$$\Pr[\left|\overline{Y^n} - F(\psi_S, \varphi_S)\right| \leq \varepsilon] \geq 1 - \delta, \tag{3.37}$$

as long as $n \geq \frac{2}{\varepsilon^2}\ln\left(\frac{2}{\delta}\right)$. Thus, the algorithm is polynomial in the inverse accuracy and logarithmic in the inverse failure probability.

We now form a simple generalization of this algorithm to estimate the fidelity of arbitrary states ρ^0_S and ρ^1_S, in which we perform a variational optimization over unitaries that act on the reference system of one of the states. For $i \in \{0,1\}$, let U^i_{RS} be an m-qubit unitary that acts on $|0\rangle_{RS}$ to generate the m-qubit state $|\psi^{\rho^i}\rangle_{RS}$; i.e.,

$$|\psi^{\rho^i}\rangle_{RS} = U^i_{RS}|0\rangle_{RS}, \tag{3.38}$$

such that

$$\rho^i_S = \mathrm{Tr}_R[|\psi^{\rho^i}\rangle\langle\psi^{\rho^i}|_{RS}]. \tag{3.39}$$

Figure 3.6 depicts Algorithm 3.6. Since this is a variational algorithm, it is not guaranteed to converge or have a specified runtime, other than running for

Algorithm 3.6 Algorithm schematic to for fidelity of two mixed states.

Input: Quantum circuits U^0 and U^1 that prepare purification of ρ^0 and ρ^1, respectively, error tolerance $\varepsilon > 0$ and $\eta, \delta \in (0, 1)$.

Output: Estimate of $F(\rho^0, \rho^1)$.

1: Prepare systems $R_1 S_1 R_2 S_2$ in the all-zeros state $|0\rangle_{R_1 S_1 R_2 S_2}$.

2: Act with the circuits U^0_{RS} and U^1_{RS} on systems $R_1 S_1 R_2 S_2$ to prepare the two pure states $|\psi^{\rho^0}\rangle_{R_1 S_1}$ and $|\psi^{\rho^1}\rangle_{R_2 S_2}$.

3: Perform a unitary $V_{R_1}(\theta)$ on system R_1.

4: For $j \in \{1, \ldots, n\}$, where $n \geq \frac{2}{\eta^2} \ln\left(\frac{2}{\delta}\right)$, for $i \in \{1, \ldots, m\}$, perform a Bell measurement on qubit i of system R_1 and qubit i of system R_2, with outcomes x^i_R and z^i_R, and perform a Bell measurement on qubit i of system S_1 and qubit i of system S_2, with outcomes x^i_S and z^i_S. Set $Y_j(\theta) = (-1)^{\sum_{i=1}^m x^i_R \cdot z^i_R + x^i_S \cdot z^i_S}$.

5: Set

$$\overline{Y^n}(\theta) := \frac{1}{n} \sum_{j=1}^{n} Y_j(\theta), \tag{3.40}$$

as an estimate of

$$F_\theta \equiv \left| \langle \psi^{\rho^1}|_{RS} V_R(\theta) \otimes I_S |\psi^{\rho^0}\rangle_{RS} \right|^2, \tag{3.41}$$

so that

$$\Pr\left[\left|\overline{Y^n}(\theta) - F_\theta\right| \leq \eta\right] \geq 1 - \delta. \tag{3.42}$$

6: Perform a maximization of the reward function $\overline{Y^n}(\theta)$ and update the parameters in θ.

7: Repeat 1-6 until the reward function $\overline{Y^n}(\theta)$ converges with tolerance ε, so that $\left|\Delta\overline{Y^n}(\theta)\right| \leq \varepsilon$, or until some maximum number of iterations is reached. (Here $\Delta\overline{Y^n}(\theta)$ represents the difference in $\overline{Y^n}(\theta)$ from the previous and current iteration.)

8: Output the final $\overline{Y^n}(\theta)$ as an estimate of the fidelity $F(\rho^0_S, \rho^1_S)$.

a maximum number of iterations. However, it is clearly a generalization of the algorithm from [GECP13, SCC19], in which we estimate the fidelity

$$\left|\langle\psi^{\rho^1}|_{RS}\, V_R(\theta)\otimes I_S\, |\psi^{\rho^0}\rangle_{RS}\right|^2 = F(\psi^{\rho^1}_{RS}, V_R(\theta)\psi^{\rho^0}_{RS} V_R(\theta)^\dagger) \tag{3.43}$$

at each iteration of the algorithm. If we could actually optimize over all possible unitaries acting on the reference system R, then the algorithm would indeed estimate the fidelity, as a consequence of Uhlmann's theorem [Uhl76]:

$$F(\rho^0_S, \rho^1_S) = \sup_{V_R} F(\psi^{\rho^1}_{RS}, V_R \psi^{\rho^0}_{RS} V_R^\dagger). \tag{3.44}$$

However, by optimizing over only a subset of all unitaries, Algorithm 3.6 estimates a lower bound on the fidelity $F(\rho^0_S, \rho^1_S)$.

Variational algorithm for Fuchs–Caves measurement

Algorithm 3.4 from Section 3.1.3 is based on Uhlmann's formula for fidelity in (3.17), and the same is true for Algorithm 3.5 from Section 3.1.3 and Algorithm 3.6 from Section 3.1.3. An alternate optimization formula for the fidelity of states ρ^0_S and ρ^1_S is as follows [FC95]:

$$F(\rho^0_S, \rho^1_S) = \left[\min_{\{\Lambda^x_S\}_x} \sum_x \sqrt{\mathrm{Tr}[\Lambda^x_S \rho^0_S]\,\mathrm{Tr}[\Lambda^x_S \rho^1_S]}\right]^2, \tag{3.45}$$

where the minimization is over every positive operator-valued measure $\left\{\Lambda^x_S\right\}_x$ (i.e., the operators satisfy $\Lambda^x_S \geq 0$ for all x and $\sum_x \Lambda^x_S = I_S$). A measurement achieving the optimal value of the fidelity is known as the Fuchs–Caves measurement [FC95] and has the form $\{|\varphi_x\rangle\langle\varphi_x|\}_x$, where $|\varphi_x\rangle$ is an eigenvector, with eigenvalue λ_x, of the following operator geometric mean of ρ^0 and $(\rho^1)^{-1}$ (also called "quantum likelihood ratio" operator in [Fuc96]):

$$M := \left(\rho^1\right)^{-1/2} \sqrt{\left(\rho^1\right)^{1/2} \rho^0 \left(\rho^1\right)^{1/2}} \left(\rho^1\right)^{-1/2}, \tag{3.46}$$

so that

$$M = \sum_x \lambda_x |\varphi_x\rangle\langle\varphi_x|. \tag{3.47}$$

That is, it is known from [FC95, Fuc96] that

$$F(\rho_S^0, \rho_S^1) = \left[\sum_x \sqrt{\mathrm{Tr}[|\varphi_x\rangle\langle\varphi_x|\rho_S^0]\,\mathrm{Tr}[|\varphi_x\rangle\langle\varphi_x|\rho_S^1]} \right]^2 . \tag{3.48}$$

Thus, we can build a variational algorithm around this formulation of fidelity, with the idea being to optimize over parameterized measurements in an attempt to optimize the fidelity, while at the same time learn the Fuchs–Caves measurement (or a different fidelity-achieving measurement). In contrast to the other variational algorithms presented in previous sections, this alternate approach leads to an upper bound on the fidelity.

Before detailing the algorithm, recall the Naimark extension theorem [Nai40] (see also [Wil17, Wat18, KW20]), which states that a general POVM $\{\Lambda_S^x\}_x$ with m outcomes, acting on a quantum state ρ of a d-dimensional system S, can be realized as a unitary interaction U_{SP} of the system S with an m-dimensional probe system P, followed by a projective measurement $\{|x\rangle\langle x|_P\}_x$ acting on the probe system. That is,

$$\mathrm{Tr}[\Lambda_S^x \rho_S] = \mathrm{Tr}[(I_S \otimes |x\rangle\langle x|_P) U_{SP} (\rho_S \otimes |0\rangle\langle 0|_P) U_{SP}^\dagger]. \tag{3.49}$$

It suffices to choose U_{SP} so that

$$U_{SP}|\psi\rangle_S|0\rangle_P = \sum_x \sqrt{\Lambda_S^x}|\psi\rangle_S|x\rangle_P. \tag{3.50}$$

Thus, we can express the optimization problem in (3.45) as follows:

$$\sqrt{F}(\rho_S^0, \rho_S^1) = \min_{U_{SP}} \sum_x \sqrt{\begin{matrix}\mathrm{Tr}[(I_S \otimes |x\rangle\langle x|_P) U_{SP} (\rho_S^0 \otimes |0\rangle\langle 0|_P) U_{SP}^\dagger] \times \\ \mathrm{Tr}[(I_S \otimes |x\rangle\langle x|_P) U_{SP} (\rho_S^1 \otimes |0\rangle\langle 0|_P) U_{SP}^\dagger]\end{matrix}} . \tag{3.51}$$

By replacing the optimization in (3.51) over all unitaries with an optimization over parameterized ones, we arrive at a variational algorithm for estimating fidelity in Algorithm 3.7.

Figure 3.7 depicts Algorithm 3.7. As before, since this is a variational algorithm, it is not guaranteed to converge or have a specified runtime, other than running for a maximum number of iterations. One advantage of this algorithm is that it does not require purifications of the states ρ_S^0 and ρ_S^1. All it requires is a circuit or method to prepare these states, and then it performs measurements on these states, in an attempt to learn an optimal measurement with respect to the cost function $F(\tilde{p}_\theta, \tilde{q}_\theta)$.

Algorithm 3.7 Algorithm schematic to for fidelity of two mixed states.

Input: Quantum states ρ^0 and ρ^1, $n \in \mathbb{N}$ and the error tolerance $\varepsilon > 0$.
Output: Estimate of $F(\rho^0, \rho^1)$.

1: For $j \in \{1, \ldots, n\}$, prepare system S_1 in the state $\rho^0_{S_1}$ and system S_2 in the state $\rho^1_{S_2}$, and prepare systems P_1 and P_2 in the all-zeros state $|0\rangle_{P_1} \otimes |0\rangle_{P_2}$.
2: Act with the circuit $U_{S_1P_1}(\theta)$ on systems S_1P_1 and act with the same circuit $U_{S_2P_2}(\theta)$ on systems S_2P_2.
3: Measure system P_1 in the computational basis and record the outcome as y_j, and measure system P_2 in the computational basis and record the outcome as z_j.
4: Using the measurement data $\left\{y_j\right\}_{j=1}^n$ and $\left\{z_j\right\}_{j=1}^n$, calculate the empirical distributions $\tilde{p}_\theta(x)$ and $\tilde{q}_\theta(x)$, where $\tilde{p}_\theta(x)$ is the empirical distribution resulting from

$$p_\theta(x) \coloneqq \text{Tr}[(I_S \otimes |x\rangle\langle x|_P)U_{SP}(\theta)(\rho^0_S \otimes |0\rangle\langle 0|_P)U^\dagger_{SP}(\theta)], \tag{3.52}$$

and $\tilde{q}_\theta(x)$ is the empirical distribution resulting from

$$q_\theta(x) \coloneqq \text{Tr}[(I_S \otimes |x\rangle\langle x|_P)U_{SP}(\theta)(\rho^1_S \otimes |0\rangle\langle 0|_P)U^\dagger_{SP}(\theta)]. \tag{3.53}$$

5: Output

$$F(\tilde{p}_\theta, \tilde{q}_\theta) \coloneqq \left[\sum_x \sqrt{\tilde{p}_\theta(x)\tilde{q}_\theta(x)}\right]^2 \tag{3.54}$$

as an estimate of $F(p_\theta, q_\theta)$.
6: Perform a minimization of the cost function $F(\tilde{p}_\theta, \tilde{q}_\theta)$ and update the parameters in θ.
7: Repeat 1-6 until the cost function $F(\tilde{p}_\theta, \tilde{q}_\theta)$ converges with tolerance ε, so that $|\Delta F(\tilde{p}_\theta, \tilde{q}_\theta)| \leq \varepsilon$, or until some maximum number of iterations is reached. (Here $\Delta F(\tilde{p}_\theta, \tilde{q}_\theta)$ represents the difference in $F(\tilde{p}_\theta, \tilde{q}_\theta)$ from the previous and current iteration.)
8: Output the final value of $F(\tilde{p}_\theta, \tilde{q}_\theta)$ as an estimate of the fidelity $F(\rho^0_S, \rho^1_S)$.

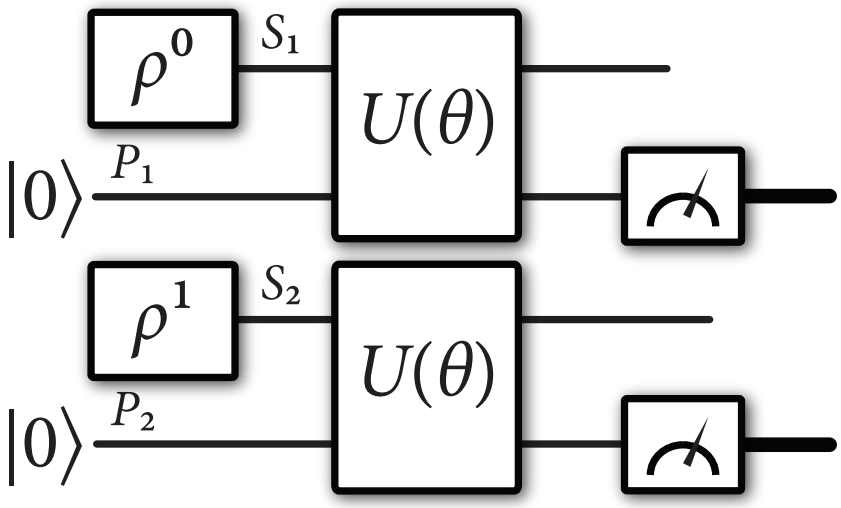


Figure 3.7: This figure depicts Algorithm 3.7 for estimating the fidelity of quantum states ρ_S^0 and ρ_S^1. The boxes enclosing ρ^0 and ρ^1 indicate that these are some mechanisms by which these states are prepared.

In Algorithm 3.7, we did not specify how large n should be in order to get a desired accuracy of the estimator in (3.54) for the classical fidelity $F(p_\theta, q_\theta)$. This estimator is called a "plug-in estimator" in the literature on this topic, and it is a biased estimator, which however converges to $F(p_\theta, q_\theta)$ in the asymptotic limit $n \to \infty$. As a consequence of the estimator in (3.54) being biased, the Hoeffding inequality does not readily apply in this case. As far as we can tell, it is an open question to determine the rate of convergence of this estimator to $F(p_\theta, q_\theta)$. Related work on this topic has been considered in [JVHW15, AOST17].

3.1.4 Estimating fidelity of channels

In this section, we outline a method for estimating the fidelity of channels on a quantum computer, by means of an interaction with competing quantum provers [GW05, Gut05, GW07, Gut09, GW13]. The goal of one prover is to maximize the acceptance probability, while the goal of the other prover is to minimize the acceptance probability. We refer to the first prover as the max-prover and the second as the min-prover. The specific setting that we deal with is called a double quan-

tum interactive proof (DQIP) [GW13], due to the fact that the min-prover goes first and then the max-prover goes last. The class of promise problems that can be solved in this model is equivalent to PSPACE [GW13], which is the class of problems that can be decided on a classical computer with polynomial memory.

Let us recall that the fidelity of channels $\mathcal{N}^0_{A\to B}$ and $\mathcal{N}^1_{A\to B}$ is defined as follows [GLN05]:

$$F(\mathcal{N}^0_{A\to B}, \mathcal{N}^1_{A\to B}) := \inf_{\rho_{RA}} F(\mathcal{N}^0_{A\to B}(\rho_{RA}), \mathcal{N}^1_{A\to B}(\rho_{RA})), \tag{3.55}$$

where the infimum is over every state ρ_{RA}, with the reference system R arbitrarily large. It is known that the infimum is achieved by a pure state ψ_{RA} with the reference system R isomorphic to the channel input system A, so that

$$F(\mathcal{N}^0_{A\to B}, \mathcal{N}^1_{A\to B}) := \min_{\psi_{RA}} F(\mathcal{N}^0_{A\to B}(\psi_{RA}), \mathcal{N}^1_{A\to B}(\psi_{RA})). \tag{3.56}$$

It is also known that it is possible to calculate the fidelity of channels by means of a semi-definite program [YF17, KW21], which provides a way to verify the output of our proposed algorithm for sufficiently small examples.

Suppose that the goal is to estimate the fidelity of channels $\mathcal{N}^0_{A\to B}$ and $\mathcal{N}^1_{A\to B}$, and we are given access to quantum circuits $U^0_{AE'\to BE}$ and $U^1_{AE'\to BE}$ that realize isometric extensions of the channels $\mathcal{N}^0_{A\to B}$ and $\mathcal{N}^1_{A\to B}$, respectively, in the sense that

$$\mathcal{N}^i_{A\to B}(\omega_A) = \operatorname{Tr}_E[U^i_{AE'\to BE}(\omega_A \otimes |0\rangle\langle 0|_{E'})(U^i_{AE'\to BE})^\dagger], \tag{3.57}$$

for $i \in \{0, 1\}$.

We now provide a DQIP algorithm for estimating the following quantity:

$$\frac{1}{2}\left(1 + \sqrt{F}(\mathcal{N}^0_{A\to B}, \mathcal{N}^1_{A\to B})\right), \tag{3.58}$$

which is based in part on Algorithm 3.4 but instead features an optimization over input states of the min-prover.

Figure 3.8 depicts Algorithm 3.8.

Theorem 3.3. *The acceptance probability of Algorithm 3.8 is equal to*

$$\frac{1}{2}\left(1 + \sqrt{F}(\mathcal{N}^0_{A\to B}, \mathcal{N}^1_{A\to B})\right). \tag{3.62}$$

Proof. The proof can be found in Appendix B.3. ■

Algorithm 3.8 Algorithm schematic to for fidelity of two channels

Input: Quantum circuits U^0 and U^1 that realize isometric extensions of the channels $\mathcal{N}^0$ and $\mathcal{N}^1$, respectively.

Output: Estimate of $F(\mathcal{N}^0, \mathcal{N}^1)$.

1: The verifier prepares a Bell state

$$|\Phi\rangle_{T'T} := \frac{1}{\sqrt{2}}(|00\rangle_{T'T} + |11\rangle_{T'T}) \tag{3.59}$$

on registers T' and T and prepares system E' in the all-zeros state $|0\rangle_{E'}$.

2: The min-prover transmits the system A of the state $|\psi\rangle_{RA}$ to the verifier.

3: Using the circuits $U^0_{AE'\to BE}$ and $U^1_{AE'\to BE'}$ the verifier performs the following controlled unitary:

$$\sum_{i\in\{0,1\}} |i\rangle\langle i|_T \otimes U^i_{AE'\to BE}. \tag{3.60}$$

4: The verifier transmits systems T' and E to the max-prover.

5: The max-prover prepares a system F in the $|0\rangle_F$ state and acts on systems T', E, and F with a unitary $P_{T'EF\to T''F'}$ to produce the output systems T'' and F', where T'' is a qubit system.

6: The max-prover sends system T'' to the verifier, who then performs a Bell measurement

$$\{\Phi_{T''T}, I_{T''T} - \Phi_{T''T}\} \tag{3.61}$$

on systems T'' and T. The verifier accepts if and only if the outcome $\Phi_{T''T}$ occurs.

Proposition 3.1. *An alternative expression for the acceptance probability of Algorithm 3.8 is*

$$\min_{\rho_{RA}} \max_{\mathcal{P}_{T'E\to T''}} \operatorname{Tr}[\Phi_{T''T}\mathcal{P}_{T'E\to T''}(\mathcal{M}_{A\to T'TBE}(\rho_{RA}))] = \max_{\mathcal{P}_{T'E\to T''}} \min_{\rho_{RA}} \operatorname{Tr}[\Phi_{T''T}\mathcal{P}_{T'E\to T''}(\mathcal{M}_{A\to T'TBE}(\rho_{RA}))], \tag{3.63}$$

where ρ_{RA} is a quantum state, $\mathcal{P}_{T'E\to T''}$ is a quantum channel, and $\mathcal{M}_{A\to T'TBE}$ is a quantum channel defined as

$$\mathcal{M}_{A\to T'TBE}(\rho_{RA}) := \frac{1}{2}\sum_{i,j\in\{0,1\}} |ii\rangle\langle jj|_{T'T} \otimes U^i(\rho_{RA}\otimes|0\rangle\langle 0|_{E'})(U^j)^\dagger, \tag{3.64}$$

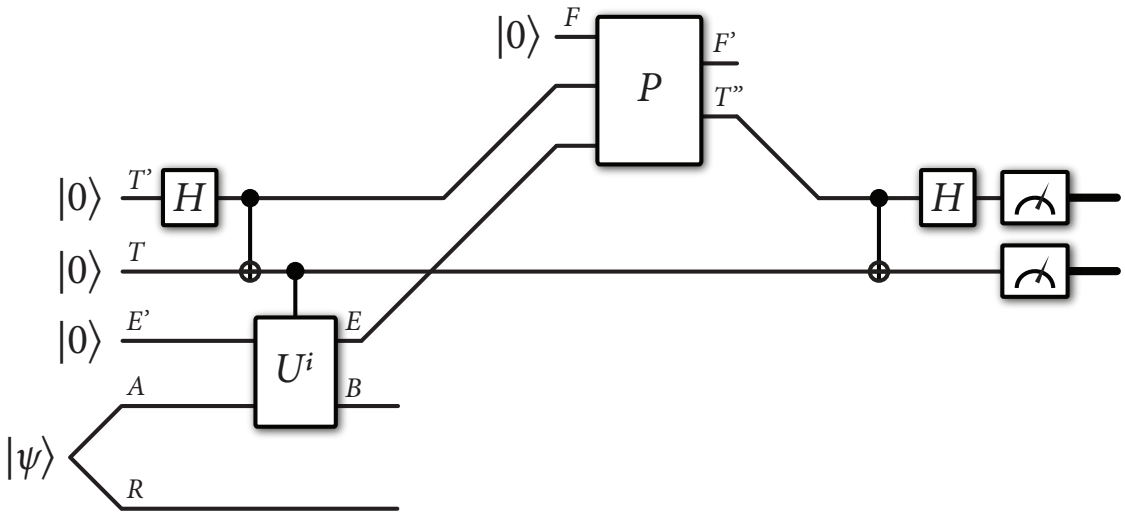


Figure 3.8: This figure depicts Algorithm 3.8 for estimating the fidelity of quantum channels generated by quantum circuits $U^0_{AE'\to BE}$ and $U^1_{AE'\to BE}$. The min-prover prepares the state $|\psi\rangle_{RA}$ and the max-prover acts with the unitary $P_{T'EF\to T''F'}$.

with $U^i \equiv U^i_{AE'\to BE}$.

Proof. In Step 2 of Algorithm 3.8, the min-prover could send a mixed quantum state ρ_{RA} instead of sending a pure state. The acceptance probability does not change under this modification due to the argument around (3.55)–(3.56). Furthermore, due to the Stinespring dilation theorem [Sti55], the actions of tensoring in $|0\rangle_F$, performing the unitary $P_{T'EF\to T''F'}$, and tracing over system F' are equivalent to performing a quantum channel $\mathcal{P}_{T'E\to T''}$. Under these observations, consider that the acceptance probability is then equal to

$$\mathrm{Tr}[\Phi_{T''T}\mathcal{P}_{T'E\to T''}(\mathcal{M}_{A\to T'TBE}(\rho_{RA}))], \tag{3.65}$$

where the quantum channel $\mathcal{M}_{A\to T'TBE}$ is defined in (3.64). Performing the optimizations $\min_{\rho_{RA}} \max_{\mathcal{P}_{T'E\to T''}}$ then leads to the first expression in (3.63). Considering that the set of channels is convex and the set of states is convex, and the objective function in (3.65) is linear in ρ_{RA} for fixed $\mathcal{P}_{T'E\to T''}$ and linear in $\mathcal{P}_{T'E\to T''}$ for fixed ρ_{RA}, the minimax theorem [Sio58] applies and we can exchange the optimizations. ■

Proposition 3.1 indicates that if the provers involved can optimize over all possible states and channels, then indeed the order of optimization can be exchanged.

However, in a variational algorithm, the optimization is generally dependent upon the order in which it is conducted because we are not optimizing over all possible states and channels, but instead optimizing over parameterized circuits. In this latter case, the state space is no longer convex and the objective function no longer linear in these parameters. However, we can still attempt the following "see-saw" strategy in a variational algorithm: first minimize the objective function with respect to the input state ψ_{RA} while keeping the unitary $P_{T'EF\to T''F'}$ fixed. Then maximize the objective function with respect to the unitary $P_{T'EF\to T''F'}$ while keeping the state ψ_{RA} fixed. Then repeat this process some number of times. We consider this approach in Section 3.3.5.

3.1.5 Alternate methods of estimating the fidelity of channels

We note briefly here that other methods for estimating fidelity of channels can be based on Algorithms 3.5, 3.6, and 3.7. It is not clear how to phrase them in the language of quantum interactive proofs, in such a way that the acceptance probability is a simple function of the channel fidelity. However, we can employ variational algorithms in which we repeat the circuit for determining an optimal input state ψ_{RA} for the channel fidelity. Then these variational algorithms employ an extra minimization step in order to approximate an optimal input state for the channel fidelity.

3.1.6 Estimating maximum output fidelity of channels

In this section, we show how a simple variation of Algorithm 3.8, in which we combine the actions of the min-prover and max-prover into a single max-prover, leads to a QIP algorithm for estimating the following fidelity function of two quantum channels $\mathcal{N}^0_{A\to B}$ and $\mathcal{N}^1_{A\to B}$:

$$F_{\max}(\mathcal{N}^0,\mathcal{N}^1) := \sup_{\rho_A} F(\mathcal{N}^0_{A\to B}(\rho_A),\mathcal{N}^1_{A\to B}(\rho_A)), \tag{3.66}$$

where the optimization is over every input state ρ_A. This algorithm is based in part on Algorithm 3.4 but instead features an optimization over input states of the prover.

Figure 3.9 depicts Algorithm 3.9.

Algorithm 3.9 Algorithm schematic for max output fidelity of channels

Input: Quantum circuits U^0 and U^1 that realize isometric extensions of the channels $\mathcal{N}^0$ and $\mathcal{N}^1$, respectively.

Output: Estimate of $F_{\max}(\mathcal{N}^0, \mathcal{N}^1)$.

1: The verifier prepares a Bell state

$$|\Phi\rangle_{T'T} := \frac{1}{\sqrt{2}}(|00\rangle_{T'T} + |11\rangle_{T'T}) \tag{3.67}$$

on registers T' and T and prepares system E' in the all-zeros state $|0\rangle_{E'}$.

2: The prover transmits the system A of the state $|\psi\rangle_{RA}$ to the verifier.

3: Using the circuits $U^0_{AE'\to BE}$ and $U^1_{AE'\to BE'}$ the verifier performs the following controlled unitary:

$$\sum_{i\in\{0,1\}} |i\rangle\langle i|_T \otimes U^i_{AE'\to BE}. \tag{3.68}$$

4: The verifier transmits systems T' and E to the prover.

5: The prover prepares a system F in the $|0\rangle_F$ state and acts on systems T', E, and F with a unitary $P_{T'EF\to T''F'}$ to produce the output systems T'' and F', where T'' is a qubit system.

6: The prover sends system T'' to the verifier, who then performs a Bell measurement

$$\{\Phi_{T''T}, I_{T''T} - \Phi_{T''T}\} \tag{3.69}$$

on systems T'' and T. The verifier accepts if and only if the outcome $\Phi_{T''T}$ occurs.

Theorem 3.4. *The acceptance probability of Algorithm 3.9 is equal to*

$$\frac{1}{2}\left(1 + \sqrt{F_{\max}}(\mathcal{N}^0_{A\to B}, \mathcal{N}^1_{A\to B})\right). \tag{3.70}$$

Proof. The proof can be found in Appendix B.4. ■

3.1.7 Generalization to multiple states

In this section, we generalize Algorithm 3.4 to multiple states, by devising a quantum algorithm that tests how similar all the states of an ensemble are to each other.

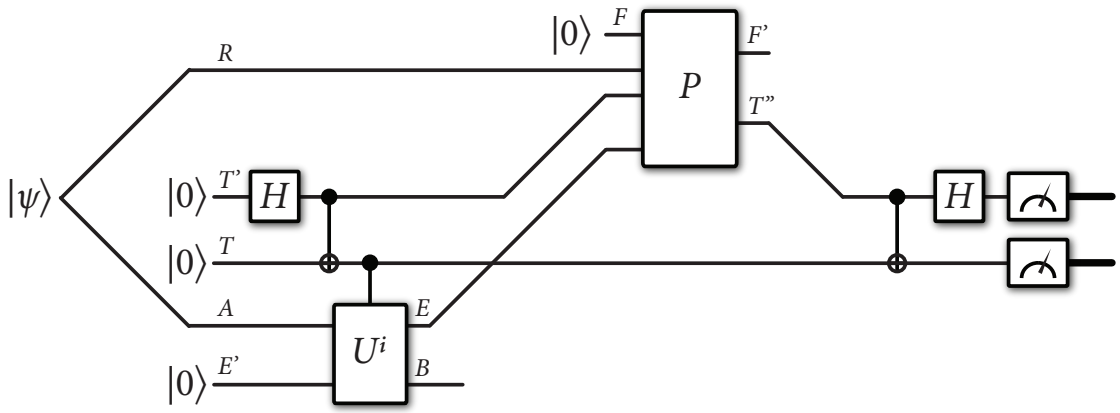


Figure 3.9: This figure depicts Algorithm 3.9 for generating a state ρ_A that maximizes the fidelity of quantum channels generated by quantum circuits $U^0_{AE'\to BE}$ and $U^1_{AE'\to BE}$.

Suppose that we are given an ensemble $\left\{p(x), \rho^x_S\right\}_{x\in\mathcal{X}}$ of states of system S, with $d = |\mathcal{X}|$, and we would like to know how similar they are to each other. Then we can perform a test like that given in Algorithm 3.4, but it is a multiple-state similarity test. The main difference is that the verifier prepares an initial entangled state that encodes the prior probabilities $\{p(x)\}_{x\in\mathcal{X}}$ and the algorithm employs d-dimensional control systems throughout, instead of qubit control systems. We suppose that, for all $x \in \mathcal{X}$, there is a circuit U^x_{RS} that generates a purification $|\psi^x\rangle_{RS}$ as follows:

$$|\psi^x\rangle_{RS} := U^x_{RS}|0\rangle_{RS}, \tag{3.71}$$

$$\rho^x_S = \mathrm{Tr}_R[|\psi^x\rangle\langle\psi^x|_{RS}]. \tag{3.72}$$

Theorem 3.5. *The acceptance probability of Algorithm 3.10 is equal to*

$$p_{\mathrm{sim}}(\{p(x), \rho^x_S\}_{x\in\mathcal{X}}) := \frac{1}{d}\left[\sup_{\sigma_S}\sum_{x\in\mathcal{X}}\sqrt{p(x)}\,\sqrt{F}(\rho^x_S, \sigma_S)\right]^2, \tag{3.78}$$

where the optimization is over every density operator σ_S. This acceptance probability is bounded from above by

$$\frac{1}{d} + \frac{2}{d}\sum_{x,y\in\mathcal{X}:x<y}\sqrt{p(x)p(y)}\,\sqrt{F}(\rho^x_S, \rho^y_S). \tag{3.79}$$

Algorithm 3.10 Algorithm schematic for fidelity of multiple states

Input: Quantum circuits $\{U^x\}_{x\in\mathcal{X}}$ that prepare purifications of states $\{\rho^x\}_{x\in\mathcal{X}}$, respectively, and probability distribution $\{p(x)\}_{x\in\mathcal{X}}$.

Output: Estimate of $p_{\text{sim}}(\{p(x),\rho^x\}_{x\in\mathcal{X}})$.

1: The verifier prepares a state

$$|\Phi^p\rangle_{T'T} \coloneqq \sum_{x\in\mathcal{X}} \sqrt{p(x)}|xx\rangle_{T'T} \tag{3.73}$$

on registers T' and T and prepares systems RS in the all-zeros state $|0\rangle_{RS}$.

2: Using the circuits in the set $\{U^x_{RS}\}_{x\in\mathcal{X}}$, the verifier performs the following controlled unitary:

$$\sum_{x\in\mathcal{X}} |x\rangle\langle x|_T \otimes U^x_{RS}. \tag{3.74}$$

3: The verifier transmits systems T' and R to the prover.

4: The prover prepares a system F in the $|0\rangle_F$ state and acts on systems T', R, and F with a unitary $P_{T'RF\to T''F'}$ to produce the output systems T'' and F', where T'' is a qudit system.

5: The prover sends system T'' to the verifier, who then performs a qudit Bell measurement

$$\{\Phi_{T''T}, I_{T''T} - \Phi_{T''T}\} \tag{3.75}$$

on systems T'' and T, where

$$\Phi_{T''T} = |\Phi\rangle\langle\Phi|_{T''T}, \tag{3.76}$$

$$|\Phi\rangle_{T''T} \coloneqq \frac{1}{\sqrt{d}} \sum_{x\in\mathcal{X}} |xx\rangle_{T''T}. \tag{3.77}$$

The verifier accepts if and only if the outcome $\Phi_{T''T}$ occurs.

When $d = 2$, this upper bound is tight.

Proof. The proof can be found in Appendix B.5. ■

Corollary 3.1. *The fact that the upper bound is achieved in Theorem 3.5 for $d = 2$ leads to the following identity for states ρ_S^0 and ρ_S^1 and probability $p \in [0, 1]$:*

$$\left[\sup_{\sigma_S} \sqrt{p}\,\sqrt{F}(\rho_S^0, \sigma_S) + \sqrt{1-p}\,\sqrt{F}(\rho_S^1, \sigma_S)\right]^2 = 1 + 2\sqrt{p(1-p)}\,\sqrt{F}(\rho_S^0, \rho_S^1), \tag{3.80}$$

where the optimization is over every density operator σ_S.

The acceptance probability in (3.78) is proportional to the secrecy measure discussed in [KRS09, Eq. (19)], which is the same as the max-conditional entropy of the following classical–quantum state:

$$\sum_{x \in \mathcal{X}} p(x)|x\rangle\langle x|_T \otimes \rho_S^x. \tag{3.81}$$

Indeed, it is a measure of secrecy because if an eavesdropper has access to system S and if $\rho_S^x \approx \sigma$ for all $x \in \mathcal{X}$ and if $p(x) \approx 1/d$, then it is difficult for the eavesdropper to guess the classical message in system T (also, the fidelity is close to one). According to [SDG+21, Remark 2.7] and the expression in (B.64) of Appendix B.5, the acceptance probability in (3.78) is also a measure of the symmetric distinguishability of the classical–quantum state in (3.81), and thus gives this measure an operational meaning.

The upper bound in (3.79) on the acceptance probability has some conceptual similarity with known upper bounds on the success probability in state discrimination [Mon08, Qiu08], in the sense that we employ the fidelity of pairs of states in the upper bound. Finally, we note some similarities between the problem outlined here and coherent channel discrimination considered recently in [Wil20]. However, these two problems are ultimately different in their objectives.

3.1.8 Generalization to multiple channels

We now generalize Algorithms 3.8 and 3.10 to the case of testing the similarity of an ensemble of channels. The resulting algorithm thus has applications in the context of private quantum reading [BDW18, DBW20], in which one goal of such a protocol is to encode a classical message into a channel selected randomly from

an ensemble of channels such that it is indecipherable by an eavesdropper who has access to the output of the channel.

Let us first consider the case of channels. In more detail, let $\{p(x), \mathcal{N}^x_{A\to B}\}_{x\in\mathcal{X}}$ be an ensemble of quantum channels. Set $d = |\mathcal{X}|$. We suppose that, for all $x \in \mathcal{X}$, there is a circuit $U^x_{AE'\to BE}$ that generates an isometric extension of the channel $\mathcal{N}^x_{A\to B}$, in the following sense:

$$\mathcal{N}^x_{A\to B}(\omega_A) = \mathrm{Tr}_E[U^x_{AE'\to BE}(\omega_A \otimes |0\rangle\langle 0|_{E'})(U^x_{AE'\to BE})^\dagger]. \tag{3.82}$$

The following algorithm employs competing provers, similar to how Algorithm 3.8 does.

Algorithm 3.11 Algorithm schematic for fidelity of multiple channels.

Input: Quantum circuits $\{U^x\}_{x\in\mathcal{X}}$ that realize isometric extensions of the channels $\{\mathcal{N}^x\}_{x\in\mathcal{X}}$, respectively, and probability distribution $\{p(x)\}_{x\in\mathcal{X}}$.

Output: Estimate of Estimate of $p_{\mathrm{sim}}(\{p(x), \mathcal{N}^x\}_{x\in\mathcal{X}})$.

1: The verifier prepares a state

$$|\Phi^p\rangle_{T'T} := \sum_{x\in\mathcal{X}} \sqrt{p(x)}|xx\rangle_{T'T} \tag{3.83}$$

on registers T' and T and prepares system E' in the all-zeros state $|0\rangle_{RS}$.

2: The min-prover transmits the system A of the state $|\psi\rangle_{RA}$ to the verifier.

3: Using the circuits in the set $\{U^x_{AE'\to BE}\}_{x\in\mathcal{X}}$, the verifier performs the following controlled unitary:

$$\sum_{x\in\mathcal{X}} |x\rangle\langle x|_T \otimes U^x_{AE'\to BE}. \tag{3.84}$$

4: The verifier transmits systems T' and E to the max-prover.

5: The max-prover prepares a system F in the $|0\rangle_F$ state and acts on systems T', R, and F with a unitary $P_{T'EF\to T''F'}$ to produce the output systems T'' and F', where T'' is a qudit system.

6: The max-prover sends system T'' to the verifier, who then performs a qudit Bell measurement

$$\{\Phi_{T''T}, I_{T''T} - \Phi_{T''T}\} \tag{3.85}$$

on systems T'' and T, where $\Phi_{T''T}$ is defined in (3.76). The verifier accepts if and only if the outcome $\Phi_{T''T}$ occurs.

Theorem 3.6. *The acceptance probability of Algorithm 3.11 is equal to*

$$p_{\text{sim}}(\{p(x), \mathcal{N}^x\}_{x\in\mathcal{X}}) = \frac{1}{d}\left[\inf_{\psi_{RA}} \sup_{\sigma_{RB}} \sum_{x\in\mathcal{X}} \sqrt{p(x)}\, \sqrt{F}(\mathcal{N}^x_{A\to B}(\psi_{RA}), \sigma_{RB})\right]^2. \tag{3.86}$$

This acceptance probability is bounded from above by

$$\frac{1}{d} + \frac{2}{d} \times \inf_{\psi_{RA}} \sum_{\substack{x,y\in\mathcal{X}:\\ x<y}} \sqrt{p(x)p(y)}\, \sqrt{F}(\mathcal{N}^x_{A\to B}(\psi_{RA}), \mathcal{N}^y_{A\to B}(\psi_{RA})). \tag{3.87}$$

When $d = 2$, this upper bound is tight.

Proof. The proof can be found in Appendix B.6. ■

Corollary 3.2. *The following identity holds in the special case of two channels $\mathcal{N}^0_{A\to B}$ and $\mathcal{N}^1_{A\to B}$ and probability $p \in [0, 1]$:*

$$\left[\inf_{\psi_{RA}} \sup_{\sigma_{RB}} \left(\begin{array}{c} \sqrt{p}\, \sqrt{F}(\mathcal{N}^0_{A\to B}(\psi_{RA}), \sigma_{RB}) \\ + \sqrt{1-p}\, \sqrt{F}(\mathcal{N}^1_{A\to B}(\psi_{RA}), \sigma_{RB}) \end{array} \right)\right]^2$$
$$= 1 + 2\sqrt{p\,(1-p)} \inf_{\psi_{RA}} \sqrt{F}(\mathcal{N}^0_{A\to B}(\psi_{RA}), \mathcal{N}^1_{A\to B}(\psi_{RA})), \tag{3.88}$$

where the supremum is with respect to every density operator σ_{RB}.

We can also generalize Algorithm 3.9 from Section 3.1.6, to estimate the following similarity measure for an ensemble $\{p(x), \mathcal{N}^x_{A\to B}\}_{x\in\mathcal{X}}$ of channels:

$$\frac{1}{d}\left[\sup_{\rho_A,\sigma_B} \sum_{x\in\mathcal{X}} \sqrt{p(x)}\, \sqrt{F}(\mathcal{N}^x_{A\to B}(\rho_A), \sigma_B)\right]^2, \tag{3.89}$$

where the optimization is over all density operators ρ_A and σ_B. As is the case with Algorithm 3.9, there is a single prover who is trying to make all of the channel outputs look like the same state. Again we suppose that there is a circuit $U^x_{AE'\to BE}$ that generates an isometric extension of the channel $\mathcal{N}^x_{A\to B}$, in the sense of (3.82).

Theorem 3.7. *The acceptance probability of Algorithm 3.12 is equal to*

$$p_{\text{sim,max}}(\{p(x), \mathcal{N}^x\}_{x\in\mathcal{X}}) = \frac{1}{d}\left[\sup_{\rho_A,\sigma_B} \sum_{x\in\mathcal{X}} \sqrt{p(x)}\, \sqrt{F}(\mathcal{N}^x_{A\to B}(\rho_A), \sigma_B)\right]^2. \tag{3.93}$$

Algorithm 3.12 Algorithm schematic for max output fidelity of multiple channels.

Input: Quantum circuits $\{U^x\}_{x\in\mathcal{X}}$ that realize isometric extensions of the channels $\{\mathcal{N}^x\}_{x\in\mathcal{X}}$, respectively, and probability distribution $\{p(x)\}_{x\in\mathcal{X}}$.

Output: Estimate of $P_{\text{sim,max}}(\{p(x),\mathcal{N}^x\}_{x\in\mathcal{X}})$.

1: The verifier prepares a state

$$|\Phi^p\rangle_{T'T} := \sum_{x\in\mathcal{X}} \sqrt{p(x)}|xx\rangle_{T'T} \tag{3.90}$$

on registers T' and T and prepares system E' in the all-zeros state $|0\rangle_{E'}$.

2: The prover transmits the system A of the state $|\psi\rangle_{RA}$ to the verifier.

3: Using the circuits in the set $\{U^x_{AE'\to BE}\}_{x\in\mathcal{X}}$, the verifier performs the following controlled unitary:

$$\sum_{x\in\mathcal{X}} |x\rangle\langle x|_T \otimes U^x_{AE'\to BE}. \tag{3.91}$$

4: The verifier transmits systems T' and E to the max-prover.

5: The prover prepares a system F in the $|0\rangle_F$ state and acts on systems T', R, and F with a unitary $P_{T'EF\to T''F'}$ to produce the output systems T'' and F', where T'' is a qudit system.

6: The prover sends system T'' to the verifier, who then performs a qudit Bell measurement

$$\{\Phi_{T''T}, I_{T''T} - \Phi_{T''T}\} \tag{3.92}$$

on systems T'' and T, where $\Phi_{T''T}$ is defined in (3.76). The verifier accepts if and only if the outcome $\Phi_{T''T}$ occurs.

This acceptance probability is bounded from above by

$$\frac{1}{d} + \frac{2}{d} \times \sup_{\rho_A} \sum_{x,y\in\mathcal{X}:x<y} \sqrt{p(x)p(y)}\, \sqrt{F}(\mathcal{N}^x_{A\to B}(\rho_A), \mathcal{N}^y_{A\to B}(\rho_A)). \tag{3.94}$$

When $d = 2$, this upper bound is tight.

Proof. For a fixed state ψ_{RA} of the prover, the problem is equivalent to that specified by Algorithm 3.10, for the ensemble $\{p(x), F(\mathcal{N}^x_{A\to B}(\rho_A))\}_{x\in\mathcal{X}}$, where $\rho_A = \text{Tr}_A[\psi_{RA}]$. Thus, all of the statements from Theorem 3.5 apply for this fixed state. We arrive at the statement of the theorem after optimizing over all input states. ∎

3.2 Estimating trace distance and diamond distance

We now review several well known algorithms for estimating trace distance [Wat02c] and diamond distance [RW05] by interacting with quantum provers. Later on, we replace the provers with parameterized circuits to see how well this approach can perform in estimating these distinguishability measures.

3.2.1 Estimating trace distance

The trace distance between quantum states ρ_S^0 and ρ_S^1 is defined as $\left\|\rho_S^0 - \rho_S^1\right\|_1$, where $\|A\|_1 = \mathrm{Tr}[\sqrt{A^\dagger A}]$. It is a well known and operationally motivated measure of distinguishability for quantum states.

We suppose, as is the case in Section 3.1.3, that quantum circuits U_{RS}^0 and U_{RS}^1 are available for generating purifications of the states ρ_S^0 and ρ_S^1. That is, for $i \in \{0, 1\}$,

$$\rho_S^i = \mathrm{Tr}_R[U_{RS}^i |0\rangle\langle 0|_{RS} (U_{RS}^i)^\dagger]. \tag{3.95}$$

However, the purifying systems are not strictly necessary in the operation of the algorithm given below, which is an advantage over some of the algorithms from Section 3.1.3.

The following QSZK algorithm allows for estimating the trace distance [Wat02c], in the sense that its acceptance probability is a simple function of the trace distance:

Algorithm 3.13 Algorithm schematic for trace distance of states.

Input: Quantum states ρ^0 and ρ^1.
Output: Estimate of $\|\rho^0 - \rho^1\|$.

1: The verifier picks a classical bit $i \in \{0, 1\}$ uniformly at random, prepares the state ρ_S^i, and sends system S to the prover.
2: The prover prepares a system F in the $|0\rangle_F$ state and acts on systems S and F with a unitary $P_{SF \to TF'}$ to produce the output systems T and F', where T is a qubit system.
3: The prover sends system T to the verifier, who then performs a measurement on system T, with outcome $j \in \{0, 1\}$. The verifier accepts if and only if $i = j$.

This algorithm has been well known for some time [Hel67, Hel69, Hol72, Wat02c] and its maximum acceptance probability is equal to

$$\max_{\Lambda:0\leq\Lambda\leq I} \frac{1}{2}\operatorname{Tr}[\Lambda\rho_S^0] + \frac{1}{2}\operatorname{Tr}[(I-\Lambda)\rho_S^1] = \frac{1}{2}\left(1 + \frac{1}{2}\left\|\rho_S^0 - \rho_S^1\right\|_1\right). \tag{3.96}$$

This follows because the acceptance probability can be written as follows, for a fixed unitary $P \equiv P_{SF\to TF'}$ of the prover:

$$\begin{aligned}
&\frac{1}{2}\sum_{i\in\{0,1\}} \operatorname{Tr}[(|i\rangle\langle i|_T \otimes I_{F'})P(\rho_S^i \otimes |0\rangle\langle 0|_F)P^\dagger] \\
&= \frac{1}{2}\sum_{i\in\{0,1\}} \operatorname{Tr}[\langle 0|_F P^\dagger(|i\rangle\langle i|_T \otimes I_{F'})P|0\rangle_F \rho_S^i] \qquad (3.97)\\
&= \frac{1}{2}\sum_{i\in\{0,1\}} \operatorname{Tr}[\Lambda_S^i \rho_S^i], \qquad (3.98)
\end{aligned}$$

where we have defined the measurement operator Λ_S^i, for $i \in \{0,1\}$, as

$$\Lambda_S^i := \langle 0|_F (P_{SF\to TF'})^\dagger (|i\rangle\langle i|_T \otimes I_{F'})P_{SF\to TF'}|0\rangle_F, \tag{3.99}$$

and it is clear that $\sum_{i\in\{0,1\}} \Lambda_S^i = I_S$. By the Naimark extension theorem [Nai40] (see also [KW20]), every measurement can be realized in this way, so that

$$\max_P \frac{1}{2}\sum_{i\in\{0,1\}} \operatorname{Tr}[(|i\rangle\langle i|_T \otimes I_{F'})P(\rho_S^i \otimes |0\rangle\langle 0|_F)P^\dagger] = \max_{\Lambda:0\leq\Lambda\leq I} \frac{1}{2}\operatorname{Tr}[\Lambda\rho_S^0] + \frac{1}{2}\operatorname{Tr}[(I-\Lambda)\rho_S^1]. \tag{3.100}$$

Thus, by replacing the actions of the prover with a parameterized circuit and repeating the algorithm, we can use a quantum computer to estimate a lower bound on the trace distance of the states ρ_S^0 and ρ_S^1. An approach similar to this has been adopted in [CSZW22].

We note here that the following identity holds also [Hel67, Hel69, Hol72] (see also [KW20, Theorem 3.13]):

$$\min_{\Lambda:0\leq\Lambda\leq I} \frac{1}{2}\operatorname{Tr}[\Lambda\rho_S^0] + \frac{1}{2}\operatorname{Tr}[(I-\Lambda)\rho_S^1] = \frac{1}{2}\left(1 - \frac{1}{2}\left\|\rho_S^0 - \rho_S^1\right\|_1\right). \tag{3.101}$$

3.2.2 Estimating diamond distance

The diamond distance between quantum channels $\mathcal{N}^0_{A\to B}$ and $\mathcal{N}^1_{A\to B}$ is defined as [Kit97]

$$\left\|\mathcal{N}^0_{A\to B} - \mathcal{N}^1_{A\to B}\right\|_\diamond := \sup_{\rho_{RA}} \left\|\mathcal{N}^0_{A\to B}(\rho_{RA}) - \mathcal{N}^1_{A\to B}(\rho_{RA})\right\|_1, \tag{3.102}$$

where the optimization is over every bipartite state ρ_{RA} and the system R can be arbitrarily large. By a well known data processing argument, the following equality holds

$$\left\|\mathcal{N}^0_{A\to B} - \mathcal{N}^1_{A\to B}\right\|_\diamond := \max_{\psi_{RA}} \left\|\mathcal{N}^0_{A\to B}(\psi_{RA}) - \mathcal{N}^1_{A\to B}(\psi_{RA})\right\|_1, \tag{3.103}$$

where the optimization is over every pure bipartite state ψ_{RA} and the system R is isomorphic to the channel input system A. The diamond distance is a well known and operationally motivated measure of distinguishability for quantum channels [RW05, GLN05].

We suppose, as is the case in Section 3.1.4, that quantum circuits $U^0_{AE'\to BE}$ and $U^1_{AE'\to BE}$ are available for generating isometric extensions of the channels $\mathcal{N}^0_{A\to B}$ and $\mathcal{N}^1_{A\to B}$. That is, for $i \in \{0, 1\}$,

$$\mathcal{N}^i_{A\to B}(\cdot) = \mathrm{Tr}_E[U^i_{AE'\to BE}((\cdot)\otimes|0\rangle\langle 0|_{E'})(U^i_{AE'\to BE})^\dagger]. \tag{3.104}$$

However, the environment systems are not strictly necessary in the operation of the algorithm given below, which is an advantage over some of the algorithms from Section 3.1.4.

The following QIP algorithm allows for estimating the diamond distance [RW05], in the sense that its acceptance probability is a simple function of the diamond distance:

This algorithm has been well known for some time [RW05] and its maximum acceptance probability is equal to

$$\frac{1}{2}\left(1 + \frac{1}{2}\left\|\mathcal{N}^0_{A\to B} - \mathcal{N}^1_{A\to B}\right\|_\diamond\right). \tag{3.105}$$

Thus, by replacing the actions of the prover with a parameterized circuit and repeating the algorithm, we can use a quantum computer to estimate a lower bound on the diamond distance of the channels $\mathcal{N}^0_{A\to B}$ and $\mathcal{N}^1_{A\to B}$.

Algorithm 3.14 Algorithm schematic for diamond distance of channels [RW05].

Input: Quantum circuits U^0 and U^1 that realize isometric extensions of the channels $\mathcal{N}^0$ and $\mathcal{N}^1$, respectively.

Output: Estimate of $\|\mathcal{N}^0 - \mathcal{N}^1\|_\diamond$.

1: The prover prepares a pure state ψ_{RA} and sends system A to the verifier.
2: The verifier picks a classical bit $i \in \{0, 1\}$ uniformly at random, applies the channel $\mathcal{N}^i_{A\to B}$, and sends system B to the prover.
3: The prover prepares a system F in the $|0\rangle_F$ state and acts on systems R, B, and F with a unitary $P_{RBF\to TF'}$ to produce the output systems T and F', where T is a qubit system.
4: The prover sends system T to the verifier, who then performs a measurement on system T, with outcome $j \in \{0, 1\}$. The verifier accepts if and only if $i = j$.

3.2.3 Estimating minimum trace distance of channels

In this section, we show how to estimate the following trace distance function of channels $\mathcal{N}^0_{A\to B}$ and $\mathcal{N}^1_{A\to B}$ by means of a short quantum game (SQG) algorithm:

$$\inf_{\rho_A} \left\| \mathcal{N}^0_{A\to B}(\rho_A) - \mathcal{N}^1_{A\to B}(\rho_A) \right\|_1 , \tag{3.106}$$

where the optimization is over every input state ρ_A. The algorithm features a min-prover and a max-prover. Short quantum games were defined and studied in [GW05, Gut05].

For a fixed state ψ_{RA} of the min-prover, it follows from Algorithm 3.13 that the acceptance probability is equal to

$$\frac{1}{2}\left(1 + \frac{1}{2}\left\| \mathcal{N}^0_{A\to B}(\rho_A) - \mathcal{N}^1_{A\to B}(\rho_A) \right\|_1\right), \tag{3.107}$$

where $\rho_A = \mathrm{Tr}_R[\psi_{RA}]$. Since the min-prover plays first and his goal is to minimize the acceptance probability, it follows that the acceptance probability of Algorithm 3.15 is given by

$$\frac{1}{2}\left(1 + \|\mathcal{N}_0 - \mathcal{N}_1\|_{\diamond,\min}\right), \tag{3.108}$$

where

$$\|\mathcal{N}_0 - \mathcal{N}_1\|_{\diamond,\min} := \frac{1}{2} \inf_{\rho_A} \left\| \mathcal{N}^0_{A\to B}(\rho_A) - \mathcal{N}^1_{A\to B}(\rho_A) \right\|_1 . \tag{3.109}$$

Algorithm 3.15 Algorithm schematic for min trace distance of channels.

Input: Quantum circuits U^0 and U^1 that realize isometric extensions of the channels $\mathcal{N}^0$ and $\mathcal{N}^1$, respectively.
Output: Estimate of $\|\mathcal{N}^0 - \mathcal{N}^1\|_{\diamond,\min}$.

1: The min-prover prepares a state ψ_{RA} and sends system A to the verifier.
2: The verifier picks a classical bit $i \in \{0,1\}$ uniformly at random, applies the channel $\mathcal{N}^i_{A\to B}$, and sends system B to the max-prover.
3: The max-prover prepares a system F in the $|0\rangle_F$ state and acts on systems R, B, and F with a unitary $P_{RBF\to TF'}$ to produce the output systems T and F', where T is a qubit system.
4: The max-prover sends system T to the verifier, who then performs a measurement on system T, with outcome $j \in \{0,1\}$. The verifier accepts if and only if $i = j$.

Another way to estimate the minimum trace distance of channels in (3.106) is to swap the roles of the max-prover and min-prover in Algorithm 3.15:

Algorithm 3.16 Algorithm schematic for min trace distance of channels, with swapped roles.

Input: Quantum circuits U^0 and U^1 that realize isometric extensions of the channels $\mathcal{N}^0$ and $\mathcal{N}^1$, respectively.
Output: Estimate of $\|\mathcal{N}^0 - \mathcal{N}^1\|_{\diamond,\min}$.

1: The max-prover prepares a state ψ_{RA} and sends system A to the verifier.
2: The verifier picks a classical bit $i \in \{0,1\}$ uniformly at random, applies the channel $\mathcal{N}^i_{A\to B}$, and sends system B to the min-prover.
3: The min-prover prepares a system F in the $|0\rangle_F$ state and acts on systems R, B, and F with a unitary $P_{RBF\to TF'}$ to produce the output systems T and F', where T is a qubit system.
4: The min-prover sends system T to the verifier, who then performs a measurement on system T, with outcome $j \in \{0,1\}$. The verifier accepts if and only if $i = j$.

For a fixed state ψ_{RA} of the max-prover, it follows from (3.101) that the acceptance probability is equal to

$$\frac{1}{2}\left(1 - \frac{1}{2}\left\|\mathcal{N}^0_{A\to B}(\rho_A) - \mathcal{N}^1_{A\to B}(\rho_A)\right\|_1\right), \tag{3.110}$$

where $\rho_A = \mathrm{Tr}_R[\psi_{RA}]$. Since the max-prover plays first and his goal is to maximize the acceptance probability, it follows that the acceptance probability of Algorithm 3.15 is given by

$$\frac{1}{2}\left(1 - \frac{1}{2}\inf_{\rho_A}\left\|\mathcal{N}^0_{A\to B}(\rho_A) - \mathcal{N}^1_{A\to B}(\rho_A)\right\|_1\right). \tag{3.111}$$

Although the quantities estimated by Algorithms 3.9 and 3.15 or 3.16 are similar (and related to each other by standard inequalities relating trace distance and fidelity [FvdG99]), the algorithms are very different in that the channel output is available at the end of Algorithm 3.9, whereas it is not at the end of Algorithms 3.15 and 3.16. This has implications for applications in which it is helpful to have access to the channel output, for example, when one is trying to find the fixed point of a quantum channel.

3.2.4 Generalization to multiple states, and channels

Each of the algorithms from the previous subsections has a generalization to multiple states, and channels. We go through them briefly here. The main idea is that, rather than randomly picking from a set of two resources, the verifier picks randomly from a set of multiple resources and then a prover has to guess which one was chosen. The main difference with the binary case is that there is not a closed-form expression for the acceptance probability in terms of a metric like the trace distance or derived metrics, but rather the optimization is phrased as a semidefinite program that can be solved numerically or used in some cases to obtain analytical solutions (for example, if there is sufficient symmetry).

Suppose that we are given an ensemble $\{p(x), \rho^x_S\}_{x\in\mathcal{X}}$ of quantum states. The verifier picks x randomly according to $p(x)$, prepares ρ^x_S, and the prover has to guess which state was prepared. The acceptance probability is given by

$$p_g(\{p(x), \rho^x\}_{x\in\mathcal{X}}) := \sup_{\{\Lambda^x_S\}_{x\in\mathcal{X}}} \sum_{x\in\mathcal{X}} p(x)\,\mathrm{Tr}[\Lambda^x_S \rho^x_S], \tag{3.112}$$

where the optimization is over every POVM $\left\{\Lambda^x_S\right\}_{x\in\mathcal{X}}$. In the case that $|\mathcal{X}| = 2$, this acceptance probability has the explicit form

$$\frac{1}{2}\left(1 + \left\|p\rho^0_S - (1-p)\rho^1_S\right\|_1\right). \tag{3.113}$$

To account for multiple states, we modify Algorithm 3.13 as follows: the verifier's variable $i \in \{0, \ldots, |\mathcal{X}| - 1\}$ is randomly selected and the prover's guess j is chosen from the same set. System T therein is generalized to be a $\lceil \log_2 |\mathcal{X}| \rceil$-qubit system. When $|\mathcal{X}|$ is a power of two, there is a perfect match between the number $|\mathcal{X}|$ of measurement outcomes and the dimension of system T. The verifier accepts if the outcome j equals the state i that was picked. If $|\mathcal{X}|$ is not a power of two, the following algorithm handles this case by coarse graining some of the measurement outcomes together. This is relevant because most quantum computers are qubit-based.

Algorithm 3.17 Algorithm schematic for trace distance of multiple states.

Input: Quantum states $\{\rho^x\}_{x\in\mathcal{X}}$, and probability distribution $\{p(x)\}_{x\in\mathcal{X}}$.
Output: Estimate of $p_g(\{p(x), \rho^x\}_{x\in\mathcal{X}})$.

1: The verifier selects an integer $i \in \{0, \ldots, |\mathcal{X}| - 1\}$ at random according to $p(i)$, prepares the state ρ_S^i, and sends system S to the prover.
2: The prover prepares a system F composed of $\lceil \log_2 |\mathcal{X}| \rceil$ qubits in the $|0\rangle_F$ state. The prover then acts on systems S and F with a unitary $P_{SF\to TF'}$, producing the output systems F' and T, where T is a system of $\lceil \log_2 |\mathcal{X}| \rceil$ qubits.
3: The prover sends system T to the verifier, who then performs a computational basis measurement on system T, with outcome $j \in \{0, \ldots, 2^{\lceil \log_2 |\mathcal{X}| \rceil} - 1\}$.
4: The verifier accepts under two conditions.

- $j \leq |\mathcal{X}| - 1$ and $i = j$.
- $j > |\mathcal{X}| - 1$ and $i = 0$.

This algorithm is a direct generalization of Algorithm 3.13. To understand its connection to (3.112), consider that, for a fixed unitary $P_{SF\to TF'}$, its acceptance

probability is given by

$$\sum_{i\in\{0,\ldots,|\mathcal{X}|-1\}} p(i)\operatorname{Tr}[(|i\rangle\langle i|_T \otimes I_{F'})P(\rho_S^i \otimes |0\rangle\langle 0|_F)P^\dagger]$$
$$+ p(0)\sum_{j=|\mathcal{X}|}^{2^{\lceil \log_2|\mathcal{X}|\rceil}} \operatorname{Tr}[(|j\rangle\langle j|_T \otimes I_{F'})P(\rho_S^i \otimes |0\rangle\langle 0|_F)P^\dagger] \tag{3.114}$$
$$= \sum_{i\in\{0,\ldots,|\mathcal{X}|-1\}} p(i)\operatorname{Tr}[\langle 0|_F P^\dagger(|i\rangle\langle i|_T \otimes I_{F'})P|0\rangle_F \rho_S^i]$$
$$+ p(0)\sum_{j=|\mathcal{X}|}^{2^{\lceil \log_2|\mathcal{X}|\rceil}} \operatorname{Tr}[\langle 0|_F P^\dagger(|j\rangle\langle j|_T \otimes I_{F'})P|0\rangle_F \rho_S^i] \tag{3.115}$$
$$= \sum_{i\in\{0,\ldots,|\mathcal{X}|-1\}} p(i)\operatorname{Tr}[\Lambda_S^i \rho_S^i], \tag{3.116}$$

where we have defined the following measurement operators:

$$\Lambda_S^0 := \langle 0|_F P^\dagger(|0\rangle\langle 0|_T \otimes I_{F'})P|0\rangle_F + \sum_{j=|\mathcal{X}|}^{2^{\lceil \log_2|\mathcal{X}|\rceil}} \langle 0|_F P^\dagger(|j\rangle\langle j|_T \otimes I_{F'})P|0\rangle_F, \tag{3.117}$$

and for all $i \in \{1, \ldots, |\mathcal{X}| - 1\}$:

$$\Lambda_S^i := \langle 0|_F P^\dagger(|i\rangle\langle i|_T \otimes I_{F'})P|0\rangle_F. \tag{3.118}$$

As such, we coarse grain all measurement outcomes in $\{0, |\mathcal{X}|, |\mathcal{X}| + 1, \ldots, 2^{\lceil \log_2|\mathcal{X}|\rceil}\}$ into a single measurement outcome. By the Naimark extension theorem, every measurement with $|\mathcal{X}|$ outcomes can be realized in this way, so that maximizing the expression in (3.114) over every unitary P gives a value equal to that in (3.112).

On the one hand, if $|\mathcal{X}|$ is a power of two, then it follows that $|\mathcal{X}| = 2^{\lceil \log_2|\mathcal{X}|\rceil}$ and the outcome $j > |\mathcal{X}| - 1$ never occurs. On the other hand, if $|\mathcal{X}|$ is not a power of two, then $|\mathcal{X}| < 2^{\lceil \log_2|\mathcal{X}|\rceil}$ and the outcome $j > |\mathcal{X}| - 1$ does occur.

The acceptance condition is split into two conditions due to the unused measurement outcomes when restricted to qubit subsystems and the number of states is not a power of two. In case of qubit systems, by Naimark's extension theorem, measuring the ancilla qubits leads to a number of outcomes that is a power of two. If the number of states is a power of two, we can create a one-to-one mapping between measurement outcomes and states. If the number of states is not a power

of two, there are unassigned measurement outcomes. We resolve this issue by assigning any unassigned outcomes to the first state. In effect, if the verifier measures one of these unassigned outcomes ($j > |\mathcal{X}| - 1$ from the algorithm above), it is equivalent to measuring the first outcome $i = 0$. In other words, we combine the POVM elements for any unassigned outcomes with the POVM element of the first state. Since the prover picks the optimal unitary, this does not affect the overall optimal acceptance probability.

Now suppose that we are given an ensemble $\{p(x), \mathcal{N}^x_{A\to B}\}_{x\in\mathcal{X}}$ of quantum channels. Then a similar modification of Algorithm 3.14 has acceptance probability

$$\sup_{\psi_{RA},\{\Lambda^x_{RB}\}_{x\in\mathcal{X}}} \sum_{x\in\mathcal{X}} p(x) \operatorname{Tr}[\Lambda^x_{RB}\mathcal{N}^x_{A\to B}(\psi_{RA})], \tag{3.119}$$

where the optimization is over every state ψ_{RA} and POVM $\left\{\Lambda^x_{RB}\right\}_{x\in\mathcal{X}}$. In the case that $|\mathcal{X}| = 2$, this acceptance probability has the explicit form

$$\frac{1}{2}\left(1 + \left\| p\mathcal{N}^0_{A\to B} - (1-p)\,\mathcal{N}^1_{A\to B}\right\|_\diamond\right). \tag{3.120}$$

Finally, we can generalize Algorithms 3.15 and 3.16, with the acceptance probabilities respectively given by

$$\inf_{\rho_A} \sup_{\{\Lambda^x_B\}_{x\in\mathcal{X}}} \sum_{x\in\mathcal{X}} p(x) \operatorname{Tr}[\Lambda^x_B\mathcal{N}^x_{A\to B}(\rho_A)], \tag{3.121}$$

$$\sup_{\rho_A} \inf_{\{\Lambda^x_B\}_{x\in\mathcal{X}}} \sum_{x\in\mathcal{X}} p(x) \operatorname{Tr}[\Lambda^x_B\mathcal{N}^x_{A\to B}(\rho_A)]. \tag{3.122}$$

In the case that $|\mathcal{X}| = 2$, these acceptance probabilities become

$$\frac{1}{2}\left(1 + \inf_{\rho_A} \left\| p\mathcal{N}^0_{A\to B}(\rho_A) - (1-p)\,\mathcal{N}^1_{A\to B}(\rho_A)\right\|_1\right), \tag{3.123}$$

$$\frac{1}{2}\left(1 - \inf_{\rho_A} \left\| p\mathcal{N}^0_{A\to B}(\rho_A) - (1-p)\,\mathcal{N}^1_{A\to B}(\rho_A)\right\|_1\right). \tag{3.124}$$

3.3 Performance evaluation of algorithms using a noiseless and noisy quantum simulator

In this section, we present results obtained from numerically simulating Algorithms 3.4–3.7 and Algorithm 3.13 on a noiseless quantum simulator and Algorithms 3.8, 3.14, and 3.17 on both a noiseless and noisy quantum simulator. In

the first subsection, we introduce and discuss the circuit ansatz employed in these numerical experiments. In the next subsection, we discuss the form of the states and channels used for the numerical simulations. In the following subsections, we present the details of our numerical simulations of Algorithms 3.4–3.7 for fidelity of states, Algorithm 3.8 for the fidelity of channels, Algorithm 3.13 for trace distance of states, Algorithm 3.14 for diamond distance of channels, and Algorithm 3.17 for multiple state discrimination.

In the simulations below, we use a maximum number of iterations to be the stopping condition. We noted that some algorithms - in particular, ones with multiple provers - were more prone to get stuck in local minima and optimization loops. We found that, in these scenarios, using convergence as the stopping condition could lead to an unbounded number of iterations. In these cases, we found that using a maximum number of iterations was sufficient and effective.

All the program code for Algorithms 3.4, 3.5, 3.6, 3.7, 3.8, 3.13, 3.14, 3.17, and corresponding SDPs can be found in the Supplementary Material of [RASW23].

3.3.1 Ansatz

To estimate the relevant quantities in this work, we employ the hardware-efficient ansatz (HEA) [KMT+17]. The HEA is a problem-agnostic ansatz that depends on the architecture and the connectivity of the given hardware. In this work, we consider a fixed structure of the HEA. Let X, Y, and Z denote the Pauli matrices. We define one layer of the HEA to consist of the single-qubit rotations $e^{-\mathrm{i}\theta/2Y}e^{-\mathrm{i}\delta/2X}$, each of which acts on a single qubit and is parameterized by θ and δ, followed by CNOTs between neighboring qubits. A CNOT between the control qubit k and the target qubit ℓ is given by

$$e^{-\mathrm{i}\pi/2(|1\rangle\langle 1|_k\otimes(X_\ell - I_\ell))} = |0\rangle\langle 0|_k \otimes I_\ell + |1\rangle\langle 1|_k \otimes X_\ell. \tag{3.125}$$

For our numerical experiments, we consider a sufficiently large number of layers of the HEA. In principle, both the circuit structure and the number of layers of the HEA can be made random and this randomness can lead to better performance of variational algorithms [BCV+21]. We leave the study of such ansatze for future work.

The HEA is used both to create the states and channels, as well as to create a parameterized unitary that replaces the provers. In the former two cases, the

rotation angles are fixed, but in the prover scenario, the angles are parameters that are optimized.

3.3.2 Test states and channels

To study the performance of our algorithms, we randomly select states and channels as follows. For n-qubit states, we apply m layers of the HEA with randomly selected angles for rotation around the x- and y-axes on $n + k$ qubits initialized to the state $|0\rangle\langle 0|$. This procedure prepares a pure state on $n + k$ qubits and hence, a mixed state on n qubits of rank $\leq 2^k$.

To realize an n-qubit channel $\mathcal{N}_{A\to B}$, we generate a unitary $U_{AE'\to BE}$ on $n + k$ qubits such that

$$\mathcal{N}_{A\to B}(\omega_A) \coloneqq \mathrm{Tr}_E\Big[U_{AE'\to BE}(\omega_A \otimes |0\rangle\langle 0|_{E'})(U_{AE'\to BE})^\dagger\Big], \tag{3.126}$$

where systems E' and E each consist of k qubits. Due the Stinespring dilation theorem [Sti55], this is a general approach by which arbitrary channels can be realized.

For our experiments, we set U to consist of m layers of the HEA itself, with randomly selected angles for rotation around the x- and y-axes on $n + 1$ qubits. Tracing out one of the qubits gives a channel on n qubits, as required.

Several algorithms in our paper (see (3.6), (3.20), (3.60)) depend on having access to unitaries of the form

$$\sum_{i\in\{0,1\}} |i\rangle\langle i|_T \otimes U_S^i = |0\rangle\langle 0| \otimes U_S^0 + |1\rangle\langle 1| \otimes U_S^1. \tag{3.127}$$

These can be split into the sequential application of the following two controlled unitaries:

$$\begin{aligned} &|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U_S^1, \\ &|1\rangle\langle 1| \otimes I + |0\rangle\langle 0| \otimes U_S^0, \end{aligned} \tag{3.128}$$

of which our algorithms make use.

3.3.3 Fidelity of states

In this section, we discuss the performance of Algorithms 3.4–3.7 in the noiseless scenario to estimate the fidelity between two three-qubit mixed states. Algorithms 3.4–3.7 require different numbers of qubits for estimating the fidelity between ρ and σ. In particular, for this case, Algorithm 3.4 requires eight qubits, along with access to controlled unitaries, as defined in (3.128). Algorithms 3.5, 3.6, and 3.7 require 13, 10, and 8 qubits, respectively. We recall that Algorithms 3.4–3.6 require purifications of both ρ and σ, while Algorithm 3.7 relies only on access to ρ and σ directly. Moreover, Algorithms 3.4 and 3.5 require measurements on two qubits, and Algorithm 3.6 requires Bell measurements on ten qubits. Finally, Algorithm 3.7 requires two single-qubit measurements.

We now summarize the HEA employed. For Algorithm 3.4, the prover unitary is created using five layers of the HEA, which acts on four qubits. Similarly, in Algorithm 3.5, we employ eight layers of the HEA that acts on six qubits. In Algorithm 3.6, the ansatz acts on two qubits, and we consider four layers of it. In Algorithm 3.7, the ansatz acts on four qubits, and we apply eight layers of it. For our implementations, we picked these circuit depths so that the cost function is minimized. A more general framework allows for the ansatz structure to be unfixed and instead variable, but we leave the detailed study of this, for our algorithms, to future work [BCV+21].

We begin the training with a random set of variational parameters. We evaluate the cost using a state vector simulator (noiseless simulator) [AAMA+21]. We then employ the gradient-descent algorithm to obtain a new set of parameters. We note that in general, the true fidelity between states ρ and σ is not known. Thus the stopping criterion for these algorithms is a maximum number of iterations. For our numerical experiments, we set the total number of iterations to be 300. For each algorithm, we run ten instances of the algorithm and pick the best run for generating Figure 3.10.

In Figure 3.10, we plot the results of the numerical simulations. The dashed-dotted line represents the true fidelity between two random three-qubit quantum states ρ and σ, as described above. Each algorithm converges to the true fidelity with high accuracy within a finite number of iterations. As discussed above, for each algorithm, the HEA is of a different size. Thus, it is not straightforward to compare these different algorithms. In terms of the convergence rate, we find that Algorithm 3.6 converges to the true fidelity faster than all other algorithms.

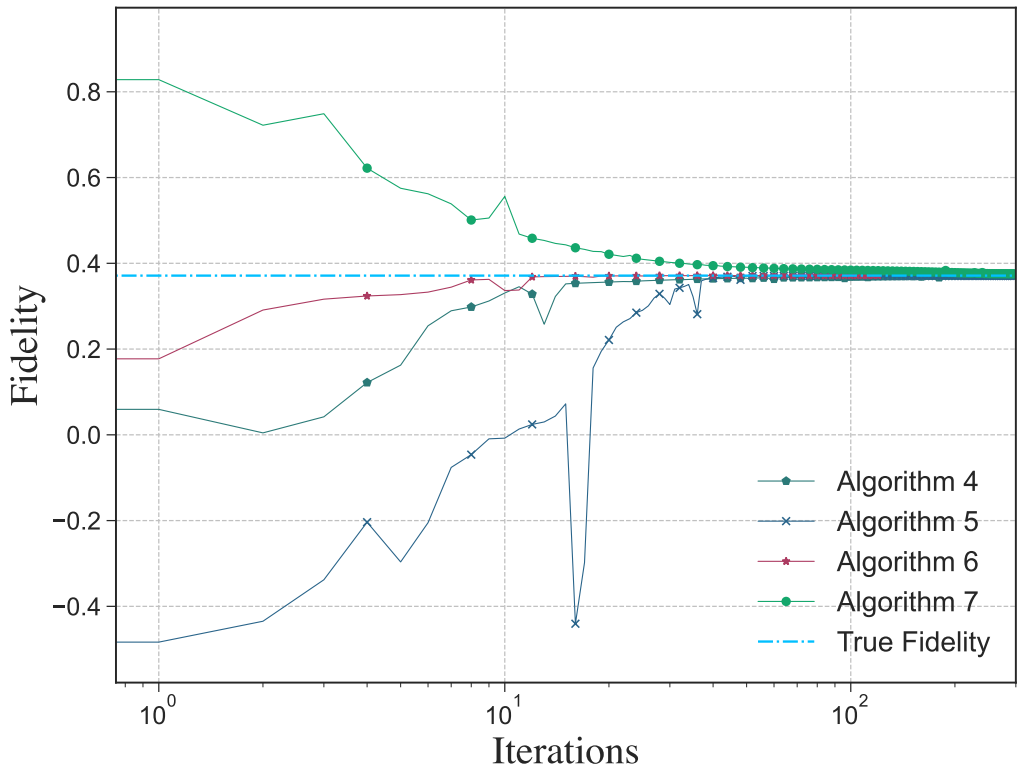


Figure 3.10: Estimation of the fidelity between quantum states versus the number of iterations. We implement Algorithms 3.4–3.7 on a noiseless simulator to estimate the fidelity between two three-qubit mixed states, each of rank ≤ 4. For each variational algorithm, we employ the HEA, as defined in Section 3.3.1. In particular, we start with a random parameter vector $\vec{\theta}$ and then update it according to a gradient-based optimization procedure. The dashed-dotted curve represents the true fidelity between two randomly chosen quantum states. In each case, the optimization procedure converges to the true fidelity with high accuracy. Algorithms 3.4–3.7 achieve an absolute error in fidelity estimation of order 10^{-5}, 10^{-4}, 10^{-9}, and 10^{-3}, respectively.

Algorithms 3.4–3.7 achieve an absolute error in fidelity estimation of order 10^{-5}, 10^{-4}, 10^{-9}, and 10^{-3}, respectively.

3.3.4 Trace distance of states

Using Algorithm 3.13, we estimate the normalized trace distance $\frac{1}{2}\|\rho - \sigma\|_1$ between two three-qubit states ρ and σ, each having rank ≤ 4, as defined above in Section 3.3.2. For our numerical experiments, we use a noiseless simulator. Algorithm 3.13 requires eight qubits in total and two single-qubit measurements. We employ ten layers of the HEA, which acts on four qubits. Similar to the fidelity-estimation algorithms detailed above, we begin with a random set of variational parameters and update them using the gradient-descent algorithm.

As the true normalized trace distance between ρ and σ is assumed to be unknown, we use a stopping criterion as the number of iterations, which we take to be 300 iterations. For Algorithm 3.13, we run ten instances of it and pick the best run for generating Figure 3.11.

In Figure 3.11, we plot the results of Algorithm 3.13. The dashed-dotted line represents the true normalized trace distance between two random three-qubit quantum states ρ and σ, as described above. The absolute error in trace-distance estimation is of order 10^{-4}.

3.3.5 Fidelity of channels

In this section, we discuss the performance of Algorithm 3.8 in both the noiseless and noisy scenarios. The channels in question are realized by using parameterized unitaries and tracing out ancilla qubits, as discussed in Section 3.3.2. The algorithm employs a min-max optimization and thus requires two parameterized unitaries representing the min- and max-provers, respectively. The controlled unitaries consist of one layer of the HEA, with each consisting of random rotations about the x-axis, on two qubits, thereby realizing the $\mathcal{N}^i_{A\to B}$ channels acting on one qubit, for $i \in \{0, 1\}$.

We now summarize the HEA employed in generating the min- and max-provers. The min-prover unitary is generated using two layers of the HEA, which acts on two qubits. The max-prover unitary is generated using two layers of the HEA, which acts on three qubits. The rotation angles for both provers around the x- and y-axes are chosen at random. The particular choices of the number of layers are made so that the cost function is minimized.

We begin the training phase with a random set of variational parameters for

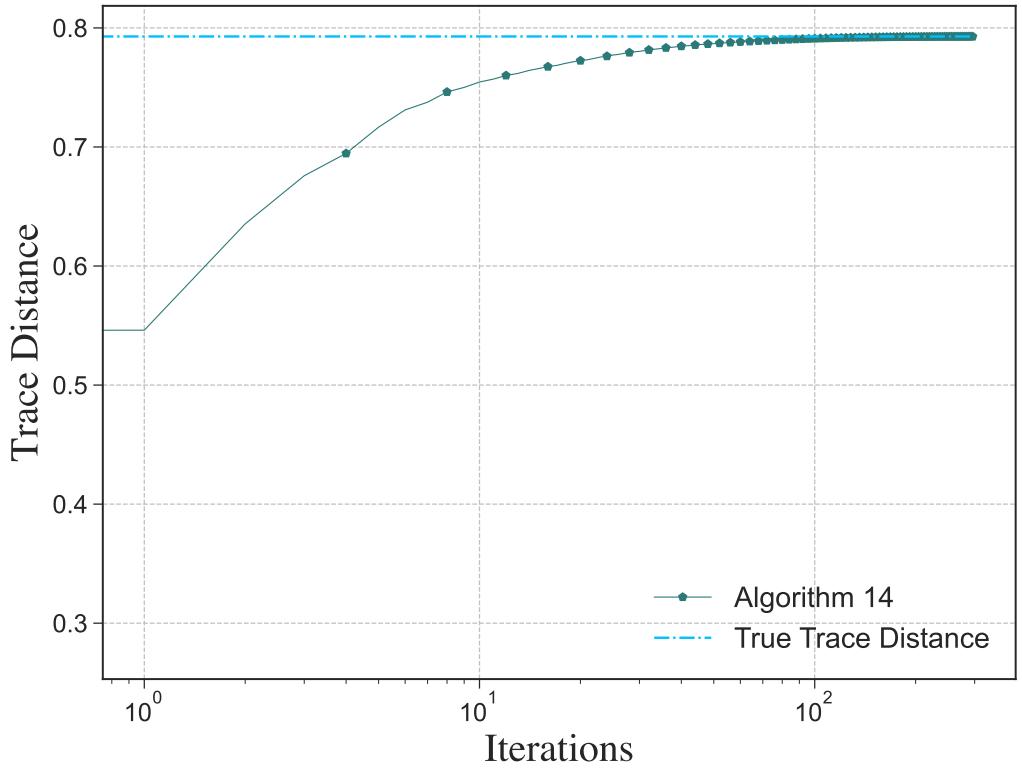


Figure 3.11: Estimation of the normalized trace distance between quantum states versus the number of iterations. We implement Algorithm 3.13 on a noiseless simulator to estimate the normalized trace distance between three-qubit mixed states, each of rank four. Algorithm 3.13 achieves an absolute error in trace distance estimation of order 10^{-4}.

both parameterized unitaries. For the noiseless simulation, we evaluate the cost using a state vector simulator (noiseless simulator) [AAMA+21]. For the noisy simulation, we use the QASM-simulator with the noise model from IBM-Jakarta. Since the number of parameters is significantly higher than the previous algorithms, to speed up the convergence, we employ both the simultaneous perturbation stochastic approximation (SPSA) method [Spa98] and the gradient-descent method to obtain a new set of parameters.

The optimization is carried out in a zig-zag fashion, explained as follows. The minimizing optimizer implements the SPSA algorithm and is allowed to run until convergence occurs. Then, the maximizing optimizer, implementing the gradi-

ent descent algorithm, runs for one iteration. We note that in general, the true fidelity between the channels $\mathcal{N}^0$ and $\mathcal{N}^1$ is not known. Thus, the stopping criterion for these algorithms is a maximum number of iterations. For our numerical experiments, we set the total number of iterations to be 6000, mostly used in the minimizing optimizer. The results of the numerical simulations are presented in Figure 3.12.

Note that the graph presented in Figure 3.12 shows that the convergence is highly non-monotonic, unlike the convergence behavior presented in previous graphs. Each iteration consists of a decrease in the function value, followed by a single increasing iteration. This is clearly indicative of the min-max optimization nature of the algorithm. Furthermore, unlike other algorithms, the optimization value in this algorithm can overshoot the true solution, due to the min-max nature of the optimization. However, the noiseless plot indicates that, once it overshoots the solution, it oscillates with decreasing amplitude and converges.

The noisy optimization converges as well, but it does not converge to the known value of the root fidelity of the two channels. However, the parameters found after convergence exhibit a noise resilience, as put forward in [SKCC20]; i.e., using the parameters obtained from the noisy optimization in a noiseless simulator gives a value much closer to the true value, as indicated by the solid orange line in Figure 3.12.

3.3.6 Diamond distance of channels

In this section, we discuss the performance of Algorithm 3.14 in the noiseless and noisy scenarios. Algorithm 3.14 requires eight qubits. Similar to the previous section, the channels in question are realized using the procedure from Section 3.3.2. The algorithm utilizes a max-max optimization and thus requires two parameterized unitaries representing the two max-provers. Each unitary $U^i_{AE'\to BE'}$, for $i \in \{0, 1\}$, consists of one layer of the HEA with random rotations about the x- and y-axes, on two qubits, each thereby realizing the one-qubit channel $\mathcal{N}^i_{A\to B}$.

We now summarize the HEA employed in generating the two provers. The first prover, called the state-prover because its goal is to realize an optimal distinguishing state, is generated using two layers of the HEA, which acts on two qubits. The second prover, called the max-prover, is generated using two layers of the HEA, which acts on three qubits. The rotation angles for both provers around

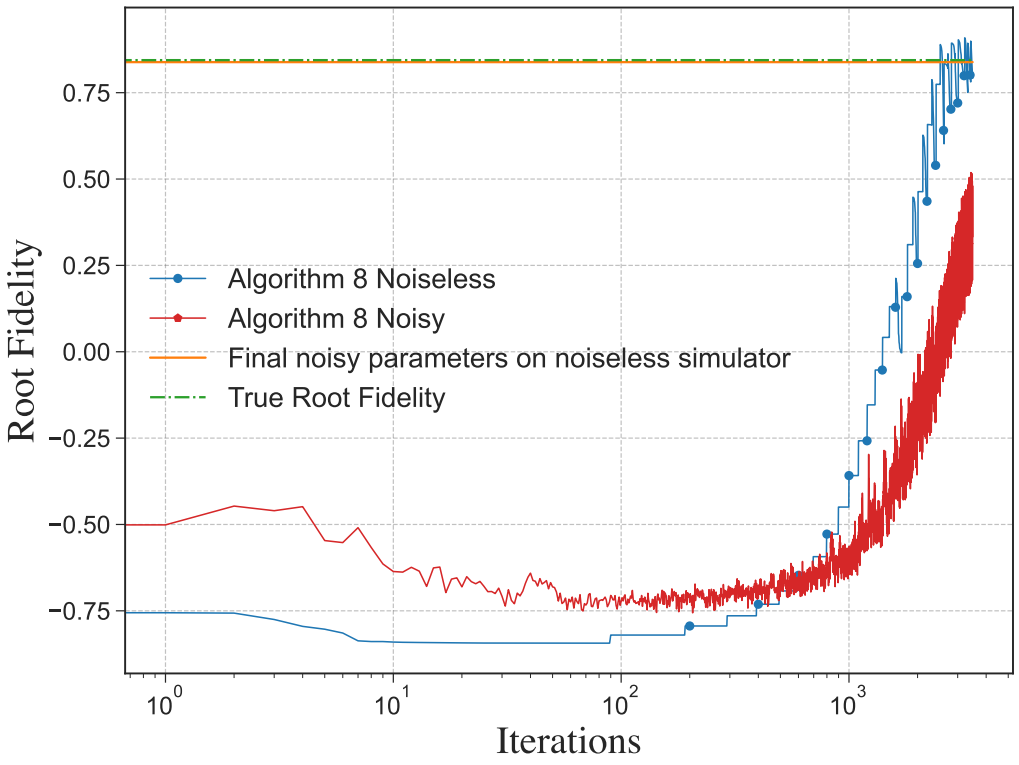


Figure 3.12: Estimation of the normalized fidelity between quantum channels versus the number of iterations. We implement Algorithm 3.8 to estimate the normalized fidelity between two-qubit channels. The noiseless simulation achieves an absolute error in fidelity estimation of order 10^{-4}. The parameters obtained from the noisy simulation, with the noise model from IBM-Jakarta, achieve an absolute error of 10^{-2} on a noiseless simulator.

the x- and y-axes are chosen at random. The particular choices of the number of layers are made so that the cost function is minimized.

We begin the training phase with a random set of variational parameters for both parameterized unitaries. In the noiseless simulation, we evaluate the cost using a state vector simulator (noiseless simulator). In the noisy setup, we use the QASM-simulator with the noise model from IBM-Jakarta. Similar to the previous section, we employ the SPSA optimization technique.

The optimization is carried out in two parts—the first part uses the COBYLA optimizer [Pow94, VGO+20] (non-gradient based), and the second part uses the

SPSA optimizer. In both stages, the optimization is carried out in a zig-zag fashion, explained as follows. The first stage allows for moving quickly into the neighbourhood of the actual solution, but then slows down dramatically. Once we approach the solution, we switch to a gradient-based method that converges to the solution more quickly. In both stages, we allow the state-prover and the max-prover to be optimized for a fixed number of iterations in a zig-zag manner. This is because, in general, the true diamond distance between channels $\mathcal{N}^0$ and $\mathcal{N}^1$ is not known. Thus the stopping criterion for these algorithms is a maximum number of iterations. For our numerical experiments, we set the total number of iterations to be 1600. The results of the numerical simulations are presented in Figure 3.13.

Note that the noiseless graph presented in Figure 3.13 shows that the convergence is highly monotonic, unlike the fidelity of channels (see Figure 3.12), because the optimization is a max-max one, as opposed to the min-max nature of Algorithm 3.8. The quick convergence, indicated by the lower number of iterations, is a consequence of this difference.

The noisy simulation converges as well, and similar to the previous section, the parameters exhibit a noise resilience. Once the COBYLA stage of the optimization is completed, the SPSA optimization is more noisy, due to the perturbative nature of the algorithm. Note that the COBYLA optimizer operates in batches of 30, giving an impression of smoothness.

3.3.7 Multiple state discrimination

In this section, we discuss the performance of Algorithm 3.17 in the noisy and noiseless scenarios. We consider a specific scenario of distinguishing three one-qubit mixed states. Recall from Section 3.3.2 that the one-qubit states are generated by using two layers of the HEA on two qubits. We execute this on a qubit system, and hence we use Algorithm 3.17. The algorithm requires twelve qubits in total and three two-qubit measurements. The measurement is realized using a parameterized unitary and ancilla qubits. By Naimark's extension theorem [Nai40], an arbitrary POVM can be realized using this procedure, so that there is no loss in expressiveness. The parameterized unitary required employs two layers of the HEA, which acts on three qubits.

To speed up convergence, we use the SPSA algorithm for the optimization. As

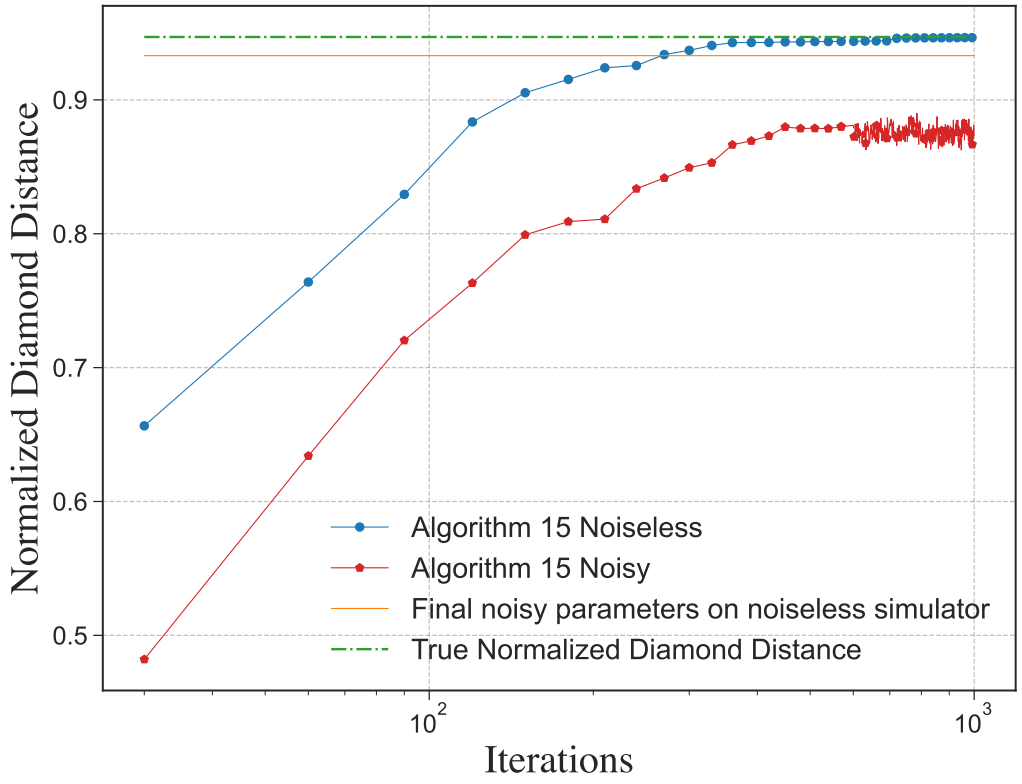


Figure 3.13: Estimation of the normalized diamond distance between quantum channels versus the number of iterations. We implement Algorithm 3.14 to estimate the normalized diamond distance between one-qubit channels. Algorithm 3.14 achieves an absolute error in diamond distance estimation of order 10^{-4}. The parameters obtained from the noisy simulation, with the noise model from IBM-Jakarta, achieve an absolute error of 10^{-2} on a noiseless simulator.

the true value of the optimal acceptance probability between the three states is assumed to be unknown, we set the stopping criterion to be a maximum number of iterations, which we take to be 250 iterations.

In Figure 3.14, we plot the results of simulating Algorithm 3.17. The dashed-dotted line represents the optimal acceptance probability of the three states, calculated using the semi-definite program corresponding to (3.112). The noiseless simulation converges to the known optimal acceptance probability. The noisy optimization converges as well, but it does not converge to the known optimal acceptance probability. However, similar to the previous sections, the parameters

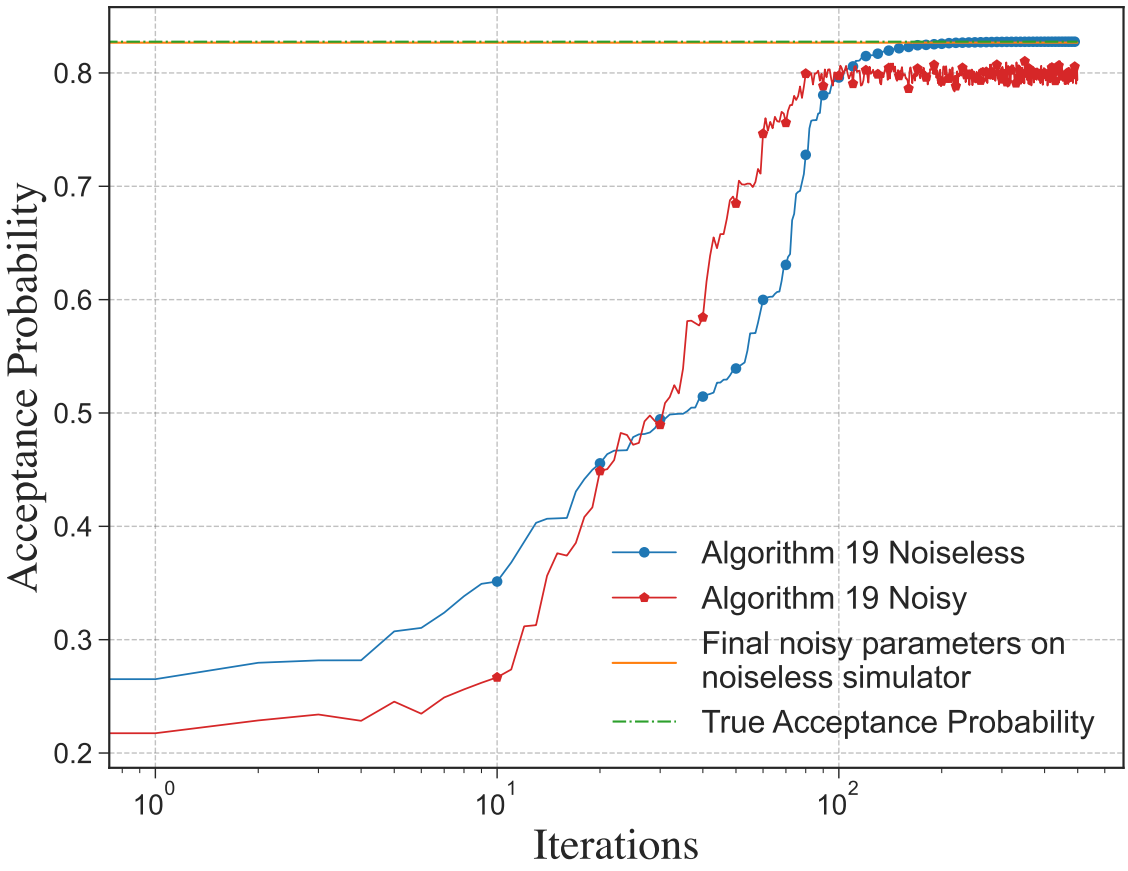


Figure 3.14: Estimation of the optimal acceptance probability for Algorithm 3.17. The noiseless simulation achieves an absolute error of order 10^{-4}. The parameters obtained from the noisy simulation, with the noise model from IBM-Jakarta, achieve an absolute error of 10^{-3} on a noiseless simulator.

exhibit noise resilience, as indicated by the solid orange line in Figure 3.14.

3.4 Estimating distance measures as complexity classes

We now turn our attention to the intersection of our algorithms with quantum computational complexity theory. In this section, we prove that several basic quantum complexity classes can be reframed as distance and fidelity estimation

problems. That is, we show that various distance and fidelity estimation problems are complete for various quantum complexity classes. Refs. [Wat09a, VW16] provide reviews of basic concepts in quantum computational complexity theory for interested readers.

In particular, here we summarize existing results linking estimation problems to complexity classes, and furthermore, we prove that five new distance estimation algorithms that are complete for some complexity classes of interest. First, we prove that promise versions of the following estimation problems are BQP-complete:

1. estimating the fidelity between two pure states,
2. estimating the fidelity between a pure state and a mixed state,
3. estimating the Hilbert–Schmidt distance of two arbitrary states.

Fourth, we prove that the promise problem version of estimating the fidelity between a pure state and a channel with arbitrary input is QMA-complete. Finally, we show that the promise problem version of estimating the fidelity between a pure state and a channel with a separable input state is QMA(2)-complete. In Figure 3.15, we summarize the various quantum complexity classes and the representative fidelity and distance estimation algorithms.

3.4.1 BQP-complete problems

First, we prove that promise versions of the problems of evaluating the fidelity between two pure states, evaluating the fidelity between a mixed state and a pure state, and evaluating the Hilbert–Schmidt distance of two arbitrary states are BQP-complete. The definition of BQP can be found in Section 2.4.1.

Fidelity between two pure states

We now prove that the promise version of the problem of estimating the fidelity between two pure states is BQP-complete. In this problem and all that follows, the parameter x is the description of the circuits involved, and the length $|x|$ is the number of bits needed to describe these circuits.

