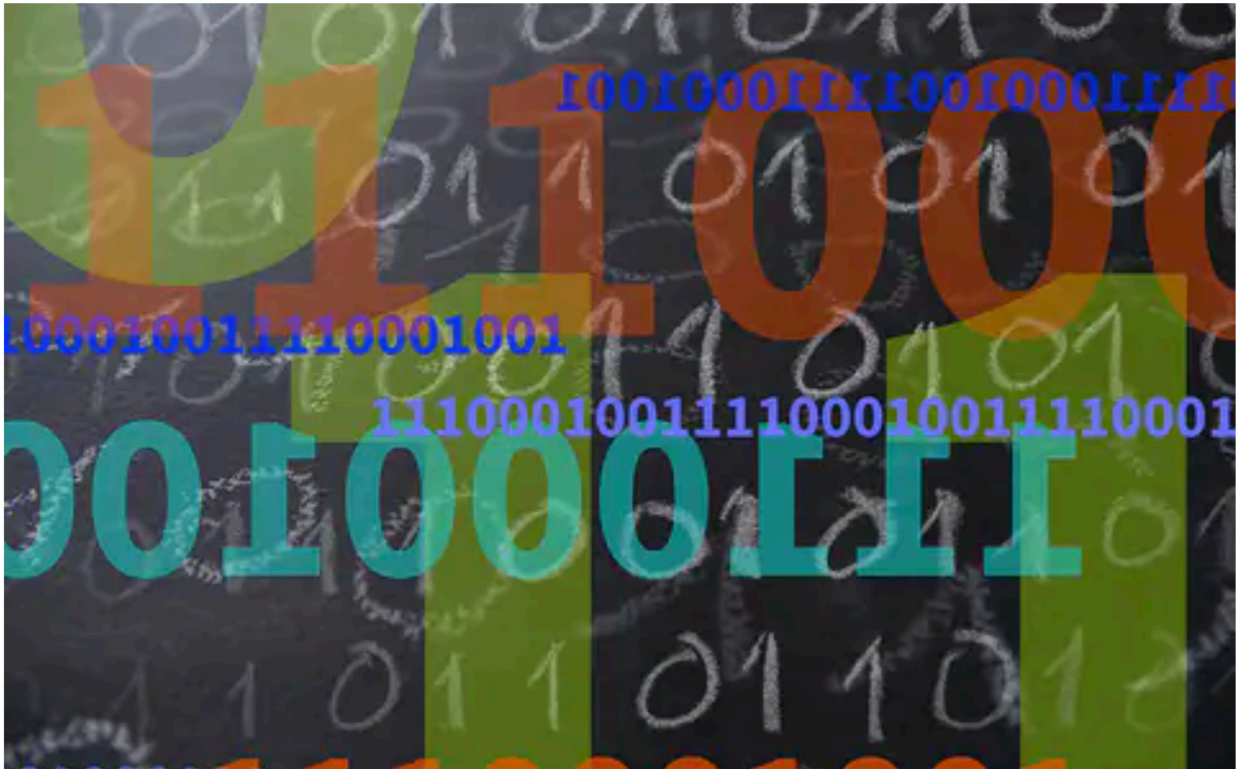
Quantum Algorithms

Google scientists say they've achieved 'quantum supremacy' breakthrough over classical computers



By **Sarah Kaplan**

Oct. 23, 2019 at 4:30 a.m. EDT

Add to list

For the first time, a machine that runs on the mind-boggling physics of quantum mechanics has reportedly solved a problem that would stump the world's top supercomputers — a breakthrough known as "quantum supremacy."

