Quantum and Post-Quantum Cryptography

Notes on Chapter 14

Jeffrey Goldberg
jeffrey@goldmark.org

May 5, 2022
Last revised May 8, 2024

No math today

Physics is all Linear Algebra and Differential Equations.

T. Goldberg (2022)

I suck at Linear Algebra and Differential Equations.

J. Goldberg (2022)

Complexity classes (again)

Complexity in terms of machines

- A problem is in **P** if it can be solved in polynomial time on a deterministic Turing machine (DTM).
- A problem is in **NP** if it can be solved in polynomial time on a non-deterministic Turing machine (NTM).
- A problem is in **BQP** if it can be probabilistically solved in polynomial time on a quantum Turing machine. (QTM)

- A problem is in **P** if it can be solved in polynomial time on a deterministic Turing machine (DTM).
- A problem is in **NP** if it can be solved in polynomial time on a non-deterministic Turing machine (NTM).
- A problem is in **BQP** if it can be probabilistically solved in polynomial time on a quantum Turing machine. (QTM)

1. “Non-derministic“ here doesn’t mean probabilistic. (There is also something called a probabilistic Turing machine (PTM)). It means that the machine is capable of making correct guesses of a certain sort.
2. An algorithm running on a BQP needs to give the correct answer most of the time. But it does not need to give the correct answer all of the time.
3. I chose earlier to teach about major complexity classes in terms other than machines, but now I have to. And so here we are.

Abstracting machine details

Consider the following variants of physical DTM.

- The read/write tape has a start point and is arbitrarily long in just one direction.
- The read/write tape is arbitrarily long in both directions.
- There are two tapes.
- Instead of a tape, there is a two dimensional grid.

What is in $\mathcal{O}(n^3)$ in one variant may be in $\mathcal{O}(n)$ in another variant.

Poly is stable

Although the complexity can vary depending on the details of the DTM, if some problem is in P on any DTM, there is a polynomial time algorithm for it on all DTMs.

Although the complexity can vary depending on the details of the DTM, if some problem is in **P** on any DTM, there is a polynomial time algorithm for it on all DTMs.

1. This is why we draw a big line between polynomial and non-polynomial, while we don't draw a big line between linear, $\mathcal{O}(n)$ and cubic, $\mathcal{O}(n^3)$.
2. I didn't lie when I said "no math". I meant that I wouldn't be introducing math we haven't already done.

Quantum Computers

All computers are quantum, but some are more quantum than others.

All computers are quantum, but some are more quantum than others.

1. Creating and designing transistors relies deeply on quantum physics. And chips are lots of transistors wired together in a very small space.
2. But tranistors do not exhibit quantum properties. They are good for storing bits, not qubits.

"Quantum computers promise more computing power because with only n qubits, the can *process* 2^n numbers." [Aum17, p. 255]

BIT VERSUS QUBIT

- n bits can store one of 2^n values.
- n qubits can do stuff with up to 2^n values.

This quote is signifcant

Unitary matrices (and quantum gates by definition) are invertible, meaning that given the result of an operation, you can compute back to the original qubit by applying the inverse matrix. [Aum17, p. 257]

This quote is signifcant

Unitary matrices (and quantum gates by definition) are invertible, meaning that given the result of an operation, you can compute back to the original qubit by applying the inverse matrix. [Aum17, p. 257]

1. Just because that quote is signifcant, that doesn't mean it is easy to understand.
2. Next slide please!

It's deterministic

Fully deterministic

Quantum mechanics is fully deterministic.

Fully deterministic
Quantum mechanics is fully deterministic.

1. We will get to quantum non-determinism, but that happens later.

Interference

"When you make a measurement, there's a rule for converting these amplitudes into ordinary probabilities. But when you're not looking, the amplitudes ... well, sometimes they do something very special and private with each other. Something very ... intimate." [AW16]

Simon's Problem

The problem

Definition 1 (Simon's Problem)

Given a function $f(\cdot)$ whose input is a string of n bits and whose output is a string of n bits, there may be a string of n bits, m, such that

- If $f(x) = f(y)$ then either $x = y$ or $x \oplus y = m$;
- And, if $x \oplus y = m$ then $f(x) = f(y)$.

Answer whether such an m exists and what it is if it does exist.

Definition 1 (Simon's Problem)

Given a function $f(\cdot)$ whose input is a string of n bits and whose output is a string of n bits, there may be a string of n bits, m, such that

- If $f(x) = f(y)$ then either $x = y$ or $x \oplus y = m$;
- And, if $x \oplus y = m$ then $f(x) = f(y)$.

Answer whether such an m exists and what it is if it does exist.

1. That could be written much more concisely if I'd taught you all more notation.
2. But notation aside, getting the intuition for what the problem is is not easy.
3. Maybe I did lie when I said there would be no math, but you are absolutely free to switch this off. I only want to get the very broadest notion of the role of this problem across.

