15-459: Undergraduate Quantum Computation August 30, 2022

Lecture 1 : Introduction

Lecturer: Ryan O'Donnell

Scribe: Rajeev Godse

1 Motivations

1.1 Computational Efficiency

Are quantum computers more powerful than classical computers?

- For what tasks?
- Near-term possibility of demonstrating the difference?

1.2 Physical and unphysical numbers

Numbers are traditionally used for counting physical objects, but even compact numbers get really big really quickly.

For example, there are only 10^{80} particles in the universe, but you can easily write down a bigger number.

Numbers greater than this cannot correspond to counting physical objects like tennis balls or even particles, so computations on them correspond more to computational puzzles or games.

2 Computational Challenges

Challenge 1: multiply two 500-digit numbers

Grade school algorithm: $\approx n^2$ steps, where $n = 500$ is the length of the numbers.

Schoenhage-Strassen algorithm: $\approx n$ steps ($O(n \log n \ldots)$) due to Fast Fourier Transform.

Challenge 2: find a prime factor of a 500-digit number, if one exists.

Grade school algorithm (check divisibility by all factors up to $\sqrt{N}$), has $\approx \sqrt{10^n} = 10^{n/2} \approx 3^n$.

There is a faster algorithm, due to Pollard, with about $10^{3\sqrt[3]{n}}$.

Hardness of factorization is important to cryptography.

Challenges to factor big numbers have exists for decades, but the best we have done is on 250 bits.

Accordingly, the fastest algorithm *we know* for factorization is not efficient, but we don't know if there exists an efficient algorithm.

In fact, Peter Shor showed in 1994 that a quantum computer could factor n-bit numbers in $\approx n^2$ steps.

Shor got many ideas for his proof from the young cryptographer Dan Simon, whose paper Shor's committee rejected. Simon knew little physics and approached the problem theoretically: "I wanted to show that this additional (apparently implementable) function of a quantum computer was useless. But I found that 'rotate, compute, rotate' was pretty powerful."

3 Quantum Computers

3.1 Quantum Mechanics

Given 1000 electrons/photons/..., their joint "state" is defined by 2^{1000} numbers ("amplitudes"), stored very compactly by nature.

Umesh Vazirani: "The goal of quantum computing is to hack into nature's computer."

Many Worlds Interpretation

Hugh Everett, in 1956/1957. Everett was advised by Tucker, a game theorist. Tucker also advised Minsky (pretty famous), who advised Manuel Blum (pretty famous), who advised Vazirani (aforementioned), who advised Ryan O'Donnell's advisor.

Everett was also advised by Wheeler, a physicist, who advised Feynman, Deutsch, and Griffiths.

Per Deutsch, quantum computations represent operations done in parallel in parallel universes.