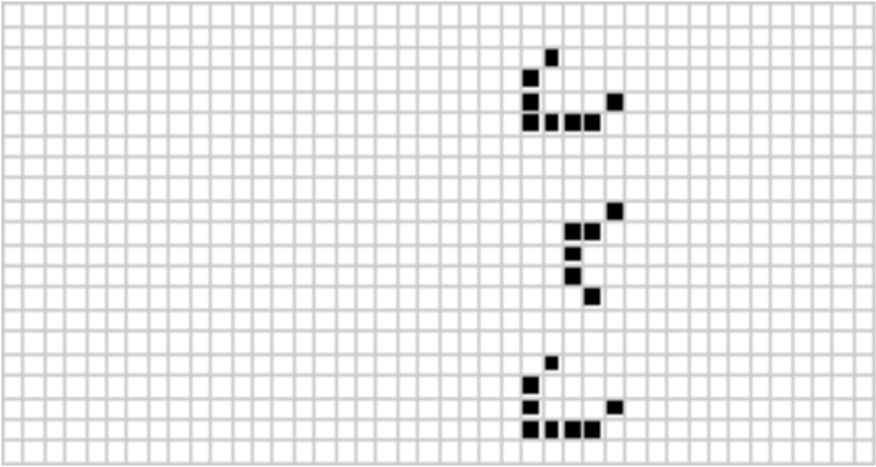
- Advances in quantum hardware

  52 qubits circuit of depth ~20, with
  gate fidelity ~ .99

- Theoretical justification that experiment
  (plausibly) achieves quantum supremacy

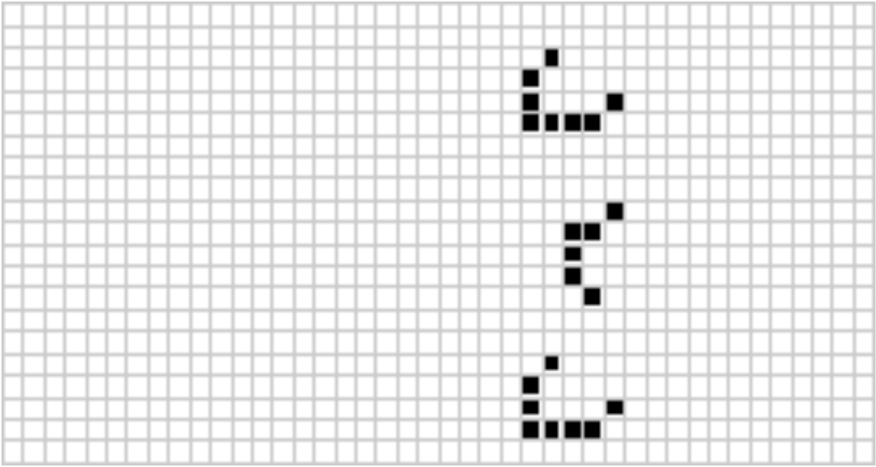
Quantum Supremacy = experimental violation of the Extended Church-Turing Thesis

Any "reasonable" model of computation can be simulated on a (probabilistic) Turing Machine with at most polynomial simulation overhead.



Quantum Supremacy = experimental violation of the Extended Church-Turing Thesis

Any “reasonable” model of computation can be simulated on a (probabilistic) Turing Machine with at most polynomial simulation overhead.



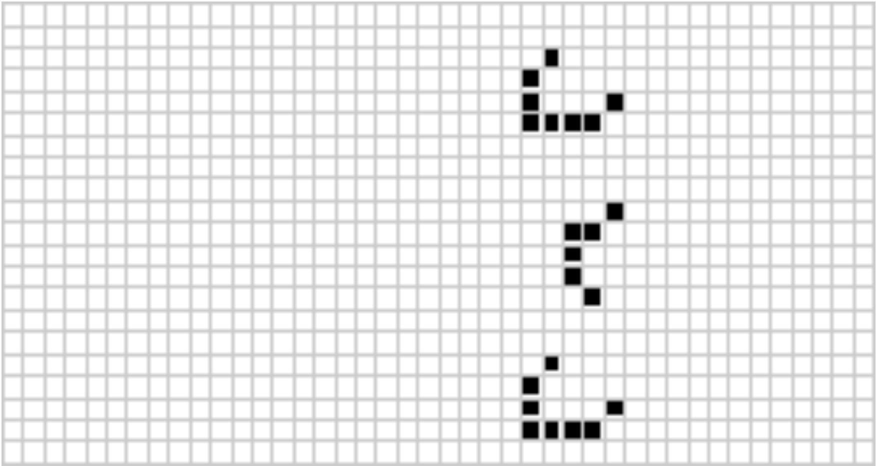
Theoretical violation of ECT showed quantum computers:

- Programmable
- Digital (wrt 1/poly(n) errors)
- Superpolynomial speedup on a challenge problem

-Bernstein,V 93

Quantum Supremacy = experimental violation of the Extended Church-Turing Thesis

Any "reasonable" model of computation can be simulated on a (probabilistic) Turing Machine with at most polynomial simulation overhead.



