Quantum Turing Machines

CSCI5444

Patrick Cooper

January 20, 2022

University of Colorado Boulder

Computer Science
UNIVERSITY OF COLORADO **BOULDER**

Outline

Quantum Computing Introduction

Quantum Computation

The conceptual core of quantum computation is the generalization of the laws of probability to allow for minus signs and complex numbers.

Quantum Computation

Quantum mechanics is like probability but operates on a 2-norm instead of a 1-norm. In other words instead of a vector where the entries sum to 1, we now want a vector (α, β) where $\alpha^2 + \beta^2 = 1$ and α^2 is the probability of some outcome 0 and β^2 is the probability of some outcome 1. This "2-norm bit" is called a **qubit**.

Quantum Computation

Given these *qubits* we can transform them by applying any two-by-two unitary matrix to arrive at the effect of quantum interference. Destructive and Constructive Interference allow quantum algorithms to be constructed and run.

Quantum Mechanics Meets Computer Science

Quantum mechanics is the operating system that other physical theories run on as application software. - Scott Aaronson

Quantum Computing involves using continuous phenomena to answer questions about discrete entities.

But Are They Useful?

The original conception of Quantum Computers was the simulation of Arbitrary Physical Systems.

Pseudorandom Permutations (PRPs), can be designed around phenomena which are difficult to solve with a Quantum Computer.

Quantum Complexity

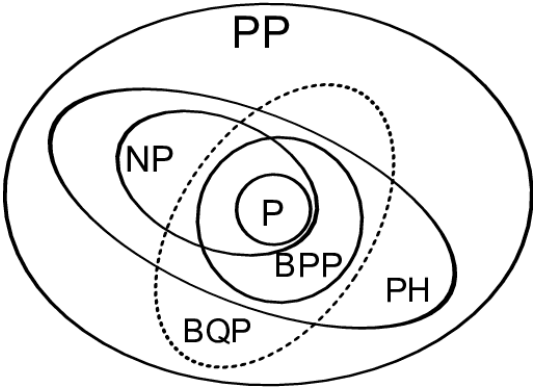
BPP vs. BQP

BPP (Bounded-Error Probabilistic Polynomial-Time) is the class of computational problems that are efficiently solvable in the physical world if classical physics is true. Acceptance is probabilistic. (Lautemann)

BQP (Bounded-Error Quantum Polynomial-Time) is the class of computational problems that are efficiently solvable in the physical world if quantum physics is true.

Quantum Complexity in an Image

NOTE: This graph is no longer correct. The oracle separation of BQP and PH has been established.



Constructing BQP

1. Initialization: We need a system consisting of n quantum bits (or qubits), and these are initialized to some simple state. That is, we need an input string x along with a collection of ancilla qubits.
2. Transformations: We are only interested in unitary transformations that can be built up by composing a small number of quantum gates.
3. Measurement: We need to know when our computation is done. We repeat the the computation a suitable number of times and then output the majority answer in accordance with our selected probabilities.
4. Uniformity: There is an infinite family of circuits, one for each input length n. This means there must be a classical algorithm that given some n as input, outputs the nth quantum circuit in time polynomial in n.

BQP Definition

BQP is the class of languages $L \subseteq \{0,1\}^*$ for which there exists a uniform family of polynomial-size quantum circuits, $\{C_n\}$ such that for all $x \in 0,1^n$:
1. if $x \in L$, then C_n accepts input $|x^?|0...0^?$ with probability at least $\frac{2}{3}$.
2. if $x \notin L$, then C_n accepts input $|x^?|0...0^?$ with probability at most $\frac{1}{3}$.
(Bernstein)

Relationship to Classical Complexity

$BPP \subseteq BQP$: Everything that can be done on a classical computer may be done on a quantum computer.

$BQP \subseteq EXP$: Everything that can be done on a quantum computer can be done on a classical computer in exponential time, because a classical computer can simulate the whole evolution of the state vector.

A Wider BQP Class

Remove the unitary restriction, and we arrive at AWPP (stands for Almost-Wide Probabilistic Polynomial-time).

This class has many interesting properties in its own right.

$AWPP \subseteq PP \subseteq PSPACE$

We have the corollary $BQP \subseteq PP \subseteq PSPACE$
(Fortnow)

No proof exists for $NP \neq BQP$ because we cannot prove $P \neq NP$.

Even if we had $P \neq NP$, we do not know how to demonstrate $NP \neq BQP$.