Simon says

- Daniel Simon called it “Is a function invariant under some xor-mask?” [Sim97, §3]
- We are not going to even attempt to go through Simon’s algorithm;
- Simon says, the problem is exponential on a probabilistic Turing machine;
- Simon says, the problem is polynomial (with bounded error) on a quantum Turing machine;
- I say it is good to get a feel for the problem because it gives a sense of the kinds of things that quantum computers can do.

Simon says

- Daniel Simon called it "Is a function invariant under some xor-mask?" [Sim97, §3]
- We are not going to even attempt to go through Simon's algorithm;
- Simon says, the problem is exponential on a probabilistic Turing machine;
- Simon says, the problem is polynomial (with bounded error) on a quantum Turing machine;
- I say it is good to get a feel for the problem because it gives a sense of the kinds of things that quantum computers can do.

1. Seriously, I feel like I understand this stuff conceptually, but I suck at Linear Algebra.
2. Indeed, every time I fail to grasp an eigenvalue, my sense of self-worth takes a hit.
3. Just because we aren't doing the math, doesn't mean you don't have to endure obscure math puns. My comment about eigenvalues was one.
4. Simon not only says these things, but he proves them.
5. Simon would almost certainly say not to do the whole "Simon says" thing.

Classically

In a classical world, you need to query the function f on the order of 2^n times to be a able to have high confidence that the xor-mask, m, exists. You can do so probabilistically, but it is with classical probabilities.

Quantumly

- Solving the problem can be recast as exploring a $n-1$ layer decision tree with n branches.
- In the classical system, each transition in the tree has a probability.
- In a quantum system, each transition in the tree has an *amplitude*.
- A magic step is performed at each layer
- The amplitudes at each node interfere with the others.
- In some cases such interference can make a branch certain or can make a branch impossible.
- After n steps only those nodes that are certain remain.
- Those amplitudes can be converted to probabilities of 0 or 1 which can be transformed into a solution of n bits.

Quantumly

- Solving the problem can be recast as exploring a $n-1$ layer decision tree with n branches.
- In the classical system, each transition in the tree has a probability.
- In a quantum system, each transition in the tree has an *amplitude*.
- A magic step is performed at each layer
- The amplitudes at each node interfere with the others.
- In some cases such interference can make a branch certain or can make a branch impossible.
- After n steps only those nodes that are certain remain.
- Those amplitudes can be converted to probabilities of 0 or 1 which can be transformed into a solution of n bits.

1. I've read textbook sections on the magical step, worked through the toy examples, read Simon's description of it. And I still don't grok it.
2. I will need to make my kid read it and then explain it to me.

Maintaining the magic

No classical interactions can happen except at the very beginning and at the very end. Everything in the middle must maintain the entanglement of the entire problem. So this requires $n-1$ quantum operations on n *logical* qubits. Thus

- Running Simon's algorithm requires $2n$ logical qubits
- The $2n$ qubits must remain entangled through $n-1$ operations

Many qubits per logical qubit

Algorithms of the sort described require something called quantum error correction. And that means that you need lots of physical qubits per logical qubit.

Algorithms of the sort described require something called quantum error correction. And that means that you need lots of physical qubits per logical qubit.

1. For those who tuned out during talk of Simon's problem, it's time to tune back in.

Random or deterministic?

- I said that quantum processes are fully deterministic,
- We all know that quantum processes lead to inherent randomness,
- It is when the quantum state docoheres that the randomness comes in,
- Decoherence turns deterministic and reversible quantum states into ordinary probabilities.

Decoherence

- Copenhagen (Niels Bohr and students) interpretation was “observation causes decoherence.”
- Erwin Schrödinger was *mocking* the Copenhagen interpretation of decoherence with the cat in the box thing.
- The standard view (most of 20th century) is ”just do the math, and don’t try to give it an interpretation.”
- Huge Everett: The math is describing reality, and we should take it at face value. The universe splits into Many Worlds when states become so different that they can’t interfere with each other.
- David Deutsch: If we take Everett seriously, it gives us a model for designing quantum computers.

Decoherence

- Copenhagen (Niels Bohr and students) interpretation was "observation causes decoherence."
- Erwin Schrödinger was *mocking* the Copenhagen interpretation of decoherence with the cat in the box thing.
- The standard view (most of 20th century) is "just do the math, and don't try to give it an interpretation."
- Huge Everett: The math is describing reality, and we should take it at face value. The universe splits into Many Worlds when states become so different that they can't interfere with each other.
- David Deutsch: If we take Everett seriously, it gives us a model for designing quantum computers.