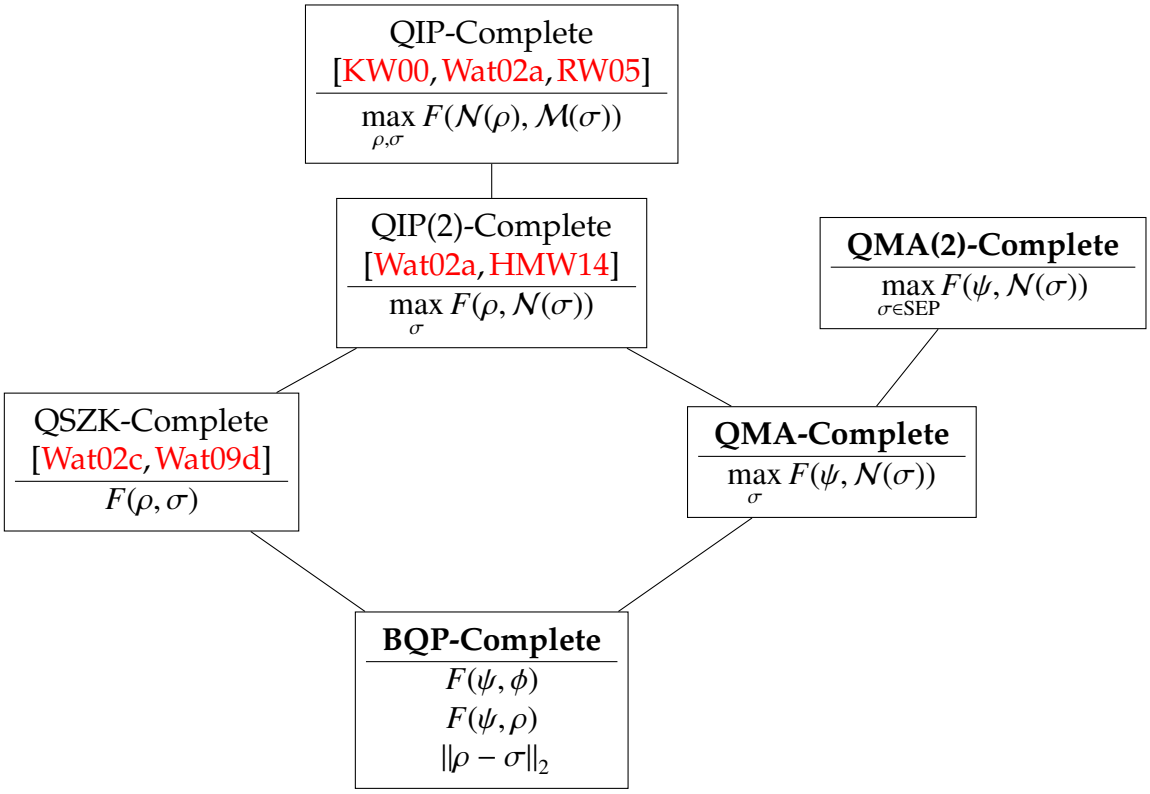


Figure 3.15: List of distance estimation problems and the corresponding quantum complexity class. Entries in bold are the results of our paper. In this diagram, ψ and ϕ are pure states, ρ and σ are mixed states, and $\mathcal{N}$ and $\mathcal{M}$ are channels. Note that ρ and σ may be of different dimensions, depending on the context. The cells are organized such that if a cell is connected to a cell above it, the complexity class for the lower cell is a subset of that for the the higher cell. For example, QMA is a subset of both QIP(2) and QMA(2).

Problem 3.1 [(α, β)-*Fidelity-Pure-Pure*]. *Let α and β be such that $0 \leq \alpha < \beta \leq 1$. Given are descriptions of circuits U_S^{ψ} and U_S^{ϕ} that prepare the pure states ψ_S and ϕ_S, respectively. Decide which of the following holds.*

$$\textit{Yes:} \quad F(\psi_S, \phi_S) \geq 1 - \alpha, \tag{3.129}$$

$$\textit{No:} \quad F(\psi_S, \phi_S) \leq 1 - \beta. \tag{3.130}$$

Theorem 3.8. *The promise problem Fidelity-Pure-Pure is BQP-complete.*

1. (α, β)-*Fidelity-Pure-Pure is in BQP for all* $\alpha < \beta$. *(It is implicit that the gap between* α *and* β *is larger than an inverse polynomial in the input length.)*
2. $(\varepsilon, 1-\varepsilon)$-*Fidelity-Pure-Pure is BQP-hard, even when* ε *decays exponentially in the input length.*

Thus, (α, β)*-Fidelity-Pure-Pure is BQP-complete for all* (α, β) *such that* $0 < \alpha < \beta < 1$.

Proof. The containment of (α, β)-Fidelity-Pure-Pure in BQP is a direct consequence of Algorithm 3.1.

So we focus on proving the hardness result. Consider an arbitrary problem L in BQP. Thus, there exists a family Q of circuits such that (2.126) and (2.127) hold. Given an instance x, the acceptance probability of the BQP algorithm is

$$\begin{aligned} p_{\text{acc}} &= \|(\langle 1|_D \otimes I_G) Q |x\rangle_S |0\rangle_A\|_2^2 \\ &= \langle x|_S \langle 0|_A Q^\dagger (|1\rangle\langle 1|_D \otimes I_G) Q |x\rangle_S |0\rangle_A . \end{aligned} \tag{3.131}$$

To prove the hardness result (i.e., to see that this is an instance of Fidelity-Pure-Pure), we use the BQP-subroutine theorem [BBBV97]. Intuitively, we act with the circuit $Q_{SA\to DG}$ on the input $|x\rangle_S |0\rangle_A$, apply a CNOT gate from the decision qubit to an ancillary qubit initialized to $|0\rangle_C$, apply the inverse unitary $Q^\dagger$, measure the output qubits, and accept if we get the state $|x\rangle_S |0\rangle_A |1\rangle_C$. The acceptance probability of this procedure is equal to

$$\tilde{p}_{\text{acc}} = \left| (\langle x|_S \langle 0|_A \langle 1|_C) Q^\dagger \, \text{CNOT}_{DC} \, Q (|x\rangle_S |0\rangle_A |0\rangle_C) \right|^2 . \tag{3.132}$$

Expanding CNOT_{DC} as

$$\text{CNOT}_{DC} := |0\rangle\langle 0|_D \otimes I_C + |1\rangle\langle 1|_D \otimes X_C, \tag{3.133}$$

where X_C denotes the Pauli-X operator, it follows that

$$\tilde{p}_{\text{acc}} = \left| \langle x|_S \langle 0|_A Q^\dagger (|1\rangle\langle 1|_D \otimes I_G) Q |x\rangle_S |0\rangle_A \right|^2 . \tag{3.134}$$

Comparing this expression to (3.131), we see that the modified circuit has an acceptance probability equal to the square of the acceptance probability of the original BQP problem. Thus, by repeating the modified algorithm sufficiently many times, we can estimate the acceptance probability $\tilde{p}_{\text{acc}}$, and by taking a square root, we can output an estimate of the acceptance probability p_{acc} of the original problem. In Appendix B.7, we derive the number of samples required to estimate p_{acc} with accuracy ε and error probability δ.

The last step to be shown is that the modified acceptance probability $\tilde{p}_{\text{acc}}$ can be rewritten as the fidelity between two pure states. From (3.132), we see that

$$\begin{aligned}\tilde{p}_{\text{acc}} &= \left|(\langle x|_S \langle 0|_A \langle 1|_C) Q^\dagger \,\text{CNOT}_{DC}\, Q(|x\rangle_S |0\rangle_A |0\rangle_C)\right|^2 \\ &= F(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|),\end{aligned} \tag{3.135}$$

where

$$|\psi\rangle := |x\rangle_S |0\rangle_A |1\rangle_C\,, \tag{3.136}$$

$$|\phi\rangle := Q^\dagger \,\text{CNOT}_{DC}\, Q\, |x\rangle_S |0\rangle_A |0\rangle_C\,. \tag{3.137}$$

Thus, an arbitrary instance of a BQP problem can be rewritten as an instance of the fidelity between two pure states, proving that Fidelity-Pure-Pure is indeed a BQP-hard problem. ■

Fidelity between a pure state and a mixed state

Problem 3.2 [(α,β)-*Fidelity-Pure-Mixed*]. *Let α and β be such that $0 \leq \alpha < \beta \leq 1$. Given are descriptions of circuits U^{ρ}_{RS} and U^{ψ}_{S} that prepare a purification of a mixed state ρ_S and a pure state ψ_S, respectively. Decide which of the following holds.*

$$\textit{Yes:} \qquad F(\rho_S, \psi_S) \geq 1 - \alpha, \tag{3.138}$$

$$\textit{No:} \qquad F(\rho_S, \psi_S) \leq 1 - \beta. \tag{3.139}$$

Theorem 3.9. *The promise problem Fidelity-Pure-Mixed is BQP-complete.*

1. *(α,β)-Fidelity-Pure-Mixed is in BQP for all $\alpha < \beta$. (It is implicit that the gap between α and β is larger than an inverse polynomial in the input length.)*
2. *$(\varepsilon, 1-\varepsilon)$-Fidelity-Pure-Mixed is BQP-hard, even when ε decays exponentially in the input length.*

Thus, (α,β)-Fidelity-Pure-Mixed is BQP-complete for all (α,β) such that $0 < \alpha < \beta < 1$.

Proof. The containment of (α,β)-Fidelity-Pure-Mixed in BQP is a direct consequence of Algorithm 3.3.

So we focus on proving the hardness result. Let L be an arbitrary promise problem in BQP, and let $\left\{\phi^x_{DG}\right\}_x$ be a family of efficiently preparable pure states witnessing membership of L in BQP. System D is a decision qubit indicating acceptance

or rejection of x, and system G is a garbage system that purifies D. Suppose that the family $\left\{\phi^x_{DG}\right\}_x$ has completeness $1-\delta$ and soundness δ. If x is a yes-instance of L, then, by the definition of BQP, it follows that $\|\langle 1|_D|\phi^x\rangle_{DG}\|_2^2 \geq 1-\delta$. On the other hand, if x is a no-instance of L, then $\|\langle 1|_D|\phi^x\rangle_{DG}\|_2^2 \leq \delta$. Since

$$\begin{aligned} \|\langle 1|_D|\phi^x\rangle_{DG}\|_2^2 &= \langle 1|_D \operatorname{Tr}_G[\phi^x_{DG}]|1\rangle_D & (3.140)\\ &= F(|1\rangle\langle 1|_D, \operatorname{Tr}_G[\phi^x_{DG}]), & (3.141)\end{aligned}$$

it follows directly that this is an instance of $(1-\delta,\delta)$-Fidelity-Pure-Mixed, given that the reduced state $\operatorname{Tr}_G[\phi^x_{DG}]$ can be prepared efficiently, as well as the state $|1\rangle\langle 1|_D$. The desired hardness result then follows because $\mathrm{BQP}(c,s) \subseteq \mathrm{BQP}(\delta, 1-\delta)$, for every δ exponentially small in the input length. ■

Hilbert–Schmidt distance

The next result we prove is that the promise version of the problem of estimating the normalized Hilbert–Schmidt distance of two arbitrary states is BQP-complete. Recall that the normalized Hilbert–Schmidt distance of two states ρ and σ is given by

$$\begin{aligned} \frac{1}{\sqrt{2}}\|\rho-\sigma\|_2 &:= \frac{1}{\sqrt{2}}\sqrt{\operatorname{Tr}[(\rho-\sigma)^2]} \\ &= \frac{1}{\sqrt{2}}\sqrt{\operatorname{Tr}[\rho^2]+\operatorname{Tr}[\sigma^2]-2\operatorname{Tr}[\rho\sigma]}. & (3.142)\end{aligned}$$

If $\rho=\sigma$, then the Hilbert–Schmidt distance is equal to zero. The prefactor of $2^{-1/2}$ is the correct normalization by the following argument. Since $\operatorname{Tr}[\rho\sigma] \geq 0$, the maximum value of the normalized distance satisfies

$$\begin{aligned} &\frac{1}{\sqrt{2}}\sqrt{\operatorname{Tr}[\rho^2]+\operatorname{Tr}[\sigma^2]-2\operatorname{Tr}[\rho\sigma]} \\ &\quad\leq \frac{1}{\sqrt{2}}\sqrt{\operatorname{Tr}[\rho^2]+\operatorname{Tr}[\sigma^2]} \\ &\quad\leq 1, & (3.143)\end{aligned}$$

where the second inequality follows because the purity of an arbitrary state ρ satisfies $\operatorname{Tr}[\rho^2] \leq 1$. The upper bound is achieved by pure orthogonal states.

Problem 3.3 [(α,β)-*Hilbert–Schmidt-Distance*]. *Let α and β be such that $0 \leq \alpha < \beta \leq 1$. Given are descriptions of circuits U^{ρ}_{RS} and U^{σ}_{RS} that prepare a purification of a mixed states ρ_S and σ_S, respectively. Decide which of the following holds.*

$$\textit{Yes:} \qquad \frac{1}{\sqrt{2}} \|\rho_S - \sigma_S\|_2 \geq 1 - \alpha, \tag{3.144}$$

$$\textit{No:} \qquad \frac{1}{\sqrt{2}} \|\rho_S - \sigma_S\|_2 \leq 1 - \beta. \tag{3.145}$$

Theorem 3.10. *The promise problem Hilbert–Schmidt-Distance is BQP-complete.*

1. *(α,β)-Hilbert–Schmidt-Distance is in BQP for all $\alpha < \beta$. (It is implicit that the gap between α and β is larger than an inverse polynomial in the input length.)*
2. *$(\varepsilon, 1-\varepsilon)$-Hilbert–Schmidt-Distance is BQP-hard, even when ε decays exponentially in the input length.*

Thus, (α,β)-Hilbert–Schmidt-Distance is BQP-complete for all (α,β) such that $0 < \alpha < \beta < 1$.

Proof. To show that the problem is BQP-complete, we need to demonstrate two facts: first, that the problem is in BQP, and second, that it is BQP-hard. Let us begin by proving that the problem is in BQP. This part of the proof is well known and understood by now, and it has been used in many quantum algorithms. We discuss it here for completeness. The intuitive idea is to estimate each term in (3.143) separately using a swap test. A term of the form $\mathrm{Tr}[\rho\sigma]$, where ρ and σ are n-qubit states, can be estimated by repeatedly performing a swap test sufficiently many times to get a good estimate. Since there are only three terms to estimate, it follows that the problem is in BQP.

Next, we show that any problem in the BQP class can be reduced to this problem. A simpler way to show this is to map a known BQP-complete problem to our problem. We now show that the BQP-complete Fidelity-Pure-Pure problem can be reduced to this problem. A special case of the Hilbert–Schmidt-Distance problem is when both inputs are pure states. In this scenario, the normalized Hilbert–Schmidt distance is given by

$$\begin{aligned} \frac{1}{\sqrt{2}} \| |\psi\rangle\langle\psi| - |\phi\rangle\langle\phi| \|_2 &= \sqrt{1 - |\langle\psi|\phi\rangle|^2} \\ &= \sqrt{1 - F(\psi,\phi)}. \end{aligned} \tag{3.146}$$

Then the YES instance condition in (3.144) and (3.146) imply that $F(\psi, \phi) \leq \alpha(2-\alpha)$, in the case of a YES instance of Hilbert–Schmidt-Distance, and the NO instance condition in (3.145) and (3.146) imply that $F(\psi, \phi) \geq \beta(2-\beta)$, in the case of a NO instance of Hilbert–Schmidt-Distance. Since the function $x \to x(2-x)$ is a bijection on the unit interval $[0, 1]$, it follows that the ability to decide Hilbert–Schmidt-Distance for pure states implies the ability to decide Fidelity-Pure-Pure, which is a BQP-complete problem by Theorem 3.8. We thus conclude that Hilbert–Schmidt-Distance is BQP-Hard. This, along with the fact that the problem is in the BQP class, concludes the proof. ■

Remark 3.1. *The normalized Schatten-p distance between two states ρ and σ is defined as*

$$\frac{1}{2^{1/p}} \|\rho - \sigma\|_p := \frac{1}{2^{1/p}} (\mathrm{Tr}[|\rho - \sigma|^p])^{1/p}. \tag{3.147}$$

We can formulate promise problems from these quantities, generalizing Hilbert–Schmidt-Distance in Problem 3.3. Plugging pure states ψ and ϕ into (3.147) and exploiting the fact that the eigenvalues of $\psi - \phi$ are equal to $|\sin\theta|$ and $-|\sin\theta|$ [Wil17, Proof of Theorem 9.3.1]*, where θ satisfies $F(\psi, \phi) = \cos^2\theta$, it follows that*

$$\frac{1}{2^{1/p}} \|\psi - \phi\|_p = \sqrt{1 - F(\psi, \phi)} \tag{3.148}$$

for all $p \geq 1$. Thus, by the same reasoning given in the second part of the proof of Theorem 3.10, we conclude that these promise problems are all BQP-hard.

Now consider that estimating the Schatten-2k distance between two states, where $k \in \mathbb{N}$, is in BQP. For constant k, each term in the expansion of $\|\rho - \sigma\|_{2k}^{2k} = \mathrm{Tr}[(\rho-\sigma)^{2k}]$ can be estimated in constant quantum depth [QKW24] *after the circuits that prepare multiples copies of ρ and σ are executed. Thus, combining with the above, we conclude that, for each constant $k \in \mathbb{N}$, the promise version of the problem of estimating $\frac{1}{2^{1/(2k)}} \|\rho - \sigma\|_{2k}$ is a BQP-complete problem.*

3.4.2 Fidelity between a pure state and a channel (QMA-complete)

Next, we provide a proof that the promise version of the problem of evaluating the fidelity between a channel and a pure state is QMA-complete. The definition of QMA can be found in Section 2.4.3.

Problem 3.4 [(α,β)-*Fidelity-Channel-Pure*]. *Let α and β be such that $0 \leq \alpha < \beta \leq 1$. Given are descriptions of circuits $U^{\mathcal{N}}_{SR\to BE}$ and U^{ψ}_{B} that prepare a unitary dilation of a channel*

$$\mathcal{N}_{S\to B}(\cdot) \coloneqq \operatorname{Tr}_E[U^{\mathcal{N}}_{SR\to BE}((\cdot)_S \otimes |0\rangle\langle 0|_R)(U^{\mathcal{N}}_{SR\to BE})^\dagger] \tag{3.149}$$

and a pure state $\psi_B \coloneqq U^{\psi}_{B}|0\rangle\langle 0|_B(U^{\psi}_{B})^\dagger$, respectively. Decide which of the following holds:

$$\textit{Yes:} \quad \max_{\rho_S} F(\mathcal{N}_{S\to B}(\rho_S),\psi_B) \geq 1-\alpha, \tag{3.150}$$

$$\textit{No:} \quad \max_{\rho_S} F(\mathcal{N}_{S\to B}(\rho_S),\psi_B) \leq 1-\beta, \tag{3.151}$$

where the maximization is over every input density operator ρ_S.

Theorem 3.11. *The promise problem Fidelity-Channel-Pure is QMA-complete.*

1. *(α,β)-Fidelity-Channel-Pure is in QMA for all $\alpha < \beta$. (It is implicit that the gap between α and β is larger than an inverse polynomial in the input length.)*
2. *$(\varepsilon, 1-\varepsilon)$-Fidelity-Channel-Pure is QMA-hard, even when ε decays exponentially in the input length.*

Thus, (α,β)-Fidelity-Channel-Pure is QMA-complete for all (α,β) such that $0 < \alpha < \beta < 1$.

Proof. To show that the problem is QMA-complete, we need to demonstrate two facts: first, that the problem is in QMA, and second, that it is QMA-hard.

Let us begin by proving that the problem is in QMA. The intuitive idea is that the prover sends an optimal state ρ_S to the verifier, who then performs the channel $\mathcal{N}_{S\to B}$ on it, followed by the unitary $(U^{\psi}_{B})^\dagger$. The verifier then performs a computational basis measurement on all registers of system B and accepts if and only if the all-zeros measurement outcome occurs. Indeed, the acceptance probability of this scheme is precisely equal to the fidelity in (3.150):

$$\begin{aligned} &\langle 0|_B(U^{\psi}_{B})^\dagger \mathcal{N}_{S\to B}(\rho_S) U^{\psi}_{B}|0\rangle_B \\ &= \langle\psi|_S \mathcal{N}_{S\to B}(\rho_S)|\psi\rangle_S \\ &= F(\mathcal{N}_{S\to B}(\rho_S),\psi_B). \end{aligned} \tag{3.152}$$

To bring the original expression more closely to the form given in (2.130), observe that

$$\begin{aligned} \langle 0|_B(U^{\psi}_{B})^\dagger \mathcal{N}_{S\to B}(\rho_S) U^{\psi}_{B}|0\rangle_B = \langle 1|_B X_B(U^{\psi}_{B})^\dagger \times \\ \operatorname{Tr}_E[U^{\mathcal{N}}_{SR\to BE}(|0\rangle\langle 0|_R \otimes \rho_S)(U^{\mathcal{N}}_{SR\to BE})^\dagger] U^{\psi}_{B} X_B|1\rangle_B, \end{aligned} \tag{3.153}$$

where X_B is understood to be the tensor power Pauli X operator acting on all qubits of the B register. To bring the final expression exactly into the form in (2.130), we need a single decision qubit that we measure. We can use a multi-controlled Toffoli gate from the B register to a single qubit decision qubit. Thus, if we identify x with 0, σ with ρ_S, and Q_n with $(X_B \otimes \mathbb{I}_E) \circ ((U_B^{\psi})^{\dagger} \otimes \mathbb{I}_E) \circ U_{SR\to BE}^{\mathcal{N}}$, it follows that the problem belongs to the QMA class.

Next, we show that any problem in the QMA class can be polynomially reduced to this problem. Let P be an arbitrary problem in the QMA class. This implies that (2.130) and (2.133) must hold. This problem can then be thought of as a fidelity problem with a channel $\mathcal{M}_x$ defined as

$$\mathcal{M}_{SAP\to D}^{x}(\cdot) \coloneqq \mathrm{Tr}_G[Q(|x\rangle\langle x|_S \otimes |0\rangle\langle 0|_A \otimes (\cdot))Q^{\dagger}]. \tag{3.154}$$

Furthermore, we identify the state ψ from the fidelity problem with $|1\rangle\langle 1|_D$, and then we find that

$$\begin{aligned} &\langle 1_D| \mathrm{Tr}_G[Q(|x\rangle\langle x|_S \otimes |0\rangle\langle 0|_A \otimes \sigma_P)Q^{\dagger})]|1\rangle_D \\ &= \langle 1|_G \, \mathcal{M}_{SAP\to D}^{x}(\sigma) \, |1\rangle_G \qquad (3.155) \\ &= F(\mathcal{M}^{x}(\sigma), |1\rangle\langle 1|). \qquad (3.156) \end{aligned}$$

It follows directly that this is an instance of $(1 - a(|x|), 1 - b(|x|))$-Fidelity-Channel-Pure, given that the channel $\mathcal{M}_x$ can be prepared efficiently, as well as the state $|1\rangle\langle 1|$. The desired hardness result then follows because $\mathrm{QMA}(1 - a(|x|), 1 - b(|x|)) \subseteq \mathrm{QMA}(\delta, 1 - \delta)$, for every δ exponentially small in the input length. ■

3.4.3 Fidelity between a pure state and a channel with separable input (QMA(2)-complete)

Lastly, we provide a proof for the result that the promise version of the problem of evaluating the fidelity between a pure state and a channel with a separable state as input is QMA(2)-complete. A state is separable if and only if is it not entangled. A separable state σ_{SR} can be expanded as follows:

$$\sigma_{SR} = \sum_k p(k) |\varphi^k\rangle\langle\varphi^k|_S \otimes |\phi^k\rangle\langle\phi^k|_R, \tag{3.157}$$

where $\{p(k)\}_k$ is a probability distribution and $\{|\varphi^k\rangle\langle\varphi^k|_S\}_k$ and $\{|\phi^k\rangle\langle\phi^k|_R\}_k$ are sets of pure states. SEP is defined as the set of all separable states.

Problem 3.5 [(α,β)-*Fidelity-Pure-Channel-Sep-Inp*]. *Let α and β be such that $0 \leq \alpha < \beta \leq 1$. Given are descriptions of circuits $U^{\mathcal{N}}_{SRE\to AE'}$ and U^{ψ}_{A} that prepare a unitary dilation of a channel*

$$\mathcal{N}_{SR\to A}(\cdot) \coloneqq \mathrm{Tr}_{E'}[U^{\mathcal{N}}_{SRE\to AE'}((\cdot)_{SR}\otimes|0\rangle\langle 0|_E)(U^{\mathcal{N}}_{SRE\to AE'})^\dagger], \tag{3.158}$$

and a pure state ψ_A, respectively. Decide which of the following holds:

$$\textit{Yes:} \quad \max_{\sigma_{SR}\in\mathrm{SEP}} F(\mathcal{N}_{SR\to A}(\sigma_{SR}),\psi_A) \geq 1-\alpha, \tag{3.159}$$

$$\textit{No:} \quad \max_{\sigma_{SR}\in\mathrm{SEP}} F(\mathcal{N}_{SR\to A}(\sigma_{SR}),\psi_A) \leq 1-\beta. \tag{3.160}$$

Theorem 3.12. *The promise problem Fidelity-Pure-Channel-Sep-Inp is QMA(2)-complete.*

1. *(α,β)-Fidelity-Pure-Channel-Sep-Inp is in QMA(2) for all $\alpha<\beta$. (It is implicit that the gap between α and β is larger than an inverse polynomial in the input length.)*
2. *$(\varepsilon, 1-\varepsilon)$-Fidelity-Pure-Channel-Sep-Inp is QMA(2)-hard, even when ε decays exponentially in the input length.*

Thus, (α,β)-Fidelity-Pure-Channel-Sep-Inp is QMA(2)-complete for all (α,β) such that $0<\alpha<\beta<1$.

Proof. To show that the problem is QMA(2)-complete, we need to demonstrate two facts: first, that the problem is in QMA(2), and second, that it is QMA(2)-hard. Let us begin by proving that the problem is in QMA(2). The intuitive idea is that the two provers, using shared randomness, send an optimal separable state σ_{SR} to the verifier, who then performs the channel $\mathcal{N}_{SR\to A}$ on it, followed by the unitary $(U^{\psi}_{A})^\dagger$. (Note that QMA(2) remains unchanged if the provers have access to shared randomness [HM10].) The verifier then performs a computational basis measurement on all registers of system A and accepts if and only if the all-zeros measurement outcome occurs.

Consider that a separable state can be decomposed as

$$\sigma_{SR} = \sum_k p(k)|\varphi^k\rangle\langle\varphi^k|_S \otimes |\phi^k\rangle\langle\phi^k|_R. \tag{3.161}$$

Indeed, the acceptance probability of this scheme is precisely equal to the fidelity in (3.159):

$$\begin{aligned} & F(\mathcal{N}_{SR\to A}(\sigma_{SR}), \psi_A) \\ & = \langle\psi|_A \mathcal{N}_{SR\to A}(\sigma_{SR})|\psi\rangle_A \\ & = \sum_k p(k)\langle\psi|_A \mathcal{N}_{SR\to A}(|\varphi^k\rangle\langle\varphi^k|_S \otimes |\phi^k\rangle\langle\phi^k|_R)|\psi\rangle_A . \end{aligned}$$

The final expression is an average of individual elements. Thus, taking a maximization over all separable states and noting that the maximum is always greater than the average, we conclude that

$$\begin{aligned} & \max_{\sigma_{SR}\in \mathrm{SEP}} F(\mathcal{N}_{SR\to A}(\sigma_{SR}), \psi_A) \\ & = \max_{|\varphi\rangle_S, |\phi\rangle_R} \langle\psi|_A \, \mathcal{N}_{SR\to A}(\varphi_S \otimes \phi_R) \, |\psi\rangle_A \\ & = \max_{|\varphi\rangle_S, |\phi\rangle_R} \langle 0|_A \, (U_A^{\psi})^\dagger \mathcal{N}_{SR\to A}(\varphi_S \otimes \phi_R) U_A^{\psi} \, |0\rangle_A \, . \end{aligned} \tag{3.162}$$

Thus, we see that

$$\begin{aligned} \max_{\sigma_{SR}\in \mathrm{SEP}} F(\mathcal{N}_{SR\to A}(\sigma_{SR}), \psi_A) = \max_{|\varphi\rangle_S, |\phi\rangle_R} & \langle 1|_A \, X_A \times \\ & (U_A^{\psi})^\dagger \, \mathrm{Tr}_{E'}[U^{\mathcal{N}}_{SRE\to AE'}(|0\rangle\langle 0|_E \otimes \varphi_S \otimes \phi_R) \times \\ & (U^{\mathcal{N}}_{SRE\to AE'})^\dagger] U_A^{\psi} X_A \, |1\rangle_A \, , \end{aligned} \tag{3.163}$$

where X_A is understood to be the tensor-power Pauli X operator acting on all qubits of the A register. To bring the final expression into the precise form in (2.134), we need a single decision qubit that we measure. We can use a multi-controlled Toffoli gate from the A register to a single qubit decision qubit. Thus, if we identify x with 0, ρ with φ_S, σ with ϕ_R and Q_n with $(X_A \otimes \mathbb{I}_R) \circ ((U_A^{\psi})^\dagger \otimes \mathbb{I}_R) \circ U^{\mathcal{N}}_{SRE\to AE'}$, it follows that the problem belongs to the QMA(2) class.

Next, we show that any problem in the QMA(2) class can be polynomially reduced to this problem. Let P be an arbitrary problem in the QMA(2) class. This implies that (2.134) and (2.136) must hold. This problem can then be thought of as a fidelity problem with a channel $\mathcal{M}_x$ defined as

$$\mathcal{M}^x_{SAP_1P_2\to D}(\cdot) := \mathrm{Tr}_G[Q_n(|x\rangle\langle x|_S \otimes |0\rangle\langle 0|_A \otimes (\cdot)_{P_1P_2})Q_n^\dagger]. \tag{3.164}$$

Furthermore, by identifying the state ψ from the fidelity problem with $|1\rangle\langle 1|$, then we find that

$$\langle 1| \operatorname{Tr}_G[Q(|x\rangle\langle x|_S \otimes |0\rangle\langle 0|_A \otimes \psi_1 \otimes \psi_2)Q^\dagger]|1\rangle \tag{3.165}$$
$$= \langle 1|\mathcal{M}^x(\psi_1 \otimes \psi_2)|1\rangle \tag{3.166}$$
$$= F(\mathcal{M}_x(\psi_1 \otimes \psi_2), |1\rangle\langle 1|). \tag{3.167}$$

It follows directly that this is an instance of $(1 - a(|x|), 1 - b(|x|))$-Fidelity-Channel-Pure, given that the channel $\mathcal{M}_x$ can be prepared efficiently, as well as the state $|1\rangle\langle 1|$. The desired hardness result then follows because $\mathrm{QMA}(1 - a(|x|), 1 - b(|x|)) \subseteq \mathrm{QMA}(\delta, 1 - \delta)$, for every δ exponentially small in the input length (see [HM10, Theorem 9]). ■

3.5 Conclusion

In this paper, we have delineated several algorithms for estimating distinguishability measures on quantum computers. All of the measures are based on trace distance or fidelity, and we have considered them for quantum states and channels. Many of the algorithms rely on interaction with a quantum prover, and in these cases, we have replaced the prover with a parameterized quantum circuit. As such, these methods are not guaranteed to converge for all possible states and channels. It is an interesting open question to determine conditions under which the algorithms are guaranteed to converge and run efficiently.

We have also simulated several of the algorithms in both the noiseless and noisy scenarios. We found that the simulations converge well for all states and channels considered, and for all algorithms simulated. As more advanced quantum computers become available (with more qubits and greater reliability), it would be interesting to simulate our algorithms for states and channels involving larger numbers of qubits. All of our Python code is written in a modular way, such that it will be straightforward to explore this direction. Lastly, we proved several complexity-theoretic results about various distance estimation algorithms; in particular, we showed and, in some cases, recalled that there is a fidelity or distance estimation problem that is complete for the commonly studied complexity classes BQP, QMA, QMA(2), QSZK, QIP(2), and QIP.

Going forward from here, it remains open to determine methods for estimating other distinguishability measures such as the Petz–Rényi relative entropy

[Pet85, Pet86] and the sandwiched Rényi relative entropy [MLDS+13, WWY14] of channels [LKDW18]. More generally, one could consider distinguishability measures beyond these. One desirable aspect of the algorithms appearing in this paper is that they provide a one-shot interpretation for the various distinguishability measures as the maximum acceptance probability in a quantum interactive proof (with the trace-distance based algorithms and interpretations being already known from [Wat02c, RW05, GW07, Gut09, Gut12]). However, it is unclear to us whether one could construct a quantum interactive proof for which the maximum acceptance probability is related to the Petz– or sandwiched Rényi relative entropy of a channel.

Note added: While finalizing the results of our initial arXiv post [ARSW21], we noticed the arXiv post [BBC21], which is related to the contents of Section 3.2. Ref. [BBC21] is now published as [BBC22].

Chapter 4

Symmetry

> *Symmetry, as wide or as narrow as you may define its meaning, is one idea by which man through the ages has tried to comprehend and create order, beauty, and perfection.* —— Hermann Weyl, Symmetry (1952)

This chapter is based on collaborative work with Dr. Margarite L. LaBorde, and Dr. Mark M. Wilde [LRW23, RLW25]. Throughout this section, 'we' refers to all three collaborators.

Symmetry plays a fundamental role in physics [FR96, Gro96a]. The evolution of a closed physical system is dictated by a Hamiltonian, which often possesses symmetry that limits transitions from one state to another in the form of superselection rules [WWW52, AS67]. Permutation symmetry in the extension of a bipartite quantum state indicates a lack of entanglement in that state [Wer89a, DPS02, DPS04]. This permutation symmetry limits entanglement, which relates to fundamental principles of quantum information like the no-cloning theorem [Par70, Die82, WZ82] and entanglement monogamy [Ter04]. Additionally, the lack of a shared reference frame between two parties implies that a quantum state prepared relative to another party's reference frame respects a certain symmetry and is less useful than one breaking that symmetry [BRS07]. In all of these cases, a state respecting a symmetry is less resourceful than one breaking it. In more recent years, quantum resource theories have been proposed for each of the above scenarios (asymmetry [MS13, MS14], unextendibility [KDWW19, KDWW21], and frameness [GS08]) in order to quantify the resourcefulness of quantum states (see [CG19] for a review). As such, it is useful to be able

to test whether a quantum state possesses symmetry and to quantify how much symmetry it possesses.

In this chapter, we show how a quantum computer can test for symmetries of quantum states and channels generated by quantum circuits. In fact, our quantum-computational tests actually quantify how symmetric a state or channel is. Given that asymmetry (i.e., breaking of symmetry) is a useful resource in a wide variety of contexts while being potentially difficult for a classical computer to verify, our tests are helpful in determining how useful a state will be for certain quantum information processing tasks. Additionally, our tests are in the spirit of the larger research program of using quantum computers to understand fundamental quantum-mechanical properties of high-dimensional quantum states, such as symmetry and entanglement, that are out of reach for classical computers. Here, we give explicit algorithmic descriptions of our tests, connect to known applications of interest, and provide a general framework that facilitates new applications and research in this area. We augment these contributions by providing novel resource-theoretic results as well.

We begin our development in Section 4.1 by introducing a general form of symmetry of quantum states that captures both the extendibility of bipartite states [Wer89a, DPS02, DPS04], as well as symmetries of a single quantum system with respect to a group of unitary transformations [MS13, MS14]. This generalization allows for incorporating several kinds of symmetry tests into a single framework. We call this notion G-symmetric extendibility, and we discuss two different forms of it.

In Section 4.2 we move on to an important contribution of our paper—namely, how a quantum computer can test for and estimate quantifiers of symmetry. These quantifiers are collectively called *maximum symmetric fidelities*, with more particular names given in what follows. We prove that our quantum computational tests of symmetry have acceptance probabilities precisely equal to the various quantifiers. These results endow these resource-theoretic measures with operational meanings and allow us to estimate them to arbitrary precision. Using complexity-theoretic language, we demonstrate that several of these quantum-computational tests of symmetry can be conducted in the form of a quantum interactive proof (QIP) system consisting of two quantum messages exchanged between a verifier and a prover [Wat09b, VW16]. Our results thus generalize previous results in the context of unextendibility and entanglement of bipartite quantum states [HMW14]; additionally, we go on to clarify the relation between our results and previous ones (Section 4.3). Simpler forms of the tests can be conducted without

the aid of a prover and are thus efficiently computable on a quantum computer.

In Section 4.3, we show how the established concepts of k-extendibility or k-Bose extendibility [Wer89a, DPS02, DPS04] can be recovered as special cases of our symmetry tests for both bipartite and multipartite states. These examples are particularly interesting as they serve as tests of separability.

Section 4.4 shows that the maximum symmetric fidelities can be calculated by means of semi-definite programs, which is helpful for benchmarking the outputs of the quantum algorithms for sufficiently small circuits. This follows from combining the known semi-definite program for fidelity [Wat13] with the semi-definite constraints corresponding to the symmetry tests. Furthermore, we employ representation theory [Ste12] to simplify some of the semi-definite programs even further, by making use of the block-diagonal form that results from performing a group twirl on a state.

We follow this in Section 4.5 by demonstrating the use of variational quantum algorithms for estimating the maximum symmetric fidelities for various example groups. In general, this approach is not guaranteed to estimate the maximum symmetric fidelities precisely, as the parameterized circuit used is not able to realize an arbitrarily powerful quantum computation. This approach thus leads only to lower bounds on the maximum symmetric fidelities. However, we find that this heuristic approach performs well for a variety of example groups, including symmetry tests with respect to $\mathbb{Z}_2$, the triangular dihedral group, a collective unitary action, etc. We note that a recent work adopted a similar variational approach for estimating the fidelity of quantum states generated by quantum circuits [CSZW22]. It is well known that this latter problem is QSZK-complete [Wat02c] and thus likely difficult for quantum computers to solve in general. It remains an open question to determine how well this variational approach performs generally, beyond the examples considered in this paper. We note that the algorithms defined in this work rely on local measurements alone and, as a consequence of the results of [CSV+213], should not suffer from the barren plateau problem in which global cost functions become untrainable. Since we have only conducted simulations of our algorithms for small quantum systems, it remains open to provide evidence that our algorithms will avoid the barren plateau problem for larger systems.

4.1 Notions of symmetry

In this section, we review the notions of symmetry presented in [MS13, MS14, LRW23, RLW25].

Definition 4.1 [*G-symmetric*]. *Let G be a group with projective unitary representation $\{U_S(g)\}_{g\in G}$, and let ρ_S be a state of system S. The state ρ_S is symmetric with respect to G* [MS13, MS14] *if*

$$\rho_S = U_S(g)\rho_S U_S(g)^\dagger \quad \forall g \in G. \tag{4.1}$$

G-symmetry is the usual notion of symmetry considered in most physical contexts. For example, in [RBN+22, LSS+22], the authors use G-symmetric states in various quantum machine learning applications, primarily in classification algorithms where the labeling of the state should remain invariant. Additionally, testing the incoherence of a state in the vein of [SAP17, BCP14] is a special case of a G-symmetry test where the group is the cyclic group of order $|G|$.

Expanding upon this definition, we recall the definition of G-Bose symmetry, a stronger notion of symmetry. G-Bose symmetry implies G-symmetry, though the reverse implication is not true in general. G-Bose symmetry checks if a state belongs to the symmetric subspace induced by the group representation. This more mathematical notion of symmetry has proven useful in deriving important results, such as the quantum de Finetti theorem [Har13]. As a practical application, a circuit construction for projecting onto the symmetric subspace corresponding to the standard symmetric group [BBD+97] has been used in a number of quantum computational tests of entanglement [HMW14, GHMW15, LRW23, BLW23]. We give the definition of G-Bose symmetry below.

Definition 4.2 [*G-Bose-symmetric*]. *Let G be a group with unitary representation $\{U_S(g)\}_{g\in G}$. A state ρ_S is Bose-symmetric with respect to G if*

$$\rho_S = U_S(g)\rho_S \quad \forall g \in G. \tag{4.2}$$

The condition in (4.2) is equivalent to the condition

$$\rho_S = \Pi_S^G \rho_S \Pi_S^G, \tag{4.3}$$

where the projector Π_S^G is defined as

$$\Pi_S^G := \frac{1}{|G|}\sum_{g\in G} U_S(g). \tag{4.4}$$

We note here that the notion of G-Bose-symmetry can be generalized to compact Lie groups. In this case, one requires an invariant measure, which exists for all such groups. An important example in quantum information is the unitary group equipped with the Haar measure. See [Har13, Proposition 2] for mathematical details of how the projector Π_S^G is defined in this case. Throughout our paper, however, we focus exclusively on finite groups.

Both of the aforementioned symmetry notions (G-symmetry and G-Bose-symmetry) can be expanded to scenarios in which the tester has limited access to the state of interest. For example, one can test whether, given a part of a state, there exists an extension that is symmetric. These notions lead to further, pertinent symmetry tests. For instance, when the group in question is the permutation group, G-Bose extendibility is relevant for detecting entanglement [NOP09] and efficiently bounding quantum discord [Pia16]. Similarly, G-symmetric extendible states have been studied in the context of entanglement distillability [Now16] and k-extendibility [Wer89a, DPS02, DPS04, BC12, KDWW19].

Definition 4.3 [*G-symmetric extendible*]. *Let G be a group with unitary representation $\{U_{RS}(g)\}_{g\in G}$. A state ρ_S is G-symmetric extendible if there exists a state ω_{RS} such that*

1. *the state ω_{RS} is an extension of ρ_S, i.e.,*

$$\mathrm{Tr}_R[\omega_{RS}] = \rho_S, \tag{4.5}$$

2. *the state ω_{RS} is G-symmetric, in the sense that*

$$\omega_{RS} = U_{RS}(g)\omega_{RS}U_{RS}(g)^\dagger \qquad \forall g \in G. \tag{4.6}$$

Definition 4.4 [*G-Bose symmetric extendible*]. *A state ρ_S is G-Bose symmetric extendible (G-BSE) if there exists a state ω_{RS} such that*

1. *the state ω_{RS} is an extension of ρ_S, i.e.,*

$$\mathrm{Tr}_R[\omega_{RS}] = \rho_S, \tag{4.7}$$

2. *the state ω_{RS} is Bose symmetric, i.e., satisfies*

$$\omega_{RS} = \Pi_{RS}^G \omega_{RS} \Pi_{RS}^G, \tag{4.8}$$

where

$$\Pi_{RS}^G := \frac{1}{|G|}\sum_{g\in G} U_{RS}(g). \tag{4.9}$$

Observe that

$$\Pi^G_{RS} = U_{RS}(g)\Pi^G_{RS} = \Pi^G_{RS} U_{RS}(g), \tag{4.10}$$

for all $g \in G$, which follows from what is called the rearrangement theorem in group theory.

Special cases of the notions of symmetry from Definitions 4.3 and 4.4 are k-extendibility of bipartite states and G-symmetry of unipartite states, as we discuss below.

Example 4.1 [*k-extendible*]. *Recall that a bipartite state ρ_{AB} is k-extendible* [Wer89a, DPS02, DPS04] *if there exists an extension state $\omega_{AB_1\cdots B_k}$ such that*

$$\mathrm{Tr}_{B_2\cdots B_k}[\omega_{AB_1\cdots B_k}] = \rho_{AB} \tag{4.11}$$

and

$$\omega_{AB_1\cdots B_k} = W_{B_1\cdots B_k}(\pi)\omega_{AB_1\cdots B_k}W_{B_1\cdots B_k}(\pi)^\dagger, \tag{4.12}$$

for all $\pi \in S_k$, where each system $B_1, \ldots, B_k$ is isomorphic to the system B and $W_{B_1\cdots B_k}(\pi)$ is a unitary representation of the permutation $\pi \in S_k$, with S_k the symmetric group. Then the established notion of k-extendibility is a special case of G-symmetric extendibility, in which we set

$$S = AB_1, \tag{4.13}$$
$$R = B_2 \cdots B_k, \tag{4.14}$$
$$G = S_k, \tag{4.15}$$
$$U_{RS}(g) = \mathbb{I}_A \otimes W_{B_1\cdots B_k}(\pi). \tag{4.16}$$

Example 4.2 [*k-Bose-extendible*]. *A bipartite state ρ_{AB} is k-Bose-extendible if there exists an extension state $\omega_{AB_1\cdots B_k}$ such that*

$$\mathrm{Tr}_{B_2\cdots B_k}[\omega_{AB_1\cdots B_k}] = \rho_{AB} \tag{4.17}$$

and

$$\omega_{AB_1\cdots B_k} = \Pi^{\mathrm{Sym}}_{B_1\cdots B_k}\omega_{AB_1\cdots B_k}\Pi^{\mathrm{Sym}}_{B_1\cdots B_k}, \tag{4.18}$$

where

$$\Pi^{\mathrm{Sym}}_{B_1\cdots B_k} := \frac{1}{k!}\sum_{\pi\in S_k} W_{B_1\cdots B_k}(\pi) \tag{4.19}$$

is the projection onto the symmetric subspace. Thus, k-Bose-extendibility is a special case of G-Bose-symmetric extendibility under the identifications in (4.13)–(4.16).

Although the concepts of G-symmetric extendibility and G-Bose-symmetric extendibility, in Definitions 4.3 and 4.4, respectively, are generally different, we can relate them by purifying a G-symmetric extendible state to a larger Hilbert space, as stated in Theorem 4.1 below. The ability to do so plays a critical role in the algorithms proposed in Section 4.2. We give a proof of Theorem 4.1 in Appendix C.1.

Theorem 4.1. *A state ρ_S is G-symmetric extendible if and only if there exists a purification $\psi^{\rho}_{RS\hat{R}\hat{S}}$ of ρ_S satisfying the following:*

$$|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}} = \left(U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g)\right)|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}} \quad \forall g \in G, \tag{4.20}$$

where the overbar denotes the entrywise complex conjugate. The condition in (4.20) is equivalent to

$$|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}} = \Pi^{G}_{RS\hat{R}\hat{S}}|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}}, \tag{4.21}$$

where

$$\Pi^{G}_{RS\hat{R}\hat{S}} := \frac{1}{|G|}\sum_{g\in G} U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g). \tag{4.22}$$

Let us finally introduce two other notions of symmetry, one of which represents a generalization of a symmetry recently considered in [PRRW24]. Before doing so, let us first recall that a bipartite state ρ_{AB} is separable with respect to the partition A, B, denoted as $\rho_{AB} \in \mathrm{SEP}(A:B)$, if it can be written in the following form [Wer89b]:

$$\rho_{AB} = \sum_{x\in\mathcal{X}} p(x)\psi^{x}_{A} \otimes \phi^{x}_{B}, \tag{4.23}$$

where $\mathcal{X}$ is a finite alphabet, $\{p(x)\}_{x\in\mathcal{X}}$ is a probability distribution, and $\{\psi^{x}_{A}\}_{x\in\mathcal{X}}$ and $\{\phi^{x}_{B}\}_{x\in\mathcal{X}}$ are sets of pure states. States that cannot be written in this form are entangled.

Definition 4.5 [*G-symmetric separably extendible*]. *Let G be a group with projective unitary representation $\{U_{RS}(g)\}_{g\in G}$, and let ρ_S be a state. The state ρ_S is G-symmetric separably extendible if there exists a state ω_{RS} such that*

1. *the state ω_{RS} is a separable extension of ρ_S, i.e.,*

$$\mathrm{Tr}_R[\omega_{RS}] = \rho_S, \tag{4.24}$$

$$\omega_{RS} \in \mathrm{SEP}(R:S), \tag{4.25}$$

2. *the state ω_{RS} is G-symmetric, in the sense that*

$$\omega_{RS} = U_{RS}(g)\omega_{RS}U_{RS}(g)^\dagger \qquad \forall g \in G. \tag{4.26}$$

Definition 4.6 [*G-Bose-symm. separably extendible*]. *Let G be a group with unitary representation $\{U_{RS}(g)\}_{g\in G}$, and let ρ_S be a state. The state ρ_S is G-Bose-symmetric separably extendible if there exists a state ω_{RS} such that*

1. *the state ω_{RS} is a separable extension of ρ_S, i.e.,*

$$\mathrm{Tr}_R[\omega_{RS}] = \rho_S, \tag{4.27}$$

$$\omega_{RS} \in \mathrm{SEP}(R:S), \tag{4.28}$$

2. *the state ω_{RS} is Bose symmetric, i.e., satisfies*

$$\omega_{RS} = \Pi^G_{RS}\omega_{RS}\Pi^G_{RS}, \tag{4.29}$$

where Π^G_{RS} is defined in (4.9).

By comparing Definitions 4.3 and 4.4 with Definitions 4.5 and 4.6, respectively, we see that the main additional constraint in the latter definitions is that the extension is required to be a separable state. As such, when the state and unitary representations are given as matrices, this additional constraint makes the search for an extension more computationally difficult than those needed for Definitions 4.3 and 4.4, because optimizing over the set of separable states is computationally difficult [Gur03, Gha10] and it is not possible to perform this search by means of SDPs [Faw21]. Here, we consider the complexity of testing the symmetry in Definition 4.6 when the state and unitary representations are given as circuit descriptions.

Let us comment briefly on the connection between Definition 4.6 and the symmetry considered in [PRRW24]. In [PRRW24], the goal was to test whether a given bipartite state ρ_{AB} is separable. It was shown that one can equivalently do so by testing whether there exists a separable extension $\rho_{A'AB} \in \mathrm{SEP}(A':AB)$ of ρ_{AB} that is Bose symmetric with respect to the unitary representation $\{I_{A'A}, F_{A'A}\}$ of the symmetric group of order two, where $F_{AA'}$ is the unitary swap operator. More concretely, the test checks whether there exists $\rho_{A'AB} \in \mathrm{SEP}(A':AB)$ such that

$$\mathrm{Tr}_{A'}[\rho_{A'AB}] = \rho_{AB}, \tag{4.30}$$

$$\rho_{A'AB} = \Pi_{A'A}\rho_{A'AB}\Pi_{A'A}, \tag{4.31}$$

where $\Pi_{A'A} := (I_{AA'} + F_{AA'})/2$. As such, this represents a non-trivial example of the symmetry presented in Definition 4.6.

Test	Algorithm	Acceptance Probability
G-Bose symmetry	4.1	$\max_{\sigma \in \text{B-Sym}_G} F(\rho, \sigma)$
G-symmetry	4.2	$\max_{\sigma \in \text{Sym}_G} F(\rho, \sigma)$
G-Bose symmetric extendibility	4.3	$\max_{\sigma \in \text{BSE}_G} F(\rho, \sigma)$
G-symmetric extendibility	4.4	$\max_{\sigma \in \text{SymExt}_G} F(\rho, \sigma)$

Table 4.1: Summary of the various symmetry tests proposed in Section 4.2 and their acceptance probabilities. For more details, see Theorems 4.2, 4.3, 4.4, and 4.5.

4.2 Testing symmetry and extendibility on quantum computers

We can use a quantum computer to test for G-symmetric extendibility of a quantum state, as well as for other forms of symmetry discussed in the previous section. We assume the following in doing so:

1. there is a quantum circuit available that prepares a purification $\psi^{\rho}_{S'S}$ of the state ρ_S,
2. there is an efficient implementation of each of the unitary operators in the set $\{U_{RS}(g)\}_{g \in G}$,
3. and there is an efficient implementation of each of the unitary operators in the set $\{\overline{U}_{RS}(g)\}_{g \in G}$.

The first assumption can be made less restrictive by employing the variational, purification-learning procedure from [CSZW22]. That is, given a circuit that prepares the state ρ_S, the variational algorithm from [CSZW22] outputs a circuit that approximately prepares a purification of ρ_S. We should note that the convergence of the algorithm from [CSZW22] has not been established, and so the first assumption might be necessary for some applications. See also [EBS+23].

The last assumption can be relaxed by the following reasoning: a standard gate set for approximating arbitrary unitaries in quantum computing consists of the controlled-NOT gate, the Hadamard gate, and the T gate [NC00]. The first two gates have only real entries while the T gate is a diagonal 2×2 unitary gate with the entries 1 and $e^{i\pi/4}$. The complex conjugate of this gate is equal to $T^\dagger$. Thus, if a circuit for $U_{RS}(g)$ is constructed from this standard gate set, then we can generate a circuit for $\overline{U}_{RS}(g)$ by replacing every T gate in the original circuit with $T^\dagger$.

We now consider various quantum computational tests of symmetry that have increasing complexity. Table 4.1 summarizes the main theoretical insight of this section, which is that the acceptance probability of each symmetry test can be expressed in terms of the fidelity of the state being tested to a set of symmetric states.

To give insight along the way, we provide an example along with the tests below. In particular, we consider the dihedral group of the triangle, D_3, which has order six and is isomorphic to the symmetric group on three elements, the smallest non-abelian group. Recall that dihedral groups are the symmetry groups of regular polygons.

Our example D_3 is generated via a flip f and a rotation r: $\langle e, f, r \mid r^3 = e, f^2 = e, frf = r^{-1} \rangle$. The group thus has six elements $\{e, f, r, r^2, fr, fr^2\}$, where e is the identity element. We will specify elements r^2, fr, fr^2 in order to enforce the rules of the group.

The group table for this dihedral group is given by

Group element	e	f	r	r^2	fr	fr^2
e	e	f	r	r^2	fr	fr^2
f	f	e	fr	fr^2	r	r^2
r	r	fr^2	r^2	e	f	fr
r^2	r^2	fr	e	r	fr^2	f
fr	fr	r^2	fr^2	f	e	r
fr^2	fr^2	r	f	fr	r^2	e

To fully realize D_3, we use a two-qubit unitary representation and specify the generators as such: $\{e \to \mathbb{I}, f \to \text{CNOT}, r \to \text{CNOT} \circ \text{SWAP}\}$. A quick check confirms that these generators obey the commutation rules of the group and generate the table above. Throughout the next four sections, we substitute this group into the presented algorithms to demonstrate their construction.

4.2.1 Testing G-Bose symmetry

Let us begin by discussing the simplest version of the problem. Suppose that the state under consideration is pure, so that we can write it as $\psi_S \equiv |\psi\rangle\langle\psi|_S$, and

suppose that the R system is trivial. We recover the traditional case of G-Bose symmetry mentioned in Definition 4.2. Thus, our goal is to decide if

$$|\psi\rangle_S = U_S(g)|\psi\rangle_S \quad \forall g \in G. \tag{4.32}$$

This condition is equivalent to

$$|\psi\rangle_S = \Pi_S^G |\psi\rangle_S, \tag{4.33}$$

where

$$\Pi_S^G := \frac{1}{|G|} \sum_{g\in G} U_S(g), \tag{4.34}$$

which is in turn equivalent to

$$\left\| \Pi_S^G |\psi\rangle_S \right\|_2 = 1. \tag{4.35}$$

The equivalence

$$|\psi\rangle_S = \Pi_S^G |\psi\rangle_S \quad \Leftrightarrow \quad \left\| \Pi_S^G |\psi\rangle_S \right\|_2 = 1 \tag{4.36}$$

holds from the Pythagorean theorem and the positive definiteness of the norm. Indeed,

$$\left\| \Pi_S^G |\psi\rangle_S \right\|_2 = 1 \quad \Rightarrow \quad \left\| \Pi_S^G |\psi\rangle_S \right\|_2^2 = 1 = \| |\psi\rangle_S \|_2^2 \tag{4.37}$$

and since the Pythagorean theorem states that

$$\left\| \Pi_S^G |\psi\rangle_S \right\|_2^2 + \left\| (\mathbb{I}_S - \Pi_S^G) |\psi\rangle_S \right\|_2^2 = \| |\psi\rangle_S \|_2^2 , \tag{4.38}$$

we conclude that $\left\| (\mathbb{I}_S - \Pi_S^G) |\psi\rangle_S \right\|_2 = 0$, which implies that $(\mathbb{I}_S - \Pi_S^G) |\psi\rangle_S = 0$ from the positive definiteness of the norm. This in turn is equivalent to the left-hand side of (4.36). Thus, if we have a method to perform the projection onto Π_S^G, then we can decide whether (4.35) holds.

There is a simple quantum algorithm to do so. This algorithm was originally proposed in [Har05, Chapter 8] under the name of "generalized phase estimation." It proceeds as follows and can be summarized as "performing the quantum phase estimation algorithm with respect to the unitary representation $\{U_S(g)\}_{g\in G}$":

Note that the register C has dimension $|G|$. Also, we can write the state $|0\rangle_C$ as $|e\rangle_C$, where e is the identity element of the group. The result of Step 2 of Algorithm 4.1 is to prepare the following uniform superposition state:

$$|+\rangle_C := \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle_C. \tag{4.40}$$

Algorithm 4.1 G-Bose symmetry test schematic.

Input: Quantum circuit U^ρ that prepares a purification of state ρ and unitary representation of group G, $\{U(g)\}_{g\in G}$.

Output: Estimate of $\max_{\sigma\in \text{B-Sym}_G} F(\rho,\sigma)$.

1: Prepare an ancillary register C in the state $|0\rangle_C$.

2: Act on register C with a quantum Fourier transform.

3: Append the state $|\psi\rangle_S$ and perform the following controlled unitary:

$$\sum_{g\in G} |g\rangle\langle g|_C \otimes U_S(g). \tag{4.39}$$

4: Perform an inverse quantum Fourier transform on register C, measure in the basis $\{|g\rangle\langle g|_C\}_{g\in G}$, and accept if and only if the zero outcome $|0\rangle\langle 0|_C$ occurs.

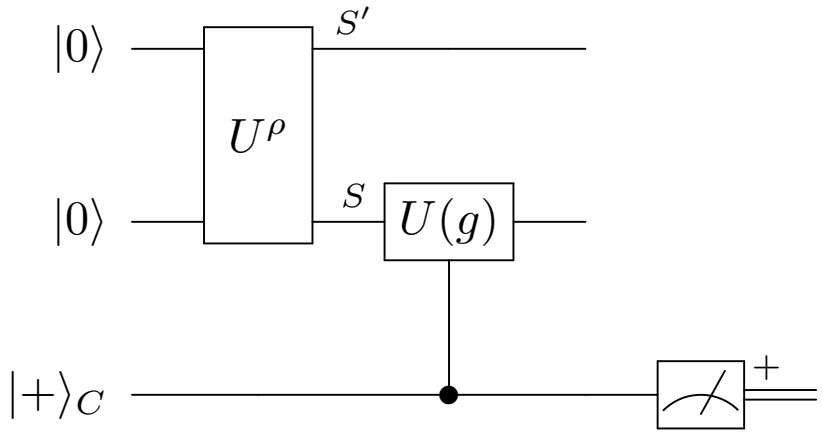


Figure 4.1: Quantum circuit to implement Algorithm 4.1. The unitary U^ρ prepares a purification $\psi_{S'S}$ of the state ρ_S. The final measurement box with the plus-sign to the right of it indicates that the measurement $\{|+\rangle\langle+|_C, \mathbb{I}_C - |+\rangle\langle+|_C\}$ is performed. (We use this same notation in several forthcoming figures.) Algorithm 4.1 tests whether the state ρ_S is G-Bose symmetric, as defined in Definition 4.2. Its acceptance probability is equal to $\text{Tr}[\Pi_S^G \rho_S]$, where Π_S^G is defined in (4.34).

Although the quantum Fourier transform is specified in Algorithm 4.1, in fact, any unitary that generates the desired superposition state $|+\rangle_C$ can serve as a replacement in Steps 2 and 4 above and oftentimes leads to an improvement in circuit depth. The same is true for all algorithms that follow.

Moving on, the overall state after Step 3 is as follows:

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C U_S(g)|\psi\rangle_S . \tag{4.41}$$

The final step of Algorithm 4.1 projects the register C onto the state $|+\rangle_C$. According to the aforementioned convention, Algorithm 4.1 accepts if the identity element outcome $|e\rangle\langle e|_C$ occurs. The probability that Algorithm 4.1 accepts is equal to

$$\begin{aligned} &\left\| (\langle +|_C \otimes \mathbb{I}_S) \left(\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle_C U_S(g)|\psi\rangle_S \right) \right\|_2^2 \\ &= \left\| \frac{1}{|G|} \sum_{g \in G} U_S(g)|\psi\rangle_S \right\|_2^2 \qquad (4.42) \\ &= \left\| \Pi_S^G |\psi\rangle_S \right\|_2^2 . \qquad (4.43) \end{aligned}$$

Figure 4.1 depicts this quantum algorithm. Not only does it decide whether the state $|\psi\rangle_S$ is symmetric, but it also quantifies how symmetric the state is. Since the acceptance probability is equal to $\left\| \Pi_S^G |\psi\rangle_S \right\|_2^2$, and this quantity is a measure of symmetry, we can repeat the algorithm a large number of times to estimate the acceptance probability to arbitrary precision.

The same quantum algorithm can decide whether a given mixed state ρ_S is G-Bose symmetric (see Example 4.2). Similar to the above, it also can estimate how G-Bose symmetric the state ρ_S is. To see this, consider that the acceptance probability for a pure state can be rewritten as follows:

$$\left\| \Pi_S^G |\psi\rangle_S \right\|_2^2 = \mathrm{Tr}[\Pi_S^G |\psi\rangle\langle\psi|_S]. \tag{4.44}$$

Then since every mixed state can be written as a probabilistic mixture of pure states, it follows that the acceptance probability of Algorithm 4.1, when acting on the mixed state ρ_S, is equal to

$$\mathrm{Tr}[\Pi_S^G \rho_S]. \tag{4.45}$$

This acceptance probability is equal to one if and only if $\rho_S = \Pi_S^G \rho_S \Pi_S^G$, and so this test is a faithful test of G-Bose symmetry. The equivalence

$$\mathrm{Tr}[\Pi_S^G \rho_S] = 1 \quad \Leftrightarrow \quad \rho_S = \Pi_S^G \rho_S \Pi_S^G \tag{4.46}$$

follows as a limiting case of the gentle measurement lemma [Win99, ON07] (see also [Wil17, Lemma 9.4.1]):

$$\frac{1}{2} \left\| \rho_S - \frac{\Pi_S^G \rho_S \Pi_S^G}{\mathrm{Tr}[\Pi_S^G \rho_S]} \right\|_1 \leq \sqrt{1 - \mathrm{Tr}[\Pi_S^G \rho_S]} \tag{4.47}$$

and the positive definiteness of the trace norm. Again, through repetition, we can estimate the acceptance probability $\mathrm{Tr}[\Pi_S^G \rho_S]$ and then employ it as a measure of G-Bose symmetry.

Interestingly, the acceptance probability of Algorithm 4.1 can be expressed as the *maximum G-Bose-symmetric fidelity*, defined for a state ρ_S as

$$\max_{\sigma_S \in \text{B-Sym}_G} F(\rho_S, \sigma_S), \tag{4.48}$$

where

$$\text{B-Sym}_G := \left\{ \sigma_S \in \mathcal{D}(\mathcal{H}_S) : \sigma_S = \Pi_S^G \sigma_S \Pi_S^G \right\}, \tag{4.49}$$

and the fidelity of quantum states ω and τ is defined as [Uhl76]

$$F(\omega, \tau) := \left\| \sqrt{\omega}\sqrt{\tau} \right\|_1^2. \tag{4.50}$$

We state this claim in Theorem 4.2 below and provide a proof of Theorem 4.2 in Appendix C.2. Thus, Algorithm 4.1 gives an operational meaning to the maximum G-Bose-symmetric fidelity in terms of its acceptance probability, and it can be used to estimate this fundamental measure of symmetry.

Theorem 4.2. *For a state ρ_S, the acceptance probability of Algorithm 4.1 is equal to the maximum G-Bose symmetric fidelity. That is,*

$$\mathrm{Tr}[\Pi_S^G \rho_S] = \max_{\sigma_S \in \text{B-Sym}_G} F(\rho_S, \sigma_S). \tag{4.51}$$

Example 4.3. *In the example of the dihedral group D_3, the $|+\rangle_C$ state is a uniform superposition of six elements. We use three qubits and the unitary U_d shown in Figure 4.2 to generate an equal superposition of six elements:*

$$U_d |000\rangle = \frac{1}{\sqrt{6}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle). \tag{4.52}$$

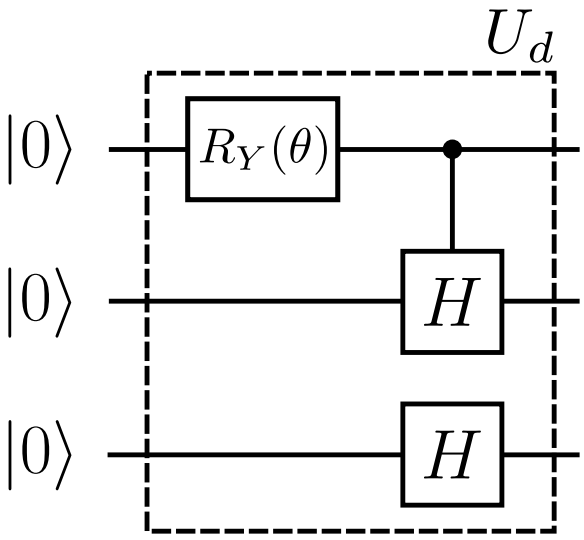


Figure 4.2: Unitary U_d, with $\theta = 2\arctan\left(\frac{1}{\sqrt{2}}\right)$, generates the equal superposition of six elements from (4.52). Note that the controlled-Hadamard is controlled on the qubit being in the state zero.

These control register states need to be mapped to group elements to be meaningful; thus, we employ the mapping $\{|000\rangle \to e, |001\rangle \to fr^2, |010\rangle \to fr, |011\rangle \to r, |100\rangle \to f, |101\rangle \to r^2\}$ *for our circuit constructions. The circuit to test for* D_3*-symmetry is shown in Figure 4.3.*

4.2.2 Testing G-symmetry

We now discuss how to modify Algorithm 4.1 to one that decides whether a state ρ_S is G-symmetric (see Definition 4.1), i.e., if

$$\rho_S = U_S(g)\rho_S U_S(g)^\dagger \quad \forall g \in G\,. \tag{4.53}$$

We also prove that the acceptance probability of the modified algorithm (Algorithm 4.2 below) is equal to the *maximum G-symmetric fidelity*, defined as

$$\max_{\sigma \in \mathrm{Sym}_G} F(\rho_S, \sigma_S), \tag{4.54}$$

where

$$\mathrm{Sym}_G := \left\{\sigma_S \in \mathcal{D}(\mathcal{H}_S) : \sigma_S = U_S(g)\sigma_S U_S(g)^\dagger \ \forall g \in G\right\}, \tag{4.55}$$

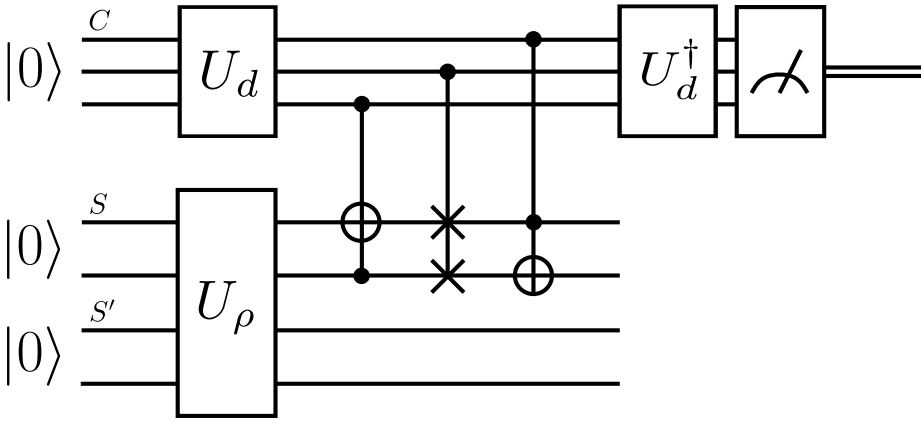


Figure 4.3: Quantum circuit implementing Algorithm 4.1 to test G-Bose symmetry for D_3. Compared to Figure 4.1, the systems S and S' are two qubits each, C consists of three qubits, and $|+\rangle_C$ is defined as $U_d|000\rangle$.

and $\mathcal{D}(\mathcal{H}_S)$ denotes the set of density operators acting on the Hilbert space $\mathcal{H}_S$. Thus, Algorithm 4.2 gives an operational meaning to the maximum G-symmetric fidelity in terms of its acceptance probability, and it can be used to estimate this fundamental measure of symmetry.

In the modified approach, we suppose that the quantum computer (now called the verifier) is equipped with access to a "quantum prover"—an agent who can perform arbitrarily powerful quantum computations. We suppose that the quantum computer is allowed to exchange two quantum messages with the prover. The resulting class of problems that can be solved using this approach is abbreviated QIP(2), for quantum interactive proofs with two quantum messages exchanged [Wat09b, VW16], and we note here that computational problems related to entanglement of bipartite states [HMW14] and recoverability of tripartite states [CHM+16] were previously shown to be decidable in QIP(2). These latter problems were proven to be QSZK-hard, and it remains an open question to determine their precise computational complexity.

Let $|\psi\rangle_{S'S}$ be a purification of the state ρ_S, and suppose that the verifier has access to a circuit U^ρ that prepares this purification of ρ_S.

Figure 4.4 depicts this quantum algorithm. The overall state after Step 3 of Algorithm 4.2 is

$$V_{S'E\to\hat{S}E'}|\psi\rangle_{S'S}|0\rangle_E. \tag{4.57}$$

Algorithm 4.2 G-symmetry test schematic.

Input: Quantum circuit U^ρ that prepares a purification of state ρ, and unitary representation of group G, $\{U(g)\}_{g\in G}$.

Output: Estimate of $\max_{\sigma\in \mathrm{Sym}_G} F(\rho,\sigma)$.

1: The verifier uses the circuit U^ρ to prepare the state $|\psi\rangle_{S'S}$.
2: The verifier transmits the purifying system S' to the prover.
3: The prover appends an ancillary register E in the state $|0\rangle_E$ and performs a unitary $V_{S'E\to\hat{S}E'}$.
4: The prover sends the system $\hat{S}$ back to the verifier.
5: The verifier prepares a register C in the state $|0\rangle_C$.
6: The verifier acts on register C with a quantum Fourier transform.
7: The verifier performs the following controlled unitary:

$$\sum_{g\in G} |g\rangle\langle g|_C \otimes U_S(g) \otimes \overline{U}_{\hat{S}}(g). \tag{4.56}$$

8: The verifier performs an inverse quantum Fourier transform on register C, measures in the basis $\{|g\rangle\langle g|_C\}_{g\in G}$, and accepts if and only if the zero outcome $|0\rangle\langle 0|_C$ occurs.

The result of Step 6 is to prepare the uniform superposition state $|+\rangle_C$, which is defined in (4.40). After Step 7, the overall state is

$$\frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle_C \left(U_S(g)\otimes \overline{U}_{\hat{S}}(g)\right) V_{S'E\to\hat{S}E'}|\psi\rangle_{S'S}|0\rangle_E. \tag{4.58}$$

For a fixed unitary $V_{S'E\to\hat{S}E'}$, the probability of accepting, by following the same reasoning in (4.42)–(4.43), is equal to

$$\left\|\Pi^G_{S\hat{S}} V_{S'E\to\hat{S}E'}|\psi\rangle_{S'S}|0\rangle_E\right\|_2^2, \tag{4.59}$$

where

$$\Pi^G_{S\hat{S}} := \frac{1}{|G|}\sum_{g\in G} U_S(g)\otimes \overline{U}_{\hat{S}}(g). \tag{4.60}$$

Since the goal of the prover in a quantum interactive proof is to convince the verifier to accept [Wat09b, VW16], the prover optimizes over every unitary $V_{S'E\to\hat{S}E'}$ and the acceptance probability of Algorithm 4.2 is given by

$$\max_{V_{S'E\to\hat{S}E'}} \left\|\Pi^G_{S\hat{S}} V_{S'E\to\hat{S}E'}|\psi\rangle_{S'S}|0\rangle_E\right\|_2^2. \tag{4.61}$$

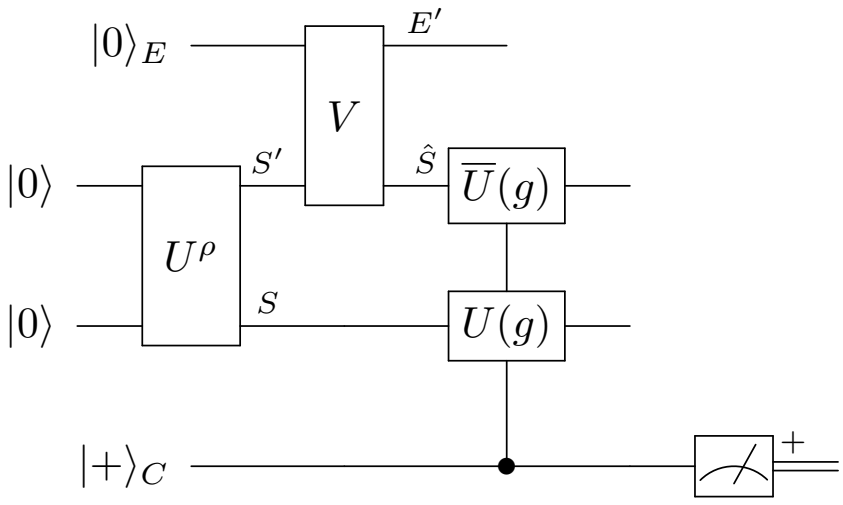


Figure 4.4: Quantum circuit to implement Algorithm 4.2. The unitary U^ρ prepares a purification $\psi_{S'S}$ of the state ρ_S. Algorithm 4.2 tests whether the state ρ_S is G-symmetric, as defined in Definition 4.1. Its acceptance probability is equal to the maximum G-symmetric fidelity, as defined in (4.54).

The main idea behind Algorithm 4.2 is that if the state ρ_S possesses the symmetry in (4.53), then Theorem 4.1 (with trivial reference system R) guarantees the existence of a purification $\phi_{S\hat{S}}$ of ρ_S such that

$$|\phi\rangle_{S\hat{S}} = \Pi^G_{S\hat{S}}|\phi\rangle_{S\hat{S}}. \tag{4.62}$$

Since all purifications of a quantum state are related by a unitary acting on the purifying system (see, e.g., [Wil17]), the prover is able to apply a unitary taking the purification $|\psi\rangle_{S'S}$ to the purification $|\phi\rangle_{S\hat{S}}$. After the prover sends back the system $\hat{S}$, the verifier then performs a quantum-computational test to determine if the condition in (4.62) holds. A discussion on how to choose the size of register E can be found in Section 4.5.

We now formally state the claim made just after (4.53). See Appendix C.3 for a proof of Theorem 4.3.

Theorem 4.3. *The acceptance probability of Algorithm 4.2 is equal to the maximum G-*

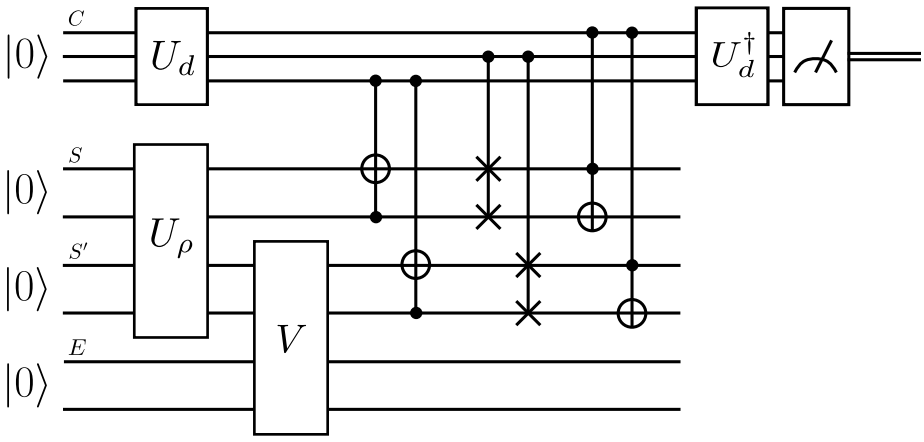


Figure 4.5: Quantum circuit implementing Algorithm 4.2 to test G-symmetry in the case that the group G is the triangular dihedral group. Compared to Figure 4.4, the systems S and S' are two qubits each, C consists of three qubits, and $|+\rangle_C$ is defined as $U_d|000\rangle$. Both the SWAP and CNOT gates have no imaginary entries, and thus they are equal to their own complex conjugates.

symmetric fidelity in (4.54)*, i.e.,*

$$\max_{V_{S'E\to\hat{S}E'}} \left\| \Pi^G_{S\hat{S}} V_{S'E\to\hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2 = \max_{\sigma_S \in \mathrm{Sym}_G} F(\rho_S, \sigma_S). \tag{4.63}$$

Example 4.4. *For the triangular dihedral group example (see Example 4.3), we use the same unitary U_d as in* (4.52) *to prepare the superposition $|+\rangle_C$ and the same mapping of control states to group elements. The circuit to test for G-symmetry is shown in Figure 4.5.*

Remark 4.1 [*Testing incoherence*]. *We note here that testing the incoherence of a quantum state, in the sense of* [BCP14, SAP17]*, is a special case of testing G-symmetry. To see this, we can pick G to be the cyclic group over d elements with unitary representation $\{Z(z)\}_z$, where $Z(z)$ is the generalized Pauli phase-shift unitary, defined as*

$$Z(z) := \sum_{j=0}^{d-1} e^{2\pi i jz/d} |j\rangle\langle j|. \tag{4.64}$$

A state is symmetric with respect to this group if the condition in (4.53) *holds. This condition is equivalent to the following one:*

$$\rho_S = \frac{1}{|G|} \sum_{g\in G} U_S(g) \rho_S U_S(g)^\dagger. \tag{4.65}$$

For the choice mentioned above, the condition in (4.65) holds if and only if the state ρ_S is diagonal in the incoherent basis, i.e., if it can be written as $\rho_S = \sum_j p(j)|j\rangle\langle j|$, where $p(j)$ is a probability distribution. Thus, Algorithm 4.2 can be used to test the incoherence of quantum states.

4.2.3 Testing G-Bose symmetric extendibility

We now describe an algorithm for testing G-Bose symmetric extendibility of a quantum state ρ_S, as defined in Definition 4.4. The algorithm bears some similarities with Algorithms 4.1 and 4.2. Like Algorithm 4.2, it involves an interaction between a verifier and a prover. We prove that its acceptance probability is equal to the maximum G-BSE fidelity:

$$\max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S), \tag{4.66}$$

where BSE_G is the set of G-Bose symmetric extendible states:

$$\mathrm{BSE}_G := \left\{ \begin{array}{c} \sigma_S : \exists\, \omega_{RS} \in \mathcal{D}(\mathcal{H}_{RS}), \mathrm{Tr}_R[\omega_{RS}] = \sigma_S, \\ \omega_{RS} = U_{RS}(g)\omega_{RS},\ \forall g \in G \end{array} \right\}. \tag{4.67}$$

Thus, the algorithm endows the maximum G-BSE fidelity with an operational meaning. Note that the condition $\omega_{RS} = U_{RS}(g)\omega_{RS}$ for all $g \in G$ is equivalent to

$$\omega_{RS} = \Pi^G_{RS}\omega_{RS}\Pi^G_{RS}, \tag{4.68}$$

where

$$\Pi^G_{RS} := \frac{1}{|G|}\sum_{g\in G} U_{RS}(g). \tag{4.69}$$

The algorithm is similar to Algorithm 4.2, but we list it here for completeness. Let $|\psi\rangle_{S'S}$ be a purification of the state ρ_S, and suppose that the circuit U^ρ prepares this purification of ρ_S.

Figure 4.6 depicts this quantum algorithm. The overall state after Step 3 is

$$V_{S'E\to RE'}|\psi\rangle_{S'S}|0\rangle_E. \tag{4.71}$$

Step 6 prepares the uniform superposition state $|+\rangle_C$, which is defined in (4.40). After Step 7, the overall state is

$$\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle_C U_{RS}(g)V_{S'E\to RE'}|\psi\rangle_{S'S}|0\rangle_E. \tag{4.72}$$

Algorithm 4.3 G-BSE test schematic.

Input: Quantum circuit U^ρ that prepares a purification of state ρ, and unitary representation of group G, $\{U(g)\}_{g\in G}$.

Output: Estimate of $\max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S)$.

1: The verifier uses the circuit provided to prepare the state $|\psi\rangle_{S'S}$.
2: The verifier transmits the purifying system S' to the prover.
3: The prover appends an ancillary register E in the state $|0\rangle_E$ and performs a unitary $V_{S'E\to RE'}$.
4: The prover sends the system R back to the verifier.
5: The verifier prepares a register C in the state $|0\rangle_C$.
6: The verifier acts on register C with a quantum Fourier transform.
7: The verifier performs the following controlled unitary:

$$\sum_{g\in G} |g\rangle\langle g|_C \otimes U_{RS}(g), \tag{4.70}$$

8: The verifier performs an inverse quantum Fourier transform on register C, measures in the basis $\{|g\rangle\langle g|_C\}_{g\in G}$, and accepts if and only if the zero outcome $|0\rangle\langle 0|_C$ occurs.

The last step can be understood as the verifier projecting the register C onto the state $|+\rangle_C$.

The probability of accepting, following the same reasoning as before, is equal to

$$\left\|\Pi^G_{RS} V_{S'E\to RE'}|\psi\rangle_{S'S}|0\rangle_E\right\|_2^2, \tag{4.73}$$

where Π^G_{RS} is defined in (4.69). As before, the goal of the prover in a quantum interactive proof is to convince the verifier to accept [Wat09b, VW16], and so the prover optimizes over every unitary $V_{S'E\to\hat{S}E'}$. The acceptance probability of Algorithm 4.3 is then given by

$$\max_{V_{S'E\to RE'}} \left\|\Pi^G_{RS} V_{S'E\to RE'}|\psi\rangle_{S'S}|0\rangle_E\right\|_2^2. \tag{4.74}$$

Our proof of the following theorem is similar to the proof given for Theorem 4.3; for completeness, we provide a proof in Appendix C.4.

Theorem 4.4. *The maximum acceptance probability of Algorithm 4.3 is equal to the*

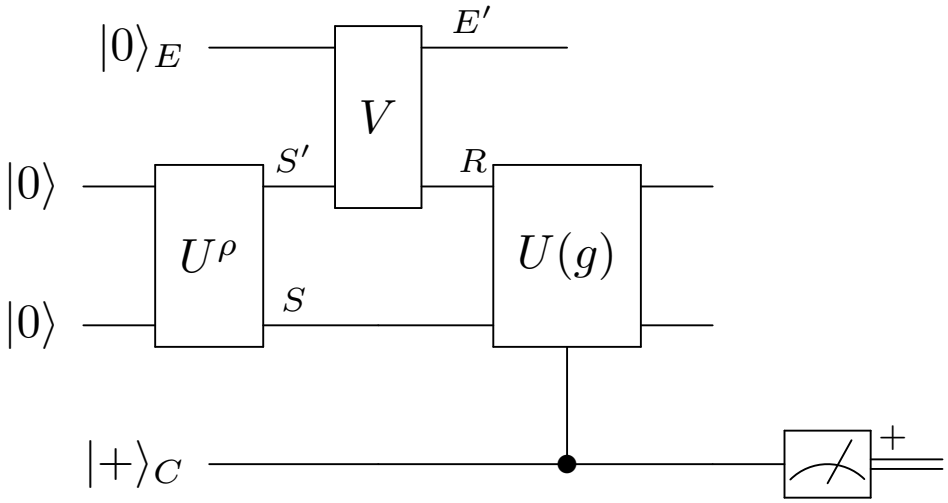


Figure 4.6: Quantum circuit to implement Algorithm 4.3. The unitary U^ρ prepares a purification $\psi_{S'S}$ of the state ρ_S. Algorithm 4.3 tests whether the state ρ_S is G-Bose symmetric extendible, as defined in Definition 4.4. Its acceptance probability is equal to the maximum G-BSE fidelity, as defined in (4.66).

maximum G-BSE fidelity in (4.66)*, i.e.,*

$$\max_{V_{S'E\to RE'}} \left\| \Pi^G_{RS} V_{S'E\to RE'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2 = \max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S), \tag{4.75}$$

where the set BSE_G *is defined in* (4.67)*.*

Example 4.5. *For the triangular dihedral group example (see Example 4.3), we use the same unitary U_d to prepare the superposition $|+\rangle_C$ and the same mapping of control states to group elements. The circuit to test for G-Bose symmetric extendibility is shown in Figure 4.7.*

4.2.4 Testing G-symmetric extendibility

The final algorithm that we introduce tests whether a state ρ_S is G-symmetric extendible (recall Definition 4.3). Similar to the algorithms in the previous sections,

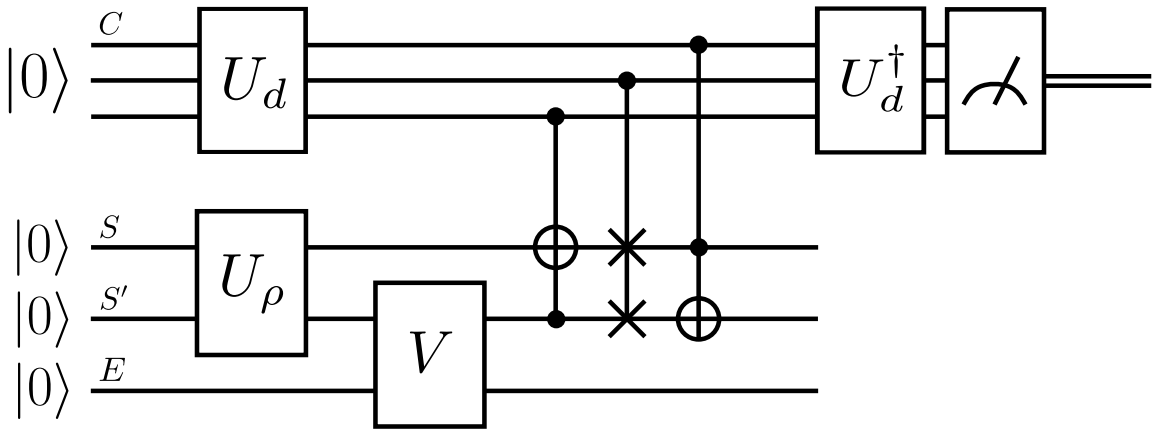


Figure 4.7: Quantum circuit implementing Algorithm 4.3 to test G-Bose symmetric extendibility for the triangular dihedral group. Compared to Figure 4.6, the systems S and S' are one qubit each, C consists of three qubits, and $|+\rangle_C$ is defined as $U_d|000\rangle$.

not only does it decide whether ρ_S is G-symmetric extendible, but it also quantifies how similar it is to a state in the set of G-symmetric extendible states. The acceptance probability is equal to the *maximum G-symmetric extendible fidelity*:

$$\max_{\sigma_S \in \text{SymExt}_G} F(\rho_S, \sigma_S), \tag{4.76}$$

where

$$\text{SymExt}_G := \left\{ \begin{array}{c} \sigma_S : \exists\, \omega_{RS} \in \mathcal{D}(\mathcal{H}_{RS}), \text{Tr}_R[\omega_{RS}] = \sigma_S, \\ \omega_{RS} = U_{RS}(g)\omega_{RS}U_{RS}(g)^\dagger \;\forall g \in G \end{array} \right\}. \tag{4.77}$$

We again operate in the model of quantum interactive proofs, in which a verifier interacts with a prover.

We list the algorithm below for completeness, noting its similarity to the previous algorithms. Let $|\psi\rangle_{S'S}$ be a purification of the state ρ_S, and suppose that the circuit U^ρ prepares this purification of ρ_S.

Figure 4.8 depicts this quantum algorithm. After Step 3, the overall state is

$$V_{S'E\to R\hat{R}\hat{S}E'}|\psi\rangle_{S'S}|0\rangle_E. \tag{4.79}$$

Step 5 prepares the uniform superposition state $|+\rangle_C$, which is defined in (4.40).

Algorithm 4.4 G-SE test schematic.

Input: Quantum circuit U^ρ that prepares a purification of state ρ, and unitary representation of group G, $\{U(g)\}_{g\in G}$.

Output: Estimate of $\max_{\sigma_S \in \mathrm{SymExt}_G} F(\rho_S, \sigma_S)$.

1: The verifier uses the circuit U^ρ to prepare the state $|\psi\rangle_{S'S}$, which is a purification of the state ρ_S.
2: The verifier transmits the purifying system S' to the prover.
3: The prover appends an ancillary register E in the state $|0\rangle_E$ and performs a unitary $V_{S'E\to R\hat{R}\hat{S}E'}$.
4: The prover sends the systems $R\hat{R}\hat{S}$ back to the verifier.
5: The verifier prepares a register C in the state $|0\rangle_C$.
6: The verifier acts on register C with a quantum Fourier transform.
7: The verifier performs the following controlled unitary:

$$\sum_{g\in G} |g\rangle\langle g|_C \otimes U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g), \tag{4.78}$$

8: The verifier performs an inverse quantum Fourier transform on register C, measures in the basis $\{|g\rangle\langle g|_C\}_{g\in G}$, and accepts if and only if the zero outcome $|0\rangle\langle 0|_C$ occurs.

After Step 7, the overall state is

$$\frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle_C \left(U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g)\right) V|\psi\rangle_{S'S}|0\rangle_E, \tag{4.80}$$

where $V \equiv V_{S'E\to R\hat{R}\hat{S}E'}$. The last step can be understood as the verifier projecting the register C onto the state $|+\rangle_C$.

The probability of accepting is equal to

$$\left\| \Pi^G_{RS\hat{R}\hat{S}} V_{S'E\to R\hat{R}\hat{S}E'} |\psi\rangle_{S'S}|0\rangle_E \right\|_2^2, \tag{4.81}$$

where $\Pi^G_{RS\hat{R}\hat{S}}$ is defined in (4.22). As before, the prover optimizes over every unitary $V_{S'E\to R\hat{R}\hat{S}E'}$. The acceptance probability of Algorithm 4.4 is then given by

$$\left\| \Pi^G_{RS\hat{R}\hat{S}} V_{S'E\to R\hat{R}\hat{S}E'} |\psi\rangle_{S'S}|0\rangle_E \right\|_2^2. \tag{4.82}$$

Our proof of the following theorem is similar to the proof given for Theorem 4.3. For completeness, we provide our proof in Appendix C.5.

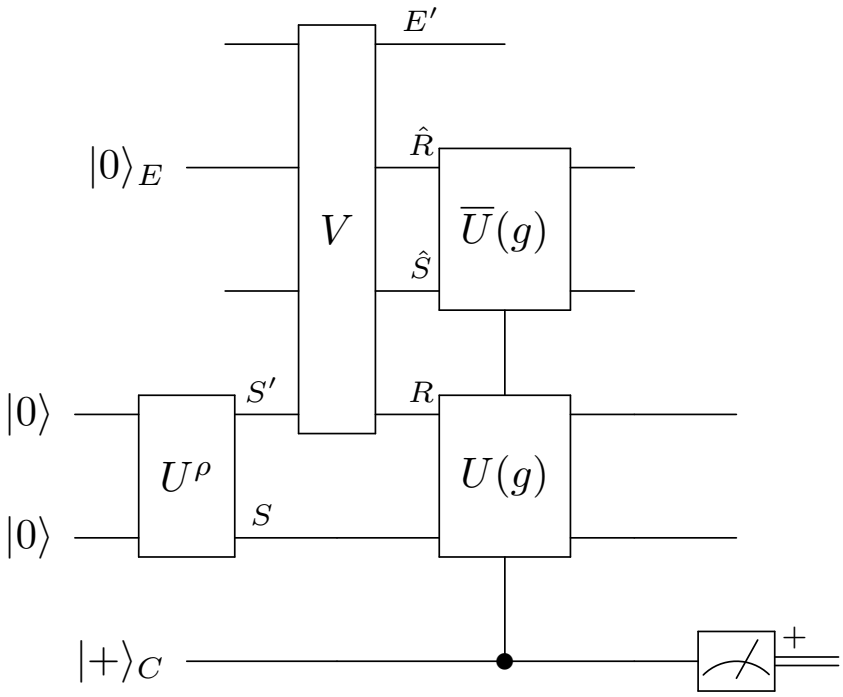


Figure 4.8: Quantum circuit to implement Algorithm 4.4. The unitary U^ρ prepares a purification $\psi_{S'S}$ of the state ρ_S. Algorithm 4.4 tests whether the state ρ_S is G-symmetric extendible, as defined in Definition 4.3. Its acceptance probability is equal to the maximum G-symmetric extendible fidelity, as defined in (4.76).

Theorem 4.5. *The maximum acceptance probability of Algorithm 4.4 is equal to the maximum G-symmetric extendible fidelity in* (4.76)*, i.e.,*

$$\max_{V_{S'E\to R\hat{R}\hat{S}E'}} \left\| \Pi^G_{RS\hat{R}\hat{S}} V_{S'E\to R\hat{R}\hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2 = \max_{\sigma_S \in \mathrm{SymExt}_G} F(\rho_S, \sigma_S), \tag{4.83}$$

where the set SymExt_G *is defined in* (4.77).

Example 4.6. *For the triangular dihedral group example (see Example 4.3), we use the same unitary U_d to prepare the superposition $|+\rangle_C$ and the same mapping of control states to group elements. The circuit to test for G-symmetric extendibility is shown in Figure 4.9.*

Remark 4.2 [*Extensions to compact groups*]. *Throughout our paper we have focused on*

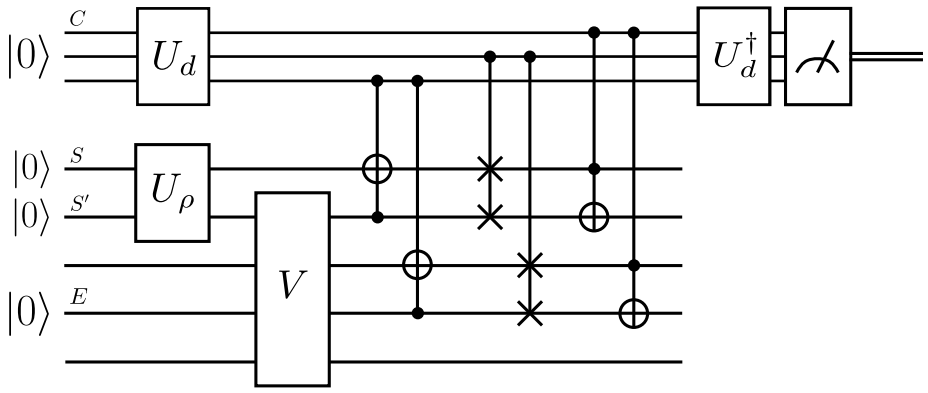


Figure 4.9: Quantum circuit implementing Algorithm 4.4 to test G-symmetric extendibility in the case that the group G is the triangular dihedral group. Compared to Figure 4.8, the systems S and S' are one qubit each, C consists of three qubits, and $|+\rangle_C$ is defined as $U_d|000\rangle$. Both the SWAP and CNOT gates have no imaginary entries and thus are equal to their own complex conjugates.

discrete, finite groups; however, these notions of symmetry and the algorithms presented above in principle may be extended to continuous groups as well, permitting certain conditions hold. We leave a detailed investigation of this topic for future work and only discuss this extension briefly here. In particular, our algorithms can be generalized to any compact Lie group represented on a finite-dimensional quantum system. The primary limitation in cases of compact groups is realizing the following projection [Har13]

$$\Pi^G := \int_{g\in G} d\mu(g)\; U(g)\,, \tag{4.84}$$

where $U(g)$ is the unitary representation of g and $\mu(g)$ is the Haar measure for the group. It follows from Caratheodory's theorem that there exists a probability mass function $\{p(g)\}_{g\in G'}$, where G' is a finite set, such that the following equality holds:

$$\Pi^G = \sum_{g\in G'} p(g)U(g). \tag{4.85}$$

As such, since our algorithms ultimately realize this projection for the case in which $p(g)$ is uniform, they can be generalized in the following way. For concreteness, we consider the following generalization of Algorithm 4.1, but we note that our other algorithms can be generalized similarly:

1. *Prepare an ancillary register C in the state*

$$|\varphi_p\rangle_C := \sum_{g\in G'} \sqrt{p(g)}|g\rangle. \tag{4.86}$$

2. *Append the state $|\psi\rangle_S$ and perform the following controlled unitary:*

$$\sum_{g\in G'} |g\rangle\langle g|_C \otimes U_S(g). \tag{4.87}$$

3. *Perform the measurement $\{|\varphi_p\rangle\langle\varphi_p|_C, \mathbb{I}_C - |\varphi_p\rangle\langle\varphi_p|_C\}$ on the register C, and accept if and only if the outcome $|\varphi_p\rangle\langle\varphi_p|_C$ occurs.*

Following similar calculations given in (4.40)–(4.44)*, we conclude that the acceptance probability of this algorithm is equal to* $\mathrm{Tr}[\Pi^G|\psi\rangle\langle\psi|_S]$.

Although this abstract presentation of the generalized algorithm seems straightforward, there are some key questions to address before realizing it in practice. What is the probability mass function $\{p(g)\}_{g\in G'}$ that results from applying Caratheodory's theorem? This theorem only guarantees the existence of such a probability mass function, but it does not construct it. Once the probability mass function is known, is the state $|\varphi_p\rangle_C$ efficiently preparable? Addressing these two questions would lead to an efficient algorithm for estimating $\mathrm{Tr}[\Pi^G|\psi\rangle\langle\psi|_S]$.

When the group representation permits a t-design [RS09]*, then it is straightforward to realize the algorithm, and we consider some examples in Sections 4.5.3 and 4.5.4. In general, addressing these questions may not be trivial; the topic of t-designs is addressed in a large body of work* [Sco08, RS09, GAE07] *beyond the scope considered here.*

4.3 Tests of k-extendibility of states

The theory developed in Section 4.2 is rather general. In the forthcoming subsections, we apply it to test for extendibility of bipartite and multipartite quantum states and to test for covariance symmetry of quantum channels and measurements. Later on in Section 4.5, we consider many other example of groups and symmetry tests and simulate the performance of Algorithms 4.1–4.4.

4.3.1 Separability test for pure bipartite states

We illustrate the G-Bose symmetry test from Section 4.2.1 on a case of interest: deciding whether a pure bipartite state is entangled. This problem is known to be BQP-complete [GHMW15], and one can decide it by means of the SWAP test as considered in [HM10]. The SWAP test as a quantum computational method of quantifying entanglement has been further studied in recent work [FKS21, BGCC21].