Theoretical violation of ECT showed quantum computers:

- Programmable
- Digital (wrt 1/poly(n) errors)
- Superpolynomial speedup on a challenge problem

-Bernstein,V 93

Exponential speedup for factoring [Shor 94]

Digital wrt constant error rate – quantum fault tolerance [Aharonov, Ben-Or][Knill Laflamme][Gottesman, Preskill]

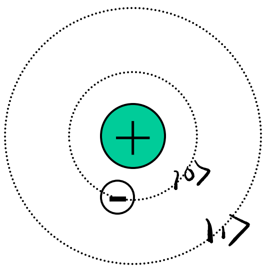
Quantum circuit models --- classically controlled quantum system

Superposition Principle

Qubit:

$\alpha, \beta \in \mathbb{C}$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



eg $\alpha = \frac{1}{\sqrt{2}}$ $\beta = \frac{1}{2} + \frac{i}{2}$

$|\alpha| = \frac{1}{\sqrt{2}}$ $|\beta| = \sqrt{\frac{1}{2^2} + \frac{1}{2^2}}$

$= \sqrt{\frac{1}{2}} = \frac{1}{\sqrt{2}}$

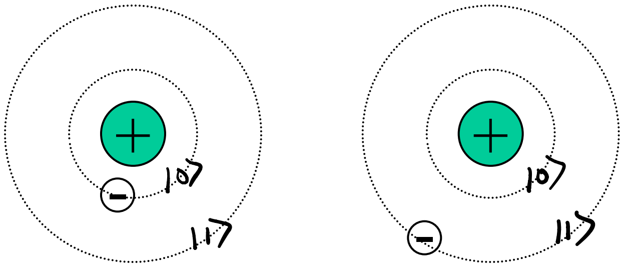
$$|\alpha|^2 + |\beta|^2 = 1$$

New state

Measure: see 0 wp $|\alpha|^2 \to |0\rangle$

1 wp $|\beta|^2 \to |1\rangle$

Two Qubits



$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

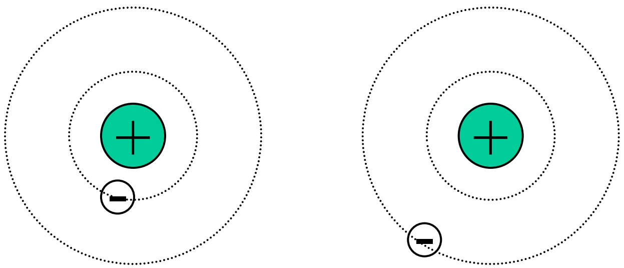
$\alpha_x \in \mathbb{C}$

$$\sum |\alpha_x|^2 = 1$$

measure : see x with prob $|\alpha_x|^2$

New state $= |x\rangle$.

Two Qubits



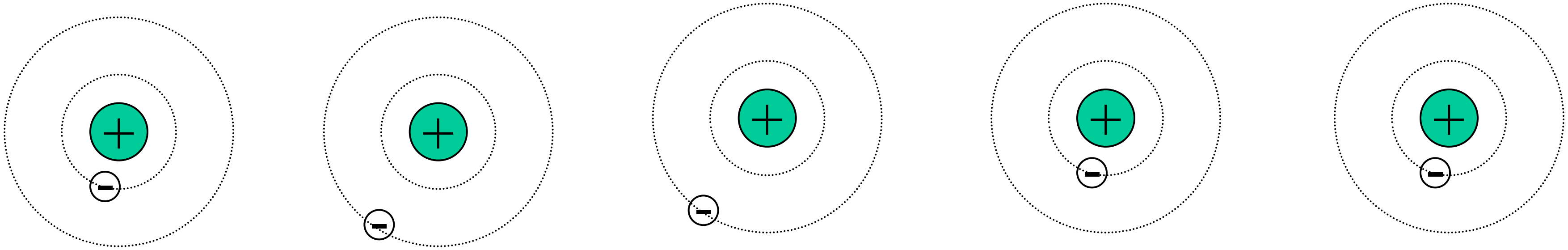
$$P[0] = |\alpha_{00}|^2 + |\alpha_{01}|^2$$