1. Roger Penrose: decoherence happens when the difference between states exceeds Plank's constant. Also, consciousness is mysterious and so is quantum stuff, so quantum mystery is the source of consciousness.
2. Also Penrose: I say silly things about Gödel's Incompleteness theorem and the minds of mathematicians despite being a genuinely very smart mathematical physicist.
3. Bohm: [Nope. Let's not open that can of hidden variables.]

Quantum advantage and quantum cryptanalysis

Quantum advantage and quantum cryptanalysis

Quantum Advantage

Quantum advantage

Definition 2 (Quantum Advantage)

A system demonstrates quantum advantage if it performs a computation that no non-quantum system in existence could perform in any feasible amount of time.

Definition 2 (Quantum Advantage)

A system demonstrates quantum advantage if it performs a computation that no non-quantum system in existence could perform in any feasible amount of time.

1. You might hear this referred to as “quantum supremecy” in older discussion.

The problem needn't be useful

All systems to date (and in the near future) aiming to demonstrate quantum advantage construct the problem of "simulating a quantum computer circuit." The QC simulates by being one, while the classical computation problem requires an actual simulation.

Answers must be checkable

The problems used to demonstrate quantum advantage must be contrived to be independently verifiable.

Sycamore

Google's Sycamore used 53 qubits and each run of it was able to maintain coherence for several milliseconds. IBM had some legitimate quibbles about whether Sycamore really achieved advantage, but the quibbles did not challenge the main point.

We now know that it is actually possible to build and run a quantum computer that compute things which contemporary supercomputers cannot.

Sycamore

Google's Sycamore used 53 qubits and each run of it was able to maintain coherence for several milliseconds. IBM had some legitimate quibbles about whether Sycamore really achieved advantage, but the quibbles did not challenge the main point.

We now know that it is actually possible to build and run a quantum computer that compute things which contemporary supercomputers cannot.

1. Very few people believed that quantum advantage couldn't be achived in principle, but there were some people (including me) who believed that it was *possible* that quantum advantage was impossible.

Quantum advantage and quantum cryptanalysis

Quantum cryptanalysis

Shor's algorithm

- Shor's algorithm [Sho94] changed everything;
- It solves factoring or the discrete logarithm problem in polynomial time;
- Shor's algorithm is clever extension of Simon's algorithm;

Grover's algorithm

- In 1996 Lov Grover presented a quantum search algorithm [Gro96].
- It is not a exponential speedup, but it is a quadratic speed up.
- It reduces a search of a 2^{128} space to 2^{64} steps.
- Grover's algorithm is why AES-256 exists.
- Grover's algorithm is a clever extension of Simon's algorithm.

Do we need to worry about it?

Running Shor's algorithm to break the RSA cryptosystem would require several thousand logical qubits. With known error-correction methods, that could easily translate into millions of physical qubits, and those probably of a higher quality than any that exist today. I don't think anyone is close to that, and we have no idea how long it will take. [Aar19]

Resources

Resources

- These slides and their sources.
- David Deutsch's book, *The Fabric of Reality* [Deu98] deeply changed the way that I think about quantum weirdness. It presents Everett's "many worlds" view.
- Scott Aaronson's blog Shtetl-Optimized.
- Saturday Morning Breakfast Cereal comic by Scott Aaronson and Zach Weinersmith. The Talk

References I

[Aar19] Scott Aaronson. **“Scott’s Supreme Quantum Supremacy FAQ!”** In: *Shtetl-Optimized* (Sept. 23, 2019). URL: https://scottaaronson.blog/?p=4317 (visited on 05/05/2022).

[Aum17] Jean-Philippe Aumasson. ***Serious cryptography: a practical introduction to modern encryption.*** No Starch Press, 2017.

[AW16] Scott Aaronson and Zach Weinersmith. ***The Talk.*** English. Saturday Morning Breakfast Cereal. Dec. 2016. URL: http://www.smbc-comics.com/comic/the-talk-3 (visited on 05/04/2022).

[Deu98] David Deutcsh. ***The Fabric of Reality. The Science of Parallel Universes–and Its Implications.*** Penguin Books, 1998.

References II

[Gro96] Lov K Grover. **"A fast quantum mechanical algorithm for database search."** In: *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. ACM. 1996, pp. 212–219.

[SC18] Charles T. Sebens and Sean M. Carroll. **"Self-locating Uncertainty and the Origin of Probability in Everettian Quantum Mechanics."** In: *The British Journal for the Philosophy of Science* 69.1 (Mar. 2018), pp. 25–74.

[Sho94] Peter W Shor. **"Algorithms for quantum computation: discrete logarithms and factoring."** In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, pp. 124–134.

References III

[Sim97] Daniel R. Simon. **"On the Power of Quantum Computation."** In: *SIAM Journal on Computing* 26.5 (1997), pp. 1474–1483. DOI: 10.1137/S0097539796298637. eprint: https://doi.org/10.1137/S0097539796298637. URL: https://doi.org/10.1137/S0097539796298637.