Let ψ_{AB} be a pure bipartite state, and let $\psi_{AB}^{\otimes k}$ denote k copies of it. Then we can consider the permutation unitaries $W_{B_1 \cdots B_k}(\pi)$ from Example 4.1. This example is a special case of G-Bose symmetry with the identifications

$$S \leftrightarrow A_1 B_1 \cdots A_k B_k, \tag{4.88}$$

$$U_S(g) \leftrightarrow \mathbb{I}_{A_1 \cdots A_k} \otimes W_{B_1 \cdots B_k}(\pi). \tag{4.89}$$

The acceptance probability of Algorithm 4.1 is equal to

$$\operatorname{Tr}[\Pi^{\mathrm{Sym}}_{B_1 \cdots B_k} \rho_B^{\otimes k}], \tag{4.90}$$

where the projection $\Pi^{\mathrm{Sym}}_{B_1 \cdots B_k}$ onto the symmetric subspace is defined in (4.19) and $\rho_B \coloneqq \operatorname{Tr}_A[\psi_{AB}]$. We note that there is an efficient quantum algorithm to implement this test [BBD+97, Section 4], which amounts to an instance of the abstract formulation in Algorithm 4.1. For $k = 2$, this reduces to the well-known SWAP test with acceptance probability

$$p_{\mathrm{acc}}^{(2)} \coloneqq \frac{1}{2}\left(1 + \operatorname{Tr}[\rho_B^2]\right). \tag{4.91}$$

For $k = 3$, the acceptance probability is

$$p_{\mathrm{acc}}^{(3)} \coloneqq \frac{1}{6}\left(1 + 3\operatorname{Tr}[\rho_B^2] + 2\operatorname{Tr}[\rho_B^3]\right). \tag{4.92}$$

For $k = 4$, the acceptance probability is

$$p_{\mathrm{acc}}^{(4)} \coloneqq \frac{1}{24}\left(1 + 6\operatorname{Tr}[\rho_B^2] + 3\left(\operatorname{Tr}[\rho_B^2]\right)^2 + 8\operatorname{Tr}[\rho_B^3] + 6\operatorname{Tr}[\rho_B^4]\right). \tag{4.93}$$

We conclude that

$$p_{\mathrm{acc}}^{(2)} \geq p_{\mathrm{acc}}^{(3)} \geq p_{\mathrm{acc}}^{(4)}, \tag{4.94}$$

because $\mathrm{Tr}[\rho^k] = \sum_j \lambda_j^k$, where the eigenvalues of ρ are $\{\lambda_j\}_j$, and for all $x, y \in [0,1]$,

$$\begin{aligned} &\frac{1}{2}\left(x + x^2\right) \\ &\geq \frac{1}{6}\left(x + 3x^2 + 2x^3\right) \qquad (4.95) \\ &\geq \frac{1}{24}\left(x + 6x^2 + 3x^2 y + 8x^3 + 6x^4\right). \qquad (4.96) \end{aligned}$$

The inequalities in (4.94) imply that the tests become more difficult to pass as k increases. In a previous version of our paper [LW21], we speculated that this trend of decreasing acceptance probability continues as k increases. Indeed, this was subsequently shown to be true in [BLW23].

We can interpret these findings in two different ways. For each k, the rejection probability $1 - p_{\mathrm{acc}}^{(k)}$ can be understood as an entanglement measure for pure states, similar to how the linear entropy $1 - \mathrm{Tr}[\rho_B^2]$ is interpreted as an entanglement measure [HHHH09]. Indeed, these quantities are non-increasing under local operations and classical communication that take pure states to pure states, as every Rényi entropy (defined as $\frac{1}{1-\alpha} \log \mathrm{Tr}[\rho_B^\alpha]$ for $\alpha \in (0,1) \cup (1,\infty)$) is an entanglement measure for pure states. Another interpretation is that, if using these tests to decide if a given pure state is product or entangled, a decision can be determined with fewer repetitions of the basic test by using tests with higher values of k.

4.3.2 Separability test for pure multipartite states

We can generalize the test from the previous section to one for pure multipartite entanglement. Let $\psi_{A_1 \cdots A_m}$ be a multipartite pure state, and let $\psi_{A_1 \cdots A_m}^{\otimes k}$ denote k copies of it. For $i \in \{1, \ldots, m\}$ and $\pi_i \in S_k$, let $W_{A_{i,1} \cdots A_{i,k}}(\pi_i)$ denote a permutation unitary, where i is an index for the ith party, and the notation $A_{i,j}$ for $j \in \{1, \ldots, k\}$ indicates the jth system of the ith party. This example is a special case of G-Bose

symmetry with the identifications:

$$S \leftrightarrow A_{1,1} \cdots A_{1,k} \cdots A_{m,1} \cdots A_{m,k}, \tag{4.97}$$

$$U_S(g) \leftrightarrow \bigotimes_{i=1}^{m} W_{A_{i,1}\cdots A_{i,k}}(\pi_i), \tag{4.98}$$

$$G \leftrightarrow \overbrace{S_k \times \cdots \times S_k}^{m \text{ times}}, \tag{4.99}$$

$$g \leftrightarrow (\pi_1, \ldots, \pi_m), \tag{4.100}$$

where $\times$ denotes the direct product of groups. The G-Bose symmetry test from Section 4.2.1 has the following acceptance probability in this case:

$$\mathrm{Tr}\left[\bigotimes_{i=1}^{m} \Pi^{\mathrm{Sym}}_{A_{i,1}\cdots A_{i,k}} \psi^{\otimes k}_{A_1 \cdots A_m}\right]. \tag{4.101}$$

Note that one can again use the circuit from [BBD+97, Section 4] to implement this test. For $k = 2$, this test is known to be a test of multipartite pure-state entanglement [HM10], which has been considered in more recent works [FKS21, BGCC21]. As far as we aware, the test proposed above, for larger values of k, has not been considered previously. Presumably, as was the case for the bipartite entanglement test mentioned above, the multipartite test is such that it becomes easier to detect an entangled state as k increases. We leave its detailed analysis for future work.

4.3.3 k-Bose extendibility test for bipartite states

We now demonstrate how the test for G-Bose symmetric extendibility from Section 4.2.3 can realize a test for k-Bose extendibility of a bipartite state. Since every separable state is k-Bose extendible, this test is then indirectly a test for separability. To see this in detail, recall that a bipartite state σ_{AB} is separable if it can be written as a convex combination of pure product states [HHHH09, KW20]:

$$\sigma_{AB} = \sum_x p_X(x) \psi^x_A \otimes \phi^x_B, \tag{4.102}$$

where p_X is a probability distribution and $\{\psi^x_A\}_x$ and $\{\phi^x_B\}_x$ are sets of pure states. A k-Bose extension for this state is as follows:

$$\omega_{AB_1\cdots B_k} = \sum_x p_X(x) \psi^x_A \otimes \phi^x_{B_1} \otimes \cdots \otimes \phi^x_{B_k}. \tag{4.103}$$

By making the identifications discussed in Example 4.2, it follows from Theorem 4.4 that the test from Section 4.2.3 is a test for k-Bose extendibility. For an input state ρ_{AB}, the acceptance probability of Algorithm 4.3 is equal to the maximum k-Bose extendible fidelity

$$\max_{\omega_{AB} \in k\text{-BE}} F(\rho_{AB}, \omega_{AB}), \tag{4.104}$$

where k-BE denotes the set of k-Bose extendible states, as defined in Example 4.2.

This test for k-Bose extendibility was proposed in [HMW14] for understanding the computational complexity of the circuit separability problem. In that work, it was not mentioned that the test employed is a test for k-Bose extendibility; instead, it was suggested to be a test for k-extendibility. Thus, our observation here (also made earlier by [Mar13]) is that the test proposed in [HMW14] is actually a test for k-Bose extendibility, and we consider in the next section a true test for k-extendibility. The main results of [HMW14] were the computational complexity of the circuit version of the separability problem, and so the precise kind of test used was not particularly important there.

4.3.4 k-Extendibility test for bipartite states

In this section, we discuss how the test for G-symmetric extendibility from Section 4.2.4 can realize a test for k-extendibility of a bipartite state. Due to the known connections between k-extendibility and separability [CKMR07, BCY11a, BCY11b, BH13], this test is an indirect test for separability of a bipartite state. Since every separable state is k-Bose extendible, as discussed in Section 4.3.3, and every k-Bose extendible state is k-extendible, it follows that every separable state is k-extendible.

By making the identifications discussed in Example 4.1, it follows from Theorem 4.5 that the test from Section 4.2.4 is a test for k-extendibility. For an input state ρ_{AB}, the acceptance probability of Algorithm 4.4 is equal to the maximum k-extendible fidelity

$$\max_{\omega_{AB} \in k\text{-E}} F(\rho_{AB}, \omega_{AB}), \tag{4.105}$$

where k-E denotes the set of k-extendible states, as defined in Example 4.1.

As far as we are aware, this quantum computational test for k-extendibility is original to this paper, however inspired by the approach from [HMW14]. It was

argued in [HMW14] that the acceptance probability of the test there is bounded from above by the maximum k-extendible fidelity, which is consistent with the fact that the set of k-Bose extendible states is contained in the set of k-extendible states and our observation here that the acceptance probability of the test in [HMW14] is equal to the maximum k-Bose extendible fidelity.

4.3.5 Extendibility tests for multipartite states

We discuss briefly how the tests from Sections 4.2.3 and 4.2.4 apply to the multipartite case, using identifications similar to those in (4.97)–(4.100).

First, let us recall the definition of multipartite extendibility [DPS05]. Let $\sigma_{A_1 \cdots A_m}$ be a multipartite state. Such a state is $(k_1, \ldots, k_m)$-extendible if there exists a state $\omega_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}}$ such that

$$\sigma_{A_1 \cdots A_m} = \operatorname{Tr}_{A_{1,2} \cdots A_{1,k_1} \cdots A_{m,2} \cdots A_{m,k_m}} [\omega_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}}] \tag{4.106}$$

and

$$\omega_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}} = W^{\pi}_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}} \omega_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}} \times (W^{\pi}_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}})^{\dagger}, \tag{4.107}$$

for all π, where $\pi = (\pi_1, \ldots, \pi_m) \in S_{k_1} \times \cdots \times S_{k_m}$ and

$$W^{\pi}_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}} := \bigotimes_{i=1}^{m} W^{\pi_i}_{A_{i,1} \cdots A_{i,k_i}}. \tag{4.108}$$

A multipartite state is $(k_1, \ldots, k_m)$-Bose extendible if there exists a state $\omega_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}}$ such that (4.106) holds and

$$\omega_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}} = \Pi_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}} \omega_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}} \Pi_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}}, \tag{4.109}$$

where

$$\Pi_{A_{1,1} \cdots A_{1,k_1} \cdots A_{m,1} \cdots A_{m,k_m}} := \bigotimes_{i=1}^{m} \Pi^{\mathrm{Sym}}_{A_{i,1} \cdots A_{i,k_i}}, \tag{4.110}$$

$$\Pi^{\mathrm{Sym}}_{A_{i,1} \cdots A_{i,k_i}} := \frac{1}{k_i!} \sum_{\pi_i \in S_{k_i}} W^{\pi_i}_{A_{i,1} \cdots A_{i,k_i}}. \tag{4.111}$$

By making the identifications

$$S \leftrightarrow A_{1,1} \cdots A_{m,1}, \tag{4.112}$$

$$R \leftrightarrow A_{1,2} \cdots A_{1,k_1} \cdots A_{m,2} \cdots A_{m,k_m}, \tag{4.113}$$

$$U_{RS}(g) \leftrightarrow \bigotimes_{i=1}^{m} W_{A_{i,1} \cdots A_{i,k_i}}(\pi_i), \tag{4.114}$$

$$G \leftrightarrow S_{k_1} \times \cdots \times S_{k_m}, \tag{4.115}$$

$$g \leftrightarrow (\pi_1, \ldots, \pi_m), \tag{4.116}$$

it follows that Algorithm 4.3 is a test for multipartite $(k_1, \ldots, k_m)$-Bose extendibility of a state $\rho_{A_1 \cdots A_m}$, with acceptance probability equal to

$$\max_{\omega_{A_1 \cdots A_m} \in (k_1, \ldots, k_m)\text{-BE}} F(\rho_{A_1 \cdots A_m}, \omega_{A_1 \cdots A_m}), \tag{4.117}$$

and Algorithm 4.4 is a test for multipartite $(k_1, \ldots, k_m)$-extendibility of a state $\rho_{A_1 \cdots A_m}$, with acceptance probability equal to

$$\max_{\omega_{A_1 \cdots A_m} \in (k_1, \ldots, k_m)\text{-E}} F(\rho_{A_1 \cdots A_m}, \omega_{A_1 \cdots A_m}), \tag{4.118}$$

where $(k_1, \ldots, k_m)$-BE and $(k_1, \ldots, k_m)$-E denote the sets of $(k_1, \ldots, k_m)$-Bose extendible and $(k_1, \ldots, k_m)$-extendible states, respectively.

4.4 Semi-definite programs for maximum symmetric fidelities

In this section, we note that the acceptance probabilities of Algorithms 4.1–4.4 can be computed by means of semi-definite programming (see [BV04, Wat18, KW20] for reviews). This is useful for comparing the true values of the acceptance probabilities of Algorithms 4.1–4.4 to estimates formed from executing them on near-term quantum computers; however, this semi-definite programming approach only works well in practice if the circuit U^ρ acts on a small number of qubits. This limitation holds because the semi-definite programs (SDPs) run in a time polynomial in the dimension of the states involved, but the dimension of a state grows exponentially with the number of qubits involved.

We note that the fact that the acceptance probabilities of Algorithms 4.1–4.4 can be computed by semi-definite programming follows from a more general fact that

the acceptance probability of a QIP(2) algorithm can be computed in this manner [Wat09b, VW16]; however, it is helpful to have the explicit form of the SDPs available.

We now list the SDPs for the acceptance probabilities of Algorithms 4.1–4.4. To begin with, let us note that the acceptance probability of Algorithm 4.1 is equal to $\mathrm{Tr}[\Pi_S^G \rho_S]$, and so there is no need for an optimization. This quantity can be calculated directly if the projection matrix Π_S^G and the density matrix ρ_S are available. Alternatively, one could employ an optimization as given below. Let us first note that the root fidelity of states ω and τ can be calculated by the following SDP [Wat13]:

$$\sqrt{F}(\omega,\tau) = \max_{X \in \mathcal{L}(\mathcal{H})} \left\{ \mathrm{Tr}[\mathrm{Re}[X]] : \begin{bmatrix} \omega & X^\dagger \\ X & \tau \end{bmatrix} \geq 0 \right\}, \tag{4.119}$$

where $\mathcal{L}(\mathcal{H})$ is the space of linear operators acting on the Hilbert space $\mathcal{H}$. Each of the sets B-Sym_G, Sym_G, BSE_G, and SymExt_G are specified by semi-definite constraints. Thus, combining the optimization in (4.119) with various constraints, we find that the acceptance probabilities of Algorithms 4.1–4.4 can be calculated by using the following SDPs, respectively:

$$\max_{\sigma_S \in \text{B-Sym}_G} \sqrt{F}(\rho_S,\sigma_S) = \max_{\substack{X \in \mathcal{L}(\mathcal{H}_S), \\ \sigma_S \geq 0}} \left\{ \begin{array}{c} \mathrm{Tr}[\mathrm{Re}[X]] : \\ \begin{bmatrix} \rho_S & X^\dagger \\ X & \sigma_S \end{bmatrix} \geq 0, \\ \mathrm{Tr}[\sigma_S] = 1, \\ \sigma_S = \Pi_S^G \sigma_S \Pi_S^G \end{array} \right\}, \tag{4.120}$$

$$\max_{\sigma_S \in \mathrm{Sym}_G} \sqrt{F}(\rho_S,\sigma_S) = \max_{\substack{X \in \mathcal{L}(\mathcal{H}_S), \\ \sigma_S \geq 0}} \left\{ \begin{array}{c} \mathrm{Tr}[\mathrm{Re}[X]] : \\ \begin{bmatrix} \rho_S & X^\dagger \\ X & \sigma_S \end{bmatrix} \geq 0, \\ \mathrm{Tr}[\sigma_S] = 1, \\ \sigma_S = U_S(g) \sigma_S U_S(g)^\dagger \ \forall g \in G \end{array} \right\}, \tag{4.121}$$

$$\max_{\sigma_S \in \mathrm{BSE}_G} \sqrt{F}(\rho_S,\sigma_S) = \max_{\substack{X \in \mathcal{L}(\mathcal{H}_S), \\ \omega_{RS} \geq 0}} \left\{ \begin{array}{c} \mathrm{Tr}[\mathrm{Re}[X]] : \\ \begin{bmatrix} \rho_S & X^\dagger \\ X & \mathrm{Tr}_R[\omega_{RS}] \end{bmatrix} \geq 0, \\ \mathrm{Tr}[\omega_{RS}] = 1, \\ \omega_{RS} = \Pi_{RS}^G \omega_{RS} \Pi_{RS}^G \end{array} \right\}, \tag{4.122}$$

$$\max_{\sigma_S \in \mathrm{SymExt}_G} \sqrt{F}(\rho_S, \sigma_S) = \max_{\substack{X \in \mathcal{L}(\mathcal{H}_S), \\ \omega_{RS} \geq 0}} \left\{ \begin{array}{c} \mathrm{Tr}[\mathrm{Re}[X]] : \\ \begin{bmatrix} \rho_S & X^\dagger \\ X & \mathrm{Tr}_R[\omega_{RS}] \end{bmatrix} \geq 0, \\ \mathrm{Tr}[\omega_{RS}] = 1, \\ \omega_{RS} = U_{RS}(g) \omega_{RS} U_{RS}(g)^\dagger \ \forall g \in G \end{array} \right\}. \tag{4.123}$$

We note here that the complexity of the SDPs in (4.121) and (4.123) can be greatly simplified by employing basic concepts from representation theory (i.e., Schur's lemma). See [Ste12] for background on representation theory and Propositions 4.2.2 and 4.2.3 therein for Schur's lemma. Focusing on the SDP in (4.121), it is well known that there exists a unitary W that block diagonalizes every unitary in the set $\{U(g)\}_{g \in G}$, as follows:

$$U(g) = W \left(\bigoplus_\lambda \mathbb{I}_{m_\lambda} \otimes U_\lambda(g) \right) W^\dagger, \tag{4.124}$$

where the variable λ labels an irreducible representation (irrep) of $U(g)$, the matrix $\mathbb{I}_{m_\lambda}$ is an identity matrix of dimension m_λ, and the unitary $U_\lambda(g)$ is an irrep of $U(g)$ with multiplicity m_λ. This same unitary W induces a direct-sum decomposition (called isotypic decomposition) of the Hilbert space $\mathcal{H}$ for ρ_S and σ_S as follows:

$$W^\dagger \mathcal{H} = \bigoplus_\lambda \mathcal{H}_\lambda, \tag{4.125}$$

$$\mathcal{H}_\lambda := \mathbb{C}^{m_\lambda} \otimes \mathcal{K}_\lambda, \tag{4.126}$$

where $\mathcal{H}_\lambda$ is the space on which $\mathbb{I}_{m_\lambda} \otimes U_\lambda(g)$ acts and $\mathcal{K}_\lambda$ is the factor on which $U_\lambda(g)$ acts. Noting that the condition

$$\sigma_S = U_S(g) \sigma_S U_S(g)^\dagger \qquad \forall g \in G \tag{4.127}$$

is equivalent to

$$\sigma_S = \mathcal{T}_G(\sigma_S), \tag{4.128}$$

where the group twirl channel is defined as

$$\mathcal{T}_G(\cdot) := \frac{1}{|G|} \sum_{g \in G} U_S(g)(\cdot) U_S(g)^\dagger, \tag{4.129}$$

it then follows from (4.124) and Schur's lemma that the twirl channel $\mathcal{T}_G$ has the following form (see page 8 of [BRS07]):

$$\mathcal{T}_G(\cdot) = \mathcal{W} \circ \left(\sum_\lambda (\mathrm{id}_{m_\lambda} \otimes \mathcal{D}_\lambda) \circ \mathcal{P}_\lambda \right) \circ \mathcal{W}^\dagger, \tag{4.130}$$

where $\mathcal{W}(\cdot) \coloneqq W(\cdot)W^\dagger$, the map $\mathcal{P}_\lambda$ projects onto $\mathcal{H}_\lambda$ (i.e., $\mathcal{P}_\lambda(\cdot) \coloneqq \Pi_\lambda(\cdot)\Pi_\lambda$, with Π_λ the projection onto $\mathcal{H}_\lambda$), the map id_{m_λ} denotes the identity channel acting on the multiplicity space, and $\mathcal{D}_\lambda$ denotes a completely depolarizing channel with the action $\mathcal{D}_\lambda(\cdot) \coloneqq \mathrm{Tr}[\cdot]\pi_\lambda$, with $\pi_\lambda \coloneqq \mathbb{I}_{d_\lambda}/d_\lambda$ and d_λ the dimension of $\mathcal{K}_\lambda$. The effect of the twirl $\mathcal{T}_G$ on a general input σ is then

$$\mathcal{T}_G(\sigma) = W\left(\bigoplus_\lambda \mathrm{Tr}_2[\Pi_\lambda W^\dagger \sigma W \Pi_\lambda] \otimes \pi_\lambda\right) W^\dagger. \tag{4.131}$$

It then follows that every state satisfying (4.128) has the following form:

$$\sigma_S = W\left(\bigoplus_\lambda \tilde{\sigma}_\lambda \otimes \pi_\lambda\right) W^\dagger, \tag{4.132}$$

where $\{\tilde{\sigma}_\lambda\}_\lambda$ is a set of positive semi-definite operators such that $\sum_\lambda \mathrm{Tr}[\tilde{\sigma}_\lambda] = 1$. Thus, when performing the optimization in (4.121), it suffices to find the diagonalizing unitary W for the representation $\{U(g)\}_{g\in G}$ (for which an algorithm is known [AL12, Section 9.2.5]) and then optimize over the set $\{\tilde{\sigma}_\lambda\}_\lambda$, thus greatly reducing the space over which the optimization needs to be conducted. This kind of reduction was recently exploited in [FST22], and a Matlab toolbox was provided in [RMMB21]. We note that we can employ similar reasoning to simplify the optimization in (4.123).

It also follows from Schur's lemma that the group projection Π_S^G has the following form [Cub18, Eqs. (1)–(2)]:

$$\Pi_S^G = W\left(\bigoplus_\lambda \delta_{\lambda,\lambda_t} \mathbb{I}_{m_\lambda} \otimes \mathbb{I}_{d_\lambda}\right) W^\dagger, \tag{4.133}$$

$$= W\Pi_{\lambda_t} W^\dagger, \tag{4.134}$$

where λ_t is the irrep for the trivial representation of $\{U_S(g)\}_{g\in G}$. Noting that $d_{\lambda_t} = 1$ for this irrep, it follows that Π_{λ_t} acts as $\mathbb{I}_{m_\lambda}$ on this subspace. Thus, in the optimization in (4.120), it follows that every state σ_S satisfying $\sigma_S = \Pi_S^G \sigma_S \Pi_S^G$ has the following form:

$$W\sigma_{\lambda_t} W^\dagger, \tag{4.135}$$

where σ_{λ_t} is a state with support only in the space $\mathcal{H}_{\lambda_t}$, i.e., satisfying $\sigma_{\lambda_t} = \Pi_{\lambda_t}\sigma_{\lambda_t}\Pi_{\lambda_t}$. In this way, we can simplify the optimization task in (4.120). We finally note that we can employ similar reasoning to simplify the optimization in (4.123).

4.5 Variational algorithms for testing symmetry

Having established that the acceptance probabilities can be computed by SDPs for circuits on a sufficiently small number of qubits, we now propose variational quantum algorithms (VQA) for use on quantum computers as a proof-of-concept implementation of these tests (see [CAB+21, BCLK+22] for reviews of variational quantum algorithms). These algorithms make use of variational machine learning techniques to mimic the action of the prover in Algorithms 4.2–4.4; however, these techniques are in general limited in terms of their capabilities and thus do not fully satisfy the all-powerful nature of the prover called for in quantum interactive proofs. Note also that training a VQA has been shown to be NP-hard [BK21]; nonetheless, implementing such methods on near-term quantum devices gives a rough lower bound on the symmetry measures of interest. In the future, more advanced techniques could be substituted into the prover's position in an equivalent manner to improve on these lower-bound estimates. We present here a series of examples and show the circuit diagrams and VQA performance for these tests. To demonstrate the wide-ranging applicability of these algorithms, we have performed symmetry tests for a variety of groups.

For the algorithms discussed in this section, all code was implemented in Python using Qiskit (a Python package used for quantum computing with IBM Quantum). For each algorithm, the noiseless variant was implemented using the IBM Quantum noiseless simulator. For the noisy versions, we use the noise model from the IBM-Jakarta quantum computer and conduct a noisy simulation. We find that the algorithms behave well in both scenarios, and for VQA tests, our results converge in a reasonable number of layers, typically less than five. In the noisy simulations, the algorithms converge well, and the parameters obtained exhibit a noise resilience as put forward in [SKCC20]; that is, the relevant quantity can be accurately estimated by inputting the parameters learned from the noisy simulator into the noiseless simulator. Note that some sections show only a noiseless simulation; for these cases, the noisy simulation requires a noise model of a larger quantum system than is currently available to us.

As with many VQAs, it is necessary in these simulations to endeavor to avoid the barren plateau problem, in which global cost functions become untrainable. The algorithms specified in Section 4.2 rely solely on local measurements alone in the regime in which the number of data qubits is much larger than the number of control qubits and thus should not suffer from this issue in this regime [CSV+213]. Furthermore, all VQAs utilized herein employ the SPSA optimization technique

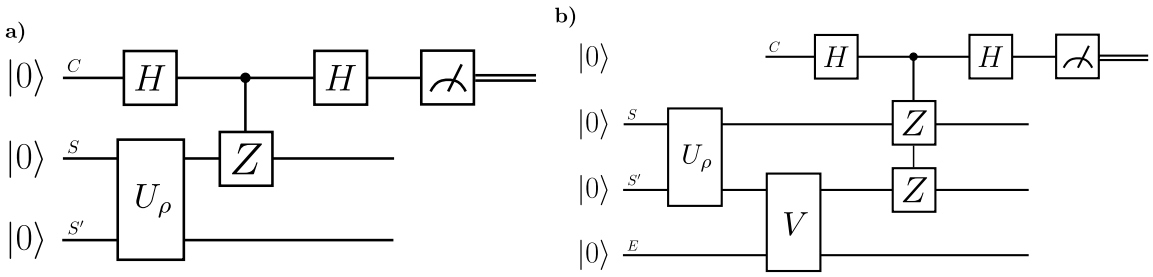


Figure 4.10: Symmetry tests for the $\mathbb{Z}_2$ group: a) G-Bose symmetry and b) G-symmetry.

discussed in [Spa98], which aims to prevent local minima problems. Indeed, our simulations did not run into either issue for any of the results discussed. However, we have only considered simulations of small quantum systems; it remains open to provide evidence that our algorithms will avoid the barren plateau problem for larger systems.

Lastly, consider that many of the algorithms in Section 4.2 allow the prover access to an environmental system, labelled E. A natural question is how best to choose the dimension of this system. In general, we find that the E system must be sufficiently large so as to match the input and output qubits, making the entire process unitary. For example, in G-symmetry tests, the dimension of the E system must be sufficiently large to provide a purification of the test state (recall Figure 4.4); for instance, if the state under test is a two-qubit state with a three-qubit purification, then E must necessarily provide the remaining qubit to get from the initial three-qubit purification to the four-qubit purification being tested. By construction, the purification of a state under test is always provided to the prover and is not considered part of the environmental system. For all simulations, we have taken the dimension of E to be the minimal viable dimension.

In what follows, we consider several groups and their unitary representations and test states for G-Bose symmetry, G-symmetry, G-Bose symmetric extendibility, and G-symmetric extendibility. We also test for two- and three-extendibility.

4.5.1 $\mathbb{Z}_2$ Group

In order to test membership in Sym_G, a group with an established unitary representation is needed. One somewhat trivial, albeit easily testable, example is the group generated by the identity and the Pauli Z gate. The group table for the $\mathbb{Z}_2$ group is given by

Group element	e	g
e	e	g
g	g	e

where e denotes the identity element. The $\mathbb{Z}_2$ group has a simple one-qubit unitary representation $\{e \to \mathbb{I}, g \to Z\}$. Since $\mathbb{Z}_2$ has two elements, the $|+\rangle_C$ state is a uniform superposition of two elements. Thus, we use one qubit and the Hadamard gate to generate the necessary state:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{4.136}$$

The control register states need to be mapped to group elements. We employ the mapping $\{|0\rangle \to e, |1\rangle \to g\}$ for our circuit constructions.

G-Bose symmetry

We begin with a test for Bose symmetry, which in this case is a test whether the state is equal to $|0\rangle\langle 0|$, because the group projector $\Pi_S^{\mathbb{Z}_2} = (\mathbb{I} + Z)/2 = |0\rangle\langle 0|$. Calculation by hand or classical computation can easily verify whether a state is Bose symmetric with respect to $\mathbb{I}$ and Z. Additionally, this simple gate set can be easily implemented on existing quantum computers.

Figure 4.10a) shows the circuit that tests for this G-Bose symmetry. Table 4.2 shows the results for various input states. The true fidelity value is calculated using (4.45), where Π_S^G is defined in (4.4).

G-symmetry

We now consider a simple test for G-symmetry. As mentioned in Remark 4.1, this is also a test for incoherence of the input state, i.e., to determine if it is diagonal in

State	True Fidelity	Noiseless	Noisy
$\|0\rangle\langle 0\|$	1	1.0	0.9998
$\|1\rangle\langle 1\|$	0	0.0	0.0013
$\|+\rangle\langle +\|$	0.5	0.5	0.5002
$\mathbb{I}/2$	0.5	0.5	0.5092

Table 4.2: Results of Z_2-Bose symmetry tests.

the computational basis. In the circuit depicted in Figure 4.10b), a parameterized circuit substitutes the role of an all-powerful prover.

A circuit that tests for G-symmetry is shown in Figure 4.10b). As this circuit involves variational parameters, an example of the training process is shown in Figure 4.11. Table 4.3 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.121) and is used as a comparison point.

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|0\rangle\langle 0\|$	1	0.9999	0.9987	0.9999
$\|1\rangle\langle 1\|$	1	1.0	1.0	0.9999
$\|+\rangle\langle +\|$	0.5	0.5	0.5087	0.5
$\mathbb{I}/2$	1	0.9999	0.9932	0.9999

Table 4.3: Results of Z_2-symmetry tests.

4.5.2 Triangular dihedral group D_3

G-Bose symmetry

Throughout Section 4.2, we have used the dihedral group of the equilateral triangle, abbreviated as D_3, as an example, and we continue to do so now. As a reminder, this group is generated by a flip of order two and a rotation of order three (denoted respectively by f and r). Then the group is specified as $D_3 = \{e, f, r, r^2, fr, fr^2\}$ where e is the identity element. General dihedral groups

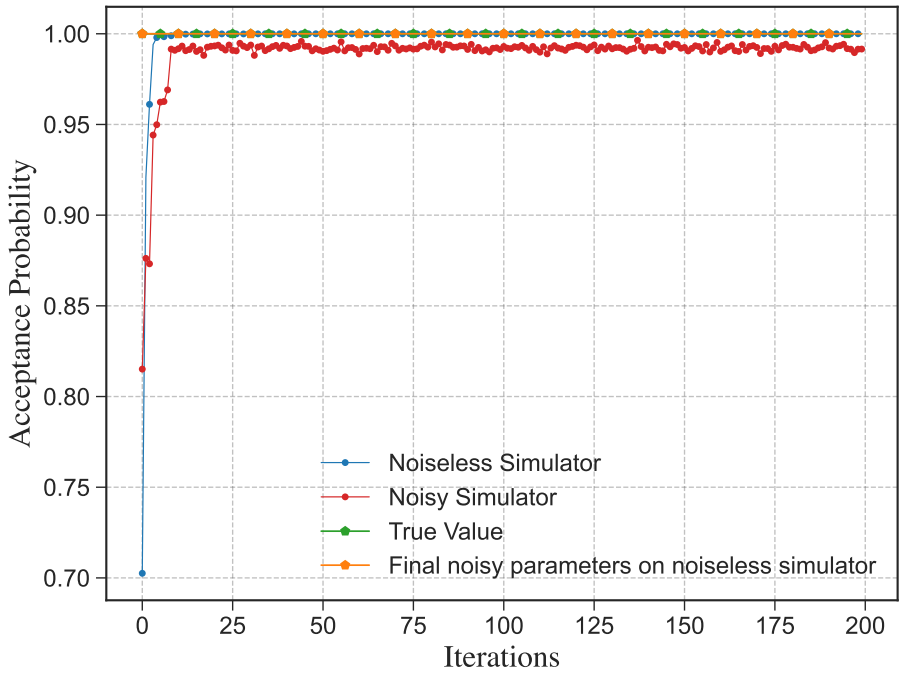


Figure 4.11: Example of the training process for testing $\mathbb{Z}_2$-symmetry of $\rho = \mathbb{I}/2$. We see that the training exhibits a noise resilience.

have previously been studied as non-abelian groups for which a quantum algorithm to find a hidden subgroup is available [Kup05].

In the introduction of Section 4.2, we provided a faithful, projective unitary representation of this group given by letting $U(f) = \text{CNOT}$, $U(r) = \text{CNOT} \cdot \text{SWAP}$, and $U(e) = \mathbb{I}_4$. Figure 4.3 shows the circuit needed to test for G-Bose symmetry. Note that we do not generate the control register using a quantum Fourier transform; as the resultant control state is still equivalent to $|+\rangle_C = \frac{1}{\sqrt{6}} \sum_{g \in D_3} |g\rangle$, this simplification suffices for our calculations. Table 4.4 shows the results for various input states. The true fidelity value is calculated using (4.45), where Π_S^G is defined in (4.4).

State	True Fidelity	Noiseless	Noisy
$\|00\rangle\langle 00\|$	1	1.0000	0.9998
ρ	1	0.9999	0.8756
Φ^+	0.6666	0.6666	0.5864
$\pi^{\otimes 2}$	0.5	0.5000	0.4716

Table 4.4: Results of D_3-Bose symmetry tests. The state ρ is defined as $|\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{\sqrt{3}}(|01\rangle + |10\rangle + |11\rangle)$.

G-symmetry

As with $\mathbb{Z}_2$, moving to G-symmetry requires the addition of a prover. This alteration was already depicted in Figure 4.5. The prover is replaced for practical purposes with a parameterized circuit involving variational parameters, and the training process is shown in Figure 4.12. Table 4.5 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.121).

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|00\rangle\langle 00\|$	1.0000	0.9999	0.9987	0.9999
ρ	1.0000	0.9999	0.6564	0.9425
Φ^+	0.6666	0.6666	0.5330	0.6415
$\pi^{\otimes 2}$	1.0000	0.9989	0.5189	0.8712

Table 4.5: Results of D_3-symmetry tests. The state ρ is defined as $|\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{\sqrt{3}}(|01\rangle + |10\rangle + |11\rangle)$.

G-Bose symmetric extendibility

A circuit that tests for G-Bose symmetric extendibility was originally shown in Figure 4.7 as the example circuit construction. Now, we show how that construction behaves under a parameterized circuit substitution of the prover. Again, we give an example of the training behavior of the algorithm in Figure 4.13. We also provide Table 4.6, which shows the final results after training for various input

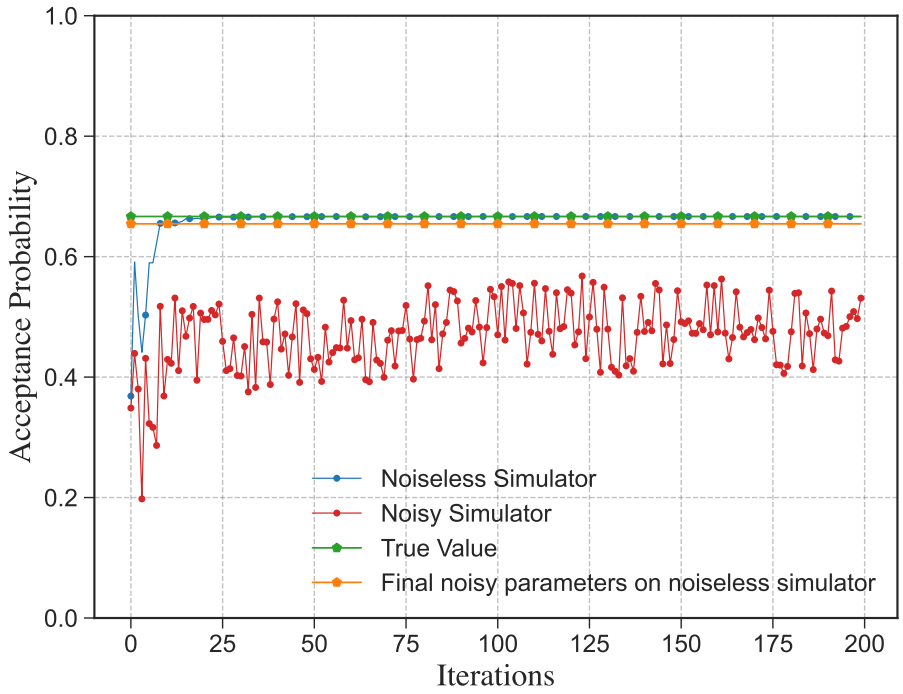


Figure 4.12: Example of the training process for testing D_3-symmetry of Φ^+. We see that the training exhibits a noise resilience.

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|0\rangle\langle 0\|$	1.0000	1.0000	0.8758	0.9988
$\|1\rangle\langle 1\|$	0.6670	0.6667	0.5834	0.6663
π	1.0000	1.0000	0.8255	0.9995
$\begin{bmatrix} \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{2}{3} \end{bmatrix}$	1.0000	0.9999	0.6564	0.9425

Table 4.6: Results of D_3-Bose symmetric extendibility tests.

states. The true fidelity is calculated using the semi-definite program given in (4.122).

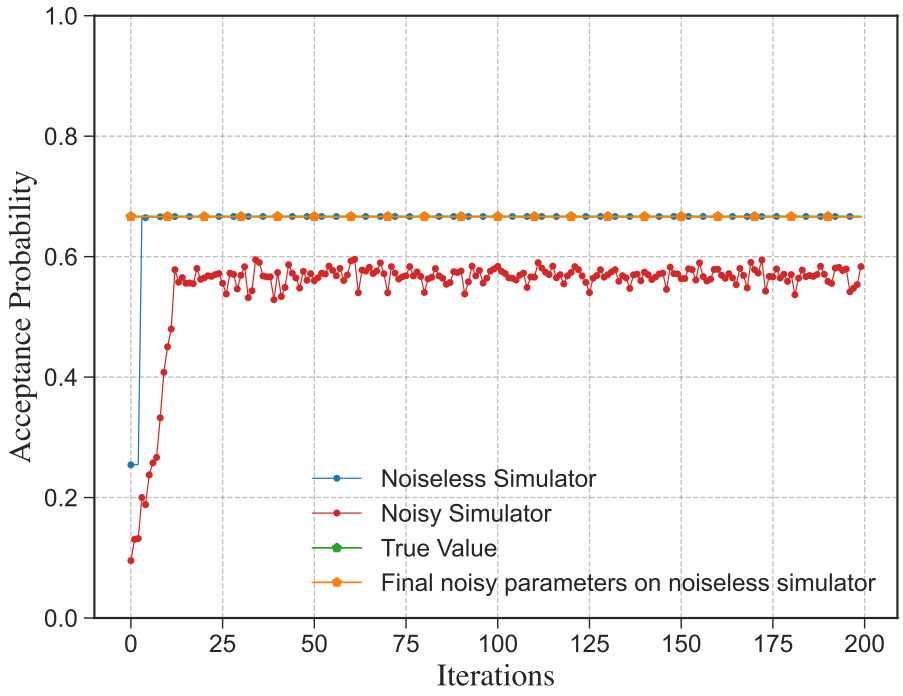


Figure 4.13: Example of the training process for testing D_3-Bose symmetric extendibility of $|1\rangle\langle 1|$. We see that the training exhibits a noise resilience.

G-symmetric extendibility

Finally, we address the circuit in Figure 4.9, which gives a test for G-symmetric extendibility. This final circuit has the prover performing two actions at once—both finding the correct purification as in the case of G-symmetry and creating the correct extension as in G-Bose symmetric extendibility tests. Once again, the prover is replaced with a parameterized circuit, and an example of the training process is shown in Figure 4.14. Table 4.7 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.123).

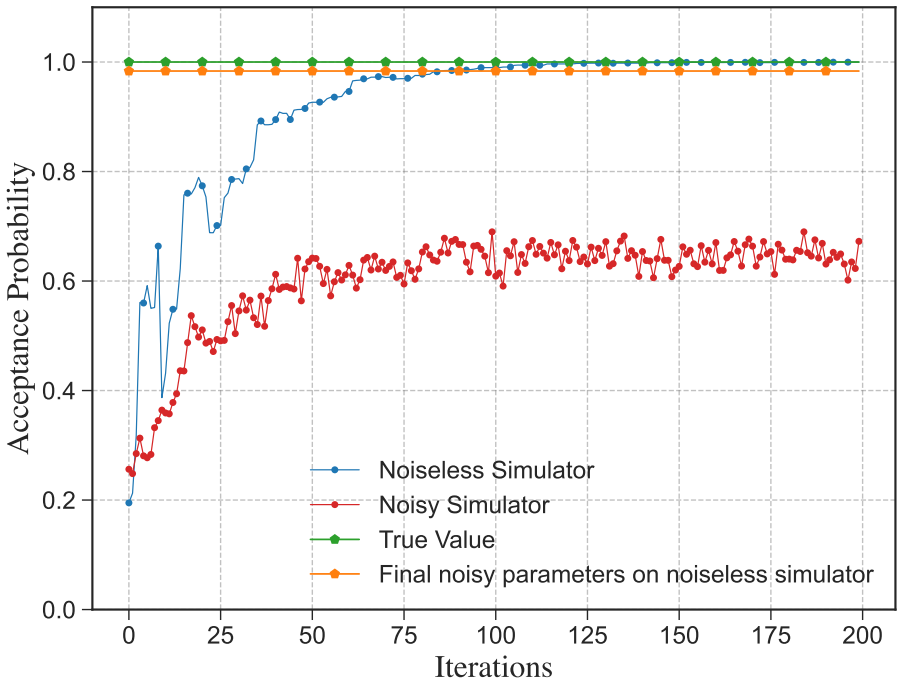


Figure 4.14: Example of the training process for testing D_3-symmetric extendibility of $|0\rangle\langle 0|$. We see that the training exhibits a noise resilience.

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|0\rangle\langle 0\|$	1.0000	0.9998	0.6725	0.9835
$\|1\rangle\langle 1\|$	0.6666	0.6641	0.4476	0.6497
π	1.0000	0.9988	0.6901	0.9764
ρ	0.9714	0.9662	0.5593	0.8789

Table 4.7: Results of D_3-symmetric extendibility tests. The state ρ is defined as $\begin{bmatrix} 0.5 & -0.354i \\ 0.354i & 0.5 \end{bmatrix}$.

4.5.3 Collective U group

Given an n-qudit state ρ, we wish to test if it is symmetric with respect to the following group:

$$G_U := \{U^{\otimes n}\}_{U \in \mathrm{SU}(d)}. \tag{4.137}$$

This is an example of a continuous group symmetry; however, we will be able to draw upon the particular properties of this projector to realize each symmetry test nonetheless.

G-Bose symmetry

A state that is G_U-Bose symmetric satisfies the condition given in (4.46), where

$$\Pi_U^{(n)} := \int dU \; U^{\otimes n}, \tag{4.138}$$

with dU being the Haar measure for the group $\mathrm{SU}(d)$.

In what follows, we focus on two-qubit states. A simple calculation shows that for $n = 2$ and $d = 2$, the singlet state $|\Psi^-\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, is the only G_U-Bose symmetric state. In other words,

$$\Pi_U^{(2)} = |\Psi^-\rangle\langle\Psi^-|. \tag{4.139}$$

Thus, testing for G_U-Bose symmetry is equivalent to testing if the state is the singlet state.

To test a symmetry of this form, we rewrite the projector in terms of a set $\{U_i\}_{i=1}^N$ of unitaries satisfying

$$\Pi_U^{(2)} = \frac{1}{N} \sum_{i=1}^{N} U_i. \tag{4.140}$$

While there exist multiple choices for the set $\{U_i\}_{i=1}^N$, we pick a set that is compatible with all of the symmetry tests that we perform in the forthcoming subsections. Our choice $\{U_i\}_{i=1}^N$ is given in [BDSW96, Appendix A] and is composed of products of bilateral rotations B_x, B_y, and B_z, where

$$B_a := R_a(-\pi/2) \otimes R_a(-\pi/2)\,, \tag{4.141}$$

and R_a is the following rotation gate about the a axis:

$$R_a(\theta) \coloneqq e^{-i\theta\sigma_a/2} \tag{4.142}$$

$$= \cos(\theta/2)\mathbb{I} - i\sin(\theta/2)\sigma_a. \tag{4.143}$$

(Note the different convention that we take here, as compared to [BDSW96], when defining bilateral rotations.) Specifically, the set $\{U_i\}_i$ is given by

$$\{U_i\}_i = \{\mathbb{I},\ B_xB_x,\ B_yB_y,\ B_zB_z,\ B_xB_y,\ B_yB_z,\ B_zB_x,\ B_yB_x,\ B_xB_yB_xB_y,\ B_yB_zB_yB_z,\ B_zB_xB_zB_x,\ B_yB_xB_yB_x\}. \tag{4.144}$$

The set $\{U_i\}_i$ forms a group isomorphic to the alternating group A_4, which is defined as the set of even permutations on four objects. Furthermore, A_4 can be written as a product of a Klein group on four objects $K_4 = \{e, a = (12)(34), b = (13)(24), c = (14)(23)\}$ and the cyclic group $C_3 = \{e, g = (123), h = (132)\}$. In other words,

$$A_4 = K_4 \times C_3. \tag{4.145}$$

The Klein group K_4 can be mapped as $\{e \to \mathbb{I}, a \to B_xB_x, b \to B_yB_y, c \to B_zB_z\}$. Similarly, the cyclic group can be mapped as $\{e \to \mathbb{I}, g \to B_xB_y, h \to B_yB_x\}$. We use this to design our control register and corresponding mapping there. Since we have 12 elements, the $|+\rangle_C$ state is a uniform superposition of 12 elements. However, the aforementioned decomposition allows us to split the control register into two sets, one controlling the K_4 group and another controlling the C_3 group. We use a unary encoding for both subgroups, leading to a five-qubit control register. The specific mapping and group assignment are as follows:

Control State	Group Element	Unitary Representation
00 000	e	$\mathbb{I}$
00 100	c	$B_z B_z$
00 010	b	$B_y B_y$
00 001	a	$B_x B_x$
01 000	g	$B_x B_y$
01 100	gc	$B_y B_z$
01 010	gb	$B_z B_x$
01 001	ga	$B_y B_x B_y B_x$
10 000	h	$B_y B_x$
10 100	hc	$B_y B_z B_y B_z$
10 010	hb	$B_x B_y B_x B_y$
10 001	ha	$B_z B_x B_z B_x$

To generate an equal superposition of the 12 basis elements, we use the unitary U_W depicted in Figure 4.15. With this construction settled, we can now test for symmetry with respect to this collective U group.

Figure 4.16a) depicts the circuit that tests for G-Bose symmetry. Table 4.8 shows the results for various input states. The true fidelity value is calculated using (4.45), where Π_S^G is defined in (4.4).

State	True Fidelity	Noiseless	Noisy
$\|00\rangle\langle 00\|$	0	0.0000	0.0459
ρ	0.6667	0.6667	0.2661
Ψ^+	0	0.0000	0.0389
Ψ^-	1.0	1.0000	0.3517

Table 4.8: Results of collective U-Bose symmetry tests. The state ρ is defined as $|\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle - |01\rangle + |10\rangle)$.

G-symmetry

An n-qudit state ρ that is G_U-symmetric satisfies the following condition:

$$\rho = \int dU \; U^{\otimes n} \rho (U^\dagger)^{\otimes n}, \tag{4.146}$$

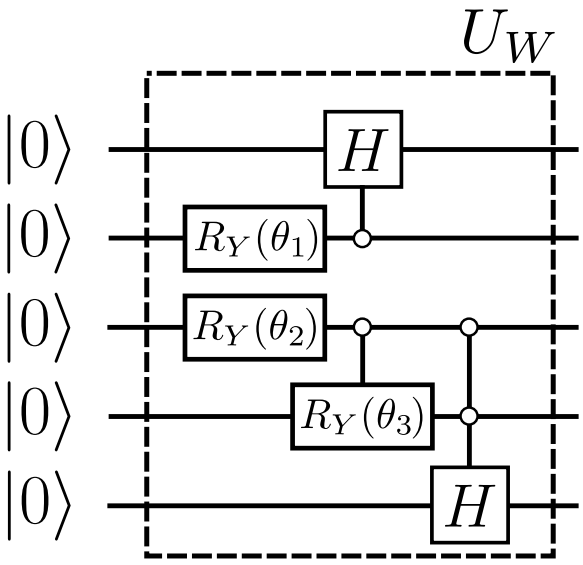


Figure 4.15: Unitary U_W, with $\theta_1 = \theta_3 = 2\arctan\left(\frac{1}{\sqrt{2}}\right)$ and $\theta_2 = \pi/3$, generates the equal superposition of 12 elements given. The circuit acting on the top two qubits generates the state $(|00\rangle + |01\rangle + |10\rangle)/\sqrt{3}$, and the circuit acting on the bottom three qubits generates the state $(|000\rangle + |001\rangle + |010\rangle + |100\rangle)/\sqrt{4}$.

where dU is the Haar measure for the group SU(d). States that satisfy this condition for $n = 2$ are called Werner states [Wer89b], i.e.,

$$\rho = \int dU \, (U \otimes U) \rho \, (U \otimes U)^\dagger. \tag{4.147}$$

As shown in [BDSW96], for $n = 2$ and $d = 2$, the continuum of rotations in the symmetry test can be replaced by a discrete sum (a two-design), as follows:

$$\bar{\rho} = \frac{1}{N} \sum_{i=1}^{N} U_i \rho U_i^\dagger, \tag{4.148}$$

where $\{U_i\}_{i=1}^N$ is the set defined in (4.144). A circuit that tests for G-symmetry is shown in Figure 4.16b). It involves variational parameters, and an example of the training process is shown in Figure 4.17. Note that, as this construction requires many qubits, only noiseless simulations results could be obtained. These results may be easily extended as access to higher-qubit machines becomes more readily available, allowing for noisy simulations of more complex systems. Table 4.9

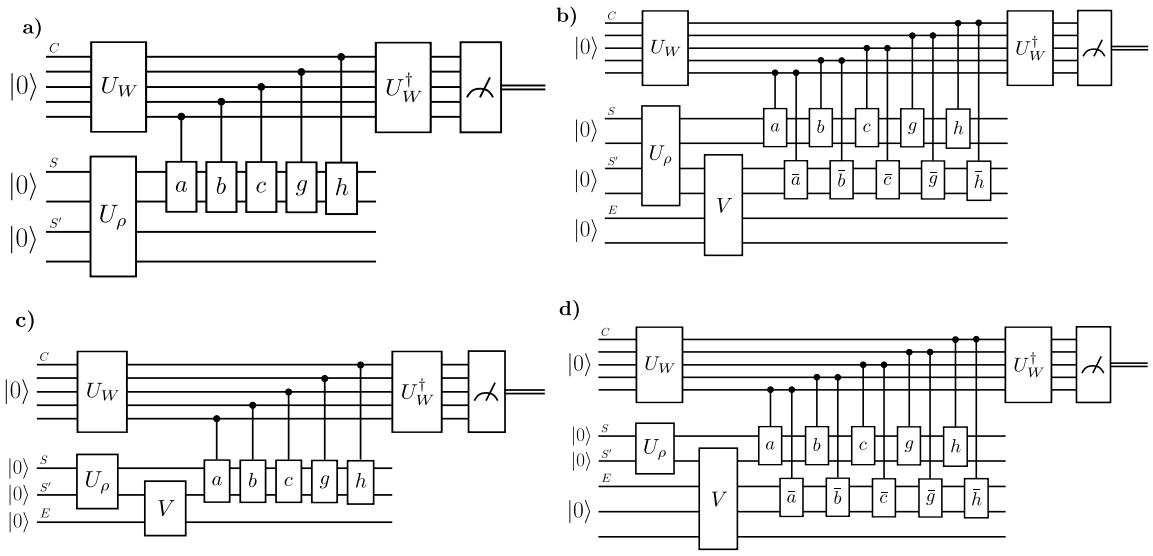


Figure 4.16: Symmetry tests for the collective-U group: a) G-Bose symmetry, b) G-symmetry, c) G-Bose symmetric extendible, and d) G-symmetric extendible.

shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.121).

State	True Fidelity	Noiseless
$\|10\rangle\langle 10\|$	0.5000	0.4997
ρ	0.6667	0.6666
Ψ^+	0.3333	0.3332
$\pi^{\otimes 2}$	1.0000	0.9988

Table 4.9: Results of collective U-symmetry tests. The state ρ is defined as $|\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle - |01\rangle + |10\rangle)$.

We note here that the G_U-symmetry test would be unaffected by redefining the integral over all unitaries $U \in \mathrm{U}(2)$ without the restriction to SU(2). However, the projector for the G_U-Bose symmetry test would be as follows in that case:

$$\Pi_U = \int_{U\in \mathrm{U}(2)} dU\; U \otimes U = 0, \tag{4.149}$$

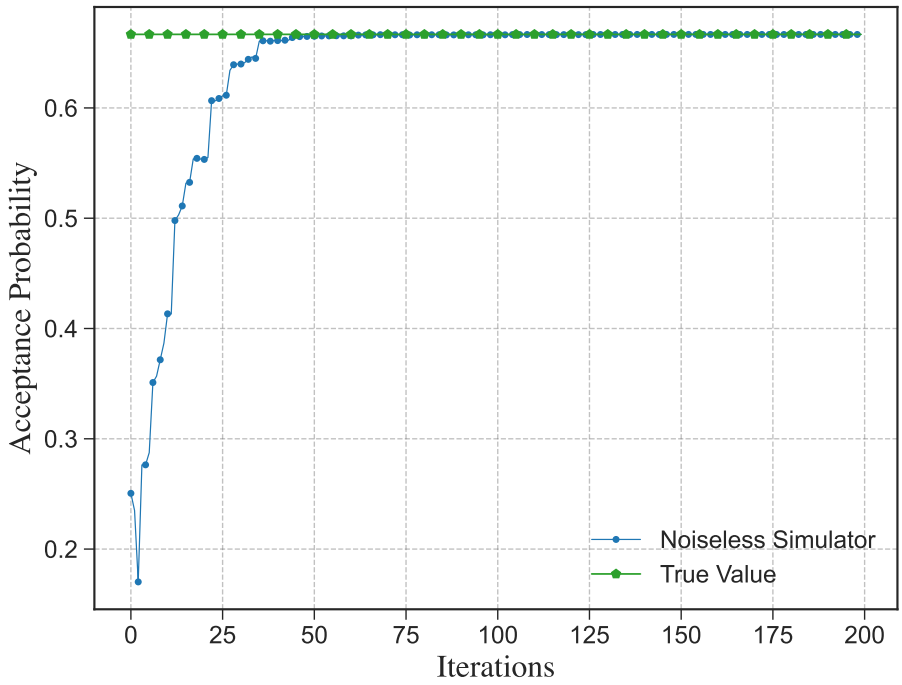


Figure 4.17: Example of the training process for testing collective U-symmetry of $\rho = |\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle - |01\rangle + |10\rangle)$.

making the test trivial. Thus, in the previous section, we chose to restrict the group to SU(2) unitaries.

G-Bose symmetric extendibility

A circuit that tests for G-Bose symmetric extendibility is shown in Figure 4.16c). It involves variational parameters, and an example of the training process is shown in Figure 4.18. Table 4.10 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.122).

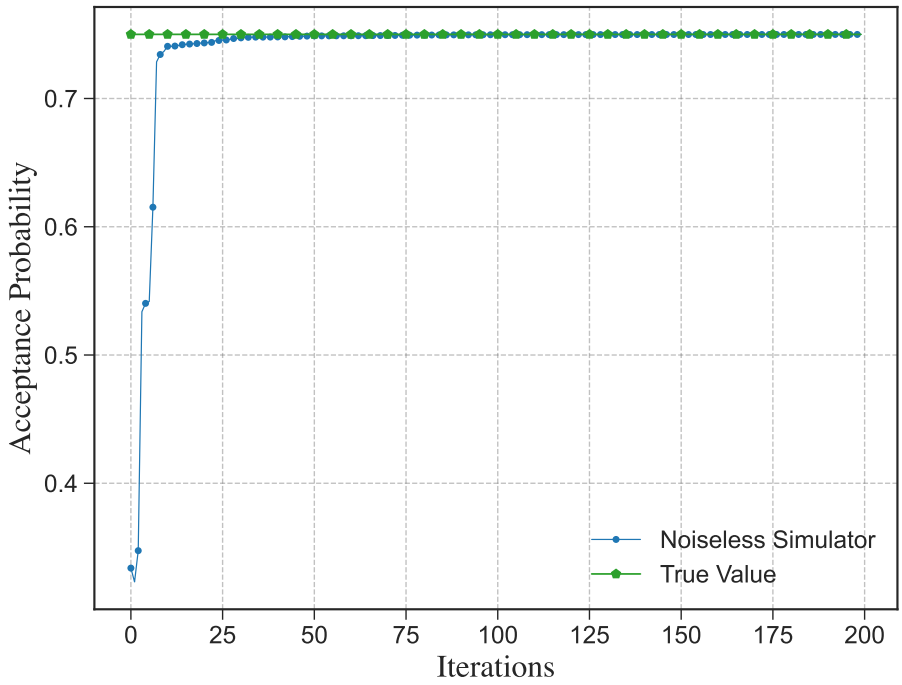


Figure 4.18: Example of the training process for testing collective U-Bose symmetric extendibility of the state $\begin{bmatrix} 0.93 & 0 \\ 0 & 0.07 \end{bmatrix}$.

State	True Fidelity	Noiseless
$\|1\rangle\langle 1\|$	0.5000	0.5000
π	1.0000	0.9998
$\begin{bmatrix} 0.93 & 0 \\ 0 & 0.07 \end{bmatrix}$	0.7500	0.7499

Table 4.10: Results of collective U-BSE tests.

G-symmetric extendibility

A circuit that tests for G-symmetric extendibility is shown in Figure 4.16d). It involves variational parameters, and an example of the training process is shown in Figure 4.19. Table 4.11 shows the final results after training for various input

State	True Fidelity	Noiseless
$\|0\rangle\langle 0\|$	0.5000	0.4995
π	1.0000	0.9996
$\begin{bmatrix} 0.95 & 0 \\ 0 & 0.05 \end{bmatrix}$	0.7169	0.7095

Table 4.11: Results of collective U-symmetric extendibility tests.

states. The true fidelity is calculated using the semi-definite program given in (4.123).

These group symmetry tests have applications in the identification and verification of Werner states, as discussed above. Current limitations include access to higher qubit machines, but also the noisiness of these machines. Our VQA results converge well in the noiseless case, but it is likely that noise will only become a bigger problem as the circuit size scales up, unless adequately addressed.

4.5.4 Collective phase group

Given an n-qubit state ρ, we wish to test if the state is symmetric with respect to the following collective phase group:

$$G_z := \{R_z(\phi)^{\otimes n}\}_{\phi\in[0,4\pi)}, \tag{4.150}$$

where we recall that $R_z(\phi) := \exp(-i\phi\sigma_z/2)$. The interval for ϕ is $[0, 4\pi)$ to ensure that G_z is a group. This is a consequence of SU(2) double covering SO(3), implying that $R_z(4\pi) = \mathbb{I}$. Additionally, the Haar measure for the group of unitaries $\{R_z(\phi)\}_{\phi\in[0,4\pi)}$ is given by

$$dU = \frac{d\phi}{4\pi}. \tag{4.151}$$

G-Bose symmetry

A state that is G_z-Bose symmetric satisfies the condition given in (4.46), where

$$\Pi_z^{(n)} := \frac{1}{4\pi}\int_0^{4\pi} R_z(\phi)^{\otimes n}\, d\phi. \tag{4.152}$$

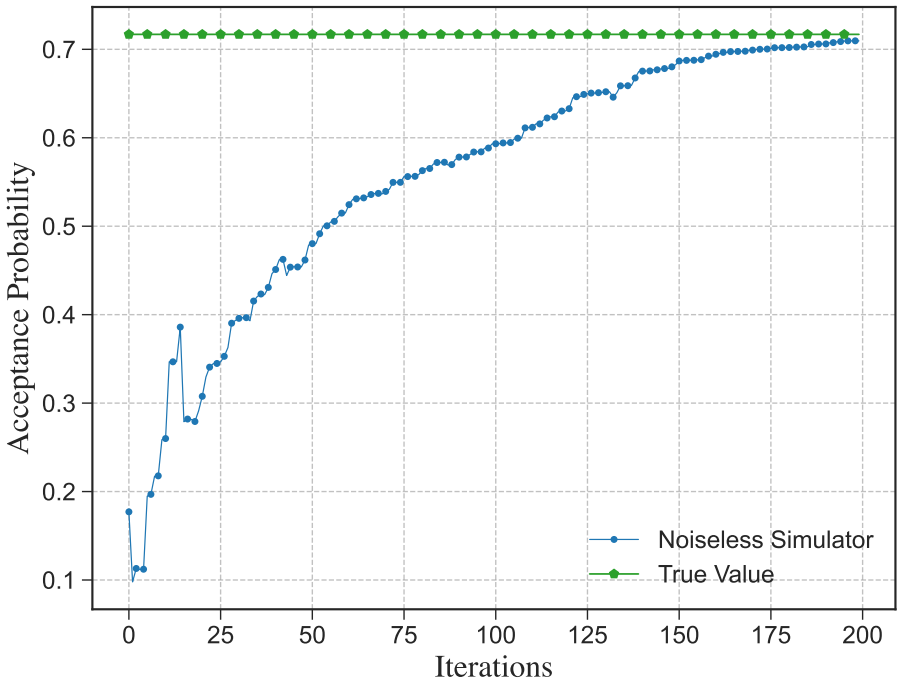


Figure 4.19: Example of the training process for testing collective U-symmetric extendibility of the state $\begin{bmatrix} 0.95 & 0 \\ 0 & 0.05 \end{bmatrix}$.

Expressing $R_z(\phi)$ in the computational basis,

$$R_z(\phi) = \text{Diag}\left\{\exp\left(-\frac{i\phi}{2}\right), \exp\left(\frac{i\phi}{2}\right)\right\}. \tag{4.153}$$

Similarly, expressing $R_z(\phi)^{\otimes 2}$ in the computational basis,

$$R_z(\phi)^{\otimes 2} = \text{Diag}\left\{\exp\left(-i\phi\right), 1, 1, \exp\left(i\phi\right)\right\}. \tag{4.154}$$

Generalizing to the case of n qubits, observe that the number of zeros in a bit-string x is $n - H(x)$ and the number of ones is $H(x)$, where $H(x)$ is the Hamming weight of x. For example, $H(6) = 2$ since $6_{10} \equiv 110_2$. Each zero contributes a phase of $-\phi/2$ for a total of $-(n - H(x))\phi/2$, and each one contributes a phase of $\phi/2$, for a total of $H(x)\phi/2$. Then the overall total for the bit-string x is

$$-(n - H(x))\phi/2 + H(x)\phi/2 = (2H(x) - n)\phi/2. \tag{4.155}$$

This implies that

$$R_z(\phi)^{\otimes n} = \mathrm{Diag}\left\{\exp\left[\left(\frac{2H(x)-n}{2}\right)i\phi\right]_{x=0}^{2^n-1}\right\}, \tag{4.156}$$

where $H(x)$ is the Hamming weight of x written in binary.

Performing the integral, we note that for $a \in \mathbb{Z} \setminus \{0\}$,

$$\int_0^{4\pi} \exp\left(\frac{a}{2}i\phi\right) d\phi = 0. \tag{4.157}$$

Thus, only terms satisfying $H(x) = n/2$ survive the integral. Observe then that $\Pi_z^{(n)} = 0$ for all odd n. Thus, it follows that

$$\Pi_z^{(n)} = \begin{cases} P_k & \text{if } n = 2k \\ 0 & \text{otherwise,} \end{cases} \tag{4.158}$$

where P_k is defined as the projector onto the subspace of computational basis elements with Hamming weight k. As an example, for $n = 2$,

$$\Pi_z^{(2)} = P_1 = |01\rangle\langle 01| + |10\rangle\langle 10|. \tag{4.159}$$

To test a symmetry of this form, we rewrite the projector in terms of unitaries. We construct a set of unitaries U_y such that

$$\Pi_z^{(n)} = \frac{1}{n+1}\sum_{y=0}^{n} U_y. \tag{4.160}$$

We use a construction similar to the form given in [Tom15, Eq. (2.59)]. Define a unitary representation $\{U_y\}_{y=0}^n$ as

$$U_y := \sum_{x=0}^{n} \exp\left[\frac{\pi i}{n+1}(2y-n)(2x-n)\right] P_x. \tag{4.161}$$

Observe that $U_y^\dagger U_y = \mathbb{I}$. Furthermore, we see that

$$\sum_{y=0}^{n} U_y = \sum_{x=0}^{n}\sum_{y=0}^{n} \exp\left[\frac{\pi i}{n+1}(2y-n)(2x-n)\right] P_x. \tag{4.162}$$

Consider that for integer $c \neq 0$,

$$\sum_{y=0}^{n} \exp\left(\frac{\pi i}{n+1} c\,(2y-n)\right)$$

$$= \exp\left(\frac{-\pi i c n}{n+1}\right) \frac{1-\exp(2\pi i c)}{1-\exp\left(\frac{2\pi i c}{n+1}\right)} \tag{4.163}$$

$$= 0. \tag{4.164}$$

Thus, only terms satisfying $2x = n$ survive the summation. Therefore,

$$\frac{1}{n+1}\sum_{y=0}^{n} U_y = \sum_{x=0}^{n} \delta_{2x,n} P_x \tag{4.165}$$

$$= \begin{cases} P_k & \text{if } n = 2k \\ 0 & \text{otherwise} \end{cases} \tag{4.166}$$

$$= \Pi_z^{(n)}. \tag{4.167}$$

Thus, testing G-Bose symmetry with respect to $G_z = \{R_z(\phi)^{\otimes n}\}_{\phi\in[0,4\pi)}$ is equivalent to testing G-Bose symmetry with respect to $\{U_y\}_{y=0}^{n}$. To summarize, testing if a n-qubit state is G_z-Bose symmetric is equivalent to testing if it belongs to the subspace of Hamming weight $n = 2k$. As an aside, we note that a generalization of our method allows for performing a projection onto constant-Hamming-weight subspaces, which is useful in tasks like entanglement concentration [Wil17]. See also [KM01] for alternative circuit constructions for performing measurements of Hamming weight.

In what follows, we test the symmetry for an example, with $n = 2$. From the definition, we see that

$$U_0 = \exp\left(-\frac{2\pi i}{3}\right) P_0 + P_1 + \exp\left(\frac{2\pi i}{3}\right) P_2, \tag{4.168}$$

$$U_1 = \mathbb{I}, \tag{4.169}$$

$$U_2 = \exp\left(\frac{2\pi i}{3}\right) P_0 + P_1 + \exp\left(-\frac{2\pi i}{3}\right) P_2$$

$$= U_0^2. \tag{4.170}$$

Thus, the set of unitaries forms a unitary representation of the cyclic group C_3. The group table can be seen in Section 4.5.5, where $\{|00\rangle \to U_1, |01\rangle \to U_0, |11\rangle \to U_2\}$.

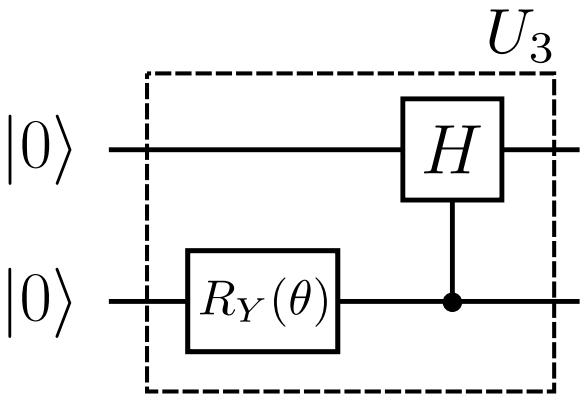


Figure 4.20: Unitary U_3, with $\theta = 2\arctan\left(\sqrt{2}\right)$, generates the equal superposition of three elements from (4.173).

Expanding terms, we see that

$$U_0 = \left(R_z\left(\frac{2\pi}{3}\right)\right)^{\otimes 2}. \tag{4.171}$$

Furthermore, since $U_2 = U_0^2$,

$$U_2 = \left(R_z\left(-\frac{2\pi}{3}\right)\right)^{\otimes 2}. \tag{4.172}$$

Since we have three elements, the $|+\rangle_C$ state is a uniform superposition of three elements. We use two qubits and the unitary U_3 used to generate the following superposition, as shown in Figure 4.20:

$$U_3 |00\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |11\rangle). \tag{4.173}$$

Figure 4.21a) depicts the circuit that tests for G-Bose symmetry. Table 4.12 shows the results for various input states. The true fidelity value is calculated using (4.45), where Π_S^G is defined in (4.4).

G-symmetry

A state that is G_z-symmetric satisfies the following condition:

$$\rho = C_z^{(n)}(\rho), \tag{4.174}$$

State	True Fidelity	Noiseless	Noisy
$\|00\rangle\langle 00\|$	0.0	0.0000	0.0220
ρ	1.0	1.0000	0.9170
$\|0\rangle\langle 0\| \otimes \|+\rangle\langle +\|$	0.5	0.5000	0.4877
$\pi^{\otimes 2}$	0.5	0.5000	0.4661

Table 4.12: Results of collective-phase-Bose symmetry tests. The state ρ is defined as $|\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

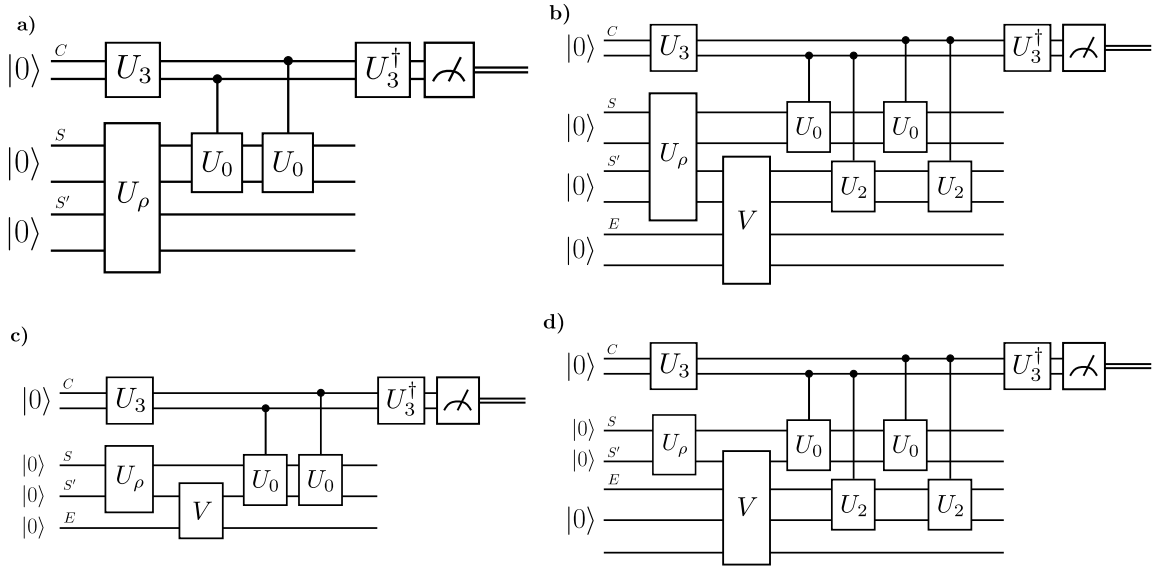


Figure 4.21: Symmetry tests for the collective phase group: a) G-Bose symmetry, b) G-symmetry, c) G-Bose symmetric extendibility, and d) G-symmetric extendibility. The unitary U_0 is defined in (4.171). Note that $U_2 = U_0^\dagger$.

where the collective dephasing channel $\mathcal{C}_z^{(n)}$ is defined as

$$\mathcal{C}_z^{(n)}(\omega) := \frac{1}{4\pi}\int_0^{4\pi} d\phi\, R_z(\phi)^{\otimes n}\omega R_z^\dagger(\phi)^{\otimes n}. \tag{4.175}$$

Using the fact that

$$R_z(\phi) = \exp(-i\phi\sigma_z/2), \tag{4.176}$$

we see that

$$R_z(\phi)\,|a\rangle\langle b|\,R_z^\dagger(\phi) = e^{i\phi(a-b)}\,|a\rangle\langle b|\,, \tag{4.177}$$

for $a, b \in \{0, 1\}$. Thus, for a general n-qubit state ρ, expanded in the computational basis as

$$\rho = \sum_{x_1,\ldots,x_n,y_1,\ldots,y_n} \rho_{x_1,\ldots,x_n,y_1,\ldots,y_n} |x_1 \cdots x_n\rangle\langle y_1 \cdots y_n| , \tag{4.178}$$

it follows that

$$C_z^{(n)}(\rho) = \sum_{x_1,\ldots,x_n,y_1,\ldots,y_n} \delta\left(\sum_i x_i, \sum_j y_j\right) \rho_{x_1,\ldots,x_n,y_1,\ldots,y_n} |x_1 \cdots x_n\rangle\langle y_1 \cdots y_n| . \tag{4.179}$$

Since $\sum_i x_i = H(x)$, it follows that

$$C_z^{(n)}(\rho) = \sum_{k=0}^{n} P_k \rho P_k, \tag{4.180}$$

where, as before, P_k is the projector onto the subspace of Hamming weight k. For the case of $n = 2$, we get the following projectors

$$P_0 = |00\rangle\langle 00|, \tag{4.181}$$
$$P_1 = |01\rangle\langle 01| + |10\rangle\langle 10|, \tag{4.182}$$
$$P_2 = |11\rangle\langle 11|. \tag{4.183}$$

To test a symmetry of this form, we can rewrite the channel in terms of a set $\{U_y\}_y$ of unitaries satisfying

$$C_z^{(n)}(\rho) = \frac{1}{n+1} \sum_{y=0}^{n} U_y \rho U_y^\dagger. \tag{4.184}$$

We now prove that the unitaries $\{U_y\}_{y=0}^n$ from (4.161) satisfy this condition:

$$\begin{aligned}
&\frac{1}{n+1} \sum_{y=0}^{n} U_y \rho U_y^\dagger \\
&= \frac{1}{n+1} \sum_{\substack{x,x',\\ y=0}}^{n} \exp\left[\frac{\pi i}{n+1} (2y - n)\, 2\,(x - x')\right] P_x \rho P_{x'} \\
&= \frac{1}{n+1} \sum_{x,x'=0}^{n} (n+1)\delta_{x,x'} P_x \rho P_{x'} \qquad (4.185) \\
&= \sum_{x=0}^{n} P_x \rho P_x, \qquad (4.186)
\end{aligned}$$

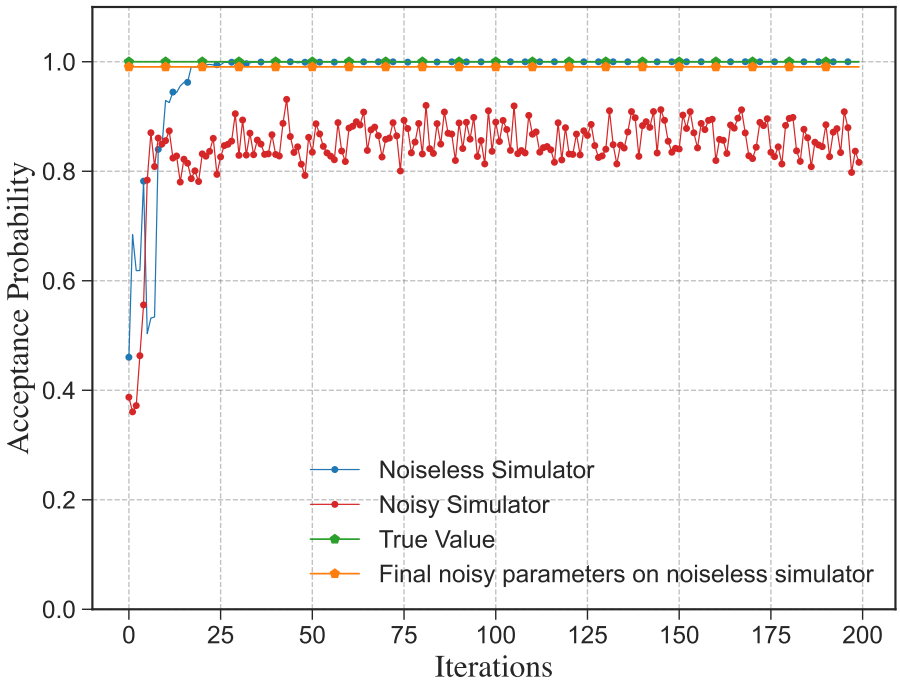


Figure 4.22: Example of the training process for testing collective-phase-symmetry of $\rho = |\Psi^+\rangle\langle\Psi^+|$, where $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

where the third equality follows from the reasoning in (4.164).

Thus, similar to the G-Bose symmetry tests, testing G-symmetry with respect to $G_z = \{R_z(\phi)^{\otimes n}\}_{\phi\in[0,4\pi)}$ is equivalent to testing G-symmetry with respect to $\{U_y\}_{y=0}^{n}$. To summarize, testing if an n-qubit state is G_z-symmetric is equivalent to testing if it belongs to a subspace of fixed Hamming weight. In this work, we test the symmetry for $n = 2$.

A circuit that tests for G-symmetry is shown in Figure 4.21b). It involves variational parameters, and an example of the training process is shown in Figure 4.22. Table 4.13 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.121).

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|00\rangle\langle 00\|$	1.0000	0.9999	0.8380	0.9928
ρ	1.0000	1.0000	0.8162	0.9906
τ	0.5001	0.5000	0.4630	0.4990
$\pi^{\otimes 2}$	1.0000	0.9998	0.8417	0.9934

Table 4.13: Results of collective-phase-symmetry tests. The state ρ is defined as $|\Psi^+\rangle\langle\Psi^+|$ where $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. The state τ is defined as $|\Phi^+\rangle\langle\Phi^+|$ where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle) + |11\rangle)$.

G-Bose symmetric extendibility

A circuit that tests for G-Bose symmetric extendibility is shown in Figure 4.21c). It involves variational parameters, and an example of the training process is shown in Figure 4.23. Table 4.14 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.122).

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|0\rangle\langle 0\|$	1.0000	1.0000	0.9783	0.9980
σ	1.0000	1.0000	0.9349	0.9993
$\|-\rangle\langle -\|$	0.5002	0.5000	0.4464	0.5000
ρ	0.9330	0.9330	0.9208	0.9328

Table 4.14: Results of collective-phase-Bose symmetric extendibility tests. The state σ is defined as $\frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$. The state ρ is defined as $\begin{bmatrix} 0.93 & 0.25 \\ 0.25 & 0.07 \end{bmatrix}$.

G-symmetric extendibility

A circuit that tests for G-symmetric extendibility is shown in Figure 4.21d). It involves variational parameters, and an example of the training process is shown in Figure 4.24. Table 4.15 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.123).

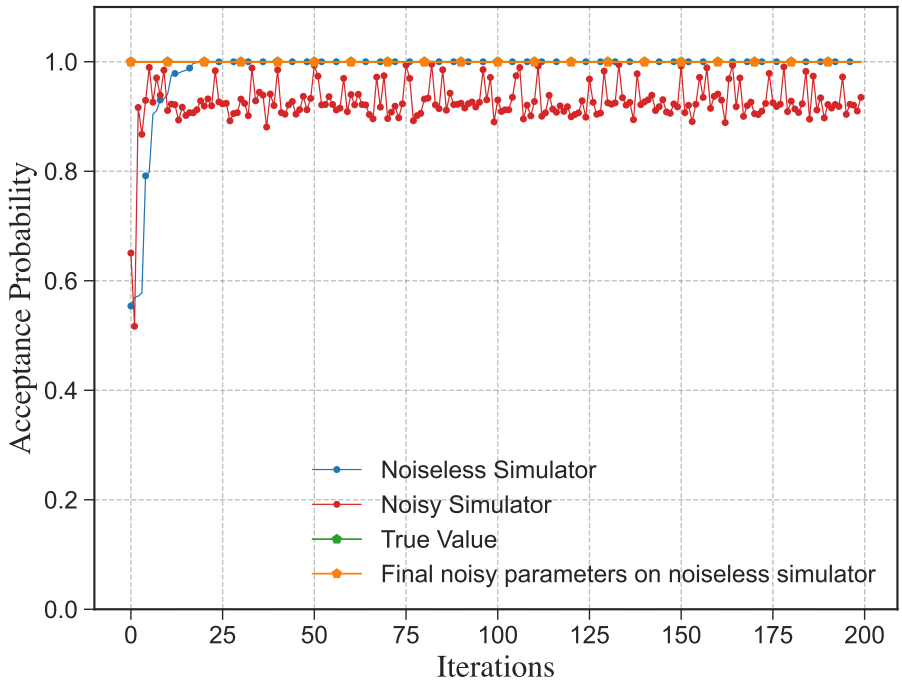


Figure 4.23: Example of the training process for testing collective-phase-Bose symmetric extendibility of $\frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$. We see that the training exhibits a noise resilience.

4.5.5 Cyclic group C_3

Cyclic groups, denoted by C_n, are abelian groups formed by cyclic shifts of n elements and always have order n. Consider first C_3, the cyclic group on three elements. The group table for C_3 is given by

Group element	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

The C_3 group has a one-dimensional representation given by the third roots of unity, but here we instead opt for a two-qubit unitary representation cor-

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|0\rangle\langle 0\|$	1.0000	0.9960	0.8632	0.9988
$\|+\rangle\langle +\|$	0.5000	0.5000	0.4580	0.4997
ρ	0.7500	0.7494	0.6577	0.7484

Table 4.15: Results of collective-phase-symmetric extendibility tests. The state ρ is defined as $\begin{bmatrix} 0.75 & 0.43 \\ 0.43 & 0.25 \end{bmatrix}$.

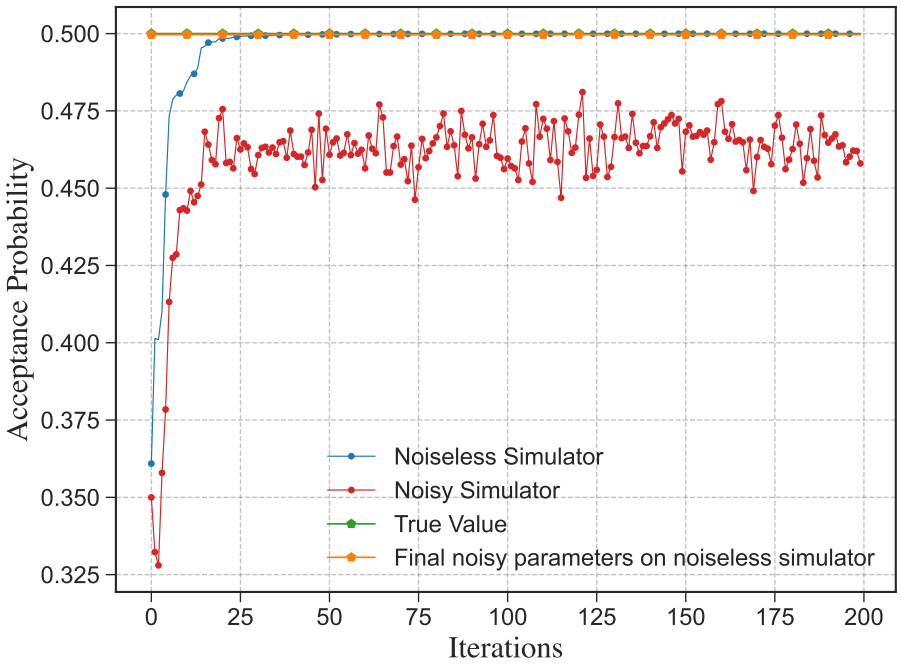


Figure 4.24: Example of the training process for testing collective-phase-symmetric extendibility of $|+\rangle\langle +|$.

responding more closely to the standard representation of C_3: $\{e \to \mathbb{I}, a \to \text{SWAP} \circ \text{CNOT}, b \to \text{SWAP} \circ \text{CNOT} \circ \text{SWAP} \circ \text{CNOT}\}$. The C_3 group has three elements, and thus, the $|+\rangle_C$ state is a uniform superposition of three elements. We use two qubits and the same unitary U_3 shown in Figure 4.20 to generate an equal

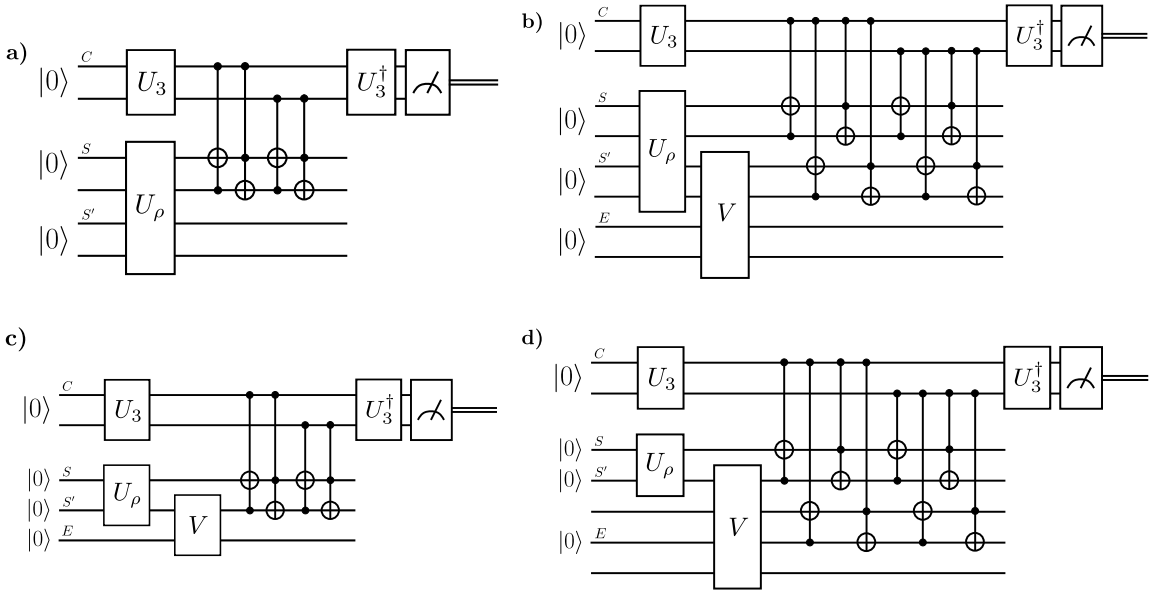


Figure 4.25: Symmetry tests for the C_3 group: a) G-Bose symmetry, b) G-symmetry, c) G-Bose symmetric extendibility, and d) G-symmetric extendibility.

superposition of three elements:

$$U_3 |00\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |11\rangle). \tag{4.187}$$

The control register states need to be mapped to group elements. We employ the mapping $\{|00\rangle \to e, |01\rangle \to a, |11\rangle \to b\}$ for our circuit constructions. The circuits required for all tests are given in Figure 4.25.

G-Bose symmetry

Figure 4.25a) shows the circuit that tests for G-Bose symmetry. Table 4.16 shows the results for various input states. The true fidelity value is calculated using (4.45), where Π_S^G is defined in (4.4).

State	True Fidelity	Noiseless	Noisy
$\|00\rangle\langle 00\|$	1.0	1.0000	0.8415
$\|-+\rangle\langle -+\|$	0.3333	0.3333	0.3408
ρ	1.0	1.0000	0.8524
$\pi^{\otimes 2}$	0.5	0.5000	0.4698

Table 4.16: Results of C_3-Bose symmetry tests. The state ρ is defined as $|\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{\sqrt{3}}(|01\rangle + |10\rangle + |11\rangle)$.

G-symmetry

A circuit that tests for G-symmetry is shown in Figure 4.25b). It involves variational parameters, and an example of the training process is shown in Figure 4.26. Table 4.17 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.121).

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|-+\rangle\langle -+\|$	0.3339	0.3333	0.3084	0.3333
Φ^+	0.6666	0.6666	0.5118	0.6639
ρ	0.7778	0.7775	0.5694	0.7760
$\pi^{\otimes 2}$	1.0000	0.9998	0.6756	0.9864

Table 4.17: Results of C_3-symmetry tests. The state ρ is defined as $|\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |10\rangle)$.

G-Bose symmetric extendibility

A circuit that tests for G-Bose symmetric extendibility is shown in Figure 4.25c). It involves variational parameters, and an example of the training process is shown in Figure 4.27. Table 4.18 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.122).

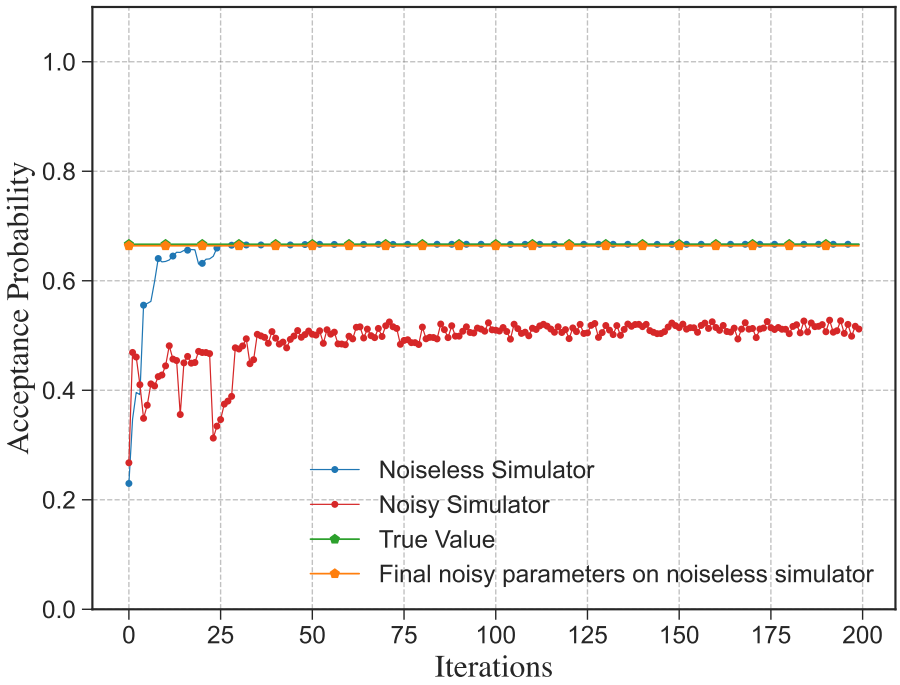


Figure 4.26: Example of the training process for testing C_3-symmetry of Φ^+. We see that the training exhibits a noise resilience.

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|0\rangle\langle 0\|$	0.6670	0.6667	0.5662	0.6665
π	1.0000	1.0000	0.8066	0.9979
ρ	0.8382	0.8380	0.7093	0.8377

Table 4.18: Results of C_3-Bose symmetric extendibility tests. The state ρ is defined as $|\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{2}(\sqrt{3}\,|0\rangle - |1\rangle)$.

G-symmetric extendibility

A circuit that tests for G-symmetric extendibility is shown in Figure 4.25d). It involves variational parameters, and an example of the training process is shown in Figure 4.28. Table 4.19 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in

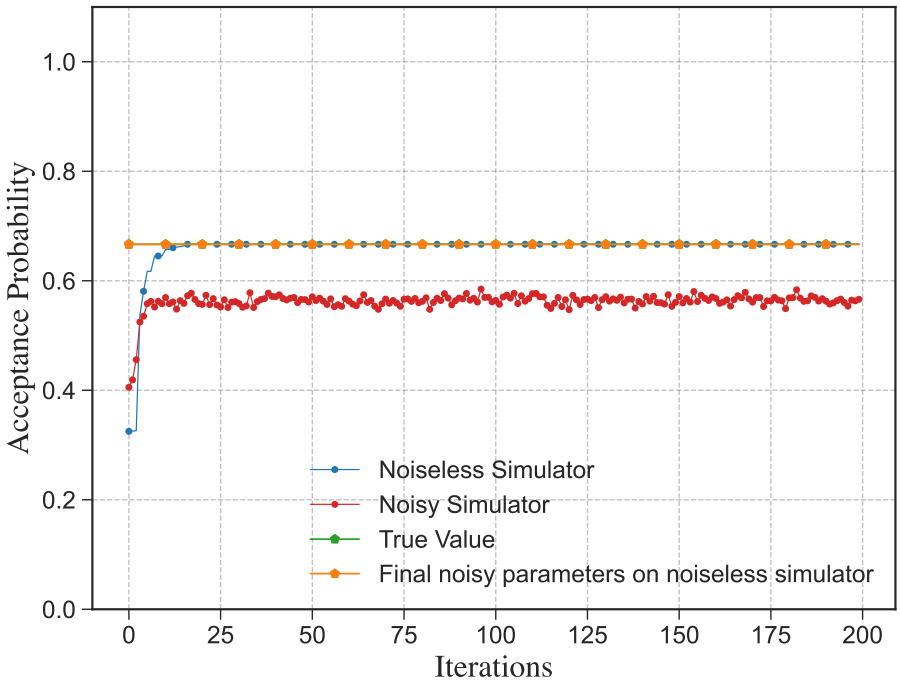


Figure 4.27: Example of the training process for testing C_3-Bose symmetric extendibility of $|1\rangle\langle 1|$. We see that the training exhibits a noise resilience.

(4.123).

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|1\rangle\langle 1\|$	0.6667	0.6660	0.4809	0.6620
π	1.0000	0.9942	0.6818	0.9812
ρ	0.8383	0.8322	0.5992	0.8327

Table 4.19: Results of C_3-symmetric extendibility tests. The state ρ is defined as $|\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{2}(\sqrt{3}\,|0\rangle - |1\rangle)$.

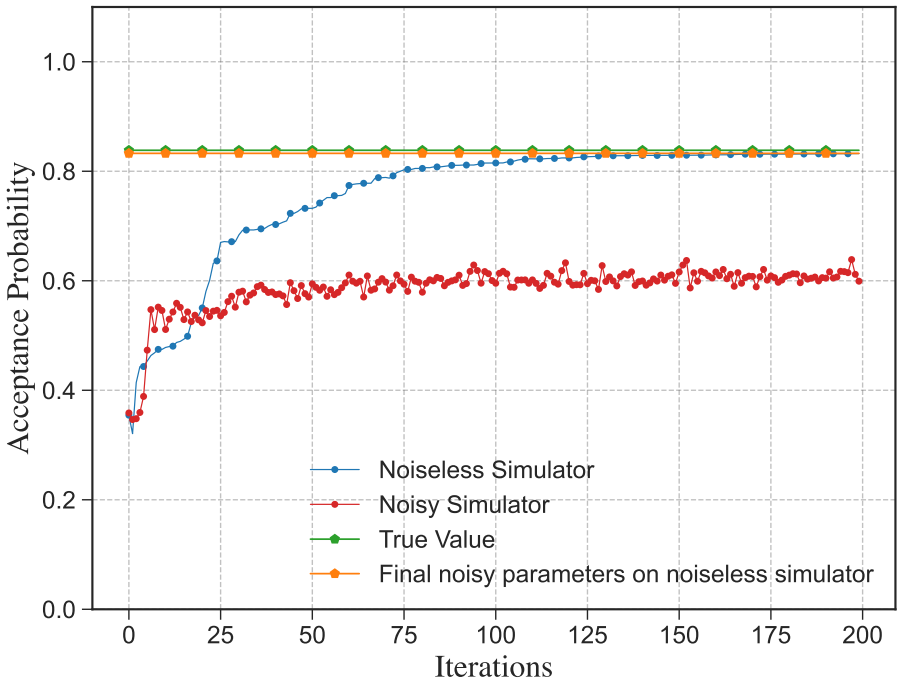


Figure 4.28: Example of the training process for testing C_3-symmetric extendibility of $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = \frac{1}{2}(\sqrt{3}\,|0\rangle - |1\rangle)$. We see that the training exhibits a noise resilience.

4.5.6 Cyclic group C_4

In this section, we consider C_4, the cyclic group on four elements. Again, as an abelian group, there exists a one-dimensional representation that we choose not to employ here. Instead, we consider again a two-qubit representation.

The group table for C_4 is given by

Group element	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

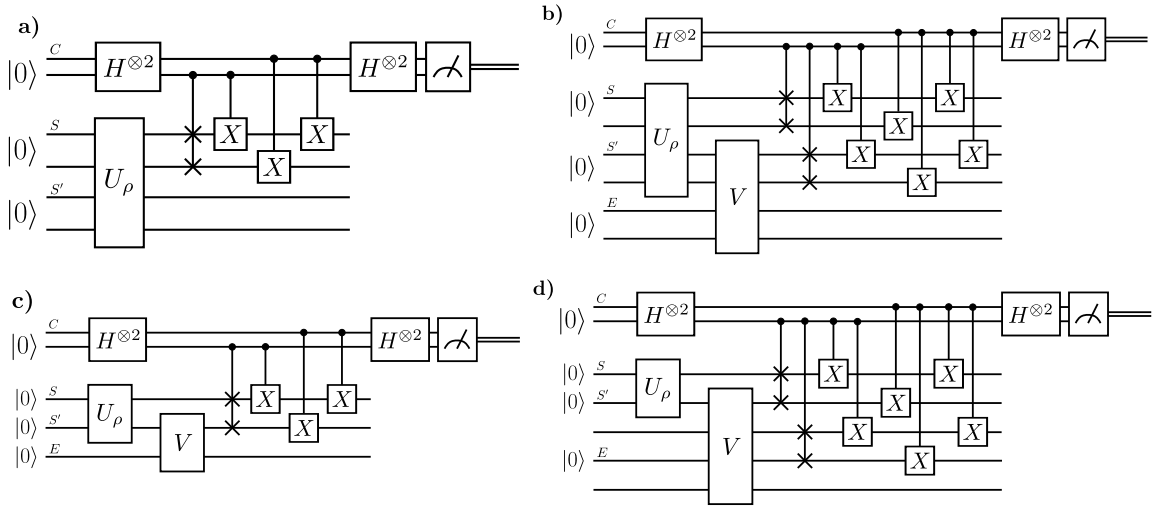


Figure 4.29: Symmetry tests for the C_4 group: a) G-Bose symmetry, b) G-symmetry, c) G-Bose symmetric extendibility, and d) G-symmetric extendibility.

