An Overview of Quantum Computing
By Ryan Y. Batubara

Scott Aaronson: "Quantum computers won't solve hard problems instantly by just trying all solutions in parallel."

Motivation: Semiprime Factoring

Given n the product of two primes p,q, recover p,q. GNFS sub-exponentially factors n with time

$$\exp\left((8/3)^{2/3} + o(1)) (\log n)^{1/3} (\log \log n)^{2/3} \right)$$

Quantum: Shor's alg. factors in $O(b^3)$ time and $O(b)$ space, where $b = \lceil \log_2 n \rceil$.

The Qubit

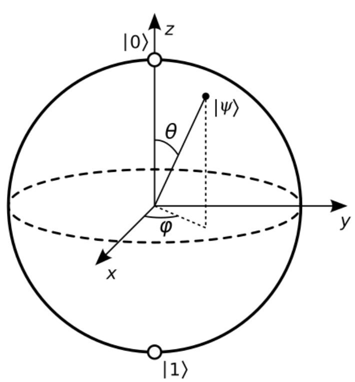
$X = \mathrm{Be}(p)$ can be represented by a vector

$$\begin{bmatrix} p \\ q \end{bmatrix} \text{ with } \left\| \begin{bmatrix} p \\ q \end{bmatrix} \right\|_1 = p + q = 1$$

Using the 2-norm, we get the qubit:

$$\begin{bmatrix} p \\ q \end{bmatrix} \text{ with } \left\| \begin{bmatrix} p \\ q \end{bmatrix} \right\|_2 = p^2 + q^2 = 1$$

This allows p,q to be negative, or complex. This gives the Bloch sphere:



Bra-ket Notation

Define ket and their tensor product as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$|a\rangle \otimes |b\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{bmatrix}$$

Multiplication of kets are assumed tensors, and

$$(A \otimes B) \otimes C = A \otimes (B \otimes C)$$
$$(A \otimes B)(C \otimes D) = AC \otimes BD$$
$$A \otimes (B + C) = A \otimes B + A \otimes C$$
$$(A + B) \otimes C = A \otimes C + B \otimes C$$
$$(xA) \otimes B = A \otimes (xB) = x(A \otimes B)$$

Define bra as the conjugate transpose

$$\langle a| = |a\rangle^\dagger = [\; a_1 \; a_2 \;]$$

Thus a braket is given by

$$\langle a|b\rangle = \langle a|\, |b\rangle = \overline{a}_1 b_1 + \overline{a}_2 b_2$$

Entanglement & Indistinguishability

Not all n-qubit a can be represented as tensor of 1-qubits. In such cases, call a entangled.

The Bell States or EPR Pairs are entangled:

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}|00\rangle \pm \frac{1}{\sqrt{2}}|11\rangle$$

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}|01\rangle \pm \frac{1}{\sqrt{2}}|10\rangle$$

Qubits a and b are indistinguishable if

$$P(a=0) = P(b=0),\ P(a=1) = P(b=1)$$

Quantum Gates & Circuits

A quantum gate is an operation on qubits that preserves the 2-norm; all quantum gates are unitary matrices U where

$$U^\dagger U = UU^\dagger = I$$

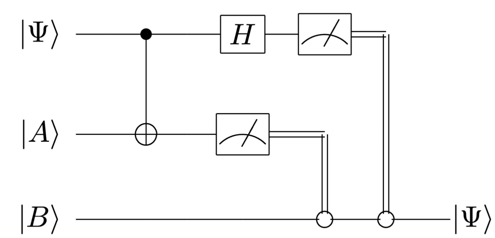
Some common quantum gates are

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad R_\beta = \begin{bmatrix} \cos(\beta) & -\sin(\beta) \\ \sin(\beta) & \cos(\beta) \end{bmatrix}$$

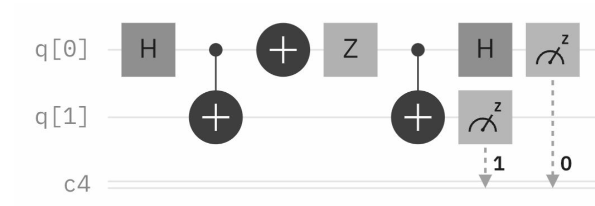
Quantum Teleportation

Alice can send Bob a qubit using $|\Phi^+\rangle$ and two classical bits, and the protocol:



Superdense Coding

Alice can send Bob two classical bits using one entangled qubit and the protocol



This means an n bit message can be sent in $n/2$ qubits, and this is a proven and strict lower bound.

