Algorithms for a Scalable Quantum Computer
Optimal Pulse Sequences, Montgomery Factoring, and Bayesian Inference

Guang Hao Low, Rich Rines, Theodore Yoder, Isaac Chuang

Introduction

Quantum computers promise speedups to a whole host of classical algorithms, from exponential advantage in factoring to a plethora of polynomial advantages in machine learning tasks. However, as the size of the problem grows, the quantum circuit required to solve it also grows, and small errors in single gates add to have a substantial effect on the output. Scaling up a quantum computer therefore requires either simplifying the circuits or reducing errors. To that end, we present open-loop error correction for single-qubit gates in the form of pulse sequences of optimal length. We also show how to reduce the circuit for Shor’s algorithm using the Montgomery product from number theory, bringing the factoring of 35 within experimental grasp. Finally, we demonstrate how a Bayesian inference task can be performed with polynomial advantage on a scalable quantum computer.

Optimal Pulse Sequences

Say that we wish to perform a single-qubit rotation $R_\theta[\phi]$ by angle $\theta$ around the axis $\sigma_\phi = X \cos \phi + Y \sin \phi$ but we only have access to a faulty operation $M_\theta[\phi] = R_\theta[\phi(1+\varepsilon)]$ which over- or under-rotates by a factor $\varepsilon$. In the presence of these amplitude errors, how can we perform $R_\theta[\phi]$ accurately?

The answer comes from the non-commutativity of single-qubit operations which allows us to chain faulty pulses in sequence such that

$$U_\theta[\phi] = \prod_{j=1}^{L} M_{\theta_j}[\phi_j] : M_0[\theta] = R_\theta[\phi] + O(\varepsilon^{n+1}).$$

The dependence of $L$ on $n$ that is implicit in this equation is crucial. We prove that $L > n$ and argue that $L = 2n$ is achievable. This is in contrast to the best sequences for arbitrary $\varepsilon \neq 0/2\pi$, which scale as $L = O(n^{10})^1$.

Solving for Sequences

The symmetries $\varepsilon = i^{\phi} + i(2\phi - \gamma j)$ result in $I_{\varepsilon}^\phi \varepsilon_{j} = 0$ for $j$ even (odd) and the resulting sequences are called initial PD (AP). All such sequences have $L = 2n$.

We introduce three techniques for solving (2):

- Analytical: The substitution $\phi_k = \tan(\phi_k/2)$ converts (2) into a system of polynomial equations, which can be solved by Groebner bases to yield $\gamma_1, 2, 3$ and $\gamma_{24}, 4$.
- Perturbative: Given a solution at $\gamma_0$ and non-zero Jacobian $\mathcal{J}_{\gamma_0}[\gamma]$, solutions $\gamma_0[\gamma]$ can be obtained. For a certain AP sequence $\gamma_0 = 0$ and we prove a non-zero Jacobian at 0.
- Numerical: We use Mathematica [2] to find roots to equation (2) up to $n = 12$.

Bibliography


The authors acknowledge the support of the NSF CUA, NSF iQuISE IGERT, IARPA QCS ORAQL, and NSF CCF-RQCC projects.