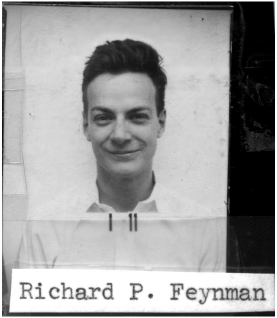
Outline

Founding Fathers

Time: early 1980-s
People: Paul Benioff, Richard Feynman, and Yuri Manin



Key Tool: Quantum Parallelism (tricky to employ)

The Pearl: Shor's Algorithm (1994)

Problem: Integer Factorization

Best "Classical" Solution: $O\left(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}}\right)$

Shor's Algorithm: $O\big((\log N)^2(\log\log N)(\log\log\log N)\big)$

State Space Postulate

Postulate 1 (State Space Postulate)

The state of a system is described by a unit vector in a Hilbert space $\mathcal{H}$.

"Systems"

A piece of physical reality used to encode information akin to trnsistors, e.g.

- electron and its spin,
- photon and its polarization,
- spins of other particles

Hilbert space

Complex **vector space** with a **scalar product** (to measure angles and lengths).

Once you pick a basis, its basically $\mathbb{C}^n$.

Example: 2 dimensions, fixed basis: $|0\rangle$, $|1\rangle$ $\Rightarrow$ qubit

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle , \qquad \alpha_i \in \mathbb{C} : |\alpha_0|^2 + |\alpha_1|^2 = 1.$$

Composite Systems

Composition of Systems Postulate

If one system is in the state $|\varphi_1\rangle$ and the second system in the state $|\varphi_2\rangle$, then the state of the combined system is described by the *tensor product*:

$$|\varphi_1\rangle \otimes |\varphi_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2, \qquad \text{if } |\varphi_i\rangle \in \mathcal{H}_i.$$

Notation Instead of $|\varphi_1\rangle \otimes |\varphi_2\rangle$ we write $|\varphi_1\rangle\,|\varphi_2\rangle$ or even $|\varphi_1\varphi_2\rangle$.

Tensor Product in a Nutshell: bilinear pairing operation.

Example: two qubits

Given

$$|\varphi_1\rangle = {}^1\!/\!\sqrt{2}(|0\rangle + |1\rangle), \qquad |\varphi_2\rangle = {}^1\!/\!\sqrt{2}(|0\rangle - |1\rangle).$$

their composite is described with: What about dimension?

$$|\varphi_1\rangle\,|\varphi_2\rangle = {}^1\!/\!2(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = {}^1\!/\!2(|00\rangle - |01\rangle + |10\rangle + |11\rangle).$$

Entangled States

Can we always un-tensor states of two qubits?

No (...t at all):

$$|\varphi\rangle = {}^{1}\!/\!\sqrt{2}(|00\rangle + |11\rangle)$$

Fancy name: EPR pair (for Einstein, Podolsky, and Rosen)

The Way To Compute

What to require from a computational tool when work with *unit vectors*?

Evolution Postulate

The time-evolution of the state of a closed quantum system is described by a unitary operator: $\exists U\colon\ |\varphi_{t0+x}\rangle = U\,|\varphi_{t0}\rangle$.

Unitary Operators

U unitary $\Leftrightarrow (Ux, Uy) = (x, y)$.

Using adjoint opertor:

$$(Ux, Uy) = (x, U^* Uy),$$

an equivalent formulation:

$$U \text{ unitary} \Leftrightarrow U^* = U^{-1}.$$

Case of Real-Valued Matrices

First, U^* is simply U^T.

$$U \text{ unitary} \Leftrightarrow U^{-1} = U^T.$$

Second, if an operator is self-inverse ($U^{-1} = U$), then

$$U \text{ unitary} \Leftrightarrow U = U^T.$$

The Cats Of It

Problem: Can't Access The Amplitudes

A "classical" observer can only get to basis states, e.g. $|0\rangle$, $|1\rangle$.
So what do superposition states mean?

$$\text{cat: } {}^1\!/\!\sqrt{2}\ \text{dead} + {}^1\!/\!\sqrt{2}\ \text{alive}\ldots$$

Measurement Postulate

Consider a system A and its state space $\mathcal{H}_A$.
For an orthonormal basis $B = \{|\varphi_i\rangle\}$ in $\mathcal{H}_A$, there exists a description of A:

$$|\varphi\rangle = \sum_i \alpha_i |\varphi_i\rangle, \qquad \sum_i |\alpha_i|^2 = 1.$$

It is possible to perform a *(Von Neumann) measurement* on system A with respect to the basis B. With probability $|\alpha_i|^2$, this act outputs a label i and leaves the system in state $|\varphi_i\rangle$.

