QI: Integer Computation: Factoring, Multiplication

Gregory Croisdale, Cade Brown, and Rebecca Ryan May 5, 2020

Abstract

In this paper, we will discuss some of the historically important quantum algorithms,

Introduction

Implementation of Shor's Algorithm for Factoring Integers

Shor's algorithm is perhaps one of the most anticipated quantum algorithms, for the risk it poses to encryption (see below in the document), as well as the interesting result that drastically improves the computational complexity of integer factorization, a very interesting problem.

This algorithm will be interesting to implement, because it uses elements such as QFT, as well as partial computation on classical and quantum systems, which combine to solve the problem in polynomial time $O((\log n)^2(\log\log n)(\log\log\log n)$.

While probabilistic algorithms already exist for primality testing on classical computers, finding out which numbers divide another number is still a very hard to solve problem using solely classical computers.

Shor's algorithm: https://qudev.phys.ethz.ch/static/content/QSIT15/Shors%20Algorithm.pdf

Presentation

We will visually demonstrate the fastest classical computing methods to the aforementioned problems in both a Jupyter notebook and an HTML5 website for easy accessibility. We will animate the algorithms using Google Charts and a small input.

All algorithms will be fully explained with interesting applications and potential set-backs. The Jupyter notebook versions will be fully interactive for any input the reader wants to insert. The work will be organized on the GitHub repository github.com/gcrois/QFastInteger.