- Measure first qubit:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \cancel{\alpha_{10}|10\rangle} + \cancel{\alpha_{11}|11\rangle}$$

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

Exponentially Large Hilbert Space

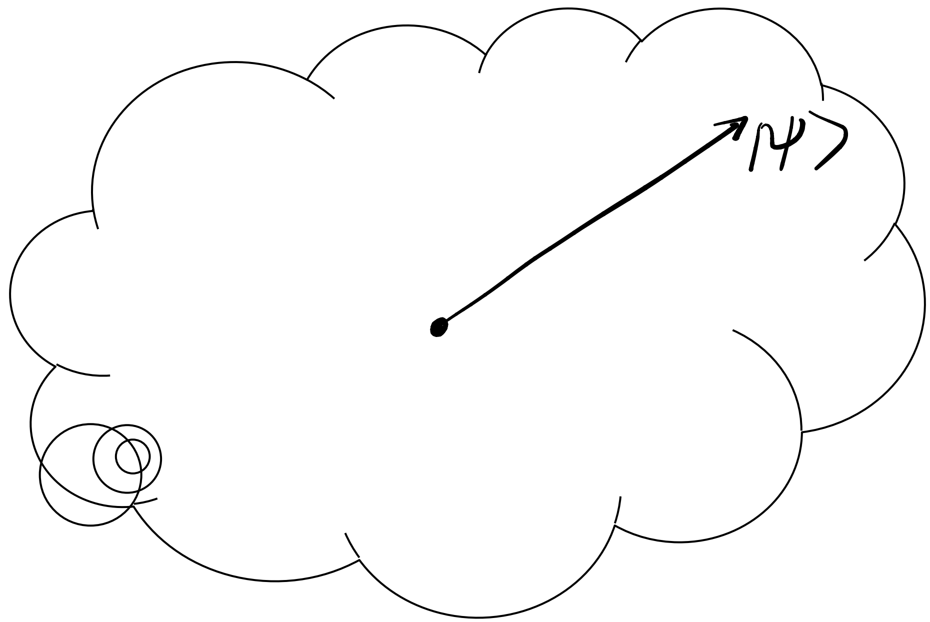


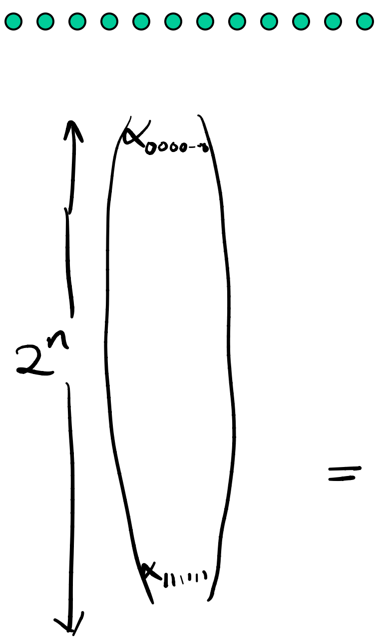
Exponentially Large Hilbert Space

Exponentially Large Hilbert Space

Storing the state

2^n dim complex vector space



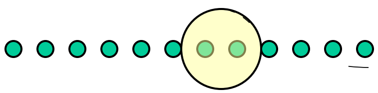


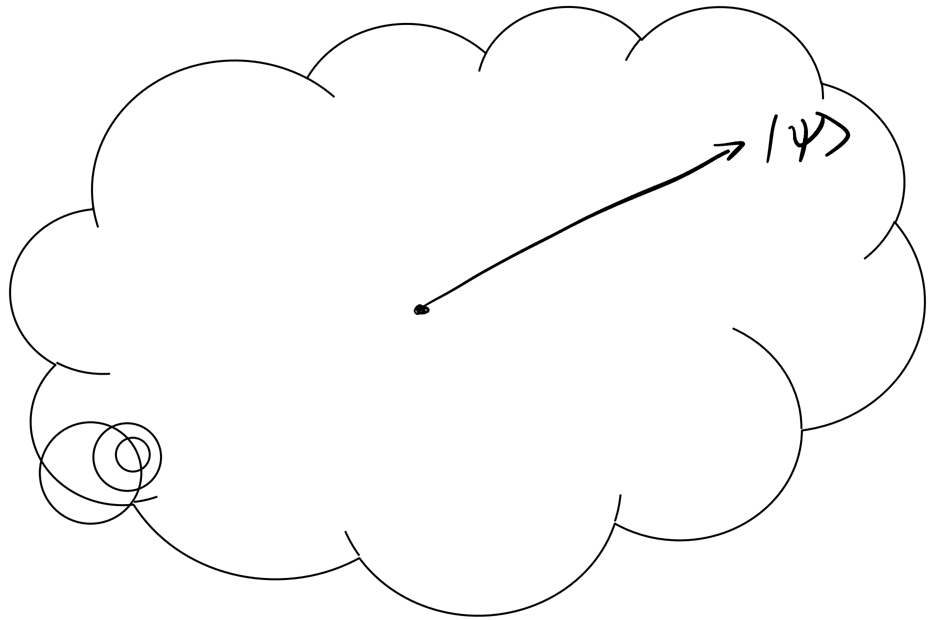
$$= \Psi = \sum_x \alpha_x |x\rangle \qquad \sum_x |\alpha_x|^2 = 1$$

