Estimating Distinguishability Measures on a Quantum Computer

Rochisha Agarwal[1], **Soorya Rethinasamy[2]**, Kunal Sharma[3,4], Mark M. Wilde[2]

[1]Department of Physics, Indian Institute of Technology Roorkee, Roorkee, Uttarakhand, India
[2]Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, and Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA
[3]Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, Maryland 20742, USA
[4]IBM Quantum, IBM T. J. Watson Research Center, Yorktown Heights, NY 10598, USA

Objectives

- We propose algorithms for estimating Fidelity of Channels and Diamond Distance on quantum computers.
- The acceptance probability of some of these algorithms is equal to the optimal probability that an all-powerful prover can convince a verifier to accept.
- We replace the all-powerful prover with a parameterized quantum circuit

Introduction

- Measuring performance of any protocol relies on distinguishing the protocol from the ideal case.
- Two commonly employed distinguishability measures are diamond distance & fidelity of channels.
- Both can be computed by means of semi-definite programming, so that they can be estimated accurately with a runtime that is polynomial in the dimension of the channels.
- The algorithms in this work rely on interaction with a quantum prover, in which case they are not necessarily efficiently computable even on a quantum computer.
- However, by replacing the quantum prover with a parameterized circuit, it is possible in some cases to estimate these quantities reliably.

Quantum Interactive Proofs

An interactive game involving two players, a prover and a verifier, who exchange fixed-size quantum registers for a fixed number of steps. At the end of the steps, the verifier produces a single classical bit indicating whether he accepts the input. Figure 1 is an example of a five-message quantum interactive proof.

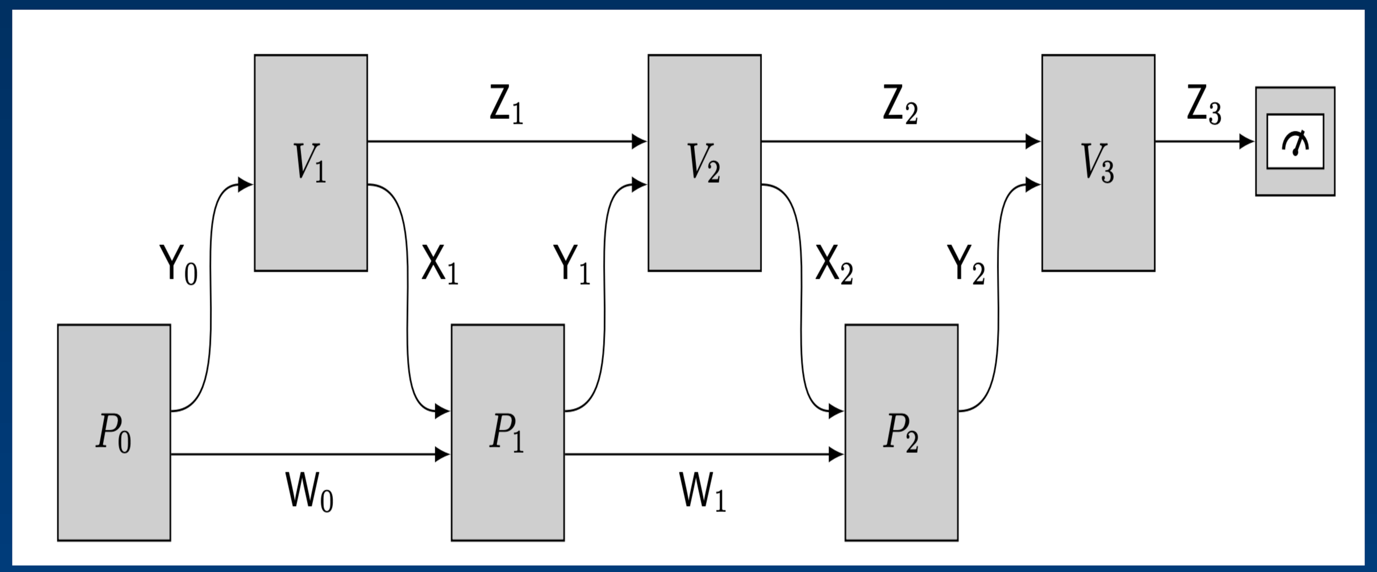


Figure 1: An example of a quantum interactive proof with five messages exchanged between the prover and receiver.

In a quantum interactive proof, the verifier is constrained to be computationally bounded. The verifier's actions are represented by quantum circuits whose descriptions can be generated in polynomial time from the problem input. No such restrictions are placed on the prover, who is computationally unbounded.