This group has a two-qubit unitary representation $\{e \to \mathbb{I}, a \to X_0 \circ \text{SWAP}, b \to X_0 X_1, c \to X_1 \circ \text{SWAP}\}$, where X_i denotes the Pauli σ_x operator acting on qubit i, for $i \in \{0, 1\}$. The C_4 group has four elements, and thus, the $|+\rangle_C$ state is a uniform superposition of four elements. We use two qubits and the Hadamard gate to generate the control state, as follows:

$$H^{\otimes 2} |00\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) . \tag{4.188}$$

The control register states need to be mapped to group elements. We employ the mapping $\{|00\rangle \to e, |01\rangle \to a, |10\rangle \to b, |11\rangle \to c\}$ for our circuit constructions.

G-Bose symmetry

Figure 4.29a) shows a circuit that tests for G-Bose symmetry. Table 4.20 shows the results for various input states. The true fidelity value is calculated using (4.45), where Π_S^G is defined in (4.4).

State	True Fidelity	Noiseless	Noisy
$\|00\rangle\langle 00\|$	0.25	0.2500	0.2579
$\|++\rangle\langle ++\|$	1.0	1.0000	0.9276
$\|+0\rangle\langle +0\|$	0.5	0.5000	0.5002
$\pi^{\otimes 2}$	0.25	0.2500	0.2449

Table 4.20: Results of C_4-Bose symmetry tests.

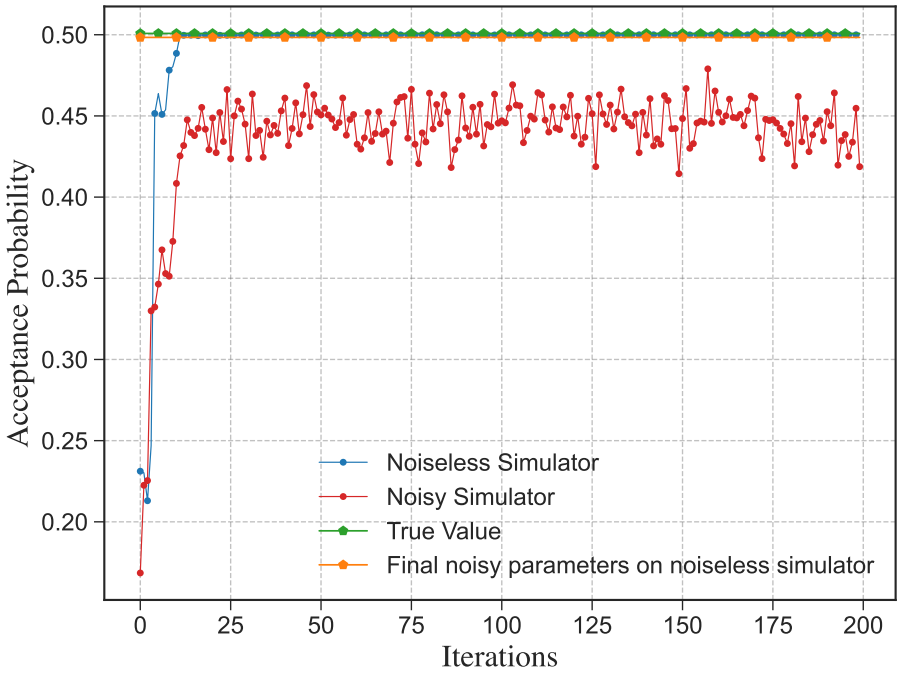


Figure 4.30: Example of the training process for testing C_4-symmetry of $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = |+-\rangle$. We see that the training exhibits a noise resilience.

G-symmetry

A circuit that tests for G-symmetry is shown in Figure 4.29b). It involves variational parameters, and an example of the training process is shown in Figure 4.30. Table 4.21 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.121).

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|00\rangle\langle 00\|$	0.2502	0.2500	0.2562	0.2500
$\|+-\rangle\langle -+\|$	0.5008	0.5000	0.4187	0.4984
$\pi \otimes \|0\rangle\langle 0\|$	0.7501	0.7498	0.6140	0.7480
$\pi^{\otimes 2}$	1.0000	0.9992	0.7606	0.9912

Table 4.21: Results of C_4-symmetry tests.

G-Bose symmetric extendibility

A circuit that tests for G-Bose symmetric extendibility is shown in Figure 4.29c). It involves variational parameters, and an example of the training process is shown in Figure 4.31. Table 4.22 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.122).

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|0\rangle\langle 0\|$	0.5000	0.5000	0.4671	0.4995
$\|+\rangle\langle +\|$	1.0000	1.0000	0.9195	1.0000
ρ	0.9330	0.9330	0.8689	0.9329

Table 4.22: Results of C_4-Bose symmetric extendibility tests. The state ρ is defined as $\begin{bmatrix} 0.75 & 0.4330 \\ 0.4430 & 0.25 \end{bmatrix}$.

G-symmetric extendibility

A circuit that tests for G-symmetric extendibility is shown in Figure 4.29d). It involves variational parameters, and an example of the training process is shown in Figure 4.32. Table 4.23 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.123).

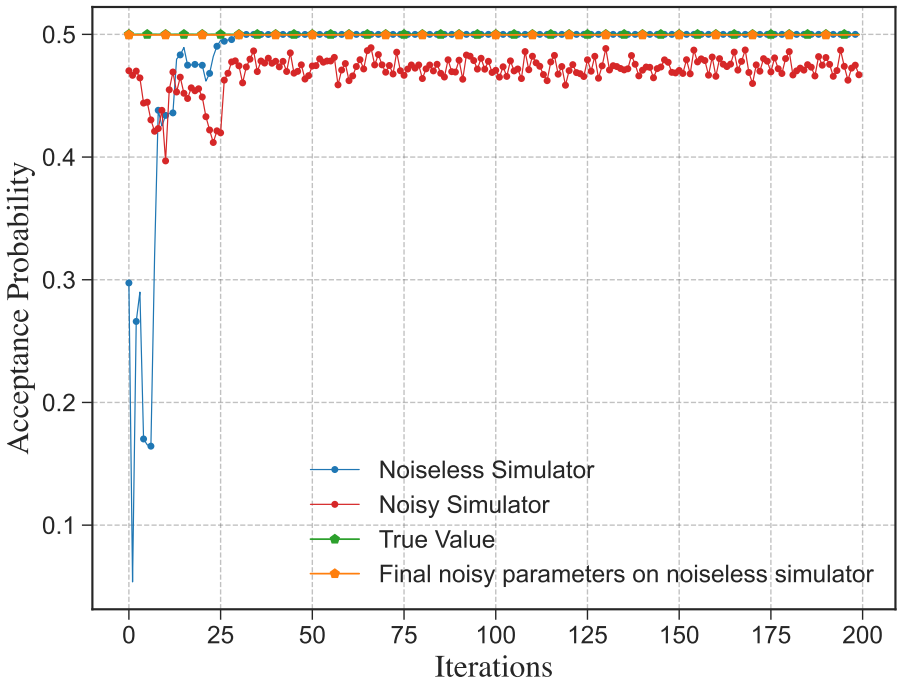


Figure 4.31: Example of the training process for testing C_4-Bose symmetric extendibility of $|00\rangle\langle 00|$. We see that the training exhibits a noise resilience.

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|0\rangle\langle 0\|$	0.5000	0.4997	0.4191	0.4982
π	1.0000	0.9996	0.7608	0.9884
ρ	0.8535	0.8533	0.6838	0.8459

Table 4.23: Results of C_4-symmetric extendibility tests. The state ρ is defined as $\begin{bmatrix} 0.854 & 0 \\ 0 & 0.146 \end{bmatrix}$.

4.5.7 Quaternion group Q_8

The Quaternion group is defined as

$$Q_8 = \langle \bar{e}, i, j, k \mid \bar{e}^2 = e, i^2 = j^2 = k^2 = ijk = \bar{e} \rangle. \tag{4.189}$$

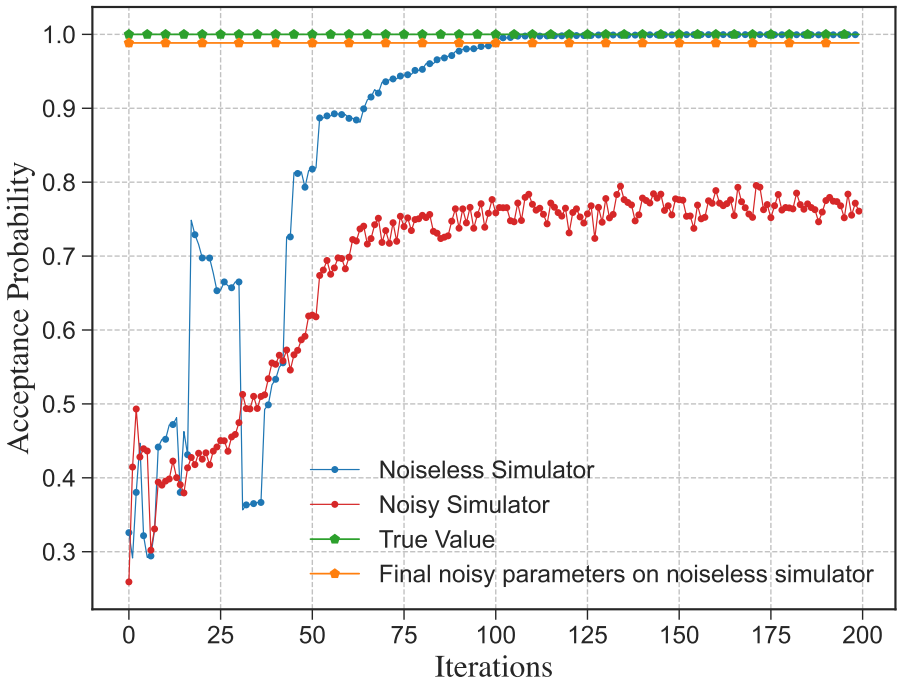


Figure 4.32: Example of the training process for testing C_4-symmetry extendibility of π. We see that the training exhibits a noise resilience.

The inverse elements of e, i, j, k are given by $\bar{e}, \bar{i}, \bar{j}, \bar{k}$ respectively. The Q_8 group has a two-qubit unitary representation

$$\begin{aligned} e &= \begin{bmatrix} \mathbb{I} & 0 \\ 0 & \mathbb{I} \end{bmatrix} \quad , \quad \bar{e} = \begin{bmatrix} \mathbb{I} & 0 \\ 0 & -\mathbb{I} \end{bmatrix}, \\ i &= \begin{bmatrix} \mathbb{I} & 0 \\ 0 & -i\sigma_x \end{bmatrix} \quad , \quad \bar{i} = \begin{bmatrix} \mathbb{I} & 0 \\ 0 & i\sigma_x \end{bmatrix}, \\ j &= \begin{bmatrix} \mathbb{I} & 0 \\ 0 & -i\sigma_y \end{bmatrix} \quad , \quad \bar{j} = \begin{bmatrix} \mathbb{I} & 0 \\ 0 & i\sigma_y \end{bmatrix}, \\ k &= \begin{bmatrix} \mathbb{I} & 0 \\ 0 & -i\sigma_z \end{bmatrix} \quad , \quad \bar{k} = \begin{bmatrix} \mathbb{I} & 0 \\ 0 & i\sigma_z \end{bmatrix}. \end{aligned} \tag{4.190}$$

The Q_8 group has eight elements and thus, the $|+\rangle_C$ state is a uniform superposition of eight elements. We use three qubits and the Hadamard gate to generate

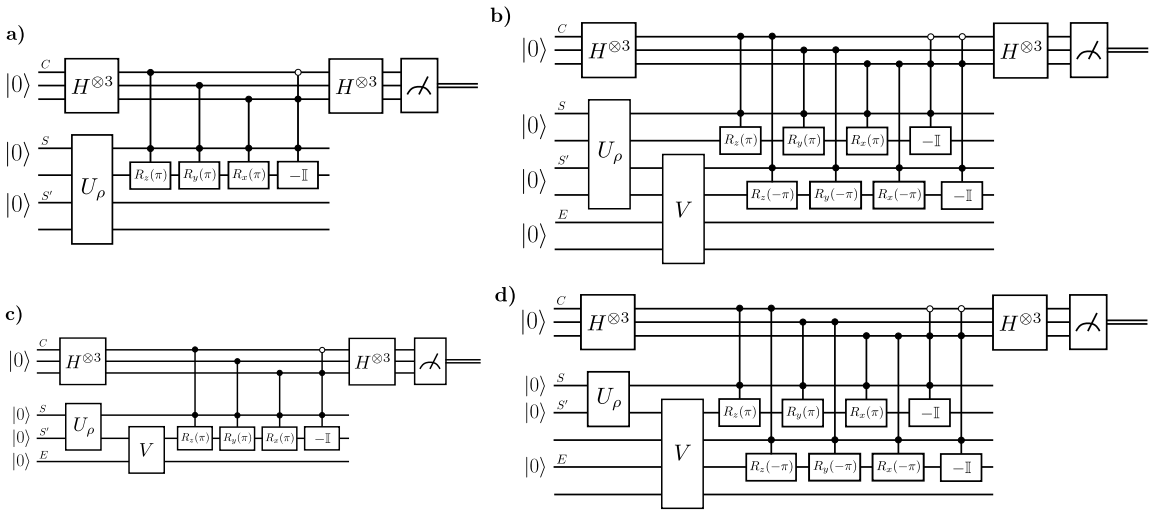


Figure 4.33: Symmetry tests for the Q_8 group: a) G-Bose symmetry, b) G-symmetry, c) G-Bose symmetric extendibility, and d) G-symmetric extendibility.

it as follows:

$$H^{\otimes 3}|000\rangle = \frac{1}{\sqrt{8}}\Big(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\Big). \quad (4.191)$$

The control register states need to be mapped to group elements. We employ the mapping $\{|000\rangle \to e, |001\rangle \to \bar{i}, |010\rangle \to j, |011\rangle \to \bar{k}, |100\rangle \to k, |101\rangle \to \bar{j}, |110\rangle \to i, |111\rangle \to \bar{e}\}$ for our circuit constructions.

G-Bose symmetry

Figure 4.33a) shows the circuit needed to test for G-Bose symmetry. Table 4.24 shows the results for various input states. The true fidelity value is calculated using (4.45), where Π_S^G is defined in (4.4).

G-symmetry

A circuit that tests for G-symmetry is shown in Figure 4.33b). It involves variational parameters, and an example of the training process is shown in Figure 4.34.

State	True Fidelity	Noiseless	Noisy
$\|00\rangle\langle 00\|$	1.0	1.0000	0.7416
$\|1+\rangle\langle 1+\|$	0.0	0.0000	0.0709
$\|+0\rangle\langle 0+\|$	0.5	0.4999	0.3961
$\pi^{\otimes 2}$	0.5	0.4999	0.3842

Table 4.24: Results of Q_8-Bose symmetry tests.

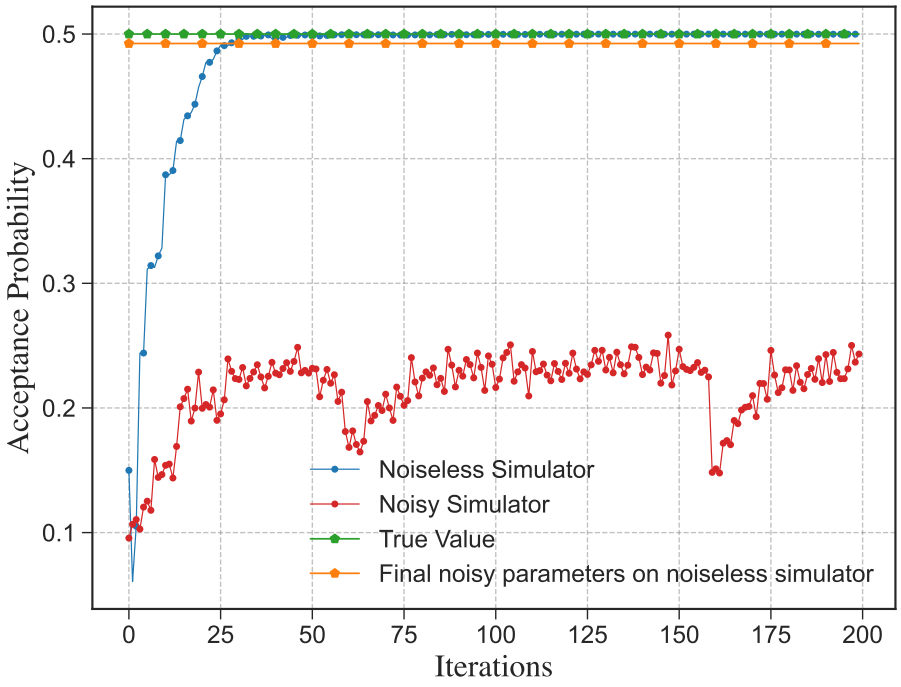


Figure 4.34: Example of the training process for testing Q_8-symmetry of $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = |1+\rangle$. We see that the training exhibits a noise resilience.

Table 4.25 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.121).

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|00\rangle\langle 00\|$	1.0000	0.9998	0.5430	0.9960
$\|1+\rangle\langle 1+\|$	0.5000	0.4999	0.2433	0.4924
ρ	0.7500	0.7499	0.4581	0.7447
$\pi^{\otimes 2}$	1.0000	0.9998	0.2448	0.3774

Table 4.25: Results of Q_8-symmetry tests. The state ρ is defined as $|\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{2}(\sqrt{3}\,|00\rangle + |11\rangle)$.

G-Bose symmetric extendibility

A circuit that tests for G-Bose symmetric extendibility is shown in Figure 4.33c). It involves variational parameters, and an example of the training process is shown in Figure 4.35. Table 4.26 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.122).

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|0\rangle\langle 0\|$	1.0000	1.0000	0.7161	1.0000
π	0.5000	0.5000	0.4086	0.5000
ρ	0.9330	0.9330	0.6519	0.9330

Table 4.26: Results of Q_8-Bose symmetric extendibility tests. The state ρ is defined as $\begin{bmatrix} 0.933 & 0.25 \\ 0.25 & 0.067 \end{bmatrix}$.

G-symmetric extendibility

A circuit that tests for G-symmetric extendibility is shown in Figure 4.33d). It involves variational parameters, and an example of the training process is shown in Figure 4.36. Table 4.27 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.123).

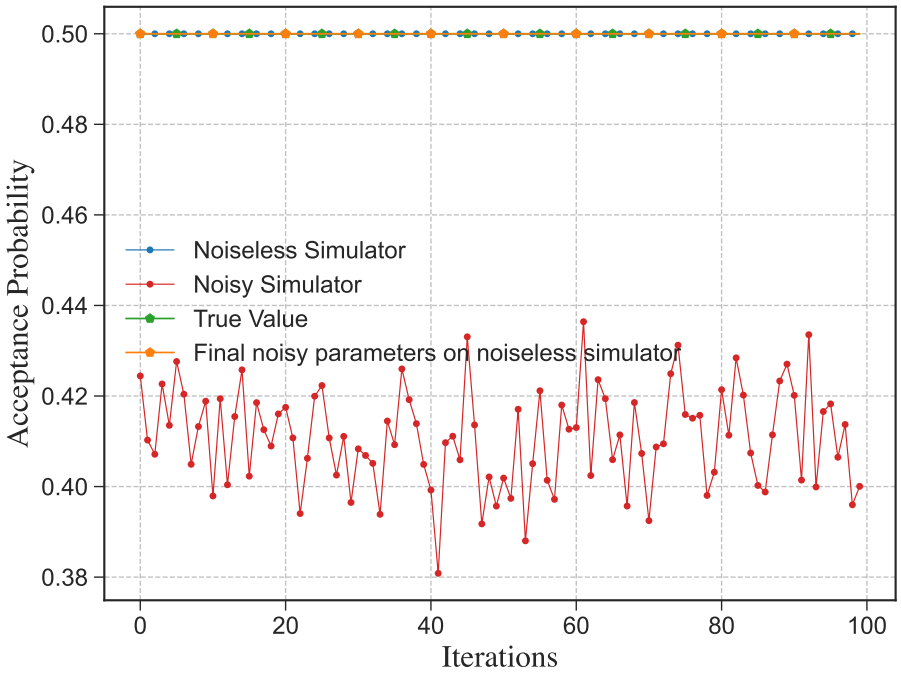


Figure 4.35: Example of the training process for testing Q_8-Bose symmetric extendibility of $|+\rangle\langle+|$. We see that the training exhibits a noise resilience.

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|0\rangle\langle 0\|$	1.0000	0.9995	0.5951	0.9964
$\|+\rangle\langle+\|$	0.5000	0.5000	0.2918	0.4974
π	1.0	0.9985	0.4605	0.8778

Table 4.27: Results of Q_8-symmetric extendibility tests.

4.5.8 k-Extendibility and k-Bose extendibility

As seen in Examples 4.1 and 4.2, k-extendibility and k-Bose extendibility are special cases of G-symmetric extendibility and G-Bose symmetric extendibility, respectively. In this section, we look at the cases of two and three extending subsystems.

As seen in (4.13)–(4.16), $U_{RS}(g) = \mathbb{I}_A \otimes W_{B_1\cdots B_k}(\pi)$, where $W_{B_1\cdots B_k}(\pi)$ is a unitary

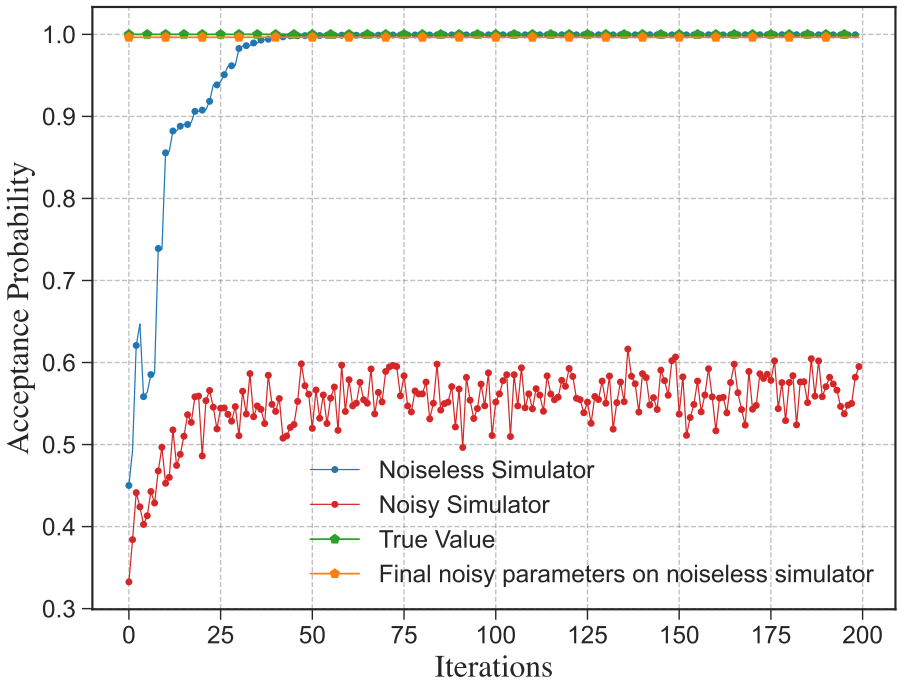


Figure 4.36: Example of the training process for testing Q_8-symmetry extendibility of $|0\rangle\langle 0|$. We see that the training exhibits a noise resilience.

representation of the symmetric group S_k. Thus, given a unitary representation of S_k, we can test for the required symmetries.

The S_2 group has two elements, and the group table is given by

Group element	e	a
e	e	a
a	a	e

The standard representation of S_2 translates easily to a two-qubit unitary representation with $\{e \to \mathbb{I}, a \to F\}$, where F is the SWAP gate. In fact, throughout this section, we will consider unitary representations corresponding to system permutations in a direct correspondence with the standard representations of S_k. Using this definition, let $U_{RS}(e) = \mathbb{I}_A \otimes \mathbb{I}_{B_1B_2}$ and $U_{RS}(a) = \mathbb{I}_A \otimes F_{B_1B_2}$. Since we have two

elements, the $|+\rangle_C$ state is a uniform superposition of two elements. We thus use one qubit and the Hadamard gate to generate the necessary state:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \tag{4.192}$$

The control register states need to be mapped to group elements; for this, we employ the mapping $\{|0\rangle \to e, |1\rangle \to a\}$ for our circuit constructions.

Similarly, the S_3 group has six elements and the group table is given by

Group element	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

The S_3 group has a three-qubit unitary representation $\{e \to \mathbb{I}, a \to F_{23}, b \to F_{13}, c \to F_{12}, d \to F_{12}F_{23}, f \to F_{13}F_{23}\}$, where F_{ij} is the SWAP gate between qubits i and j. Since we have six elements, the $|+\rangle_C$ state is a uniform superposition of six elements. We use three qubits and the same unitary U_d used to generate the superposition for the triangular dihedral group, as shown in Figure 4.2, to generate an equal superposition of six elements,

$$U_d|000\rangle = \frac{1}{\sqrt{6}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle). \tag{4.193}$$

The control register states need to be mapped to group elements, and we do so via the mapping $\{|000\rangle \to e, |001\rangle \to a, |010\rangle \to b, |011\rangle \to f, |100\rangle \to c, |101\rangle \to d\}$.

Two-Bose extendibility

A circuit that tests for two-Bose extendibility is shown in Figure 4.37a). It involves variational parameters, and an example of the training process is shown in Figure 4.38. Table 4.28 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.122).

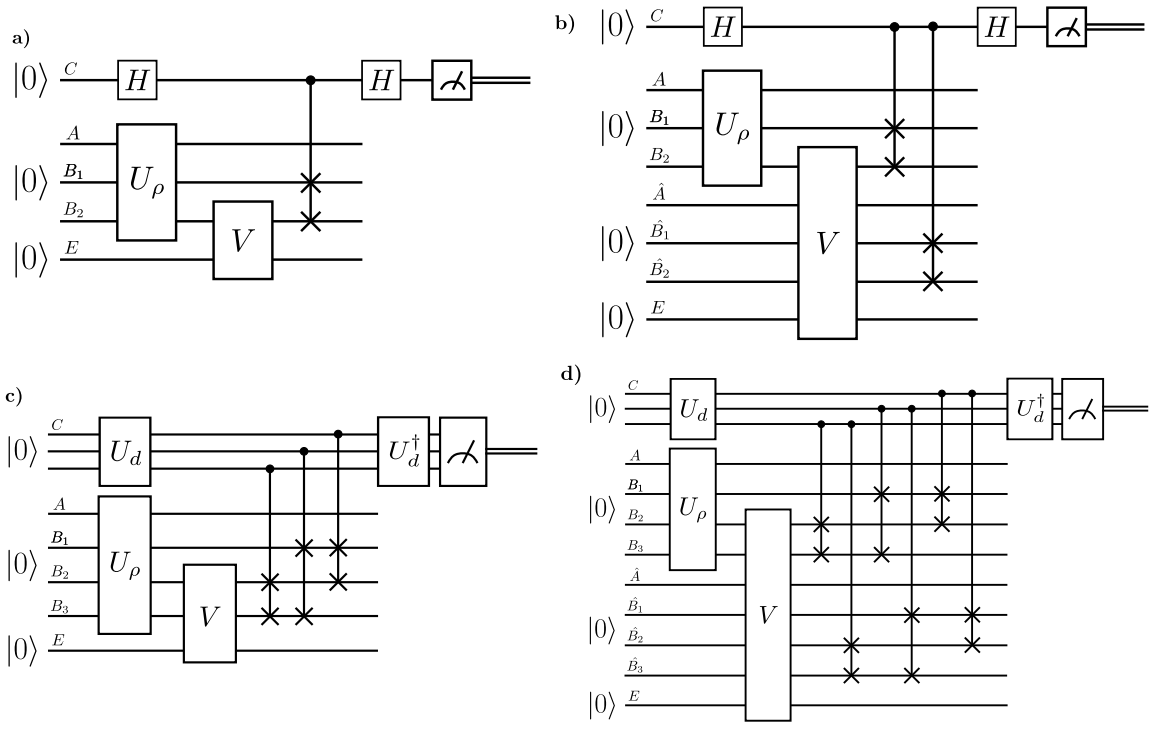


Figure 4.37: Tests for extendibility: a) two-Bose extendibility, b) two-extendibility, c) three-Bose extendibility, and d) three-extendibility.

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|00\rangle\langle 00\|$	1.0000	1.0000	0.9544	0.9995
ρ	1.0000	1.0000	0.9584	0.9995
Ψ^+	0.7500	0.7500	0.7256	0.7500

Table 4.28: Results of S_2-Bose symmetric extendibility tests. The state ρ is defined as $\frac{3}{4}|00\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11|$.

Two-Extendibility

Similar to the non-extended cases, it is simpler to test if a state exhibits G-BSE—or, in this case, if the state is k-Bose-symmetric extendible—than to test if it is symmetric extendible. This is reflected in Figure 4.37b), which shows a test for 2-BSE. The circuit involves variational parameters, and an example of the training

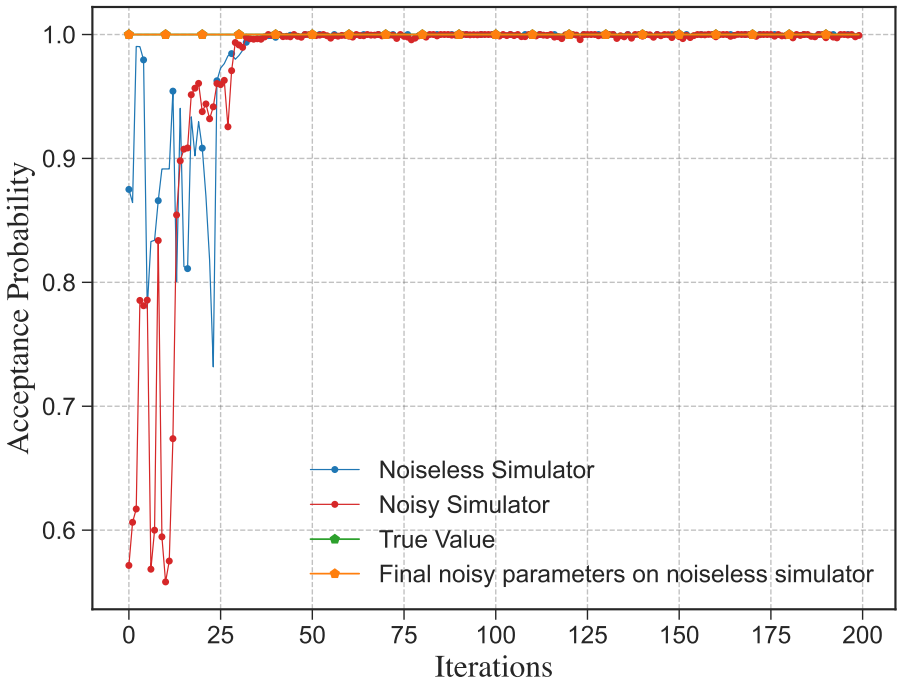


Figure 4.38: Example of the training process for testing two-Bose extendibility of $\rho = \frac{3}{4}|00\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11|$. We see that the training exhibits a noise resilience.

process is shown in Figure 4.39. Table 4.29 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.123).

Three-Bose Extendibility

A circuit that tests for three-Bose extendibility is shown in Figure 4.37c). It involves variational parameters, and an example of the training process is shown in Figure 4.40. Table 4.30 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.122).

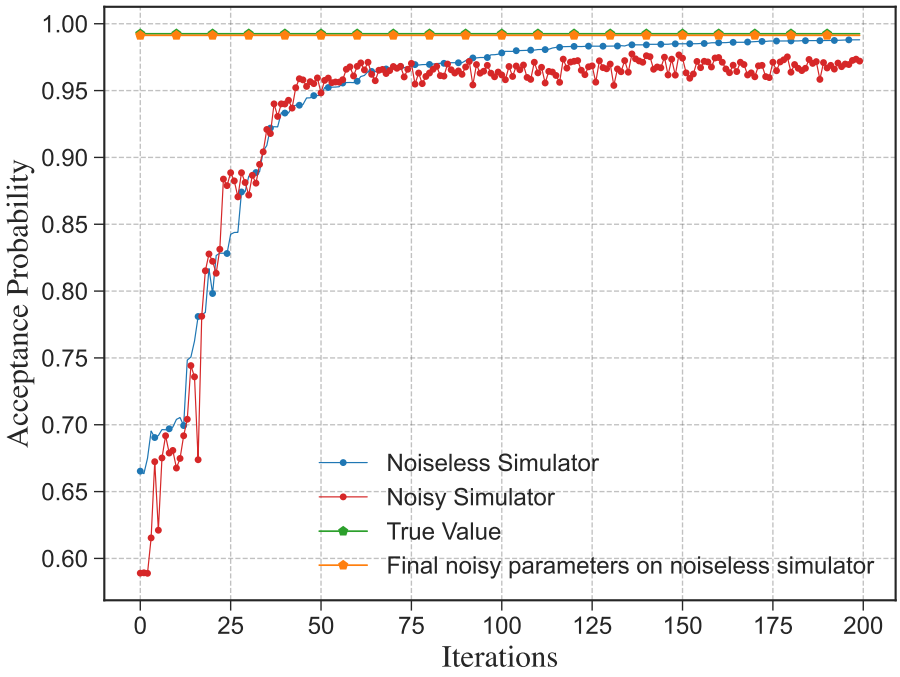


Figure 4.39: Example of the training process for testing two-extendibility of $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{6}}(|00\rangle + |01\rangle + |10\rangle)$. We see that the training exhibits a noise resilience.

Three-Extendibility

A circuit that tests for three-extendibility is shown in Figure 4.37d). It involves variational parameters, and an example of the training process is shown in Figure 4.41. Table 4.31 shows the final results after training for various input states. The true fidelity is calculated using the semi-definite program given in (4.123).

For all of the above cases, we see that results achieved via parameterized circuit substitutions for the prover demonstrate noise resilience, and thus give some confidence for practical applications. In this final case, we have shown explicitly how our algorithm allows for tests of k-extendibility and related quantities. While only small systems are considered here, this is a limitation of current hardware more so than of the algorithm itself. Indeed, it would be interesting to observe the performance of this algorithm on higher fidelity machines with more qubits,

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|00\rangle\langle 00\|$	1.0000	0.9991	0.9267	0.9960
ρ	0.9925	0.9901	0.9720	0.9913
Ψ^+	0.7506	0.7498	0.6959	0.7480

Table 4.29: Results of S_2-symmetric extendibility tests. The state ρ is defined as $|\psi\rangle\langle\psi|$ where $|\psi\rangle = \frac{1}{\sqrt{2}}|11\rangle + \frac{1}{\sqrt{6}}(|00\rangle + |01\rangle + |10\rangle)$. The reduced state of ρ has eigenvalues $\frac{1}{6}\left(3 + \sqrt{5 + 2\sqrt{3}}\right) \approx 0.985$ and $\frac{1}{6}\left(3 - \sqrt{5 + 2\sqrt{3}}\right) \approx 0.015$. It is thus not so entangled, and we expect its two-extendible fidelity to be close to one.

State	True Fidelity	Noiseless	Noisy	Noise Resilient
$\|00\rangle\langle 00\|$	1.0000	0.9999	0.8644	0.9982
ρ	1.0000	0.9994	0.8403	0.9851
Ψ^+	0.6675	0.6667	0.5666	0.6666

Table 4.30: Results of S_3-Bose symmetric extendibility tests. The state ρ is defined as $\frac{3}{4}|00\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11|$.

which could possibly be achievable in the near future.

4.6 Estimating symmetry measures as complexity classes

In this section, we present results connecting the quantum complexity classes hierarchy and different symmetry testing algorithms. Figure 4.42 provides all the

State	True Fidelity	Noiseless
$\|00\rangle\langle 00\|$	1.0000	0.9970
ρ	1.0000	0.9988
Ψ^+	0.6670	0.6650

Table 4.31: Results of S_3-symmetric extendibility tests. Here, $\rho = \frac{3}{4}|00\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11|$.

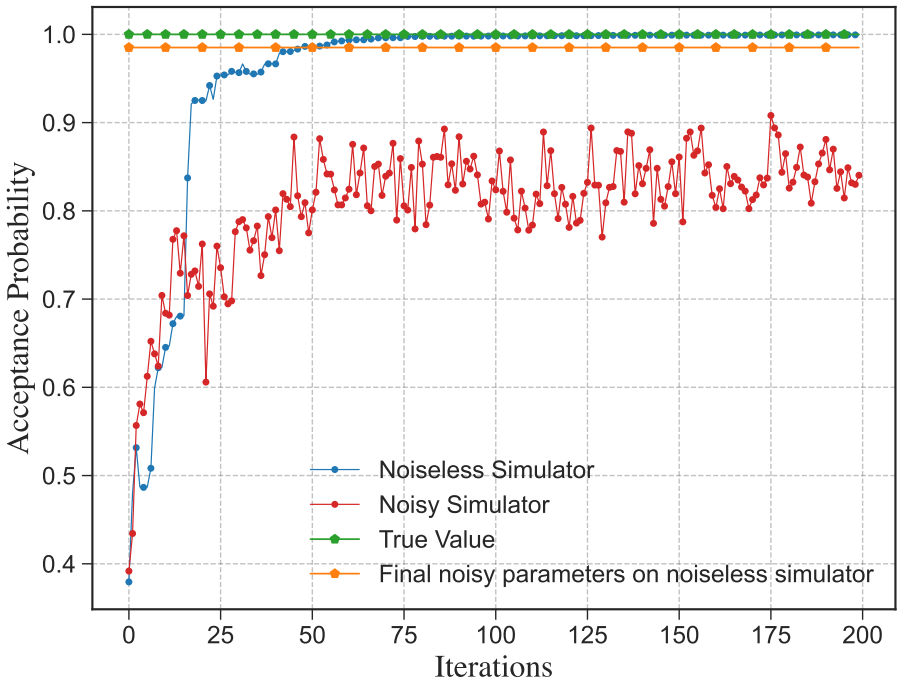


Figure 4.40: Example of the training process for testing three-Bose extendibility of $\rho = \frac{3}{4}|00\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11|$. We see that the training exhibits a noise resilience.

results and details of our paper at a glance and places some of them in a containment diagram for ease of access. The results presented here all have a similar proof idea – prove that the promise problem is in the complexity class of interest and that the problem is hard for the same complexity class. For all the hardness results, we either map an existing complete problem to the problem of interest, or we show that a generic problem that defines the class can be rewritten in terms of the problem of interest. In the latter case, we select the group and the input state such that the acceptance probability of the problem maps to the corresponding symmetry quantity. In most cases, we pick the group to be $C_2 = \{I, V\}$, with $V^2 = I$. We find that this is the simplest choice of the group G. The choice of V is then "reverse-engineered" in a way to match the symmetry quantity. While this preview discussion might seem a bit abstract as of now, we make the concepts more concrete in the specific examples that follow, with the first being discussed in more detail around (4.196)–(4.198).

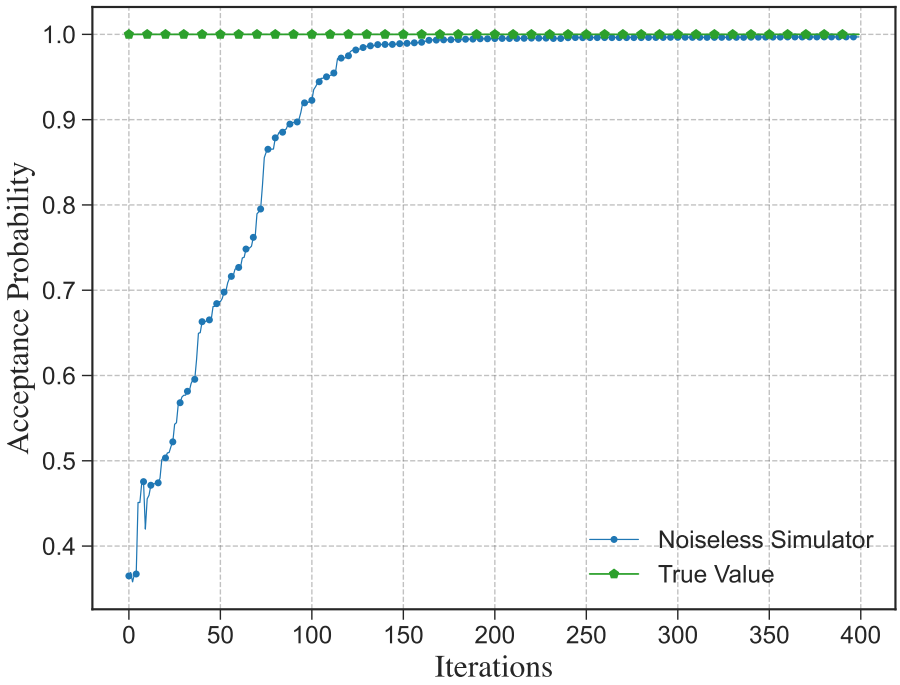


Figure 4.41: Example of the training process for testing three-extendibility of $|00\rangle\langle 00|$.

4.6.1 Testing G-Bose symmetry of a state is BQP-Complete

In this section, we show that testing the G-Bose Symmetry of a state is BQP-Complete. We begin now by specifying this problem statement in precise terms.

Problem 4.1 [(α,β)-*State-G-Bose-Symmetry*]. *Let α and β be such that $0 \leq \beta < \alpha \leq 1$. Given are descriptions of a circuit U^{ρ}_{RS} that generates a purification of a state ρ_S and circuit descriptions of a representation $\{U_S(g)\}_{g\in G}$ of a group G. Decide which of the following holds:*

$$\textit{Yes:} \quad \mathrm{Tr}\left[\Pi^G_S \rho_S\right] \geq \alpha, \tag{4.194}$$

$$\textit{No:} \quad \mathrm{Tr}\left[\Pi^G_S \rho_S\right] \leq \beta, \tag{4.195}$$

where the group representation projector Π^G_S is defined in (4.4).

As observed in [LRW23, Section 3.1], the measure $\mathrm{Tr}\left[\Pi^G_S \rho_S\right]$ is a faithful sym-

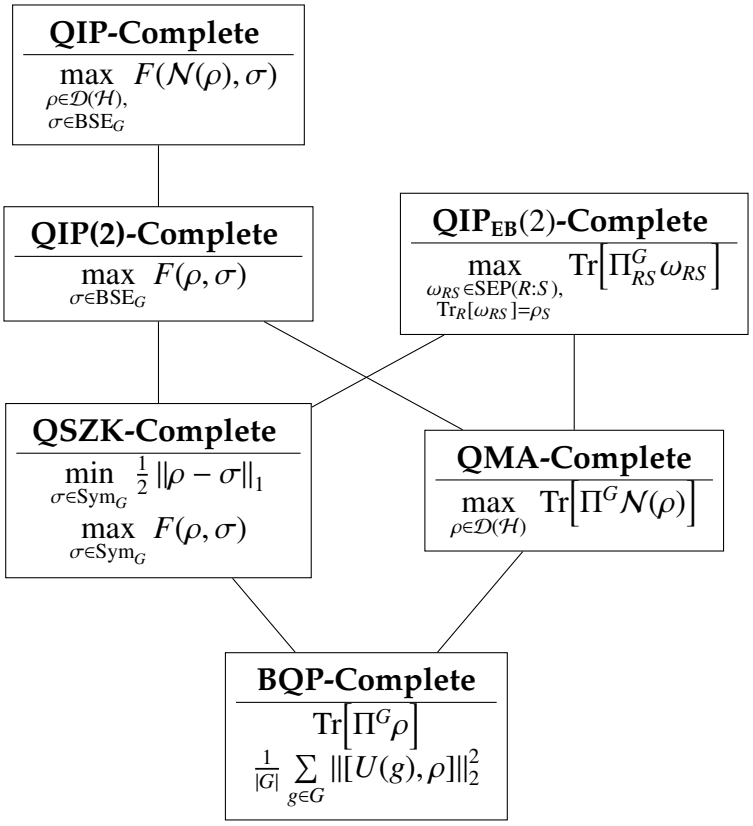


Figure 4.42: List of complete symmetry-testing problems and the corresponding quantum complexity class. The cells are organized such that if a cell is connected to a cell above it, the complexity class for the lower cell is a subset of that for the higher cell. For example, QMA is a subset of QIP(2).

metry measure, in the sense that it is equal to one if and only if the state ρ_S is Bose-symmetric.

Theorem 4.6. *The promise problem State-G-Bose-Symmetry is BQP-Complete.*

1. (α,β)*-State-G-Bose-Symmetry is in BQP for all* $\beta<\alpha$*, whenever the gap between* α *and* β *is larger than an inverse polynomial in the input length.*
2. $(1-\varepsilon,\varepsilon)$*-State-G-Bose-Symmetry is BQP-Hard, even when* ε *decays exponentially in the input length.*

Thus, (α,β)*-State-G-Bose-Symmetry is BQP-Complete for all* (α,β) *such that* $0\leq\beta<$

$\alpha \leq 1$.

Remark 4.3. *In the statement of Theorem 4.6, the first part indicates the largest range of parameters for which we can show that the problem is contained in BQP. Similarly, the second part indicates the largest range of parameters for which we can show that the problem is BQP-hard. Both of these parameter ranges include the case when α and β are constants. As such, this leads to the final statement above that the problem is BQP-complete for constant values of α and β satisfying the inequality constraint given. We present all subsequent theorems in a similar way.*

Proof of Theorem 4.6. To show that the problem is BQP-Complete, we need to demonstrate two facts: first, that the problem is in BQP, and second, that it is BQP-Hard. Let us begin by proving that the problem is in BQP. In [Har05, Chapter 8] (see also [LRW23, Algorithm 1]), an algorithm was proposed to test for G-Bose symmetry of a state ρ_S given a circuit description of unitary that generates a purification of the state and circuit descriptions of a unitary representation of a group G, $\{U(g)\}_{g\in G}$. Since the algorithm can be performed efficiently, the problem is contained in BQP.

Next, we show that any problem in the BQP class can be reduced to an instance of this problem. The acceptance and rejection probabilities are encoded in the state of the decision qubit, with zero indicating acceptance. Now, we need to map this problem to an instance of State-G-Bose-Symmetry; i.e., using the circuit descriptions for a general BQP algorithm, we need to define a state $\rho_{S'}$ and a unitary representation $\{U_{S'}(g)\}_{g\in G}$, and also show how the symmetry-testing condition $\mathrm{Tr}[\Pi^G_{S'}\rho_{S'}]$ can be written in terms of the BQP algorithm's acceptance probability. To this end, we define the group G to be the cyclic group on two elements $C_2 = \{I, V\}$ such that $V^2 = I$, where V is simply given by

$$V_D = -Z_D, \tag{4.196}$$

and the input state to be

$$\rho_D = \mathrm{Tr}_G[Q_{SA\to DG}(|x\rangle\langle x|_S \otimes |0\rangle\langle 0|_A)(Q_{SA\to DG})^\dagger]. \tag{4.197}$$

As such, we are making the identification $S' \leftrightarrow D$ between the system label S' of a general symmetry-testing problem and the system D for a BQP algorithm. The group representation and circuit to generate ρ_D are thus efficiently implementable. Furthermore, the state of interest is just the state of the decision qubit, and the group projector for the unitary representation above is given by

$$\Pi^G_D = \frac{1}{2}(I_D - Z_D) = |1\rangle\langle 1|_D. \tag{4.198}$$

Furthermore, we find that the symmetry-testing condition $\mathrm{Tr}[\Pi_D^G \rho_D]$ maps to the BQP algorithm's acceptance probability as follows:

$$\begin{aligned}\mathrm{Tr}[\Pi_D^G \rho_D] &= \mathrm{Tr}[|1\rangle\langle 1|_D \rho_D] \\ &= \mathrm{Tr}[(|1\rangle\langle 1|_D \otimes I_G)(Q_{SA\to DG}(|x\rangle\langle x|_S \otimes |0\rangle\langle 0|_A)(Q_{SA\to DG})^\dagger)] \\ &= \| (\langle 1|_D \otimes I_G) Q_{SA\to DG} |x\rangle_S |0\rangle_A \|_2^2 . \end{aligned} \tag{4.199}$$

Comparing with (2.126), we observe that the acceptance probability of the BQP algorithm exactly matches the symmetry-testing condition of the constructed G-Bose symmetry-testing problem. As such, we have proven that any BQP problem can be efficiently mapped to a G-Bose symmetry test, concluding the proof. ■

4.6.2 Testing G-symmetry of a state using Hilbert–Schmidt norm is BQP-Complete

In this section, we show that testing the G-symmetry of a state using the Hilbert–Schmidt norm is BQP-Complete, and it is thus emblematic of the class of problems efficiently solvable using quantum computers.

Problem 4.2 [(α,β)-*State-HS-Symmetry*]. *Given are a circuit description of a unitary U_{RS}^{ρ} that generates a purification of the state ρ_S and circuit descriptions of a unitary representation $\{U_S(g)\}_{g\in G}$ of a group G. Let α and β be such that $0 \le \beta < \alpha \le \gamma$, where*

$$\gamma := 2\left(1 - \frac{1}{|G|}\right). \tag{4.200}$$

Decide which of the following holds:

$$\textit{Yes:} \quad \frac{1}{|G|}\sum_{g\in G} \|[U(g),\rho]\|_2^2 \le \beta, \tag{4.201}$$

$$\textit{No:} \quad \frac{1}{|G|}\sum_{g\in G} \|[U(g),\rho]\|_2^2 \ge \alpha, \tag{4.202}$$

where the Hilbert–Schmidt norm of a matrix A is defined as $\|A\|_2 := \sqrt{\mathrm{Tr}[A^\dagger A]}$.

As observed in [BRRW23, Section 1], the quantity in (4.201) is a faithful symmetry measure in the sense that it is equal to zero if and only if the state ρ is G-symmetric, as in Definition 4.1.

The quantity γ in (4.200) arises as a natural upper bound for $\frac{1}{|G|}\sum_{g\in G}\|[U(g),\rho]\|_2^2$ because

$$\begin{aligned}
&\frac{1}{|G|}\sum_{g\in G}\|[U(g),\rho]\|_2^2 \\
&= \frac{1}{|G|}\sum_{g\in G} 2\left(\mathrm{Tr}[\rho^2] - \mathrm{Tr}[\rho U(g)\rho U(g)^\dagger]\right) \\
&= \frac{1}{|G|}\sum_{g\in G, g\neq e} 2\left(\mathrm{Tr}[\rho^2] - \mathrm{Tr}[\rho U(g)\rho U(g)^\dagger]\right) \\
&\leq \gamma,
\end{aligned} \tag{4.203}$$

where the first equality follows from (4.204) below and the inequality follows because $\mathrm{Tr}[\rho^2] \leq 1$ and $\mathrm{Tr}[\rho U(g)\rho U(g)^\dagger] \geq 0$. Furthermore, the upper bound is saturated by choosing ρ to be $|0\rangle\langle 0|$ in a d-dimensional space and the unitary representation to be the Heisenberg–Weyl shift operators $\{X(x)\}_{x=0}^{d-1}$, such that $X(x)|0\rangle = |x\rangle$.

Theorem 4.7. *The promise problem State-HS-Symmetry is BQP-Complete.*

1. *(α,β)-State-HS-Symmetry is in BQP for all $\beta < \alpha$. (It is implicit that the gap between α and β is larger than an inverse polynomial in the input length.)*
2. *$(\gamma-\varepsilon,\varepsilon)$-State-HS-Symmetry is BQP-Hard, even when ε decays exponentially in the input length.*

Thus, (α,β)-State-HS-Symmetry is BQP-Complete for all (α,β) such that $0 \leq \beta < \alpha \leq \gamma$.

Proof. To show that the problem is BQP-Complete, we first show that it is in the BQP class and then show that it is BQP-Hard. For the first part, let us briefly recall the development from [BRRW23, Section 3.1]. Consider the following equalities:

$$\begin{aligned}
\|[U(g),\rho]\|_2^2 &= \|\rho U(g) - U(g)\rho\|_2^2 \\
&= \left\|\rho - U(g)\rho U(g)^\dagger\right\|_2^2 \\
&= \mathrm{Tr}[\rho^2] + \mathrm{Tr}[(U(g)\rho U(g)^\dagger)^2] - 2\,\mathrm{Tr}[\rho U(g)\rho U(g)^\dagger] \\
&= 2\left(\mathrm{Tr}[\rho^2] - \mathrm{Tr}[\rho U(g)\rho U(g)^\dagger]\right),
\end{aligned} \tag{4.204}$$

where the second equality is due to the unitary invariance of the Hilbert–Schmidt norm. Thus, we see that

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G}\|[U(g),\rho]\|_2^2 &= \frac{1}{|G|}\sum_{g\in G}2\left(\mathrm{Tr}[\rho^2]-\mathrm{Tr}[\rho U(g)\rho U(g)^\dagger]\right)\\ &= 2\left(\mathrm{Tr}[\rho^2]-\mathrm{Tr}[\rho\mathcal{T}_G(\rho)]\right)\\ &= 2\left(\mathrm{Tr}[\mathrm{SWAP}(\rho\otimes\rho)]-\mathrm{Tr}[\mathrm{SWAP}(\rho\otimes\mathcal{T}_G(\rho))]\right),\end{aligned} \tag{4.205}$$

where $\mathcal{T}_G$ is the twirl channel given by

$$\mathcal{T}_G(\cdot) := \frac{1}{|G|}\sum_{g\in G}U(g)(\cdot)U(g)^\dagger \tag{4.206}$$

and SWAP is the unitary swap operator. The two terms can be individually estimated by means of the destructive SWAP test [GECP13]. To realize the twirl, one can pick an element g uniformly at random and apply $U(g)$ to the state ρ. Since the twirl and the SWAP test can be efficiently performed, it follows that the problem is in the BQP class.

Next, we show that the problem is BQP-Hard by providing an efficient mapping from a general BQP problem to our problem of interest. Consider a general BQP algorithm as described in Section 2.4.1. The output state of the BQP algorithm is given by

$$Q_{SA\to DG}\,|x\rangle_S\,|0\rangle_A\,. \tag{4.207}$$

Then, the acceptance and rejection probabilities of the BQP algorithm are given by

$$p_{\mathrm{acc}} = \|(\langle 1|_D\otimes I_G)Q_{SA\to DG}\,|x\rangle_S\,|0\rangle_A\|_2^2\,, \tag{4.208}$$

$$\begin{aligned}p_{\mathrm{rej}} &= 1-p_{\mathrm{acc}}\\ &= \|(\langle 0|_D\otimes I_G)Q_{SA\to DG}\,|x\rangle_S\,|0\rangle_A\|_2^2\,.\end{aligned} \tag{4.209}$$

Now, we need to map this problem to an instance of State-HS-Symmetry; i.e., we need to define a state ρ and a unitary representation $\{U(g)\}_{g\in G}$. To this end, let us define the group G to be the cyclic group on two elements, $C_2 = \{I, V\}$, such that $V^2 = I$, where V is given by

$$V_{SAC} = (Q_{SA\to DG})^\dagger\,\mathrm{CNOT}_{DC}\,Q_{SA\to DG}, \tag{4.210}$$

and the input state to be

$$\rho_{SAC} = |x\rangle\langle x|_S\otimes|0\rangle\langle 0|_{AC}. \tag{4.211}$$

From (4.204), we see that

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G}\|[U(g),\rho]\|_2^2 &= \frac{1}{|G|}\sum_{g\in G} 2(\mathrm{Tr}[\rho^2] - \mathrm{Tr}[\rho U(g)\rho U(g)^\dagger]) \\ &= 1 - \mathrm{Tr}[\rho V \rho V^\dagger] \\ &= 1 - |(\langle x|_S \otimes \langle 0|_{AC}) V (|x\rangle_S \otimes |0\rangle_{AC})|^2 . \end{aligned} \tag{4.212}$$

To show the equivalence, we now expand V as follows:

$$V(|x\rangle_S \otimes |0\rangle_{AC}) = (Q_{SA\to DG})^\dagger \,\mathrm{CNOT}_{DC}\, Q_{SA\to DG}(|x\rangle_S \otimes |0\rangle_{AC}). \tag{4.213}$$

Next, we insert an identity operator I_D to simplify:

$$\begin{aligned}&(Q_{SA\to DG})^\dagger \,\mathrm{CNOT}_{DC}\, Q_{SA\to DG}(|x\rangle_S \otimes |0\rangle_{AC}) \\ &\quad = (Q_{SA\to DG})^\dagger \,\mathrm{CNOT}_{DC}(|0\rangle\langle 0|_D \otimes I_{GC} + |1\rangle\langle 1|_D \otimes I_{GC}) Q_{SA\to DG}(|x\rangle_S \otimes |0\rangle_{AC}). \end{aligned} \tag{4.214}$$

Expanding, this reduces to

$$\begin{aligned}&(Q_{SA\to DG})^\dagger (|0\rangle\langle 0|_D \otimes I_{GC} + |1\rangle\langle 1|_D \otimes I_G \otimes X_C) Q_{SA\to DG}(|x\rangle_S \otimes |0\rangle_{AC}) \\ &\qquad = (Q_{SA\to DG})^\dagger (|0\rangle\langle 0|_D) Q_{SA\to DG}(|x\rangle_S \otimes |0\rangle_{AC}) \\ &\qquad\quad + (Q_{SA\to DG})^\dagger (|1\rangle\langle 1|_D) Q_{SA\to DG}(|x\rangle_S \otimes |0\rangle_A |1\rangle_C). \end{aligned} \tag{4.215}$$

Thus, by expanding p_{rej} as

$$\begin{aligned} p_{\mathrm{rej}} &= \|(\langle 0|_D \otimes I_G) Q_{SA\to DG}(|x\rangle_S \otimes |0\rangle_A)\|_2^2 \\ &= (\langle x|_S \otimes \langle 0|_A)(Q_{SA\to DG})^\dagger (|0\rangle\langle 0|_D) Q_{SA\to DG}(|x\rangle_S \otimes |0\rangle_A), \end{aligned} \tag{4.216}$$

we find that

$$\begin{aligned}(\langle x|_S \otimes \langle 0|_{AC}) V (|x\rangle_S \otimes |0\rangle_{AC}) &= (\langle x|_S \otimes \langle 0|_A)(Q_{SA\to DG})^\dagger (|0\rangle\langle 0|_D) Q_{SA\to DG}(|x\rangle_S \otimes |0\rangle_A) \\ &= p_{\mathrm{rej}}. \end{aligned} \tag{4.217}$$

We then finally see that

$$q \coloneqq \frac{1}{|G|}\sum_{g\in G}\|[U(g),\rho]\|_2^2 = 1 - p_{\mathrm{rej}}^2. \tag{4.218}$$

Thus, given a method to estimate q within additive error ε, we can estimate p_{rej} within an additive error of $\sqrt{\varepsilon}$. A proof of this can be found in Appendix C.6. We can then estimate $p_{\mathrm{acc}} = 1 - \sqrt{1-q}$ within an additive error of $\sqrt{\varepsilon}$ as well. As such, a general BQP problem can be efficiently mapped to our problem of interest, showing that State-HS-Symmetry is BQP-Hard. This along with that the fact that the problem lies in BQP, completes the proof of BQP-Completeness. ■

4.6.3 Testing G-Bose symmetry of the output of a channel is QMA-Complete

In this section, we show that testing the G-Bose symmetry of the output of a channel with optimized input is QMA-Complete.

Problem 4.3 [(α,β)-*Channel-G-Bose-Symmetry*]. *Let α and β be such that $0 \leq \beta < \alpha \leq 1$. Given is a circuit description of a unitary $U^{\mathcal{N}}_{BD'\to SD}$ that realizes a unitary dilation of a channel*

$$\mathcal{N}_{B\to S}(\cdot) \coloneqq \mathrm{Tr}_D[U^{\mathcal{N}}_{BD'\to SD}((\cdot)_B \otimes |0\rangle\langle 0|_{D'})(U^{\mathcal{N}}_{BD'\to SD})^\dagger] \tag{4.219}$$

and circuit descriptions of a unitary representation $\{U_S(g)\}_{g\in G}$ of a group G. Decide which of the following holds:

$$\textit{Yes:} \quad \max_{\rho_B} \mathrm{Tr}\left[\Pi^G_S \mathcal{N}_{B\to S}(\rho_B)\right] \geq \alpha, \tag{4.220}$$

$$\textit{No:} \quad \max_{\rho_B} \mathrm{Tr}\left[\Pi^G_S \mathcal{N}_{B\to S}(\rho_B)\right] \leq \beta, \tag{4.221}$$

where the optimization is over every input state ρ_B.

Let us observe that the measure in (4.220) is a faithful symmetry measure, in the sense that it is equal to one if and only if there exists an input state ρ_B such that the output state $\mathcal{N}_{B\to S}(\rho_B)$ is Bose-symmetric. This follows from continuity of $\mathrm{Tr}\left[\Pi^G_S \mathcal{N}_{B\to S}(\rho_B)\right]$ and from the arguments in [LRW23, Section 3.1].

Theorem 4.8. *The promise problem Channel-G-Bose-Symmetry is QMA-Complete.*

1. (α,β)*-Channel-G-Bose-Symmetry is in QMA for all $\beta < \alpha$. (It is implicit that the gap between α and β is larger than an inverse polynomial in the input length.)*
2. $(1-\varepsilon,\varepsilon)$*-Channel-G-Bose-Symmetry is QMA-Hard, even when ε decays exponentially in the input length.*

Thus, (α,β)-Channel-Bose-Symmetry is QMA-Complete for all (α,β) such that $0 \leq \beta < \alpha \leq 1$.

Proof. To show that the problem is QMA-Complete, we need to demonstrate two facts: first, that the problem is in QMA, and second, that it is QMA-Hard. Let us begin by proving that the problem is in QMA. Let ρ_B be a state sent by the prover. This state is input to the channel $\mathcal{N}_{B\to S}$ defined in (4.219). This leads

to the output state $\mathcal{N}_{B\to S}(\rho_B)$, on which the G-Bose symmetry test is conducted. From [LRW23, Algorithm 1], we see that testing G-Bose symmetry can be done efficiently when circuit descriptions of the unitaries $\{U(g)\}_{g\in G}$ are provided. The acceptance probability of this test, for an input state ρ_B, is equal to $\mathrm{Tr}\left[\Pi_S^G \mathcal{N}_{B\to S}(\rho_B)\right]$. Since the prover can optimize this probability over all possible input states, the acceptance probability is then

$$\max_{\rho_B} \mathrm{Tr}\left[\Pi_S^G \mathcal{N}_{B\to S}(\rho_B)\right]. \tag{4.222}$$

Thus, the entire estimation can be done efficiently when aided by an all-powerful prover, establishing that the problem lies in QMA.

To show that the problem is QMA-Hard, we pick an arbitrary QMA problem and map it to Channel-G-Bose-Symmetry. We use a similar construction proposed above in Section 4.6.1. For the mapping, we need to define a channel $\mathcal{N}$ and a unitary representation $\{U(g)\}_{g\in G}$; i.e., using the circuit descriptions for a general QMA algorithm, we need to define a channel $\mathcal{N}_{P\to S'}$ and a unitary representation $\{U_{S'}(g)\}_{g\in G}$, and also show how the symmetry-testing condition

$$\max_{\rho_P} \mathrm{Tr}[\Pi_{S'}^G \mathcal{N}_{P\to S'}(\rho_P)] \tag{4.223}$$

can be written in terms of the QMA algorithm's acceptance probability. To this end, we define the group G to be the cyclic group on two elements $C_2 = \{I, V\}$ such that $V^2 = I$, where V is simply given by

$$V_D = -Z_D, \tag{4.224}$$

and we define the channel $\mathcal{N}_{P\to D}$ to be

$$\mathcal{N}_{P\to D}(\cdot) \coloneqq \mathrm{Tr}_G[Q_{SAP\to DG}(|x\rangle\langle x|_S \otimes |0\rangle\langle 0|_A \otimes (\cdot)_P)(Q_{SAP\to DG})^\dagger]. \tag{4.225}$$

As such, we are making the identification $S' \leftrightarrow D$ between the system label S' of a general symmetry-testing problem and the system D for a QMA algorithm. The group representation and the channel are thus efficiently implementable. Thus, the channel output state of interest is just the state of the decision qubit, and the group projector for the given unitary representation is given by

$$\Pi_D^G = \frac{1}{2}(I_D - Z_D) = |1\rangle\langle 1|_D. \tag{4.226}$$

We then find, for a fixed input state ρ_P, the following equalities relating the symmetry-testing condition to the QMA algorithm's acceptance probability:

$$\begin{aligned}
&\mathrm{Tr}\Big[\Pi_D^G \mathcal{N}_{P\to D}(\rho_P)\Big] \\
&= \mathrm{Tr}[|1\rangle\langle 1|_D \mathcal{N}_{P\to D}(\rho_P)] \\
&= \mathrm{Tr}[(|1\rangle\langle 1|_D \otimes I_G)(Q_{SAP\to DG}(|x\rangle\langle x|_A \otimes |0\rangle\langle 0|_A \otimes \rho_P)(Q_{SAP\to DG})^\dagger)] \\
&= \Pr[Q \text{ accepts } (x,\rho_P)].
\end{aligned} \tag{4.227}$$

The prover then optimizes this probability over every input state ρ_P, and we observe that the acceptance probability of the QMA algorithm exactly matches the symmetry-testing condition of the constructed G-Bose symmetry testing algorithm. As such, we have proven that any QMA problem can be efficiently mapped to an instance of a Channel-G-Bose symmetry-testing problem, concluding the proof. ■

4.6.4 Testing G-symmetry of a state using trace norm is QSZK-Complete

In Section 4.6.2, we showed that testing G-symmetry of a state using the Hilbert–Schmidt norm is BQP-Complete. In this section, we show that testing the G-symmetry of a state using the trace norm is QSZK-Complete. As such, the complexity of a G-symmetry test depends on the measure being used, much like what was observed in [RASW23, Section V].

Problem 4.4 [(α,β)-*State-G-Sym-TD*]. *Let α and β be such that $0 \le \beta < \alpha \le 1$. Given are a circuit description of a unitary U_{RS}^{ρ} that generates a purification of a state ρ_S and circuit descriptions of a unitary representation $\{U_S(g)\}_{g\in G}$ of a group G. Decide which of the following holds:*

$$\textit{Yes:} \quad \min_{\sigma\in \mathrm{Sym}_G} \frac{1}{2}\|\rho-\sigma\|_1 \ge \alpha, \tag{4.228}$$

$$\textit{No:} \quad \min_{\sigma\in \mathrm{Sym}_G} \frac{1}{2}\|\rho-\sigma\|_1 \le \beta, \tag{4.229}$$

where the set Sym_G is defined as follows:

$$\mathrm{Sym}_G := \{\sigma \in \mathcal{D}(\mathcal{H}) : U(g)\sigma U(g)^\dagger = \sigma \quad \forall g \in G\}. \tag{4.230}$$

Let us observe that the asymmetry measure in (4.228) is faithful, in the sense that it is equal to zero if and only if the state ρ is G-symmetric. This follows from the faithfulness of the trace norm and its continuity properties.

Theorem 4.9. *The promise problem State-G-Sym-TD is QSZK-Complete.*

1. (α,β)*-State-G-Sym-TD is in QSZK for all* $2\beta < \alpha$. *(It is implicit that the gap between* α *and* 2β *is larger than an inverse polynomial in the input length.)*
2. $(1-\varepsilon,\varepsilon)$*-State-G-Sym-TD is QSZK-Hard, even when* ε *decays exponentially in the input length.*

Thus, (α,β)*-State-G-Sym-TD is QSZK-Complete for all* (α,β) *such that* $0 < 2\beta < \alpha < 1$.

Proof. To prove that the problem is QSZK-Complete, we need to show two facts. First, we need to show that the problem is in the QSZK class. Next, we show that the problem is QSZK-Hard; i.e., every problem in QSZK can be efficiently mapped to this problem.

First, we show that it is in QSZK. We begin with a simple calculation. Consider the case of a No instance, for which the following inequality holds

$$\min_{\sigma\in \mathrm{Sym}_G} \frac{1}{2}\|\rho-\sigma\|_1 \leq \beta. \tag{4.231}$$

Let $\sigma^* \in \mathrm{Sym}_G$ be a state achieving the minimum, so that

$$\frac{1}{2}\|\rho-\sigma^*\|_1 \leq \beta. \tag{4.232}$$

Define $\overline{\rho}$ as the result of twirling ρ with respect to the group elements of G. More concretely,

$$\overline{\rho} := \mathcal{T}_G(\rho) = \frac{1}{|G|}\sum_{g\in G} U(g)\rho U^\dagger(g). \tag{4.233}$$

From the data-processing inequality for the trace distance [Wil17, Chapter 9], and the fact that $\mathcal{T}_G(\sigma^*) = \sigma^*$, we conclude that

$$\begin{aligned}\frac{1}{2}\|\overline{\rho}-\sigma^*\|_1 &= \frac{1}{2}\|\mathcal{T}_G(\rho)-\mathcal{T}_G(\sigma^*)\|_1\\ &\leq \frac{1}{2}\|\rho-\sigma^*\|_1\\ &\leq \beta.\end{aligned} \tag{4.234}$$

Now, using the triangle inequality for the trace distance, (4.232), and (4.234), we find that

$$\frac{1}{2}\left\|\rho-\overline{\rho}\right\|_1 \leq \frac{1}{2}\left\|\rho-\sigma^*\right\|_1+\frac{1}{2}\left\|\sigma^*-\overline{\rho}\right\|_1 \tag{4.235}$$

$$\leq \beta+\beta=2\beta. \tag{4.236}$$

Having established the above, we now construct a QSZK algorithm consisting of the following steps:

1. The verifier randomly prepares the state ρ or $\overline{\rho}$. The verifier can prepare the latter state by preparing ρ and performing the group twirl $\mathcal{T}_G$.
2. The verifier sends the state to the prover, who performs an optimal measurement to distinguish ρ from $\overline{\rho}$.
3. The verifier accepts if the prover can guess the state that was prepared, and the maximum acceptance probability of the prover is given by [Hel69, Hol72]

$$\frac{1}{2}\left(1+\frac{1}{2}\left\|\rho-\overline{\rho}\right\|_1\right). \tag{4.237}$$

In the case of a No instance, by applying (4.235)–(4.236), this probability is bounded from above as

$$\frac{1}{2}\left(1+\frac{1}{2}\left\|\rho-\overline{\rho}\right\|_1\right) \leq \frac{1}{2}\left(1+2\beta\right)=\frac{1}{2}+\beta. \tag{4.238}$$

In the case of a Yes instance, we find that

$$\begin{aligned}\frac{1}{2}\left\|\rho-\overline{\rho}\right\|_1 &\geq \frac{1}{2}\left\|\rho-\sigma^*\right\|_1\\ &\geq \alpha.\end{aligned} \tag{4.239}$$

This then implies, in this case, that the acceptance probability satisfies

$$\frac{1}{2}\left(1+\frac{1}{2}\left\|\rho-\overline{\rho}\right\|_1\right) \geq \frac{1}{2}\left(1+\alpha\right) \tag{4.240}$$

$$=\frac{1}{2}+\frac{1}{2}\alpha. \tag{4.241}$$

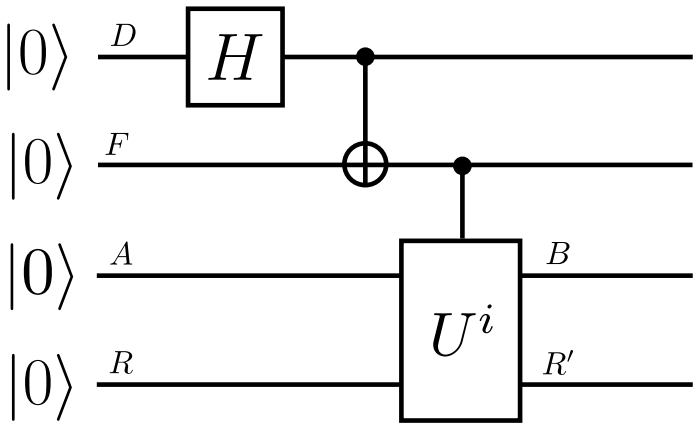


Figure 4.43: Circuit to create the classical–quantum state τ_{FB}. The unitaries U^0 and U^1 generate purification of states ω^0 and ω^1, respectively. More concretely, $\omega_B^i = \mathrm{Tr}_{R'}[U^i|00\rangle\langle 00|_{AR}(U^i)^\dagger]$ for $i \in \{0,1\}$.

Thus, there is a gap as long as

$$\frac{1}{2} + \frac{1}{2}\alpha > \frac{1}{2} + \beta, \tag{4.242}$$

which is the same as $\alpha > 2\beta$.

The interactive proof system is quantum statistical zero-knowledge because, in the case of a Yes instance, the verifier can efficiently simulate the whole interaction on their own, and the statistical difference between the simulation and the actual protocol is negligible. Thus, the problem is in the QSZK class.

Next, we show that an arbitrary problem in the QSZK class can be efficiently mapped to this problem. We do so by mapping a known QSZK-Complete problem to this problem. We pick the (α_s,β_s)-State Distinguishability Problem (see Definition 2.6).

Given circuits to generate the states ρ_B^0 and ρ_B^1 with the following soundness and completeness parameters

$$\textit{Yes:} \quad \frac{1}{2}\left\|\rho_B^0 - \rho_B^1\right\|_1 \geq \alpha_s, \tag{4.243}$$

$$\textit{No:} \quad \frac{1}{2}\left\|\rho_B^0 - \rho_B^1\right\|_1 \leq \beta_s, \tag{4.244}$$

we use the construction from [Wat02b, Theorem 1] to create circuits that generate

states ω^0, ω^1 such that

$$\textit{Yes:} \quad \frac{1}{2}\left\|\omega^0 - \omega^1\right\|_1 \geq 1 - 2^{-n} \tag{4.245}$$

$$\textit{No:} \quad \frac{1}{2}\left\|\omega^0 - \omega^1\right\|_1 \leq 2^{-n}. \tag{4.246}$$

The value of n will be chosen later in the proof. The procedure from [Wat02b, Theorem 1] runs in time polynomial in n and the size of the circuits that generate ρ^i, and thus it is efficient.

Next, we define the following state

$$\tau_{FB} \coloneqq \frac{1}{2}\left(|0\rangle\langle 0|_F \otimes \omega_B^0 + |1\rangle\langle 1|_F \otimes \omega_B^1\right), \tag{4.247}$$

and define the group G to be $\{I_F \otimes I_B, X_F \otimes I_B\}$. A circuit to create the state τ_{FB} is given in Figure 4.43. Twirling this state with respect to the group elements results in the state

$$\overline{\tau}_{FB} \coloneqq \mathcal{T}_G(\tau_{FB}) = \pi_F \otimes \frac{1}{2}(\omega_B^0 + \omega_B^1), \tag{4.248}$$

where $\pi_F \coloneqq \frac{1}{2}(|0\rangle\langle 0|_F + |1\rangle\langle 1|_F)$. Then we find that

$$\begin{aligned}
&\tau_{FB} - \overline{\tau}_{FB} \\
&= \frac{1}{2}|0\rangle\langle 0| \otimes \omega^0 + \frac{1}{2}|1\rangle\langle 1| \otimes \omega^1 - \pi \otimes \frac{1}{2}\left(\omega^0 + \omega^1\right) \\
&= \frac{1}{2}|0\rangle\langle 0| \otimes \omega^0 + \frac{1}{2}|1\rangle\langle 1| \otimes \omega^1 - \left(\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|\right) \otimes \frac{1}{2}\left(\omega^0 + \omega^1\right) \\
&= \frac{1}{2}|0\rangle\langle 0| \otimes \left(\omega^0 - \frac{1}{2}\left(\omega^0 + \omega^1\right)\right) + \frac{1}{2}|1\rangle\langle 1| \otimes \left(\omega^1 - \frac{1}{2}\left(\omega^0 + \omega^1\right)\right) \\
&= \frac{1}{2}|0\rangle\langle 0| \otimes \frac{1}{2}\left(\omega^0 - \omega^1\right) + \frac{1}{2}|1\rangle\langle 1| \otimes \frac{1}{2}\left(\omega^1 - \omega^0\right),
\end{aligned} \tag{4.249}$$

which implies that

$$\frac{1}{2}\left\|\tau_{FB} - \overline{\tau}_{FB}\right\|_1 = \frac{1}{4}\left\|\omega^0 - \omega^1\right\|_1. \tag{4.250}$$

We now map Yes instances of Quantum-State-Distinguishability to Yes instances of State-G-Sym-TD. For a Yes instance,

$$\frac{1}{2}\left\|\rho^0 - \rho^1\right\|_1 \geq \alpha_s \implies \frac{1}{2}\left\|\omega^0 - \omega^1\right\|_1 \geq 1 - 2^{-n}. \tag{4.251}$$

Define σ^* to be a state that achieves the following minimum:

$$\frac{1}{2}\left\|\tau_{FB}-\sigma^*\right\|_1 \coloneqq \min_{\sigma\in \mathrm{Sym}_G}\frac{1}{2}\left\|\tau_{FB}-\sigma\right\|_1. \tag{4.252}$$

Using the triangle inequality and the data-processing inequality (the latter being similar to how it was used before in (4.234)), we find that

$$\begin{aligned}\frac{1}{2}\left\|\tau_{FB}-\overline{\tau}_{FB}\right\|_1 &\leq \frac{1}{2}\left\|\tau_{FB}-\sigma^*\right\|_1+\frac{1}{2}\left\|\sigma^*-\overline{\tau}_{FB}\right\|_1\\ &\leq 2\left(\frac{1}{2}\left\|\tau_{FB}-\sigma^*\right\|_1\right)\\ &= 2\left(\min_{\sigma\in \mathrm{Sym}_G}\frac{1}{2}\left\|\tau_{FB}-\sigma\right\|_1\right).\end{aligned} \tag{4.253}$$

Thus, using (4.250), we see that

$$\begin{aligned}\min_{\sigma\in \mathrm{Sym}_G}\frac{1}{2}\left\|\tau_{FB}-\sigma\right\|_1 &\geq \frac{1}{2}\left(\frac{1}{2}\left\|\tau_{FB}-\overline{\tau}_{FB}\right\|_1\right)\\ &= \frac{1}{4}\left(\frac{1}{2}\left\|\omega^0-\omega^1\right\|_1\right)\\ &\geq \frac{1-2^{-n}}{4}.\end{aligned} \tag{4.254}$$

As such, the Yes instances are mapped as follows:

$$\frac{1}{2}\left\|\rho^0-\rho^1\right\|_1\geq\alpha_s \Rightarrow \min_{\sigma\in \mathrm{Sym}_G}\frac{1}{2}\left\|\tau_{FB}-\sigma\right\|_1\geq\frac{1-2^{-n}}{4}. \tag{4.255}$$

Similarly, consider a NO instance of Quantum-State-Distinguishability,

$$\frac{1}{2}\left\|\rho^0-\rho^1\right\|_1\leq\beta_s. \tag{4.256}$$

Then using (4.246) and (4.250),

$$\begin{aligned}\min_{\sigma\in \mathrm{Sym}_G}\frac{1}{2}\left\|\tau_{FB}-\sigma\right\|_1 &\leq \frac{1}{2}\left\|\tau_{FB}-\overline{\tau}_{FB}\right\|_1\\ &= \frac{1}{2}\left(\frac{1}{2}\left\|\omega^0-\omega^1\right\|_1\right)\\ &\leq 2^{-n-1}.\end{aligned} \tag{4.257}$$

As such, we have shown that (α_s, β_s)-Quantum-State-Distinguishability is efficiently mapped to $\left(\frac{1}{4}(1-2^{-n}), 2^{-n-1}\right)$-State-$G$-Sym-TD. Thus, a gap exists between the soundness and completeness conditions if

$$\frac{(1-2^{-n})}{4} > 2^{-n-1}, \tag{4.258}$$

which is equivalent to $n > \log_2(3)$.

To conclude that State-G-Sym-TD is QSZK-Complete for arbitrary constants α and β, one can use the constructions from Lemmas 2 and 3 of [Wat02b] to manipulate the parameters $\frac{1}{4}(1-2^{-n})$ and 2^{-n-1} as desired. The reasoning for this latter statement is similar to that given at the end of the proof of [Wat02b, Theorem 6]. ■

4.6.5 Testing G-symmetry of a state using fidelity is QSZK-Complete

In this section, we show that testing G-Symmetry of a state using fidelity is QSZK-Complete, where the fidelity of states ρ and σ is defined as [Uhl76]

$$F(\rho, \sigma) := \left\| \sqrt{\rho}\sqrt{\sigma} \right\|_1^2 . \tag{4.259}$$

To show hardness, we provide an efficient mapping from the problem State-G-Sym-TD, defined in Section 4.6.4, to the problem of interest State-G-Sym-Fid.

Problem 4.5 [(α, β)-*State-G-Sym-Fid*]. *Let α and β be such that $0 \leq \beta < \alpha \leq 1$. Given are a circuit description of a unitary U_{RS}^{ρ} that generates a purification of a state ρ_S and circuit descriptions of a unitary representation $\{U(g)\}_{g\in G}$ of a group G. Decide which of the following holds:*

$$\textit{Yes:} \quad \max_{\sigma \in \mathrm{Sym}_G} F(\rho, \sigma) \geq \alpha, \tag{4.260}$$

$$\textit{No:} \quad \max_{\sigma \in \mathrm{Sym}_G} F(\rho, \sigma) \leq \beta, \tag{4.261}$$

where the set Sym_G *is defined in* (4.230).

Let us observe that the symmetry measure in (4.260) is faithful, in the sense that it is equal to one if and only if the state ρ is G-symmetric. This follows from the faithfulness and continuity properties of fidelity.

Theorem 4.10. *The promise problem State-G-Sym-Fid is QSZK-Complete.*

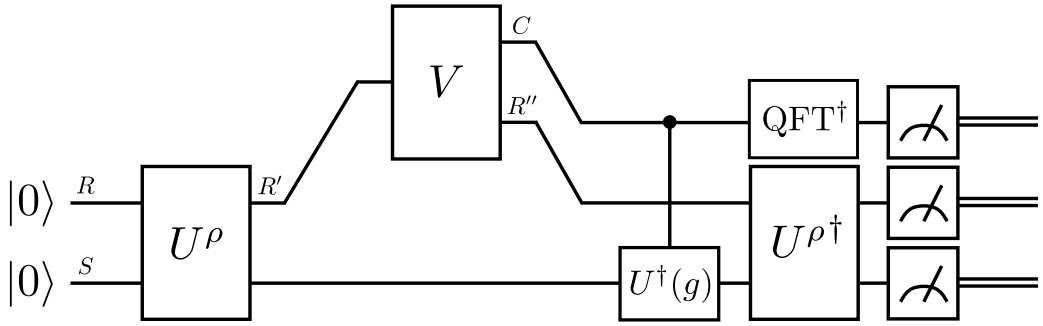


Figure 4.44: QSZK algorithm to estimate the fidelity $F(\rho, \overline{\rho})$ given a unitary U^ρ that prepares a purification of ρ and a unitary representation $\{U(g)\}_{g\in G}$ over which the twirled state $\overline{\rho}$ is defined. The probability of measuring the all-zeros state gives an estimate of the required fidelity. The isometry V is implemented by an all-powerful prover. QFT is an abbreviation of the standard quantum Fourier transform, which in this case takes $|0\rangle$ to $|G|^{-1/2}\sum_{g\in G}|g\rangle$.

1. (α, β)-*State-G-Sym-Fid is in QSZK for all* $\beta < 4\alpha - 3$. *(It is implicit that the gap between* $4\alpha - 3$ *and* β *is larger than an inverse polynomial in the input length.)*
2. $(1-\varepsilon, \varepsilon)$-*State-G-Sym-Fid is QSZK-Hard, even when* ε *decays exponentially in the input length.*

Thus, (α, β)-*State-G-Sym-Fid is QSZK-Complete for all* (α, β) *such that* $0 \leq \beta < 4\alpha - 3 \leq 1$.

Proof. Before we get into the proof, let us recall the sine distance of two quantum states ρ, σ [Ras06]:

$$P(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)}. \tag{4.262}$$

The sine distance has a triangle-inequality property for states ρ, σ, ω:

$$P(\rho, \sigma) \leq P(\rho, \omega) + P(\sigma, \omega). \tag{4.263}$$

Furthermore, it has a data-processing inequality inherited from that of fidelity:

$$P(\rho, \sigma) \geq P(\mathcal{N}(\rho), \mathcal{N}(\sigma)). \tag{4.264}$$

To prove that State-G-Sym-Fid is QSZK-Complete, we need to show two results. First, we need to show that the problem belongs to QSZK and, second, that the problem is QSZK-Hard.

We first show that the problem belongs to QSZK. To this end, we propose an algorithm to estimate the quantity $F(\rho, \overline{\rho})$. The underlying principle is Uhlmann's theorem [Uhl76], which can be simply understood as follows:

$$F(\rho_S, \sigma_S) = \max_{V_{R\to R'}} |\langle\psi^\sigma|_{R'S}(V_{R\to R'} \otimes I_S)|\psi^\rho\rangle_{RS}|^2 , \tag{4.265}$$

where the maximization is over every isometry $V_{R\to R'}$ and $|\psi^\rho\rangle_{RS}$ and $|\psi^\sigma\rangle_{RS}$ are purifications of ρ_S and σ_S, respectively. In other words, the fidelity of two states is given by the maximum squared overlap between their purifications. To calculate the fidelity of ρ and $\overline{\rho}$, we then need purifications of both states. We are given a unitary U^ρ to prepare a purification of ρ that is used in the following manner:

$$\begin{aligned} |\psi^\rho\rangle_{RS} &= U^\rho_{RS} |0\rangle_{RS} , \\ \rho_S &= \mathrm{Tr}_R[|\psi^\rho\rangle\langle\psi^\rho|_{RS}]. \end{aligned} \tag{4.266}$$

The following unitary generates a purification of $\overline{\rho}$:

$$U^{\overline{\rho}}_{CRS} := \left(\sum_g |g\rangle\langle g|_C \otimes U_S(g)\right) \mathrm{QFT}_C \, U^\rho_{RS}, \tag{4.267}$$

as follows:

$$\begin{aligned} \left|\psi^{\overline{\rho}}\right\rangle &= U^{\overline{\rho}}_{CR''S} |0\rangle_{CR''S} \\ &= \left(\sum_{g\in G} |g\rangle\langle g|_C \otimes U_S(g)\right) \frac{1}{\sqrt{|G|}} \sum_{g'\in G} |g'\rangle_C |\psi^\rho\rangle_{R''S} \\ &= \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle_C \otimes U_S(g) |\psi^\rho\rangle_{R''S} . \end{aligned} \tag{4.268}$$

Thus, performing the partial trace over $R''C$, we see that

$$\begin{aligned} \mathrm{Tr}_{R''C}[|\psi^{\overline{\rho}}\rangle\langle\psi^{\overline{\rho}}|_{R''C}] &= \frac{1}{|G|} \sum_g U_S(g) \rho_S U_S^\dagger(g) \\ &= \overline{\rho}. \end{aligned} \tag{4.269}$$

Therefore, using the unitaries U^ρ_{RS} and $U^{\overline{\rho}}_{R'S}$ (where $R' \equiv R''C$), we can apply Uhlmann's theorem in tandem with an all-powerful prover (to implement the isometry V) to estimate the fidelity. The construction for the algorithm can be seen in Figure 4.44.

In the case of a Yes-instance,

$$\max_{\sigma \in \mathrm{Sym}_G} F(\rho, \sigma) \geq \alpha. \tag{4.270}$$

Let σ^* be a state achieving the maximum, i.e.,

$$\begin{aligned} & F(\rho, \sigma^*) \geq \alpha, \\ \Leftrightarrow \quad & P(\rho, \sigma^*) \leq \sqrt{1-\alpha}. \end{aligned} \tag{4.271}$$

Then

$$\begin{aligned} P(\rho, \overline{\rho}) &\leq P(\rho, \sigma^*) + P(\sigma^*, \overline{\rho}) \\ &\leq 2P(\rho, \sigma^*) \\ &\leq 2\sqrt{1-\alpha}, \\ \Leftrightarrow \quad F(\rho, \overline{\rho}) &\geq 4\alpha - 3, \end{aligned} \tag{4.272}$$

where the second inequality follows from the data-processing inequality (see (4.264)) under the application of the twirling channel $\mathcal{T}_G$ and the fact that σ^* is unchanged under the application of this channel.

In the case of a No-instance,

$$F(\rho, \overline{\rho}) \leq \max_{\sigma \in \mathrm{Sym}_G} F(\rho, \sigma) \leq \beta. \tag{4.273}$$

Thus, there exists a gap as long as

$$\alpha > \frac{3+\beta}{4}. \tag{4.274}$$

The interactive proof system is quantum statistical zero-knowledge because, in the case of a Yes instance, the input state ρ is close to the twirled state $\overline{\rho}$. Thus, the verifier can efficiently simulate the whole interaction on their own, and the statistical difference between the simulation and the actual protocol is negligible. As such, the problem is in the QSZK class.

Next, we show that the problem is QSZK-Hard. To do this, we map the QSZK-Complete problem State-G-Sym-TD to our problem. To show this, we make use of two standard inequalities that relate the trace distance and fidelity of two states [FvdG99]:

$$1 - \sqrt{F(\rho, \sigma)} \leq \frac{1}{2} \left\| \rho - \sigma \right\|_1, \tag{4.275}$$

$$\sqrt{1 - F(\rho, \sigma)} \geq \frac{1}{2} \left\| \rho - \sigma \right\|_1. \tag{4.276}$$

Consider a No-instance of State-G-Sym-TD. Then,

$$\frac{1}{2}\min_{\sigma\in\mathrm{Sym}_G}\|\rho-\sigma\|_1\leq\beta. \tag{4.277}$$

Using (4.275), we see that

$$\min_{\sigma\in\mathrm{Sym}_G}1-\sqrt{F(\rho,\sigma)}\leq\min_{\sigma\in\mathrm{Sym}_G}\frac{1}{2}\|\rho-\sigma\|_1\leq\beta. \tag{4.278}$$

Therefore, after some basic algebra,

$$\max_{\sigma\in\mathrm{Sym}_G}F(\rho,\sigma)\geq(1-\beta)^2. \tag{4.279}$$

Similarly, consider a Yes-instance of State-G-Sym-TD. Then,

$$\min_{\sigma\in\mathrm{Sym}_G}\frac{1}{2}\|\rho-\sigma\|_1\geq\alpha. \tag{4.280}$$

Using (4.276), we see that

$$\alpha\leq\min_{\sigma\in\mathrm{Sym}_G}\frac{1}{2}\|\rho-\sigma\|_1\leq\min_{\sigma\in\mathrm{Sym}_G}\sqrt{1-F(\rho,\sigma)}. \tag{4.281}$$

Therefore, after some basic algebra,

$$\max_{\sigma\in\mathrm{Sym}_G}F(\rho,\sigma)\leq1-\alpha^2. \tag{4.282}$$

Thus, (α,β)-State-G-Sym-TD reduces to $((1-\beta)^2,1-\alpha^2)$-State-G-Sym-Fid. Since we mapped Yes (No) instances to No (Yes) instances, this proves that State-G-Sym-Fid belongs to co-QSZK. Since QSZK is closed under complement, the problem belongs to QSZK [Wat02b]. Thus, State-G-Sym-Fid is QSZK-Hard. ■

4.6.6 Testing G-Bose symmetric extendibility of a state is QIP(2)-Complete

In this section, we show that testing G-Bose symmetric extendibility (G-BSE) of a state is QIP(2)-Complete.

Problem 4.6 [(α,β)-*State-G-BSE*]. *Let α and β be such that $0 \leq \beta < \alpha \leq 1$. Given are a circuit description of a unitary U^{ρ}_{RS} that generates a purification of a state ρ_S and circuit descriptions of a unitary representation $\{U_{RS}(g)\}_{g\in G}$ of a group G. Decide which of the following holds:*

$$\textit{Yes:} \quad \max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S) \geq \alpha, \tag{4.283}$$

$$\textit{No:} \quad \max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S) \leq \beta, \tag{4.284}$$

where the set BSE_G is defined in (4.67).

Let us observe that the symmetry measure in (4.283) is faithful, in the sense that it is equal to one if and only if the state ρ is G-Bose symmetric extendible. This follows from the faithfulness and continuity properties of fidelity.

Theorem 4.11. *The promise problem State-G-BSE is QIP(2)-Complete.*

1. *(α,β)-State-G-BSE is in QIP(2) for all $\beta < \alpha$. (It is implicit that the gap between α and β is larger than an inverse polynomial in the input length.)*
2. *$(1-\varepsilon,\varepsilon)$-State-G-BSE is QIP(2)-Hard, even when ε decays exponentially in the input length.*

Thus, (α,β)-State-G-BSE is QIP(2)-Complete for all (α,β) such that $0 \leq \beta < \alpha \leq 1$.

Proof. To show that the problem is QIP(2)-Complete, we need to demonstrate two facts: first, that the problem is in QIP(2), and second, that it is QIP(2)-Hard. Let us begin by proving that the problem is in QIP(2). In our previous work [LRW23, Algorithm 3], we proposed an algorithm to test for G-Bose symmetric extendibility of a state ρ_S given a circuit description of unitary that generates a purification of the state and circuit descriptions of a unitary representation $\{U_{RS}(g)\}_{g\in G}$ of a group G (see also [LRW23, Figure 6]). By inspection, the algorithm can be conducted efficiently given two messages exchanged with an all-powerful prover; therefore, this promise problem is clearly in QIP(2).

To show that the problem is QIP(2)-Hard, we map an arbitrary QIP(2) problem to a G-BSE problem. Specifically, from the circuit descriptions for a QIP(2) algorithm, we will identify a state $\rho_{S'}$ and a unitary representation $\{V_{R'S'}(g)\}_{g\in G}$ corresponding to a G-BSE problem, and we will show how the symmetry-testing condition

$$\max_{\sigma_{S'} \in \mathrm{BSE}_G} F(\rho_{S'}, \sigma_{S'}) \tag{4.285}$$

can be written in terms of the QIP(2) algorithm's acceptance probability.

To begin, recall that a QIP(2) problem consists of a first verifier circuit $U^1_{SA\to S'R'}$, a prover circuit $P_{RE\to R'E'}$, and a second verifier circuit $U^2_{S'R'\to DG}$, where D is the decision qubit. (Here and in what follows, we keep implicit the dependence of the prover's unitary on the problem input x.) The acceptance probability is given by

$$p_{\text{acc}} = \max_{P_{RE\to R'E'}} \left\| (\langle 1|_D \otimes I_{E'G}) U^2_{S'R'\to DG} P_{RE\to RE'} U^1_{SA\to S'R} |x\rangle_S |0\rangle_A |0\rangle_E \right\|_2^2. \tag{4.286}$$

Define $|\psi\rangle_{S'R} \coloneqq U^1_{SA\to S'R} |x\rangle_S |0\rangle_A$, and we identify the aforementioned state $\rho_{S'}$ as

$$\rho_{S'} \coloneqq \text{Tr}_R[|\psi\rangle\langle\psi|_{S'R}]. \tag{4.287}$$

The acceptance probability can then be rewritten as

$$p_{\text{acc}} = \max_{P_{RE\to R'E'}} \text{Tr}[(|1\rangle\langle 1|_D \otimes I_{E'G}) U^2 P (|0\rangle\langle 0|_E \otimes |\psi\rangle\langle\psi|_{S'R}) P^\dagger (U^2)^\dagger], \tag{4.288}$$

where we omitted system labels for brevity. Using the cyclicity of trace, consider that

$$p_{\text{acc}} = \max_{P_{RE\to R'E'}} \text{Tr}[(U^2)^\dagger (|1\rangle\langle 1|_D \otimes I_{E'G}) U^2 P (|0\rangle\langle 0|_E \otimes |\psi\rangle\langle\psi|_{S'R}) P^\dagger]. \tag{4.289}$$

Motivated by this, we pick the group G to be C_2 with unitary representation $\{I_{R'S'}, V_{R'S'}\}$, where

$$V_{R'S'} \coloneqq (U^2_{R'S'\to DG})^\dagger \, (-Z_D \otimes I_G) \, U^2_{R'S'\to DG}, \tag{4.290}$$

We note that $V^2_{RS} = I_{RS}$, establishing that this is indeed a representation of C_2. The resulting group projection is then

$$\begin{aligned}
\Pi^G_{R'S'} &= \frac{1}{2}(I_{R'S'} + V_{R'S'}) \\
&= \frac{1}{2}\left(U^{2\dagger}(I_D \otimes I_G) U^2 + U^{2\dagger} \, (-Z_D \otimes I_G) \, U^2 \right) \\
&= \frac{1}{2}\left(U^{2\dagger} \, (I_{DG} - (Z_D \otimes I_G)) \, U^2 \right) \\
&= U^{2\dagger}(|1\rangle\langle 1|_D \otimes I_G) U^2,
\end{aligned} \tag{4.291}$$

which is precisely the acceptance projection in the first line of (4.289). That is,

$$p_{\text{acc}} = \max_{P_{RE\to R'E'}} \text{Tr}[\Pi^G_{R'S'} P (|0\rangle\langle 0|_E \otimes |\psi\rangle\langle\psi|_{S'R}) P^\dagger]. \tag{4.292}$$

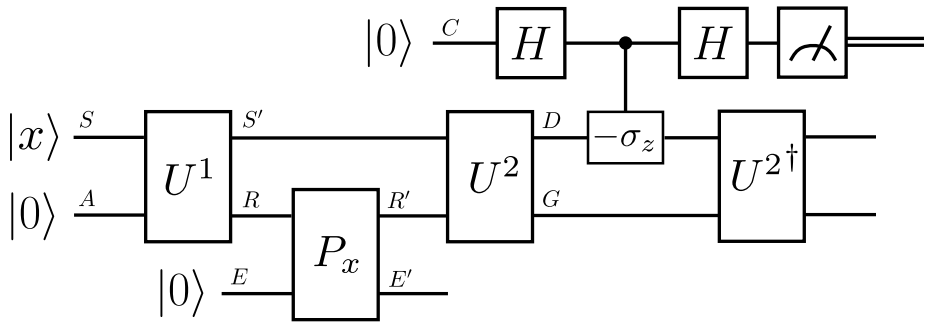


Figure 4.45: Circuit to map an arbitrary QIP(2) computation to a G-Bose symmetric extendibility test.

Now invoking [LRW23, Theorem III.3], we conclude that

$$\begin{aligned}
&\max_{P_{RE\to R'E'}} \mathrm{Tr}[\Pi^G_{R'S'} P(|0\rangle\langle 0|_E \otimes |\psi\rangle\langle\psi|_{S'R}) P^\dagger] \\
&= \max_{P_{RE\to R'E'}} \left\| \Pi^G_{R'S'} P(|0\rangle_E \otimes |\psi\rangle_{S'R}) \right\|_2^2 \\
&= \max_{\sigma_{S'} \in \mathrm{BSE}_G} F(\rho_{S'}, \sigma_{S'}),
\end{aligned} \tag{4.293}$$

where BSE_G in this case is

$$\mathrm{BSE}_G := \left\{ \begin{array}{c} \sigma_{S'} : \exists\, \omega_{R'S'} \in \mathcal{D}(\mathcal{H}_{R'S'}), \mathrm{Tr}_{R'}[\omega_{R'S'}] = \sigma_{S'}, \\ \omega_{R'S'} = V_{R'S'} \omega_{R'S'}, \end{array} \right\}. \tag{4.294}$$

To help visualize the reduction, the G-Bose symmetric extendibility test corresponding to a general QIP(2) algorithm is depicted in Figure 4.45.