all n-bit strings

Quantum entanglement

Unitary Evolution



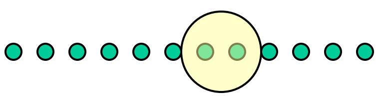


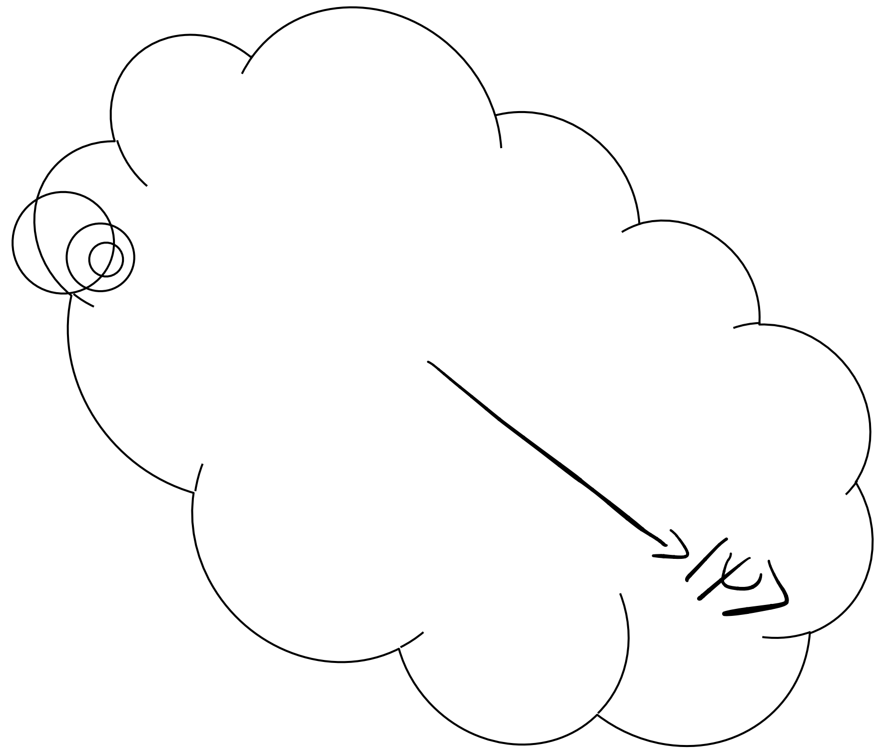
$$\Psi = \sum_x \alpha_x |x\rangle$$

$$\sum_x |\alpha_x|^2 = 1$$

all n-bit strings

Unitary Evolution





$$\Psi = \sum_x \alpha_x |x\rangle \qquad \sum_x |\alpha_x|^2 = 1$$