Material from
Quantum Computing Since Democritus by Scott Aaronson
Quantum Computation: Lecture Notes by John Watrous

To run quantum circuit simulations go to
https://quantum.ibm.com/composer
https://www.ibm.com/quantum/qiskit

Shor's Algorithm

Choose $1 < a < N$ with $\gcd(a,N) = 1$, $N = pq$.
The order of a mod N is the smallest r where

$$a^r \equiv 1 \pmod N$$

Let a be n bits. Define an n-qubit transformation

$$U_a |x\rangle \equiv | ax \pmod N \rangle$$
$$(U_a)^r |1\rangle \equiv | a^r \pmod N \rangle$$

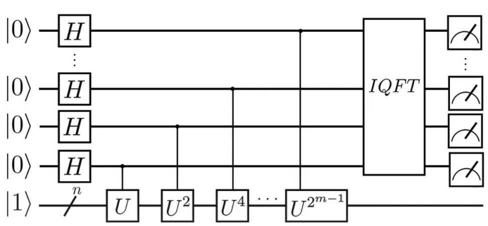
U has eigenvectors $|u_s\rangle$, $0 \le s < r$ with the property

$$U |u_s\rangle = \exp(2\pi i\, s/r)\, |u_s\rangle$$
$$\frac{1}{\sqrt{r}} \Sigma_s |u_s\rangle = |1 \bmod (N)\rangle$$

Measuring the procedure below gives eigenvalue(s) for one s, such that we recover r. But as

$$a^r - 1 \equiv \pmod N \rightarrow (a^{r/2} - 1)(a^{r/2} + 1) = N$$

So $\gcd(a^{r/2} \pm 1, N)$ has high P of being p or q.



Quantum Speedups

Many problems have real, quantum speedups:

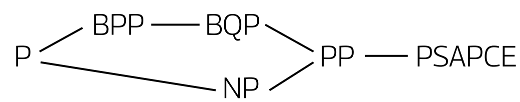
- Quantum Fourier transform
- Unstructured search problem
- Discrete logarithms
- Hidden subgroup problem
- CHSH games
- Constant vs. balanced functions
- Quantum machine learning

Material from
Quantum Computing Since Democritus by Scott Aaronson
Quantum Computation: Lecture Notes by John Watrous

Quantum Supremacy

Shor works by computing superpositions of finite #possibilities simultaneously. As such, quantum computing does not mean all problems can be solved in *P* time by running all solutions in parallel.

Semiprime factoring is in *NP* and *coNP*, in between *P* and *NP*. Indeed, *BQP* and *NP* are incomparable:



No-Cloning Theorem

There is no copying non-basis states, i.e. DNE *A* s.t.

$$A |x\rangle |0\rangle = |x\rangle |x\rangle$$

Proof. Let $|x\rangle = a |x\rangle + b |x\rangle$. Then

$$|x\rangle |x\rangle = a^2 |00\rangle + ab |01\rangle + ab |10\rangle + b^2 |11\rangle$$
$$A |x\rangle |0\rangle = aA |0\rangle |0\rangle + bA |1\rangle |0\rangle = a |00\rangle + b |11\rangle$$

a contradiction. □

Quantum Hardware

In 2001, Shor was run on 7 qubits. In 2025, Willow has 105 qubits and 0 quantum gates. The lifetime of a qubit now is <1 second. Quantum & qubit measurement is error prone. Despite this, at the current (stable) trajectory, there is a high probability quantum computers will have commercial applications in a few decades.

The Quantum Revolution

A useful QC would break most modern encryption, though would open possibilities of quantum key teleportation and other post-quantum cryptographic solutions (search NIST quantum).

Discussion question: If you had a QC, would you want to tell the world? Why or why not?

Quantum Programming

With no cloning, what would quantum programs look like? How should variables be defined?

$$\begin{array}{ccc} & \textbf{Category Theory} & \\ \swarrow\!\!\nearrow & & \nwarrow\!\!\searrow \\ \textbf{Type Theory} & \longleftrightarrow & \textbf{Logic} \end{array}$$

Quantum Linearity

1998: If Quantum gates were nonlinear, $P = NP$ so all proof would be efficiently automated. Furthermore, you can teleport faster than light.

Quantum Post-Selection

If you can post select the outcome of qubits, $PostBQP = PP \supset NP, coNP$. Example: Given a binary function taking n bits, do at least half of the inputs output 1? Output correctly with $P > ½$. How does this differ from *BPP* where $P > ⅔$?

Quantum Decoherence

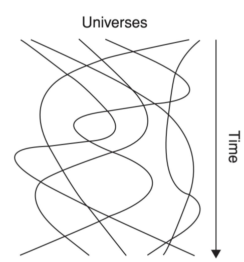
Why do we not observe quantum mechanics at the macroscopic scale? Consider

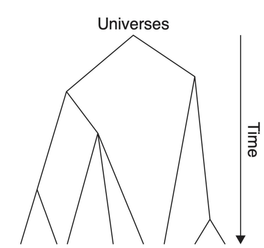
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}e^{i\theta}\,|11\rangle$$

The density matrix ρ is defined

$$\rho = |\Phi^+\rangle\langle\Phi^+| = \begin{bmatrix} ½ & ½\, e^{-i\theta} \\ ½\, e^{i\theta} & ½ \end{bmatrix}$$

Decoherence says that we measure the average of all θ, so ρ is a diag. matrix with ½ on the diagonals. But no such state exists with such a ρ!





To run quantum circuit simulations go to
https://quantum.ibm.com/composer
https://www.ibm.com/quantum/qiskit