Thus, the acceptance probability of the QIP(2) algorithm exactly matches the symmetry-testing condition of the constructed G-BSE problem. As such, any QIP(2) problem can be efficiently mapped to a G-BSE problem, proving that the problem State-G-BSE is QIP(2)-Hard. Along with the fact that the problem lies in the QIP(2) class, this concludes the proof. ■

4.6.7 Testing G-Bose symmetric separable extendibility of a state is $\mathbf{QIP_{EB}}(2)$-Complete

In this section, we introduce the following problem: decide whether a state has a separable extension that is G-Bose symmetric. We also prove that it is a $\mathrm{QIP}_{\mathrm{EB}}(2)$-

Complete problem.

Problem 4.7 [(α,β)-*Sep-Ext-G-Bose-Symmetry*]. *Let α and β be such that $0 \leq \beta < \alpha \leq 1$. Given is a circuit description of a unitary $U^{\rho}_{SS'}$ that generates a purification of a state ρ_S, as well as circuit descriptions of a unitary representation $\{U_{RS}(g)\}_{g\in G}$ of a group G. Decide which of the following holds:*

$$\textit{Yes:} \quad \max_{\substack{\omega_{RS}\in \mathrm{SEP}(R:S),\\ \mathrm{Tr}_R[\omega_{RS}]=\rho_S}} \mathrm{Tr}[\Pi^G_{RS}\omega_{RS}] \geq \alpha, \tag{4.295}$$

$$\textit{No:} \quad \max_{\substack{\omega_{RS}\in \mathrm{SEP}(R:S),\\ \mathrm{Tr}_R[\omega_{RS}]=\rho_S}} \mathrm{Tr}[\Pi^G_{RS}\omega_{RS}] \leq \beta, \tag{4.296}$$

where Π^G_{RS} is defined in (4.9).

Let us observe that the following equality holds:

$$\max_{\substack{\omega_{RS}\in \mathrm{SEP}(R:S),\\ \mathrm{Tr}_R[\omega_{RS}]=\rho_S}} \mathrm{Tr}[\Pi^G_{RS}\omega_{RS}] = \max_{\substack{\omega_{RS}\in \mathrm{SEP}(R:S),\\ \mathrm{Tr}_R[\omega_{RS}]=\rho_S,\\ \sigma_{RS}\in \text{B-Sym}_G}} F(\omega_{RS},\sigma_{RS}), \tag{4.297}$$

where the set B-Sym_G in this case is defined as

$$\text{B-Sym}_G := \{\sigma_{RS} : \sigma_{RS} = U_{RS}(g)\sigma_{RS},\ \forall g \in G\}. \tag{4.298}$$

The identity in (4.297) follows as a consequence of [LRW23, Theorem 3.1]. Rewriting the expression in this way allows for a fidelity interpretation of the symmetry condition, which implies that the symmetry-testing condition in (4.295) is equal to one if and only if there exists a separable extension of ρ_S that is Bose-symmetric according to the unitary representation $\{U_{RS}(g)\}_{g\in G}$. As such, this is a faithful measure of G-Bose symmetric separable extendibility.

Theorem 4.12. *The promise problem Sep-Ext-G-Bose-Symmetry is $QIP_{EB}(2)$-Complete.*

1. *(α,β)-Sep-Ext-G-Bose-Symmetry is in $QIP_{EB}(2)$ for all $\beta < \alpha$. (It is implicit that the gap between α and β is larger than an inverse polynomial in the input length.)*
2. *$(1-\varepsilon,\varepsilon)$-Sep-Ext-G-Bose-Symmetry is $QIP_{EB}(2)$-Hard, even when ε decays exponentially in the input length.*

Thus, (α,β)-Sep-Ext-G-Bose-Symmetry is $QIP_{EB}(2)$-Complete for all (α,β) such that $0 \leq \beta < \alpha \leq 1$.

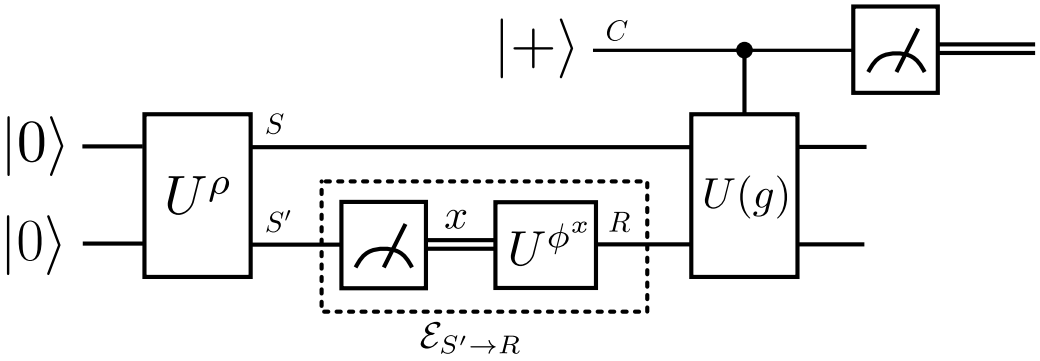


Figure 4.46: $\mathrm{QIP}_{\mathrm{EB}}(2)$ algorithm to test for G-Bose symmetry of a separable extension of the state ρ_S, where the prover's actions are depicted in the dashed box. The prover's channel $\mathcal{E}_{S'\to R}$ is entanglement breaking.

Proof. To show that the problem is $\mathrm{QIP}_{\mathrm{EB}}(2)$-Complete, we need to demonstrate two facts: first, that the problem is in $\mathrm{QIP}_{\mathrm{EB}}(2)$, and second, that it is $\mathrm{QIP}_{\mathrm{EB}}(2)$-Hard. Let us begin by proving that the problem is in $\mathrm{QIP}_{\mathrm{EB}}(2)$.

The algorithm to estimate the quantity in (4.295) is given in Figure 4.46. The general form of an entanglement-breaking channel is given by

$$\mathcal{E}_{S'\to R}(\cdot) = \sum_{x\in\mathcal{X}} \mathrm{Tr}[\mu^x_{S'}(\cdot)]\phi^x_R, \tag{4.299}$$

as discussed in (2.143). Thus, the acceptance probability of the algorithm for a fixed channel $\mathcal{E}_{S'\to R}$ is given by

$$\begin{aligned}
&\mathrm{Tr}[\Pi^G_{RS}\mathcal{E}_{S'\to R}(|\psi^\rho\rangle\langle\psi^\rho|_{SS'})] \\
&= \sum_{x\in\mathcal{X}} \mathrm{Tr}[\Pi^G_{RS}\ \mathrm{Tr}_{S'}[\mu^x_{S'}(|\psi^\rho\rangle\langle\psi^\rho|_{SS'})]\otimes\phi^x_R] \\
&= \sum_{x\in\mathcal{X}} p(x)\,\mathrm{Tr}[\Pi^G_{RS}(\phi^x_R\otimes\psi^x_S)],
\end{aligned} \tag{4.300}$$

where

$$p(x) := \mathrm{Tr}[\mu^x_{S'}(|\psi^\rho\rangle\langle\psi^\rho|_{SS'})], \tag{4.301}$$

$$\psi^x_S := \frac{1}{p(x)}\mathrm{Tr}_{S'}[\mu^x_{S'}(|\psi^\rho\rangle\langle\psi^\rho|_{SS'})]. \tag{4.302}$$

Note that

$$\begin{aligned}\sum_{x\in\mathcal{X}} p(x)\psi_S^x &= \sum_{x\in\mathcal{X}} \mathrm{Tr}_{S'}[\mu_{S'}^x(|\psi^\rho\rangle\langle\psi^\rho|_{SS'})] \\ &= \mathrm{Tr}_{S'}[|\psi^\rho\rangle\langle\psi^\rho|_{SS'}] \\ &= \rho_S . \end{aligned} \tag{4.303}$$

Thus, maximizing over all possible entanglement-breaking channels, the acceptance probability is given by

$$\max_{\{(p(x),\psi_S^x,\phi_R^x)\}_x} \sum_{x\in\mathcal{X}} p(x)\,\mathrm{Tr}[\Pi_{RS}^G(\phi_R^x\otimes\psi_S^x)] = \max_{\omega_{RS}\in\mathrm{SEP}(R:S)} \mathrm{Tr}[\Pi_{RS}^G\omega_{RS}], \tag{4.304}$$

with the condition that $\mathrm{Tr}_R[\omega_{RS}] = \sum_x p(x)\psi_S^x = \rho_S$. Since the entire algorithm can be performed efficiently when augmented by an entanglement-breaking prover, the problem is in $\mathrm{QIP}_{\mathrm{EB}}(2)$.

Next, we show that the problem is $\mathrm{QIP}_{\mathrm{EB}}(2)$-Hard. To do this, we need to map a general $\mathrm{QIP}_{\mathrm{EB}}(2)$ problem to an instance of Sep-Ext-G-Bose-Symmetry; i.e., using the circuit descriptions for a general $\mathrm{QIP}_{\mathrm{EB}}(2)$ algorithm, we need to define a state ρ_S and a unitary representation $\{U_{RS}(g)\}_{g\in G}$.

Consider a general interactive proof system in $\mathrm{QIP}_{\mathrm{EB}}(2)$ that begins with the verifier preparing a bipartite pure state ψ_{RS}, followed by the system R being sent to the prover, who subsequently performs an entanglement-breaking channel $\mathcal{E}_{R\to R'}$ and sends the R' register to the verifier. The verifier then performs a unitary $V_{R'S\to DG}$, measures the decision qubit, and accepts if the outcome $|1\rangle$ is observed. Indeed, the acceptance probability is given by

$$\max_{\mathcal{E}\in\mathrm{EB}} \mathrm{Tr}[(|1\rangle\langle 1|_D\otimes I_G)\mathcal{V}_{R'S\to DG}(\mathcal{E}_{R\to R'}(\psi_{RS}))], \tag{4.305}$$

where $\mathcal{V}_{R'S\to DG}$ is the unitary channel corresponding to the unitary operator $V_{R'S\to DG}$ and EB denotes the set of entanglement-breaking channels. Following the reasoning in (4.300), the output of an entanglement-breaking channel can be written in the form

$$\mathcal{E}_{R\to R'}(\psi_{RS}) = \sum_x p(x)\phi_{R'}^x\otimes\psi_S^x, \tag{4.306}$$

with the condition that $\sum_x p(x)\psi_S^x = \mathrm{Tr}_R[\psi_{RS}] = \rho_S$. In other words, the output of the entanglement-breaking channel is a separable extension of the state ρ_S. Thus,

the acceptance probability is given by

$$\max_{\omega_{R'S} \in \mathrm{SEP}(R':S)} \mathrm{Tr}[(|1\rangle\langle 1|_D \otimes I_G) V(\omega_{R'S}) V^\dagger] = \max_{\omega_{R'S} \in \mathrm{SEP}(R':S)} \mathrm{Tr}[(V^\dagger(|1\rangle\langle 1|_D \otimes I_G) V) \omega_{R'S}], \tag{4.307}$$

subject to the constraint $\mathrm{Tr}_{R'}[\omega_{R'S}] = \rho_S$, where we have used the shorthand $V \equiv V_{R'S \to DG}$. The second inequality results from the cyclicity of trace.

Let us then define the group G to be the cyclic group on two elements $C_2 = \{I, W\}$ such that $W^2 = I$, where W is simply given by

$$W_{R'S} := (V_{RS' \to DG})^\dagger \, (-Z_D \otimes I_G) \, V_{R'S \to DG}, \tag{4.308}$$

We note that $W_{R'S}^2 = I_{R'S}$, establishing that this is indeed a representation of C_2. The resulting group projection is then

$$\begin{aligned} \Pi_{R'S}^G &= \frac{1}{2}(I_{R'S} + W_{R'S}) \\ &= \frac{1}{2}\left(V^\dagger (I_D \otimes I_G) V + V^\dagger \, (-Z_D \otimes I_G) \, V\right) \\ &= \frac{1}{2}\left(V^\dagger \, (I_{DG} - (Z_D \otimes I_G)) \, V\right) \\ &= V^\dagger (|1\rangle\langle 1|_D \otimes I_G) V. \end{aligned} \tag{4.309}$$

Next, we define the state ρ_S to be

$$\rho_S := \mathrm{Tr}_R[\psi_{RS}]. \tag{4.310}$$

Thus, the symmetry-testing condition of the instance of Sep-Ext-G-Bose-Symmetry is given by

$$\max_{\omega_{R'S} \in \mathrm{SEP}(R':S)} \mathrm{Tr}[\Pi_{R'S}^G \omega_{R'S}] = \max_{\omega_{R'S} \in \mathrm{SEP}(R':S)} \mathrm{Tr}[V^\dagger (|1\rangle\langle 1|_D \otimes I_G) V \omega_{R'S}], \tag{4.311}$$

where the maximization over $\omega_{R'S}$ is subject to the constraint that $\mathrm{Tr}_{R'}[\omega_{R'S}] = \rho_S$. This exactly matches the acceptance probability of the $\mathrm{QIP}_{\mathrm{EB}}(2)$ problem, establishing that Sep-Ext-G-Bose-Symmetry is $\mathrm{QIP}_{\mathrm{EB}}(2)$-Hard, thus completing the proof. ■

4.6.8 Testing G-Bose symmetric extendibility of the output of a channel is QIP-Complete

In this section, we show that testing the G-Bose symmetric extendibility (G-BSE) of the output of a channel state is QIP-Complete.

Problem 4.8 [(α,β)-*Channel-G-BSE*]. *Let α and β be such that $0 \leq \beta < \alpha \leq 1$. Given are descriptions of circuits $U^{\mathcal{N}}_{BC'\to S'S}$ that prepare a unitary dilation of a channel*

$$\mathcal{N}_{B\to S}(\cdot) \coloneqq \mathrm{Tr}_{S'}[U^{\mathcal{N}}_{BC'\to S'S}((\cdot)_B \otimes |0\rangle\langle 0|_{C'})(U^{\mathcal{N}}_{BC'\to S'S})^\dagger] \tag{4.312}$$

and descriptions of a unitary representation $\{U_S(g)\}_{g\in G}$ of a group G. Decide which of the following holds:

$$\textit{Yes:} \quad \max_{\substack{\rho_B\in\mathcal{D}(\mathcal{H}_B),\\ \sigma_S\in \mathrm{BSE}_G}} F(\mathcal{N}_{B\to S}(\rho_B),\sigma_S) \geq \alpha, \tag{4.313}$$

$$\textit{No:} \quad \max_{\substack{\rho_B\in\mathcal{D}(\mathcal{H}_B),\\ \sigma_S\in \mathrm{BSE}_G}} F(\mathcal{N}_{B\to S}(\rho_B),\sigma_S) \leq \beta, \tag{4.314}$$

where the set BSE_G *is defined to be:*

$$\mathrm{BSE}_G \coloneqq \left\{ \begin{array}{c} \sigma_S : \exists\, \omega_{RS} \in \mathcal{D}(\mathcal{H}_{RS}), \mathrm{Tr}_R[\omega_{RS}] = \sigma_S, \\ \omega_{RS} = U_{RS}(g)\omega_{RS},\ \forall g \in G \end{array} \right\}. \tag{4.315}$$

Let us observe that the symmetry measure in (4.313) is faithful, in the sense that it is equal to one if and only if there is a channel input state ρ_B such that the output state $\mathcal{N}_{B\to S}(\rho_B)$ is G-Bose symmetric extendible.

Theorem 4.13. *The promise problem Channel-G-BSE is QIP-Complete.*

1. *(α,β)-Channel-G-BSE is in QIP for all $\beta < \alpha$. (It is implicit that the gap between α and β is larger than an inverse polynomial in the input length.)*
2. *$(1-\varepsilon,\varepsilon)$-Channel-G-BSE is QIP-Hard, even when ε decays exponentially in the input length.*

Thus, (α,β)-Channel-G-BSE is QIP-Complete for all (α,β) such that $0 \leq \beta < \alpha \leq 1$.

Proof. To show that the problem is QIP-Complete, we need to demonstrate two facts: first, that the problem is in QIP, and second, that it is QIP-Hard. Let us

begin by proving that the problem is in QIP. In our previous work [LRW23, Algorithm 3], we proposed an algorithm to test for G-Bose Symmetric Extendibility of a state ρ_S given a circuit description of unitary that generates a purification of the state and circuit descriptions of a unitary representation $\{U_{RS}(g)\}_{g\in G}$ of a group G. By inspection, the algorithm can be executed efficiently given two messages exchanged with an all-powerful prover. The optimal input state to the channel is sent by another message of the prover, thus adding up to three messages in total. As such, the algorithm is clearly in QIP.

To show that the problem is QIP-Hard, we map an arbitrary QIP problem to an instance $(\mathcal{N}, \{U_{RS}(g)\}_{g\in G})$ of Channel-G-BSE. Since QIP(3) ≡ QIP [KW00], our goal is to find a correspondence between an arbitrary QIP(3) protocol and a choice of channel and group, $(\mathcal{N}, \{U_{RS}(g)\}_{g\in G})$. Specifically, from the circuit descriptions for a QIP(3) algorithm, we will identify a channel $\mathcal{N}_{R''\to S'}$ and a unitary representation $\{V_{R'S'}(g)\}_{g\in G}$ corresponding to a G-BSE problem, and we will show how the symmetry-testing condition

$$\max_{\substack{\rho_{R''}\in\mathcal{D}(\mathcal{H}_{R''}),\\ \sigma_{S'}\in \mathrm{BSE}_G}} F(\mathcal{N}_{R''\to S'}(\rho_{R''}), \sigma_{S'}) \tag{4.316}$$

can be written in terms of the QIP(3) algorithm's acceptance probability.

To begin, recall that an arbitrary QIP(3) problem consists of three messages exchanged and involves a first prover unitary $P^1_{E''\to R''E}$, a first verifier unitary $U^1_{SAR''\to S'R}$, a second prover unitary $P^2_{RE\to R'E'}$, and a second verifier unitary $U^2_{S'R'\to DG'}$ where D is the decision qubit. (Here we leave the dependence of the prover unitaries on x to be implicit.) The acceptance probability is thus,

$$p_{\mathrm{acc}} = \max_{\substack{P^1_{E''\to R''E},\\ P^2_{RE\to R'E'}}} \left\| (\langle 1|_D \otimes I_{GE'}) U^2_{S'R'\to DG} P^2_{RE\to R'E'} U^1_{SAR''\to S'R} P^1_{E''\to R''E} |x\rangle_S |0\rangle_A |0\rangle_{E''} \right\|_2^2. \tag{4.317}$$

Defining the first state after the action of the prover's unitary P^1 to be

$$|\psi\rangle_{R''E} := P^1_{E''\to R''E} |0\rangle_{E''}, \tag{4.318}$$

and the isometry

$$W_{R''\to S'R} := U^1_{SAR''\to S'R} |x\rangle_S |0\rangle_A, \tag{4.319}$$

the acceptance probability can then be written as

$$\begin{aligned} p_{\text{acc}} &= \max_{\psi_{R''E}, P^2_{RE\to R'E'}} \operatorname{Tr}[(|1\rangle\langle 1|_D \otimes I_{E'G}) U^2 P^2 W \psi_{R''E} W^\dagger P^{2\dagger} U^{2\dagger}] \\ &= \max_{\psi_{R''E}, P^2_{RE\to R'E'}} \operatorname{Tr}[U^{2\dagger}(|1\rangle\langle 1|_D \otimes I_{E'G}) U^2 P^2 W \psi_{R''E} W^\dagger P^{2\dagger}], \end{aligned} \tag{4.320}$$

where we have used cyclicity of trace in the last line. We can also identify the aforementioned channel $\mathcal{N}_{R''\to S'}$ as follows:

$$\mathcal{N}_{R''\to S'}(\cdot) \coloneqq \operatorname{Tr}_R[W(\cdot)_{R''} W^\dagger]. \tag{4.321}$$

Motivated by the expression in (4.320), we pick the group G to be C_2 with unitary representation $\{I_{R'S'}, V_{R'S'}\}$, where

$$V_{R'S'} \coloneqq (U^2_{R'S'\to DG})^\dagger \, (-Z_D \otimes I_G) \, U^2_{R'S'\to DG}. \tag{4.322}$$

We note that $V^2_{RS} = I_{RS}$, proving that this is indeed a representation of C_2. The resulting group projection is then

$$\begin{aligned} \Pi^G_{R'S'} &= \frac{1}{2}(I_{R'S'} + V_{R'S'}) \\ &= \frac{1}{2}\left(U^{2\dagger}(I_D \otimes I_G) U^2 + U^{2\dagger} \, (-Z_D \otimes I_G) \, U^2\right) \\ &= \frac{1}{2}\left(U^{2\dagger} \, (I_{DG} - (Z_D \otimes I_G)) \, U^2\right) \\ &= U^{2\dagger}(|1\rangle\langle 1|_D \otimes I_G) U^2, \end{aligned} \tag{4.323}$$

which is precisely the acceptance projection in (4.320). That is,

$$p_{\text{acc}} = \max_{\substack{\psi_{R''E}, \\ P^2_{RE\to R'E'}}} \operatorname{Tr}[\Pi^G_{R'S'} P^2 W \psi_{R''E} W^\dagger P^{2\dagger}] \tag{4.324}$$

Now invoking [LRW23, Theorem III.3], we conclude that

$$\begin{aligned} p_{\text{acc}} &= \max_{\psi_{R''E}, P^2_{RE\to R'E'}} \operatorname{Tr}[\Pi^G_{R'S'} P^2 W \psi_{R''E} W^\dagger P^{2\dagger}] \\ &= \max_{\psi_{R''E}, P^2_{RE\to R'E'}} \left\| \Pi^G_{R'S'} P^2 W |\psi\rangle_{R''E} \right\|_2^2 \\ &= \max_{\substack{\rho_{R''} \in \mathcal{D}(\mathcal{H}_{R''}), \\ \sigma_{S'} \in \text{BSE}_G}} F(\mathcal{N}_{R''\to S'}(\rho_{R''}), \sigma_{S'}), \end{aligned} \tag{4.325}$$

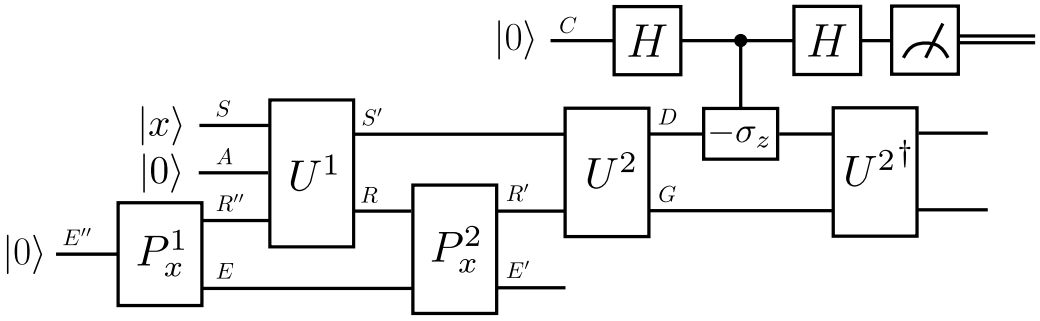


Figure 4.47: Circuit to map an arbitrary QIP algorithm to a G-Bose symmetric extendibility test on the output of a channel.

where in this case BSE_G is defined in the same way as in (4.294). To help visualize the reduction, the G-Bose symmetric extendibility test corresponding to a general QIP algorithm is depicted in Figure 4.47.

Thus, the acceptance probability of the QIP algorithm now exactly matches the symmetry-testing condition of the constructed G-BSE problem. As such, any QIP problem can be efficiently mapped to testing G-BSE of the output of a channel, proving that the problem Channel-G-BSE is QIP-Hard. Along with the fact that the problem lies in the QIP class, this concludes the proof. ■

4.6.9 Testing Hamiltonian symmetry using maximum spectral norm is in QMA

In this section, we show that testing whether a Hamiltonian is symmetric with respect to a group representation and the maximum spectral norm is in QMA. In particular, we consider the following task: given a group G with unitary representation $\{U(g)\}_{g\in G}$, a time $t \in \mathbb{R}$, and a classical description of a local or sparse Hamiltonian H, estimate the following quantity:

$$\max_{g\in G} \left\| [U(g), e^{-iHt}] \right\|_\infty^2 , \tag{4.326}$$

where the spectral norm of a matrix A is defined as

$$\|A\|_\infty := \sup_{|\psi\rangle\in\mathcal{H}} \{ \|A|\psi\rangle\|_2 : \||\psi\rangle\|_2 = 1 \} . \tag{4.327}$$

The quantity in (4.326) is a faithful measure of asymmetry in the following sense:

$$\begin{aligned} &\max_{g\in G} \left\| [U(g), e^{-iHt}] \right\|_\infty^2 = 0 \quad \forall t \in (-\delta, \delta), \\ \Leftrightarrow \quad &[U(g), e^{-iHt}] = 0 \quad \forall g \in G, t \in (-\delta, \delta), \\ \Leftrightarrow \quad &[U(g), H] = 0 \quad \forall g \in G, \end{aligned} \tag{4.328}$$

where $\delta > 0$. The first equivalence follows from faithfulness of the spectral norm, and the second equivalence follows by taking the derivative of the second line at $t = 0$.

Problem 4.9 [*Ham-Sym-Max-Spec*]. *Let α and β be such that $0 \leq \beta < \alpha \leq 2$, and fix $t \in \mathbb{R}$. Given are circuit descriptions of a unitary representation $\{U(g)\}_{g\in G}$ of a group G and a classical description of a k-local or sparse Hamiltonian H. Decide which of the following holds:*

$$\textit{Yes:} \quad \max_{g\in G} \left\| [U(g), e^{-iHt}] \right\|_\infty^2 \geq \alpha, \tag{4.329}$$

$$\textit{No:} \quad \max_{g\in G} \left\| [U(g), e^{-iHt}] \right\|_\infty^2 \leq \beta, \tag{4.330}$$

In what follows, we show that Ham-Sym-Max-Spec is in QMA, and it remains an interesting open question to determine whether this problem is QMA-Hard or hard for some other complexity class.

Theorem 4.14. *The promise problem Ham-Sym-Max-Spec is in QMA.*

Proof. Consider the following steps of a QMA interactive proof (see Figure 4.48):

1. The prover sends a state in registers C and P, with the dimension of C being equal to $|G|$ and the dimension of P being equal to the dimension of H.
2. The verifier measures the register C and obtains the outcome $g \in G$.
3. The verifier adjoins a qubit C' in the state $|+\rangle$, performs the Hamiltonian evolution e^{iHt}, the controlled unitary $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U^\dagger(g)$, the Hamiltonian evolution e^{-iHt}, and the controlled unitary $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U(g)$.
4. The verifier measures the qubit C' in the Hadamard basis $\{|+\rangle, |-\rangle\}$ and accepts if the outcome $|-\rangle$ occurs.

As noted in the previous section, there exist multiple methods to realize an efficient circuit for the Hamiltonian evolutions e^{-iHt} and e^{iHt} (see [CMN+18] and

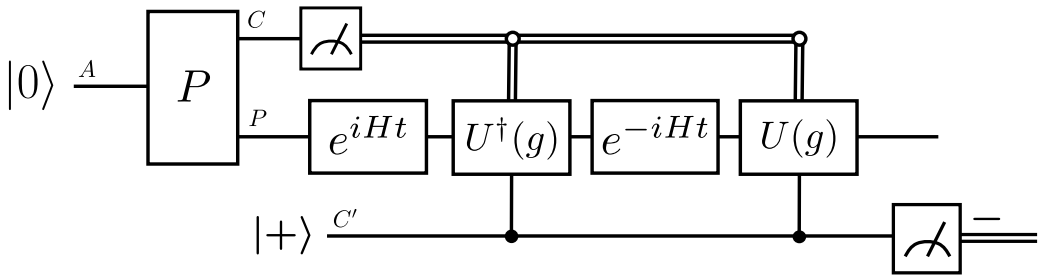


Figure 4.48: Circuit depicting a QMA test for Hamiltonian symmetry with respect to a group, where it is understood that the unitary P is implemented by an all-powerful prover. The final measurement is in the Hadamard basis, and the algorithm accepts if the $|-\rangle$ outcome occurs.

references therein). We also note that there are some similarities, as well as key differences, between this algorithm and that given in Figure 3 of [PVM21].

Let us now analyze the acceptance probability of this interactive proof. It suffices for the prover to send a pure state, as this maximizes the acceptance probability. Let us expand a fixed pure state $|\psi\rangle_{CP}$ of registers C and P as follows:

$$|\psi\rangle_{CP} = \sum_{g\in G} \sqrt{p(g)}|g\rangle_C|\psi_g\rangle_P, \tag{4.331}$$

where $\{p(g)\}_g$ is a probability distribution and $\{|\psi_g\rangle_P\}_g$ is a set of states. After the verifier's measurement in Step 2, the probability of obtaining outcome $g \in G$ is $p(g)$ and the post-measurement state of register P is $|\psi_g\rangle_P$. Conditioned on the outcome g and defining the unitary $W(g,t) \equiv U(g)e^{-iHt}U^\dagger(g)e^{iHt}$, the acceptance probability of Steps 3-4 is then given by

$$\left\|(\langle -|_{C'} \otimes I_P)\frac{1}{\sqrt{2}}(|0\rangle_{C'}|\psi_g\rangle_P + |1\rangle_{C'}W(g,t)|\psi_g\rangle_P)\right\|_2^2 = \frac{1}{4}\left\|(I - W(g,t))|\psi_g\rangle_P\right\|_2^2. \tag{4.332}$$

Thus, for a fixed state $|\psi\rangle_{CP}$ of the prover, the acceptance probability is given by

$$\frac{1}{4}\sum_{g\in G} p(g)\left\|(I - W(g,t))|\psi_g\rangle_P\right\|_2^2, \tag{4.333}$$

and finally maximizing over all such states leads to the following expression for

the acceptance probability:

$$\begin{aligned}
&\max_{|\psi\rangle_{CP}} \frac{1}{4} \sum_{g\in G} p(g) \left\| (I - W(g,t))|\psi_g\rangle_P \right\|_2^2 \\
&= \frac{1}{4} \max_{\substack{\{p(g)\}_g, \\ \{|\psi_g\rangle_P\}_g}} \sum_{g\in G} p(g) \left\| (I - W(g,t))|\psi_g\rangle_P \right\|_2^2 \\
&= \frac{1}{4} \max_{\{p(g)\}_g} \sum_{g\in G} p(g) \max_{\{|\psi_g\rangle_P\}_g} \left\| (I - W(g,t))|\psi_g\rangle_P \right\|_2^2 \\
&= \frac{1}{4} \max_{\{p(g)\}_g} \sum_{g\in G} p(g) \left\| I - W(g,t) \right\|_\infty^2 \\
&= \frac{1}{4} \max_{g\in G} \left\| I - W(g,t) \right\|_\infty^2 \\
&= \frac{1}{4} \max_{g\in G} \left\| I - U(g) e^{-iHt} U^\dagger(g) e^{iHt} \right\|_\infty^2 \\
&= \frac{1}{4} \max_{g\in G} \left\| e^{-iHt} U(g) - U(g) e^{-iHt} \right\|_\infty^2 \\
&= \frac{1}{4} \max_{g\in G} \left\| [U(g), e^{-iHt}] \right\|_\infty^2 . \qquad (4.334)
\end{aligned}$$

The third equality follows from the definition of the spectral norm. The fourth equality follows because the optimal distribution is a point mass on the largest value of $\|I - W(g,t)\|_\infty^2$. The penultimate equality follows from unitary invariance of the spectral norm. In light of the above analysis, the best strategy of the prover is to compute $\max_{g\in G} \left\| [U(g), e^{-iHt}] \right\|_\infty^2$ in advance, send the maximizing value of g in register C, and send the corresponding state that achieves the spectral norm in register P. As the acceptance probability of this QMA interactive proof is precisely related to the decision criteria in Problem 4.9, this concludes the proof. ■

4.6.10 Testing Hamiltonian symmetry using average spectral norm is in QAM

In this section, we show that testing whether a Hamiltonian is symmetric with respect to a group representation and the average spectral norm is in QAM. In particular, we consider the following task: given a group G with unitary representation $\{U(g)\}_{g\in G}$, a time $t \in \mathbb{R}$, and a classical description of a local or sparse

Hamiltonian H, estimate the following quantity:

$$\frac{1}{|G|}\sum_{g\in G}\left\|[U(g),e^{-iHt}]\right\|_\infty^2. \tag{4.335}$$

This is a faithful measure of symmetry in the following sense:

$$\begin{aligned}\frac{1}{|G|}\sum_{g\in G}\left\|[U(g),e^{-iHt}]\right\|_\infty^2 = 0 \quad &\forall t\in(-\delta,\delta),\\ \Leftrightarrow \qquad [U(g),e^{-iHt}] = 0 \quad &\forall g\in G, t\in(-\delta,\delta),\\ \Leftrightarrow \qquad [U(g),H] = 0 \quad &\forall g\in G,\end{aligned} \tag{4.336}$$

where $\delta > 0$. The first equivalence follows from faithfulness of the spectral norm, and the second equivalence follows by taking the derivative of the second line at $t = 0$.

Problem 4.10 [*Ham-Sym-Avg-Spec*]. *Let α and β be such that $0 \leq \beta < \alpha \leq \gamma$, where γ is defined in (4.200), and fix $t \in \mathbb{R}$. Given are circuit descriptions of a unitary representation $\{U(g)\}_{g\in G}$ of a group G and a classical description of a k-local or sparse Hamiltonian H. Decide which of the following holds:*

$$\textit{Yes:} \quad \frac{1}{|G|}\sum_{g\in G}\left\|[U(g),e^{-iHt}]\right\|_\infty^2 \geq \alpha, \tag{4.337}$$

$$\textit{No:} \quad \frac{1}{|G|}\sum_{g\in G}\left\|[U(g),e^{-iHt}]\right\|_\infty^2 \leq \beta, \tag{4.338}$$

In what follows, we show that Ham-Sym-Avg-Spec is in QAM, and it remains an interesting open question to determine whether this problem is QAM-Hard or hard for some other complexity class.

Theorem 4.15. *The promise problem Ham-Sym-Avg-Spec is in QAM.*

Proof. Consider the following steps of a QAM interactive proof (see Figure 4.49):

1. The verifier and prover are given a value $g \in G$ chosen uniformly at random.
2. The prover prepares a state $|\psi_g\rangle$ in register P, which depends on the value g and which has dimension equal to that of H.
3. The verifier adjoins a qubit C' in the state $|+\rangle$, performs the Hamiltonian evolution e^{iHt}, the controlled unitary $|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes U^\dagger(g)$, the Hamiltonian evolution e^{-iHt}, and the controlled unitary $|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes U(g)$.

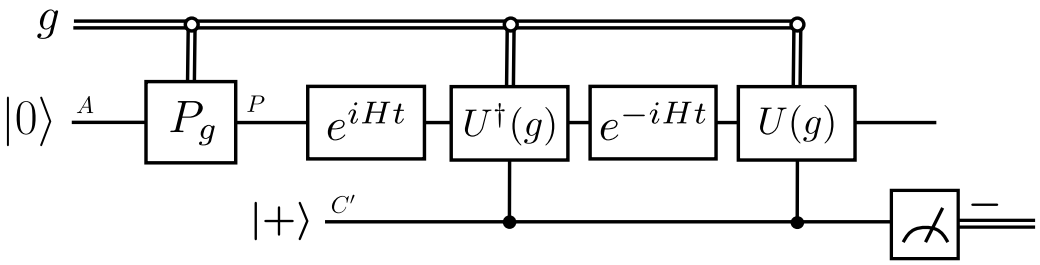


Figure 4.49: Circuit depicting a QAM test for Hamiltonian symmetry with respect to a group, where it is understood that the unitary P is implemented by an all-powerful prover. The final measurement is in the Hadamard basis, and the algorithm accepts if the $|-\rangle$ outcome occurs.

4. The verifier measures the qubit C' in the Hadamard basis $\{|+\rangle, |-\rangle\}$ and accepts if the outcome $|-\rangle$ occurs.

Let us now analyze the acceptance probability of this interactive proof. We define the set of states $\{\left|\psi_g\right\rangle = P_g |0\rangle\}_{g\in G}$. Conditioned on the value g, the prover's state is $\left|\psi_g\right\rangle$, and defining the unitary $W(g,t) \equiv U(g)e^{-iHt}U^\dagger(g)e^{iHt}$, the acceptance probability of Steps 3-4 is then given by

$$\left\| (\langle -|_{C'} \otimes I_P) \frac{1}{\sqrt{2}} (|0\rangle_{C'} |\psi_g\rangle_P + |1\rangle_{C'} W(g,t)|\psi_g\rangle_P) \right\|_2^2 = \frac{1}{4} \left\| (I - W(g,t))|\psi_g\rangle_P \right\|_2^2 . \quad (4.339)$$

Thus, for a fixed set $\{P_g\}_g$ of prover unitaries and averaging over the shared uniform randomness, the acceptance probability is given by

$$\frac{1}{4|G|} \sum_{g\in G} \left\| (I - W(g,t))|\psi_g\rangle_P \right\|_2^2 . \quad (4.340)$$

Finally maximizing over all such prover unitaries leads to the following expression for the acceptance probability:

$$\begin{aligned} &\max_{\{P_g\}_g} \frac{1}{4|G|} \sum_{g\in G} \left\| (I - W(g,t))|\psi_g\rangle_P \right\|_2^2 \\ &= \frac{1}{4|G|} \sum_{g\in G} \|I - W(g,t)\|_\infty^2 \\ &= \frac{1}{4|G|} \sum_{g\in G} \left\| [U(g), e^{-iHt}] \right\|_\infty^2 , \end{aligned} \quad (4.341)$$

where the reasoning is the same as that in (4.334). As the acceptance probability of this QAM interactive proof is precisely related to the decision criteria in Problem 4.10, this concludes the proof. ■

4.7 Conclusion

In summary, we have proposed various quantum computational tests of symmetry, as well as various notions of symmetry like G-symmetric extendibility and G-Bose symmetric extendibility, which include previous notions of symmetry from [MS13, MS14, Wer89a, DPS02, DPS04] as special cases, showing that these these new notions of symmetry provide a generalization with interesting applications. These tests have acceptance probabilities equal to various maximum symmetric fidelities, thus endowing these measures with operational meanings. We have also established resource theories of asymmetry beyond those proposed in [MS13], which put the maximum symmetric fidelities on firm ground in a resource-theoretic sense. Finally, we evaluated the quantum computational tests on existing quantum computers, by employing a variational algorithm to replace the role of the prover in a quantum interactive proof.

We have also established the computational complexity of various symmetry-testing problems. In particular, we showed that the various problems are complete for BQP, QMA, QSZK, QIP(2), $\mathrm{QIP}_{\mathrm{EB}}(2)$, and QIP, encompassing much of the known suite of quantum interactive proof models. We proved hardness results by embedding various circuits involved in a given computation into the preparation of a state or channel or into a unitary representation of a group. Finally, we introduced two Hamiltonian symmetry-testing problems and proved that they are contained in QMA and QAM.

Going forward from here, there are several directions to consider:

- Let us observe that several key resources such as entanglement and distinguishability have been connected to the quantum interactive proof hierarchy, through the findings of [HMW14, GHMW15] and [KW00, Wat02a, RW05, Wat09d, HMW14, RASW23], respectively. Our work makes a nontrivial link between this hierarchy and asymmetry, another key resource. These connections make us wonder whether other resources in quantum mechanics, such as coherence, magic, athermality, etc. [CG19], can be linked with the same hierarchy.

- We are curious whether the two aforementioned Hamiltonian symmetry-testing problems could be shown to be complete for QMA and QAM, respectively, or complete for some other quantum complexity class of interest.
- Several multipartite separability problems were identified in [PRRW24] and related to a quantum interactive proof setting in which there is a prover who performs a measurement, sends the classical outcome to multiple provers, who then send states to the verifier. One could thus try to find a symmetry-testing problem that is complete for this class.
- Various quantum algorithms for testing symmetries of channels, measurements, and Lindbladians under the Hilbert–Schmidt norm were proposed recently in [BRRW23]. One could attempt to show that corresponding symmetry-testing problems are complete for BQP.

All code and data used to generate these results is available via the GitHub repository located at https://github.com/Soorya-Rethin/Testing-Symmetry.

Chapter 5

Energy

Nature prefers the path of least energy — the quiet equilibrium where all forces balance. -— Anonymous (or Physics folklore)

This chapter is based on collaborative work with Alexander Wei, Ethan Guo, Dr. Mark M. Wilde, and Dr. Kristina D. Launey [RGW+24a]. Throughout this section, 'we' refers to all five collaborators.

5.1 Introduction

The atomic nucleus is a quantum many-body system made of nucleons that are subject to residual strong forces that have no analytical solution. For an A-particle system, the nuclear problem needs to be solved numerically in the infinite-dimensional Hilbert space of A particles with Hamiltonians that admit state-of-the-art nucleon-nucleon (NN) forces, often three-nucleon (3N), and even four-nucleon (4N) forces. This leads to the so-called scale explosion problem in nuclear structure calculations, i.e., the explosive growth in computational resource demands with increasing number of particles and size of the spaces in which they reside. Major progress in the development of high-precision inter-nucleon interactions [BvK02, ENG+02, EM03, Epe06, EKM15] along with the utilization of high-performance computing resources have tremendously advanced nuclear science

explorations. This has placed *ab initio* (or from first principles) large-scale simulations at the frontier of physics, including, for example, accurate theoretical predictions for light muonic atoms [JNDBB13], scattering calculations of interest to astrophysics and energy applications [ELR+15, HQN19, LMD21], as well as input to high-precision beta-decay measurements that probe physics beyond the standard model [SLB+22, B+22].

The situation is even more complicated when one needs accurate descriptions of nuclear reactions – the dynamics of several nuclei (reaction fragments) that interact, – especially in regions of the nuclear chart where experiments are currently infeasible. A general approach to reactions, especially suitable for heavier nuclear systems, is based on identifying few-body degrees, typically the reaction fragments (or clusters) involved in the reaction, and reduce the many-body problem to a few-body technique [TN09]. This reduction results in effective interactions (often referred to as optical potentials) between the clusters. Here again, the demand in classical computational resources grows exponentially with the number of reaction fragments and the range of their interaction.

With a view toward addressing such challenges in the long term by harnessing the advantages of quantum computing – as demonstrated for various low- and high-energy nuclear physics problems (e.g., see [DMH+18, CLB+21, TRA+22, SBC22, JJMS22, KGL+22, IS23, T+23, W+23, DSS23, PORM+23, BS24]) – in this paper, we start with the simplest case of two clusters, one of which is a neutron. We provide, for the first time, solutions of the neutron-nucleus dynamics from quantum simulations suitable for the far-term error-corrected regime as well as for the noisy intermediate-scale quantum (NISQ) processors coupled with the noise-resilient (NR) training method [SKCC20]: this is illustrated for the bound-state physics of the neutron-alpha (n-^{4}He) optical potential rooted in first principles [BLM+24], as well as for the lowest $\frac{1}{2}^+$ energy in Carbon isotopes calculated through the n+^{10}C, n+^{12}C, and n+^{14}C dynamics. We note that, in distinction to terminology often used in quantum computing, "dynamics simulation" or "simulation of (nuclear) dynamics" refer here to the problem of modeling the nuclear multi-cluster system using a specific inter-cluster potential.

The present method utilizes the Variational Quantum Eigensolver (VQE) [PMS+14, CAB+21, BCLK+22] and is based on the pioneering nuclear simulations of the deuteron on quantum computers, where the potential is given only by a single matrix element [DMH+18]. In our study, we design a novel quantum algorithm for a two-cluster system and a very general potential, which allows for versatile applications, including widely used exponential potentials in reaction

calculations (see, e.g., Ref. [DB10]) and most importantly, optical potentials derived *ab initio*. We note here that the choice of VQE can be replaced with any other technique, for example, tensor network warm starting, etc.

In this paper, we provide a generalized, extensible, and strong mathematical formulation of three mappings to qubits: one-hot, binary, and Gray encodings (see, e.g., [SMK+20]), explore their relative advantages, and illustrate these for simulations with the above-mentioned potentials. Going beyond the scope of earlier work that explored specific properties of mappings based on simulations only (e.g., see [SA21]), we provide mathematical proofs of scaling for these three encodings. Furthermore, the techniques that we use to prove these results are applicable for general encodings. Based on this, we show that the Gray encoding (introduced to nuclear calculations in Ref. [DMMG+21]) allows for an efficient scaling of the model-space size N (or number of the basis states used) and is more resource efficient not only for tridiagonal Hamiltonians ($K = 1$), as suggested in Ref. [SMK+20], but also for band-diagonal Hamiltonians for $K < N/2$, where $2K + 1$ is the bandwidth of the Hamiltonian. Interestingly, we show that for bandwidths larger than N, more off-diagonals can be added, if needed for an increased accuracy, without increasing the complexity of the problem. Another outcome of this study relates to the efficacy of measurements, which is of key importance to obtaining acceptable outcomes on quantum devices. In particular, we introduce a new commutativity scheme called distance-grouped commutativity (DGC), which is especially useful for band-diagonal matrices. We compare its performance with the well-known qubit-commutativity (QC) scheme. We lay out the explicit grouping of Pauli strings and the diagonalizing unitary under the DGC scheme. We show that the DGC scheme outperforms the QC scheme, at the cost of a more complex diagonalizing unitary. We note here that the diagonalizing unitary turns out to be the GHZ preparation unitary (See Lemma D.16 for the mathematical definition), and these have been used for diagonalization in quantum simulations [SCLW22, FCP+23].

We note that, in this study, the quantum simulations are reported for the lowest bound states of two clusters, for which a manageable number of qubits can be currently used (three or four qubits). Ultimately, the algorithm presented here can underpin multi-cluster dynamics simulations at low energies, such as those relevant to astrophysical studies, and can be utilized for weakly-bound states (e.g., for n+^{16}C and n+^{18}C) and even for isolated low-lying resonances that require solutions in much larger model spaces (larger N)[1]. Knowledge about the bound-

[1]Applications of the present quantum algorithm are shown here for the use of har-

state physics is key, e.g., to the description of deuteron break-up reactions, such as (d,p) and (d,n) reactions, for which standard distorted-wave Born approximation methods rely on the physics of the bound states of the proton-nucleus and neutron-nucleus systems. As another important implication, exploring trade-offs of band-diagonal and full Hamiltonian matrices for different encodings is critical for the simplest two-cluster system of two nucleons; namely, this allows quantum simulations of nuclear structure to handle the complete form of the chiral nucleon-nucleon (NN) potentials (e.g., see [EM03, Epe06, EKM15]), which are in turn key to *ab initio* large-scale simulations of light, medium-mass, and even selected heavy nuclei.

We provide solutions for various n+C systems using an exponential potential, and for n+α based on the *ab initio* optical potential derived in Ref. [BLM+24]. We find that the quantum simulations are successful in finding the lowest $\frac{1}{2}^+$ bound-state energies. We develop a warm-start algorithm, inspired by perturbation theory, that is particularly useful for band-diagonal Hamiltonians. In this method, we first simulate the system for a simpler, leading-order, Hamiltonian, and use the endpoint of the simulation as the start for the full-scale simulation. We find that this method allows for a quicker convergence to the true energy value.

Our paper is intended to serve interdisciplinary research at the intersection of nuclear physics and quantum information science, and in some cases includes details that may be well known in one of the fields but are pedagogical for researchers of the other field: our aim here is to provide a complete framework for the problem at hand. Our paper is organized as follows. In Sec. 5.2, we introduce the nuclear problem of solving the neutron-nucleus dynamics and its Hamiltonian. In Sec. 5.3, we discuss different encoding methods of mapping the given Hamiltonian to a form that can be simulated on a quantum computer. The different encoding methods we discuss include the one-hot encoding, binary encoding, and the Gray encoding. In Sec. 5.4, we briefly explain the variational principle, for completeness of presentation. Since the variational principle depends on the choice of a trial state, called ansatz, we delineate the different ansatz choices for the different encodings. In Sec. 5.5, we analyze various advantages between the different encodings considered, including the number of Pauli terms and the number of commuting sets, for a most general local potential and its band-diagonal

monic oscillator single-particle basis states, the same square-integrable basis utilized in Refs. [QN09, DLE+20, BLM+24, SLB+22], while the asymptotics are recovered in an R-matrix technique [TN09]. Alternatively, one can use the quantum algorithm for a square-nonintegrable basis, such as the eigenstates of the Woods-Saxon potential as utilized, e.g., in Ref. [MMP19].

approximation. As part of our trade-off analysis for the different encodings of Hamiltonians, we introduce the new DGC measurement scheme to group Pauli strings into commuting operator sets. For this scheme we provide the explicit diagonalizing unitary and an analysis of the number of commuting sets. In Sec. 5.6, we provide quantum simulations for different encodings and nuclear systems, including comparisons of the different commuting sets. We discuss the results and challenges for weakly bound states.

5.2 Problem description

A many-body "configuration interaction" (CI) method (often called the shell model in nuclear physics [BG77, Sha98, BNV13]) solves the many-body Schrödinger equation for A particles:

$$H\Psi(\vec{r}_1, \vec{r}_2, \ldots, \vec{r}_A) = E\Psi(\vec{r}_1, \vec{r}_2, \ldots, \vec{r}_A), \tag{5.1}$$

for which the interaction and basis configurations are adopted as follows. The intrinsic non-relativistic nuclear and Coulomb interaction Hamiltonian is defined as

$$H = T_{\text{rel}} + V_{\text{NN}} + V_{\text{3N}} + \cdots + V_{\text{Coulomb}}, \tag{5.2}$$

where $T_{\text{rel}} = \frac{1}{A}\sum_{i<j}\frac{(\vec{p}_i-\vec{p}_j)^2}{2m_{\text{N}}}$ is the relative kinetic energy (m_{N} is the nucleon mass), $V_{\text{NN}} = \sum_{i<j}^{A}(V_{\text{NN}})_{ij}$ is the nucleon-nucleon (NN) interaction (and possibly, $V_{\text{3N}} = \sum_{i<j<k}^{A}(V_{\text{NNN}})_{ijk}$, V_{4N}, ... interactions), and V_{Coulomb} is the Coulomb interaction between the protons. The Hamiltonian may also include higher-order electromagnetic interactions, such as magnetic dipole-dipole terms.

A complete orthonormal basis $\{\psi_i\}_i$ is adopted, such that the expansion $\Psi(\vec{r}_1, \vec{r}_2, \ldots, \vec{r}_A)$ in terms of unknown coefficients c_k, $\Psi(\vec{r}_1, \vec{r}_2, \ldots, \vec{r}_A) = \sum_k c_k\psi_k(\vec{r}_1, \vec{r}_2, \ldots, \vec{r}_A)$, renders Eq. (5.1) into a matrix eigenvalue equation:

$$\sum_{k'} H_{kk'}c_{k'} = Ec_k, \tag{5.3}$$

where the many-particle Hamiltonian matrix elements $H_{kk'} = \langle\psi_k|H|\psi_{k'}\rangle$ are in general complex and are calculated for the given interaction Eq. (5.2). Typically, the basis is a finite set of antisymmetrized products of single-particle states (Slater determinants), referred to as a "model space". In this study, we use the

single-particle states of a three-dimensional spherical harmonic oscillator (HO), $\phi_{n_r(\ell\frac{1}{2})jmt_z}(\vec{r})$, where n_r is the radial quantum number, the orbital angular momentum ℓ and spin-$\frac{1}{2}$ are coupled to the total angular momentum j, and t_z distinguishes between protons and neutrons (we use the convention of HO wavefunctions that are positive at infinity). Such a basis allows for preservation of translational invariance of the nuclear self-bound system and provides solutions in terms of single-particle wave functions that are analytically known. With larger model spaces utilized in the shell-model theory, the eigensolutions converge to the exact ones.

To describe the neutron-nucleus (NA) dynamics, e.g., for n-α, where α (with $A = 4$ particles) is in its ground state $\left|\Psi_0^{(A=4)}\right\rangle$ with energy $E_0^{(4)}$, one can deduce an effective non-local interaction $\tilde{V}(r, r')$ between the neutron and the four-body system using the Green's function approach [BLM+24], where r (and r') is the relative distance between the two clusters before (and after) scattering. This is based on solutions of the five-body system, that is, all states $\left|\Psi_k^{(5)}\right\rangle$ with their energy $E_k^{(5)}$, along with their single-particle overlaps $u_k(\vec{r}) = \left\langle\Psi_k^{(5)}\right| a_{\vec{r}}^\dagger \left|\Psi_0^{(4)}\right\rangle$, where $a_{\vec{r}}^\dagger$ creates a single particle at distance $\vec{r}$. This $\tilde{V}(r, r')$ potential, which can be readily derived in the *ab initio* framework (see Ref. [BLM+24] for n-α), can be rendered into an equivalent local form $V(r)$ according to Eq. (31) of Ref. [RDH+17],

$$V(r)u(r) = \int dr'\, r'^2\, \tilde{V}(r, r')\, u(r'), \tag{5.4}$$

where $u(r)$ is in units of fm$^{-3/2}$ and $V(r)$ is in units of MeV. We note that for bound states and resonances for which only the elastic channel is open, the potentials are real, except on the poles, which can be numerically avoided through the principal value theorem as shown in Ref. [BLM+24]; while in this study, we do not need the imaginary part of the $\tilde{V}(r, r')$ optical potential for the bound-state simulations at hand, the generalization to complex matrices is straightforward and feasible. The potential energy $V(r)$ enters into the two-body Schrödinger equation, as described next.

Let $\vec{r}_1$ and $\vec{p}_1$ be the position and momentum vector of the nucleus, and let $\vec{r}_2$ and $\vec{p}_2$ be the position and momentum vector of the neutron (or any reaction fragment). Thus, the Hamiltonian of the $A + 1$ nuclear system is given by

$$\tilde{H} = \frac{p_1^2}{2m_1} + \frac{p_2^2}{2m_2} + V(|\vec{r}_1 - \vec{r}_2|), \tag{5.5}$$

where m_1 is the mass of the nucleus and m_2 is the mass of the neutron. Since we are interested in the relative motion of the projectile (the neutron) relative to the target (nucleus), we make a transformation to the center-of-mass coordinate, $\vec{R} = \frac{m_1\vec{r_1}+m_2\vec{r_2}}{m_1+m_2}$, and relative coordinate, $\vec{r} = \vec{r_1} - \vec{r_2}$:

$$\tilde{H} = \frac{P^2}{2M} + \frac{p^2}{2\mu} + V(r), \text{ with } H = \frac{p^2}{2\mu} + V(r), \tag{5.6}$$

where $M = m_1 + m_2$ is the total mass, $\mu = \frac{m_1 m_2}{m_1+m_2}$ is the reduced mass (usually reported in terms of the nucleon mass m_N and the mass numbers of the target A and projectile a as $\mu = \frac{Aa}{A+a}m_\mathrm{N}$), and we use that $\vec{P} = \vec{p_1} + \vec{p_2}$ and $\vec{p} = \frac{m_2\vec{p_1}-m_1\vec{p_2}}{m_1+m_2}$. The term $\frac{P^2}{2M}$ represents the kinetic energy of the centre of mass. Since $[P, p] = 0$ and $[P, r] = 0$, this term can be dealt with independently. Thus, in the center-of-mass reference frame, we need to solve Eq. (5.3), where $T = \frac{p^2}{2\mu}$ is the relative kinetic energy and $V(r)$ is the potential energy or the effective neutron-nucleus interaction. We focus on the ${}^2S_{\frac{1}{2}}$ partial wave (following the notation ${}^{2s+1}\ell_J$): α (or an even-even Carbon isotope) is in a 0^+ ground state, the relative orbital angular momentum is $\ell = 0$, the spin of the neutron is $s = 1/2$, yielding total angular momentum $J = 1/2$ (and since the projectile is a neutron, there is no Coulomb interaction). For this channel (and any positive-parity channel), the most general central potential can be expressed as

$$V(r) = \sum_{k=0}^{\infty} v_k r^{2k}, \tag{5.7}$$

where the coefficients v_k are taken to be real for all k in this work, since we are interested in the bound-state physics. To represent this Hamiltonian on a quantum computer, we use a discrete-variable representation in the harmonic-oscillator basis, for which the radial wave functions are known analytically. In this basis, the Hamiltonian is an infinite-dimensional matrix. However, in order to perform simulations, we truncate the matrix to an $N \times N$ matrix, called H_N (retaining the notations of Ref. [DMH+18]). As the size N of the matrix increases, the approximation to the true Hamiltonian becomes more accurate. Expanding in this basis,

$$H_N \coloneqq \sum_{n_r,n_r'=0}^{N-1} \langle n_r'|T + V|n_r\rangle |n_r'\rangle\langle n_r|, \tag{5.8}$$

where n_r denotes a relative harmonic oscillator radial node number. The matrix

elements of T for every ℓ are given by

$$\langle n_r'\ell|T|n_r\ell\rangle := \frac{\hbar\omega}{2}\Bigg[\left(2n_r+\frac{3}{2}\right)\delta_{n_r',n_r} - \sqrt{\left(n_r-\frac{\ell}{2}\right)\left(n_r+\frac{\ell+1}{2}\right)}\delta_{n_r',n_r-1} - \sqrt{\left(n_r-\frac{\ell-2}{2}\right)\left(n_r+\frac{\ell+3}{2}\right)}\delta_{n_r',n_r+1}\Bigg], \quad (5.9)$$

where in Ref. [DMH+18] and in this paper we use $\ell = 0$ (hence, we will omit the ℓ notation henceforth). The matrix representation of T is tridiagonal; i.e., the only non-zero elements are the main diagonal and one diagonal each above and below it.

The matrix elements of V are given as

$$\langle n_r'|V|n_r\rangle = \sum_{k=0}^{\infty} v_k \langle n_r'|r^{2k}|n_r\rangle. \quad (5.10)$$

To calculate the matrix elements of r^{2k}, we use a recursive approach,

$$\langle n_r'|r^{2k}|n_r\rangle = \sum_{n_r''=0}^{\infty} \langle n_r'|r^{2k-2}|n_r''\rangle\langle n_r''|r^2|n_r\rangle, \quad (5.11)$$

with the base case for every ℓ being

$$\langle n_r'\ell|r^2|n_r\ell\rangle := b_s^2\Bigg[\left(2n_r+\frac{3}{2}\right)\delta_{n_r',n_r} + \sqrt{\left(n_r-\frac{\ell}{2}\right)\left(n_r+\frac{\ell+1}{2}\right)}\delta_{n_r',n_r-1} + \sqrt{\left(n_r-\frac{\ell-2}{2}\right)\left(n_r+\frac{\ell+3}{2}\right)}\delta_{n_r',n_r+1}\Bigg], \quad (5.12)$$

where the oscillator length is defined in terms of the reduced mass and $\hbar\omega$. Also, $b_s := \sqrt{\frac{\hbar}{\mu\omega}}$ (and $\ell = 0$ is used in this study).

A schematic of the matrices of this problem description is given in Fig. 5.1b, as compared to the one used in Ref. [DMH+18] with a single matrix element (Fig. 5.1a).

In many cases, it is advantageous to approximate, to a very good degree, the neutron-nucleus potential by an exponential form:

$$V(r) \approx V_{\mathrm{E}}(r) = V_0 \exp\left(-c(r/b_s)^2\right). \quad (5.13)$$

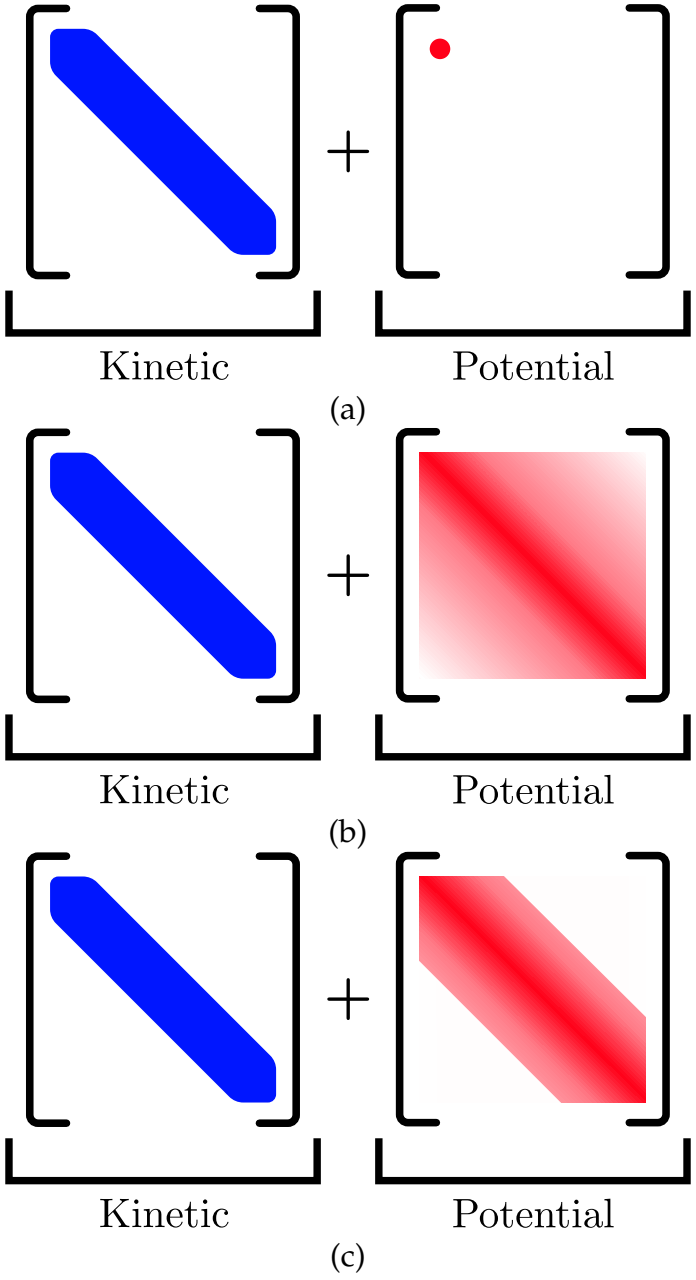


Figure 5.1: The kinetic and potential energy matrices: (a) for the contact potential used in Refs. [DMH+18, DMMG+21], (b) for the complete potential $V(r)$, and (c) for the truncated potential $V_K(r) = \sum_{k=0}^{K} v_k r^{2k}$ used in this work.

Expanding the potential as a Taylor series around $r = 0$ leads to

$$V_{\rm E}(r) = V_0 \sum_{k=0}^{\infty} \frac{(-1)^k c^k}{k!} \left(\frac{r}{b_s}\right)^{2k} . \tag{5.14}$$

Finally, for the quantum simulations, we set an upper truncation parameter K for the number of terms in the expansion. Therefore, the potential is given by

$$\langle n_r' | V_K | n_r \rangle = \sum_{k=0}^{K} v_k \langle n_r' | r^{2k} | n_r \rangle, \tag{5.15}$$

with $v_k = V_0(-1)^k c^k/(k! b_s^{2k})$ in the case of the exponential approximation $V_{\rm E}(r)$ of Eq. (5.13). We note that the matrix representation of r^2 is tridiagonal and in general, the matrix representation of r^{2K} is $(2K+1)$-diagonal. A schematic of the truncated matrices of this problem description suitable for quantum simulations is given in Fig. 5.1c.

The quantum computational simulations of nuclear systems of Ref. [DMH+18, DMMG+21] have used a contact potential for $\ell = 0$, or $\langle n_r' | V | n_r \rangle = V_0 \delta_{n_r, n_r'} \delta_{n_r, 0}$ (Fig. 5.1a). In this work, the Hamiltonian is generalized for any band-diagonal to full matrix and can now accommodate a general central potential, such as exponential Gaussian-like potentials using Eq. (5.13) (e.g., [DB10]), along with *ab initio* inter-cluster potentials (as those derived in Ref. [BLM+24]) and the central part of chiral NN potentials using Eq. (5.7). In general, chiral NN potentials, such as in Refs. [EM03, Epe06, EKM15], used in *ab initio* nuclear calculations require, in addition, spin and isospin degrees of freedom $\alpha = n_r(\ell \frac{1}{2}) jmt_z$, as described above. Including the additional spin-isospin quantum numbers leads to a larger set of basis states, but nonetheless, in the present framework this is straightforward by generalizing Eq. (5.8) to

$$H = \sum_{\alpha,\alpha'} \langle \alpha' | T + V | \alpha \rangle | \alpha' \rangle\langle \alpha |, \tag{5.16}$$

where $\langle \alpha' | V | \alpha \rangle$ are known matrix elements for any chiral NN potential and the enumerating index α replaces n_r in the mappings to qubits discussed next. Importantly, physically relevant potentials with a comparatively soft core or widely used potentials renormalized using, e.g., the Similarity Renormalization Group (SRG) technique [BFP07], are band-diagonal as a result of the decoupling of low- and high-momentum configurations. Hence, the advantages found in this study as a function of the bandwidth $2K+1$ directly generalize to the complete form of the chiral NN potentials and their routinely used band-diagonal structure.

5.3 Mapping onto a quantum computer

In the current form, the Hamiltonian from Eq. (5.8) is given in terms of number operators of the form $|m\rangle\langle m|$ and step-i ladder operators of the form $|m\rangle\langle m-i|$ and $|m\rangle\langle m+i|$ for $i \in \{1, \ldots, K\}$ (using the notation of Ref. [DMMG+21]). To find the bound-state energy of this Hamiltonian, we first need to map these operators into Pauli strings.

Mappings from operators in the Fock space to Pauli strings are called *encodings*. Multiple encodings can be found in existing literature, for example, the one-hot encoding (OH), the Bravyi-Kitaev encoding, the Verstraete-Cirac encoding, the binary encoding, and the Gray encoding (see, e.g., [SMK+20, DMMG+21, VC05]. In addition, there has been substantial work on using qudits (higher dimensional systems) rather than qubits, which has been shown to provide some advantage in specific scenarios [IRS23, VENN24, BRS+21]. In this work, we focus on three qubit encodings - OH, binary, and Gray - and analyze various properties and trade-offs.

To provide an illustrative example, for each encoding above, we show the explicit Pauli terms for the $N = 4, K = 2$ Hamiltonian with the exponential potential in Eq. (5.13) with parameters

$$V_0 = -2.79\,\text{MeV},\ c = 0.05,\ \hbar\omega = 15.95\,\text{MeV}, \tag{5.17}$$

for the case of n+^{16}C with reduced mass $\mu = \frac{16}{17} m_N$ (here we use $m_N = 938.272029$ MeV for both protons and neutrons). The Hamiltonians for the different encodings can be found in their respective sections below.

We note that the development for the ladder operators and step-1 operators follows directly from [DMMG+21]. We generalize these results to step-k operators, for $k > 1$, in this section.

One-hot encoding

For fixed N, the one-hot encoding maps the number and ladder operators to Pauli strings on N qubits. The Fock basis states are mapped as follows:

$$|m\rangle \to |q_0 q_1 \ldots q_{N-1}\rangle\,, \tag{5.18}$$

for $m \in \{0, \ldots, N-1\}$, where $q_m = 1$ and all other bits are zero. For example, for $N = 4$, the states are mapped as

$$\begin{aligned} |0\rangle &\rightarrow |1000\rangle, \\ |1\rangle &\rightarrow |0100\rangle, \\ |2\rangle &\rightarrow |0010\rangle, \\ |3\rangle &\rightarrow |0001\rangle. \end{aligned} \tag{5.19}$$

Next, we define the number operators and ladder operators. The number operator $|m\rangle\langle m|$ maps $|m\rangle$ to itself and maps all other basis states to 0:

$$(|m\rangle\langle m|)\,|m'\rangle = \delta_{m,m'}\,|m\rangle\,. \tag{5.20}$$

Thus, in the encoded basis, the number operators are mapped to

$$|m\rangle\langle m| \rightarrow |1\rangle\langle 1|_m \coloneqq \frac{1}{2}(I_m - Z_m), \tag{5.21}$$

where the subscript m indicates the qubit on which the operator acts, that is, e.g., $Z_2 = I \otimes I \otimes Z \otimes I \otimes \cdots \otimes I$.

Next, the action of the ladder operator $|m\rangle\langle m \pm i|$ on the number states is as follows:

$$(|m\rangle\langle m \pm i|)\,|m'\rangle = \delta_{m\pm i,m'}\,|m\rangle\,. \tag{5.22}$$

In this encoded basis, this action involves flipping the $(m \pm i)$ qubit to 0 and the m qubit to 1:

$$\begin{aligned} |m\rangle\langle m \pm i| &\rightarrow |1\rangle\langle 0|_m \otimes |0\rangle\langle 1|_{m\pm i} \\ &= \frac{1}{2}(X_m - \mathrm{i}Y_m) \otimes \frac{1}{2}(X_{m\pm i} + \mathrm{i}Y_{m\pm i}) \\ &= \frac{1}{4}(X_m X_{m\pm i} + \mathrm{i}X_m Y_{m\pm i} - \mathrm{i}Y_m X_{m\pm i} + Y_m Y_{m\pm i}). \end{aligned} \tag{5.23}$$

We note that these ladder operators always occur in pairs due to the Hermiticity of the Hamiltonian. Thus,

$$|m\rangle\langle m \pm i| + |m \pm i\rangle\langle m| = \frac{1}{2}(X_m X_{m\pm i} + Y_m Y_{m\pm i}). \tag{5.24}$$

The rest of the operators can be constructed similarly. The list of all operators for $N = 4$ can be found in Appendix D.2.

Substituting the above defined number and ladder operators into Eq. (5.8), we find the representation of $H_{N,K}$ in the one-hot encoding to be

$$H_{N,K} = \frac{1}{2}\sum_{m=0}^{N-1}\langle m|H|m\rangle(I_m - Z_m) + \frac{1}{2}\sum_{m=0}^{N-1}\sum_{k=1}^{\max(K,1)}\langle m+k|H|m\rangle(X_mX_{m+k} + Y_mY_{m+k}). \quad (5.25)$$

The upper limit of the k summation is $\max(K, 1)$ due to the fact that even if $K = 0$, the first off-diagonal term in the Hamiltonian is non-zero as a result of the kinetic energy having two off-diagonal terms. Note that, to preserve the size of the matrix to be N, the summation over k terminates if $m + k > N - 1$. Thus, in the encoded one-hot basis, if $K > 1$, the resulting matrix is $(2K + 1)$-diagonal.

For the example under consideration in Eq. (5.17), the encoded Hamiltonian is given by

$$\begin{aligned} H_{4,2} = {} & 67.117\ IIII - 4.674\ IIIZ - 12.751\ IIZI - 20.812\ IZII - 28.880\ ZIII \\ & - 4.814\ IIXX - 4.814\ IIYY - 8.801\ IXXI - 8.801\ IYYI - 12.772\ XXII \\ & - 12.772\ YYII - 0.004\ IXIX - 0.004\ IYIY - 0.014\ XIXI - 0.014\ YIYI, \end{aligned} \quad (5.26)$$

where we have truncated the coefficients to three decimal places.

Remark 5.1. *The Jordan–Wigner transformation is a mapping from fermionic operators to Pauli operators of the form:*

$$a_m^\dagger \to \frac{1}{2}\left[\prod_{j=0}^{m-1} Z_j\right](X_m - \mathrm{i}Y_m) \quad (5.27)$$

$$a_m \to \frac{1}{2}\left[\prod_{j=0}^{m-1} Z_j\right](X_m + \mathrm{i}Y_m). \quad (5.28)$$

We note that the Jordan–Wigner transformation and the one-hot encoding do not map a fermionic operator to the same Pauli string. The Jordan–Wigner transformation results in the following mapping:

$$a_m^\dagger a_{m+i} + a_{m+i}^\dagger a_m \to \frac{1}{2}\left(X_m\overline{Z}X_{m+i} + Y_m\overline{Z}Y_{m+i}\right), \quad (5.29)$$

where $\overline{Z} \equiv Z_{m+1}\otimes\cdots\otimes Z_{m+i-1}$. *On the other hand, the one-hot encoding results in the map:*

$$|m\rangle\langle m+i| + |m+i\rangle\langle m| \to \frac{1}{2}\left(X_mX_{m+i} + Y_mY_{m+i}\right). \quad (5.30)$$

While the operators in Eqs. (5.29) and (5.30) in general act differently, their action is identical on the set of encoded basis states given in Eq. (5.19). Thus, if we restrict the states to be superpositions of the encoded basis states only, these operators can be used interchangeably.

Binary encoding

For fixed N, the binary encoding maps the number and ladder operators to Pauli strings on $n = \lceil \log_2(N) \rceil$ qubits. For simplicity, we restrict N to be a power of two, in which case the encoded basis set is exactly of size $n = \log_2(N)$. The Fock basis states are mapped as follows:

$$|m\rangle \to |q_0 q_1 \dots q_{n-1}\rangle\,, \tag{5.31}$$

for $m \in \{0, \dots, N-1\}$, where the bitstring $q = q_0 q_1 \dots q_{n-1}$ is the binary representation of m, denoted by b_m, on n qubits. For the case of $N = 8$, the encoded basis consists of three qubits and is given by

$$\begin{aligned}
|0\rangle &\to |000\rangle,\\
|1\rangle &\to |001\rangle,\\
|2\rangle &\to |010\rangle,\\
|3\rangle &\to |011\rangle,\\
|4\rangle &\to |100\rangle,\\
|5\rangle &\to |101\rangle,\\
|6\rangle &\to |110\rangle,\\
|7\rangle &\to |111\rangle.
\end{aligned}$$

Thus, the binary basis $\mathcal{B}_n$, on $n = \log_2(N)$ qubits, is a list of N basis elements:

$$\mathcal{B}_n = (b_0, b_1, \dots, b_{2^n-1}), \tag{5.32}$$

where b_m is the binary representation of the integer m.

Next, let us consider how the number and ladder operators map. To this end, let us establish some notation for the following operators:

$$|m+k\rangle\langle m| \to B_m^k. \tag{5.33}$$

The number operators $|m\rangle\langle m|$ map to B_m^0, which are defined as

$$\begin{aligned} |m\rangle\langle m| \to B_m^0 &:= |b_m\rangle\langle b_m| \\ &= P_0^{b_{m,0}} \otimes P_1^{b_{m,1}} \otimes \cdots \otimes P_{n-1}^{b_{m,n-1}} \\ &= \bigotimes_{i=0}^{n-1} P_i^{b_{m,i}}, \end{aligned} \tag{5.34}$$

where $b_{m,i}$ denotes bit i of b_m and the operators P^0 and P^1 are defined as

$$\begin{aligned} P^0 &:= |0\rangle\langle 0| = \frac{1}{2}(I + Z), \\ P^1 &:= |1\rangle\langle 1| = \frac{1}{2}(I - Z). \end{aligned} \tag{5.35}$$

For example, the number operator $|6\rangle\langle 6|$ is mapped to

$$\begin{aligned} |6\rangle\langle 6| \to B_6^0 &= P_0^1 \otimes P_1^1 \otimes P_2^0 \\ &= |1\rangle\langle 1|_0 \otimes |1\rangle\langle 1|_1 \otimes |0\rangle\langle 0|_2. \end{aligned} \tag{5.36}$$

In a similar fashion, the step-1 ladder operators are mapped as follows:

$$|m+1\rangle\langle m| \to B_m^1 := \bigotimes_{i=0}^{n-1} |b_{m+1,i}\rangle\langle b_{m,i}|. \tag{5.37}$$

For example, the ladder operator

$$|4\rangle\langle 3| \to B_3^1 = |1\rangle\langle 0|_0 \otimes |0\rangle\langle 1|_1 \otimes |0\rangle\langle 1|_2, \tag{5.38}$$

as $|3\rangle$ and $|4\rangle$ are mapped to $|011\rangle$ and $|100\rangle$, respectively.

Step-k ladder operators for $k > 1$ are defined recursively in terms of step-1 ladder operators:

$$|m+k\rangle\langle m| \to B_m^k := B_{m+k-1}^1 B_m^{k-1}. \tag{5.39}$$

The list of all operators for $N = 4$ can be found in Appendix D.2.

Thus, substituting for the number and ladder operators in Eq. (5.8), we find the representation of $H_{N,K}$ in the binary encoding to be

$$H_{N,K} = \sum_{m=0}^{N-1} \langle m|H|m\rangle B_m^0 + \sum_{m=0}^{N-1} \sum_{k=1}^{\max(1,K)} \langle m+k|H|m\rangle (B_m^k + (B_m^k)^\dagger). \tag{5.40}$$

Note that the summation over i terminates if $m + k > N - 1$.

For the example under consideration Eq. (5.17), the encoded Hamiltonian is given by

$$H_{4,2} = 33.556\, II - 8.073\, ZI - 16.134\, IZ - 0.004\, ZZ - 0.014\, IX \\ + 7.959\, XZ - 0.006 ZX - 17.586\, XI - 8.801\, XX - 8.801\, YY. \quad (5.41)$$

Gray encoding

For a fixed N, the Gray encoding maps the number and ladder operators to Pauli strings on $n = \lceil \log_2(N) \rceil$ qubits. For simplicity, we restrict N to be a power of two, in which case the encoded basis set is exactly of size $n = \log_2(N)$. We first define the Gray basis on n bits, $\mathcal{G}_n$, as a list of 2^n basis elements:

$$\mathcal{G}_n = (g_0, g_1, \ldots, g_{2^n-1}), \quad (5.42)$$

where each $g_i = (g_{i,0}, g_{i,1}, \ldots g_{i,L-1})$ is a bitstring of length n. The only characteristic of a Gray encoding is that each bitstring entry g_i differs from its neighbor at a single bit. Thus, for a given n, there are multiple possible Gray codes. In this work, drawing inspiration from Ref. [DMMG+21], we use a binary reflective Gray code on n bits. Such a code is defined recursively as follows:

$$\mathcal{G}_n = (\mathcal{G}_{n-1} \cdot 0, \overline{\mathcal{G}_{n-1}} \cdot 1), \quad (5.43)$$

where $\overline{\mathcal{G}_n}$ is the Gray code on n bits with the entries in reverse order, and $X \cdot y$ is the list of entries of X with y appended at the end. For example, given that $\mathcal{G}_2 = (00, 10, 11, 01)$, we can construct $\mathcal{G}_3$ as follows:

$$\begin{aligned} \mathcal{G}_3 &= (\mathcal{G}_2 \cdot 0, \overline{\mathcal{G}_2} \cdot 1) \\ &= ((00, 10, 11, 01) \cdot 0, \overline{(00, 10, 11, 01)} \cdot 1) \\ &= (000, 100, 110, 010, 011, 111, 101, 001). \end{aligned} \quad (5.44)$$

Thus, for a fixed N, the Fock basis states are mapped to the corresponding entry in a Gray basis $\mathcal{G}_n$, where $n = \log_2(N)$:

$$|m\rangle \to |q_0 q_1 \ldots q_{n-1}\rangle, \quad (5.45)$$

for $m \in \{0, \ldots, N-1\}$, where the bitstring $q = q_0 q_1 \cdots q_{n-1}$ is the mth entry in the Gray basis g_m. For example, for $N = 8$, the encoded basis is made of three qubits:

$$
\begin{aligned}
|0\rangle &\rightarrow |000\rangle, \\
|1\rangle &\rightarrow |100\rangle, \\
|2\rangle &\rightarrow |110\rangle, \\
|3\rangle &\rightarrow |010\rangle, \\
|4\rangle &\rightarrow |011\rangle, \\
|5\rangle &\rightarrow |111\rangle, \\
|6\rangle &\rightarrow |101\rangle, \\
|7\rangle &\rightarrow |001\rangle.
\end{aligned}
$$

Next, let us consider how the number and ladder operators map. To this end, let us define the following operators:

$$
|m+k\rangle\langle m| \rightarrow G_m^k. \tag{5.46}
$$

The number operator $|m\rangle\langle m|$ is mapped to G_m^0, which is defined as

$$
|m\rangle\langle m| \rightarrow G_m^0 := \bigotimes_{i=0}^{n-1} P_i^{g_{m,i}}. \tag{5.47}
$$

To define the step-1 ladder operators, we use a similar construction as in the previous section:

$$
|m+1\rangle\langle m| \rightarrow G_m^1 := \bigotimes_{i=0}^{n-1} |g_{m+1,i}\rangle\langle g_{m,i}|. \tag{5.48}
$$

For example, the ladder operator connecting the basis elements $|2\rangle$ and $|3\rangle$ is given by

$$
|3\rangle\langle 2| \rightarrow G_2^1 = |0\rangle\langle 1|_0 \otimes P_1^1 \otimes P_2^0, \tag{5.49}
$$

since the $|3\rangle$ and $|2\rangle$ basis elements differ on the first bit and the other two bits are in the state $|10\rangle$. However, since the Hamiltonian is Hermitian, both the ladder-1 up and down operators are scaled with the same coefficient. Thus,

$$
G_2^1 + (G_2^1)^\dagger = X_0 \otimes P_1^1 \otimes P_2^0. \tag{5.50}
$$

We then go on to define the step-i ladder operators recursively with the step-1 ladder operators being the base case:

$$
\begin{aligned}
|m+i\rangle\langle m| &\rightarrow G_m^i \\
&:= (|m+i\rangle\langle m+i-1|)(|m+i-1\rangle\langle m|),
\end{aligned} \tag{5.51}
$$

where the ladder operators in the first parenthesis are defined as above. Next, we add an extra term that leads to the recursive definition needed. For example,

$$\begin{aligned} |4\rangle\langle 1| &= (|4\rangle\langle 3|)(|3\rangle\langle 1|) \\ &= (|4\rangle\langle 3| + |3\rangle\langle 4|)(|3\rangle\langle 1|) \\ &= (P_0^0 \otimes P_1^1 \otimes X_2)(|3\rangle\langle 1|), \end{aligned} \tag{5.52}$$

where $|3\rangle\langle 1|$ is defined similarly. The list of all operators for $N = 4$ can be found in Appendix D.2.

Thus, substituting for the number and ladder operators in Eq. (5.8), we find the representation of H_N in a Gray encoding with the potential truncation parameter set to K:

$$H_{N,K} = \sum_{m=0}^{N-1} \langle m|H|m\rangle G_m^0 + \sum_{m=0}^{N-1} \sum_{k=1}^{\max(K,1)} \langle m+k|H|m\rangle (G_m^k + (G_m^k)^\dagger). \tag{5.53}$$

Note that the summation over k terminates if $m + k > N - 1$.

For the example under consideration Eq. (5.17), the encoded Hamiltonian is given by

$$\begin{aligned} H_{4,2} = 33.556\, II - 16.133\, ZI - 0.004\, IZ - 8.073\, ZZ - 17.586\, IX \\ + 7.959\, ZX + 8.801 XZ - 8.801\, XI - 0.014\, XX - 0.006\, YY. \end{aligned} \tag{5.54}$$

5.4 Lowest-state energy computation by variational quantum eigensolver

5.4.1 Variational principle

For completeness, we summarize the variational principle that underpins the Variational Quantum Eigensolver (VQE). Given a Hamiltonian, the minimum energy eigenstate is called the ground state $|\psi_g\rangle$ and its energy E_g is called the ground-state energy[2]. More precisely, given a Hamiltonian H, the ground-state

[2]We note that for a model space restricted to a given total angular momentum J (spin) and parity π of the nucleus, the minimum energy eigenstate provides the lowest state for the given J^π and coincides with the ground state only if the ground state has the same spin-parity. For example,

energy and the ground state are defined as:

$$\begin{aligned} E_g &:= \min_{|\psi\rangle} \langle\psi|H|\psi\rangle, \\ \left|\psi_g\right\rangle &:= \operatorname*{argmin}_{|\psi\rangle} \langle\psi|H|\psi\rangle. \end{aligned} \tag{5.55}$$

To estimate the ground-state energy (lowest J^π state energy), we use a parameterized quantum circuit to attempt achieve the minimum. As discussed in Section 2.5, the loss function for a problem is defined in terms of the ansatz and the observable O. In this problem, the observable O is the Hamiltonian H, and the loss is relabelled as $E(\boldsymbol{\theta})$, where $\boldsymbol{\theta}$ are the parameters of the ansatz of choice. Thus,

$$\begin{aligned} E_{\boldsymbol{\theta}} &= \langle 0|U^\dagger(\boldsymbol{\theta})HU(\boldsymbol{\theta})\,|0\rangle \\ &= \langle\psi(\boldsymbol{\theta})|H\,|\psi(\boldsymbol{\theta})\rangle \geq \langle\psi_g|H\left|\psi_g\right\rangle = E_g. \end{aligned} \tag{5.56}$$

Since the inequality holds for every value $\boldsymbol{\theta}$, minimizing over every $\boldsymbol{\theta}$ provides an upper bound on the true ground-state energy:

$$E_g \leq \min_{\boldsymbol{\theta}} E_{\boldsymbol{\theta}}, \tag{5.57}$$

where the equality is achieved is the ansatz is fully expressive (See Section 2.5.1).

In this work, we use the Hamiltonian $H_{N,K}$ described in Sec. 5.2, with truncation parameter N for the size of the matrix and K for the potential (referred to as hyperparameters). The choice of the potential is either a general central potential deduced *ab initio* Eq. (5.7) or an exponential potential Eq. (5.13).

5.4.2 Ansatz description

The choice of ansatz depends on the encoding scheme used. The structure of the ansatz chosen should ideally be able to express all possible combinations of the encoded basis states. A general hardware-efficient ansatz can be used [KMT+17], but the symmetry and structure of the Hamiltonian can influence and direct the ansatz definition.

in the present study of Carbon isotopes, the lowest $\frac{1}{2}^+$ state is the ground state only for ^{15}C (the composite system for n+^{14}C) and ^{19}C (the composite system for n+^{18}C), while the other Carbon isotopes under consideration have a ground state of different spin-parity.

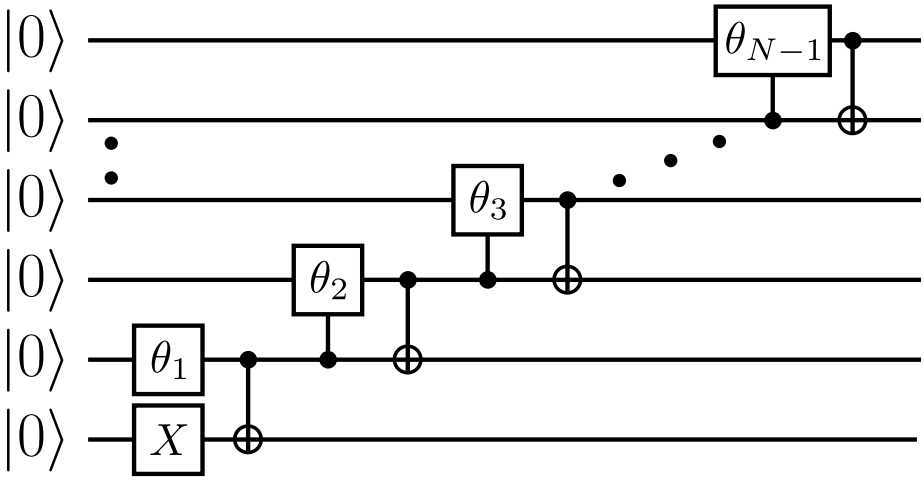


Figure 5.2: Recursive circuit ansatz to generate the superposition of the one-hot basis states. The input to the circuit is $|0\rangle^{\otimes N}$, and θ_i denotes the $R_y(2\theta_i) = \exp(-\mathrm{i}\theta_i Y_i)$ rotation gate.

Since the Hamiltonian is purely real, the eigenstates must be fully real. In conjunction with the fact that Hermitian matrices have real eigenvalues, this means that the Hamiltonian is diagonalized by an orthogonal transformation, and not a general unitary transformation. Thus, the ansatz unitary generates a real superposition of the basis states.

One-hot ansatz

For a given N, the ansatz choice for the one-hot encoding creates a real-coefficient superposition of the basis states. A pure state for an N-qubit one-hot basis with real coefficients can be expressed using generalized spherical coordinates. For example, with $N = 4$,

$$|\psi(\boldsymbol{\theta})\rangle = \cos\theta_1 |0001\rangle + \sin\theta_1 \cos\theta_2 |0010\rangle + \sin\theta_1 \sin\theta_2 \cos\theta_3 |0100\rangle + \sin\theta_1 \sin\theta_2 \sin\theta_3 |1000\rangle . \quad (5.58)$$

Thus, for a truncation parameter N, the state is parameterized by $N-1$ parameters. The encoded state can be generated recursively using R_y rotation gates and CNOT gates, as seen in Fig. 5.2.

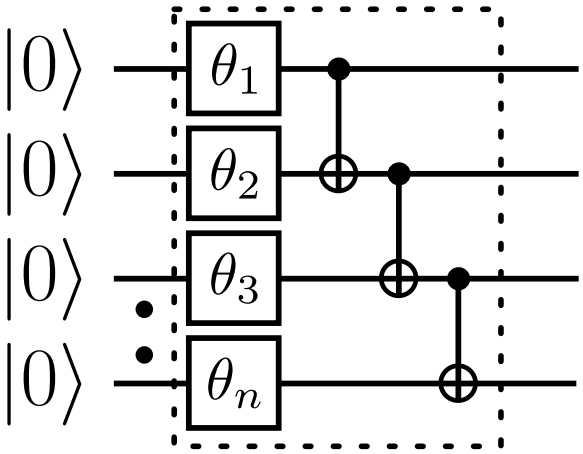


Figure 5.3: Circuit ansatz to generate a parameterized real superposition of all basis states. The input to the circuit is $|0\rangle^{\otimes n}$, where $n = \log_2(N)$. Each layer (marked with dotted lines) is repeated L times. Thus, the total number of parameters is nL.

Binary and Gray ansatz

In these encodings, we make use of the entire space spanned by the encoded basis states. This enables the use of a general hardware-efficient ansatz [KMT+17]. However, from the argument above, we restrict this ansatz to create real superpositions of the basis states. This can be done with R_y rotation gates and CNOT as the entangling gate. The ansatz is build up using multiple layers, each having a set of Y-rotations and entangling gates (see Fig. 5.3). The number of layers L is a hyperparameter that needs to be chosen such that the ansatz is expressive enough without increasing the number of parameters too much.

5.5 Encoding techniques and trade-offs

In this section, we explore the various trade-offs between the encoding techniques. Important parameters for any simulation include the number of Pauli terms in the encoded Hamiltonian, the number of commuting sets, etc. A comprehensive analysis for a contact potential, or $\langle n_r' | V | n_r \rangle = V_0 \delta_{n_r, n_r'} \delta_{n_r, 0}$ (see Fig. 5.1a), can be found in Ref. [DMMG+21]. We generalize these results for any band-diagonal to full Hamiltonian matrix needed to accommodate a general central potential, including exponential Gaussian-like potentials, *ab initio* inter-cluster potentials,

and the central part of any chiral NN potential for *ab initio* nuclear calculations. Furthermore, we provide new insights and we discuss open research directions proposed in Ref. [DMMG+21].

We note that, in the present study, the Hamiltonian for $K = 0$ (diagonal potential) is tridiagonal due to the kinetic energy term. As a result, the entries for $K = 1$ are used for $K = 0$. On the other hand, the most general results for a Hamiltonian matrix of $2K + 1$ bandwidth (that permits a diagonal matrix) are summarized in Table 5.1 for the one-hot encoding, Table 5.2 for the binary encoding and Table 5.3 for the Gray encoding.

5.5.1 Number of Pauli terms

One-hot encoding

As seen in Eq. (5.25), the encoded Hamiltonian for truncation parameters N, K is given by

$$H_{N,K} = \frac{1}{2}\sum_{m=0}^{N-1}\langle m|H|m\rangle(I_m - Z_m) + \frac{1}{2}\sum_{m=0}^{N-1}\sum_{k=1}^{K}\langle m+k|H|m\rangle(X_m X_{m+k} + Y_m Y_{m+k}), \tag{5.59}$$

with the k summation terminating when $m + k > N - 1$. The above equation is true for $K \geq 1$; the case for $K = 0$ is the same as $K = 1$, since the kinetic energy term is tridiagonal. This results from the truncation of the matrix to size $N \times N$.

In the first summation, the identity operator ($I^{\otimes N}$) and the N individual Z operators give a total of $N + 1$ Pauli terms (e.g., for three qubits, the terms are III, ZII, IZI, and IIZ). For the second term, we split the m summation into two parts: one with $m < N - K$ and $m \geq N - K$. In the first part, each k summation goes from 1 to K, contributing $2K$ terms. Thus, this part adds a total of $2K(N - K)$ terms. In the second part, the k summation is truncated before it reaches K. This contributes a total of $2[(K - 1) + (K - 2) + \ldots + 1]$. Thus, the total of the number of Pauli terms is

$$\left|H_{N,K}\right| = 1 + N + 2NK - K(K + 1), \tag{5.60}$$

as depicted in Fig. 5.4.

For the example of $N = 4$ and $K = 2$, we see that the number of terms is 15, confirmed by (5.26). Note that each of these terms acts on N qubits. We note that for $K > N/2$, we see that the number of Pauli terms is $O(N^2)$.

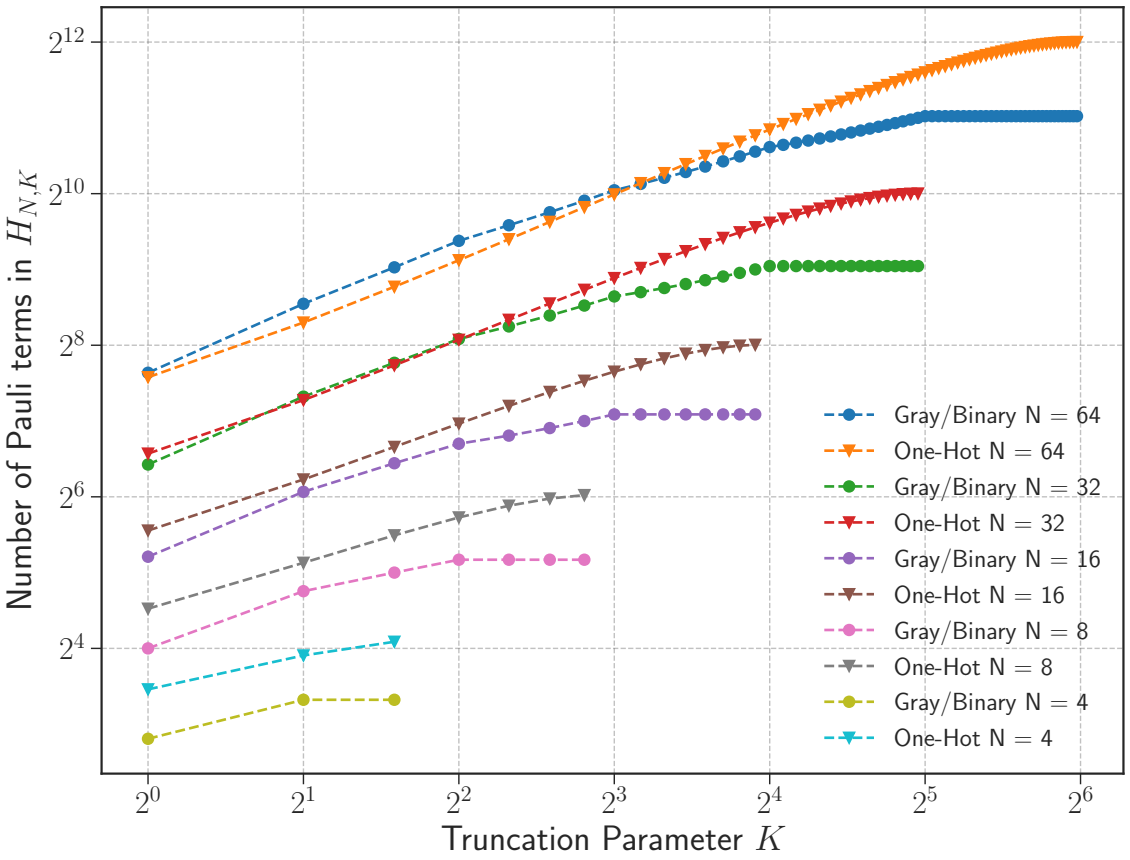


Figure 5.4: Number of Pauli terms for one-hot, binary, and Gray encodings for a general potential of the form $V_K(r) = \sum_{k=0}^{K} v_k r^{2k}$ and a general (tridiagonal to full) Hamiltonian matrix. Note that in the one-hot encoding, each term acts on N qubits, while in the binary and Gray encodings, each term acts on $n = \log_2(N)$ qubits.

Binary and Gray encoding

As seen in Eqs. (5.40) and (5.53), the encoded Hamiltonian for truncation parameters N, K is given by

$$H_{N,K} = \sum_{m=0}^{N-1} \langle m|H|m\rangle L_m^0 + \sum_{m=0}^{N-1} \sum_{k=1}^{K} \langle m+k|H|m\rangle (L_m^k + (L_m^k)^\dagger), \tag{5.61}$$

$H_{N,K}$	One-hot
	$0 \leq K \leq N$
Qubits	N
Pauli Terms	$1 + N + 2NK - K(K+1)$
QC Sets	3
Ansatz	2 one-qubit gates + $(2N-3)$ two-qubit gates

Table 5.1: Number of qubits, Pauli terms, and qubit-wise commuting sets for the one-hot code, for a general Hamiltonian matrix of $2K+1$ bandwidth. In the present study, the Hamiltonian for $K = 0$ (diagonal potential) is tridiagonal because of the kinetic energy term, in which case the entries for $K = 1$ should be used. More details can be found in Sec. 5.6.

where $L^i_j = B^i_j$ for the binary encoding and $L^i_j = G^i_j$ for the Gray encoding. The above equation is true for $K \geq 1$; the case for $K = 0$ is the same as $K = 1$, since the kinetic energy term is tridiagonal.

The number of Pauli terms in the Hamiltonian for both encodings is

$$|H(N,K)| = \begin{cases} \mathrm{d}(n,1) + n2^{n-1} & K = 0 \\ \mathrm{d}(n,K) + 2^{n-1} \sum_{k=1}^{K} \overline{n}_k & 1 \leq K \leq 2^{n-1} \\ 2^{n-1}(1+2^n) & K > 2^{n-1}, \end{cases} \tag{5.62}$$

as depicted in Fig. 5.4, where

$$\mathrm{d}(n,K) = \sum_{m=0}^{K} \binom{n}{m}, \tag{5.63}$$

and $\overline{n}_k := n - \lceil \log_2(k) \rceil$. The proof for this can be found in Lemma D.11. For the example of $N = 4, K = 2$, we see that the number of terms is 10, confirmed by Eqs. (5.41) and (5.54). For $K > N/2$, we see that the number of Pauli terms is $O(N^2)$.