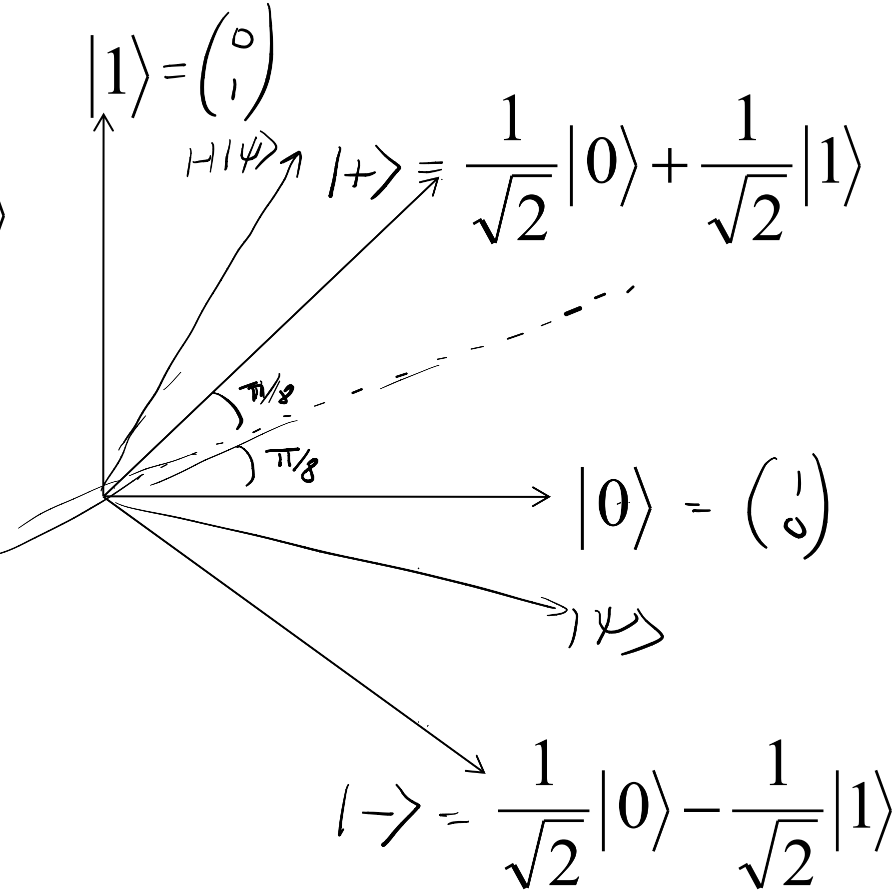
all n-bit strings

Hadamard Gate

$\alpha|0\rangle+\beta|1\rangle \longrightarrow \boxed{H} \longrightarrow \alpha'|0\rangle+\beta'|1\rangle$

$$|0\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$$

$$|1\rangle \longrightarrow \boxed{H} \longrightarrow \frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle$$