Fidelity of Channels

- Given two channels $\mathcal{N}^0_{A\to B}$ and $\mathcal{N}^1_{A\to B}$, the fidelity of the channels is given by

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

- We are given access to unitary extensions of the channels

$$\mathcal{N}^i_{A\to B}(\omega_A) = \mathrm{Tr}_E(U^i(\omega_A \otimes |0\rangle\langle 0|)(U^i)^\dagger)$$

- We propose a competing-prover interactive proof to estimate the fidelity of channels.

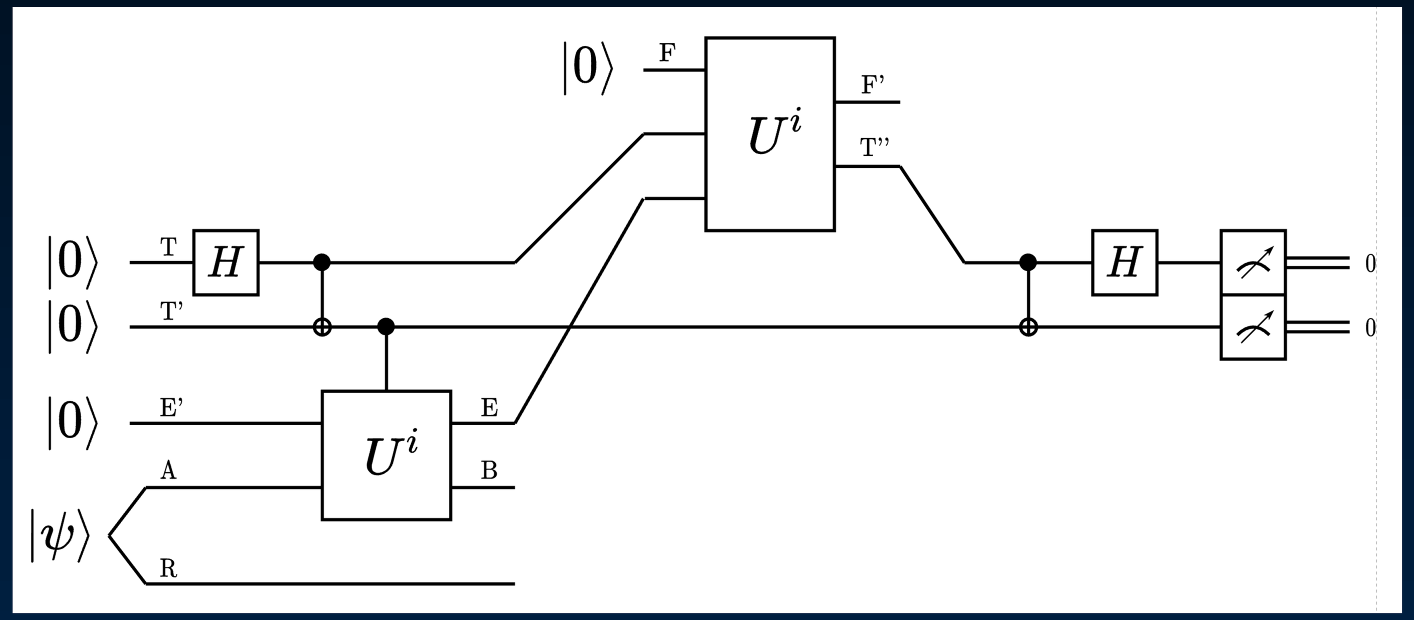


Figure 2: Algorithm to estimate the Fidelity of Channels.