To summarize, we show that the Gray and binary codes have the same number of Pauli terms for all N and K. Furthermore, the number of Pauli terms saturates above $K = N/2$. The one-hot encoding does not saturate, and at $K = 2^{n-1}$, the one-hot encoding always has more Pauli terms than the Gray or binary encoding. For the general potential in consideration (5.7), Fig. 5.4 plots the number of terms as a function of K for different N values.

5.5.2 Number of commuting sets

To measure any operator provided as a linear combination of Pauli strings,

$$O = \sum_{i=1}^{N_P} a_i P_i, \tag{5.64}$$

we can measure individual Pauli terms and sum the results, because

$$\mathrm{Tr}[O\rho] = \sum_{i=1}^{N_P} a_i \,\mathrm{Tr}[P_i\rho]. \tag{5.65}$$

Thus, for an operator consisting of N_P terms, we estimate the measurement statistics for each of the N_P terms.

Most quantum computers allow for measurements in the computational basis alone, i.e., in the Pauli-Z basis. If the Pauli term does not have Pauli-Z on a particular qubit, the qubit must first be rotated before a computational basis measurement. For example, to measure $X \otimes Z$ on a two-qubit state ρ,

$$\begin{aligned}\mathrm{Tr}[(X \otimes Z)\rho] &= \mathrm{Tr}[(H \otimes I)(Z \otimes Z)(H \otimes I)\rho] \\ &= \mathrm{Tr}[(Z \otimes Z)(H \otimes I)\rho(H \otimes I)].\end{aligned} \tag{5.66}$$

Thus, measuring $X \otimes Z$ is equivalent to applying Hadamard on the first qubit and then measuring in the computational basis.

A method to reduce the number of measurements is to measure commuting observables in their common eigenbasis. The idea of reducing the measurement complexity has led to a large number of advances [VYI2003, YVI2004, HMR+21]. Two commuting Pauli strings are guaranteed to have a common eigenbasis. Consider two Pauli strings A and B such that $[A, B] = 0$, and denote the common

eigenbasis as $\{|\psi_i\rangle\}_i$. Thus,

$$A = \sum_i a_i |\psi_i\rangle\langle\psi_i|, \qquad B = \sum_i b_i |\psi_i\rangle\langle\psi_i|. \tag{5.67}$$

The elements $|\psi_i\rangle$ are related to the computational basis elements $|i\rangle$ by a unitary transformation. More concretely,

$$|\psi_i\rangle = U\,|i\rangle\,. \tag{5.68}$$

Thus, to measure A and B simultaneously, we first apply the unitary $U^\dagger$ and then measure in the computational basis:

$$\begin{aligned} \mathrm{Tr}[A\rho] &= \sum_i a_i \,\mathrm{Tr}[|\psi_i\rangle\langle\psi_i|\rho] \\ &= \sum_i a_i \,\mathrm{Tr}[U|i\rangle\langle i|U^\dagger\rho] \\ &= \sum_i a_i \,\mathrm{Tr}[|i\rangle\langle i|U^\dagger\rho U], \end{aligned} \tag{5.69}$$

and similarly for B:

$$\mathrm{Tr}[B\rho] = \sum_i b_i \,\mathrm{Tr}[|i\rangle\langle i|U^\dagger\rho U]. \tag{5.70}$$

Thus, we can recreate the measurement statistics of both A and B by measuring the state $U^\dagger\rho U$ in the computational basis. To measure multiple observables, each element needs to pair-wise commute with all other elements. However, splitting a set of observables into commuting sets and finding the common eigenbasis is non-trivial. Furthermore, finding the U that rotates the computational basis into this common eigenbasis is also non-trivial.

We now look at two alternate simpler strategies. The first strategy is to look at qubit-wise commutativity (QC). Two Pauli strings qubit-wise commute if the corresponding operators acting on each qubit commute. For example, XIZ and XZI qubit-wise commute since $[X, X] = [I, Z] = [Z, I] = 0$. Qubit-wise commutativity is a sufficient, but not necessary, condition for general commutativity. For example, XX and YY commute but do not qubit-wise commute. Thus, this strategy leads to a sub-optimal grouping of Pauli strings. However, the grouping itself can be done efficiently, and the unitary that rotates the computational basis into the common eigenbasis is always a tensor product of individual Pauli operators.

In addition, in this paper, we introduce a new strategy that is based on grouping Pauli strings in terms of the distance operators defined in Appendix D.1. We

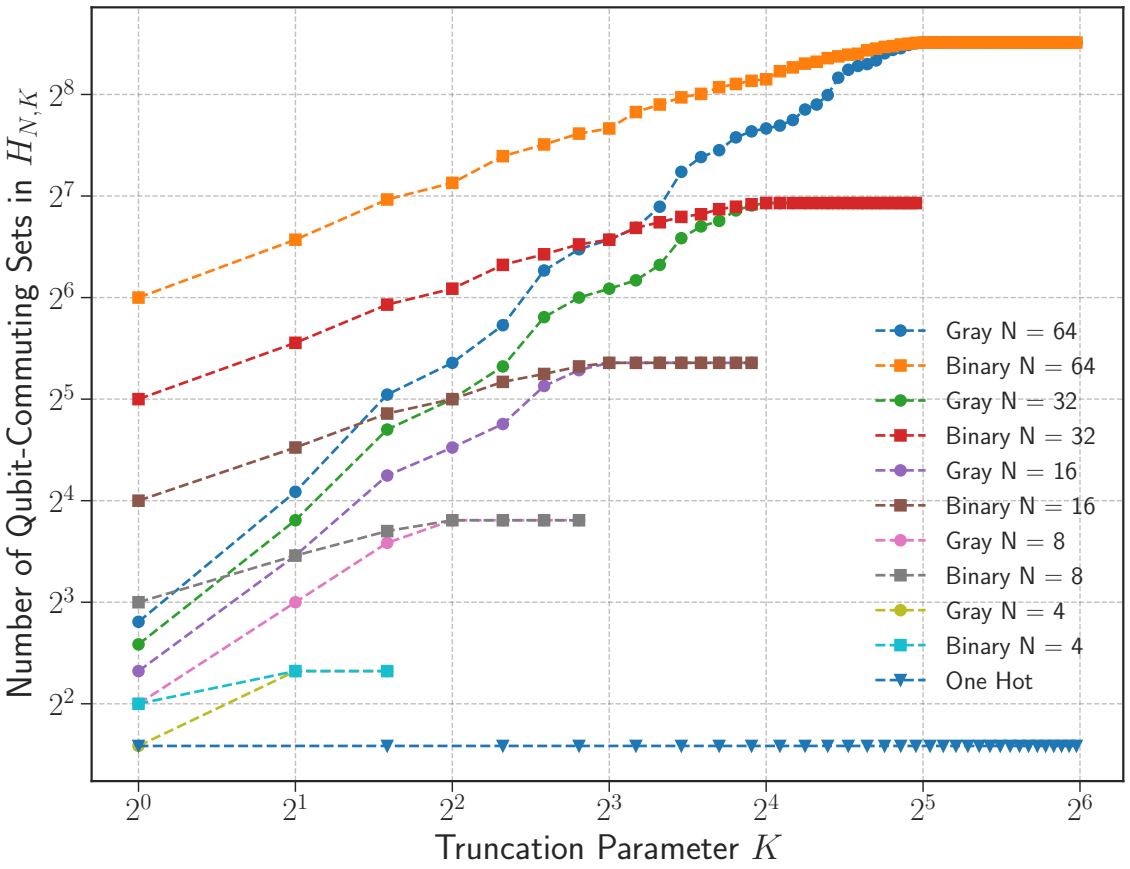


Figure 5.5: Number of qubit-wise commuting Pauli sets terms for one-hot, binary, and Gray encodings for a general potential of the form $V_K(r) = \sum_{k=0}^{K} v_k r^{2k}$ and a general (tridiagonal to full) Hamiltonian matrix.

refer to this grouping as distance-grouped commutativity (DGC). While the precise structure is not relevant here, it leads to a more optimal set of Pauli operators as compared to the qubit-wise scheme. However, the diagonalizing unitary, while simple conceptually, is no longer a tensor-product of individual Pauli operators (see Appendix D.1 for further details).

In this section, we analyze the number of QC and DGC sets that the Pauli terms can be split into, for all encodings. The number of sets as a function of the hyperparameter K and for various model-space sizes N is shown in Figs. 5.5-5.7.

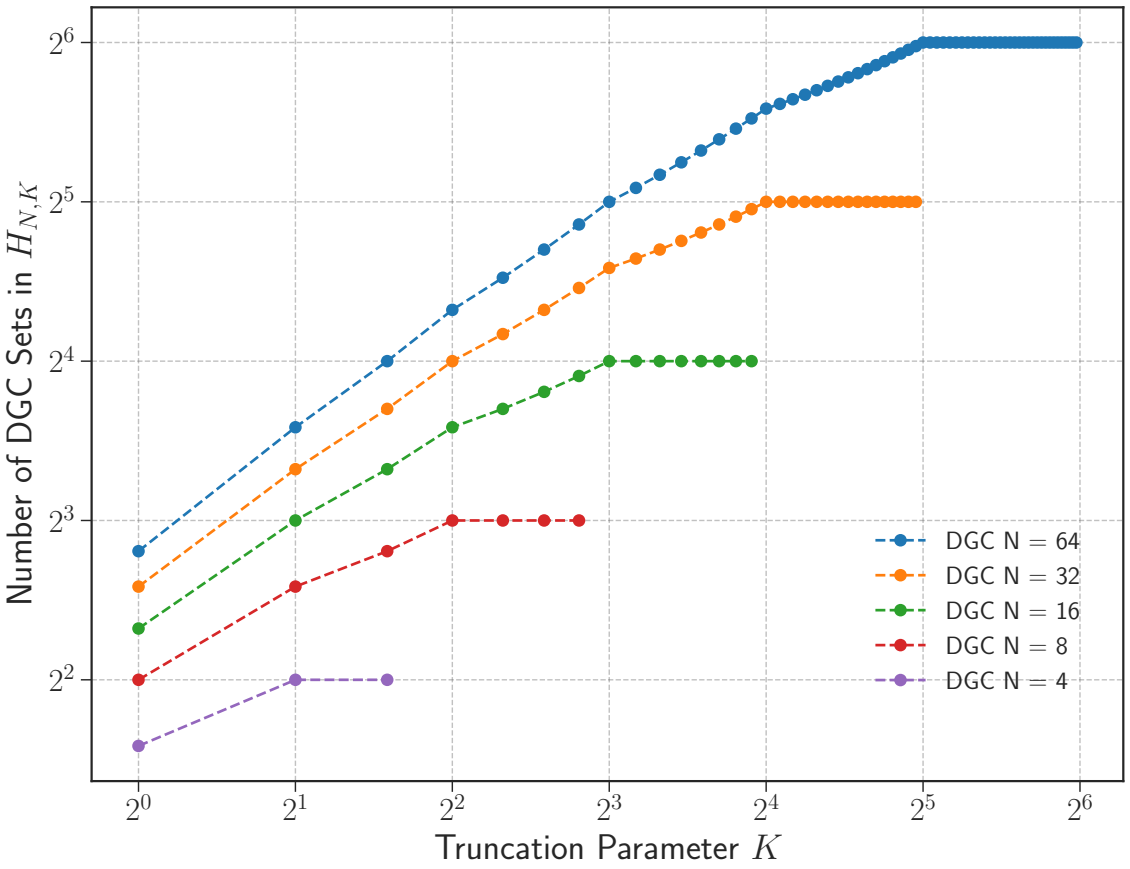


Figure 5.6: Number of DGC sets for the binary, and Gray encodings for a general potential of the form $V_K(r) = \sum_{k=0}^{K} v_k r^{2k}$ and a general (tridiagonal to full) Hamiltonian matrix.

One-hot encoding: Qubit-wise commutativity

As seen in Eq. (5.25), the first summation results from the number operators. These operators all qubit-wise commute, and their common eigenbasis is the computational basis. Thus, the statistics of these operators can be inferred from a measurement of $Z^{\otimes N}$. Similarly, the ladder operators can be split into two sets – one with only X and I, and another with only Y and I. Within each of these sets, all operators qubit-wise commute. Thus, the measurement statistics of all the operators can be inferred from the measurement of $\{X^{\otimes N}, Y^{\otimes N}\}$. Thus, the number of qubit-wise commuting sets is three.

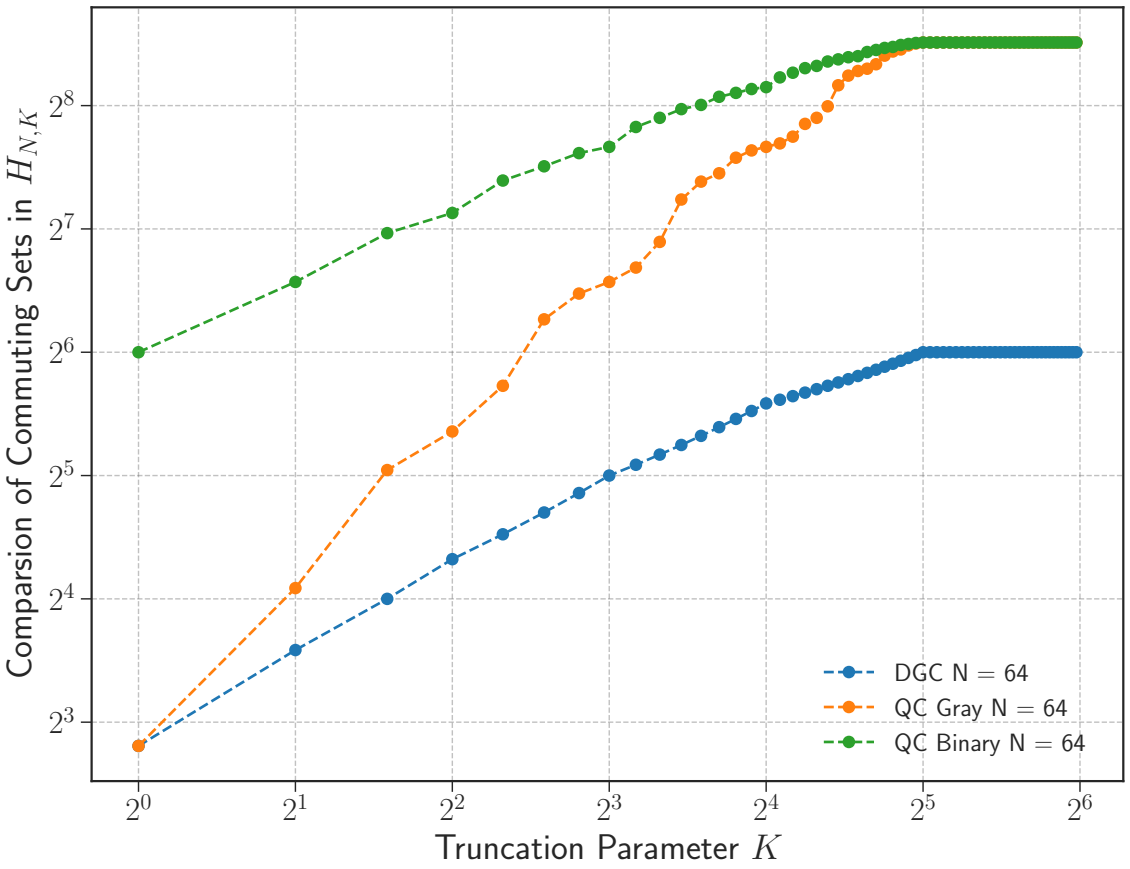


Figure 5.7: Comparing the two commutativity schemes for a general potential of the form $V_K(r) = \sum_{k=0}^{K} v_k r^{2k}$ and a general (tridiagonal to full) Hamiltonian matrix. We note that the DGC leads to fewer terms to be measured, at the cost of a more complex rotation gate into a common eigenbasis.

Binary encoding: Qubit-wise commutativity

As stated in Lemma D.13 in Appendix D.1, the number of qubit-wise commuting sets in a binary encoding is given by

$$|H(N,K)|_C = \begin{cases} 2^n & K = 0 \\ 1 + \sum_{k=1}^{K} 2^{|b_{\bar{k}}|} \left[1 - 2^{-\bar{n}_k}\right] & 1 \leq K \leq 2^{n-1} \\ \frac{1}{2}\left(1 + 3^n\right) & K > 2^{n-1}, \end{cases} \tag{5.71}$$

where $|w|$ is the Hamming weight of the string w, the variable $\bar{k}$ is defined as $2^n - k$, $\overline{n}_k := n - \lceil \log_2(k) \rceil$, and b_i denotes the binary representation of i. We first notice that the number of qubit-wise commuting sets for $K > N/2$ is $O(N^{\log_2(3)})$.

For the example of $N = 4, K = 2$ from Eq. (5.41), qubit-wise commutativity leads to the following sets:

$$\begin{aligned} &\{II, ZI, IZ, ZZ\}, \\ &\{IX, ZX\}, \\ &\{XI, XZ\}, \\ &\{XX\}, \\ &\{YY\}. \end{aligned} \tag{5.72}$$

Gray encoding: Qubit commutativity

As stated in Lemma D.14 in Appendix D.1, the number of qubit-wise commuting sets in a Gray encoding is given by

$$|H(N,K)|_C = \begin{cases} 1 + n & K = 0 \\ 1 + \sum_{k=1}^{K} 2^{|g_{k-1}|} \overline{n}_k & 1 \leq K \leq 2^{n-1} \\ \frac{1}{2}(1 + 3^n) & K > 2^{n-1}, \end{cases} \tag{5.73}$$

where $|w|$ is the Hamming weight of the string w, $\overline{n}_k := n - \lceil \log_2(k) \rceil$, and g_k denotes the kth entry in the Gray basis. We first notice that the number of sets for $K > N/2$ is $O(N^{\log_2(3)})$. The set of Pauli strings for $K > N/2$ being exactly the same as the binary encoding, leads to the number of commuting sets being equal. However, we note that for $K < N/2$ the Gray encoding leads to a lower number of qubit-wise commuting sets than the binary encoding. Indeed, the ordering of the computational basis elements in the Gray encoding favors low-weight Pauli strings for lower K, leading to a lower number of qubit-wise commuting sets.

For the example of $N = 4, K = 2$ from Eq. (5.54), qubit-wise commutativity

leads to the following sets:

$$\begin{aligned}&\{II, ZI, IZ, ZZ\},\\&\{IX, ZX\},\\&\{XI, XZ\},\\&\{XX\},\\&\{YY\}.\end{aligned} \tag{5.74}$$

Since this example is for the case of $K = N/2$, as expected, the number of QC sets is the same for both binary and Gray encodings.

Binary/Gray encoding: Distance-grouped commutativity

As seen in Lemma D.17, the number of distance-grouped commuting sets is given by

$$|H(N,K)|_C = \begin{cases} 1+n & K = 0 \\ 1 + \sum_{k=1}^{K} \overline{n}_k & 1 \leq K \leq 2^{n-1} \\ 2^n & K > 2^{n-1}, \end{cases} \tag{5.75}$$

where $\overline{n}_k \coloneqq n - \lceil \log_2(k) \rceil$. We note that the number of DGC sets for $K > N/2$ is $\mathcal{O}(N)$. However, each measurement requires a more complex unitary transformation to a common eigenbasis as compared to the qubit-commutative sets.

For the example of $N = 4, K = 2$ from Eqs. (5.54) and (5.41), distance-grouped commutativity leads to the following sets:

$$\begin{aligned}&\{II, ZI, IZ, ZZ\},\\&\{IX, ZX\},\\&\{XI, XZ\},\\&\{XX, YY\}.\end{aligned} \tag{5.76}$$

While the number of DGC sets for the Gray and binary encoding are exactly the same for all N and K, the complexity in the measurement procedure is not the same. We now quantify the complexity of the measurement scheme based on the number of two-qubit gates in the diagonalizing unitaries for both encodings.

As stated in Lemma D.19 in Appendix D.1, the number of two-qubit gates in the diagonalizing unitary using the DGC scheme for the binary code is given by

$$|H(N,K)|_{DU} = \begin{cases} 0.5n(n-1) & K = 0 \\ 0.5 \sum_{k=1}^{K} \overline{n}_k \left[2|b(\bar{k})| - 1 - \overline{n}_k \right] & 1 \leq K \leq 2^{n-1} \\ 1 + 2^{n-1}(n-2) & K > 2^{n-1}, \end{cases} \tag{5.77}$$

where $\overline{n}_k \coloneqq n - \lceil \log_2(k) \rceil$.

Similarly, from Lemma D.18 in Appendix D.1, the number of two-qubit gates in the diagonalizing unitary using the DGC scheme for the Gray code is given by

$$|H(N,K)|_{DU} = \begin{cases} 0 & K = 0 \\ \sum_{k=1}^{K} \overline{n}_k g_{k-1} & 1 \leq K \leq 2^{n-1} \\ 1 + 2^{n-1}(n-2) & K > 2^{n-1}, \end{cases} \tag{5.78}$$

where $\overline{n}_k \coloneqq n - \lceil \log_2(k) \rceil$, $\bar{k}$ is defined as $2^n - k$, and $|b(k)|$ is Hamming weight of the binary representation of k. A comparison of the two encoding schemes is given in Fig. 5.8.

To summarize, compared to the binary encoding, the Gray encoding has the same number of Pauli strings, and for a bandwidth of up to N, it has a lower number of QC sets, the same number of DGC sets but a less complex diagonalizing unitary. The advantage of the Gray encoding over other encodings comes from the fact that every basis entry differs from its neighbours on a single bit. This, coupled with the fact that the Hamiltonian must be Hermitian, guarantees $G_m^1 + (G_m^1)^\dagger$ to be Pauli-X on the single flipped qubit, and single-qubit projectors on the remaining qubits. This leads to the same number of Pauli strings as compared to the binary encoding, a lower number of QC sets, and the same number of DGC sets but with a lower number of two-qubit gates for low bandwidths.

For example, using the Gray encoding for $N = 8$, the step-1 ladder operator G_1^1 along with its Hermitian conjugate consists of the following Pauli strings:

$$\begin{aligned} G_1^1 + (G_1^1)^\dagger &= P_1^1 \otimes X_1 \otimes P_2^0 \\ &= IXI + IXZ - ZXI - ZXZ, \end{aligned} \tag{5.79}$$

where the qubit numbers are omitted for clarity. The measurement statistics of all these Pauli strings, using both the QC and DGC scheme, can be inferred from the measurement statistics of ZXZ.

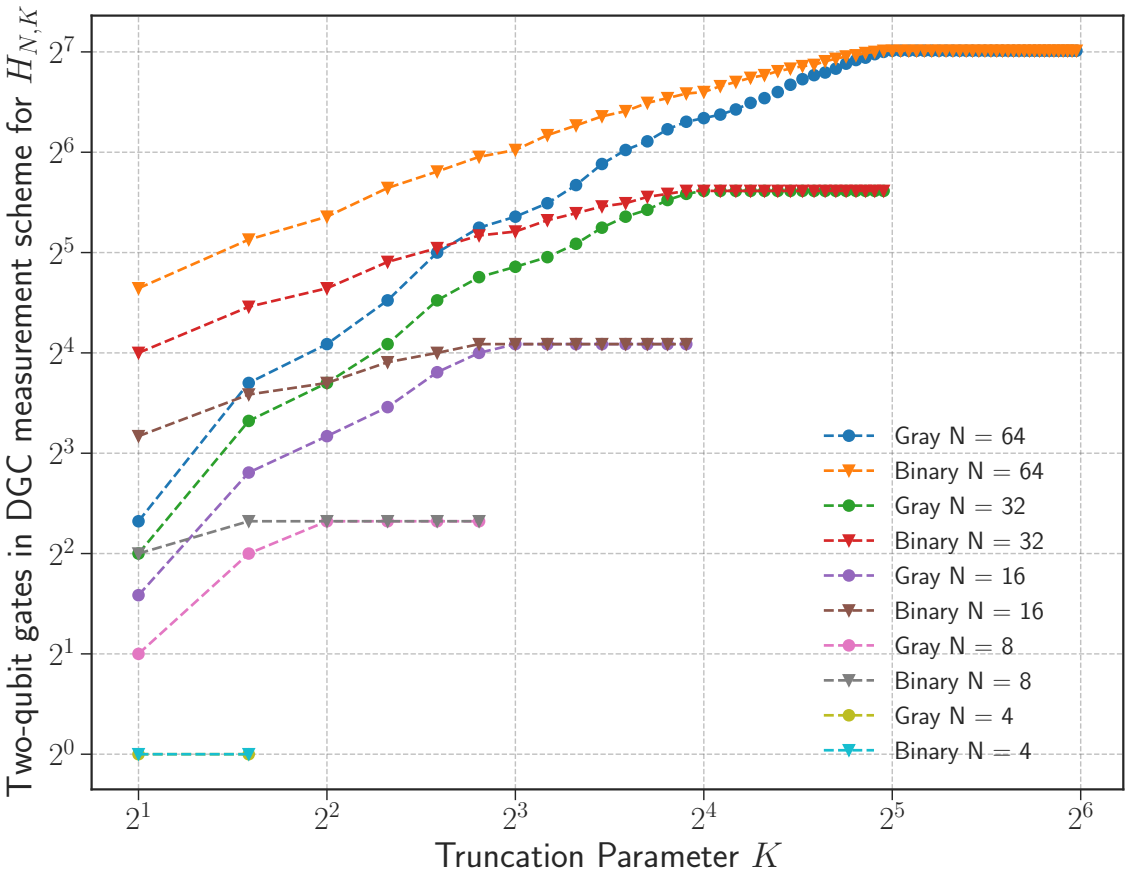


Figure 5.8: Comparing the number of two-qubit gates needed in the DGC measurement scheme for the binary and Gray codes for a general potential of the form $V_K(r) = \sum_{k=0}^{K} v_k r^{2k}$ and a general (tridiagonal to full) Hamiltonian matrix.

In comparison, the binary encoding for the same step-1 ladder operator B_1^1 along with its Hermitian conjugate consists of the following Pauli strings:

$$\begin{aligned} & B_1^1 + (B_1^1)^\dagger \\ & = P_0^1 \otimes [(|1\rangle\langle 0|_1 \otimes |0\rangle\langle 1|_2) + (|0\rangle\langle 1|_1 \otimes |1\rangle\langle 0|_2)] \,, \\ & = IXX + IYY - ZXX - ZYY, \end{aligned} \tag{5.80}$$

where the qubit numbers are omitted for clarity. In the QC scheme, we need to measure ZXX and ZYY to infer the measurement statistics of all the above operators. In the DGC scheme, we need to measure $Z_0 \otimes (U_{1,2}^{\mathrm{GHZ}})^\dagger (Z_1 \otimes Z_2) U_{1,2}^{\mathrm{GHZ}}$, where U^{GHZ} is defined in Lemma D.16 in Appendix D.1.

Remark 5.2. *As seen in Table 5.1, the number of commuting sets for the one-hot encoding is always three, independent of system size. On the other hand, for the binary and Gray encodings detailed in Table 5.2 and Table 5.3, we find that the number of qubit-wise commuting sets and distance-grouped commuting sets depends on N, K and is strictly greater than three. While this gives the impression that the one-hot encoding leads to simpler measurements, we note that these measurements are on N qubits, as opposed to $\log_2(N)$ qubits.*

5.6 Quantum simulations and discussions

In this section, we perform quantum simulations using the Gray and one-hot encodings, with and without noise effects, and we discuss the results. The aim is to illustrate if nuclear problems with band-diagonal Hamiltonian matrices can be solved on current quantum devices and to compare the two types of encodings. Specifically, we study the lowest $\frac{1}{2}^+$ bound state in the n+^{10}C, n+^{12}C, and n+^{14}C, using an exponential potential given in Eq. (5.13). We also perform quantum simulations for the lowest $\frac{1}{2}^+$ orbit in the *ab initio* deduced n-α local potential[3].

5.6.1 Exponential potentials for neutron-Carbon dynamics

For Carbon targets, we use the exponential potential of Eq. (5.13) with parameters given in Table 5.4. These parameterizations yield effective interactions that closely reproduce the experimental energy of the lowest $\frac{1}{2}^+$ state in the composite n+C system (cf. the calculated energy $E_{\rm th}$ and experimental energy $E_{\rm expt}$ in Table 5.4).

For Gaussian-like exponential potentials, the truncation parameter K needs to be odd, since for even K values, the potential curves downward with increasing distance and leads to spurious bound states. Furthermore, the $K = 3$ case provides a reasonable approximation, as illustrated by the $K = 3$ error band in Fig. 5.9. This error is smaller for the lighter isotopes, where the $\frac{1}{2}^+$ state is more deeply bound (larger binding energy) compared to the one for n+^{16}C and n+^{18}C (see also $E_{\rm th}^{K=3}$ in

[3]We note that an optical potential, such as the one derived in the Green's function approach [BLM+24], provides a mean field that, for n+α, yields a negative-energy $\frac{1}{2}^+$ orbit, occupied by the protons and neutron of the α particle, and is associated with the physics of a hole in ^{4}He, that is, with the ground state of ^{3}He. The next $\frac{1}{2}^+$ eigensolution (in increasing energy) corresponds to a scattering state in ^{5}He.

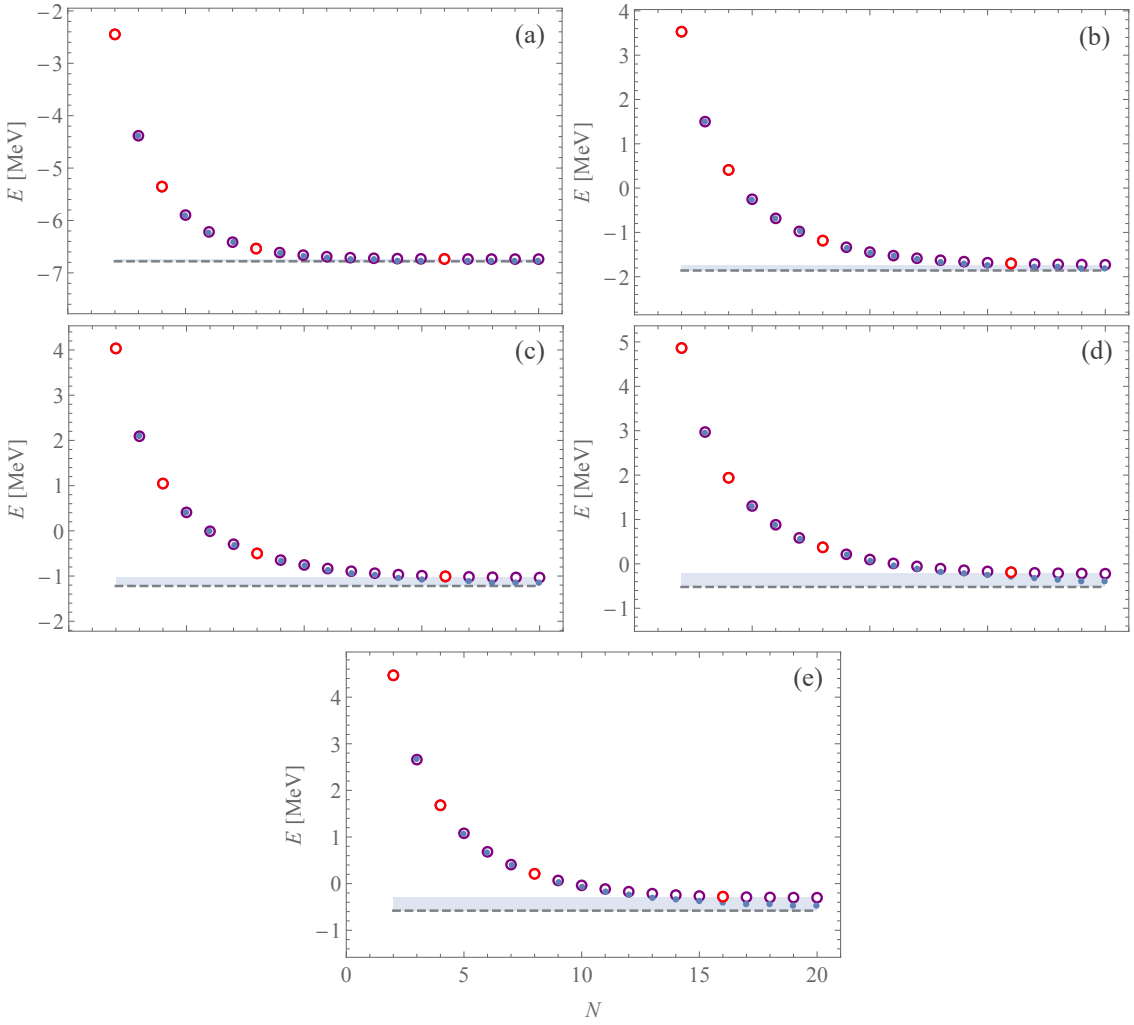


Figure 5.9: Energy of the lowest $\frac{1}{2}^+$ state in (a) n+^{10}C, (b) n+^{12}C, (c) n+^{14}C, (d) n+^{16}C, and (e) n+^{18}C, vs. the model-space size N for $V_{\rm E}$ (5.13) (blue filled) and its $K = 3$ approximation (purple open, for N qubits; red open, for $n = \log_2 N$ qubits), as compared to experiment (dashed line) [KKP+12, AS91, 22]. Shaded area provides the error associated with the $K = 3$ approximation (the small error band for n+^{10}C is not visible on the plot).

Table 5.4). It is important to note that weakly bound states converge at a slower rate compared to states with larger binding energies. As shown in Fig. 5.9, the N = 8 energy (or 3 qubits for the Gray encoding) closely agrees with the exact value for n+^{10}C, but larger model spaces are needed for the other systems. The model-space size requirements become even larger for resonances. This suggests that the use of the Gray encoding that can reach large model spaces with fewer qubits becomes advantageous for weakly bound states and resonances. To illustrate the advantages of the Gray encoding compared to the one-hot encoding, we perform quantum simulations for n+^{14}C using both encodings, which is detailed below.

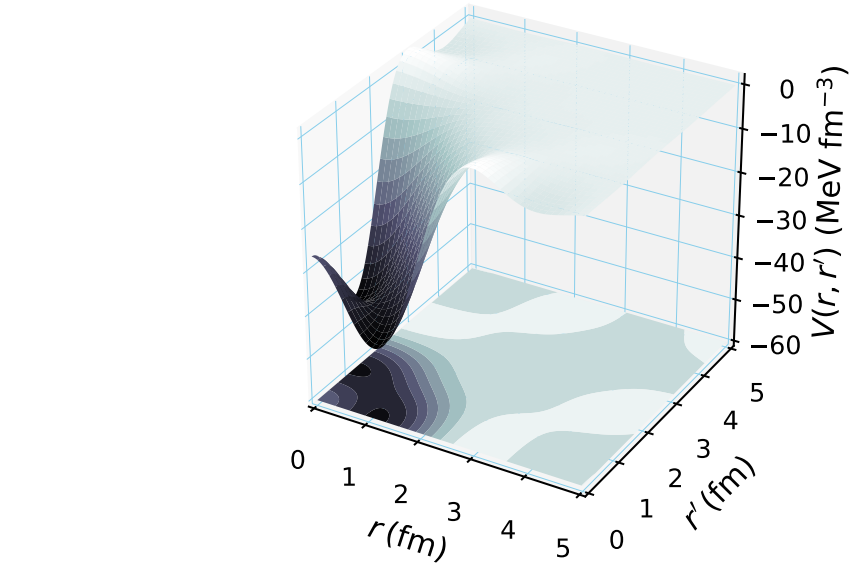
5.6.2 *Ab initio* deduced local optical potential for n+α

The n+^{4}He optical potential is calculated using the *ab initio* symmetry-adapted no-core shell model with Green's function approach (SA-NCSM/GF) [BLM+24], with the chiral NNLO$_{\rm opt}$ nucleon-nucleon potential [EBF+13], at a center-of-mass energy E = 0 MeV, and for 15 HO shells with $\hbar\omega$ = 12 and 16 MeV (see Fig. 5.10a). The choice for the basis parameters, the total number of HO shells and $\hbar\omega$, is based on a systematic study of large-scale calculations reported in Ref. [BLM+24]; namely, Ref. [BLM+24] has shown that for these parameters, n+α phase shifts are converged with respect to the model-space size (see Fig. 8 of Ref. [BLM+24]), leading to a parameter-free estimate for the total cross section that is shown to reproduce the experiment (see Fig. 3 of Ref. [BLM+24]). From the *ab initio* optical potential and using Eq. (5.4), one can calculate the local potential $V(r)$ for $\hbar\omega$ = 12 MeV (Fig. 5.10b):

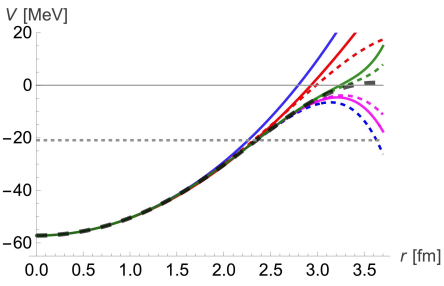
$$\begin{aligned} V(r) &= -57.207 + 6.653r^2 + 0.086r^4 - 0.013r^6 \\ &- 0.001r^8 - 1.8\times10^{-5}r^{10} + 2.3\times10^{-6}r^{12} \\ &+ 2.1\times10^{-7}r^{14} + 5.7\times10^{-9}r^{16} - 3.6\times10^{-10}r^{18} \\ &- 4.3\times10^{-11}r^{20} - 1.5\times10^{-12}r^{22} \\ &+ 5.0\times10^{-14}r^{24} + O(r^{26}) \quad (r \lesssim 3.5\text{fm}), \end{aligned} \tag{5.81}$$

with the corresponding lowest eigenvalue of the original nonlocal potential E_0 = −18.85 MeV.

(a) n+^{4}He *ab initio* potential



(b) $\hbar\omega$ = 12 MeV



(c) $\hbar\omega$ = 16 MeV

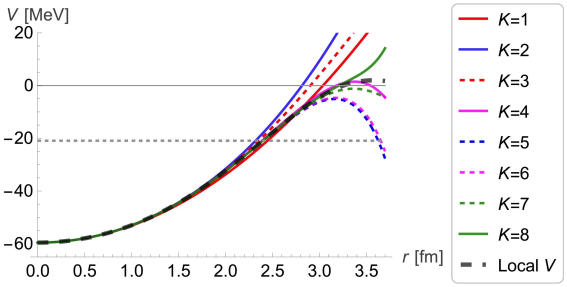


Figure 5.10: (a) *Ab initio* nonlocal n+^{4}He potential as a function of the distance r from the center-of-mass of the α particle for the $S_{\frac{1}{2}}$ partial wave, calculated in the SA-NCSM/GF with $\hbar\omega$ = 16 MeV and 15 HO shells, for zero projectile energy (see also Fig. 4 in Ref. [BLM+24] for other energies and partial waves). (b) & (c) Approximate potentials for different truncation parameters K, as compared to the *ab initio* deduced local potential labeled as "Local V" (black, solid) for (b) $\hbar\omega$ = 12 MeV and (c) $\hbar\omega$ = 16 MeV. The corresponding exact lowest eigenvalue E_0 is also shown (gray, dotted).

The local potential $V(r)$ for $\hbar\omega = 16$ MeV (Fig. 5.10c):

$$\begin{aligned} V(r) &= -59.571 + 6.448r^2 + 0.133r^4 - 0.007r^6 \\ &- 0.001r^8 - 4.8\times10^{-5}r^{10} + 4.1\times10^{-7}r^{12} \\ &+ 2.3\times10^{-7}r^{14} + 1.5\times10^{-8}r^{16} + 3.0\times10^{-10}r^{18} \\ &- 3.6\times10^{-11}r^{20} - 3.8\times10^{-12}r^{22} \\ &- 1.5\times10^{-13}r^{24} + O(r^{26}) \quad (r \lesssim 3.5\text{fm}), \end{aligned} \tag{5.82}$$

with the corresponding lowest eigenvalue of the original nonlocal potential $E_0 = -20.84$ MeV. Hence, across the range of $\hbar\omega$ = 12-16 MeV, the *ab initio* potential yields the lowest $1/2^+$ orbit at energy $E_0 = -19.8 \pm 1.0$ MeV, which closely agrees with the corresponding ^{3}He experimental energy of -20.58 MeV associated with a neutron removal from the ^{4}He target.

Before running simulations, the hyperparameter K of Eq. (5.15) needs to be chosen. From Figs. 5.10b & c, one determines that K = 1, 2, and 7(8) represent reasonable approximations to the local potential with $\hbar\omega$ = 12(16) MeV at small distances, without the possibility of introducing spurious bound states. Indeed, as seen in Figs. 5.10b & c, truncations at other K values yield potentials that are attractive around 3.5 fm (the $K = 3$ approximation becomes largely attractive beyond 5 fm). The quantum simulations for n+α discussed below are performed for K = 1 and 2, since the low-K regime with the Gray encoding is expected to benefit largely from the use of commuting sets (see Sec. 5.5) on existing and far-term quantum devices.

5.6.3 Description of the quantum simulations

The ansatz choice for the different simulations is given in Sec. 5.4.2. For the n+C systems with an exponential potential, we perform simulations with $N = 8$ and $N = 16$, with $K = 3$ (7-diagonal matrix). For the n+α systems, we use $N = 8$, with $K = 1$ and $K = 2$. The type of the simulations are as follows:

- Exact diagonalization (referred to as “true value"): We diagonalize the matrix exactly (using classical methods) and find the minimum eigenvalue, which is used to validate the quantum simulation outcomes.
- Noiseless simulation: We use a perfect noiseless state-vector simulator to simulate ideal behavior.

- Shot-noise simulation: We perform a shot-noise simulation using a variable number of shots (see Appendices D.3 and D.4). The shot-noise simulation is useful in the scenario where the quantum device is perfect and noiseless. However, the shot noise from the final measurements is unavoidable. This method gives a good estimate of performance in the far-term error-corrected regime.
- Noisy simulation: We perform a noisy quantum simulation with noise models from existing quantum devices. Specifically, in this study, the cost function estimates use a fake IBMQ backend `ibm_manila`. This method gives a good estimate of performance in the near-term NISQ regime.
- Noise-resilient estimation: We use the final parameters $\boldsymbol{\theta}$ from the noisy simulation and calculate the expectation value of the Hamiltonian on a classical machine to find a noiseless estimate for the minimum energy, which we refer to as the noise-resilient (NR) value. The idea of noise-resilient training was first introduced in [SKCC20]. We find that the algorithm exhibits noise resilience; i.e., the NR value is more accurate than the noisy simulation outcome. In other words, training is still possible in a noisy scenario.

In all examples, we use a combination of the Simultaneous Perturbation Stochastic Approximation (SPSA) algorithm [Spa92], and gradient descent to estimate the gradient (see Appendices D.3 and D.4 for specific details). The SPSA method provides an unbiased estimator of the gradient with a runtime independent of the number of parameters. We find that deviation from the true value caused the noise introduced by SPSA to increase with the problem size. However, we find that it is useful to quickly obtain a solution close to the optimal value. From here, we use gradient descent to improve the accuracy of the optimal solution.

For the n+C system, we take as input N, K, $\hbar\omega$, V_0, and c. For the n+α system, we take as input N, K, $\hbar\omega$, and the list of coefficients $\{v_k\}_{k=0}^{K}$.

We note that in all simulations, the overall Hamiltonian matrix is constructed and then the expectation value is calculated as an inner product. Nonetheless, for runs on a quantum device, further advantages will stem from using qubit-wise or distance-grouped commuting sets. For example, in the case of the Gray encoding, for $N = 16$ (four qubits) and $K = 3$, there are 88 Pauli strings, 19 QC sets, and 10 DGC sets (e.g., see Table D.2).

In our simulations, we use a warm-start initialization for the ansatz parameters, inspired by perturbation theory. For the exponential potential, see Eq. (5.13), and for the local potentials deduced *ab initio*, see Eqs. (5.82) and (5.83), each progressive diagonal is scaled by an increasingly smaller coefficient. As a result, we expect each additional diagonal to alter the eigenvalue to a lesser extent than the previous diagonals. Inspired by this, we run the simulations for a lower K value using fewer iterations and shots. This enables the optimization to quickly reach an approximate solution. Then, we use the endpoint of this simulation as the start for the full-scale simulation. We find that, in practice, this leads to finding the optimal solution in fewer iterations. In Figs. 5.11-5.17, the large peaks in energy during the optimization occur due to this switch from a lower K to the required value. We note that switching from SPSA to gradient descent can also introduce these peaks. However, the initial learning rate of the gradient descent stage can be tuned to remove this source.

5.6.4 Quantum simulations for neutron-Carbon dynamics

In this section we present the results of the different simulations for n-Carbon dynamics. The specific details, including the number of iterations, type of gradient estimator, and number of shots, can be found in Appendix D.3. We provide simulations that, for the first time, show the efficacy of the Gray code for a Hamiltonian matrix beyond the tridiagonal case, that is, for $K = 1$ (bandwidth of 3). With the Gray code, we can utilize only three and four qubits to simulate model spaces of $N = 8$ and 16 basis states, respectively. This provides acceptable results that closely agree with the energy for the $K = 3$ approximation, which lies near the exact theoretical energy as discussed above (see Fig. 5.9 for $N = 8$ and $N = 16$). The quantum simulations for n+^{10}C, n+^{12}C, and n+^{14}C are shown in Figs. 5.11-5.13, and the case of n+^{14}C is compared to the one-hot encoding in Fig. 5.14.

We summarize the energy estimates from the various quantum simulations in Table 5.5.

In particular, in all cases the noiseless and shot-noise simulations with the Gray code yield results with very small errors, mostly, 10^{-10}-10^{-3}. Importantly, they reproduce the true value within 0-2%, with the only exception being the 6% deviation in $E^{K=3}_{\text{shot}}$ for ^{12}C and $N = 16$.

A very significant result is that the noisy simulations, which are expected to

simulate runs on current NISQ processors, provide very reasonable energy estimates through the use of the NR value. In particular, we find that the algorithm exhibits noise resilience; i.e., the NR value $E_{\rm NR}^{K=3}$ is more accurate than the noisy simulation outcome and training of the wavefunctions parameters is still possible in a noisy scenario. Furthermore, for these n-C systems, we show that the $E_{\rm NR}^{K=3}$ energies differ from the corresponding true value only by 600-950 keV, which surpasses the accuracy of many nuclear models. The only exception is the four-qubit simulation for n+^{14}C (Fig. 5.13), which predicts an unbound $\frac{1}{2}^+$ state at 0.59 MeV for the weakly bound state at −1.0 MeV. While this is still a reasonable estimate, weakly bound states require larger model spaces to achieve convergence, as discussed above, which implies the need for larger number of qubits. This means that special care needs to be taken in the quantum simulations of such systems, including n+^{16}C and n+^{18}C, when performed on NISQ devices. One way to improve this is to try different ansatz structures, or a larger model space, which remains to be shown in future work.

We note here that for the example of n+^{10}C, with $N = 8$ and $K = 3$, in addition to the noise resilient final estimate, we report the mean and standard deviation of the noiseless estimates of the last 100 noisy iterations. In other words, we use the parameters from last 100 noisy iterations, calculate the noiseless estimate, and report the mean and standard deviation to be -6.05 ± 0.07. This is $\sim 2\sigma$ away from the $E_{NR}^{K=3}$ value reported in Table 5.5 calculated from the last iteration only, which is very reasonable. This further solidifies the idea that the noise resilient method offers a much better estimate as compared to the noisy estimate. However, in any large-scale experiment, we would not recommend running the noiseless simulation for hundreds of iterations. This is because each noiseless simulation is prohibitively expensive. Instead, in this study, we use the standard deviation for n+^{10}C as a guidance to the number of the significant digits we report for the noise resilient estimates in all simulations.

Furthermore, even in the case of weakly bound states, the Gray code with three qubits is superior to the one-hot encoding with eight qubits, as illustrated in Fig. 5.14 and Table 5.5. Indeed, compared to the Gray-code case, the one-hot simulations are much slower and show worse performance in the presence of noise. In particular, the one-hot simulation yields larger errors [e.g., by six (two) orders of magnitude for the noiseless (shot noise) simulations], as well as a deviation for $E_{\rm NR}^{K=3}$ from the true value that is twice as large as the corresponding Gray-code estimate. In addition, as shown in Figs. 5.2 and 5.3 as well as in Tables 5.1, 5.2, 5.3, the one-hot ansatz utilizes 13 two-qubit gates compared to only 8 two-qubit (CNOT)

gates in the Gray encoding ansatz with $L = 4$ used in our simulations. This suggests that the Gray encoding and the use of fewer qubits are indeed highly advantageous for nuclear problems that achieve convergence in larger model spaces, with the case of weakly bound systems presented here being an illustrative example.

5.6.5 Quantum simulations with the Gray encoding for n+α using *ab initio* optical potentials

In this section, we present the results of the simulations for the n+α dynamics. The specific details, including the number of iterations, type of gradient estimator, and number of shots, can be found in Appendix D.4. The quantum simulations for n+α are carried out for model spaces of $N = 8$ (Fig. 5.15) and $N = 16$ (Fig. 5.16) for $\hbar\omega = 12$ MeV and of $N = 8$ (Fig. 5.17) for $\hbar\omega = 16$ MeV. We show the cases of $K = 2$ for a potential of $O(r^4)$ and $K = 3$ for a potential of $O(r^6)$.

We summarize the energy estimates from the various quantum simulations in Table 5.6. The energies E_{th}^K from the exact diagonalization for $K = 1$ and 2 converge within the first four to five digits with the increasing model space from $N = 8$ to $N = 16$, as illustrated in Table 5.6 for $\hbar\omega = 12$ MeV (for $\hbar\omega = 16$ MeV, $E_{\text{th}}^{K=1} = -20.77$ MeV and $E_{\text{th}}^{K=2} = -18.95$ MeV for $N = 16$). Hence, the final estimates are based on the $N = 8$ results, where the uncertainties are estimated for a 14% variation of the $\hbar\omega$ values ($\hbar\omega$ = 12-16 MeV), the same range that yields a total cross section for the neutron scattering on ^{4}He that is converged and in agreement with experiment, as discussed in Ref. [BLM+24]. In addition, the $K = 1$ and $K = 2$ approximation energies are very close to the corresponding E_0 eigenenergy of the original non-local *ab initio* optical potential. In fact, across the $\hbar\omega$ range, the energy of the lowest $\frac{1}{2}^+$ orbit is estimated at $-19.3(1.5)$ MeV for $K = 1$ and at $-17.8(1.2)$ MeV for $K = 2$, both of which agree within the uncertainties with the non-local estimate of $-19.8(1.0)$ reported above. Exactly the same energy estimates are obtained by the noiseless and shot simulations (-19.3 ± 1.5 MeV for $K = 1$ and at -17.8 ± 1.2 MeV for $K = 2$). We note that the errors that stem from these simulations (of order of a few keV) are inconsequential compared to the ones associated with the $\hbar\omega$ variation ($\sim 1 - 1.5$ MeV). Importantly, while the noisy simulations yield unacceptably large energies, the corresponding NR energies agree with the shot-noise outcomes within 1σ: $-18.6(1.7)$ MeV for $K = 1$ and $-17.1(1.2)$ MeV for $K = 2$, while leading to slightly larger or comparable error bars. This suggests that

deep bound states described by an *ab initio* deduced NA optical potential can be reasonably well approximated by tri- to five-diagonal potentials, and in turn, can be successfully simulated on far-term error-corrected devices (practically yielding the true result) and even on NISQ processors (yielding energies within 1σ across a 14% $\hbar\omega$ variation).

5.6.6 Comparing QC and DGC schemes

In this section we compare the efficacy of QC and DGC schemes using both the Gray and binary encodings. We perform both noiseless and shot noise simulations for all cases. In the shot noise runs, we keep the total number of shots per variational run to be fixed. This is to simulate a fixed amount of "quantum" resources. Furthermore, in contrast with the preceding simulations in this work, here we only use gradient descent with a varying learning rate scheme to estimate the gradient. This removes the effects of the SPSA noise and gives a clearer picture of the inherent shot noise. However, this also leads to results of the noiseless simulations in this section being slightly different from those reported in Table 5.6, since the noise introduced by SPSA can take the system out of a local minima and converge to a better solution.

We first compare QC and DGC using the Gray encoding (Fig. 5.18). We perform simulations for the n+α system using a model space of $N = 8$, $\hbar\omega = 12$MeV, and $K = 1$ for a potential of $O(r^2)$. We expect the noiseless QC and DGC to be exactly the same, and the plots reflect this. However, since DGC leads to a more optimal grouping of Pauli terms, each group is allocated more shots. Thus, we expect DGC to outperform QC in the shot noise runs, which is what the data in Fig. 5.18 indicates. The results are summarized in Table 5.7.

Next, we compare the Gray and binary encoding using the QC scheme. From the results of Sec. 5.5.2, we expect the Gray encoding to outperform the binary encoding, and the data in Fig. 5.19 clearly corroborates this. The outcomes of these simulations are summarized in Table 5.8. While the Gray encoding agrees with the noiseless result within 1σ, the binary encoding leads to a larger standard deviation and at least a 2σ agreement.

5.7 Conclusion

In this work, we developed a quantum algorithm to simulate neutron-nucleus dynamics on a quantum processor. We generalize the form of the nuclear Hamiltonian to any band-diagonal to full matrices, which can accommodate a general central potential and a complete form of the chiral NN potential. We compare and contrast three encoding schemes, namely, the one-hot, binary, and Gray encodings. We show that the Gray encoding remains more resource efficient beyond the tridiagonal case, resolving an open problem posed in Ref. [DMMG+21].

To estimate the measurement statistics, which is of key importance to successful simulations on quantum devices, we provide an extensive numerical analysis of the number of Pauli terms and qubit-wise commuting sets in the Hamiltonian as a function of the matrix size and the number of off-diagonals. We show that when the number of off-diagonals $2K + 1$ exceeds the size of the matrix N, the number of Pauli terms and commuting sets saturate, with the Gray/binary encoding having fewer Pauli terms than the one-hot encoding. Beyond this point, more off-diagonals can be added to the problem, improving the approximation, without further load to the quantum device.

We also introduce a new commutativity scheme, DGC, that allows for a more optimal grouping of Pauli strings at the cost of a more complex diagonalizing unitary, as compared to the qubit-commutativity scheme. We show that for small bandwidths ($K < N/2$), the Gray encodings leads to the same number of Pauli strings as compared to the binary encoding, a lower number of QC sets, and the same number of DGC sets but with a lower number of two-qubit gates. While the number of commuting sets for the one-hot encoding is always three, we note that these measurements are on N qubits, as opposed to $\log_2(N)$ qubits.

To demonstrate the efficacy of the Gray encoding, the one-hot and Gray encodings are compared in quantum simulations of the lowest $\frac{1}{2}^+$ state of n+^{14}C, only bound by 1.04 MeV in the $K = 3$ approximate potential, for $N = 8$ basis states. Indeed, compared to the Gray-code simulations with three qubits, the one-hot simulations with eight qubits are much slower and show worse performance in the presence of noise. In addition, we perform quantum simulations using a shot-noise and noisy simulator to inform the suitability of these simulations in the far-term error-corrected and NISQ regimes, respectively. It is remarkable that for n+^{10,12}C and n+α, we find that the shot-noise energies practically reproduce the corresponding exact value, whereas the noisy simulations coupled with the noise-

resilient training method yield energies that deviate by less than one MeV. Finally, for the bound $\frac{1}{2}^+$ orbit of the neutron-alpha optical potential deduced *ab initio*, we report energy from the noisy quantum simulation that lies only within 1σ of the shot-noise outcome across a 14% $\hbar\omega$ variation. For this case, we also show that simulations with the DGC scheme outperform those using the QC scheme, and that the Gray encoding (for the QC scheme) leads to better precision and agreement with the noiseless outcome compared to the binary encoding.

Going forward from here, one could simulate systems of three clusters or larger (multi-channel reaction descriptions or multiple pairs of nucleons for reaching heavy nuclei) to give a better understanding of the scaling of the problem and whether the Gray efficacy shown here for two clusters propagates to more complex systems. It is also important to explore the dependence on the energy scale, and in particular, to seek further improvements to manage very weakly bound states and resonances. Another open theoretical question is about the optimality of the Gray code. In this work, we use the binary reflective Gray code, but any Gray code will lead to the same performance.

The code for the simulations can be found as a Zenodo repository [RGW+24b].

$H_{N,K}$	$K \leq N/2$	$K > N/2$
Qubits	$\log_2(N)$	
Pauli Terms	$\mathrm{d}(n,K) + 2^{n-1}\sum_{k=1}^{K}\overline{n}_k$	$2^{n-1}(1+2^n)$
QC Sets	$1+\sum_{k=1}^{K} 2^{\lvert b(\bar{k})\rvert}[1-2^{-\overline{n}_k}]$	$\frac{1}{2}(1+3^n)$
DGC Sets	$1+\sum_{k=1}^{K}\overline{n}_k$	2^n
2QG in Diag. Unitary	$\frac{1}{2}\sum_{k=1}^{K}\overline{n}_k\left[2\lvert b(\bar{k})\rvert - 1 - \overline{n}_k\right]$	$1+2^{n-1}(n-2)$
Ansatz	nL one-qubit gates + $(n-1)L$ two-qubit gates	

Table 5.2: Number of qubit, Pauli terms, qubit-wise commuting sets and distance-grouped commuting sets for the binary encoding, for a general Hamiltonian matrix of $2K+1$ bandwidth. Here we use $N = 2^n$ and $\overline{n}_k := n - \lceil \log_2(k) \rceil$. The quantity $\mathrm{d}(n,K)$ is defined in (5.63). For the ansatz, L refers to the number of layers, which is chosen large enough beforehand. In the present study, the Hamiltonian for $K = 0$ (diagonal potential) is tridiagonal because of the kinetic energy term, in which case the entries for $K = 1$ should be used. Notably, for $K > N/2$, there is a saturation in all quantities, implying that larger diagonal width (better approximation) can be handled without an increase in the complexity of the problem. More details can be found in Sec. 5.6.

$H_{N,K}$	$K \leq N/2$	$K > N/2$
Qubits	$\log_2(N)$	
Pauli Terms	$\mathrm{d}(n,K) + 2^{n-1}\sum_{k=1}^{K}\overline{n}_k$	$2^{n-1}(1+2^n)$
QC Sets	$1 + \sum_{k=1}^{K}\overline{n}_k 2^{\lvert g(k-1)\rvert}$	$\frac{1}{2}(1+3^n)$
DGC Sets	$1 + \sum_{k=1}^{K}\overline{n}_k$	2^n
2QG in Diag. Unitary	$\sum_{k=1}^{K}\overline{n}_k \lvert g_{k-1}\rvert$	$1 + 2^{n-1}(n-2)$
Ansatz	nL one-qubit gates + $(n-1)L$ two-qubit gates	

Table 5.3: Number of qubit, Pauli terms, qubit-wise commuting sets and distance-grouped commuting sets for the Gray encoding, for a general Hamiltonian matrix of $2K+1$ bandwidth. Here we use $N = 2^n$ and $\overline{n}_k := n - \lceil \log_2(k) \rceil$. The quantity $\mathrm{d}(n,K)$ is defined in (5.63). For the ansatz, L refers to the number of layers, which is chosen large enough beforehand. In the present study, the Hamiltonian for $K = 0$ (diagonal potential) is tridiagonal because of the kinetic energy term, in which case the entries for $K = 1$ should be used. Notably, for $K > N/2$, there is a saturation in all quantities, implying that larger diagonal width (better approximation) can be handled without an increase in the complexity of the problem. More details can be found in Sec. 5.6.

	A	E_{expt} [MeV]	E_{th} [MeV]	$E_{\text{th}}^{K=3}$ [MeV]	$\frac{1}{\hbar\omega}V_0$	$c^{-\frac{1}{2}}$
n+^{10}C	10	−6.78	−6.78	−6.74	−0.650	5.43
n+^{12}C	12	−1.86	−1.86	−1.74	−0.283	5.35
n+^{14}C	14	−1.22	−1.22	−1.04	−0.242	5.0
n+^{16}C	16	−0.52	−0.52	−0.23	−0.175	4.7
n+^{18}C	18	−0.58	−0.59	−0.30	−0.192	4.6

Table 5.4: Experimental energy for the lowest $\frac{1}{2}^+$ state for each neutron-Carbon system, with the corresponding theoretical energy E_{th} of the exponential potential V_{E} (5.13) and its $K = 3$ approximation $E_{\text{th}}^{K=3}$. For each case, the parameters (V_0 and c) of the Hamiltonian are shown, with $\hbar\omega = \frac{41}{(A+1)^{1/3}}$ MeV, where A is the mass of the target.

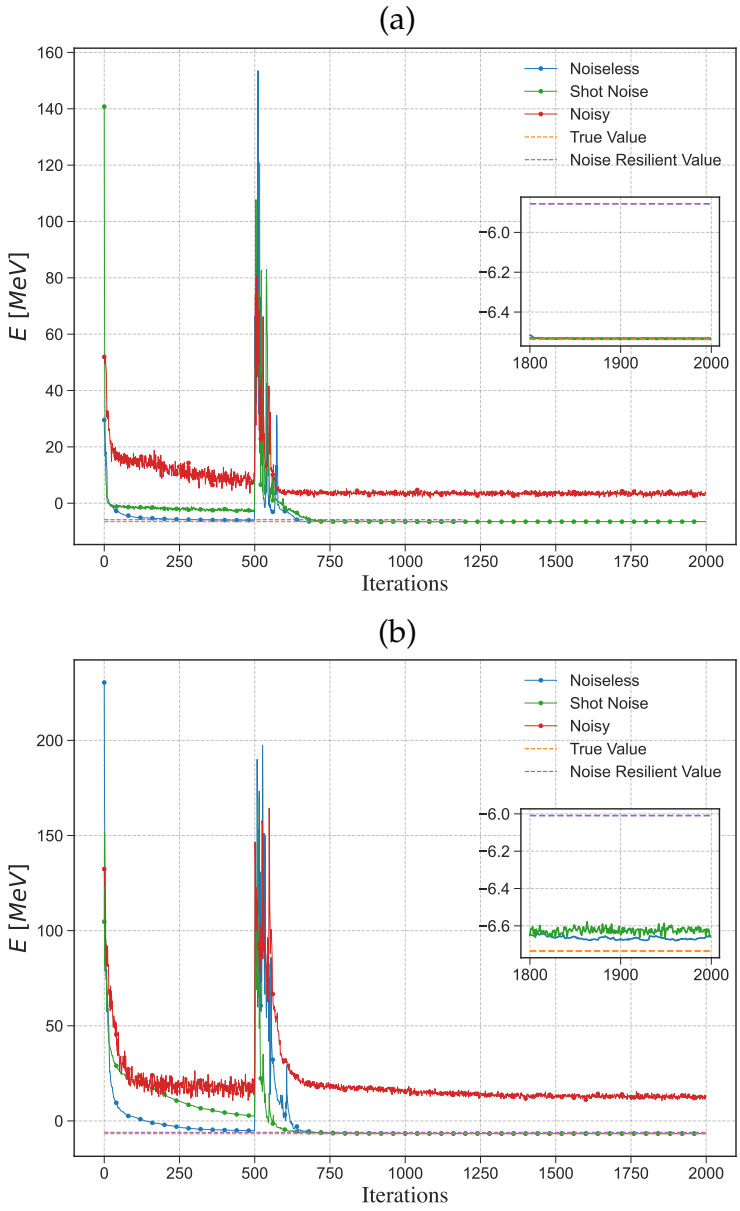


Figure 5.11: Quantum simulation using the Gray encoding for the energy of the lowest $\frac{1}{2}^+$ state for n+^{10}C modeled by the $V_{\rm E}$ exponential potential Eq. (5.13) with (a) $N = 8$ ($n = 3$ qubits) and (b) $N = 16$ ($n = 4$ qubits), with $K = 3$ and for different types of simulations detailed in Sec. 5.6.3, as compared to the theoretical energy $E_{\rm th}^{K=3}$ labeled as "True Value" (for the Hamiltonian parameters and $E_{\rm th}^{K=3}$, see Table 5.4). The inset plots are the last 200 iterations.

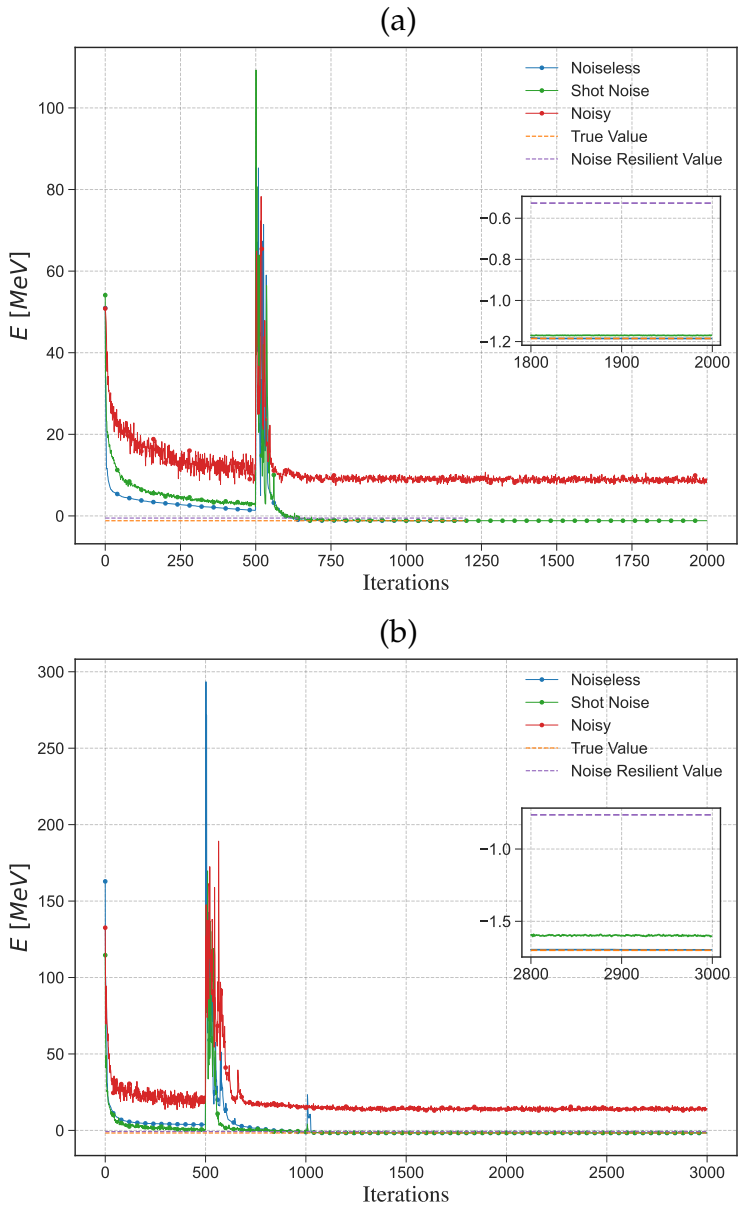


Figure 5.12: Quantum simulation using the Gray encoding for the energy of the lowest $\frac{1}{2}^+$ state for n+^{12}C modeled by the $V_{\rm E}$ exponential potential Eq. (5.13) with (a) $N = 8$ ($n = 3$ qubits) and (b) $N = 16$ ($n = 4$ qubits), with $K = 3$ and for different types of simulations detailed in Sec. 5.6.3, as compared to the theoretical energy $E_{\rm th}^{K=3}$ labeled as "True Value" (for the Hamiltonian parameters and $E_{\rm th}^{K=3}$, see Table 5.4). The inset plots are the last 200 iterations.

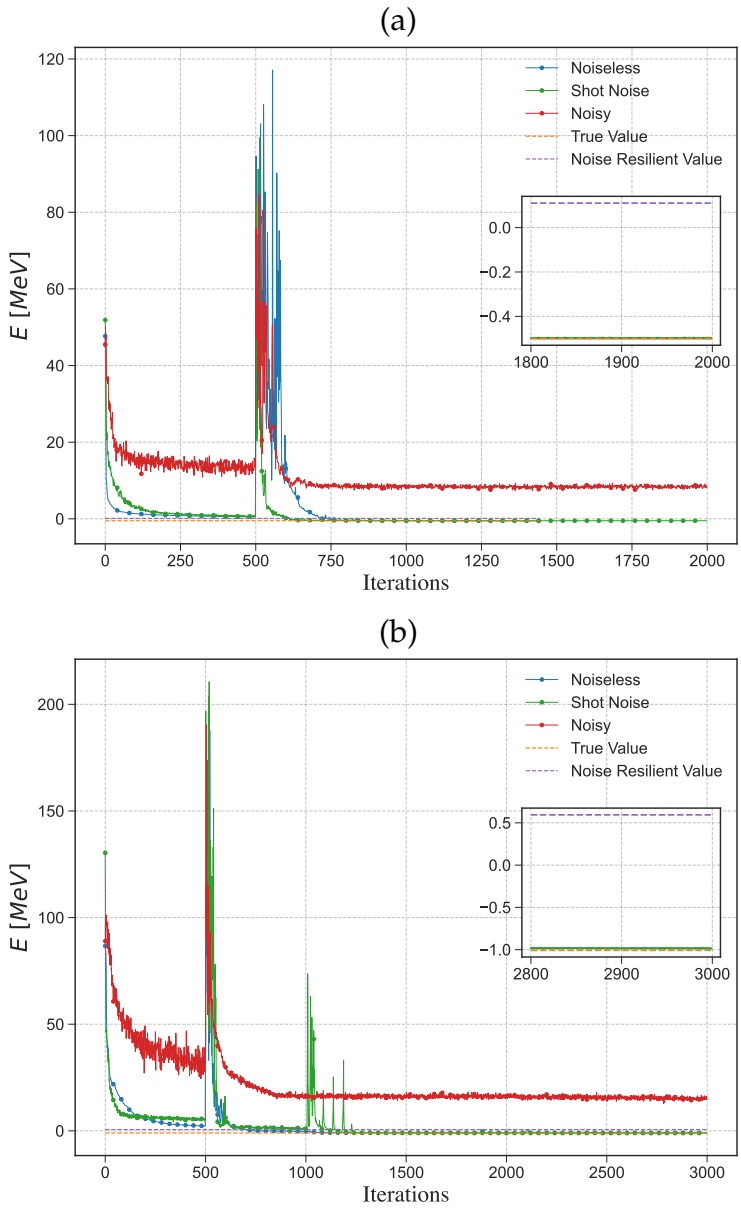


Figure 5.13: Quantum simulation using the Gray encoding for the energy of the lowest $\frac{1}{2}^+$ state for n+^{14}C modeled by the $V_{\rm E}$ exponential potential Eq. (5.13) with (a) $N = 8$ ($n = 3$ qubits) and (b) $N = 16$ ($n = 4$ qubits), with $K = 3$ and for different types of simulations detailed in Sec. 5.6.3, as compared to the theoretical energy $E_{\rm th}^{K=3}$ labeled as "True Value" (for the Hamiltonian parameters and $E_{\rm th}^{K=3}$, see Table 5.4). The inset plots are the last 200 iterations.

	E_{th} [MeV]	Encoding	Figure	N	$E_{\text{th}}^{K=3}$ [MeV]	$E_{\text{NL}}^{K=3}$ [MeV]	$E_{\text{shot}}^{K=3}$ [MeV]	$E_{\text{noisy}}^{K=3}$ [MeV]	$E_{\text{NR}}^{K=3}$ [MeV]
n+^{10}C	−6.78	Gray	5.11	8	−6.5364	$-6.5364 \pm 2 \times 10^{-10}$	-6.5305 ± 0.0005	3.5 ± 0.5	−5.9
				16	−6.7346	-6.668 ± 0.007	-6.62 ± 0.02	12.6 ± 0.7	−6.0
n+^{12}C	−1.86	Gray	5.12	8	−1.18495	$-1.184993 \pm 1 \times 10^{-6}$	-1.1701 ± 0.0006	8.7 ± 0.5	−0.5
				16	−1.70020	-1.6973 ± 0.0001	-1.599 ± 0.003	13.9 ± 0.7	−0.8
n+^{14}C	−1.22	Gray	5.13	8	−0.49963	$-0.4996 \pm 6 \times 10^{-10}$	-0.4966 ± 0.0005	8.4 ± 0.3	0.1
				16	−1.0070	-0.9860 ± 0.0005	-0.982 ± 0.002	15.2 ± 0.5	0.6
		One-hot	5.14	8	−0.49963	-0.4987 ± 0.0001	-0.49 ± 0.03	9.0 ± 0.6	0.7

Table 5.5: Simulation energy for the lowest $\frac{1}{2}^+$ state for each neutron-Carbon system, for the $K = 3$ approximation with $N = 8$ or $N = 16$, corresponding to Figs. 5.11-5.14: the true value $E_{\text{th}}^{K=3}$; $E_{\text{NL}}^{K=3}$ from the noiseless simulations, $E_{\text{shot}}^{K=3}$ from the shot-noise simulations, and $E_{\text{noisy}}^{K=3}$ from the noisy simulations, reported as the mean and standard deviation of the last 100 iterations; and the NR value $E_{\text{NR}}^{K=3}$. The theoretical eigenenergy E_{th} of the exact potential is also shown (cf. Table 5.4).

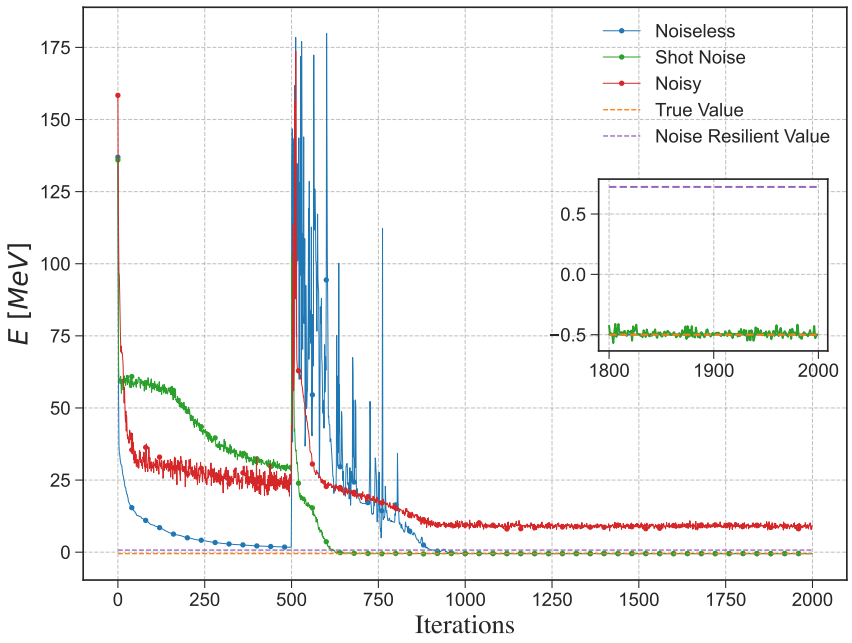


Figure 5.14: Simulation using the one-hot encoding for the energy of the lowest $\frac{1}{2}^+$ state for n+^{14}C modeled by the exponential potential Eq. (5.13) with $N = 8$ ($n = 8$ qubits) and $K = 3$. The different types of simulations are detailed in Sec. 5.6.3. The inset plots the last 200 iterations.

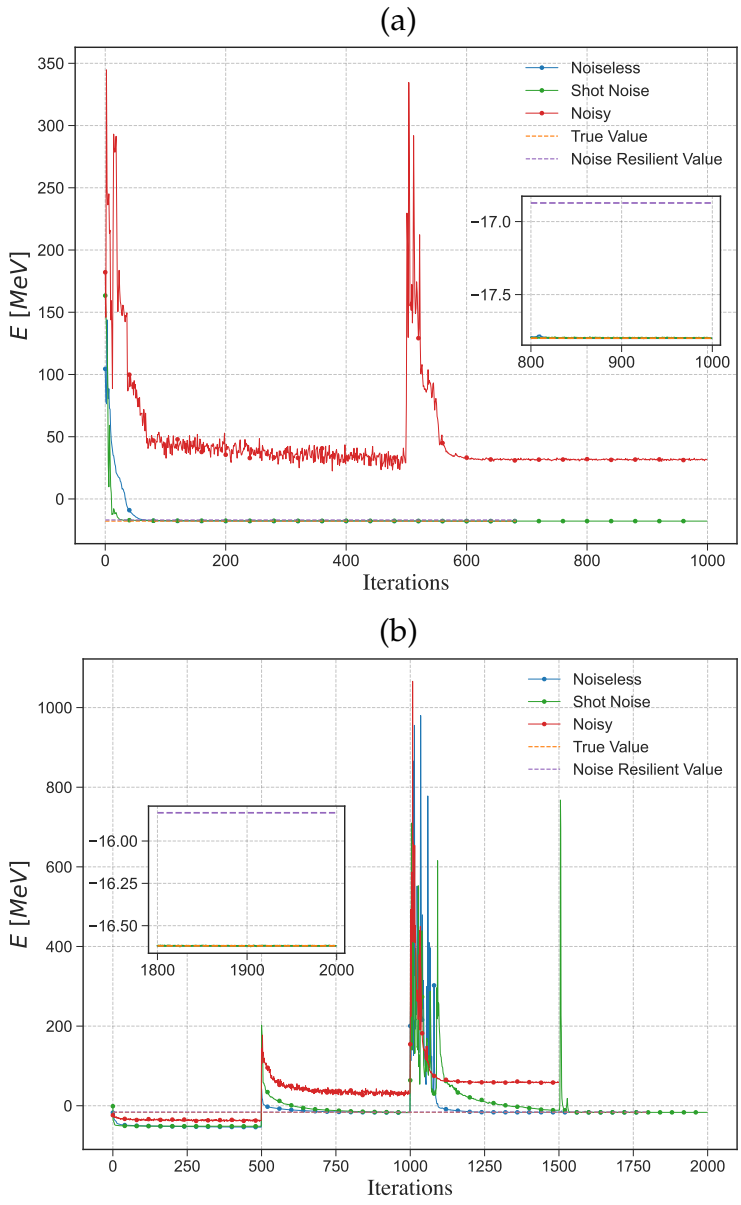


Figure 5.15: Simulation with the Gray encoding for the n-α *ab initio* potential for $\hbar\omega = 12$ MeV Eq. (5.82) with $N = 8$ ($n = 3$), and (a) $K = 1$ and (b) $K = 2$. The different types of simulations are detailed in Sec. 5.6.3. The inset plots the last 200 iterations.

$\hbar\omega$	E_0 [MeV]	N	Figure	K	E_{th}^K [MeV]	E_{NL} [MeV]	E_{shot} [MeV]	E_{noisy} [MeV]	E_{NR} [MeV]
12	−18.85	8	5.15	1	−17.7986	$-17.7986 \pm 4 \times 10^{-10}$	-17.796 ± 0.001	31.6 ± 0.4	−16.9
				2	−16.6190	$-16.6189 \pm 1.7 \times 10^{-13}$	-16.618 ± 0.001	58.7 ± 0.7	−15.8
		16	5.16	1	−17.7987	-17.7852 ± 0.0008	-17.791 ± 0.007	68.8 ± 0.7	−16.8
				2	−16.6191	-16.615 ± 0.005	-16.60 ± 0.02	162 ± 2	−14.9
16	−20.84	8	5.17	1	−20.7735	$-20.7735 \pm 3.2 \times 10^{-11}$	-20.7733 ± 0.0005	8.8 ± 0.3	−20.3
				2	−18.9470	$-18.9470 \pm 1.8 \times 10^{-13}$	-18.9470 ± 0.0006	43.2 ± 0.6	−18.3

Table 5.6: Simulation energy for the lowest $\frac{1}{2}^+$ orbit of the n–α *ab initio* deduced local potential, using the Gray code with $N = 8$ or $N = 16$, corresponding to Figs. 5.15-5.17: the true value E_{th}^K; E_{NL} from the noiseless simulations, E_{shot} from the shot-noise simulations, and E_{noisy} from the noisy simulations, reported as the mean and standard deviation of the last 100 iterations; and the NR value E_{NR}. The exact theoretical eigenenergy E_0 of original non-local *ab initio* potential is also shown.

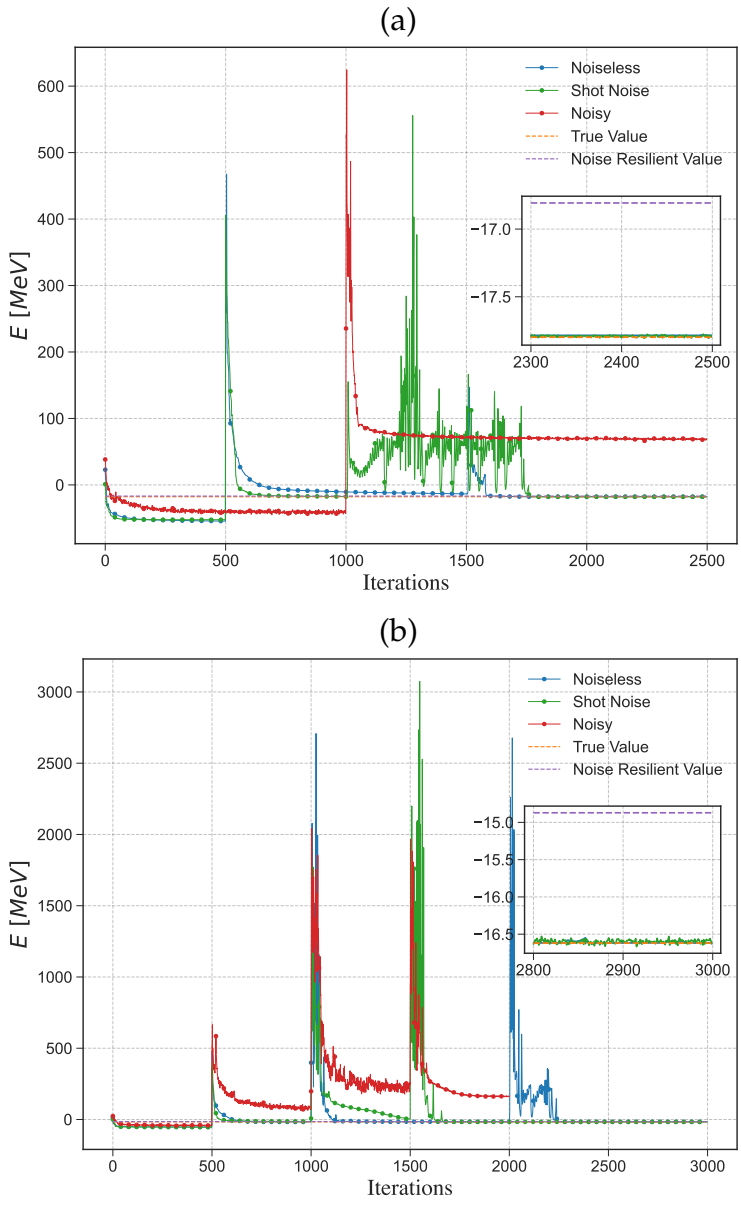


Figure 5.16: Simulation with the Gray encoding for the n-α *ab initio* potential for $\hbar\omega = 12$ MeV Eq. (5.82) with $N = 16$ ($n = 4$), and (a) $K = 1$ and (b) $K = 2$. The different types of simulations are detailed in Sec. 5.6.3. The inset plots the last 200 iterations.

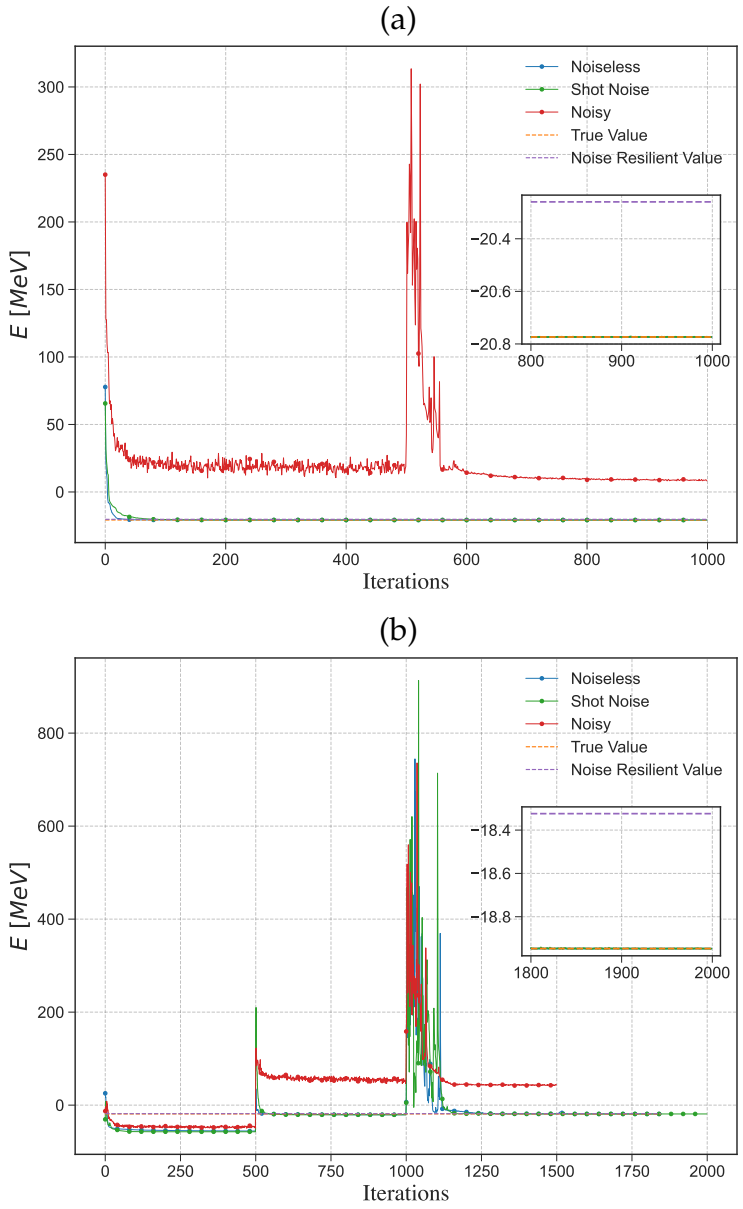


Figure 5.17: Simulation for the n-α *ab initio* potential for $\hbar\omega = 16$ MeV Eq. (5.83) with $N = 8$, and (a) $K = 1$ and (b) $K = 2$. The different types of simulations are detailed in Sec. 5.6.3. The inset plots the last 200 iterations.

Simulation	Mean and Standard Deviation
Noiseless + QC	-17.78384 ± 0.00009
Noiseless + DGC	-17.78384 ± 0.00009
Shot Noise + QC	-17.67 ± 0.14
Shot Noise + DGC	-17.72 ± 0.13

Table 5.7: Comparing the QC and DGC schemes using the Gray encoding, in the case of the n+α system for $N = 8$ (three qubits), $\hbar\omega = 12$, and $K = 1$, corresponding to Figure 5.18. The total number of shots per variational run is 10^6. The mean and standard deviation reported are calculated using the last 100 iterations.

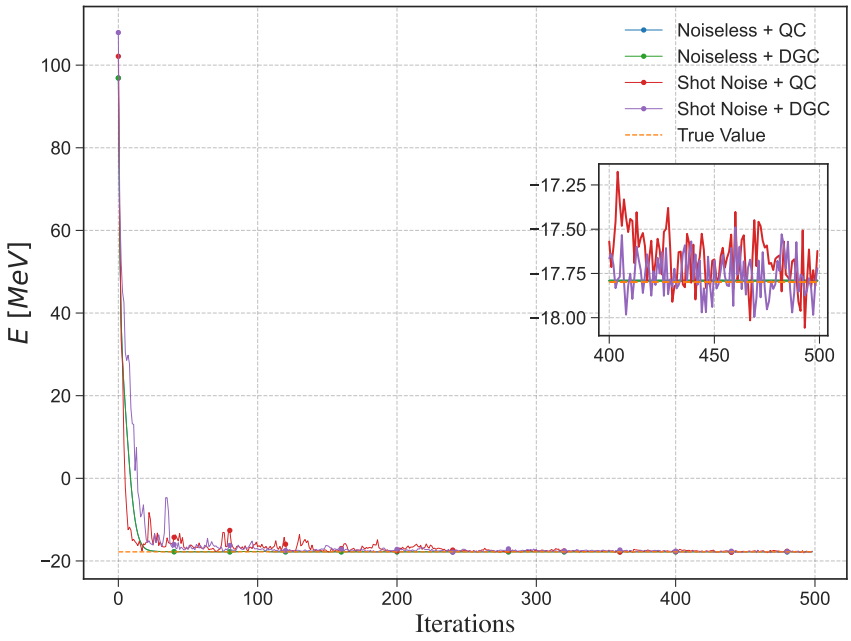


Figure 5.18: Comparison of the QC and DGC schemes for simulations with the Gray encoding of the n+α system using a model space of $N = 8$, $K = 1$, and $\hbar\omega = 12$MeV. The different types of simulations are detailed in Sec. 5.6.3 (the curves for the two noiseless simulations are indistinguishable). The inset plots the last 100 iterations.

Simulation	Mean and Standard Deviation
Noiseless	$-16.5990 \pm 8 \times 10^5$
Shot Noise + QC + Gray	-16.31 ± 0.34
Shot Noise + QC + binary	-15.80 ± 0.57

Table 5.8: Comparing the Gray and binary encodings using the QC scheme, in the case of the n+α system for, $N = 8$ (three qubits), $\hbar\omega = 12$, and $K = 2$, corresponding to Figure 5.19. The total number of shots per variational run is 10^6. The mean and standard deviation reported are calculated using the last 100 iterations.

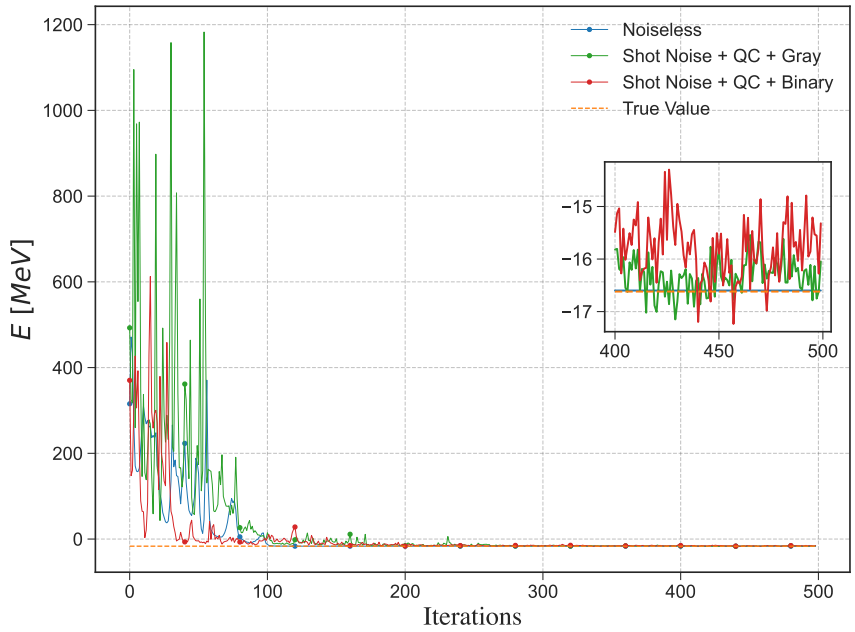


Figure 5.19: Comparison of the Gray and binary encodings using the QC scheme for simulations of the n+α system using a model space of $N = 8$, $K = 2$, and $\hbar\omega = 12$MeV. The different types of simulations are detailed in Sec. 5.6.3. The inset plots the last 100 iterations.

Bibliography

[AAMA+21] M. D. Sajid Anis, Abby-Mitchell, Héctor Abraham, AduOffei, Rochisha Agarwal, et al., *Qiskit: An open-source framework for quantum computing*, 2021.

[AJL06] Dorit Aharonov, Vaughan Jones, and Zeph Landau, *A polynomial quantum algorithm for approximating the jones polynomial*, Proceedings of the thirty-eighth annual acm symposium on theory of computing, 2006, pp. 427–436. arXiv:quant-ph/0511096.

[AL12] Miguel F. Anjos and Jean B. Lasserre (eds.), *Handbook on semidefinite, conic and polynomial optimization*, Springer, 2012.

[AOST17] Jayadev Acharya, Alon Orlitsky, Ananda Theertha Suresh, and Himanshu Tyagi, *Estimating Rényi entropy of discrete distributions*, IEEE Transactions on Information Theory **63** (January 2017), no. 1, 38–56. arXiv:1408.1000.

[ARSW21] Rochisha Agarwal, Soorya Rethinasamy, Kunal Sharma, and Mark M. Wilde, *Estimating distinguishability measures on quantum computers* (August 2021). arXiv:2108.08406v1.

[AS67] Yakir Aharonov and Leonard Susskind, *Charge superselection rule*, Physical Review **155** (March 1967), no. 5, 1428–1431.

[AS91] F. Ajzenberg-Selove, *Energy levels of light nuclei $A = 13 - 15$*, Nuclear Physics A **523** (1991), no. 1, 1–196.

[BC12] Fernando G. S. L. Brandão and Matthias Christandl, *Detection of multiparticle entanglement: Quantifying the search for symmetric extensions*, Physical Review Letters **109** (October 2012), no. 16, 160502, available at 1105.5720.

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani, *Strengths and weaknesses of quantum computing*, SIAM Journal on Computing **26** (October 1997), no. 5, 1510–1523.

[BBC21] Paolo Braccia, Leonardo Banchi, and Filippo Caruso, *Quantum noise sensing by generating fake noise* (July 2021). arXiv:2107.08718v1.

[BBC22] ———, *Quantum noise sensing by generating fake noise*, Physical Review Applied **17** (February 2022), no. 2, 024002.

[BBD+97] Adriano Barenco, André Berthiaume, David Deutsch, Artur Ekert, Richard Jozsa, and Chiara Macchiavello, *Stabilization of quantum computations by symmetrization*, SIAM Journal on Computing **26** (1997), no. 5, 1541–1557, available at https://doi.org/10.1137/S0097539796302452.

[BCLK+22] Kishor Bharti, Alba Cervera-Lierta, Thi Ha Kyaw, Tobias Haug, Sumner Alperin-Lea, Abhinav Anand, Matthias Degroote, Hermanni Heimonen, Jakob S. Kottmann, Tim Menke, Wai-Keong Mok, Sukin Sim, Leong-Chuan Kwek, and Alán Aspuru-Guzik, *Noisy intermediate-scale quantum (NISQ) algorithms*, Reviews of Modern Physics **94** (February 2022), no. 1, 015004. arXiv:2101.08448.

[BCP14] Tillman Baumgratz, Marcus Cramer, and Martin B. Plenio, *Quantifying coherence*, Physical Review Letters **113** (September 2014), no. 14, 140401, available at 1311.0275.

[BCV+21] M. Bilkis, M. Cerezo, Guillaume Verdon, Patrick J. Coles, and Lukasz Cincio, *A semi-agnostic ansatz with variable structure for quantum machine learning* (2021March). arXiv:2103.06712.

[BCWdW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf, *Quantum fingerprinting*, Physical Review Letters **87** (September 2001), no. 16, 167902. arXiv:quant-ph/0102001.

[BCY11a] Fernando G. S. L. Brandão, Matthias Christandl, and Jon Yard, *Faithful squashed entanglement*, Communications in Mathematical Physics **306** (2011September), no. 3, 805–830, available at 1010.1750.

[BCY11b] ———, *A quasipolynomial-time algorithm for the quantum separability problem*, Proceedings of ACM Symposium on Theory of Computation (2011June), 343–351, available at 1011.2751.

[BDSW96] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters, *Mixed-state entanglement and quantum error correction*, Physical Review A **54** (November 1996), no. 5, 3824–3851, available at quant-ph/9604024.

[BDW18] Stefan Bäuml, Siddhartha Das, and Mark M. Wilde, *Fundamental limits on the capacities of bipartite quantum interactions*, Physical Review Letters **121** (December 2018), no. 25, 250504. arXiv:1812.08223.

[BFP07] S. K. Bogner, R. J. Furnstahl, and R. J. Perry, *Similarity renormalization group for nucleon-nucleon interactions*, Phys. Rev. C **75** (June 2007), 061001.

[BG77] P.J. Brussard and P.W.M. Glaudemans, *Shell-model applications in nuclear spectroscopy*, North-Holland Publishing Company, Amsterdam, 1977.

[BGCC21] Jacob L. Beckey, N. Gigena, Patrick J. Coles, and M. Cerezo, *Computable and operationally meaningful multipartite entanglement measures*, Physical Review Letters **127** (September 2021), no. 14, 140501, available at 2104.06923.

[BH13] Fernando G. S. L. Brandão and Aram W. Harrow, *Quantum de Finetti theorems under local measurements with applications*, Proceedings of the 45th annual acm symposium on the theory of computing, 2013June, pp. 861–870.

[BK21] Lennart Bitte and Martin Kliesch, *Training variational quantum algorithms is NP-hard – even for logarithmically many qubits and free fermionic systems*, Physical Review Letters **127** (September 2021), no. 12, 120502, available at 2101.07267.

[BLM+24] M. Burrows, K. D. Launey, A. Mercenne, R. B. Baker, G. H. Sargsyan, T. Dytrych, and D. Langr, *Ab initio translationally invariant nucleon-nucleus optical potentials*, Phys. Rev. C **109** (2024Jan), 014616.

[BLW23] Zachary P. Bradshaw, Margarite L. LaBorde, and Mark M. Wilde, *Cycle index polynomials and generalized quantum separability tests*, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **479** (2023), no. 2274, 20220733, available at 2208.14596.

[BNV13] Bruce R. Barrett, Petr Navrátil, and James P. Vary, *Ab initio no core shell model*, Progress in Particle and Nuclear Physics **69** (2013), 131–181.

[BRRW23] Rahul Bandyopadhyay, Alex H. Rubin, Marina Radulaski, and Mark M. Wilde, *Efficient quantum algorithms for testing symmetries of open quantum systems*, Open Systems & Information Dynamics **30** (September 2023), no. 03, 2350017, available at 2309.02515.

[BRS07] Stephen D. Bartlett, Terry Rudolph, and Robert W. Spekkens, *Reference frames, superselection rules, and quantum information*, Reviews of Modern Physics **79** (April 2007), no. 2, 555–609, available at quant-ph/0610030.

[BRS+21] M. S. Blok, V. V. Ramasesh, T. Schuster, K. O'Brien, J. M. Kreikebaum, D. Dahlen, A. Morvan, B. Yoshida, N. Y. Yao, and I. Siddiqi, *Quantum information scrambling on a superconducting qutrit processor*, Phys. Rev. X **11** (2021Apr), 021010.