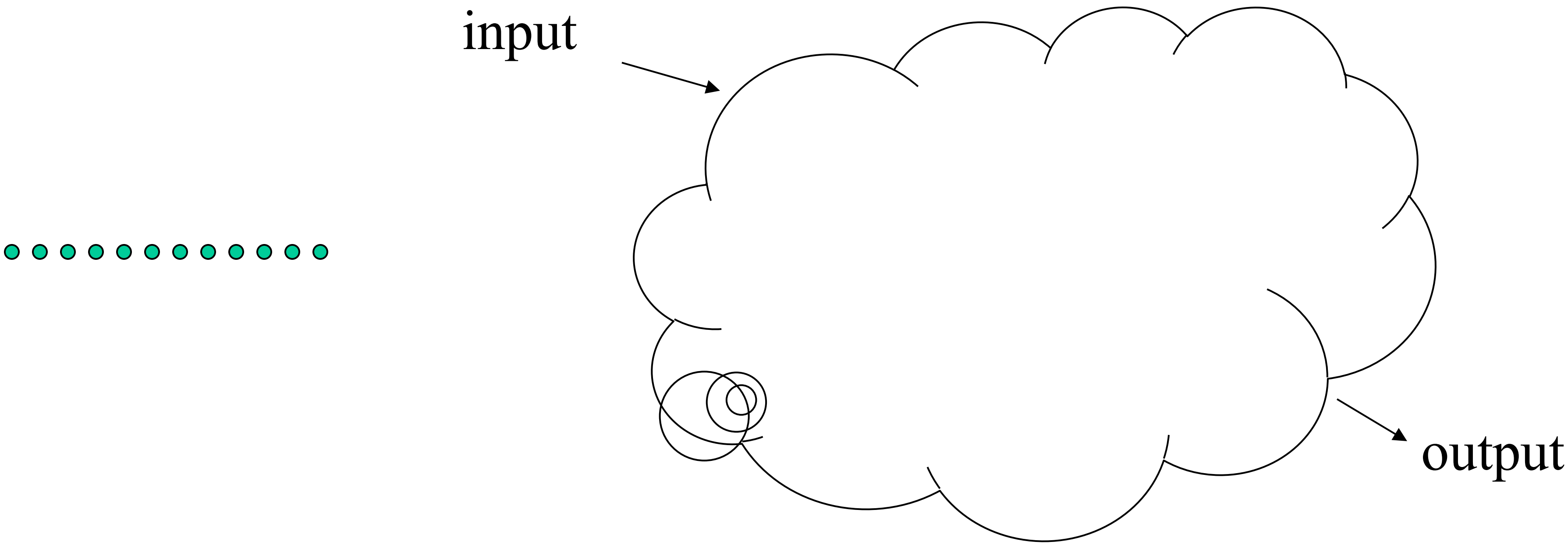
$$H^2 = I$$

$$\alpha|0\rangle+\beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$$

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$$

$$|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

Limited Access - Measurement



$$\Psi = \sum_x \alpha_x |x\rangle \qquad \sum_x |\alpha_x|^2 = 1$$

- Measurement: See $|x\rangle$ with probability $|\alpha_x|^2$

Quantum supremacy = experimental violation of
Extended Church-Turing thesis

Shor's quantum factoring algorithm as the
basis for quantum supremacy:

Create a challenge problem: choose large primes P, Q
Multiply to get N = PQ

Ask quantum computer to factor N

"*Proving a quantum system's computational power by having it factor integers is a bit like proving a dolphin's intelligence by teaching it to solve arithmetic problems*"
[Aaronson & Arkhipov '11]

IN RSA WE TRUST

IN RSA WE TRUST

Until Shor's quantum factoring algorithm spoilt the party!

Fourier Transform

$$\begin{pmatrix} \beta_0 \\ \beta_1 \\ . \\ . \\ \beta_{m-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & . & 1 \\ 1 & \omega & \omega^2 & . & \omega^{m-1} \\ . & . & . & . & . \\ . & . & . & . & . \\ 1 & \omega^{m-1} & \omega^{2(m-1)} & . & \omega^{(m-1)(m-1)} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ . \\ . \\ \alpha_{m-1} \end{pmatrix}$$

output

input

Classical: FFT O(m logm)

Quantum Fourier Transform

$k = \log m$.

$$\begin{pmatrix} \beta_0 \\ \beta_1 \\ . \\ . \\ \beta_{m-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & . & 1 \\ 1 & \omega & \omega^2 & . & \omega^{m-1} \\ . & . & . & . & . \\ . & . & . & . & . \\ 1 & \omega^{m-1} & \omega^{2(m-1)} & . & \omega^{(m-1)(m-1)} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ . \\ . \\ \alpha_{m-1} \end{pmatrix}$$

$m = 2^k$

k qubit system

State:

$$|\alpha\rangle = \sum_{x \in \{0,1\}^k} \alpha_x |x\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{2^k-1} \end{pmatrix}$$