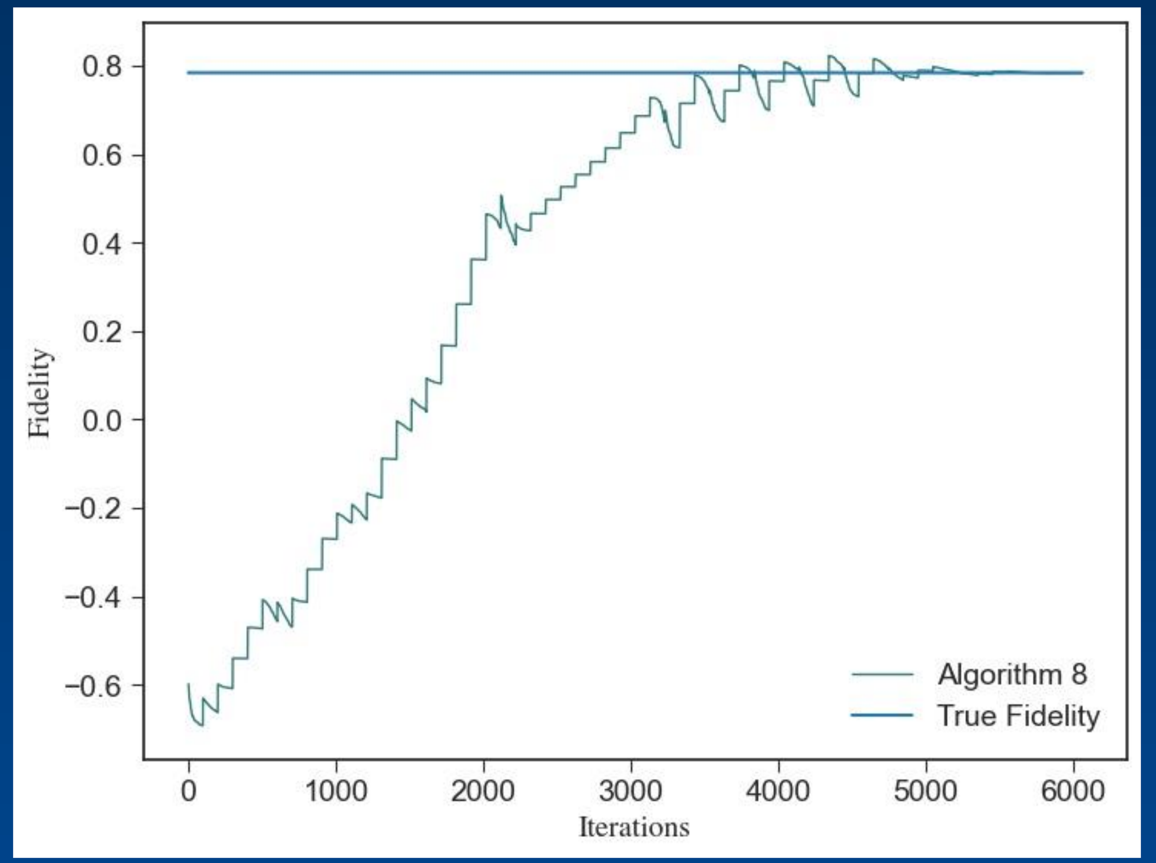
- The acceptance probability is thus,

$$p_{\mathrm{acc}} = \min_{|\psi\rangle_{RA}} \max_{P} \frac{1}{2} \left\| \langle \Phi|_{T''T} P \sum_{i\in\{0,1\}} |ii\rangle_{T'T} U^i |\psi\rangle_{RA} |00\rangle_{E'F} \right\|_2^2$$

- Expanding and simplifying,

$$p_{\mathrm{acc}} = \frac{1}{2}\left(1 + \sqrt{F}(\mathcal{N}^0_{A\to B}, \mathcal{N}^1_{A\to B})\right)$$

- We simulate the algorithm on local machines with no noise and find that the algorithm converges to the known fidelity with an absolute error of 10^{-4} in 6000 iterations.



Diamond Distance

- Given two channels $\mathcal{N}^0_{A\to B}$ and $\mathcal{N}^1_{A\to B}$, the diamond distance of the channels is given by

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

- We are given access to unitary extensions of the channels

$$\mathcal{N}^i_{A\to B}(\omega_A) = \mathrm{Tr}_E(U^i(\omega_A \otimes |0\rangle\langle 0|)(U^i)^\dagger)$$

- We propose a quantum interactive proof to estimate the diamond distance of channels.