[Bru04] Todd A. Brun, *Measuring polynomial functions of states*, Quantum Information and Computation **4** (2004September), no. 5, 401–408. arXiv:quant-ph/0401067.

[BS24] Bharti Bhoy and Paul Stevenson, *Shell-model study of 58ni using quantum computing algorithm*, New Journal of Physics **26** (2024jul), no. 7, 075001.

[B+22] M. T. Burkey et al., *Improved limit on tensor currents in the weak interaction from* ^{8}Li β *decay*, Phys. Rev. Lett. **128** (2022May), 202502.

[BV04] Stephen Boyd and Lieven Vandenberghe, *Convex optimization*, Cambridge University Press, The Edinburgh Building, Cambridge, CB2 8RU, UK, 2004.

[BV97] Ethan Bernstein and Umesh Vazirani, *Quantum complexity theory*, SIAM Journal on Computing **26** (1997), no. 5, 1411–1473.

[BvK02] Paulo F. Bedaque and Ubirajara van Kolck, *Effective field theory for few-nucleon systems*, Annu. Rev. Nucl. Part. Sci. **52** (2002), no. 1, 339–396.

[CAB+21] M. Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, and Patrick J. Coles, *Variational quantum algorithms*, Nature Reviews Physics **3** (August 2021), 625–644, available at 2012.09265.

[CG19] Eric Chitambar and Gilad Gour, *Quantum resource theories*, Reviews of Modern Physics **91** (April 2019), no. 2, 025001, available at 1806.06107.

[CHM+16] Tom Cooney, Christoph Hirche, Ciara Morgan, Jonathan P. Olson, Kaushik P. Seshadreesan, John Watrous, and Mark M. Wilde, *Operational meaning of quantum measures of recovery*, Physical Review A **94** (August 2016), no. 2, 022310. arXiv:1512.05324.

[CKMR07] Matthias Christandl, Robert Koenig, Graeme Mitchison, and Renato Renner, *One-and-a-half quantum de Finetti theorems*, Communications in Mathematical Physics **273** (2007July), no. 2, 473–498, available at quant-ph/0602130 (English).

[CLB+21] Kenneth Choi, Dean Lee, Joey Bonitati, Zhengrong Qian, and Jacob Watkins, *Rodeo algorithm for quantum computing*, Phys. Rev. Lett. **127** (2021Jul), 040505.

[CMN+18] Andrew M. Childs, Dmitri Maslov, Yunseong Nam, Neil J. Ross, and Yuan Su, *Toward the first quantum simulation with quantum speedup*, Proceedings of the National Academy of Sciences **115** (2018), no. 38, 9456–9461, available at 1711.10980.

[CPCC20] M. Cerezo, Alexander Poremba, Lukasz Cincio, and Patrick J. Coles, *Variational quantum fidelity estimation*, Quantum **4** (2020March), 248. arXiv:1906.09253.

[CSV+213] Marco Cerezo, Akira Sone, Tyler James Volkoff, Lukasz Cincio, and Patrick Joseph Coles, *Cost function dependent barren plateaus in shallow parametrized quantum circuits*, Nature Communications **12** (20213), no. 1, 1791, available at 2001.00550.

[CSZW22] Ranyiliu Chen, Zhixin Song, Xuanqiang Zhao, and Xin Wang, *Variational quantum algorithms for trace distance and fidelity estimation*, Quantum Science and Technology **7** (January 2022), no. 1, 015019. arXiv:2012.05768.

[Cub18] Toby Cubitt, *Truths about proofs and groups*, 2018. https://www.dr-qubit.org/Truths_about_proofs_and_groups.html.

[DB10] P. Descouvemont and D. Baye, *The R-matrix theory*, Reports on Progress in Physics **73** (2010feb), no. 3, 036301.

[DBW20] Siddhartha Das, Stefan Bäuml, and Mark M. Wilde, *Entanglement and secret-key-agreement capacities of bipartite quantum interactions and read-only memory devices*, Physical Review A **101** (January 2020), no. 1, 012344. arXiv:1712.00827.

[Deu85] David Deutsch, *Quantum theory, the Church–Turing principle and the universal quantum computer*, Proc. R. Soc. Lond **400** (July 1985), no. 1818, 97–117 (en).

[Die82] D. Dieks, *Communication by EPR devices*, Physics Letters A **92** (1982), 271.

[DLE+20] A. C. Dreyfuss, K. D. Launey, J. E. Escher, G. H. Sargsyan, R. B. Baker, T. Dytrych, and J. P. Draayer, *Clustering and α-capture reaction rate from ab initio symmetry-adapted descriptions of ^{20}Ne*, Phys. Rev. C **102** (2020Oct), 044608. arXiv:2006.11208.

[DMH+18] E. F. Dumitrescu, A. J. McCaskey, G. Hagen, G. R. Jansen, T. D. Morris, T. Papenbrock, R. C. Pooser, D. J. Dean, and P. Lougovski, *Cloud quantum computing of an atomic nucleus*, Phys. Rev. Lett. **120** (2018May), 210501.

[DMMG+21] Olivia Di Matteo, Anna McCoy, Peter Gysbers, Takayuki Miyagi, R. M. Woloshyn, and Petr Navrátil, *Improving Hamiltonian encodings with the Gray code*, Phys. Rev. A **103** (April 2021), 042405.

[DPS02] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri, *Distinguishing separable and entangled states*, Physical Review Letters **88** (2002April), no. 18, 187904, available at quant-ph/0112007.

[DPS04] _____, *Complete family of separability criteria*, Physical Review A **69** (2004February), no. 2, 022308, available at quant-ph/0308032.

[DPS05] _____, *Detecting multipartite entanglement*, Physical Review A **71** (2005March), no. 3, 032333, available at quant-ph/0407143.

[DSS23] Zohreh Davoudi, Alexander F. Shaw, and Jesse R. Stryker, *General quantum algorithms for Hamiltonian simulation with applications to a non-Abelian lattice gauge theory*, Quantum **7** (2023), 1213.

[EBF+13] A. Ekström, G. Baardsen, C. Forssén, G. Hagen, M. Hjorth-Jensen, G. R. Jansen, R. Machleidt, W. Nazarewicz, T. Papenbrock, J. Sarich, and S. M. Wild, *Optimized chiral nucleon-nucleon interaction at next-to-next-to-leading order*, Phys. Rev. Lett. **110** (2013May), 192502.

[EBS+23] Nic Ezzell, Elliott M. Ball, Aliza U. Siddiqui, Mark M. Wilde, Andrew T. Sornborger, Patrick J. Coles, and Zoë Holmes, *Quantum mixed state compiling*, Quantum Science and Technology **8** (2023apr), no. 3, 035001, available at 2209.00528.

[EKM15] E. Epelbaum, H. Krebs, and U.-G. Meißner, *Precision nucleon-nucleon potential at fifth order in the chiral expansion*, Phys. Rev. Lett. **115** (2015Sep), 122301.

[ELR+15] Serdar Elhatisari, Dean Lee, Gautam Rupak, Evgeny Epelbaum, et al., *Ab initio alpha-alpha scattering*, Nature **528** (2015), 111.

[EM03] D. R. Entem and R. Machleidt, *Accurate charge-dependent nucleon-nucleon potential at fourth order of chiral perturbation theory*, Phys. Rev. C **68** (October 2003), 041001.

[ENG+02] E. Epelbaum, A. Nogga, W. Glöckle, H. Kamada, U.-G. Meißner, and H. Witala, *Three-nucleon forces from chiral effective field theory*, Phys. Rev. C **66** (2002), 064001.

[Epe06] Evgeny Epelbaum, *Few-nucleon forces and systems in chiral effective field theory*, Progress in Particle and Nuclear Physics **57** (2006), no. 2, 654–741.

[22] 2022. From ENSDF database as of July, 2022 https://www.nndc.bnl.gov/ensdf/.

[Faw21] Hamza Fawzi, *The set of separable states has no finite semidefinite representation except in dimension 3× 2*, Communications in Mathematical Physics **386** (2021), 1319–1335, available at 1905.02575.

[FC95] Christopher A. Fuchs and Carlton M. Caves, *Mathematical techniques for quantum communication theory*, Open Systems & Information Dynamics **3** (1995), no. 3, 345–356. arXiv:quant-ph/9604001.

[FCP+23] Roland C. Farrell, Ivan A. Chernyshev, Sarah J. M. Powell, Nikita A. Zemlevskiy, Marc Illa, and Martin J. Savage, *Preparations for quantum simulations of quantum chromodynamics in* 1 + 1 *dimensions. I. Axial gauge*, Phys. Rev. D **107** (2023Mar), 054512.

[Fey82] Richard P. Feynman, *Simulating physics with computers*, International Journal of Theoretical Physics **21** (1982), no. 6, 467–488.

[FKS21] Steph Foulds, Viv Kendon, and Tim Spiller, *The controlled SWAP test for determining quantum entanglement*, Quantum Science and Technology **6** (April 2021), no. 3, 035002, available at 2009.07613.

[FR96] Ugo Fano and A. Ravi P. Rau, *Symmetries in quantum physics*, Academic Press, 1996.

[FST22] Omar Fawzi, Ala Shayeghi, and Hoang Ta, *A hierarchy of efficient bounds on quantum capacities exploiting symmetry*, IEEE Transactions on Information Theory **68** (2022), no. 11, 7346–7360, available at 2203.02127.

[Fuc96] Christopher Fuchs, *Distinguishability and accessible information in quantum theory*, Ph.D. Thesis, 1996. arXiv:quant-ph/9601020.

[FvdG99] Christopher A. Fuchs and Jeroen van de Graaf, *Cryptographic distinguishability measures for quantum-mechanical states*, IEEE Transactions on Information Theory **45** (1999May), no. 4, 1216. arXiv:quant-ph/9712042.

[GAE07] David Gross, Koenraad Audenaert, and Jens Eisert, *Evenly distributed unitaries: On the structure of unitary designs*, Journal of Mathematical Physics **48** (May 2007), no. 5, 052104, available at quant-ph/0611002.

[GECP13] Juan Carlos Garcia-Escartin and Pedro Chamorro-Posada, *SWAP test and Hong-Ou-Mandel effect are equivalent*, Physical Review A **87** (2013May), no. 5, 052330. arXiv:1303.6814.

[Gha10] Sevag Gharibian, *Strong NP-hardness of the quantum separability problem*, Quantum Information and Computation **10** (March 2010), no. 3, 343–360, available at 0810.4507.

[GHMW15] Gus Gutoski, Patrick Hayden, Kevin Milner, and Mark M. Wilde, *Quantum interactive proofs and the complexity of separability testing*, Theory of Computing **11** (March 2015), no. 3, 59–103. arXiv:1308.5788.

[GLN05] Alexei Gilchrist, Nathan K. Langford, and Michael A. Nielsen, *Distance measures to compare real and ideal quantum processes*, Physical Review A **71** (2005June), no. 6, 062310, available at quant-ph/0408063. arXiv:quant-ph/0408063.

[Gro96a] David J. Gross, *The role of symmetry in fundamental physics*, Proceedings of the National Academy of Sciences **93** (1996December), no. 25, 14256–14259.

[Gro96b] Lov K. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings of the twenty-eighth annual acm symposium on theory of computing, 1996, pp. 212–219.

[GRS83] E. Gerjuoy, A. R. P. Rau, and Larry Spruch, *A unified formulation of the construction of variational principles*, Reviews of Modern Physics **55** (July 1983), no. 3, 725–774.

[GS08] Gilad Gour and Robert W. Spekkens, *The resource theory of quantum reference frames: manipulations and monotones*, New Journal of Physics **10** (2008March), 033023, available at 0711.0043.

[Gur03] Leonid Gurvits, *Classical deterministic complexity of Edmonds' problem and quantum entanglement*, Proceedings of the thirty-fifth annual acm symposium on theory of computing, 2003, pp. 10–19.

[Gut05] Gus Gutoski, *Short quantum games*, Master's Thesis, 2005. arXiv:quant-ph/0604183.

[Gut09] ———, *Quantum strategies and local operations*, Ph.D. Thesis, 2009. arXiv:1003.0038.

[Gut12] ———, *On a measure of distance for quantum strategies*, Journal of Mathematical Physics **53** (March 2012), no. 3, 032202, available at https://doi.org/10.1063/1.3693621. arXiv:1008.4636.

[GW05] Gus Gutoski and John Watrous, *Quantum interactive proofs with competing provers*, Proceedings of the 22nd symposium on theoretical aspects of computer science (stacs 2005), 2005February, pp. 605–616. arXiv:cs/0412102.

[GW07] ———, *Toward a general theory of quantum games*, Proceedings of 39th acm symposium on the theory of computing, June 2007, pp. 565–574. arXiv:quant-ph/0611234.

[GW13] Gus Gutoski and Xiaodi Wu, *Parallel approximation of min-max problems*, Computational Complexity **22** (2013June), no. 2, 385–428. arXiv:1011.2787.

[Har05] Aram W. Harrow, *Applications of coherent classical communication and the Schur transform to quantum information theory*, Ph.D. Thesis, 2005.

[Har13] ———, *The church of the symmetric subspace*, 2013.

[Hel67] Carl W. Helstrom, *Detection theory and quantum mechanics*, Information and Control **10** (1967), no. 3, 254–291.

[Hel69] ———, *Quantum detection and estimation theory*, Journal of Statistical Physics **1** (1969), 231–252.

[HHHH09] Ryszard Horodecki, Pawel Horodecki, Michal Horodecki, and Karol Horodecki, *Quantum entanglement*, Rev. Mod. Phys. **81** (2009Jun), 865–942.

[HHL09] Aram W. Harrow, Avinatan Hassidim, and Seth Lloyd, *Quantum algorithm for linear systems of equations*, Physical Review Letters **103** (October 2009), no. 15, 150502. arXiv:0811.3171.

[HM10] Aram Harrow and Ashley Montanaro, *An efficient test for product states with applications to quantum Merlin-Arthur games*, Proceedings of the 51st annual ieee symposium on the foundations of computer science (focs), 2010October, pp. 633–642. arXiv:1001.0017.

[HMR+21] William J. Huggins, Jarrod R. McClean, Nicholas C. Rubin, Zhang Jiang, Nathan Wiebe, K. Birgitta Whaley, and Ryan Babbush, *Efficient and noise resilient measurements for quantum chemistry on near-term quantum computers*, npj Quantum Information **7** (February 2021), no. 1, 23.

[HMW14] Patrick Hayden, Kevin Milner, and Mark M. Wilde, *Two-message quantum interactive proofs and the quantum separability problem*, Quantum Information and Computation **14** (April 2014), no. 5–6, 384–416, available at 1211.6120.

[Hoe63] Wassily Hoeffding, *Probability inequalities for sums of bounded random variables*, Journal of the American Statistical Association **58** (1963March), no. 301, 13–30.

[Hol72] Alexander S. Holevo, *An analog of the theory of statistical decisions in noncommutative theory of probability*, Trudy Moskovskogo Matematicheskogo Obshchestva **26** (1972), 133–149. English translation: Trans. Moscow Math Soc. 26, 133–149 (1972).

[HQN19] Guillaume Hupin, Sofia Quaglioni, and Petr Navrátil, *Ab initio predictions for polarized deuterium-tritium thermonuclear fusion*, Nature Communications **10** (2019), 351.

[HSCC22] Zoë Holmes, Kunal Sharma, M. Cerezo, and Patrick J. Coles, *Connecting ansatz expressibility to gradient magnitudes and barren plateaus*, PRX Quantum **3** (2022Jan), 010313.

[HSR03] Michal Horodecki, Peter W. Shor, and Mary Beth Ruskai, *Entanglement breaking channels*, Reviews in Mathematical Physics **15** (2003August), no. 6, 629–641, available at quant-ph/0302031.

[IRS23] Marc Illa, Caroline E. P. Robin, and Martin J. Savage, *Quantum simulations of SO(5) many-fermion systems using qudits*, Phys. Rev. C **108** (2023Dec), 064306.

[IS23] Marc Illa and Martin J. Savage, *Multi-neutrino entanglement and correlations in dense neutrino systems*, Phys. Rev. Lett. **130** (2023May), 221003.

[JJMS22] Pejman Jouzdani, Calvin W. Johnson, Eduardo R. Mucciolo, and Ionel Stetcu, *Alternative approach to quantum imaginary time evolution*, Phys. Rev. A **106** (2022Dec), 062435.

[JJUW10] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous, *QIP = PSPACE*, Communications of the ACM **53** (2010), no. 12, 102–109, available at 0907.4737.

[JNDBB13] C. Ji, N. Nevo Dinur, S. Bacca, and N. Barnea, *Nuclear polarization corrections to the μ^4He$^+$ Lamb shift*, Phys. Rev. Lett. **111** (2013Oct), 143402.

[JUW09] Rahul Jain, Sarvagya Upadhyay, and John Watrous, *Two-message quantum interactive proofs are in PSPACE*, Proceedings of the 2009 50th annual ieee symposium on foundations of computer science, 2009, pp. 534–543.

[JVHW15] Jiantao Jiao, Kartik Venkat, Yanjun Han, and Tsachy Weissman, *Minimax estimation of functionals of discrete distributions*, IEEE Transactions on Information Theory **61** (May 2015), no. 5, 2835–2885. arXiv:1406.6956.

[JW07] Dominik Janzing and Pawel Wocjan, *A simple PromiseBQP-complete matrix problem*, Theory of Computing **3** (2007), no. 1, 61–79.

[KDWW19] Eneet Kaur, Siddhartha Das, Mark M. Wilde, and Andreas Winter, *Extendibility limits the performance of quantum processors*, Physical Review Letters **123** (August 2019), no. 7, 070502, available at 2108.03137.

[KDWW21] _____, *Resource theory of unextendibility and nonasymptotic quantum capacity*, Physical Review A **104** (August 2021), 022401, available at 1803.10710.

[KGL+22] Oriel Kiss, Michele Grossi, Pavel Lougovski, Federico Sanchez, Sofia Vallecorsa, and Thomas Papenbrock, *Quantum computing of the* ^{6}Li *nucleus via ordered unitary coupled clusters*, Phys. Rev. C **106** (2022Sep), 034325.

[Kit97] Alexei Kitaev, *Quantum computations: algorithms and error correction*, Russian Mathematical Surveys **52** (1997), no. 6, 1191–1249.

[KKP+12] J.H. Kelley, E. Kwan, J.E. Purcell, C.G. Sheu, and H.R. Weller, *Energy levels of light nuclei A = 11*, Nuclear Physics A **880** (2012), 88–195.

[KL01] Emanuel Knill and Raymond Laflamme, *Quantum computing and quadratically signed weight enumerators*, Information Processing Letters **79** (August 2001), no. 4, 173–179. arXiv:quant-ph/9909094.

[KM01] Phillip Kaye and Michele Mosca, *Quantum networks for concentrating entanglement*, Journal of Physics A: Mathematical and General **34** (August 2001), no. 35, 6939, available at quant-ph/0101009.

[KMT+17] Abhinav Kandala, Antonio Mezzacapo, Kristan Temme, Maika Takita, Markus Brink, Jerry M. Chow, and Jay M. Gambetta, *Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets*, Nature **549** (2017), no. 7671, 242–246. arXiv:1704.05018.

[KMY01] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami, *Quantum certificate verification: Single versus multiple quantum certificates* (2001). arXiv:quant-ph/0110006.

[KRS09] Robert Koenig, Renato Renner, and Christian Schaffner, *The operational meaning of min- and max-entropy*, IEEE Transactions on Information Theory **55** (2009September), no. 9, 4337–4347. arXiv:0807.1338.

[Kup05] Greg Kuperberg, *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem*, SIAM Journal on Computing **35** (2005), no. 1, 170–188, available at quant-ph/0302112.

[KW00] Alexei Kitaev and John Watrous, *Parallelization, amplification, and exponential time simulation of quantum interactive proof systems*, Proceedings of the thirty-second annual acm symposium on theory of computing, 2000, pp. 608–617.

[KW20] Sumeet Khatri and Mark M. Wilde, *Principles of quantum communication theory: A modern approach*, 2020. arXiv:2011.04672v1.

[KW21] Vishal Katariya and Mark M. Wilde, *Geometric distinguishability measures limit quantum channel estimation and discrimination*, Quantum Information Processing **20** (2021April), 78, available at 2004.10708. arXiv:2004.10708.

[LKDW18] Felix Leditzky, Eneet Kaur, Nilanjana Datta, and Mark M. Wilde, *Approaches for approximate additivity of the Holevo information of quantum channels*, Physical Review A **97** (January 2018), no. 1, 012332. arXiv:1709.01111.

[LLSL21] Sheng-Jie Li, Jin-Min Liang, Shu-Qian Shen, and Ming Li, *Variational quantum algorithms for trace norms and their applications*, Communications in Theoretical Physics **73** (October 2021), no. 10, 105102.

[LMD21] K. D. Launey, A. Mercenne, and T. Dytrych, *Nuclear dynamics and reactions in the ab initio symmetry-adapted framework*, Annu. Rev. Nucl. Part. Sci. **71** (2021), 253.

[LRW23] Margarite L. LaBorde, Soorya Rethinasamy, and Mark M. Wilde, *Testing symmetry on quantum computers*, Quantum **7** (September 2023), 1120.

[LSS+22] Martín Larocca, Frédéric Sauvage, Faris M. Sbahi, Guillaume Verdon, Patrick J. Coles, and M. Cerezo, *Group-invariant quantum machine learning*, PRX Quantum **3** (September 2022), no. 3, 030341, available at 2205.02261.

[LTW+24] Martin Larocca, Supanut Thanasilp, Samson Wang, Kunal Sharma, Jacob Biamonte, Patrick J. Coles, Lukasz Cincio, Jarrod R. McClean, Zoë Holmes, and M. Cerezo, *A review of barren plateaus in variational quantum computing*, 2024.

[LW21] Margarite L. LaBorde and Mark M. Wilde, *Testing symmetry on quantum computers*, arXiv, 2021.

[Mar13] Iman Marvian, *Comment during seminar "how hard is it to decide if a quantum state is separable or entangled?"*, 2013.

[MLDS+13] Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel, *On quantum Rényi entropies: a new generalization and some properties*, Journal of Mathematical Physics **54** (2013December), no. 12, 122203, available at 1306.3142. arXiv:1306.3142.

[MMP19] A. Mercenne, N. Michel, and M. Płoszajczak, *Gamow shell model description of* ^{4}He(d, d) *elastic scattering reactions*, Phys. Rev. C **99** (2019Apr), 044606.

[Mon08] Ashley Montanaro, *A lower bound on the probability of error in quantum state discrimination*, 2008 ieee information theory workshop, May 2008, pp. 378–380. arXiv:0711.2012.

[MS13] Iman Marvian and Robert W. Spekkens, *The theory of manipulations of pure state asymmetry: I. basic tools, equivalence classes and single copy transformations*, New Journal of Physics **15** (March 2013), no. 3, 033001, available at 1104.0018.

[MS14] ———, *Modes of asymmetry: The application of harmonic analysis to symmetric quantum dynamics and quantum reference frames*, Physical Review A **90** (December 2014), no. 6, 062110, available at 1312.0680.

[MW05] Chris Marriott and John Watrous, *Quantum Arthur–Merlin games*, Computational Complexity **14** (2005), 122–152, available at cs/0506068.

[Nai40] Mark Aronovich Naimark, *Spectral functions of a symmetric operator*, Izv. Akad. Nauk SSSR Ser. Mat. **4** (1940), no. 3, 277–318.

[NC00] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, 2000.

[NC10] _____, *Quantum computation and quantum information: 10th anniversary edition*, Cambridge University Press, 2010.

[NOP09] Miguel Navascués, Masaki Owari, and Martin B. Plenio, *Power of symmetric extensions for entanglement detection*, Physical Review A **80** (November 2009), no. 5, 052306, available at 0906.2731.

[Now16] Marcin L. Nowakowski, *The symmetric extendibility of quantum states*, Journal of Physics A: Mathematical and Theoretical **49** (August 2016), no. 38, 385301, available at 1504.00388.

[ON07] Tomohiro Ogawa and Hiroshi Nagaoka, *Making good codes for classical-quantum channel coding via quantum hypothesis testing*, IEEE Transactions on Information Theory **53** (2007June), no. 6, 2261–2266.

[Par70] James L. Park, *The concept of transition in quantum mechanics*, Foundations of Physics **1** (March 1970), no. 1, 23–33.

[Pet85] Dénes Petz, *Quasi-entropies for states of a von Neumann algebra*, Publ. RIMS, Kyoto University **21** (1985), 787–800.

[Pet86] _____, *Quasi-entropies for finite quantum systems*, Reports in Mathematical Physics **23** (1986), 57–65.

[Pia16] Marco Piani, *Hierarchy of efficiently computable and faithful lower bounds to quantum discord*, Physical Review Letters **117** (August 2016), no. 8, 080401, available at 1501.06855.

[PMS+14] Alberto Peruzzo, Jarrod McClean, Peter Shadbolt, Man-Hong Yung, Xiao-Qi Zhou, Peter J. Love, Alán Aspuru-Guzik, and Jeremy L. O'Brien, *A variational eigenvalue solver on a photonic quantum processor*, Nature Communications **5** (2014), no. 1, 4213.

[PORM+23] A. Perez-Obiol, A. M. Romero, J. Menendez, et al., *Nuclear shell-model simulation in digital quantum computers*, Scientific Reports **13** (July 2023), 12291.

[Pow94] M. J. D. Powell, *A direct search optimization method that models the objective and constraint functions by linear interpolation*, Advances in optimization and numerical analysis, 1994, pp. 51–67.

[PRRW24] Aby Philip, Soorya Rethinasamy, Vincent Russo, and Mark M. Wilde, *Schrödinger as a Quantum Programmer: Estimating Entanglement via Steering*, Quantum **8** (June 2024), 1366, available at 2303.07911.

[PV10] Yury Polyanskiy and Sergio Verdú, *Arimoto channel coding converse and rényi divergence*, 2010 48th annual allerton conference on communication, control, and computing (allerton), 2010, pp. 1327–1333.

[PVM21] Sreeram PG, Naga Dileep Varikuti, and Vaibhav Madhok, *Exponential speedup in measuring out-of-time-ordered correlators and gate fidelity with a single bit of quantum information*, Physics Letters A **397** (2021), 127257, available at 2009.03415.

[Qiu08] Daowen Qiu, *Minimum-error discrimination between mixed quantum states*, Physical Review A **77** (January 2008), no. 1, 012328. arXiv:0707.3970.

[QKW24] Yihui Quek, Eneet Kaur, and Mark M. Wilde, *Multivariate trace estimation in constant quantum depth*, Quantum **8** (January 2024), 1220.

[QN09] Sofia Quaglioni and Petr Navrátil, *Ab initio many-body calculations of nucleon-nucleus scattering*, Phys. Rev. C **79** (2009Apr), 044606.

[Ras06] Alexey E. Rastegin, *Sine distance for quantum states*, 2006.

[RASW23] Soorya Rethinasamy, Rochisha Agarwal, Kunal Sharma, and Mark M. Wilde, *Estimating distinguishability measures on quantum computers*, Physical Review A **108** (July 2023), no. 1, 012409, available at 2108.08406.

[RBN+22] Michael Ragone, Paolo Braccia, Quynh T. Nguyen, Louis Schatzki, Patrick J. Coles, Frederic Sauvage, Martin Larocca, and M. Cerezo, *Representation theory for geometric quantum machine learning*, 2022.

[RDH+17] J. Rotureau, P. Danielewicz, G. Hagen, F. M. Nunes, and T. Papenbrock, *Optical potential from first principles*, Phys. Rev. C **95** (2017Feb), 024315.

[RGW+24a] Soorya Rethinasamy, Ethan Guo, Alexander Wei, Mark M Wilde, and Kristina D Launey, *Neutron-nucleus dynamics simulations for quantum computers*, arXiv preprint arXiv:2402.14680 (2024).

[RGW+24b] Soorya Rethinasamy, Ethan Guo, Alexander Wei, Mark M. Wilde, and Kristina D. Launey, *Neutron-nucleus dynamics simulations for quantum computers*, Zenodo, 2024.

[RLW25] Soorya Rethinasamy, Margarite L. LaBorde, and Mark M. Wilde, *Quantum computational complexity and symmetry*, Canadian Journal of Physics **103** (2025), no. 2, 215–239, available at https://doi.org/10.1139/cjp-2023-0260.

[RMMB21] Denis Rosset, Felipe Montealegre-Mora, and Jean-Daniel Bancal, *Replab: A computational/numerical approach to representation theory*, Quantum theory and symmetries, 2021, pp. 643–653.

[RS09] Aidan Roy and A. J. Scott, *Unitary designs and codes*, Designs, Codes and Cryptography **53** (April 2009), 13–31.

[RW05] Bill Rosgen and John Watrous, *On the hardness of distinguishing mixed-state quantum computations*, Proceedings of the 20th IEEE Conference on Computational Complexity (2005June), 344–354. arXiv:cs/0407056.

[SA21] Pooja Siwach and P. Arumugam, *Quantum simulation of nuclear Hamiltonian with a generalized transformation for Gray code encoding*, Physical Review C **104** (September 2021), no. 3, 034301.

[SAP17] Alexander Streltsov, Gerardo Adesso, and Martin B. Plenio, *Colloquium: Quantum coherence as a resource*, Reviews of Modern Physics **89** (October 2017), no. 4, 041003, available at 1609.02439.

[SBC22] I. Stetcu, A. Baroni, and J. Carlson, *Variational approaches to constructing the many-body nuclear ground state for quantum computing*, Phys. Rev. C **105** (2022Jun), 064308.

[SCC19] Yiğit Subaşı, Lukasz Cincio, and Patrick J Coles, *Entanglement spectroscopy with a depth-two quantum circuit*, Journal of Physics A: Mathematical and Theoretical **52** (January 2019), no. 4, 044001. arXiv:1806.08863.

[SCLW22] Torin F. Stetina, Anthony Ciavarella, Xiaosong Li, and Nathan Wiebe, *Simulating Effective QED on Quantum Computers*, Quantum **6** (January 2022), 622.

[Sco08] A. J. Scott, *Optimizing quantum process tomography with unitary 2-designs*, Journal of Physics A: Mathematical and Theoretical **41** (2008jan), no. 5, 055308, available at 0711.1017.

[SDG+21] Robert Salzmann, Nilanjana Datta, Gilad Gour, Xin Wang, and Mark M. Wilde, *Symmetric distinguishability as a quantum resource*, New Journal of Physics **23** (August 2021), 083016. arXiv:2102.12512.

[Sha98] I. Shavitt, *The history and evolution of configuration interaction*, Molecular Physics **94** (1998), no. 1, 3–17.

[Sho97] Peter W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal on Computing **26** (1997), no. 5, 1484–1509, available at https://doi.org/10.1137/S0097539795293172.

[Sio58] Maurice Sion, *On general minimax theorems*, Pacific Journal of Mathematics **8** (1958March), no. 1, 171–176.

[SKCC20] Kunal Sharma, Sumeet Khatri, M Cerezo, and Patrick J Coles, *Noise resilience of variational quantum compiling*, New Journal of Physics **22** (2020apr), no. 4, 043006.

[SLB+22] G. H. Sargsyan, K. D. Launey, M. T. Burkey, A. T. Gallant, N. D. Scielzo, G. Savard, A. Mercenne, T. Dytrych, D. Langr, L. Varriano, B. Longfellow, T. Y. Hirsh, and J. P. Draayer, *Impact of clustering on the* ^{8}Li β *decay and recoil form factors*, Phys. Rev. Lett. **128** (2022May), 202503.

[SMK+20] N. P. D. Sawaya, T. Menke, T. H. Kyaw, et al., *Resource-efficient digital quantum simulation of d-level systems for photonic, vibrational, and spin-s Hamiltonians*, npj Quantum Information **6** (2020).

[Spa92] James C. Spall, *Multivariate stochastic approximation using a simultaneous perturbation gradient approximation*, IEEE Transactions on Automatic Control **37** (1992), no. 3, 332–341.

[Spa98] ———, *An overview of the simultaneous perturbation method for efficient optimization*, Johns Hopkins Applied Technical Digest **19** (1998), no. 4, 482–492.

[Ste12] Benjamin Steinberg, *Representation theory of finite groups: An introductory approach*, Springer, 2012.

[Sti55] W. F. Stinespring, *Positive functions on C*-algebras*, Proceedings of the American Mathematical Society **6** (1955), 211–216.

[SW15] Kaushik P. Seshadreesan and Mark M. Wilde, *Fidelity of recovery, squashed entanglement, and measurement recoverability*, Physical Review A **92** (2015October), no. 4, 042321. arXiv:1410.1441.

[Ter04] Barbara M. Terhal, *Is entanglement monogamous?*, IBM Journal of Research and Development **48** (January 2004), no. 1, 71–78, available at quant-ph/0307120.

[TN09] Ian J. Thompson and Filomena M. Nunes, *Nuclear reactions for astrophysics: Principles, calculation and applications of low-energy reactions*, Cambridge University Press, 2009.

[Tom15] Marco Tomamichel, *Quantum information processing with finite resources: mathematical foundations*, Springer, 2015.

[TRA+22] F. Turro, A. Roggero, V. Amitrano, P. Luchi, K. A. Wendt, J. L. Dubois, S. Quaglioni, and F. Pederiva, *Imaginary-time propagation on a quantum chip*, Phys. Rev. A **105** (2022Feb), 022440.

[T+23] F. Turro et al., *A quantum-classical co-processing protocol towards simulating nuclear reactions on contemporary quantum hardware*, 2023.

[TV21] Kok Chuan Tan and Tyler Volkoff, *Variational quantum algorithms to estimate rank, quantum entropies, fidelity and Fisher information via purity minimization*, Physical Review Research **3** (September 2021), no. 3, 033251. arXiv:2103.15956.

[Uhl76] Armin Uhlmann, *The "transition probability" in the state space of a *-algebra*, Reports on Mathematical Physics **9** (1976April), no. 2, 273–279.

[VC05] F Verstraete and J I Cirac, *Mapping local Hamiltonians of fermions to local Hamiltonians of spins*, Journal of Statistical Mechanics: Theory and Experiment **2005** (2005sep), no. 09, P09012.

[VENN24] Arian Vezvaee, Nathan Earnest-Noble, and Khadijeh Najafi, *Quantum simulation of Fermi–Hubbard model based on transmon qudit interaction*, 2024.

[VGO+20] Pauli Virtanen, Ralf Gommers, Travis E. Oliphant, Matt Haberland, et al., *SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python*, Nature Methods **17** (2020), 261–272.

[VW16] Thomas Vidick and John Watrous, *Quantum proofs*, Foundations and Trends in Theoretical Computer Science **11** (2016March), no. 1–2, 1–215. arXiv:1610.01664.

[VYI2003] Vladyslav Verteletskyi, Tzu-Ching Yen, and Artur F. Izmaylov, *Measurement optimization in the variational quantum eigensolver using a minimum clique cover*, The Journal of Chemical Physics **152** (202003), no. 12, 124114.

[Wat02a] John Watrous, *Capturing quantum complexity classes via quantum channels*, Talk at the 6th Workshop on Quantum Information Processing, 2002. http://www.msri.org/workshops/204/schedules/1235.

[Wat02b] ———, *Limits on the power of quantum statistical zero-knowledge*, Proceedings of the 43rd annual ieee symposium on foundations of computer science, 2002November, pp. 459–468.

[Wat02c] ———, *Limits on the power of quantum statistical zero-knowledge*, Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (2002November), 459–468. arXiv:quant-ph/0202111.

[Wat03] ———, *PSPACE has constant-round quantum interactive proof systems*, Theoretical Computer Science **292** (2003), no. 3, 575–588.

[Wat06] ———, *Zero-knowledge against quantum attacks*, Proceedings of the thirty-eighth annual acm symposium on theory of computing, 2006, pp. 296–305.

[Wat09a] ———, *Quantum computational complexity*, Encyclopedia of Complexity and System Science (2009), available at 0804.3401.

[Wat09b] ———, *Quantum computational complexity*, Encyclopedia of Complexity and System Science (2009). arXiv:0804.3401.

[Wat09c] ———, *Semidefinite programs for completely bounded norms*, Theory of Computing **5** (2009November), no. 11, 217–238, available at 0901.4709. arXiv:0901.4709.

[Wat09d] ———, *Zero-knowledge against quantum attacks*, SIAM Journal on Computing **39** (2009), no. 1, 25–58. arXiv:quant-ph/0511020.

[Wat13] ———, *Simpler semidefinite programs for completely bounded norms*, Chicago Journal of Theoretical Computer Science **2013** (2013July), no. 8, 1–19, available at 1207.5726. arXiv:1207.5726.

[Wat18] ———, *The theory of quantum information*, Cambridge University Press, 2018.

[Wer89a] Reinhard F. Werner, *An application of Bell's inequalities to a quantum state extension problem*, Letters in Mathematical Physics **17** (1989May), no. 4, 359–363.

[Wer89b] ———, *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*, Physical Review A **40** (October 1989), no. 8, 4277–4281.

[WGL+22] Qisheng Wang, Ji Guan, Junyi Liu, Zhicheng Zhang, and Mingsheng Ying, *New quantum algorithms for computing quantum entropies and distances* (March 2022). arXiv:2203.13522.

[Wil17] Mark M. Wilde, *Quantum information theory*, Second Edition, Cambridge University Press, 2017.

[Wil20] ———, *Coherent quantum channel discrimination*, Proceedings of the 2020 ieee international symposium on information theory (isit), June 2020, pp. 1915–1920. arXiv:2001.02668.

[Win99] Andreas Winter, *Coding theorem and strong converse for quantum channels*, IEEE Transactions on Information Theory **45** (1999November), no. 7, 2481–2485, available at 1409.2536.

[W+23] James D. Watson et al., *Quantum algorithms for simulating nuclear effective field theories*, 2023.

[WWW52] G. C. Wick, A. S. Wightman, and E. P. Wigner, *The intrinsic parity of elementary particles*, Physical Review **88** (October 1952), no. 1, 101–105.

[WWY14] Mark M. Wilde, Andreas Winter, and Dong Yang, *Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy*, Communications in Mathematical Physics **331** (2014October), no. 2, 593–622. arXiv:1306.1586.

[WZ23] Qisheng Wang and Zhicheng Zhang, *Fast quantum algorithms for trace distance estimation* (January 2023). arXiv:2301.06783.

[WZ82] William K. Wootters and Wojciech H. Zurek, *A single quantum cannot be cloned*, Nature **299** (1982), 802–803.

[WZC+21] Qisheng Wang, Zhicheng Zhang, Kean Chen, Ji Guan, Wang Fang, and Mingsheng Ying, *Quantum algorithm for fidelity estimation*, IEEE Transactions on Information Theory **69** (January 2021), no. 1, 273–282. arXiv:2103.09076.

[YF17] Haidong Yuan and Chi-Hang Fred Fung, *Fidelity and Fisher information on quantum channels*, New Journal of Physics **19** (November 2017), no. 11, 113039. arXiv:1506.00819.

[YVI2004] Tzu-Ching Yen, Vladyslav Verteletskyi, and Artur F. Izmaylov, *Measuring all compatible operators in one series of single-qubit measurements using unitary transformations*, Journal of Chemical Theory and Computation **16** (202004), no. 4, 2400–2409.

[Zha11] Fuzhen Zhang, *Matrix theory: Basic results and techniques*, Springer, 2011.

[Zha12] Shengyu Zhang, *Bqp-complete problems*, Handbook of natural computing, 2012, pp. 1545–1571.

Appendix A

Big-O Notation

In this appendix, we give a short summary of the Big-O notation that gives us a method to describe the long-term behavior of functions and is commonly used to describe the performance of an algorithm. Consider the following two functions $f(x) = 100x$ and $g(x) = x^2$. The plots for these two functions can be found in Figure A.1. For small values of x, $f(x) > g(x)$, but after $x = 100$, $g(x) > f(x)$ for all x. Given two algorithms to solve the same problem, Algorithm 1, requiring $f(x)$ time and Algorithm 2, requiring $g(x)$ time, we should always prefer to use Algorithm 1 despite the fact that it takes longer for smaller inputs. This is because we are interested in the performance for larger inputs, where Algorithm 1 outperforms Algorithm 2. Let us now look at a formal definition.

Definition A.1 [*Big-O*]. *Consider two functions $f(x)$ and $g(x)$. We write that*

$$f(x) = O(g(x)) \tag{A.1}$$

if and only if there exists constants N and c such that

$$f(x) \leq cg(x) \qquad \forall x > N. \tag{A.2}$$

Intuitively, this means that f does not grow faster than g. In the example above, we can pick $c = 1$ and $N = 100$ to satisfy the constraints.

When $f(x) = O(g(x))$, this means that $g(x)$ is an asymptotic upper bound on $f(x)$. An important point here is that we can always pick larger and larger functions $g(x)$ such that this is true. For example, say a function $f(x) = O(x^2)$. Then, it

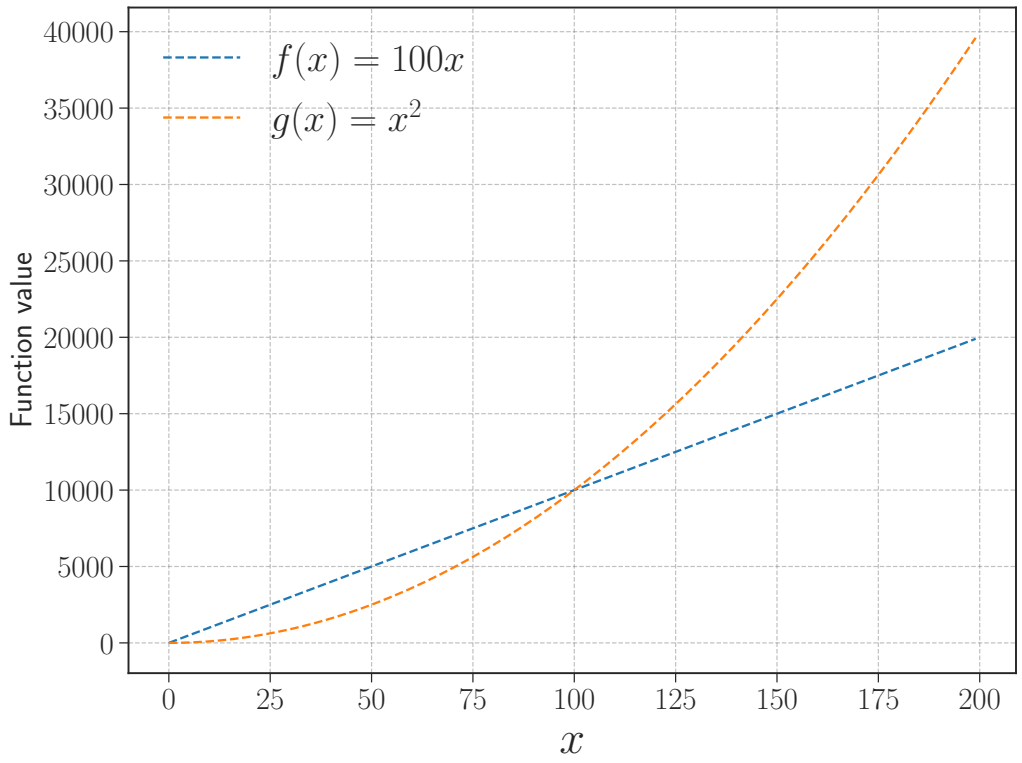


Figure A.1: Comparison of the asymptotic growth of two functions.

is clear that $f(x) = O(x^3)$ as well. The idea is to find the tightest asymptotic upper bound.

Using the Big-O notation, functions can be classified based on the growth. A few examples classes, in increasing magnitude, are as follows:

1. **Constant** - $f(x) = 5$.
2. **Log** - $f(x) = 100 \log(x)$.
3. **Linear** - $f(x) = 2x$.
4. **LogLinear** - $f(x) = x \log(x)$.
5. **Polynomial** - $f(x) = x^c$.
6. **Exponential** = $f(x) = c^x$.
7. **Factorial** = $f(x) = 2x!$.

Appendix B

Supplementary material of Chapter 3

B.1 Proof of Theorem 3.1

Proof of Theorem 3.1. After Step 1 of Algorithm 3.4, the global state is

$$|\Phi\rangle_{T'T}|0\rangle_{RS}\,. \tag{B.1}$$

After Step 2 of Algorithm 3.4, it is

$$\frac{1}{\sqrt{2}}\sum_{i\in\{0,1\}}|i\rangle_{T'}|i\rangle_{T}|\psi^i\rangle_{RS}\,. \tag{B.2}$$

After Step 4 of Algorithm 3.4, it is

$$P_{T'RF\to T''F'}\left(\frac{1}{\sqrt{2}}\sum_{i\in\{0,1\}}|i\rangle_{T'}|i\rangle_{T}|\psi^i\rangle_{RS}|0\rangle_{F}\right). \tag{B.3}$$

For a fixed unitary $P\equiv P_{T'RF\to T''F'}$ of the prover, the acceptance probability is then

$$\left\|\langle\Phi|_{T''T}P\left(\frac{1}{\sqrt{2}}\sum_{i\in\{0,1\}}|i\rangle_{T'}|i\rangle_{T}|\psi^i\rangle_{RS}|0\rangle_{F}\right)\right\|_2^2=\frac{1}{2}\left\|\langle\Phi|_{T''T}P\sum_{i\in\{0,1\}}|i\rangle_{T'}|i\rangle_{T}|\psi^i\rangle_{RS}|0\rangle_{F}\right\|_2^2. \tag{B.4}$$

In a quantum interactive proof, the prover is trying to maximize the probability that the verifier accepts. So the acceptance probability of Algorithm 3.4 is given

by

$$\max_{P_{T'RF\to T''F'}} \frac{1}{2}\left\|\langle\Phi|_{T''T}P\sum_{i\in\{0,1\}}|i\rangle_{T'}|i\rangle_{T}|\psi^i\rangle_{RS}|0\rangle_F\right\|_2^2. \tag{B.5}$$

Setting

$$P^0_{R\to F'} := \langle 0|_{T''}P_{T'RF\to T''F'}|0\rangle_{T'}|0\rangle_F, \tag{B.6}$$

$$P^1_{R\to F'} := \langle 1|_{T''}P_{T'RF\to T''F'}|1\rangle_{T'}|0\rangle_F, \tag{B.7}$$

we have that

$$\frac{1}{2}\left\|\langle\Phi|_{T''T}P\sum_{i\in\{0,1\}}|i\rangle_{T'}|i\rangle_{T}|\psi^i\rangle_{RS}|0\rangle_F\right\|_2^2 = \frac{1}{4}\left\|\sum_{i\in\{0,1\}}P^i_{R\to F'}|\psi^i\rangle_{RS}\right\|_2^2 \tag{B.8}$$

$$= \frac{1}{4}\sum_{i,j\in\{0,1\}}\langle\psi^i|_{RS}(P^i_{R\to F'})^\dagger P^j_{R\to F'}|\psi^j\rangle_{RS} \tag{B.9}$$

$$\leq \frac{1}{2}\left(1+\mathrm{Re}\left\{\langle\psi^0|_{RS}(P^0_{R\to F'})^\dagger P^1_{R\to F'}|\psi^1\rangle_{RS}\right\}\right) \tag{B.10}$$

$$\leq \frac{1}{2}\left(1+\left|\langle\psi^0|_{RS}(P^0_{R\to F'})^\dagger P^1_{R\to F'}|\psi^1\rangle_{RS}\right|\right). \tag{B.11}$$

The first inequality follows because $P^i_{R\to F'}$ is a contraction for $i\in\{0,1\}$, so that $(P^i_{R\to F'})^\dagger P^i_{R\to F'}\leq I_{F'}$. Then consider that

$$\left|\langle\psi^0|_{RS}(P^0_{R\to F'})^\dagger P^1_{R\to F'}|\psi^1\rangle_{RS}\right| =\leq \max_{P^0,P^1}\left\{\begin{array}{c}\left|\langle\psi^0|_{RS}(P^0_{R\to F'})^\dagger P^1_{R\to F'}|\psi^1\rangle_{RS}\right| \\ : \left\|P^i\right\|_\infty\leq 1\ \forall i\end{array}\right\} \tag{B.12}$$

$$= \sqrt{F}(\rho^0_S,\rho^1_S). \tag{B.13}$$

The last line is a consequence of the following reasoning (which is the same as that employed in Section III in [CHM+16]). The inequality

$$\max_{P^0,P^1}\left\{\begin{array}{c}\left|\langle\psi^0|_{RS}(P^0_{R\to F'})^\dagger P^1_{R\to F'}|\psi^1\rangle_{RS}\right| \\ : \left\|P^i\right\|_\infty\leq 1\ \forall i\end{array}\right\} \geq \sqrt{F}(\rho^0_S,\rho^1_S) \tag{B.14}$$

holds because the isometries $P^0_{R\to F'}$ and $P^1_{R\to F'}$ that achieve the maximum for the fidelity are each contractions and the optimization is conducted over all contractions. The opposite inequality

$$\max_{P^0,P^1}\left\{\begin{array}{c}\left|\langle\psi^0|_{RS}(P^0_{R\to F'})^\dagger P^1_{R\to F'}|\psi^1\rangle_{RS}\right| \\ : \left\|P^i\right\|_\infty\leq 1\ \forall i\end{array}\right\} \leq \sqrt{F}(\rho^0_S,\rho^1_S) \tag{B.15}$$

is a consequence of the fact that every contraction can be written as a convex combination of isometries [Zha11, Theorem 5.10]. Indeed, this means that, for each $i \in \{0,1\}$,

$$P^i_{R\to F'} = \sum_x p_i(x) W^{i,x}_{R\to F'}, \tag{B.16}$$

where $\{p_i(x)\}_x$ is a probability distribution and $W^{i,x}_{R\to F'}$ is an isometry, for each i and x. Then we find that

$$\begin{aligned}
\left|\langle\psi^0|_{RS} (P^0_{R\to F'})^\dagger P^1_{R\to F'} |\psi^1\rangle_{RS}\right| &= \left| \begin{array}{c} \langle\psi^0|_{RS} \left(\sum_x p_0(x) W^{0,x}_{R\to F'}\right)^\dagger \times \\ \left(\sum_{x'} p_1(x') W^{1,x'}_{R\to F'}\right) |\psi^1\rangle_{RS} \end{array} \right| && \text{(B.17)} \\
&= \left| \sum_{x,x'} p_0(x) p_1(x') \langle\psi^0|_{RS} \left(W^{0,x}_{R\to F'}\right)^\dagger W^{1,x'}_{R\to F'} |\psi^1\rangle_{RS} \right| && \text{(B.18)} \\
&\leq \sum_{x,x'} p_0(x) p_1(x') \left| \langle\psi^0|_{RS} \left(W^{0,x}_{R\to F'}\right)^\dagger W^{1,x'}_{R\to F'} |\psi^1\rangle_{RS} \right| && \text{(B.19)} \\
&\leq \max_{x,x'} \left| \langle\psi^0|_{RS} \left(W^{0,x}_{R\to F'}\right)^\dagger W^{1,x'}_{R\to F'} |\psi^1\rangle_{RS} \right| && \text{(B.20)} \\
&\leq \sqrt{F}(\rho^0_S, \rho^1_S). && \text{(B.21)}
\end{aligned}$$

Thus, an upper bound on the acceptance probability of Algorithm 3.4 is as follows:

$$\frac{1}{2}\left(1 + \sqrt{F}(\rho^0_S, \rho^1_S)\right). \tag{B.22}$$

This upper bound can be achieved if the prover applies a unitary extension of the following isometry:

$$P_{T'RF\to T''F'} = \sum_{i\in\{0,1\}} |i\rangle_{T''}\langle i|_{T'} \otimes P^i_{R\to F'} \otimes \langle 0|_F, \tag{B.23}$$

where $P^0_{R\to F'}$ and $P^1_{R\to F'}$ are isometries achieving the maximum in the fidelity $F(\rho^0_S, \rho^1_S)$. ■

B.2 Proof of Theorem 3.2

Proof of Theorem 3.2. After Step 1 of Algorithm 3.5, the global state is

$$|\Phi\rangle_{T'T} |0\rangle_{R_1 S_1 R_2 S_2}. \tag{B.24}$$

After Step 2, the global state is

$$|\Phi\rangle_{T'T}|\psi^{\rho^0}\rangle_{R_1S_1}|\psi^{\rho^1}\rangle_{R_2S_2}. \tag{B.25}$$

After Step 3, it becomes

$$\frac{1}{\sqrt{2}}|0\rangle_T|0\rangle_{T'}|\psi^{\rho^0}\rangle_{R_1S_1}|\psi^{\rho^1}\rangle_{R_2S_2} + \frac{1}{\sqrt{2}}|1\rangle_T|1\rangle_{T'}|\psi^{\rho^1}\rangle_{R_2S_1}|\psi^{\rho^0}\rangle_{R_1S_2}. \tag{B.26}$$

The verifier then sends systems T', R_1, and R_2 to the prover, who appends the state $|0\rangle_F$ and acts with a unitary $P_{T'R_1R_2F\to T''F'}$. Without loss of generality, and for simplicity of the ensuing analysis, we can imagine that before applying the unitary $P_{T'R_1R_2F\to T''F'}$, the prover applies a controlled SWAP to systems T', R_1, and R_2, so that the state before applying $P_{T'R_1R_2F\to T''F'}$ is as follows:

$$\frac{1}{\sqrt{2}}|0\rangle_T|0\rangle_{T'}|\psi^{\rho^0}\rangle_{R_1S_1}|\psi^{\rho^1}\rangle_{R_2S_2} + \frac{1}{\sqrt{2}}|1\rangle_T|1\rangle_{T'}|\psi^{\rho^1}\rangle_{R_1S_1}|\psi^{\rho^0}\rangle_{R_2S_2}. \tag{B.27}$$

This follows because the prover can apply arbitrary unitaries to his received systems, and one such possible unitary is to apply this controlled SWAP, undo it, and then apply $P_{T'R_1R_2F\to T''F'}$. However, the latter two unitaries are a particular example of a unitary $P_{T'R_1R_2F\to T''F'}$. So we proceed with the ensuing analysis assuming that the global state, before the prover applies $P_{T'R_1R_2F\to T''F'}$, is given by (B.27). Note that the actions of tensoring in the state $|0\rangle_F$ and applying $P_{T'R_1R_2F\to T''F'}$ together constitute an isometry

$$P_{T'R_1R_2\to T''F'} := P_{T'R_1R_2F\to T''F'}|0\rangle_F, \tag{B.28}$$

resulting in the state

$$\frac{1}{\sqrt{2}}P_{T'R_1R_2\to T''F'}|0\rangle_T|0\rangle_{T'}|\psi^{\rho^0}\rangle_{R_1S_1}|\psi^{\rho^1}\rangle_{R_2S_2} + \frac{1}{\sqrt{2}}P_{T'R_1R_2\to T''F'}|1\rangle_T|1\rangle_{T'}|\psi^{\rho^1}\rangle_{R_1S_1}|\psi^{\rho^0}\rangle_{R_2S_2}. \tag{B.29}$$

Let us set

$$P^{00}_{R_1R_2\to F'} := \langle 0|_{T''}P_{T'R_1R_2\to T''F'}|0\rangle_{T'}, \tag{B.30}$$

$$P^{11}_{R_1R_2\to F'} := \langle 1|_{T''}P_{T'R_1R_2\to T''F'}|1\rangle_{T'}. \tag{B.31}$$

The verifier finally performs a Bell measurement and accepts if and only if the outcome $\Phi_{T''T}$ occurs. The acceptance probability is then

$$\left\| \langle \Phi |_{TT''} \frac{1}{\sqrt{2}} \left(|0\rangle_T P_{T'R_1R_2 \to T''F'} |0\rangle_{T'} |\psi^{\rho_0}\rangle_{R_1S_1} |\psi^{\rho_1}\rangle_{R_2S_2} + |1\rangle_T P_{T'R_1R_2 \to T''F'} |1\rangle_{T'} |\psi^{\rho_1}\rangle_{R_1S_1} |\psi^{\rho_0}\rangle_{R_2S_2} \right) \right\|_2^2$$

$$= \frac{1}{4} \left\| \langle 0 |_{T''} P_{T'R_1R_2 \to T''F'} |0\rangle_{T'} |\psi^{\rho_0}\rangle_{R_1S_1} |\psi^{\rho_1}\rangle_{R_2S_2} + \langle 1 |_{T''} P_{T'R_1R_2 \to T''F'} |1\rangle_{T'} |\psi^{\rho_1}\rangle_{R_1S_1} |\psi^{\rho_0}\rangle_{R_2S_2} \right\|_2^2 \tag{B.32}$$

$$= \frac{1}{4} \left\| P^{00}_{R_1R_2 \to F'} |\psi^{\rho_0}\rangle_{R_1S_1} |\psi^{\rho_1}\rangle_{R_2S_2} + P^{11}_{R_1R_2 \to F'} |\psi^{\rho_1}\rangle_{R_1S_1} |\psi^{\rho_0}\rangle_{R_2S_2} \right\|_2^2 \tag{B.33}$$

$$= \frac{1}{4} \begin{pmatrix} \langle \psi^{\rho_0} |_{R_1S_1} \langle \psi^{\rho_1} |_{R_2S_2} \left(P^{00}_{R_1R_2 \to F'} \right)^\dagger P^{00}_{R_1R_2 \to F'} |\psi^{\rho_0}\rangle_{R_1S_1} |\psi^{\rho_1}\rangle_{R_2S_2} \\ + \langle \psi^{\rho_1} |_{R_1S_2} \langle \psi^{\rho_0} |_{R_2S_1} \left(P^{11}_{R_1R_2 \to F'} \right)^\dagger P^{11}_{R_1R_2 \to F'} |\psi^{\rho_1}\rangle_{R_1S_1} |\psi^{\rho_0}\rangle_{R_2S_2} \\ + \langle \psi^{\rho_0} |_{R_1S_1} \langle \psi^{\rho_1} |_{R_2S_2} \left(P^{00}_{R_1R_2 \to F'} \right)^\dagger P^{11}_{R_1R_2 \to F'} |\psi^{\rho_1}\rangle_{R_1S_1} |\psi^{\rho_0}\rangle_{R_2S_2} \\ + \langle \psi^{\rho_1} |_{R_1S_1} \langle \psi^{\rho_0} |_{R_2S_2} \left(P^{11}_{R_1R_2 \to F'} \right)^\dagger P^{00}_{R_1R_2 \to F'} |\psi^{\rho_0}\rangle_{R_1S_1} |\psi^{\rho_1}\rangle_{R_2S_2} \end{pmatrix} \tag{B.34}$$

$$\leq \frac{1}{4} \left(2 + 2 \operatorname{Re} \left\{ \langle \psi^{\rho_0} |_{R_1S_1} \langle \psi^{\rho_1} |_{R_2S_2} \left(P^{00}_{R_1R_2 \to F'} \right)^\dagger P^{11}_{R_1R_2 \to F'} |\psi^{\rho_1}\rangle_{R_1S_1} |\psi^{\rho_0}\rangle_{R_2S_2} \right\} \right) \tag{B.35}$$

$$\leq \frac{1}{4} \left(2 + 2 \left| \langle \psi^{\rho_0} |_{R_1S_1} \langle \psi^{\rho_1} |_{R_2S_2} \left(P^{00}_{R_1R_2 \to F'} \right)^\dagger P^{11}_{R_1R_2 \to F'} |\psi^{\rho_1}\rangle_{R_1S_1} |\psi^{\rho_0}\rangle_{R_2S_2} \right| \right) \tag{B.36}$$

$$= \frac{1}{2} \left(1 + \left| \langle \psi^{\rho_0} |_{R_1S_1} \langle \psi^{\rho_1} |_{R_2S_2} \left(P^{00}_{R_1R_2 \to F'} \right)^\dagger P^{11}_{R_1R_2 \to F'} |\psi^{\rho_1}\rangle_{R_1S_1} |\psi^{\rho_0}\rangle_{R_2S_2} \right| \right) \tag{B.37}$$

$$\leq \frac{1}{2} \left(1 + \max_{U_{R_1R_2}} \left| \langle \psi^{\rho_0} |_{R_1S_1} \langle \psi^{\rho_1} |_{R_2S_2} U_{R_1R_2} |\psi^{\rho_1}\rangle_{R_1S_1} |\psi^{\rho_0}\rangle_{R_2S_2} \right| \right). \tag{B.38}$$

The steps given above follow for reasons very similar to those given in the proof of Theorem 3.1. Continuing, we find that

$$\text{Eq. (B.38)} = \frac{1}{2} \left(1 + \sqrt{F(\rho^0 \otimes \rho^1, \rho^1 \otimes \rho^0)} \right) \tag{B.39}$$

$$= \frac{1}{2} \left(1 + \sqrt{F(\rho^0, \rho^1) F(\rho^1, \rho^0)} \right) \tag{B.40}$$

$$= \frac{1}{2} \left(1 + F(\rho^0, \rho^1) \right), \tag{B.41}$$

where we used the multiplicativity of the fidelity for tensor-product states to get (B.40) and the symmetric property of fidelity to arrive at (B.41). Thus, we have established (3.25) as an upper bound on the acceptance probability. This upper

bound can be achieved by setting $F' \simeq R_1 R_2$ and

$$P_{T'R_1R_2F\to T''F'} = |0\rangle_{T''}\langle 0|_{T'} \otimes I_{R_1R_2\to F'} \otimes \langle 0|_F \tag{B.42}$$

$$+ |1\rangle_{T''}\langle 1|_{T'} \otimes U_{R_1} \otimes U_{R_2}^\dagger \otimes \langle 0|_F, \tag{B.43}$$

where U_{R_1} is a unitary that achieves the fidelity for $F(\rho^0, \rho^1)$, so that

$$\sqrt{F}(\rho^0, \rho^1) = \langle \psi^{\rho^0}|_{R_1S_1} U_{R_1} |\psi^{\rho^1}\rangle_{R_1S_1}. \tag{B.44}$$

This concludes the proof. ■

B.3 Proof of Theorem 3.3

Proof of Theorem 3.3. After Step 1 of Algorithm 3.8, the global state is

$$|\Phi\rangle_{T'T}|\psi\rangle_{RA}|0\rangle_{E'}. \tag{B.45}$$

After Step 2 of Algorithm 3.8, it is

$$\frac{1}{\sqrt{2}} \sum_{i\in\{0,1\}} |i\rangle_{T'}|i\rangle_T U^i |\psi\rangle_{RA}|0\rangle_{E'}, \tag{B.46}$$

where $U^i \equiv U^i_{AE'\to BE}$ for $i \in \{0, 1\}$. After Step 4 of Algorithm 3.8, it is

$$P\left(\frac{1}{\sqrt{2}} \sum_{i\in\{0,1\}} |i\rangle_{T'}|i\rangle_T U^i |\psi\rangle_{RA}|00\rangle_{E'F}\right), \tag{B.47}$$

where $P \equiv P_{T'EF\to T''F'}$. For a fixed unitary $P_{T'EF\to T''F'}$ of the max-prover and fixed state $|\psi\rangle_{RA}$ of the min-prover, the acceptance probability is then

$$\left\| \langle\Phi|_{T''T} P \left(\frac{1}{\sqrt{2}} \sum_{i\in\{0,1\}} |i\rangle_{T'}|i\rangle_T U^i |\psi\rangle_{RA}|00\rangle_{E'F}\right)\right\|_2^2$$

$$= \frac{1}{2} \left\| \langle\Phi|_{T''T} P \sum_{i\in\{0,1\}} |i\rangle_{T'}|i\rangle_T U^i |\psi\rangle_{RA}|00\rangle_{E'F}\right\|_2^2, \tag{B.48}$$

In a competing-provers quantum interactive proof, the max-prover is trying to maximize the probability that the verifier accepts, while the min-prover is trying

to minimize the acceptance probability. Since the max-prover plays second in this game, the acceptance probability of Algorithm 3.8 is given by

$$\min_{|\psi\rangle_{RA}} \max_{P} \frac{1}{2} \left\| \langle \Phi|_{T''T} P \sum_{i\in\{0,1\}} |ii\rangle_{T'T} U^i |\psi\rangle_{RA} |00\rangle_{E'F} \right\|_2^2 . \tag{B.49}$$

Applying the analysis of Theorem 3.1, it follows that

$$\max_{P} \frac{1}{2} \left\| \langle \Phi|_{T''T} P \sum_{i\in\{0,1\}} |ii\rangle_{T'T} U^i |\psi\rangle_{RA} |00\rangle_{E'F} \right\|_2^2 = \frac{1}{2}\left(1 + \sqrt{F}(\mathcal{N}^0_{A\to B}(\psi_{RA}), \mathcal{N}^1_{A\to B}(\psi_{RA}))\right). \tag{B.50}$$

Thus, after applying the minimization over every input state ψ_{RA}, the claim in (3.62) follows. ■

B.4 Proof of Theorem 3.4

Proof of Theorem 3.4. After Step 2 of Algorithm 3.9, the global state is

$$|\Phi\rangle_{T'T} |\psi\rangle_{RA} |0\rangle_{E'}. \tag{B.51}$$

After Step 3, the global state is

$$\frac{1}{\sqrt{2}} \sum_{i\in\{0,1\}} |i\rangle_{T'} |i\rangle_T U^i_{AE'\to BE} |\psi\rangle_{RA} |0\rangle_{E'}. \tag{B.52}$$

After Step 5, it is

$$\frac{1}{\sqrt{2}} P \sum_{i\in\{0,1\}} |i\rangle_{T'} |i\rangle_T U^i_{AE'\to BE} |\psi\rangle_{RA} |0\rangle_{E'}, \tag{B.53}$$

where $P \equiv P_{T'EF\to T''F'}$. For a fixed state $|\psi\rangle_{RA}$ and unitary $P_{T'EF\to T''F'}$ of the prover, the acceptance probability is

$$\frac{1}{2} \left\| \langle \Phi|_{T''T} P \sum_{i\in\{0,1\}} |i\rangle_{T'} |i\rangle_T U^i_{AE'\to BE} |\psi\rangle_{RA} |0\rangle_{E'} \right\|_2^2 . \tag{B.54}$$

In a QIP algorithm, the prover chooses his actions in order to maximize the acceptance probability, so that the acceptance probability is

$$\frac{1}{2}\sup_{|\psi\rangle_{RA},\, P}\left\|\langle\Phi|_{T''T}P\sum_{i\in\{0,1\}}|i\rangle_{T'}|i\rangle_{T}U^{i}_{AE'\to BE}|\psi\rangle_{RA}|0\rangle_{E'}\right\|_2^2. \tag{B.55}$$

By the same reasoning employed in the proof of Theorem 3.1, we conclude that

$$\frac{1}{2}\sup_{P}\left\|\langle\Phi|_{T''T}P\sum_{i\in\{0,1\}}|i\rangle_{T'}|i\rangle_{T}U^{i}_{AE'\to BE}|\psi\rangle_{RA}|0\rangle_{E'}\right\|_2^2 = \frac{1}{2}\left(1+\sqrt{F}(\mathcal{N}^{0}_{A\to B}(\rho_A),\mathcal{N}^{1}_{A\to B}(\rho_A))\right), \tag{B.56}$$

where ρ_A is the reduced state of ψ_{RA} (i.e., $\mathrm{Tr}_R[\psi_{RA}]=\rho_A$). Now including the optimization over every pure state ψ_{RA}, we conclude the claim in (3.70). ■

B.5 Proof of Theorem 3.5

Proof of Theorem 3.5. After Step 2 of Algorithm 3.10, the global state is

$$\sum_{x\in\mathcal{X}}\sqrt{p(x)}|xx\rangle_{T'T}|\psi^{x}\rangle_{RS}. \tag{B.57}$$

After Step 4, it is

$$P\sum_{x\in\mathcal{X}}\sqrt{p(x)}|xx\rangle_{T'T}|\psi^{x}\rangle_{RS}|0\rangle_{F}, \tag{B.58}$$

where $P\equiv P_{T'RF\to T''F'}$. Then, for a fixed unitary $P_{T'RF\to T''F'}$, the acceptance probability is

$$\left\|\langle\Phi|_{T''T}P\sum_{x\in\mathcal{X}}\sqrt{p(x)}|xx\rangle_{T'T}|\psi^{x}\rangle_{RS}|0\rangle_{F}\right\|_2^2 = \sup_{|\varphi\rangle_{F'S}}\left|\langle\Phi|_{T''T}\langle\varphi|_{F'S}P\sum_{x\in\mathcal{X}}\sqrt{p(x)}|xx\rangle_{T'T}|\psi^{x}\rangle_{RS}|0\rangle_{F}\right|^2, \tag{B.59}$$

where the optimization is over every pure state $|\varphi\rangle_{F'S}$ and we have used the fact that $\||\phi\rangle\|_2^2 = \sup_{|\psi\rangle:\||\psi\rangle\|_2=1} |\langle\psi|\phi\rangle|^2$. This implies that the acceptance probability is given by

$$\sup_{|\varphi\rangle_{F'S},P} \left| \langle\Phi|_{T''T}\langle\varphi|_{F'S} P \sum_{x\in\mathcal{X}} \sqrt{p(x)}|xx\rangle_{T'T}|\psi^x\rangle_{RS}|0\rangle_F \right|^2 . \tag{B.60}$$

Recall Uhlmann's theorem [Uhl76], which is the statement that

$$F(\omega_C, \tau_C) = \sup_{V_B} |\langle\varphi^\tau|_{BC} V_B \otimes I_C |\varphi^\omega\rangle_{BC}|^2 , \tag{B.61}$$

where ω_C and τ_C are density operators with respective purifications $|\varphi^\omega\rangle_{BC}$ and $|\varphi^\tau\rangle_{BC}$ and the optimization is over every unitary V_B. Observing that the unitary $P_{T'RF\to T''F'}$ acts on systems $T'RF$ of $\sum_{x\in\mathcal{X}} \sqrt{p(x)}|xx\rangle_{T'T}|\psi^x\rangle_{RS}|0\rangle_F$ and systems $T''F'$ of $|\Phi\rangle_{T''T}|\varphi\rangle_{F'S}$, that their respective reduced states on systems TS are

$$\sum_{x\in\mathcal{X}} p(x)|x\rangle\langle x|_T \otimes \rho_S^x, \tag{B.62}$$

$$\pi_T \otimes \sigma_S , \tag{B.63}$$

where π_T is the maximally mixed state and $\sigma_S := \mathrm{Tr}_{F'}[\varphi_{F'S}]$, and applying Uhlmann's theorem, we conclude that the acceptance probability is given by

$$\sup_{\sigma_S} F\left(\sum_{x\in\mathcal{X}} p(x)|x\rangle\langle x|_T \otimes \rho_S^x, \pi_T \otimes \sigma_S \right) \tag{B.64}$$

$$= \left[\sup_{\sigma_S} \sqrt{F}\left(\sum_{x\in\mathcal{X}} p(x)|x\rangle\langle x|_T \otimes \rho_S^x, \pi_T \otimes \sigma_S \right) \right]^2 \tag{B.65}$$

$$= \frac{1}{d}\left[\sup_{\sigma_S} \sum_{x\in\mathcal{X}} \sqrt{p(x)}\,\sqrt{F}(\rho_S^x, \sigma_S) \right]^2 . \tag{B.66}$$

In the second equality, we made use of the direct-sum property of the root fidelity [KW20, Proposition 4.29]. We note here that the analysis employed is the same as that used to show that the CLOSE-IMAGE problem is QIP(2)-complete [HMW14].

We can also write the acceptance probability as

$$\left\| \langle\Phi|_{T''T} P \sum_{x\in\mathcal{X}} \sqrt{p(x)}|xx\rangle_{T'T}|\psi^x\rangle_{RS}|0\rangle_F \right\|_2^2 = \frac{1}{d}\left\| \sum_{x\in\mathcal{X}} \sqrt{p(x)} P^x_{R\to F'}|\psi^x\rangle_{RS} \right\|_2^2 \tag{B.67}$$

where we have defined

$$P^x_{R\to F'} := \langle x|_{T''} P_{T'RF\to T''F'} |x\rangle_{T'} |0\rangle_F. \tag{B.68}$$

The upper bound in (3.79) follows because

$$\begin{aligned}
&\frac{1}{d}\left\| \sum_{x\in\mathcal{X}} \sqrt{p(x)} P^x_{R\to F'} |\psi^x\rangle_{RS} \right\|_2^2 \\
&= \frac{1}{d} \sum_{x,y\in\mathcal{X}} \sqrt{p(x)p(y)} \langle\psi^x|_{RS} (P^x_{R\to F'})^\dagger P^y_{R\to F'} |\psi^y\rangle_{RS} \qquad \text{(B.69)} \\
&= \frac{1}{d} \sum_{x\in\mathcal{X}} p(x) \langle\psi^x|_{RS} (P^x_{R\to F'})^\dagger P^x_{R\to F'} |\psi^x\rangle_{RS} \\
&+ \frac{2}{d} \sum_{\substack{x,y\in\mathcal{X} \\ :x<y}} \sqrt{p(x)p(y)}\, \mathrm{Re}[\langle\psi^x|_{RS} (P^x)^\dagger P^y |\psi^y\rangle_{RS}] \qquad \text{(B.70)} \\
&\leq \frac{1}{d} + \frac{2}{d} \sum_{x,y\in\mathcal{X}:x<y} \sqrt{p(x)p(y)}\, \sqrt{F}(\rho^x_S, \rho^y_S) \qquad \text{(B.71)}
\end{aligned}$$

where the first equality follows by expanding the norm, the second by splitting the terms into those for which $x = y$ and $x < y$, and the inequality follows because $(P^x_{R\to F'})^\dagger P^x_{R\to F'} \leq I_R$ and from reasoning similar to that in the proof of Theorem 3.1.

The final statement about tightness of the upper bound for the case $d = 2$ follows by picking P^x and P^y for $x < y$ to be isometries from Uhlmann's theorem, as was done at the end of the proof of Theorem 3.1. ■

B.6 Proof of Theorem 3.6

Proof of Theorem 3.6. We can employ the result of Theorem 3.5. For a fixed state ψ_{RA} of the min-prover, the acceptance probability is equal to

$$\frac{1}{d}\left[\sup_{\sigma_{RB}} \sum_{x\in\mathcal{X}} \sqrt{p(x)}\, \sqrt{F}(\mathcal{N}^x_{A\to B}(\psi_{RA}), \sigma_{RB}) \right]^2, \tag{B.72}$$

as a consequence of Theorem 3.5. Thus, we arrive at the claim in (3.86) by minimizing over every state ψ_{RA} of the min-prover.

The upper bound in (3.87) follows from the upper bound in (3.79). Indeed, for a fixed state ψ_{RA} of the min-prover, the acceptance probability in (B.72) is bounded from above by

$$\frac{1}{d} + \frac{2}{d} \sum_{\substack{x,y \in \mathcal{X}: \\ x<y}} \sqrt{p(x)p(y)}\, \sqrt{F}(\mathcal{N}^x_{A\to B}(\psi_{RA}), \mathcal{N}^y_{A\to B}(\psi_{RA})). \tag{B.73}$$

After taking infima, we arrive at (3.87).

The final statement follows from the same reasoning employed at the end of the proof of Theorem 3.5. ■

B.7 Number of samples for Fidelity-Pure-Pure

In Theorem 3.8, we argued that the problem Fidelity-Pure-Pure is BQP-complete; i.e., every problem in BQP can be reduced to this problem in polynomial time. In this section, we discuss the number of samples required to obtain a desired accuracy and confidence. Let us first recall Hoeffding's bound.

Lemma B.1 [*Hoeffding's Bound* [Hoe63]]. *Suppose that we are given n independent samples $Y_1, \ldots, Y_n$ of a bounded random variable Y taking values in the interval $[a, b]$ and having mean μ. Set*

$$\overline{Y_n} := \frac{1}{n}(Y_1 + \ldots + Y_n) \tag{B.74}$$

to be the sample mean. Let $\varepsilon \in (0, 1)$ be the desired accuracy, and let $1 - \delta$ be the desired success probability, where $\delta \in (0, 1)$. Then

$$\Pr[|\overline{Y_n} - \mu| \leq \varepsilon] \geq 1 - \delta, \tag{B.75}$$

as long as

$$n \geq \frac{M^2}{2\varepsilon^2} \ln\left(\frac{2}{\delta}\right), \tag{B.76}$$

where $M := b - a$.

In the main text, we mapped a general BQP algorithm to Fidelity-Pure-Pure. In a general BQP algorithm, we measure a single qubit called the decision qubit, leading to a random variable Y taking the value 0 with probability $1 - p$ and the value 1 with probability p, where p is the acceptance probability of the algorithm.

We repeat this procedure n times and label the outcomes $Y_1, \ldots, Y_n$. We output the mean

$$\overline{Y_n} = \frac{1}{n}(Y_1 + \ldots + Y_n) \tag{B.77}$$

as an estimate for the true value p (as seen in (3.131))

$$p = \langle x|_S \langle 0|_A Q^\dagger (|1\rangle\langle 1|_D \otimes I_G) Q |x\rangle_S |0\rangle_A . \tag{B.78}$$

By plugging into Lemma B.1, setting

$$\mu = p \tag{B.79}$$

therein, and taking n to satisfy the condition $n \geq \frac{1}{2\varepsilon^2} \ln\left(\frac{2}{\delta}\right)$, we can achieve an error ε and confidence δ (as defined in (B.75)).

Now, we see from (3.134) that the modified algorithm has an acceptance probability p^2, i.e., equal to the square of the original BQP problem's acceptance probability. In the modified algorithm, we measure the decision qubit, leading to a random variable Z taking value 0 with probability $1 - p^2$ and the value 1 with probability p^2. We repeat the procedure m times and label the outcomes $Z_1, \ldots, Z_m$. We output the mean

$$\overline{Z}_m = \frac{1}{m}(Z_1 + \ldots + Z_m) \tag{B.80}$$

as an estimate for the true value p^2 (as seen in (3.134)). Setting $\tilde{\mu} = p^2$, and plugging into Lemma B.1, it follows that

$$\Pr[|\overline{Z}_m - \tilde{\mu}| \leq \varepsilon^2] \geq 1 - \delta, \tag{B.81}$$

if

$$m \geq \frac{1}{2\varepsilon^4} \ln\left(\frac{2}{\delta}\right). \tag{B.82}$$

Consider the following inequalities:

$$\begin{aligned}
\varepsilon^2 &\geq \left|\overline{Z}_m - \tilde{\mu}\right| \\
&= \left|\overline{Z}_m - \mu^2\right| \\
&= \left|\sqrt{\overline{Z}_m} - \mu\right| \left|\sqrt{\overline{Z}_m} + \mu\right| \\
&\geq \left|\sqrt{\overline{Z}_m} - \mu\right|^2 ,
\end{aligned} \tag{B.83}$$

where the second inequality is derived from the fact that $\overline{Z}_m, \mu \in [0,1]$, so that $\left|\overline{Z}_m + \mu\right| \geq \left|\overline{Z}_m - \mu\right|$. Thus,

$$\left|\sqrt{\overline{Z}_m} - \mu\right| \leq \varepsilon. \tag{B.84}$$

In other words,

$$\varepsilon^2 \geq \left|\overline{Z}_m - \mu^2\right| \implies \varepsilon \geq \left|\sqrt{\overline{Z}_m} - \mu\right| \tag{B.85}$$

so that

$$\begin{aligned} \Pr\left[\left|\sqrt{\overline{Z}_m} - \mu\right| \leq \varepsilon\right] &\geq \Pr[\left|\overline{Z}_m - \mu^2\right| \leq \varepsilon^2] \\ &\geq 1 - \delta. \end{aligned} \tag{B.86}$$

Thus, $\sqrt{\overline{Z}_m}$ is an estimator for p and taking

$$m \geq \frac{1}{2\varepsilon^4} \ln\left(\frac{2}{\delta}\right) \tag{B.87}$$

suffices to achieve an error ε and confidence δ in estimating p.

Appendix C

Supplementary material of Chapter 4

C.1 Proof of Theorem 4.1

We give the proof for completeness, and we note here that it is very close to the proof of [CKMR07, Lemma II.5] (see also [KW20, Lemma 3.6]).

We begin with the forward implication. Suppose that ρ_S is G-symmetric extendible. By definition, this means that there exists a state ω_{RS} satisfying (4.5) and (4.6). Suppose that ω_{RS} has the following spectral decomposition:

$$\omega_{RS} = \sum_k \lambda_k \Pi^k_{RS}, \tag{C.1}$$

where λ_k is an eigenvalue and Π^k_{RS} is a spectral projection. We can write Π^k_{RS} as

$$\Pi^k_{RS} = \sum_\ell |\phi^k_\ell\rangle\langle\phi^k_\ell|_{RS}, \tag{C.2}$$

where $\{|\phi^k_\ell\rangle_{RS}\}_\ell$ is an orthonormal basis. Now define

$$|\Gamma^k\rangle_{RS\hat{R}\hat{S}} := \sum_\ell |\phi^k_\ell\rangle_{RS} \otimes \overline{|\phi^k_\ell\rangle}_{\hat{R}\hat{S}}, \tag{C.3}$$

$$|\psi^\rho\rangle_{RS\hat{R}\hat{S}} := \sum_k \sqrt{\lambda_k}|\Gamma^k\rangle_{RS\hat{R}\hat{S}}, \tag{C.4}$$

where $\overline{|\phi_\ell^k\rangle}_{\hat{R}\hat{S}}$ is the complex conjugate of $|\phi_\ell^k\rangle_{RS}$ with respect to the standard basis. Observe that $|\psi^\rho\rangle\langle\psi^\rho|_{RS\hat{R}\hat{S}}$ is a purification of ω_{RS}. Now let us establish (4.20). Given that ω_{RS} satisfies (4.6), it follows that

$$U_{RS}(g)^\dagger \omega_{RS} U_{RS}(g)|\phi_\ell^k\rangle_{RS} = \omega_{RS}|\phi_\ell^k\rangle_{RS} \tag{C.5}$$

$$= \lambda_k|\phi_\ell^k\rangle_{RS}, \tag{C.6}$$

for all k, ℓ, and g. Left multiplying by $U_{RS}(g)$ implies that

$$\omega_{RS} U_{RS}(g)|\phi_\ell^k\rangle_{RS} = \lambda_k U_{RS}(g)|\phi_\ell^k\rangle_{RS}, \tag{C.7}$$

so that $U_{RS}(g)|\phi_\ell^k\rangle_{RS}$ is an eigenvector of ω_{RS} with eigenvalue λ_k. We conclude that the kth eigenspace corresponding to eigenvalue λ_k is invariant under the action of $U_{RS}(g)$ because $|\phi_\ell^k\rangle_{RS}$ and $U_{RS}(g)|\phi_\ell^k\rangle_{RS}$ are eigenvectors of ω_{RS} with eigenvalue λ_k. This implies that the restriction of $U_{RS}(g)$ to the kth eigenspace is equivalent to a unitary $U_{RS}^k(g)$. Then it follows that

$$(U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g))|\Gamma^k\rangle_{RS\hat{R}\hat{S}}$$

$$= (U_{RS}^k(g) \otimes \overline{U}_{\hat{R}\hat{S}}^k(g))|\Gamma^k\rangle_{RS\hat{R}\hat{S}} \tag{C.8}$$

$$= |\Gamma^k\rangle_{RS\hat{R}\hat{S}}, \tag{C.9}$$

for all $g \in G$. The first equality follows from the fact stated just above. The second equality follows from the invariance of the maximally entangled vector $|\Gamma^k\rangle_{RS\hat{R}\hat{S}}$ under unitaries of the form $V \otimes \overline{V}$. Thus, it follows by linearity that

$$|\psi^\rho\rangle_{RS\hat{R}\hat{S}} = (U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g))|\psi^\rho\rangle_{RS\hat{R}\hat{S}}, \tag{C.10}$$

for all $g \in G$, which is the statement of (4.20).

Let us now consider the opposite implication. Suppose that $\psi^\rho_{RS\hat{R}\hat{S}}$ is a purification of ρ_S and $\psi^\rho_{RS\hat{R}\hat{S}}$ satisfies (4.20). Set

$$\omega_{RS} = \mathrm{Tr}_{\hat{R}\hat{S}}[\psi^\rho_{RS\hat{R}\hat{S}}]. \tag{C.11}$$

Then ω_{RS} is an extension of ρ_S. Furthermore, employing the shorthand $U_{RS} \equiv$

$U_{RS}(g)$ and $\overline{U}_{\hat{R}\hat{S}} \equiv \overline{U}_{\hat{R}\hat{S}}(g)$, we find that $\omega_{RS} = U_{RS}(g)\omega_{RS}U_{RS}(g)^\dagger$ for all $g \in G$ because

$$\begin{aligned}
&\omega_{RS} \\
&= \mathrm{Tr}_{\hat{R}\hat{S}}[\psi^{\rho}_{RS\hat{R}\hat{S}}] && \text{(C.12)}\\
&= \mathrm{Tr}_{\hat{R}\hat{S}}[(U_{RS}\otimes\overline{U}_{\hat{R}\hat{S}})\psi^{\rho}_{RS\hat{R}\hat{S}}(U_{RS}\otimes\overline{U}_{\hat{R}\hat{S}})^\dagger] && \text{(C.13)}\\
&= U_{RS}(g)\,\mathrm{Tr}_{\hat{R}\hat{S}}[\overline{U}_{\hat{R}\hat{S}}(g)\psi^{\rho}_{RS\hat{R}\hat{S}}\overline{U}_{\hat{R}\hat{S}}(g)^\dagger]U_{RS}(g)^\dagger && \text{(C.14)}\\
&= U_{RS}(g)\,\mathrm{Tr}_{\hat{R}\hat{S}}[\overline{U}_{\hat{R}\hat{S}}(g)^\dagger\overline{U}_{\hat{R}\hat{S}}(g)\psi^{\rho}_{RS\hat{R}\hat{S}}]U_{RS}(g)^\dagger && \text{(C.15)}\\
&= U_{RS}(g)\,\mathrm{Tr}_{\hat{R}\hat{S}}[\psi^{\rho}_{RS\hat{R}\hat{S}}]U_{RS}(g)^\dagger && \text{(C.16)}\\
&= U_{RS}(g)\omega_{RS}U_{RS}(g)^\dagger. && \text{(C.17)}
\end{aligned}$$

Thus, it follows that ρ_S is G-symmetric extendible.

We now justify the equivalence of (4.20) and (4.21). Using the result in (C.10), observe that

$$|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}} = \frac{1}{|G|}\sum_{g\in G}(U_{RS}(g)\otimes\overline{U}_{\hat{R}\hat{S}}(g))|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}}, \tag{C.18}$$

which simplifies to (4.21) by substituting in (4.22). Now starting with (4.22), let us apply the property in (4.10), and we have that

$$|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}} = (U_{RS}(g)\otimes\overline{U}_{\hat{R}\hat{S}}(g))\Pi^{G}_{RS\hat{R}\hat{S}}|\psi^{\rho}\rangle_{RS\hat{R}\hat{S}}, \tag{C.19}$$

for all $g \in G$. This reduces to (4.20) by applying (4.21).

C.2 Proof of Theorem 4.2

Let ψ_{RS} be an arbitrary purification of ρ_S, and consider that

$$\begin{aligned}
\mathrm{Tr}[\Pi^{G}_{S}\rho_S] &= \mathrm{Tr}[(\mathbb{I}_R\otimes\Pi^{G}_{S})\psi_{RS}] && \text{(C.20)}\\
&= \left\|\left(\mathbb{I}_R\otimes\Pi^{G}_{S}\right)|\psi\rangle_{RS}\right\|_2^2. && \text{(C.21)}
\end{aligned}$$

Recall the following property of the norm of an arbitrary vector $|\varphi\rangle$:

$$\||\varphi\rangle\|_2^2 = \max_{|\phi\rangle:\||\phi\rangle\|_2=1}|\langle\phi|\varphi\rangle|^2. \tag{C.22}$$

This follows from the Cauchy–Schwarz inequality and the conditions for saturating it. This implies that

$$\left\|\left(\mathbb{I}_R \otimes \Pi_S^G\right)|\psi\rangle_{RS}\right\|_2^2 = \max_{|\phi\rangle:\||\phi\rangle\|_2=1} \left|\langle\phi|_{RS}\left(\mathbb{I}_R \otimes \Pi_S^G\right)|\psi\rangle_{RS}\right|^2 \tag{C.23}$$

Let us also recall Uhlmann's theorem [Uhl76]: For positive semi-definite operators ω_A and τ_A and corresponding rank-one operators ψ_{RA}^{ω} and ψ_{RA}^{τ} satisfying

$$\mathrm{Tr}_R[\psi_{RA}^{\omega}] = \omega_A, \tag{C.24}$$
$$\mathrm{Tr}_R[\psi_{RA}^{\tau}] = \tau_A, \tag{C.25}$$

Uhlmann's theorem [Uhl76] states that

$$F(\omega_A, \tau_A) = \left\| \sqrt{\omega_A}\sqrt{\tau_A}\right\|_1^2 \tag{C.26}$$
$$= \max_{V_R} \left|\langle\psi^{\omega}|_{RA}\left(V_R \otimes \mathbb{I}_A\right)|\psi^{\tau}\rangle_{RA}\right|^2, \tag{C.27}$$

where the optimization is over every unitary V_R acting on the reference system R. We also implicitly defined fidelity more generally for positive semi-definite operators. Considering that

$$\rho_S = \mathrm{Tr}_R[\psi_{RS}], \qquad \sigma_S := \mathrm{Tr}_R[\phi_{RS}], \tag{C.28}$$

so that

$$\Pi_S^G \sigma_S \Pi_S^G = \mathrm{Tr}_R[\Pi_S^G \phi_{RS} \Pi_S^G], \tag{C.29}$$

we conclude that

$$\max_{|\phi\rangle:\||\phi\rangle\|_2=1} \left|\langle\phi|_{RS}\left(\mathbb{I}_R \otimes \Pi_S^G\right)|\psi\rangle_{RS}\right|^2$$
$$= \max_{|\phi\rangle:\||\phi\rangle\|_2=1} \max_{U_R} \left|\langle\phi|_{RS}\left(U_R \otimes \Pi_S^G\right)|\psi\rangle_{RS}\right|^2 \tag{C.30}$$
$$= \max_{\sigma_S \in \mathcal{D}(\mathcal{H}_S)} F(\rho_S, \Pi_S^G \sigma_S \Pi_S^G). \tag{C.31}$$

where the last equality follows from Uhlmann's theorem with the identifications $|\psi^{\omega}\rangle \leftrightarrow (\mathbb{I} \otimes \Pi^G)|\phi\rangle$ and $|\psi^{\tau}\rangle \leftrightarrow |\psi\rangle$. Clearly, we have that

$$\max_{\sigma_S \in \mathcal{D}(\mathcal{H}_S)} F(\rho_S, \Pi_S^G \sigma_S \Pi_S^G)$$
$$\geq \max_{\sigma \in \text{B-Sym}_G} F(\rho_S, \Pi_S^G \sigma_S \Pi_S^G) \tag{C.32}$$
$$= \max_{\sigma \in \text{B-Sym}_G} F(\rho_S, \sigma_S), \tag{C.33}$$

because B-Sym$_G \subset \mathcal{D}(\mathcal{H})$. Now let us consider showing the opposite inequality. Let $\sigma \in \mathcal{D}(\mathcal{H})$. If $\Pi^G \sigma \Pi^G = 0$, then this is a suboptimal choice as it follows that the objective function $F(\rho_S, \Pi^G_S \sigma_S \Pi^G_S) = 0$ in this case. So, let us suppose this is not the case. Then define

$$\sigma' := \frac{1}{p} \Pi^G \sigma \Pi^G, \tag{C.34}$$

$$p := \operatorname{Tr}[\Pi^G \sigma], \tag{C.35}$$

and observe that $\sigma'_S \in$B-Sym$_G$. Consider that

$$F(\rho_S, \Pi^G_S \sigma_S \Pi^G_S) = pF(\rho_S, \sigma'_S) \tag{C.36}$$

$$\leq F(\rho_S, \sigma'_S) \tag{C.37}$$

$$\leq \max_{\sigma_S \in \text{B-Sym}_G} F(\rho_S, \sigma_S). \tag{C.38}$$

We have thus proved the opposite inequality, concluding the proof.

C.3 Proof of Theorem 4.3

The formula in (C.22) implies that

$$\max_{V_{S'E\to\hat{S}E'}} \left\| \Pi^G_{S\hat{S}} V_{S'E\to\hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2 = \max_{\substack{V_{S'E\to\hat{S}E'}, \\ |\phi\rangle_{S\hat{S}E'}}} \left| \langle\phi|_{S\hat{S}E'} \Pi^G_{S\hat{S}} V_{S'E\to\hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E \right|^2. \tag{C.39}$$

Applying Uhlmann's theorem (see (C.24)–(C.27)) to (C.39) with the identifications $R \leftrightarrow \hat{S}E' \simeq S'E$ and $S \leftrightarrow A$ and noting that

$$\operatorname{Tr}_{S'E}[|\psi\rangle\langle\psi|_{S'S} \otimes |0\rangle\langle 0|_E] = \rho_S, \tag{C.40}$$

$$\operatorname{Tr}_{\hat{S}E'}[\Pi^G_{S\hat{S}} |\phi\rangle\langle\phi|_{S\hat{S}E'} \Pi^G_{S\hat{S}}] = \operatorname{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}}], \tag{C.41}$$

where $\sigma_{S\hat{S}'}$ is a quantum state satisfying $\sigma_{S\hat{S}'} = \operatorname{Tr}_{E'}[|\phi\rangle\langle\phi|_{S\hat{S}E'}]$, we conclude that

$$\max_{\substack{V_{S'E\to\hat{S}E'}, \\ |\phi\rangle_{S\hat{S}E'}}} \left| \langle\phi|_{S\hat{S}E'} \Pi^G_{S\hat{S}} V_{S'E\to\hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E \right|^2 = \max_{\sigma_{S\hat{S}'}} F(\rho_S, \operatorname{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}}]), \tag{C.42}$$

with the optimization in the last line over every quantum state $\sigma_{S\hat{S}'}$.

We finally prove that

$$\max_{\sigma_{S\hat{S}'}} F(\rho_S, \mathrm{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}}]) = \max_{\sigma_S \in \mathrm{Sym}_G} F(\rho_S, \sigma_S). \tag{C.43}$$

To justify the inequality $\geq$ in (C.43), let $\sigma_S \in \mathrm{Sym}_G$, and pick $\sigma_{S\hat{S}}$ to be the purification $\varphi_{S\hat{S}}$ of σ_S from Theorem 4.1 (with trivial reference systems $R\hat{R}$) that satisfies

$$\Pi^G_{S\hat{S}} \varphi_{S\hat{S}} \Pi^G_{S\hat{S}} = \varphi_{S\hat{S}}. \tag{C.44}$$

Then we find that

$$\mathrm{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}} \varphi_{S\hat{S}} \Pi^G_{S\hat{S}}] = \mathrm{Tr}_{\hat{S}}[\varphi_{S\hat{S}}] = \sigma_S, \tag{C.45}$$

and so, given that $\sigma_S \in \mathrm{Sym}_G$ is arbitrary, it follows that

$$\max_{\sigma_{S\hat{S}'}} F(\rho_S, \mathrm{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}}]) \geq \max_{\sigma_S \in \mathrm{Sym}_G} F(\rho_S, \sigma_S). \tag{C.46}$$

To justify the inequality $\leq$ in (C.43), let $\sigma_{S\hat{S}}$ be an arbitrary state. If $\sigma_{S\hat{S}'}$ is outside of the subspace onto which $\Pi^G_{S\hat{S}}$ projects, then $\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}} = 0$ and the fidelity in (C.42) is equal to zero. Let us then suppose that this is not the case, and let us define

$$\sigma'_{S\hat{S}} := \frac{1}{p} \Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}}, \tag{C.47}$$

$$p := \mathrm{Tr}[\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'}]. \tag{C.48}$$

Then we find that

$$F(\rho_S, \mathrm{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}} \sigma_{S\hat{S}'} \Pi^G_{S\hat{S}}]) = pF(\rho_S, \tau_S) \tag{C.49}$$

$$\leq F(\rho_S, \tau_S), \tag{C.50}$$

where

$$\tau_S := \mathrm{Tr}_{\hat{S}}[\sigma'_{S\hat{S}}], \tag{C.51}$$

and we used the fact that $p \leq 1$. It remains to be proven that $\tau_S \in \mathrm{Sym}_G$. To see

this, consider that

$$\begin{aligned}
\tau_S &= \operatorname{Tr}_{\hat{S}}[\sigma'_{S\hat{S}}] && \text{(C.52)}\\
&= \operatorname{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}}\sigma'_{S\hat{S}}\Pi^G_{S\hat{S}}] && \text{(C.53)}\\
&= \operatorname{Tr}_{\hat{S}}[\left(U_S \otimes \overline{U}_{\hat{S}}\right)\Pi^G_{S\hat{S}}\sigma'_{S\hat{S}}\Pi^G_{S\hat{S}}\left(U_S \otimes \overline{U}_{\hat{S}}\right)^\dagger] && \text{(C.54)}\\
&= U_S \operatorname{Tr}_{\hat{S}}[\overline{U}_{\hat{S}}\Pi^G_{S\hat{S}}\sigma'_{S\hat{S}}\Pi^G_{S\hat{S}}\overline{U}^\dagger_{\hat{S}}]U_S^\dagger && \text{(C.55)}\\
&= U_S \operatorname{Tr}_{\hat{S}}[\overline{U}^\dagger_{\hat{S}}\overline{U}_{\hat{S}}\Pi^G_{S\hat{S}}\sigma'_{S\hat{S}}\Pi^G_{S\hat{S}}]U_S^\dagger && \text{(C.56)}\\
&= U_S \operatorname{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}}\sigma'_{S\hat{S}}\Pi^G_{S\hat{S}}]U_S^\dagger && \text{(C.57)}\\
&= U_S(g) \operatorname{Tr}_{\hat{S}}[\sigma'_{S\hat{S}}]U_S^\dagger(g) && \text{(C.58)}\\
&= U_S(g)\tau_S U_S^\dagger(g). && \text{(C.59)}
\end{aligned}$$

where we have used the shorthand $U_S \equiv U_S(g)$ and $\overline{U}_{\hat{S}} \equiv \overline{U}_{\hat{S}}(g)$. Since the equality $\tau_S = U_S(g)\tau_S U_S^\dagger(g)$ holds for all $g \in G$, it follows that

$$\max_{\sigma_{S\hat{S}'}} F(\rho_S, \operatorname{Tr}_{\hat{S}}[\Pi^G_{S\hat{S}}\sigma_{S\hat{S}'}\Pi^G_{S\hat{S}}]) \leq \max_{\tau_S \in \operatorname{Sym}_G} F(\rho_S, \sigma_S), \tag{C.60}$$

concluding the proof.