Measurement Examples

$$|\varphi\rangle = \sqrt{1/11}\,|00\rangle + \sqrt{5/11}\,|01\rangle + \sqrt{2/11}\,|10\rangle + \sqrt{3/11}\,|11\rangle$$

Measure both qubits

What are the possible outcomes of measuring the pair of qubits?
Here they are:

- 00 — with probability $1/11$; the system turns into $|00\rangle$
- 01 — with probability $5/11$; the system turns into $|01\rangle$ ...

Measure the first qubit

Note from above:
the probability of getting 0 for the first qubit is $1/11 + 5/11 = 6/11$.
So, we factor out $\sqrt{6/11}$ first to get:

$$|\varphi\rangle = \sqrt{6/11}\,|0\rangle\left(\sqrt{1/6}\,|0\rangle + \sqrt{5/6}\,|1\rangle\right) + \sqrt{5/11}\,|1\rangle\left(\sqrt{2/5}\,|0\rangle + \sqrt{3/5}\,|1\rangle\right).$$

When output=0 the system becomes: $|0\rangle\,(\sqrt{1/6}\,|0\rangle + \sqrt{5/6}\,|1\rangle)$.

The Road to Shor

Idea 1 (a simple one)

We only need to be able to find one factor of the input N.

Idea 2 (a technical one)

Take random $A < N$ coprime to N. An integer r is called the order of A modulo N if $A^r \equiv 1 \pmod{N}$.
Finding a factor of N can be efficiently reduced to the order-finding problem.

The Insight About Periodicity

The order-finding problem can be seen as the problem of finding the period of the following mapping:

$$\exp_{A,N}: \quad b \mapsto A^b \pmod{N}, \qquad \text{where } b \in \mathbb{Z}.$$

Periodic Functions: What and Why

Definition

$f\colon G \to X$ defined on a group G is *periodic with period* $r \in G$ ($r \neq e$) if:

$$\forall n \in \mathbb{Z}\,\forall g \in G\colon f(g + rn) = f(g).$$

Shor's Problem

Find the period of a particular function ($\exp_{A,N}$) defined on the group $\mathbb{Z}$.
Note: In fact, on a smaller group, $\mathbb{Z}_{\varphi(N)}$, but we don't know it in advance, hence the other name: the *hidden subgroup problem*.

We are in rush, so we tackle an easier instance of the same problem.

Simon's Problem

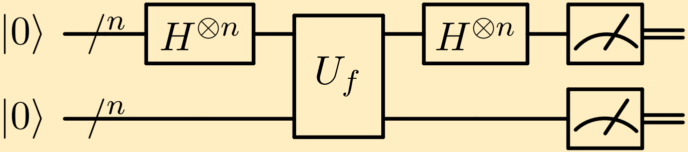
Find the period of a function defined on the group $\mathbb{Z}_2^n$.

Simon's Problem

Formulation

Input: A black-box for computing an unknown function $f : \mathbb{Z}_2^n \to X$.
Promise: There exists $\bar{s}$, s.t.: $f(\bar{x}) = f(\bar{y})$ iff $\bar{x} = \bar{y}$ or $\bar{x} = \bar{y} \oplus \bar{s}$.
Problem: Determine $\bar{s}$ by making queries to f.

The Circuit



$$|0^{2n}\rangle \xmapsto{(1)} \sum_{\bar{x}\in\mathbb{Z}_2^n} |\bar{x}\, 0^n\rangle \xmapsto{(2)} \sum_{\bar{x}\in\mathbb{Z}_2^n} |\bar{x}\rangle\, |f(\bar{x})\rangle \xmapsto{(3)} (|\bar{x}\rangle + |\bar{x} \oplus \bar{s}\rangle)\, |f(\bar{x})\rangle \xmapsto{(4)} \ldots$$

Why The Circuit Works (And What it Outputs)

Hadamard on a coset

$$H^{\oplus n}(|\bar{x}\rangle + |\bar{x} \oplus \bar{s}\rangle) = \sum_{\bar{z} \in \bar{s}^{\perp}} (-1)^{\bar{x} \cdot \bar{z}} |\bar{z}\rangle .$$

Output of The Circuit

Claim: the output on the first n wires of the circuit is a vector $\bar{z} \in \bar{s}^{\perp}$.

Quantum Computing

- Massively data-parallel model with probablistic outcomes;
- good only for certain classes of tasks,
  esp. when searching for global properties of functions;
- some of the applications are very important (e.g. in cryptography);
- practise lags behind theory.