The Big Ideas

Quadratic Speedup

The reason we get a quadratic speedup is that quantum mechanics is based on the 2-norm rather than the 1-norm.

If there are N solutions, only one of which is right. We have a $\frac{1}{N}$ chance of guessing correctly on our first try and we need N to have a nonnegligible probability.

Alternatively, our quantum solution applies linear transformations to vectors of amplitudes. So after one guess we have $\frac{1}{\sqrt{N}}$ chance of being correct, and we only need T queries to be nonnelgibly close or $T \approx \sqrt{N}$ queries. (Aaronson)

Where Does All This Power Come From?

Suppose we factor a massive digit integer using a quantum computer. Where exactly does this computation take place? Some suggest, it most arise from a sort of “multiverse.”

This makes the assumption that our computation BPP is not in BQP.

The Preferred Basis Problem

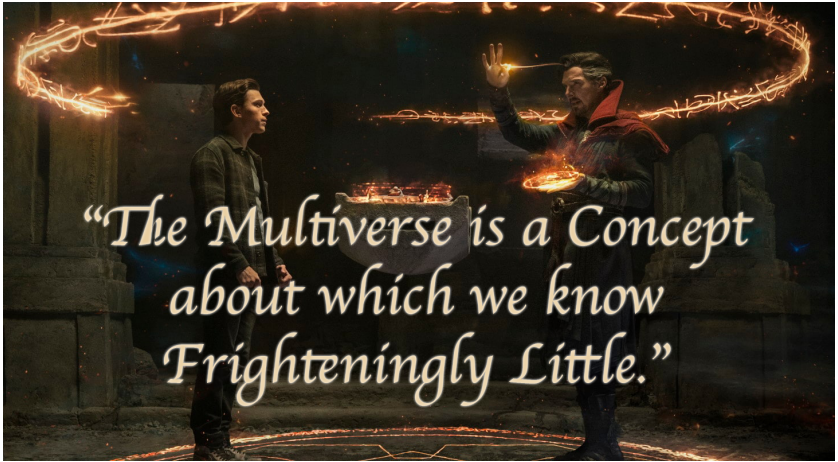
Where does the split between universes occur? There are an infinite number of ways to “split up” quantum states, so what might determine a valid arrangement?

Physicists and Philosophers disagree on the exact definition of the problem, let alone the solution.

We can say that the universes collaborate through combination.

We can be sure they do not simultaneously try every possibility.

Meme Time


"The Multiverse is a Concept
about which we know
Frighteningly Little."

Resources

Scott Aaronson

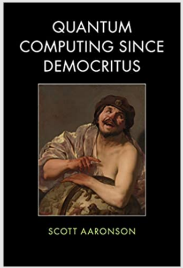
Scott Aaronson is a quantum computing theorist and outspoken proponent of quantum computing. His work is a fascinating collision of computing, physics, math, and philosophy.

Classical Scott

Scott Aaronson

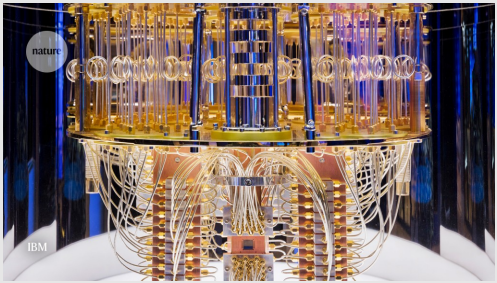
Covers the relationship between discrete and continuous interpretations of quantum computing, the epistemology of quantum phenomena, how number theory, Cantor's Theorem, and other discoveries shaped the evolution of quantum computing. Discusses new possibilities surrounding supercomputation.

Scott's Book



Demonstrations of quantum supremacy, do not solve useful problems per say. For the time being they involve outputting a verifiable distribution in a superior manner to a classical computer.

Quantum Scott



Some Remarkable Publications

- Aaronson, S. (2018). Quantum Computing Since Democritus. Cambridge: Cambridge University Press.
- Bernstein, E. (1997), Quantum Complexity Theory. SIAM Journal on Computing, 26(5). doi: 1411–1473
- Fortnow, L. (2003). One complexity theorists view of quantum computing. Theoretical Computer Science, 292(3), 597-610. doi:10.1016/s0304-3975(01)00377-2
- Lautemann, C. (1983). BPP and the polynomial hierarchy. Information Processing Letters, 17(4), 215-217. doi:10.1016/0020-0190(83)90044-3

Watch Devs

Thank You

Questions?