C.4 Proof of Theorem 4.4

Following the same reasoning given in (C.39)–(C.42), by using Uhlmann's theorem, we conclude that

$$\max_{V_{S'E\to RE'}} \left\|\Pi^G_{RS} V_{S'E\to RE'}|\psi\rangle_{S'S}|0\rangle_E\right\|_2^2 = \max_{\sigma_{RS}} F(\rho_S, \operatorname{Tr}_R[\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS}]), \tag{C.61}$$

where the optimization is over every state σ_{RS} and Π^G_{RS} is defined in (4.69). The next part of the proof shows that

$$\max_{\sigma_{RS}} F(\rho_S, \operatorname{Tr}_R[\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS}]) = \max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S) \tag{C.62}$$

and is similar to (C.43)–(C.60). To justify the inequality $\geq$, let σ_S be an arbitrary state in BSE_G. Then by Definition 4.4, this means that there exists a state ω_{RS} such

that $\mathrm{Tr}_R[\omega_{RS}] = \sigma_S$ and $\Pi^G_{RS}\omega_{RS}\Pi^G_{RS} = \omega_{RS}$. We find that

$$\begin{aligned} F(\rho_S, \sigma_S) &= F(\rho_S, \mathrm{Tr}_R[\omega_{RS}]) && \text{(C.63)} \\ &= F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS}\omega_{RS}\Pi^G_{RS}]) && \text{(C.64)} \\ &\leq \max_{\sigma_{RS}} F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS}]), && \text{(C.65)} \end{aligned}$$

which implies that

$$\max_{\sigma_{RS}} F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS}]) \geq \max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S). \tag{C.66}$$

To justify the inequality $\leq$, let σ_{RS} be an arbitrary state. If $\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS} = 0$, then the desired inequality trivially follows. Supposing then that this is not the case, let us define

$$\begin{aligned} \sigma'_{RS} &:= \frac{1}{p}\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS}, && \text{(C.67)} \\ p &:= \mathrm{Tr}[\Pi^G_{RS}\sigma_{RS}]. && \text{(C.68)} \end{aligned}$$

We then find that

$$\begin{aligned} &F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS}]) \\ &= pF(\rho_S, \mathrm{Tr}_R[\sigma'_{RS}]) && \text{(C.69)} \\ &\leq F(\rho_S, \mathrm{Tr}_R[\sigma'_{RS}]). && \text{(C.70)} \end{aligned}$$

Consider that $\sigma'_S := \mathrm{Tr}_R[\sigma'_{RS}]$ is G-Bose symmetric extendible because σ'_{RS} is an extension of it that satisfies $\Pi^G_{RS}\sigma'_{RS}\Pi^G_{RS} = \sigma'_{RS}$. We conclude that

$$F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS}]) \leq \max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S). \tag{C.71}$$

Since this inequality holds for every state σ_{RS}, we surmise the desired result

$$\max_{\sigma_{RS}} F(\rho_S, \mathrm{Tr}_R[\Pi^G_{RS}\sigma_{RS}\Pi^G_{RS}]) \leq \max_{\sigma_S \in \mathrm{BSE}_G} F(\rho_S, \sigma_S). \tag{C.72}$$

C.5 Proof of Theorem 4.5

Following the same reasoning given in (C.39)–(C.42), by using Uhlmann's theorem, we conclude that

$$\max_{V_{S'E\to R\hat{R}\hat{S}E'}} \left\| \Pi^G_{RS\hat{R}\hat{S}} V_{S'E\to R\hat{R}\hat{S}E'} |\psi\rangle_{S'S} |0\rangle_E \right\|_2^2 = \max_{\sigma_{R\hat{R}S\hat{S}}} F(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]), \tag{C.73}$$

where the optimization is over every state $\sigma_{RS\hat{R}\hat{S}}$ and $\Pi^G_{RS\hat{R}\hat{S}}$ is defined in (4.22). The next part of the proof shows that

$$\max_{\sigma_{R\hat{R}S\hat{S}}} F(\rho_S, \operatorname{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]) = \max_{\sigma_S \in \operatorname{SymExt}_G} F(\rho_S, \sigma_S) \tag{C.74}$$

and is similar to (C.43)–(C.60). To justify the inequality $\geq$, let σ_S be a state in SymExt_G. Then by Theorem 4.1, there exists a purification $\varphi_{RS\hat{R}\hat{S}}$ of σ_S satisfying $\varphi_{RS\hat{R}\hat{S}} = \Pi^G_{RS\hat{R}\hat{S}}\varphi_{RS\hat{R}\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}$. We find that

$$\begin{aligned}
&F(\rho_S, \sigma_S) \\
&= F(\rho_S, \operatorname{Tr}_{R\hat{R}\hat{S}}[\varphi_{RS\hat{R}\hat{S}}]) && \text{(C.75)}\\
&= F(\rho_S, \operatorname{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\varphi_{RS\hat{R}\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]) && \text{(C.76)}\\
&\leq \max_{\sigma_{R\hat{R}S\hat{S}}} F(\rho_S, \operatorname{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]). && \text{(C.77)}
\end{aligned}$$

Since the inequality holds for all $\sigma_S \in \operatorname{SymExt}_G$, we conclude that

$$\max_{\sigma_S \in \operatorname{SymExt}_G} F(\rho_S, \sigma_S) \leq \max_{\sigma_{R\hat{R}S\hat{S}}} F(\rho_S, \operatorname{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]). \tag{C.78}$$

To justify the inequality $\leq$, let $\sigma_{R\hat{R}S\hat{S}}$ be an arbitrary state. If $\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^G_{RS\hat{R}\hat{S}} = 0$, then the desired inequality follows trivially. Supposing this is not the case, then define

$$\sigma'_{R\hat{R}S\hat{S}} := \frac{1}{p}\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}, \tag{C.79}$$

$$p := \operatorname{Tr}[\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}]. \tag{C.80}$$

Then we find that

$$\begin{aligned}
&F(\rho_S, \operatorname{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]) \\
&= pF(\rho_S, \operatorname{Tr}_{R\hat{R}\hat{S}}[\sigma'_{R\hat{R}S\hat{S}}]) && \text{(C.81)}\\
&\leq F(\rho_S, \operatorname{Tr}_{R\hat{R}\hat{S}}[\sigma'_{R\hat{R}S\hat{S}}]) && \text{(C.82)}\\
&= F(\rho_S, \tau_S), && \text{(C.83)}
\end{aligned}$$

where $\tau_S := \operatorname{Tr}_{R\hat{R}\hat{S}}[\sigma'_{R\hat{R}S\hat{S}}]$. We now aim to show that $\tau_S \in \operatorname{SymExt}_G$. To do so, it suffices to prove that $\sigma'_{RS} = U_{RS}(g)\sigma'_{RS}U_{RS}(g)^\dagger$ for all $g \in G$. Abbreviating $U \otimes \overline{U} \equiv$

$U_{RS}(g) \otimes \overline{U}_{\hat{R}\hat{S}}(g)$, consider that

$$
\begin{aligned}
&\sigma'_{RS} \\
&= \mathrm{Tr}_{\hat{R}\hat{S}}[\sigma'_{RS\hat{R}\hat{S}}] && \text{(C.84)}\\
&= \mathrm{Tr}_{\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\sigma'_{RS\hat{R}\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}] && \text{(C.85)}\\
&= \mathrm{Tr}_{\hat{R}\hat{S}}[(U\otimes\overline{U})\Pi^G_{RS\hat{R}\hat{S}}\sigma'_{RS\hat{R}\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}(U\otimes\overline{U})^\dagger] && \text{(C.86)}\\
&= U\,\mathrm{Tr}_{\hat{R}\hat{S}}[\overline{U}\Pi^G_{RS\hat{R}\hat{S}}\sigma'_{RS\hat{R}\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}\overline{U}^\dagger]U^\dagger && \text{(C.87)}\\
&= U\,\mathrm{Tr}_{\hat{R}\hat{S}}[\overline{U}^\dagger\overline{U}\Pi^G_{RS\hat{R}\hat{S}}\sigma'_{RS\hat{R}\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]U^\dagger && \text{(C.88)}\\
&= U\,\mathrm{Tr}_{\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\sigma'_{RS\hat{R}\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]U^\dagger && \text{(C.89)}\\
&= U\,\mathrm{Tr}_{\hat{R}\hat{S}}[\sigma'_{RS\hat{R}\hat{S}}]U^\dagger && \text{(C.90)}\\
&= U_{RS}(g)\sigma'_{RS}U_{RS}(g)^\dagger. && \text{(C.91)}
\end{aligned}
$$

It follows that $\tau_S \in \mathrm{SymExt}_G$, and we conclude that

$$F(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]) \leq \max_{\sigma_S\in\mathrm{SymExt}_G} F(\rho_S,\sigma_S). \tag{C.92}$$

Since the inequality holds for every state $\sigma_{R\hat{R}S\hat{S}}$, we conclude that

$$\max_{\sigma_{R\hat{R}S\hat{S}}} F(\rho_S, \mathrm{Tr}_{R\hat{R}\hat{S}}[\Pi^G_{RS\hat{R}\hat{S}}\sigma_{R\hat{R}S\hat{S}}\Pi^G_{RS\hat{R}\hat{S}}]) \leq \max_{\sigma_S\in\mathrm{SymExt}_G} F(\rho_S,\sigma_S). \tag{C.93}$$

C.6 Error and Number of Samples in State-HS-Symmetry

In Theorem 4.7, we proved that the problem State-HS-Symmetry is BQP-Complete. In this section, we discuss the number of samples required to obtain the desired accuracy and confidence. To do this, we invoke Hoeffding's bound from Lemma B.1.

In Section 4.6.2, we mapped a general BQP algorithm to State-HS-Symmetry. In a general BQP algorithm, we measure a single qubit called the decision qubit, leading to a random variable Y taking the value 0 with probability p_{rej} and the value 1 with probability p_{acc}, where p_{acc} is the acceptance probability of the algorithm. We repeat this procedure n times and label the outcomes $Y_1,\ldots,Y_n$. We output the mean

$$\overline{Y_n} = \frac{1}{n}(Y_1 + \cdots + Y_n) \tag{C.94}$$

as an estimate for the true value p_{acc}

$$p_{\text{acc}} = \langle x|_S \langle 0|_A Q^\dagger (|1\rangle\langle 1|_D \otimes I_G) Q |x\rangle_S |0\rangle_A . \tag{C.95}$$

By plugging into Lemma B.1, setting

$$\mu = p_{\text{acc}} \tag{C.96}$$

therein, and taking n to satisfy the condition $n \geq \frac{1}{2\varepsilon^2} \ln\left(\frac{2}{\delta}\right)$, we can achieve an error ε and confidence δ (as defined in (B.75)).

Now, we see from (4.218) that the modified algorithm has an acceptance probability $1 - p_{\text{rej}}^2$, i.e., equal to one minus the square of the original BQP algorithm's rejection probability. In the modified algorithm, we measure the decision qubit, leading to a random variable Z taking value 0 with probability p_{rej}^2 and the value 1 with probability $1 - p_{\text{rej}}^2$. We repeat the procedure m times and label the outcomes $Z_1, \ldots, Z_m$. We output the mean

$$\overline{Z}_m = 1 - \frac{1}{m}(Z_1 + \cdots + Z_m) \tag{C.97}$$

as an estimate for the true value p_{rej}^2. Setting $\tilde{\mu} = p_{\text{rej}}^2$, and plugging into Lemma B.1, it follows that

$$\Pr[|\overline{Z}_m - \tilde{\mu}| \leq \varepsilon^2] \geq 1 - \delta, \tag{C.98}$$

if

$$m \geq \frac{1}{2\varepsilon^4} \ln\left(\frac{2}{\delta}\right). \tag{C.99}$$

Consider the following inequalities:

$$\begin{aligned} \varepsilon^2 &\geq \left|\overline{Z}_m - \tilde{\mu}\right| \\ &= \left|\overline{Z}_m - \mu^2\right| \\ &= \left|\sqrt{\overline{Z}_m} - \mu\right| \left|\sqrt{\overline{Z}_m} + \mu\right| \\ &\geq \left|\sqrt{\overline{Z}_m} - \mu\right|^2 , \end{aligned} \tag{C.100}$$

where the second inequality is derived from the fact that $\overline{Z}_m, \mu \in [0, 1]$, so that $\left|\overline{Z}_m + \mu\right| \geq \left|\overline{Z}_m - \mu\right|$. Thus,

$$\left|\sqrt{\overline{Z}_m} - \mu\right| \leq \varepsilon. \tag{C.101}$$

In other words,

$$\varepsilon^2 \geq \left|\overline{Z}_m - \mu^2\right| \implies \varepsilon \geq \left|\sqrt{\overline{Z}_m} - \mu\right| \tag{C.102}$$

so that

$$\begin{aligned}\Pr\left[\left|\sqrt{\overline{Z}_m} - \mu\right| \leq \varepsilon\right] &\geq \Pr[\left|\overline{Z}_m - \mu^2\right| \leq \varepsilon^2] \\ &\geq 1 - \delta.\end{aligned} \tag{C.103}$$

Thus, $\sqrt{\overline{Z}_m}$ is an estimator for p_{rej} and taking

$$m \geq \frac{1}{2\varepsilon^4} \ln\left(\frac{2}{\delta}\right) \tag{C.104}$$

suffices to achieve an error ε and confidence δ in estimating p_{rej}.

Appendix D

Supplementary material of Chapter 5

D.1 Definitions and Lemmas

In this section, we introduce new notation that we use throughout the paper. We also provide a wide range of lemmas and proofs for the results from the main text.

Lemma D.1. *Let O_i denote the projector onto the computational basis element i:*

$$O_i := |i\rangle\langle i|, \tag{D.1}$$

where the right-hand side is understood to be the binary representation of i. For example, $O_4 = |100\rangle\langle 100|$. Furthermore, define $\tilde{O}_j$ to be the Pauli string composed of I and Z operators such that the bits of j determine if the operator at each position is Z or I. For a concrete example, consider that for $j = 6_{10} = 110_2$, each 1 is represented by Z, and each 0 by I. The operator is then given by

$$\tilde{O}_6 = ZZI. \tag{D.2}$$

Then the following equality holds:

$$O_i = \frac{1}{2^n} \sum_{j=0}^{2^n-1} (-1)^{i \cdot j} \tilde{O}_j, \tag{D.3}$$

where n is the size of the register for O and $\tilde{O}$, and $i \cdot j$ denotes the bit-wise dot-product modulo 2 of the binary representations of i and j.

Proof. Let $a = a_1 a_2 \cdots a_n$. Then

$$\begin{aligned} O_a &= |a\rangle\langle a| \\ &= |a_1\rangle\langle a_1| \otimes \cdots \otimes |a_n\rangle\langle a_n| \\ &= \bigotimes_{i=1}^{n} \frac{I + (-1)^{a_i} Z}{2} \\ &= \frac{1}{2^n} \sum_{c=0}^{2^n-1} (-1)^{a \cdot c} \tilde{O}_c, \end{aligned} \tag{D.4}$$

concluding the proof. ■

Definition D.1 [*Projection Operators*]. *The projector onto a basis element a on qubits f is defined as*

$$\begin{aligned} P_f^a &:= |a\rangle\langle a|_f \\ &= \bigotimes_{i=1} |a_i\rangle\langle a_i|_{f_i}. \end{aligned}$$

We also define a projector onto a subspace labelled by b and $\bar{b}$ on qubits f as follows:

$$P_f^{b,\bar{b}} := \left(|b\rangle\langle b| + |\bar{b}\rangle\langle \bar{b}| \right)_f . \tag{D.5}$$

Definition D.2 [*Distance-k operators*]. *In an n-qubit Gray or binary code (see Sec. 5.3 for definitions), the set of distance-k operators consists of all operators that connect two bitstrings that differ on k bits:*

$$D(n,k) := \{ |a\rangle\langle b| + |b\rangle\langle a| : w(a \oplus b) = k \}, \tag{D.6}$$

where a, b are bitstrings of length n, the variable w denotes the Hamming weight, and $\oplus$ denotes bit-wise addition modulo 2. For a two-qubit Gray code, an example of a distance-1 operator is

$$|01\rangle\langle 11| + |11\rangle\langle 01|. \tag{D.7}$$

We see that the bitstrings 01 and 11 differ in one position. The Hermitian operator above connects the two basis elements. The number of distinct distance-k operators is given by

$$|D(n,k)| = \binom{n}{k} 2^{n-1}. \tag{D.8}$$

To establish this equality, we first pick the k bits that are different, which can be done in $\binom{n}{k}$ ways, the unflipped bits are in one of 2^{n-k} bitstrings, and the flipped bits can be chosen in 2^{k-1} ways since the operators connect two bitstrings with k-bits flipped.

Remark D.1. *The set $D(n,k)$ of distance-k operators can be split into subsets depending on the set of k flipped qubits. For example, consider $n = 3$ and $k = 2$. The set $D(3,2)$ consists of the following operators:*

$$
\begin{aligned}
&|000\rangle\langle 011| + |011\rangle\langle 000|,\\
&|001\rangle\langle 010| + |010\rangle\langle 001|,\\
&|100\rangle\langle 111| + |111\rangle\langle 100|,\\
&|101\rangle\langle 110| + |110\rangle\langle 101|,\\
&|000\rangle\langle 110| + |110\rangle\langle 000|,\\
&|010\rangle\langle 100| + |100\rangle\langle 010|,\\
&|001\rangle\langle 111| + |111\rangle\langle 001|,\\
&|011\rangle\langle 101| + |101\rangle\langle 011|,\\
&|000\rangle\langle 101| + |101\rangle\langle 000|,\\
&|001\rangle\langle 100| + |100\rangle\langle 001|,\\
&|010\rangle\langle 111| + |111\rangle\langle 010|,\\
&|011\rangle\langle 110| + |110\rangle\langle 011|.
\end{aligned}
\tag{D.9}
$$

As seen in Definition D.2, $|D(3,2)| = 12$. We can split up the set of operators into three sets based on which two qubits are flipped – $\{2,3\}$, $\{1,3\}$, $\{1,2\}$. Thus, the operators of $D(3,2)$ are then split as

$$
\begin{aligned}
\{2,3\} = \Big\{&|000\rangle\langle 011| + |011\rangle\langle 000|, |001\rangle\langle 010| + |010\rangle\langle 001|,\\
&|100\rangle\langle 111| + |111\rangle\langle 100|, |101\rangle\langle 110| + |110\rangle\langle 101|.\Big\},\\
\{1,2\} = \Big\{&|000\rangle\langle 110| + |110\rangle\langle 000|, |010\rangle\langle 100| + |100\rangle\langle 010|,\\
&|001\rangle\langle 111| + |111\rangle\langle 001|, |011\rangle\langle 101| + |101\rangle\langle 011|.\Big\},\\
\{1,3\} = \Big\{&|000\rangle\langle 101| + |101\rangle\langle 000|, |001\rangle\langle 100| + |100\rangle\langle 001|,\\
&|010\rangle\langle 111| + |111\rangle\langle 010|, |011\rangle\langle 110| + |110\rangle\langle 011|.\Big\}.
\end{aligned}
\tag{D.10}
$$

Since $k = 2$, each of the above operators can be thought of as two-qubit flips in a particular subspace. For example, $|000\rangle\langle 011| + |011\rangle\langle 000|$ acts like IXX in the subspace spanned by $\{|000\rangle, |011\rangle\}$ since its action on any state in this subspace is the same as the action of IXX. This is a unifying feature—any distance-ℓ operator can be thought of as a product of I (on the unchanged qubits) and X (on the ℓ flipped qubits) acting on a particular subspace. Thus, an alternate way to represent the distance operators is as a composition of a projection onto the subspace of interest, followed by a string consisting of X and I. For example,

$$\begin{aligned} |000\rangle\langle 011| + |011\rangle\langle 000| &= (IXX) \circ (P^0_{\{1\}} \otimes P^{00,11}_{\{2,3\}}), \\ |001\rangle\langle 010| + |010\rangle\langle 001| &= (IXX) \circ (P^0_{\{1\}} \otimes P^{01,10}_{\{2,3\}}), \end{aligned} \tag{D.11}$$

and the remaining operators can be constructed similarly.

Definition D.3. *In Remark D.1, we saw that $D(n,k)$ can be split into subsets depending on the set of k flipped qubits. We label these subsets with a set f of flipped qubits of size k. Furthermore, we saw that the distance-k operators can be written as a composition of a projector onto a particular subspace and a Pauli string consisting of X and I. Thus, we define the following sets of distance-k operators for a fixed set of k flipped qubits labelled by f:*

$$D(n,k,f) := \left\{ \left(I_{\bar{f}} \otimes X_f\right) P^a_{\bar{f}} \otimes P^{b,\bar{b}}_f : \forall a \in \{0,1\}^{|\bar{f}|},\ \forall b \in \{0,1\}^{|f|} \right\}, \tag{D.12}$$

where $P^a_{\bar{f}}$ and $P^{b,\bar{b}}_f$ are defined in Definition D.1.

For example, $D(3,2,\{2,3\})$ is the set consisting of the following operators:

$$\begin{aligned} |000\rangle\langle 011| + |011\rangle\langle 000| &= IXX(P^0_{\{1\}} \otimes P^{00,11}_{\{2,3\}}), \\ |001\rangle\langle 010| + |001\rangle\langle 010| &= IXX(P^0_{\{1\}} \otimes P^{01,10}_{\{2,3\}}), \\ |100\rangle\langle 111| + |111\rangle\langle 100| &= IXX(P^1_{\{1\}} \otimes P^{00,11}_{\{2,3\}}), \\ |101\rangle\langle 110| + |101\rangle\langle 110| &= IXX(P^1_{\{1\}} \otimes P^{01,10}_{\{2,3\}}). \end{aligned} \tag{D.13}$$

Motivated by the example above, we also use a shorthand to refer to a particular set $D(n,k,f)$ of operators – we define a string of I and X such that for all flipped qubits in f, we label them by X. Therefore, $D(3,2,\{2,3\}) \equiv IXX$. We use the notations interchangeably.

Lemma D.2. *For an n-qubit Gray or binary code, the distance-k operators are expressed as a linear combination of a set of Pauli strings that only depends on the set of the k flipped qubits. Alternatively, a set f of flipped qubits completely determines the set of Pauli strings.*

Proof. Consider the set $D(n,k,f)$ of operators where f is the set of flipped qubits. From Definition D.3, we know that the operators in this set are of the form

$$\left(I_{\bar{f}} \otimes X_f\right) P^a_{\bar{f}} \otimes P^{b,\bar{b}}_f, \tag{D.14}$$

where a and b are bitstrings of length $|f| = k$ and $|\bar{f}| = n-k$, respectively. On the flipped qubits, the operator is of the form

$$X^{\otimes k}(|b_1 \cdots b_k\rangle\langle b_1 \cdots b_k| + |\overline{b_1} \cdots \overline{b_k}\rangle\langle \overline{b_1} \cdots \overline{b_k}|), \tag{D.15}$$

where $b_i \in \{0,1\}$. We now show that all these operators lead to the same set of Pauli strings, independent of the values of $\{b_i\}_i$. To show this, consider that

$$\begin{aligned} &X^{\otimes k}(|b_1 \cdots b_k\rangle\langle b_1 \cdots b_k| + |\overline{b_1} \cdots \overline{b_k}\rangle\langle \overline{b_1} \cdots \overline{b_k}|) \\ &= X^{\otimes k}(O_b + O_{\bar{b}}) \\ &= \frac{1}{2^k} \sum_j \left((-1)^{b\cdot j} + (-1)^{\bar{b}\cdot j}\right) X^{\otimes k} \tilde{O}_j, \end{aligned} \tag{D.16}$$

where the second equality follows from Lemma D.1. Upon expanding, we see that the coefficient of any $\tilde{O}_j$ is non-zero if and only if the binary representation of j has even parity. The signs of the different $\tilde{O}_j$ depend on b, but the set of surviving $\tilde{O}_j$ is independent of b. The number of terms left is 2^{k-1}.

Next, if we consider the unflipped qubits, the operators are of the form

$$|a\rangle\langle a| = \bigotimes_i |a_i\rangle\langle a_i|. \tag{D.17}$$

Since the two possible cases $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$ are both linear combinations of I and Z, and only differ by a negative sign, the set of Pauli strings is independent of a.

To summarize, for a given n and k, all the operators in the set $D(n,k,f)$ are composed of the same Pauli strings and different sets f leads to different Pauli strings. Thus, the set of Pauli strings depends only on the set f, i.e., on the position of the flipped qubits. ■

Corollary D.1. *As a result of Lemma D.2, we see that if a Hamiltonian contains an operator from the set $D(n,k,f)$, any other operator from the same set can be added to the Hamiltonian without an increase in the number of Pauli terms. Since every operator from the set $D(n,k,f)$ consists of the same Pauli strings, adding another operator from the same set changes only the coefficients, and not the set of Pauli strings themselves.*

Lemma D.3. *The set of Pauli strings corresponding to $D(n,k,f)$ is of size 2^{n-1}.*

Proof. Consider the set of operators $D(n,k,f)$, where f is the set of flipped qubits. From Definition D.3, we know that the operators in this set are of the form

$$\left(I_{\bar{f}} \otimes X_f\right) P^a_{\bar{f}} \otimes P^{b,\bar{b}}_f, \tag{D.18}$$

where a and b are bitstrings of length $|f| = k$ and $|\bar{f}| = n-k$, respectively. There are 2^{n-k} possible choices for a and the flipped operator is of size 2^{k-1}, as discussed in Lemma D.2. Thus, the total number of operators is

$$2^{n-k} \times 2^{k-1} = 2^{n-1}, \tag{D.19}$$

concluding the proof. ■

Definition D.4 [*Alternate Representation*]. *An encoding represents a one-to-one mapping between Fock basis elements and computational basis elements. As seen in the main text, a Gray basis $\mathcal{G}_n$ on n bits is a list of 2^n basis elements:*

$$\mathcal{G}_n = (g_0, g_1, \ldots, g_{2^n-1}), \tag{D.20}$$

where each g_i differs from its neighbors by a single bit. Another example considered in the main text is the binary encoding. The binary basis $\mathcal{B}_n$ on n bits is a list of 2^n basis elements:

$$\mathcal{B}_n = (b_0, b_1, \ldots, b_{2^n-1}), \tag{D.21}$$

where b_i is the binary representation of the integer i.

A basis encoding can alternatively be represented using a sequence of flipped bits. This alternate representation is defined as S_n. Thus, for an encoding of size 2^n, the alternate representation is of size $2^n - 1$.

The alternate representation for the Gray code is straightforward. Since any two neighboring entries only have a single bit flipped, the entries of the alternate representation are the flipped bits. For example, the entry that connects 010 *and* 011 *is* 3.

For the binary code, we use a different notation. Each entry of the alternate representation is the decimal equivalent of the bit-wise addition modulo 2 of the two entries of the encoding. For example, the entry that connects 1011 *and* 1100 *is* $0111_2 \equiv 7_{10}$.

For $N = 8$, the alternate representation for the two encodings can be seen in Table D.1.

Basis	Gray	Binary
$\|0\rangle \leftrightarrow \|1\rangle$	1	1
$\|1\rangle \leftrightarrow \|2\rangle$	2	3
$\|2\rangle \leftrightarrow \|3\rangle$	1	1
$\|3\rangle \leftrightarrow \|4\rangle$	3	7
$\|4\rangle \leftrightarrow \|5\rangle$	1	1
$\|5\rangle \leftrightarrow \|6\rangle$	2	3
$\|6\rangle \leftrightarrow \|7\rangle$	1	1

Table D.1: Alternate representations for the Gray and binary code on three qubits.

Lemma D.4. *The alternate representation for $\overline{\mathcal{G}_n}$ and $\overline{\mathcal{B}_n}$ is the same as $\mathcal{G}_n$ and $\mathcal{B}_n$, respectively.*

Proof. The binary reflective Gray code on n bits is given by

$$\mathcal{G}_n = (\mathcal{G}_{n-1} \cdot 0, \overline{\mathcal{G}_{n-1}}, \cdot 1), \tag{D.22}$$

where $\overline{G}_n$ is the Gray code on n bits with the entries in reverse order. Reversing the entire code, we find that

$$\overline{\mathcal{G}_n} = (\mathcal{G}_{n-1} \cdot 1, \overline{\mathcal{G}_{n-1}}, \cdot 0). \tag{D.23}$$

Thus, the reversed code has the same structure as the existing code with the first half entries ending with 1, and the second half ending with 0. The entries of alternate representation indicate which bits are flipped and therefore, is unaffected if $0 \leftrightarrow 1$. Thus, the alternate representation for the reversed Gray code is the same as the original.

For the binary code $\mathcal{B}_n$, the reversed binary code is the same as the original with all zeros and ones flipped. Again, the entries of alternate representation indicate which bits are flipped and therefore, is unaffected if $0 \leftrightarrow 1$. Thus, the alternate representation for the reversed binary code is the same as the original. ■

Definition D.5 [*Subsequences*]. *An entry in the alternate representation of an encoding represents the flipped qubits between the two corresponding entries of the encoding. We now define a subsequence of the alternate representation as an ordered subset that connects the two corresponding entries of the encoding. For example, in the Gray encoding, if* 3 *connects* 010 *and* 011*, and* 1 *connects* 011 *and* 111*, then* $\underline{3, 1}$ *connects* 010 *and* 111*. In*

this work, we represent subsequences using an underscore. For example, in the Gray encoding, the following subsequence

$$(1, 2, \underline{1, 3, 1, 2}, 1) \tag{D.24}$$

connects the basis states 110 *and* 101.

Lemma D.5. *There exists an equivalence between subsequences of the alternate representation of an n-qubit encoding and Pauli strings of the form* $\{I, X\}^{\otimes n} \setminus I^{\otimes n}$.

Proof. In the alternate representation of the Gray code, each entry i indicates that the operator connecting the corresponding basis state has Pauli X acting on qubit i. For example, in an $n = 3$ qubit Gray code, an entry 2 indicates that the two basis elements differ on the second qubit; i.e., the operator connecting them is IXI. Subsequences, therefore, encode a string from $\{I, X\}^{\otimes n}$ that connect the endpoints of the subsequence. For example,

$$(1, 2, \underline{1, 3, 1, 2}, 1) \tag{D.25}$$

corresponds to $X_1X_3X_1X_2 = IXX$.

Similarly, for the binary code, we act with a bit-wise addition modulo 2 between the binary representation of every element in the subsequence. The resulting binary string is then translated into a Pauli string of $\{I, X\}$ – each 1 is mapped to X, and each 0 is mapped to I. For example,

$$(1, 3, \underline{1, 7, 1, 3}, 1) \tag{D.26}$$

corresponds to 100 and ultimately, XII. ■

Lemma D.6. *The alternate representation for the Gray and binary code on n qubits can be expressed in the form*

$$S_n = (S_{n-1}, P_n, S_{n-1}), \tag{D.27}$$

where P_i *stands for* i *and* $2^i - 1$ *in the Gray and binary codes, respectively, and we refer to each* P_i *as a pivot. The term pivot refers to the fact that about* P_n*, the alternate representation* S_n *is symmetric.*

Proof. Consider the form of the binary reflective Gray code on n qubits

$$\mathcal{G}_n = (\mathcal{G}_{n-1} \cdot 0, \overline{\mathcal{G}_{n-1}} \cdot 1), \tag{D.28}$$

where $\overline{G}_n$ is the Gray code on n qubits with the entries in reverse order. Thus the alternate representation for the code is given by

$$S_n = (S_{n-1}, n, \tilde{S}_{n-1}), \tag{D.29}$$

where $\tilde{S}_n$ is the alternate representation of the reversed code $\mathcal{G}_n$. Using Lemma D.4, the alternate representation is

$$S_n = (S_{n-1}, n, S_{n-1}). \tag{D.30}$$

The binary code on n bits is given by

$$\mathcal{B}_n = (0 \cdot \mathcal{B}_{n-1}, 1 \cdot \mathcal{B}_{n-1}). \tag{D.31}$$

The last entry of $\mathcal{B}_{n-1}$ is 1^{n-1}, and the first entry of $\mathcal{B}_{n-1}$ is 0^{n-1}. In the first and second half of the overall code, the first bit is never flipped, and between the halves all bits are flipped. Since the decimal representation of 1^n is $2^n - 1$, the alternate representation is then given by

$$S_n = (S_{n-1}, 2^n - 1, S_{n-1}), \tag{D.32}$$

concluding the proof. ■

In the next two lemmas, we prove that we only need to consider subsequences that end at a power of two index. We show that those subsequences are optimal, and for all other subsequences, there exists a shorter (or equal length) subsequence ending at a power of two index that maps to the same Pauli string of $\{I, X\}$ as defined in Lemma D.5.

Lemma D.7. *Consider any subsequence of the alternate representation S_n on n qubits. Let H be the largest entry of the subsequence. Using Lemma D.5, we know that the subsequence corresponds to a Pauli string consisting of X and I.*

Then the corresponding Pauli string can be formed by another subsequence that ends at the first instance of H (which is guaranteed to occur at an index that is a power of two) and has a length less than or equal to the original length.

Let us consider a few examples before we go into the proof. For the Gray code,

$$\begin{aligned}
(1, 2, \underline{1, 3, 1, 2}, 1) &\equiv (\underline{1, 2, 1, 3}, 1, 2, 1), \\
(\underline{1, 2, 1, 3, 1}, 2, 1) &\equiv (1, \underline{2, 1, 3}, 1, 2, 1), \\
(\underline{1, 2, 1}, 3, 1, 2, 1) &\equiv (1, \underline{2}, 1, 3, 1, 2, 1).
\end{aligned} \tag{D.33}$$

Similarly, for the binary code

$$\begin{aligned}
&(1,3,\underline{1,7,1,3},1) \equiv (\underline{1,3,1,7},1,3,1),\\
&(\underline{1,3,1,7,1},3,1) \equiv (1,\underline{3,1,7},1,3,1),\\
&(\underline{1,3,1},7,1,3,1) \equiv (1,\underline{3},1,7,1,3,1).
\end{aligned} \tag{D.34}$$

Proof of Lemma D.7. We prove the result using an inductive approach on n, where n is the number of qubits. We have two base cases, $n = 1$ and $n = 2$. For $n = 1$, $S_1 = \{1\}$. There exists only one possible subsequence and it ends at a power of two. For $n = 2$, $S_2 = \{1, 2, 1\}$ or $\{1, 3, 1\}$ for the Gray and binary code, respectively. There are six possible subsequences:

$$\begin{aligned}
(\underline{1},2,1) &\equiv (\underline{1},2,1), & (\underline{1},3,1) &\equiv (\underline{1},3,1),\\
(\underline{1,2},1) &\equiv (\underline{1,2},1), & (\underline{1,3},1) &\equiv (\underline{1,3},1),\\
(\underline{1,2,1}) &\equiv (1,\underline{2},1), & (\underline{1,3,1}) &\equiv (1,\underline{3},1),\\
(1,\underline{2},1) &\equiv (1,\underline{2},1), & (1,\underline{3},1) &\equiv (1,\underline{3},1),\\
(1,\underline{2,1}) &\equiv (\underline{1,2},1), & (1,\underline{3,1}) &\equiv (\underline{1,3},1),\\
(1,2,\underline{1}) &\equiv (\underline{1},2,1), & (1,3,\underline{1}) &\equiv (\underline{1},3,1),
\end{aligned} \tag{D.35}$$

where the columns represent a Gray code and binary code, respectively. We see that there always exists a subsequence with length less than or equal to the original length, ending at a power of two index.

Next, we state the induction hypothesis: Lemma D.7 holds for some positive integer n. The induction step is to now show that it holds for $n + 1$. From Lemma D.6, we see that

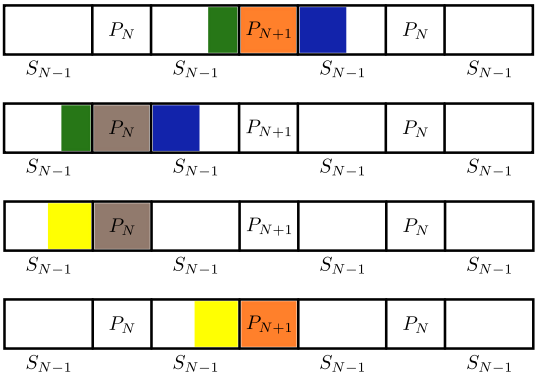
$$S_n = (S_{n-1}, P_n, S_{n-1}), \tag{D.36}$$

$$\begin{aligned}
S_{n+1} &= (S_n, P_{n+1}, S_n)\\
&= (S_{n-1}, P_n, S_{n-1}, P_{n+1}, S_{n-1}, P_n, S_{n-1}),
\end{aligned} \tag{D.37}$$

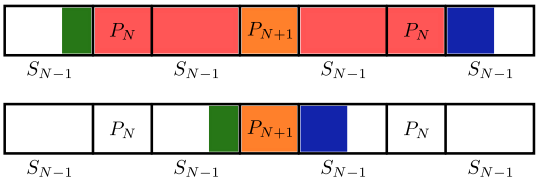
where P_i stands for i and $2^i - 1$ in the Gray and binary codes, respectively, and we refer to each P_i as a pivot. The pivots P_n, P_{n+1}, and P_n occur at indices 2^{n-1}, 2^n, and $3 \cdot 2^{n-1}$, respectively. Consider an arbitrary subsequence

$$a \coloneqq (a[L], \ldots, a[R]) \tag{D.38}$$

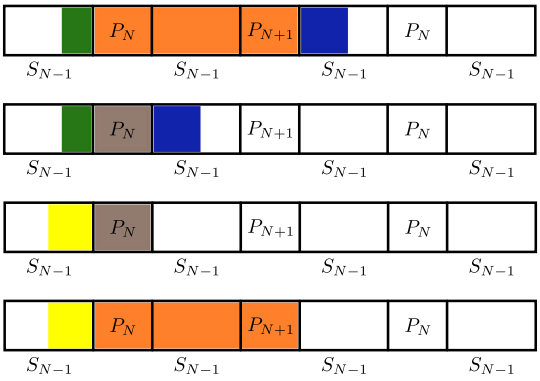
with endpoint indices L and R, where $L \leq R$. Let $\text{len} \coloneqq R - L + 1$ be the length of this subsequence. Based on the values of L and R, we split the problem into multiple cases.



(a) Case 3: We construct a new subsequence with the green section, P_n, and the blue section. Using the induction hypothesis, a new subsequence ending at P_n can be found. Lastly, we replace P_n with P_{n+1} again.



(b) Case 4: The red section of the subsequence can be canceled out. We construct a new subsequence with the green section, P_{n+1}, and the blue section, which reduces to Case 3.



(c) Case 5: We preserve the orange section of the subsequence and construct a new subsequence with the green section, P_n, and the blue section. Using the induction hypothesis, a new subsequence ending at P_n can be found. The yellow section can now be appended to the orange section.

Figure D.1: Proof of Lemma D.7 can be broken down into multiple cases. We label sections of the subsequence with different colors. P_i stands for i and $2^i - 1$ in the Gray and binary codes respectively.

Note that in the following cases, we use the different brackets to indicate if the endpoint of the interval is included – square brackets indicate that the endpoint is included and regular parentheses indicate that the endpoint is not included. For example, $(5, 11]$ is the set $\{6, 7, 8, 9, 10, 11\}$.

- Case 1: $L, R \in [0, 2^n)$. Since both L and R are in the left half of the sequence, the subsequence must exist in $S_n = (S_{n-1}, P_n, S_{n-1})$. Using the induction hypothesis, there exists an alternate subsequence that lies in S_n ending at a power of two index. The same subsequence thus exists in the left half of S_{n+1}.
- Case 2: $L, R \in (2^n, 2^{n+1})$. Since both L and R are in the right half of the sequence, the subsequence must exist in $S_n = (S_{n-1}, P_n, S_{n-1})$. Thus, this case is similarly covered by the induction hypothesis; i.e., there exists an alternate subsequence that lies in S_n ending at a power of two index. The same subsequence thus exists in the left half of S_{n+1}.
- Case 3: $L \in (2^{n-1}, 2^n)$, $R \in (2^n, 3 \cdot 2^{n-1})$. A pictorial representation of the proof can be found in Fig. D.1a. Intuitively, this subsequence, with P_{n+1} replaced with P_n, must already exist in the left half of the overall sequence. To formalize this notion, we now construct a new subsequence

  $$(a[L], \ldots, a[2^n - 1], P_n, a[2^n + 1], \ldots, a[R]).$$

  In essence, we have replaced P_{n+1} with P_n in the original subsequence. This subsequence is now guaranteed to exist in $S_n = (S_{n-1}, P_n, S_{n-1})$. By the inductive hypothesis, there exists a subsequence $(a[k], \ldots, a[2^{n-1} - 1], P_n)$ of length $\leq$ len, where $k \in [0, 2^{n-1})$. By symmetry, the following subsequence

  $$(a[k + 2^{n-1}], \ldots, a[2^n - 1], P_{n+1}),$$

  where we have replaced P_n with P_{n+1} again, must exist, has length $\leq$ len, and ends at $n + 1$.
- Case 4: $L \in [0, 2^{n-1}]$, $R \in [3 \cdot 2^{n-1}, 2^{n+1})$. A pictorial representation of the proof can be found in Fig. D.1b. Intuitively, this subsequence contains $(P_n, S_{n-1}, P_{n+1}, S_{n-1}, P_n)$ as a part of it. This part can be effectively reduced to just P_{n+1} since every other entry occurs an even number of times. Thus, we create a new subsequence

  $$(a[L], \ldots, a[2^{n-1} - 1], P_{n+1}, a[3 \cdot 2^{n-1} + 1], \ldots, a[R]).$$

By symmetry, this subsequence is the same as

$$(a[L + 2^{n-1}], \ldots, a[2^n - 1], P_{n+1}, a[2^n + 1], \ldots, a[R - 2^{n-1}]),$$

where we have shifted the indices of the left and right half by 2^{n-1} up and down respectively. This then reduces to Case 3, handled earlier.

- Case 5: $L \in [0, 2^{n-1}]$, $R \in [2^n, 3 \cdot 2^{n-1})$. A pictorial representation of the proof can be found in Fig. D.1c. In this case, we preserve the subsequence (P_n, S_{n-1}, P_{n+1}) and create a new subsequence of the form

$$(a[L], \ldots, a[2^{n-1} - 1], P_n, a[2^{n-1} + 1], \ldots, a[R - 2^{n-1}]).$$

This subsequence is guaranteed to exist in $S_n = (S_{n-1}, P_n, S_{n-1})$. By the inductive hypothesis, there exists a subsequence $(a[k], \ldots, a[2^{n-1} - 1], P_n)$. We now reconstruct the original subsequence as follows

$$(a[k], \ldots, a[2^{n-1} - 1], P_n, S_{n-1}, P_{n+1}).$$

The length of this subsequence is $\leq$ len and it ends at a power of two.

- Case 6: $L \in (2^{n-1}, 2^n]$, $R \in [3 \cdot 2^{n-1}, 2^{n+1}]$. By symmetry, this subsequence can be reflected about the midpoint $n + 1$. This then reduces to Case 5, handled earlier.

Thus, in all possible cases, we have shown that the inductive step holds if we assume the inductive hypothesis to be true. ■

Lemma D.8. *Given a subsequence that ends at an index which is a power of two, there does not exist another subsequence of a shorter length that leads to the same Pauli string.*

Proof. Given a subsequence ending at index 2^m, the corresponding Pauli string must have X acting on qubit $m + 1$. We now provide a proof by contradiction. We first assume that a shorter subsequence exists. The two possible cases are:

- Case 1: The shorter subsequence ends before index 2^m. More concretely, the shorter subsequence exists within $[0, 2^m)$ and using Lemma D.7, there exists an equivalent subsequence that ends at index 2^{m-1}. No possible subsequence in this region can have its corresponding Pauli string with X acting on qubit $m + 1$.

- Case 2: A shorter subsequence ends at index 2^m. This subsequence has X acting on qubit $m+1$. There are 2^m subsequences of the form $(k, \ldots, 2^m)$ for $k \in \{1, \ldots, 2^m\}$. These subsequences map to all possible Pauli strings of length m. Thus, two different subsequences ending at 2^m cannot lead to the same Pauli string.

Thus, we see that there cannot exist any other subsequence of a shorter length that leads to the same Pauli string. ■

We note that in the present study, the Hamiltonian for $K = 0$ (diagonal potential) is tridiagonal because of the kinetic energy term. As a result, the entries for $K = 1$ in the following lemmas and remarks are used for $K = 0$.

Lemma D.9. *Let i, j be two n-bit binary strings, and let $N = 2^n$. Then, the following statement is true*

$$P(n, K): \sum_{i=0}^{2^n-1} (-1)^{i \cdot j} i^K = 0 \iff |j| > K, \tag{D.39}$$

for all $0 \leq K \leq N$ and $n > 0$.

Proof. We prove the statement using induction. More concretely, we use simple induction on n and strong induction on K. Thus, we assume $P(n-1, K), P(n-1, K-1), \ldots, P(n-1, 0)$ to be true, and use them to prove $P(n, K)$. We first show the sets of base cases $P(1, K)$ and $P(n, 0)$.

Base Case 1 : $P(1, K)$. The left hand side now becomes

$$\begin{aligned} &(-1)^{0 \cdot j} 0^K + (-1)^{1 \cdot j} 1^K \\ &= 0^K + (-1)^j = 0 \iff K = 0, j = 1, . \end{aligned} \tag{D.40}$$

where we use the fact that $0^0 = 1$. Thus, $|j| > K$.

Base Case 2 : $P(n, 0)$. The left hand side now becomes

$$\sum_{i=0}^{2^n-1} (-1)^{i \cdot j} i^0 = 0, \tag{D.41}$$

which is true $\forall\, j \neq 0$. Thus, $|j| > 0$.

To prove the equivalence $P(n, K)$, we start from the right hand side $|j| > K$, and show that it is equivalent to the left hand side. Let the binary expansion of j be given by $j_1 j_2 \dots j_n$.

Case 1: $j_1 = 0$. Thus, $|j_2 \dots j_n| > K$. Using the inductive hypotheses and the fact that $|j_2 \dots j_n| > K$ satisfies the right hand side of all the hypotheses, we have the following equalities:

$$\sum_{i=0}^{2^{n-1}-1} (-1)^{i\cdot(j_2\dots j_n)} i^K = 0 \qquad \text{Using } P(n-1, K) \tag{D.42}$$

$$\sum_{i=0}^{2^{n-1}-1} (-1)^{i\cdot(j_2\dots j_n)} i^{K-1} = 0 \qquad \text{Using } P(n-1, K-1) \tag{D.43}$$

$$\vdots$$

$$\sum_{i=0}^{2^{n-1}-1} (-1)^{i\cdot(j_2\dots j_n)} i^0 = 0 \qquad \text{Using } P(n-1, 0). \tag{D.44}$$

In each of the statements above, i is an $(n-1)$-bit binary string. Now consider the following equation:

$$\begin{aligned}
&\binom{K}{0}(2^n)^0 \left[\sum_{i=0}^{2^{n-1}-1} (-1)^{i\cdot(j_2\dots j_n)} i^K\right] \\
&+ \binom{K}{1}2^n \left[\sum_{i=0}^{2^{n-1}-1} (-1)^{i\cdot(j_2\dots j_n)} i^{K-1}\right] \\
&+ \binom{K}{2}(2^n)^2 \left[\sum_{i=0}^{2^{n-1}-1} (-1)^{i\cdot(j_2\dots j_n)} i^{K-2}\right] \\
&+ \dots + \binom{K}{K}(2^n)^K \left[\sum_{i=0}^{2^{n-1}-1} (-1)^{i\cdot(j_2\dots j_n)} i^0\right] \\
&= 0.
\end{aligned} \tag{D.45}$$

The equality is because each term within square brackets is zero (using (D.42)-(D.44)). Thus, using the binomial theorem,

$$\left[\sum_{i=0}^{2^{n-1}-1} (-1)^{i\cdot(j_2\dots j_n)} (2^n + i)^K\right] = 0. \tag{D.46}$$

Combining with the first step of the inductive tree (D.42),

$$\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\dots j_n)}(i)^K\right]+\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\dots j_n)}(2^n+i)^K\right]=0. \tag{D.47}$$

In the above two summations, i is an $n-1$ bit binary string. We now create an n bit binary string i' by appending either 0 or 1 to the front of i and append j_1 to the front of $j_2\dots j_n$. Since $j_1=0$, this extra bit has no effect. Thus, the equation becomes

$$\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{0i\cdot(j_1 j_2\dots j_n)}(i)^K\right]+\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{1i\cdot(j_1 j_2\dots j_n)}(2^n+i)^K\right]=0. \tag{D.48}$$

Now, we notice that $1i$ is the binary expansion of 2^n+i. Thus, the summation can be written as

$$\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{0i\cdot(j_1 j_2\dots j_n)}(i)^K\right]+\left[\sum_{i'=2^{n-1}}^{2^n-1}(-1)^{i'\cdot(j_1 j_2\dots j_n)}(i')^K\right]=0. \tag{D.49}$$

Since i' is just a dummy index, we replace it with i and combine it with the first term, finally leading to

$$\sum_{i=0}^{2^n-1}(-1)^{i\cdot j}i^K=0. \tag{D.50}$$

Case 2: $j_1=1$. Thus, $|j_2\dots j_n|>K-1$. Using the inductive hypotheses and the fact that $|j_2\dots j_n|>K-1$ satisfies the right hand side of all the hypotheses, we have the following equalities:

$$\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\dots j_n)}i^{K-1}=0 \qquad \text{Using } P(n-1,K-1) \tag{D.51}$$

$$\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\dots j_n)}i^{K-2}=0 \qquad \text{Using } P(n-1,K-2) \tag{D.52}$$

$$\vdots$$

$$\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\dots j_n)}i^{0}=0 \qquad \text{Using } P(n-1,0). \tag{D.53}$$

In each of the statements above, i is an $(n-1)$-bit binary string. Now consider the following equation:

$$\begin{aligned}
&-\binom{K}{1}2^n\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\ldots j_n)}i^{K-1}\right]\\
&-\binom{K}{2}(2^n)^2\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\ldots j_n)}i^{K-2}\right]\\
&-\cdots-\binom{K}{K}(2^n)^K\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\ldots j_n)}i^{0}\right]\\
&=0. \qquad \text{(D.54)}
\end{aligned}$$

The equality is because each term within square brackets is zero (using (D.51)-(D.53)). Adding and subtracting the following term,

$$\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\ldots j_n)}i^{K}\right], \qquad \text{(D.55)}$$

we get

$$\begin{aligned}
&\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\ldots j_n)}i^{K}\right]\\
&-\left\{\binom{K}{0}(2^n)^0\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\ldots j_n)}i^{K}\right]\right.\\
&+\binom{K}{1}2^n\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\ldots j_n)}i^{K-1}\right]\\
&+\binom{K}{2}(2^n)^2\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\ldots j_n)}i^{K-2}\right]\\
&\left.+\cdots+\binom{K}{K}(2^n)^K\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\ldots j_n)}i^{0}\right]\right\}=0. \qquad \text{(D.56)}
\end{aligned}$$

Combining the terms within the curly brackets using the binomial theorem, we get

$$\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\ldots j_n)}i^{K}\right]-\left[\sum_{i=0}^{2^{n-1}-1}(-1)^{i\cdot(j_2\ldots j_n)}(2^n+i)^{K}\right]=0. \qquad \text{(D.57)}$$

In the above two summations, i is an $n-1$ bit binary string. We now create an n bit binary string i' by appending either 0 or 1 to the front of i and append j_1 to the front of $j_2 \dots j_n$. Since $j_1 = 1$, this extra bit accounts for the negative sign. Thus, the equation becomes

$$\left[\sum_{i=0}^{2^{n-1}-1} (-1)^{0i\cdot(j_1 j_2 \dots j_n)} (i)^K\right] + \left[\sum_{i=0}^{2^{n-1}-1} (-1)^{1i\cdot(j_1 j_2 \dots j_n)} (2^n + i)^K\right] = 0. \tag{D.58}$$

Now, we notice that $1i$ is the binary expansion of $2^n + i$. Thus, the summation can be written as

$$\left[\sum_{i=0}^{2^{n-1}-1} (-1)^{0i\cdot(j_1 j_2 \dots j_n)} (i)^K\right] + \left[\sum_{i'=2^{n-1}}^{2^n-1} (-1)^{i'\cdot(j_1 j_2 \dots j_n)} (i')^K\right]. \tag{D.59}$$

Since i' is just a dummy index, we replace it with i and combine it with the first term, finally leading to

$$\sum_{i=0}^{2^n-1} (-1)^{i\cdot j} i^K = 0. \tag{D.60}$$

Thus, for both cases $j_1 = 0, 1$, we showed that $P(n, K)$ follows from the inductive hypotheses, concluding the proof. ■

Lemma D.10. *Consider an $N \times N$ matrix H with diagonal entries of the form*

$$H_{i,i} = \sum_{k=0}^{K} a_k i^k, \tag{D.61}$$

for some set $\{a_k\}_{k=0}^K$ of real constants and for all $i \in \{0, \dots, N-1\}$. Considering only the diagonal part of the matrix, and using the binary encoding, we get the following equality:

$$\begin{aligned} H_{\text{diag}} &= \sum_{i=0}^{N-1} \sum_{k=0}^{K} a_k i^k |i\rangle\langle i| \\ &= \sum_{i=0}^{N-1} \sum_{k=0}^{K} a_k i^k O_i \\ &= \frac{1}{2^n} \sum_{j=0}^{N-1} \sum_{k=0}^{K} a_k \left[\sum_{i=0}^{N-1} (-1)^{i\cdot j} i^k\right] \tilde{O}_j, \end{aligned} \tag{D.62}$$

where the third equality follows from Lemma D.1. Then, the number of Pauli terms accounted for by the diagonal part of the matrix is given by

$$\mathrm{d}(n, K) := \sum_{m=0}^{K} \binom{n}{m}, \tag{D.63}$$

where $n = \log_2(N)$.

Proof. In (D.62), using Lemma D.9, the term in square brackets is non-zero if and only if $|j| \leq K$ and all terms with $|j| > K$ get cancelled. Thus, the surviving terms have $|j| \leq K$ and the number of such terms is given by

$$\sum_{m=0}^{K} \binom{n}{m}, \tag{D.64}$$

which is the number of ways to pick j such that $|j| \leq K$. ■

Remark D.2. *Lemma D.10 shows that the number of Pauli terms for the diagonal part of the Hamiltonian, using the binary encoding, is given by* $\mathrm{d}(n, K)$. *Instead, if we use the Gray encoding, the diagonal part of the Hamiltonian is given by*

$$\begin{aligned} H_{\text{diag}} &= \sum_{i=0}^{N-1} \sum_{k=0}^{K} a_k i^k |i\rangle\langle i| \\ &= \sum_{i=0}^{N-1} \sum_{k=0}^{K} a_k i^k O_i \\ &= \frac{1}{2^n} \sum_{j=0}^{N-1} \sum_{k=0}^{K} a_k \left[\sum_{i=0}^{N-1} (-1)^{e(i)\cdot j} i^k \right] \tilde{O}_j. \end{aligned} \tag{D.65}$$

Replacing i with $e(i)$ in the exponent changes the relative signs of each term. Thus, the set of surviving j is different for the binary and Gray encodings. However, since we consider a sum of all possible j, the size of the set of surviving terms is the same and is equal to $\mathrm{d}(n, K)$.

Lemma D.11. *The number of Pauli terms in the Hamiltonian $H_{N,K}$ for the Gray and binary code is given by ($N = 2^n$),*

$$|H(N, K)| = \begin{cases} \mathrm{d}(n, 1) + n2^{n-1} & K = 0 \\ \mathrm{d}(n, K) + 2^{n-1} \sum_{k=1}^{K} \overline{n}_k & 1 \leq K \leq 2^{n-1} \\ 2^{n-1}(1 + 2^n) & K > 2^{n-1}, \end{cases} \tag{D.66}$$

where $\overline{n}_k := n - \lceil \log_2(k) \rceil$.

Proof. From Lemmas D.7 and D.8, we see that we are interested in subsequences ending at powers of two only. For any subsequence not ending at a power of two, Lemma D.7 states that there exists an equivalent subsequence ending at a power of two of shorter (or equal) length. Furthermore, Lemma D.8 states that for any subsequence ending at a power of two, no shorter subsequence gives the same Pauli string. Lastly, the set of subsequences ending at a power of two covers all Pauli strings. Thus, the set of subsequences ending at a power of two forms a complete and optimal set.

To prove the current lemma, we establish a correspondence between subsequences and Pauli strings of the Hamiltonian. As seen in Remark D.5, for every subsequence, we can associate a Pauli string composed of $\{I, X\}$. The Pauli string corresponds to the flipped bits in the two encoded basis states at the end of the subsequence. For example, consider an $n = 3$ Gray code as seen in Table D.1. The subsequence

$$\underline{(1, 2, 1, 3}, 1, 2, 1) \equiv IXX, \tag{D.67}$$

indicates that $|0\rangle \to |000\rangle$ and $|4\rangle \to |011\rangle$ differ on qubits 2 and 3, as the equivalent Pauli string has X acting on qubits 2 and 3. Next, we saw in Definition D.3 that the set of flipped qubits specifies a particular set of operators, each composed of the same Pauli strings but differing only in their coefficients. Thus, the set can be specified by the set of Pauli strings that its operators are composed of. For example IXX corresponds to the set

$$D(3, 2, \{2, 3\}) = \{(I_1 \otimes X_{2,3})\, P_1^a \otimes P_{2,3}^{b,\bar{b}} : \forall a, \forall b\}. \tag{D.68}$$

Each operator in this example is made up of the following set of Pauli strings:

$$\left\{(I \otimes XX)\left(\frac{I \pm Z}{2} \otimes \frac{II \pm ZZ}{2}\right)\right\}. \tag{D.69}$$

Thus, there exists a one-to-one mapping between subsequences ending at a power of two and Pauli strings of the form $\{I, X\}^{\otimes n} \setminus I^{\otimes n}$. We also showed that there exists a one-to-one mapping between Pauli strings of the form $\{I, X\}^{\otimes n} \setminus I^{\otimes n}$ and sets of distance operators with fixed flipped qubits, completing the connection to subsequences. Since we are only interested in subsequences ending at a power of two, we need to find the number of such subsequences.

Next, we provide an important connection that allows us to quantify the number of Pauli terms for a particular N and K. The truncation parameter K in $H_{N,K}$

specifies the maximum length of subsequences allowed; thus, to quantify the number of Pauli terms, we consider all subsequences of length $k \in \{1, \ldots, K\}$.

We first provide an example. In the case of $K = 3$ for a three-qubit Gray code, we need to consider subsequences of length $k \in \{1, 2, 3\}$. Furthermore, we need to only consider subsequences ending at a power of two index. Thus, the subsequences we need to consider are

$$(\underline{1}, 2, 1, 3, 1, 2, 1) \equiv XII, \tag{D.70}$$
$$(1, \underline{2}, 1, 3, 1, 2, 1) \equiv IXI, \tag{D.71}$$
$$(1, 2, 1, \underline{3}, 1, 2, 1) \equiv IIX, \tag{D.72}$$
$$(\underline{1, 2}, 1, 3, 1, 2, 1) \equiv XXI, \tag{D.73}$$
$$(1, 2, \underline{1, 3}, 1, 2, 1) \equiv XIX, \tag{D.74}$$
$$(1, \underline{2, 1, 3}, 1, 2, 1) \equiv XXX, \tag{D.75}$$

where the first three entries account for $k = 1$, the next two account for $k = 2$, and the last entry accounts for $k = 3$.

A subsequence of length k cannot end at index 2^m if $k > 2^m$. Since the highest power of two in an n-qubit Gray code is 2^{n-1}, for $k > 2^{n-1}$, we expect to see no new Pauli strings. Thus, for a fixed k such that $1 < k < 2^{n-1}$, we need to count all powers of two greater than k and less than 2^n. There are

$$\overline{n}_k = n - \lceil \log_2(k) \rceil \tag{D.76}$$

subsets, each contributing 2^{n-1} Pauli terms (see Lemma D.3). For a concrete example, the subsets for different k for a Gray code on $n = 4$ qubits is shown in Table D.2. The columns represent the index endpoints of the subsequences.

Similarly, the table for a binary code is shown in Table D.3.

Thus, the total number of Pauli terms for $1 \leq K \leq 2^{n-1}$ is given by

$$\mathrm{d}(n, K) + \sum_{k=1}^{K} \overline{n}_k 2^{n-1}, \tag{D.77}$$

where the first term arises when $k = 0$, i.e., the number operators of the form $\{I, Z\}^{\otimes n}$ using Lemma D.10.

k	1	2	4	8
1	XIII	IXII	IIXI	IIIX
2		XXII	XIXI	XIIX
3			XXXI	XXIX
4			IXXI	IXIX
5				IXXX
6				XXXX
7				XIXX
8				IIXX

Table D.2: Gray encoding subsequences as a function of k for an $n = 4$ code. For a fixed k, we see that there are $\overline{n}_k = n - \lceil \log_2(k) \rceil$ entries and for $k > 2^{n-1}$, there are no new entries.

k	1	2	4	8
1	IIIX	IIXX	IXXX	XXXX
2		IIXI	IXXI	XXXI
3			IXIX	XXIX
4			IXII	XXII
5				XIXX
6				XIXI
7				XIIX
8				XIII

Table D.3: Binary encoding subsequences as a function of k for an $n = 4$ code. For a fixed k, we see that there are $\overline{n}_k = n - \lceil \log_2(k) \rceil$ entries and for $k > 2^{n-1}$, there are no new entries.

Thus, we finally see that

$$|H(N,K)| = \begin{cases} \mathrm{d}(n,1) + n2^{n-1} & K = 0 \\ \mathrm{d}(n,K) + 2^{n-1} \sum_{k=1}^{K} \overline{n}_k & 1 \leq K \leq 2^{n-1} \\ 2^{n-1}(1+2^n) & K > 2^{n-1}, \end{cases} \tag{D.78}$$

concluding the proof. ■

Lemma D.12. *The set of Pauli strings corresponding to $D(n,k,f)$ consists of $2^{|f|-1}$ qubit-wise commuting sets.*

Proof. As a reminder, the set of operators $D(n,k,f)$ is defined as

$$D(n,k,f) \coloneqq \left\{ \left(I_{\bar{f}} \otimes X_f \right) P^a_{\bar{f}} \otimes P^{b,\bar{b}}_f : \forall a \in \{0,1\}^{|\bar{f}|},\ \forall b \in \{0,1\}^{|f|} \right\}, \tag{D.79}$$

where $P^a_{\bar{f}}$ and and $P^{b,\bar{b}}_f$ are defined in Definition D.1. Since we are interested in qubit-wise commutativity, we consider the f and $\bar{f}$ qubits separately. On the unflipped qubits $\bar{f}$, the action of every element in $D(n,k,f)$ is P^a for every bitstring a. Expanding, we know that for all a, P^a is a linear combination of Pauli strings composed of $\{I,Z\}$ only. Thus, all of them pairwise-qubit commute.

On the flipped qubits f, the action of every element in $D(n,k,f)$ is $X_f \circ P^{b,\bar{b}}_f$ for every bitstring b. As seen before, $P^{b,\bar{b}}_f$ is composed of $2^{|f|-1}$ Pauli strings. None of the Pauli strings qubit-wise commute because of the overall composition with the Pauli X string. Thus, every set $D(n,k,f)$ consists of $2^{|f|-1}$ qubit-wise commuting Pauli terms. ■

As an example related to Lemma D.12, consider the set $D(4,2,\{3,4\})$, alternatively labeled $IIXX$,

$$IIXX = \left\{ \left(I_{1,2} \otimes X_{3,4} \right) P^a_{\{1,2\}} \otimes P^{b,\bar{b}}_{\{3,4\}} \right\}. \tag{D.80}$$

As mentioned earlier, the values of a and b change the coefficient of the different Pauli strings, but not the set of strings themselves. Thus, we consider $a = 00$ and $b = 00$. For this choice, the operator is given by

$$\begin{aligned} &\left(I_{1,2} \otimes X_{3,4} \right) \left((II + IZ + ZI + ZZ) \otimes (II + ZZ) \right) \\ &\qquad = (II + IZ + ZI + ZZ) \otimes (XX + YY), \end{aligned} \tag{D.81}$$

up to a normalization constant. Thus, we see that the set of Pauli terms in the linear combination can be split into the following two qubit-wise commuting sets:

$$\{IIXX, IZXX, ZIXX, ZZXX\}, \tag{D.82}$$

$$\{IIYY, IZYY, ZIYY, ZZYY\}. \tag{D.83}$$

Note that different values of a and b will change the relative sign of some Pauli strings, but preserve the set of Pauli strings.

Lemma D.13. *The number of qubit-wise commuting sets for $H_{N,K}$ for the binary code is given by*

$$|H(N,K)|_C = \begin{cases} 2^n & K = 0 \\ 1 + \sum_{k=1}^{K} 2^{|b(\bar{k})|} \left[1 - 2^{-\bar{n}_k}\right] & 1 \leq K \leq 2^{n-1} \\ \frac{1}{2}\left(1 + 3^n\right) & K > 2^{n-1}, \end{cases} \tag{D.84}$$

where $|w|$ is the Hamming weight of the string w, $\bar{n}_k := n - \lceil \log_2(k) \rceil$, and $\bar{k} := 2^n - k$.

Proof. Consider $1 \leq K \leq 2^{n-1}$ and consider a column in Table D.3 labeled by 2^j. For a particular k value, the entry represents a subsequence of length k ending at index 2^j. From the ordering of the binary code basis elements, we see that the entry is given by $b(2^{j+1} - k)$. Thus, the total number is given by

$$\sum_{j=\lceil \log_2(k) \rceil}^{n-1} 2^{|b(2^{j+1}-k)|-1}. \tag{D.85}$$

This can be simplified by noting that moving a column to the left reduces the weight of the string by one. Thus, we consider the weight of the last string in the row and move left. For the last column, the entry is given by $\bar{k} := 2^n - k$. Thus, the number of QC sets for a given k is given by

$$\sum_{i=0}^{\bar{n}_k - 1} 2^{|b(\bar{k})|-i-1} = 2^{|b(\bar{k})|}\left[1 - 2^{-\bar{n}_k}\right]. \tag{D.86}$$

Thus, for a given $1 \leq K \leq 2^{n-1}$, we get

$$1 + \sum_{k=1}^{K} 2^{|b(\bar{k})|}\left[1 - 2^{-\bar{n}_k}\right] \tag{D.87}$$

qubit-wise commuting sets. The case $K = 0$ is equal to the value of $K = 1$ since the kinetic energy term accounts for two off-diagonal terms anyway.

Lastly, for $K > 2^{n-1}$, we have considered all subsets, leading to

$$1 + \frac{1}{2}\sum_{i=1}^{n} 2^i \binom{n}{i} = \frac{1}{2}\left(1 + 3^n\right), \tag{D.88}$$

concluding the proof. ■

Lemma D.14. *The number of qubit-wise commuting sets for $H_{N,K}$ for the Gray code is given by*

$$|H(N,K)|_C = \begin{cases} 1+n & K=0 \\ 1+\sum_{k=1}^{K} \overline{n}_k 2^{|g_{k-1}|} & 1 \leq K \leq 2^{n-1} \\ \frac{1}{2}\left(1+3^n\right) & K > 2^{n-1}, \end{cases} \tag{D.89}$$

where $|w|$ is the Hamming weight of the string w, and $\overline{n}_k \coloneqq n - \lceil \log_2(k) \rceil$.

Proof. Consider $1 \leq K \leq 2^{n-1}$ and consider a column in Table D.2 labeled by 2^j. Since the columns represent subsequences ending at index j, we see that strings in a column have a fixed structure – the strings end with XI^{n-j-1}. The first j bits are a Gray representation of the row index $k-1$. For example, for the cell with row index 3 and column index 2^2, the entry is of the form

$$g_{3-1} \otimes X \otimes I = XX \otimes X \otimes I. \tag{D.90}$$

As seen in Lemma D.12, this set contributes 2^{3-1} Pauli terms.

Thus, for a particular k, the number of Pauli terms is

$$\begin{aligned} &\sum_{j=\lceil \log_2(k) \rceil}^{n-1} 2^{|g_{k-1}XI^{n-j-1}|-1} \\ &= \sum_{j=\lceil \log_2(k) \rceil}^{n-1} 2^{|g_{k-1}|} \\ &= \overline{n}_k 2^{|g_{k-1}|}, \end{aligned} \tag{D.91}$$

where the first non-zero j for a row k is $\lceil \log_2(k) \rceil$. Thus, for a fixed $1 \leq K \leq 2^{n-1}$, we see that

$$1 + \sum_{k=1}^{K} \overline{n}_k 2^{|g_{k-1}|}, \tag{D.92}$$

where the first term arises from the all-Z measurement for the diagonal terms. The case $K = 0$ is equal to the value of $K = 1$ since the kinetic energy terms accounts for two off-diagonal terms anyway.

Lastly, for $K > 2^{n-1}$, we consider all possible subsets $D(n,k,f)$ for all $k \in \{1,\ldots,n\}$. Thus, the total is given by

$$1 + \sum_{i=1}^{n} 2^{i-1} \binom{n}{i} = \frac{1}{2}\left(1+3^n\right). \tag{D.93}$$

This concludes the proof. ■

Lemma D.15. *The set of Pauli strings corresponding to $D(n,k,f)$ all pairwise commute with each other. Alternatively, the set of Pauli strings corresponding to $D(n,k,f)$ forms a distance-grouped commuting set.*

Proof. The set of operators in $D(n,k,f)$ are

$$D(n,k,f) \coloneqq \left\{ \left(I_{\bar{f}} \otimes X_f\right) P^a_{\bar{f}} \otimes P^{b,\bar{b}}_f : \forall a \in \{0,1\}^{|\bar{f}|},\ \forall b \in \{0,1\}^{|f|} \right\}. \tag{D.94}$$

We already saw that when mapped to Pauli strings, all the operators from the set lead to combinations of the same Pauli strings with different coefficients only. In other words, independent of the value of a and b, the operators all map to the same Pauli strings. Since they all map the same set of Pauli strings, without loss of generality, we consider the fixed operator $a = 0^{|\bar{f}|}$ and $b = 0^{|f|}$:

$$\left(I_{\bar{f}} \otimes X_f\right) P^0_{\bar{f}} \otimes P^{0,\bar{0}}_f. \tag{D.95}$$

Now consider, using Lemma D.1, we see that

$$P^0_{|\bar{f}|} = \frac{1}{2^{|\bar{f}|}} \sum_{j=0}^{2^{|\bar{f}|}-1} \tilde{O}_j. \tag{D.96}$$

Next, we see that

$$\begin{aligned} P^{0,\bar{0}}_f &= \frac{1}{2^{|f|}} \sum_l \left((-1)^{0\cdot l} + (-1)^{1\cdot l}\right) \tilde{O}_l \\ &= \frac{1}{2^{|f|}} \sum_l (-1)^{1\cdot l} \tilde{O}_l \\ &= \frac{1}{2^{|f|}} \sum_{l : p(l) \bmod 2 = 0} \tilde{O}_l. \end{aligned} \tag{D.97}$$

As mentioned earlier, only terms with even parity l survive the summation. Thus the Pauli strings are of the form

$$(I \otimes X)\tilde{O}_j \otimes \tilde{O}_l, \tag{D.98}$$

where we use the shorthand X for X_f and the constraint that l has even parity. Finally, we see that the Pauli strings all commute since

$$\begin{aligned}
&[(I\otimes X)\tilde{O}_j\otimes\tilde{O}_l,(I\otimes X)\tilde{O}_m\otimes\tilde{O}_n]\\
&=(I\otimes X)[\tilde{O}_j\otimes\tilde{O}_l,(I\otimes X)\tilde{O}_m\otimes\tilde{O}_n]+[(I\otimes X),(I\otimes X)\tilde{O}_m\otimes\tilde{O}_n]\tilde{O}_j\otimes\tilde{O}_l\\
&=[\tilde{O}_j\otimes\tilde{O}_l,\tilde{O}_m\otimes\tilde{O}_n]+(I\otimes X)[\tilde{O}_j\otimes\tilde{O}_l,(I\otimes X)]\tilde{O}_m\otimes\tilde{O}_n\\
&\quad+(I\otimes X)[(I\otimes X),\tilde{O}_m\otimes\tilde{O}_n]\tilde{O}_j\otimes\tilde{O}_l+[(I\otimes X),(I\otimes X)](\tilde{O}_m\otimes\tilde{O}_n)(\tilde{O}_j\otimes\tilde{O}_l)\\
&=(I\otimes X)[\tilde{O}_j\otimes\tilde{O}_l,(I\otimes X)]\tilde{O}_m\otimes\tilde{O}_n+(I\otimes X)[(I\otimes X),\tilde{O}_m\otimes\tilde{O}_n]\tilde{O}_j\otimes\tilde{O}_l,
\end{aligned}\tag{D.99}$$

where the first term is zero since all $\tilde{O}$ are composed of I, Z only. Next, consider that

$$\begin{aligned}
[\tilde{O}_j\otimes\tilde{O}_l,(I\otimes X)]&=\tilde{O}_j\otimes[\tilde{O}_l,X]\\
&=0,
\end{aligned}\tag{D.100}$$

where the last equality is because the parity of l is even. Similarly, the other term is also zero since the parity of n is even. Thus, the overall commutator is zero. Thus, the set of Pauli strings corresponding to the set $D(n,k,f)$ all commute. Since the operators in the set are linear combinations of these Pauli strings, they also commute. ■

Lemma D.16. *The unitary transformation that rotates the computational basis to the common eigenbasis for set of Pauli strings corresponding to $D(n,k,f)$ is given by*

$$I_{\bar{f}}\otimes U_f^{\mathrm{GHZ}},\tag{D.101}$$

where U_f^{GHZ} is the unitary operator

$$U_f^{\mathrm{GHZ}}:=\prod_{i=|f|}^{2}\mathrm{CNOT}_{f_1\to f_i}H_{f_1}.\tag{D.102}$$

The number of two-qubit gates in the diagonalizing unitary for $D(k,n,f)$ is thus given by $(|f|-1)$.

Proof. To show the above result, we show that the output basis when the unitary acts on the computational basis is the common eigenbasis of the Pauli operators

$D(n,k,f)$. Consider the action on a computational basis state of the form $|i\rangle_{\bar{f}} \otimes |j\rangle_f$.

$$\begin{aligned}
&I_{\bar{f}} \otimes U_f^{\mathrm{GHZ}}(|i\rangle_{\bar{f}} \otimes |j\rangle_f) \\
&= I_{\bar{f}} \otimes U_f^{\mathrm{GHZ}}(|i\rangle_{\bar{f}} \otimes |j_1 \cdots j_k\rangle_f) \\
&= |i\rangle_{\bar{f}} \otimes \left(\prod_{t=|f|}^{2} \mathrm{CNOT}_{1\to t} H_1 \, |j_1 \cdots j_k\rangle_f \right) \\
&= |i\rangle_{\bar{f}} \otimes \\
&\left(\frac{1}{\sqrt{2}} \prod_{t=|f|}^{2} \mathrm{CNOT}_{1\to t} (|0\rangle_{j_1} + (-1)^{j_1} |1\rangle_{j_1}) \, |j_2 \cdots j_k\rangle \right) \\
&= |i\rangle_{\bar{f}} \otimes \left(\frac{1}{\sqrt{2}} (|0 j_2 \cdots j_k\rangle_f + (-1)^{j_1} \left|1 \bar{j}_2 \cdots \bar{j}_k\right\rangle_f) \right).
\end{aligned} \tag{D.103}$$

Next, we show that these basis elements are eigenstates of the Pauli operators $D(n,k,f)$. From Lemma D.15, we know that the Pauli strings associated with $D(n,k,f)$ are given by

$$\left\{ (\tilde{O}_l)_{\bar{f}} \otimes X_f(\tilde{O}_m)_f : \forall l \in \{0,\ldots,2^{|\bar{f}|}-1\},\ \forall m \in \{0,\ldots,2^{|f|}-1\},\ p(m) \bmod 2 = 0 \right\}, \tag{D.104}$$

where $p(m)$ is the parity of the bitstring m.

We first consider the action of the above Pauli strings on the individual subspaces f and $\bar{f}$. On the unflipped subspace $\bar{f}$, the action is given by

$$(\tilde{O}_l)_{\bar{f}} |i\rangle_{\bar{f}} = (-1)^{l \cdot i} |i\rangle_{\bar{f}} . \tag{D.105}$$

Thus, $|i\rangle$ is an eigenstate. Next, we consider the flipped subspace.

$$\begin{aligned}
&X_f(\tilde{O}_m)_f \left(\frac{1}{\sqrt{2}} (|0 j_2 \cdots j_k\rangle_f + (-1)^{j_1} \left|1 \bar{j}_2 \cdots \bar{j}_k\right\rangle_f) \right) \\
&= X_f \left(\frac{1}{\sqrt{2}} ((-1)^{m \cdot 0 j_2 \cdots j_k} |0 j_2 \cdots j_k\rangle_f + (-1)^{j_1} (-1)^{m \cdot 1 \bar{j}_2 \cdots \bar{j}_k} \left|1 \bar{j}_2 \cdots \bar{j}_k\right\rangle_f) \right). \\
&= \frac{1}{\sqrt{2}} \left((-1)^{m \cdot 0 j_2 \cdots j_k} \left|1 \bar{j}_2 \cdots \bar{j}_k\right\rangle_f + (-1)^{j_1} (-1)^{m \cdot 1 \bar{j}_2 \cdots \bar{j}_k} |0 j_2 \cdots j_k\rangle_f \right) \\
&= \frac{1}{\sqrt{2}} (-1)^{j_1 + m \cdot 1 \bar{j}_2 \cdots \bar{j}_k} \left(|0 j_2 \cdots j_k\rangle_f + (-1)^{j_1 + m \cdot 0 j_2 \cdots j_k + m \cdot 1 \bar{j}_2 \cdots \bar{j}_k} \left|1 \bar{j}_2 \cdots \bar{j}_k\right\rangle_f \right).
\end{aligned} \tag{D.106}$$

Consider the following equality:

$$\begin{aligned}(-1)^{m\cdot 0 j_2\cdots j_k + m\cdot 1 \bar{j}_2\cdots\bar{j}_k} &= (-1)^{m_1+\cdots+m_k} \\ &= (-1)^{\sum_i m_i} \\ &= 1, \end{aligned} \tag{D.107}$$

where the last equality is because the parity of m is even. Thus, the action on the flipped qubits is given by

$$\begin{aligned} &X_f(\tilde{O}_m)_f \left(\frac{1}{\sqrt{2}}(|0 j_2\cdots j_k\rangle_f + (-1)^{j_1}\left|1\bar{j}_2\cdots\bar{j}_k\right\rangle_f)\right) \\ &= \frac{1}{\sqrt{2}}(-1)^{j_1+m\cdot 1\bar{j}_2\cdots\bar{j}_k}\left(|0 j_2\cdots j_k\rangle_f + (-1)^{j_1}\left|1\bar{j}_2\cdots\bar{j}_k\right\rangle_f\right). \end{aligned} \tag{D.108}$$

Thus, using Eqs. (D.105) and (D.108), the action of any of the Pauli strings on the rotated basis states Eq. (D.103) is given by

$$\begin{aligned} &\left[(\tilde{O}_l)_{\bar{f}}\otimes X_f(\tilde{O}_m)_f\right] I_{\bar{f}}\otimes U_f^{\mathrm{GHZ}}(|i\rangle_{\bar{f}}\otimes|j\rangle_f) \\ &= \left[(-1)^{l\cdot i + j_1 + m\cdot 1\bar{j}_2\cdots\bar{j}_k}\right] I_{\bar{f}}\otimes U_f^{\mathrm{GHZ}}(|i\rangle_{\bar{f}}\otimes|j\rangle_f). \end{aligned} \tag{D.109}$$

Thus, we see that the unitary transformation that rotates the computational basis to the common eigenbasis for the set of Pauli strings corresponding to $D(n,k,f)$ is given by

$$I_{\bar{f}}\otimes U_f^{\mathrm{GHZ}}, \tag{D.110}$$

concluding the proof. ■

Lemma D.17. *The number of distance-grouped commuting sets for $H_{N,K}$ for the binary and the Gray code is given by*

$$|H(N,K)|_C = \begin{cases} 1+n & K=0 \\ 1+\sum_{k=1}^{K}\overline{n}_k & 1\le K\le 2^{n-1} \\ 2^n & K>2^{n-1}. \end{cases} \tag{D.111}$$

Proof. Consider $1\le K\le 2^{n-1}$ and a column in Table D.3 labeled by 2^j. For a particular k value, the entry represents a subsequence of length k ending at index

2^j. From the ordering of the binary code basis elements, we see that the entry is given by $b(2^{j+1} - k)$. Thus, the total number is given by

$$\sum_{i=\lceil \log_2(k) \rceil}^{n-1} 1 = \overline{n}_k. \tag{D.112}$$

Thus, for a given $1 \leq K \leq 2^{n-1}$, we get

$$1 + \sum_{k=1}^{K} \overline{n}_k \tag{D.113}$$

distance-grouped commuting sets. Lastly, for $K > 2^{n-1}$, we have considered all subsets, leading to

$$1 + \sum_{i=1}^{n} \binom{n}{i} = 2^n. \tag{D.114}$$

We notice that the number of distance-grouped commuting sets depends only on the number of filled entries in the Table D.3, and not the individual entries. This is because each entry contributes a single DGC set. Since the Gray code has the same number of filled entries per row as the binary code, the number of DGC sets are the same. ■

Lemma D.18. *The number of two-qubit gates in the diagonalizing unitary using the DGC scheme for the Gray code is given by*

$$|H(N,K)|_{DU} = \begin{cases} 0 & K = 0 \\ \sum_{k=1}^{K} |g_{k-1}| \overline{n}_k & 1 \leq K \leq 2^{n-1} \\ 1 + 2^{n-1}(n-2) & K > 2^{n-1}. \end{cases} \tag{D.115}$$

Proof. As seen in Lemma D.16, the number of two-qubit gates for the diagonalizing unitary for the set $D(n,k,f)$ is $(|f| - 1)$. Similar to the proof of Lemma D.14, consider $1 \leq K \leq 2^{n-1}$ and consider a column in Table D.2 labeled by 2^j. Since the columns represent subsequences ending at j, we see that strings in a column have a fixed structure – the strings end with XI^{n-j-1}. The first j bits are a Gray representation of the row index $k - 1$. For example, the cell with row index 3 and column index 2^2, the entry is of the form

$$g_{3-1} \otimes X \otimes I = XX \otimes X \otimes I. \tag{D.116}$$

As seen in Lemma D.16, the diagonalizing unitary for this set contains 2 two-qubit gates.

Thus, for a particular k, the number of two-qubit gates for all the diagonalizing unitaries are is

$$\sum_{j=\lceil \log_2(k) \rceil}^{n-1} |g_{k-1}| = \overline{n}_k |g_{k-1}|, \tag{D.117}$$

where the first non-zero j for a row k is $\lceil \log_2(k) \rceil$. Thus, for a fixed $1 \leq K \leq 2^{n-1}$, we see that

$$\sum_{k=1}^{K} \overline{n}_k |g_{k-1}|. \tag{D.118}$$

The case $K = 0$ is equal to the value of $K = 1$ since the kinetic energy term accounts for two off-diagonal terms anyway.

Lastly, for $K > 2^{n-1}$, we consider all possible subsets $D(n, k, f)$ for all $k \in \{1, \ldots, n\}$. Thus, the total is given by

$$\sum_{i=1}^{n} (i-1) \binom{n}{i} = 1 + 2^{n-1}(n-2), \tag{D.119}$$

concluding the proof. ■

Lemma D.19. *The number of two-qubit gates in the diagonalizing unitary using the DGC scheme for the binary code is given by*

$$|H(N,K)|_{DU} = \begin{cases} 0.5n(n-1) & K = 0 \\ 0.5 \sum_{k=1}^{K} \overline{n}_k \left[2|b(\overline{k})| - 1 - \overline{n}_k \right] & 1 \leq K \leq 2^{n-1} \\ 1 + 2^{n-1}(n-2) & K > 2^{n-1}. \end{cases} \tag{D.120}$$

Proof. As seen in Lemma D.16, the number of two-qubit gates for the diagonalizing unitary for the set $D(n, k, f)$ is $(|f| - 1)$. Similar to the proof of Lemma D.13, Consider $1 \leq K \leq 2^{n-1}$ and consider a column in Table D.3 labeled by 2^j. For a particular k value, the entry represents a subsequence of length k ending at index 2^j. From the ordering of the binary code basis elements, we see that the entry is given by $b(2^{j+1} - k)$. Thus, the total number is given by

$$\sum_{j=\lceil \log_2(k) \rceil}^{n-1} |b(2^{j+1} - k)| - 1. \tag{D.121}$$

This can be simplified by noting that moving a column to the left reduces the weight of the string by 1. Thus, we consider the weight of the last string in the row and move left. For the last column, the entry is given by $\bar{k} := 2^n - k$. Thus, the number of QC sets for a given k is given by

$$\sum_{i=0}^{\overline{n}_k - 1} |b(\bar{k})| - i - 1 = 0.5\overline{n}_k \left[2|b(\bar{k})| - 1 - \overline{n}_k\right], \tag{D.122}$$

where $\overline{n}_k := n - \lceil \log_2(k) \rceil$. Thus, for a given $1 \leq K \leq 2^{n-1}$, we get

$$0.5 \sum_{k=1}^{K} \overline{n}_k \left[2|b(\bar{k})| - 1 - \overline{n}_k\right] \tag{D.123}$$

two-qubit gates. The case $K = 0$ is equal to the value of $K = 1$ since the kinetic energy term accounts for two off-diagonal terms anyway.

Lastly, for $K > 2^{n-1}$, we consider all possible subsets $D(n, k, f)$ for all $k \in \{1, \ldots, n\}$. Thus, the total is given by

$$\sum_{i=1}^{n} (i-1)\binom{n}{i} = 1 + 2^{n-1}(n-2), \tag{D.124}$$

concluding the proof. ■

D.2 List of Operators

In this section, as an example, we give the complete list of number and ladder operators for all encodings with $N = 4$.

Table D.4 lists the encoded operators for the one-hot encoding. Table D.5 lists the encoded operators for the binary encoding. Lastly, Table D.6 lists the encoded operators for the Gray encoding.

D.3 Simulation Details for n+C

We now provide specific simulation details in Tables D.7, D.8, and D.9 for the different simulations for the energy of the lowest $\frac{1}{2}^+$ state for the n+C systems under consideration. We mainly use the Gray encoding, with truncation parameter

Fock operator	Encoded operator
$\|0\rangle\langle 0\|$	$0.5(I - Z_1)$
$\|1\rangle\langle 1\|$	$0.5(I - Z_2)$
$\|2\rangle\langle 2\|$	$0.5(I - Z_3)$
$\|3\rangle\langle 3\|$	$0.5(I - Z_4)$
$\|0\rangle\langle 1\| + \|1\rangle\langle 0\|$	$0.5(X_1X_2 + Y_1Y_2)$
$\|1\rangle\langle 2\| + \|2\rangle\langle 1\|$	$0.5(X_2X_3 + Y_2Y_3)$
$\|2\rangle\langle 3\| + \|3\rangle\langle 2\|$	$0.5(X_3X_4 + Y_3Y_4)$
$\|0\rangle\langle 2\| + \|2\rangle\langle 0\|$	$0.5(X_1X_3 + Y_1Y_3)$
$\|1\rangle\langle 3\| + \|3\rangle\langle 1\|$	$0.5(X_2X_4 + Y_2Y_4)$
$\|0\rangle\langle 3\| + \|3\rangle\langle 0\|$	$0.5(X_1X_4 + Y_1Y_4)$

Table D.4: Encoded operators for the one-hot encoding with $N = 4$. For the ladder operators, each term has its Hermitian conjugate added as well. This is because the Hamiltonian is Hermitian, leading to them having the same coefficient.

$N = 8$ ($n = 3$) and $N = 16$ ($n = 4$), and $K = 3$. For all Gray encoding simulations, we use $L = 4$ layers.

For gradient descent, we use a adaptive learning rate scheme. Every 10 iterations, fit a straight line of the last 10 cost function values. If the slope is negative, increase learning rate lr to $\min(1.05lr, lr_{\max})$. If the slope is positive, reduce learning rate lr to $\max(0.8lr, lr_{\min})$.

D.4 Simulation Details for n+α

We now provide specific simulation details for the different simulations in Tables D.10, D.11, and D.11 for the energy of the lowest $\frac{1}{2}^+$ orbit for the n+α optical potential derived *ab initio*. For all the simulations, we use the Gray encoding, with truncation parameter $N = 8$ ($n = 3$) and $N = 16$ ($n = 4$), and $K = 1, 2$. For all Gray encoding simulations, we use $L = 5$ layers.

Fock operator	Encoded operator
$\|0\rangle\langle 0\|$	$0.25(II + IZ + ZI + ZZ)$
$\|1\rangle\langle 1\|$	$0.25(II - IZ + ZI - ZZ)$
$\|2\rangle\langle 2\|$	$0.25(II + IZ - ZI - ZZ)$
$\|3\rangle\langle 3\|$	$0.25(II - IZ - ZI + ZZ)$
$\|0\rangle\langle 1\| + \|1\rangle\langle 0\|$	$0.5(IX + ZX)$
$\|1\rangle\langle 2\| + \|2\rangle\langle 1\|$	$0.5(XX + YY)$
$\|2\rangle\langle 3\| + \|3\rangle\langle 2\|$	$0.5(IX - ZX)$
$\|0\rangle\langle 2\| + \|2\rangle\langle 0\|$	$0.5(XI + XZ)$
$\|1\rangle\langle 3\| + \|3\rangle\langle 1\|$	$0.5(XI - XZ)$
$\|0\rangle\langle 3\| + \|3\rangle\langle 0\|$	$0.5(XX - YY)$

Table D.5: Encoded operators for the binary encoding with $N = 4$. For the ladder operators, each term has its Hermitian conjugate added as well. This is because the Hamiltonian is Hermitian, leading to them having the same coefficient.

For gradient descent, we use an adaptive learning rate scheme. Every 10 iterations, fit a straight line of the last 10 cost function values. If the slope is negative, increase the learning rate lr to $\min(1.05lr, lr_{\max})$. If the slope is positive, reduce the learning rate lr to $\max(0.8lr, lr_{\min})$.

Fock operator	Encoded operator
$\|0\rangle\langle 0\|$	$0.25(II + IZ + ZI + ZZ)$
$\|1\rangle\langle 1\|$	$0.25(II + IZ - ZI - ZZ)$
$\|2\rangle\langle 2\|$	$0.25(II - IZ - ZI + ZZ)$
$\|3\rangle\langle 3\|$	$0.25(II - IZ + ZI - ZZ)$
$\|0\rangle\langle 1\| + \|1\rangle\langle 0\|$	$0.5(XI + XZ)$
$\|1\rangle\langle 2\| + \|2\rangle\langle 1\|$	$0.5(IX - ZX)$
$\|2\rangle\langle 3\| + \|3\rangle\langle 2\|$	$0.5(XI - XZ)$
$\|0\rangle\langle 2\| + \|2\rangle\langle 0\|$	$0.5(XX - YY)$
$\|1\rangle\langle 3\| + \|3\rangle\langle 1\|$	$0.5(XX + YY)$
$\|0\rangle\langle 3\| + \|3\rangle\langle 0\|$	$0.5(IX + ZX)$

Table D.6: Encoded operators for the Gray encoding with $N = 4$. For the ladder operators, each term has its Hermitian conjugate added as well. This is because the Hamiltonian is Hermitian, leading to them having the same coefficient.

n+^{10}C		
N	Type	Details
8, 16 - Gray	Noiseless	$K = 1$ for 500 iterations followed by $K = 3$ for 500 iterations, both using SPSA. Lastly, $K = 3$ for 1000 iterations using gradient descent and a varying learning rate scheme.
	Shot Noise	Same as noiseless but using a shot based estimator for 10^3 shots.
	Noisy	$K = 1$ for 500 iterations using 10^3 shots, followed by $K = 3$ for 1500 iterations using 2×10^4 shots, both using SPSA. Cost function estimated using a fake IBMQ backend `ibm_manila`.

Table D.7: Simulation details for n+^{10}C **(Part 1)**. Plots shown in Fig. 5.11.

n+^{12}C		
N	Type	Details
8 - Gray	Noiseless	$K = 1$ for 500 iterations followed by $K = 3$ for 500 iterations, both using SPSA. Lastly, $K = 3$ for 1000 iterations using gradient descent and a varying learning rate scheme.
	Shot Noise	Same as noiseless but using a shot based estimator for 10^3 shots.
	Noisy	$K = 1$ for 500 iterations using 10^3 shots, followed by $K = 3$ for 1500 iterations using 2×10^4 shots, both using SPSA. Cost function estimated using a fake IBMQ backend `ibm_manila`.
16 - Gray	Noiseless	$K = 1$ for 500 iterations followed by $K = 3$ for 1000 iterations, both using SPSA. Lastly, $K = 3$ for 1500 iterations using gradient descent and a varying learning rate scheme.
	Shot Noise	Same as noiseless but using a shot based estimator for 10^3 shots.
	Noisy	$K = 1$ for 500 iterations using 10^3 shots, followed by $K = 3$ for 1500 iterations using 2×10^4 shots, both using SPSA. Cost function estimated using a fake IBMQ backend `ibm_manila`.

Table D.8: Simulation details for n+^{12}C **(Part 2)**. Plots shown in Fig. 5.12.

n+^{14}C		
N	Type	Details
8 - Gray	Noiseless	$K = 1$ for 500 iterations followed by $K = 3$ for 500 iterations, both using SPSA. Lastly, $K = 3$ for 1000 iterations using gradient descent and a varying learning rate scheme.
	Shot Noise	Same as noiseless but using a shot based estimator for 10^3 shots.
	Noisy	$K = 1$ for 500 iterations using 10^3 shots, followed by $K = 3$ for 1500 iterations using 2×10^4 shots, both using SPSA. Cost function estimated using a fake IBMQ backend `ibm_manila`.
16 - Gray	Noiseless	$K = 1$ for 500 iterations followed by $K = 3$ for 1000 iterations, both using SPSA. Lastly, $K = 3$ for 1500 iterations using gradient descent and a varying learning rate scheme.
	Shot Noise	Same as noiseless but using a shot based estimator for 10^3 shots.
	Noisy	$K = 1$ for 500 iterations using 10^3 shots, followed by $K = 3$ for 2500 iterations using 2×10^4 shots, both using SPSA. Cost function estimated using a fake IBMQ backend `ibm_manila`.
8 - OH	Noiseless	$K = 1$ for 500 iterations followed by $K = 3$ for 1500 iterations, both using SPSA.
	Shot Noise	Same as noiseless but using a shot based estimator for 10^3 shots.
	Noisy	$K = 1$ for 500 iterations followed by $K = 3$ for 1500 iterations, both using SPSA. Cost function estimated using a fake IBMQ backend `ibm_manila`.

Table D.9: Simulation details for n+^{14}C **(Part 3)**. Plots shown in Fig. 5.13 for n+^{14}C Gray, and Fig. 5.14 for n+^{14}C OH.

$\hbar\omega = 12$, $N = 8$		
K	Type	Details
1	Noiseless	$K = 0$ for 500 iterations using SPSA, followed by $K = 1$ for 500 iterations using gradient descent and a varying learning rate scheme.
	Shot Noise	Same as noiseless but using a shot based estimator for 10^5 shots.
	Noisy	$K = 0$ for 500 iterations using 10^3 shots, followed by $K = 1$ for 500 iterations using 10^5 shots, both using SPSA. Cost function estimated using a fake IBMQ backend `ibm_manila`.
2	Noiseless	$K = 0$ for 500 iterations, $K = 1$ for 500 iterations, followed by $K = 2$ for 500 iterations, all using SPSA, followed by $K = 2$ for 500 iterations using gradient descent and a varying learning rate scheme.
	Shot Noise	Same as noiseless but using a shot based estimator for 10^5 shots.
	Noisy	$K = 0$ for 500 iterations using 10^3 shots, $K = 1$ for 500 iterations using 10^3 shots, followed by $K = 2$ for 500 iterations using 10^5 shots, all using SPSA. Cost function estimated using a fake IBMQ backend `ibm_manila`.

Table D.10: Simulation details for n+α. Plots shown in Fig. 5.15.

$\hbar\omega = 12$, $N = 16$		
K	Type	Details
1	Noiseless	$K = 0$ for 500 iterations, $K = 1$ for 1000 iterations, both using SPSA, followed by $K = 1$ for 1000 iterations using gradient descent and a varying learning rate scheme.
	Shot Noise	$K = 0$ for 500 iterations, $K = 1$ for 500 iterations, both using SPSA, following by $K = 1$ for 1500 iterations using gradient descent and a varying learning rate scheme. All estimations use 10^5 shots.
	Noisy	$K = 0$ for 1000 iterations using 10^3 shots, followed by $K = 1$ for 1500 iterations using 10^5 shots, both using SPSA. Cost function estimated using a fake IBMQ backend `ibm_manila`.
2	Noiseless	$K = 0$ for 500 iterations, $K = 1$ for 500 iterations, $K = 2$ for 1000 iterations, all using SPSA, followed by $K = 2$ for 1000 iterations using gradient descent and a varying learning rate scheme.
	Shot Noise	$K = 0$ for 500 iterations, $K = 1$ for 500 iterations, $K = 2$ for 500 iterations, all using SPSA, following by $K = 2$ for 1500 iterations using gradient descent and a varying learning rate scheme. All estimations use 10^5 shots.
	Noisy	$K = 0$ for 500 iterations using 10^3 shots, $K = 1$ for 500 iterations using 10^3 shots, $K = 2$ for 500 iterations using 10^3 shots, followed by $K = 2$ for 500 iterations using 10^5 shots, all using SPSA. Cost function estimated using a fake IBMQ backend `ibm_manila`.

Table D.11: Simulation details for n+α. Plots shown in Fig. 5.16.

$\hbar\omega = 16$, $N = 8$		
K	Type	Details
1	Noiseless	$K = 0$ for 500 iterations using SPSA, followed by $K = 1$ for 500 iterations using gradient descent and a varying learning rate scheme.
	Shot Noise	Same as noiseless but using a shot based estimator for 10^5 shots.
	Noisy	$K = 0$ for 500 iterations using 10^3 shots, followed by $K = 1$ for 500 iterations using 10^5 shots, both using SPSA. Cost function estimated using a fake IBMQ backend `ibm_manila`.
2	Noiseless	$K = 0$ for 750 iterations, $K = 1$ for 750 iterations, followed by $K = 2$ for 750 iterations, all using SPSA.
	Shot Noise	Same as noiseless but using a shot based estimator for 10^5 shots.
	Noisy	Same as noiseless, but using a fake IBMQ backend `ibm_manila` with 10^3, 10^3, and 10^5 shots for $K = 0, 1, 2$, respectively, to estimate expectation values. Cost function estimated using a fake IBMQ backend `ibm_manila`.

Table D.12: Simulation details for n+α. Plots shown in Fig. 5.17.