Quantum Computing – Introduction

Bill Celmaster

April 13, 2026

Good Problems for Quantum Computers

An example: Finding passwords (an example of Grover's algorithm) in a database of millions of passwords. Success if we find 99% of passwords.

- Pretend all passwords are combinations of 32 binary digits.
  - e.g. 01101111010100101100101001011011
  - There are $2^{32} = 4,294,967,296$ possibilities
- Classical computer: correct password in $\mathcal{O}(4,294,967,296)$ steps
- Quantum computer: candidate password in $\mathcal{O}(65,536)$ steps
  but only correct 90% of the time
  - So repeat the algorithm once. Correct 99% of the time.
  - And again, until we achieve desired accuracy
- Grover method: $\text{quantum-steps} = C * \sqrt{\text{classical-steps}}$

Some conditions for effective use of quantum computers:

- It's easy to verify a correct solution but hard to find it
- It's useful to be approximately correct. Egs.
  - Monte Carlo simulations
  - Numerical approximations on a discrete mesh
  - Decryption
  - No severe consequences if there's a mistake

Brief history

- The math of quantum computing was known about 100 years ago
  20 years after Einstein's 1905 papers
- But intuitions about computing waited until 1960's
  - Bell's theorem in 1964
  - Feynman, Deutch in 1980's plus Albert and Benioff
- And first experiments starting in 1980's
  - Aspect et al. experiments on entanglement 1981 etc.
  - First quantum computer at MIT in 1998
- Important quantum algorithms starting about 1994
  - Schor prime factorization 1994 – faster than classical
  - Grover database search 1996 – faster than classical
- IBM made quantum computer publicly available in 2016
- Commercial adoption is beginning

What is Quantum Mechanics?

From Richard Feynman QED: The Strange Theory of Light and Matter

"No, you're not going to be able to understand it.... You see, my physics students don't understand it either. That is because I don't understand it. Nobody does. ... The theory of quantum electrodynamics describes Nature as absurd from the point of view of common sense. And it agrees fully with an experiment. So I hope that you can accept Nature as She is – absurd"

What is a quantum computer?

- First – what is a classical computer?
  - A collection (**circuit**) of connected *classical* **gates**.
    - A classical **gate** maps binary *inputs* to binary *outputs*.

Figure: Classical (Boolean) gate with 1 input and 1 output

- By contrast, a quantum computer:
  - A collection (**circuit**) of connected *quantum* **gates**.
    - A quantum **gate** maps state *inputs* to state *outputs*.

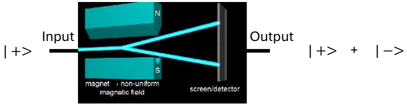


Figure: Schematic quantum gate with 1 input and 1 measured output

  - Plus a measurement of the final circuit output.

The first quantum computers

The Stern-Gerlach experiment split mixed states into $|+\rangle$ and $|-\rangle$.

Figure: Otto Stern in lab c. 1922 with a *simple quantum gate*

IBM quantum computer

IBM quantum computers currently scale to 5000+ gates.

Figure: IBM Poughkeepsie Quantum Data Center with > 20 quantum computers

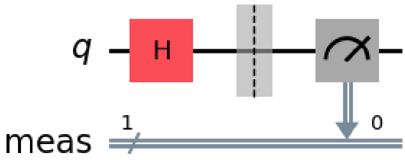
Quantum Circuit Recipe

A recipe from `ironchefai.com`

Figure: Quantum Circuit Chia Crepes

A quantum computation on IBM hardware

- I wrote a Python script for IBM hardware.
- The program creates a circuit with a single *Hadamard* (**H**) gate
  - Takes input q
  - Creates output $|+\rangle + |-\rangle$
  - Measures whether the state is $|+\rangle$ ("1)" or $|-\rangle$ ("0")
- The program prints out the circuit
- The program executes the circuit 100 times
- Finally the program prints the measured percents of "0" and "1".



{'0': 57, '1': 43}

Topics to be covered

- Hello World
  - States, gates and quantum circuits
  - Writing and executing a program for IBM's quantum computer
- Classical boolean circuits and quantum circuits
  - Reversibility
  - Qbits
- Entanglement
  - Bell's theorem and EPR pairs
  - Quantum teleportation
  - The no-cloning theorem
  - The CHSH game
- Grover's algorithm
- Quantum computing hardware