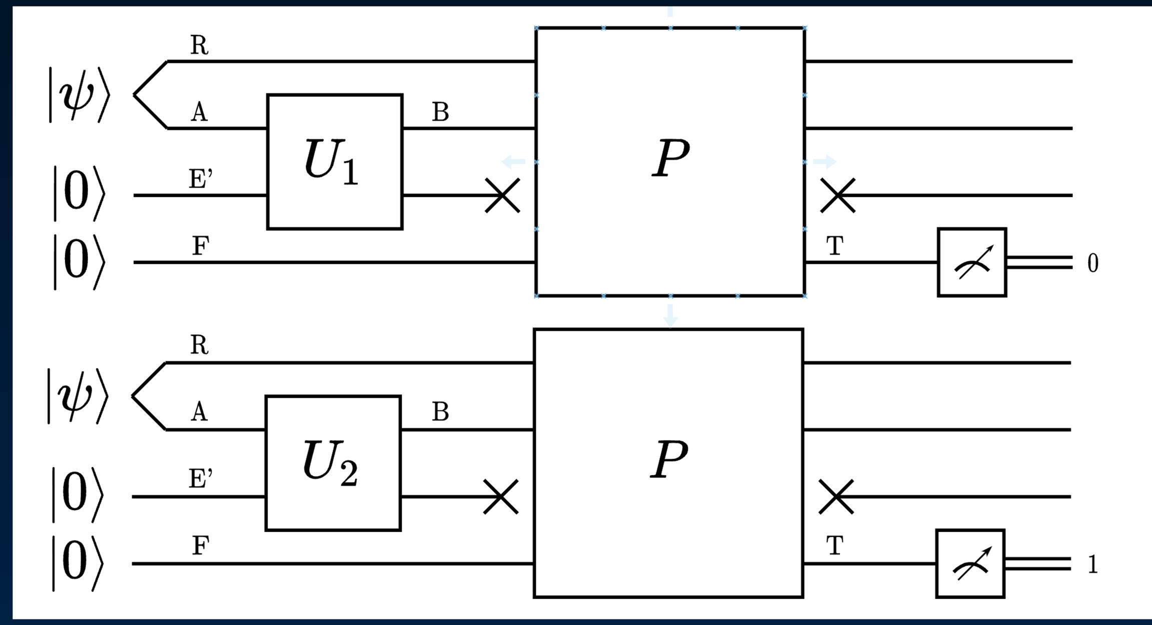
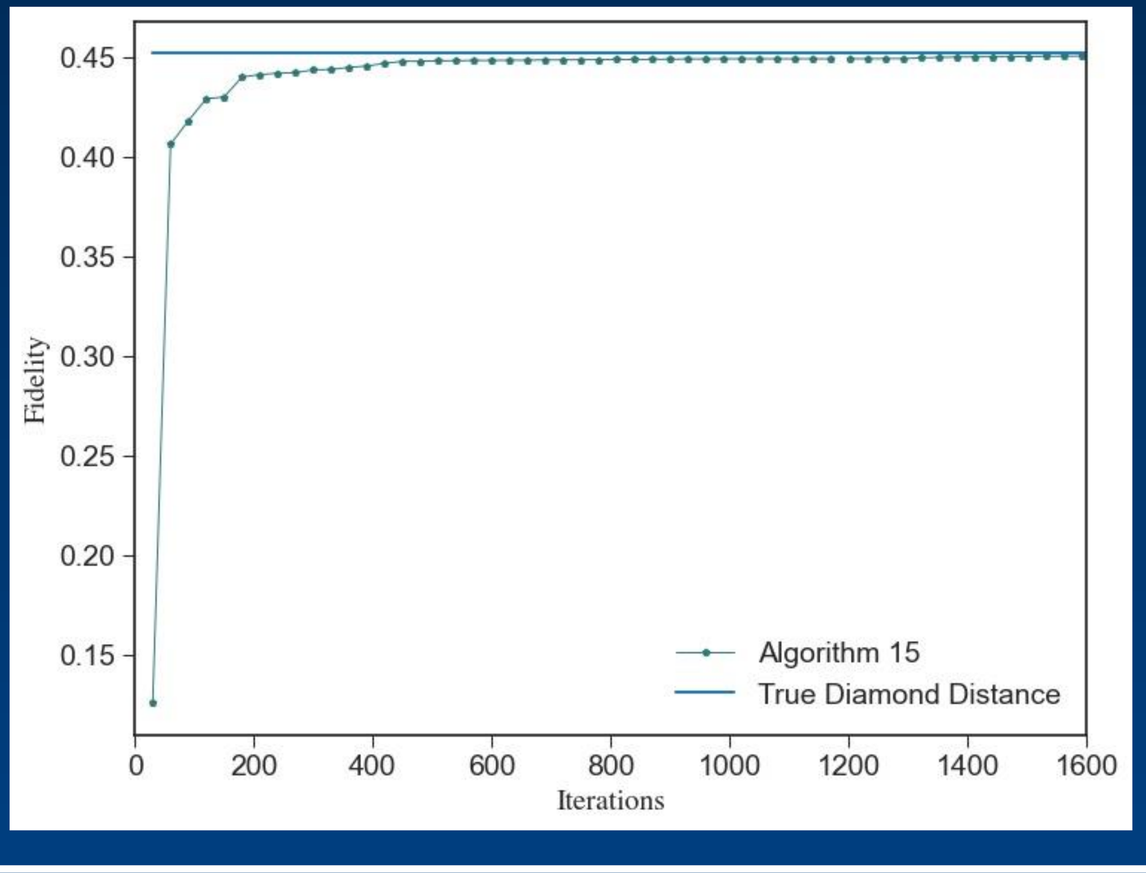


Figure 3: Algorithm to estimate the Diamond Distance of Channels.

- The acceptance probability can be expressed as

$$p_{\mathrm{acc}} = \frac{1}{2}\left(1 + \frac{1}{2}\left\|\mathcal{N}^0_{A\to B} - \mathcal{N}^1_{A\to B}\right\|_\diamond\right)$$

- We simulate the algorithm on local machines with no noise and find that the algorithm converges to the known diamond distance with an absolute error of 10^{-4} in 2000 iterations.



Acknowledgements

The authors would like to thank Elliott Ball, Dhrumil Patel, Zoe Holmes, Aliza Siddiqui, and Margarite LaBorde for discussions.