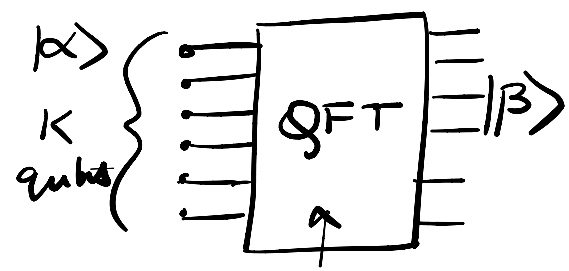
Classical: FFT O(m logm)

Quantum:

Input: Quantum state of log m qubits

$$\Psi = \sum_j \alpha_j |j\rangle$$

all log m-bit strings



$\approx k \log k$ gates.

$\approx \log m$

measure:

see j wp $|\beta_j|^2$

Quantum Fourier Transform

$$\begin{pmatrix} \beta_0 \\ \beta_1 \\ . \\ . \\ \beta_{m-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & . & 1 \\ 1 & \omega & \omega^2 & . & \omega^{m-1} \\ . & . & . & . & . \\ . & . & . & . & . \\ 1 & \omega^{m-1} & \omega^{2(m-1)} & . & \omega^{(m-1)(m-1)} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ . \\ . \\ \alpha_{m-1} \end{pmatrix}$$

Classical: FFT O(m logm)

Quantum:

Input: Quantum state of log m qubits

Fourier transform: Quantum state after $O(\log^2 m)$ gates

Limited Access:

Don't get access to output vector. Not even one entry!

Measure: see index j with probability $|\beta_j|^2$

$\underline{N} = P \cdot Q$ $\qquad$ $21 = 3 \cdot 7$

$\underline{\underline{x}}$ random $\pmod N$

$\gcd(x, N) = 1.$

<u>Goal</u>: Find $\overset{\min}{r} : x^r \equiv 1 \pmod N$ $\Big\}$ $r =$ order $x \pmod N$

$r > 0$

<u>Lemma</u>: with prob $\geq \frac{1}{2}$ $\quad$ r is even & $x^{r/2} \not\equiv \pm 1 \pmod N$

$N \mid (x^{r/2}+1)(x^{r/2}-1)$

$\gcd(N, x^{r/2}+1) =$ nontrivial factor.

<u>eg</u> $\quad x = 2 \qquad N = 21$

$r = 6$

$2^6 = 64 \equiv 1 \pmod{21}$

$2^3 \pmod{21} = 8 \not\equiv \pm 1 \pmod{21}$

$8^2 \equiv (2^3)^2 = 2^6 \equiv 1 \pmod{21}$ $\quad$ but $\quad 8 \not\equiv \pm 1 \pmod{21}$

$21 \mid 8^2 - 1$ $\qquad$ but $\qquad 21 \nmid (8 \pm 1)$

$21 \mid \underline{(8+1)}\,\underline{(8-1)}$ $\qquad$ but $\qquad 21 \nmid (8 \pm 1)$

$\gcd(8+1, 21) = \gcd(9, 21) = 3$ $\qquad$ $\gcd(8-1, 21) = \gcd(7, 21) = 7$

Given N, x Find $r = \operatorname{ord}_N(x)$

$|0\rangle_M |0\rangle_N$

$\downarrow$ QFT

$\sum_{a=0}^{M-1} |a\rangle\, |0\rangle$

$\downarrow$

$\frac{1}{\sqrt{M}} \sum_{a=0}^{M} |a\rangle\, |\underbrace{x^a \pmod N}\rangle$

$x^k \pmod N$

$\sum |jr + \cancel{k}\rangle$

$\downarrow$ QFT

extract r

$x^{jr+k} \equiv x^k \pmod N$

$FFT_M \longleftrightarrow M$ mult

of $(p-1)(q-1)$

$$\begin{pmatrix} \frac{1}{\sqrt{M}} & & \\ \frac{1}{\sqrt{M}} & FT & \\ \vdots & & \\ \frac{1}{\sqrt{M}} & & \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$\parallel$

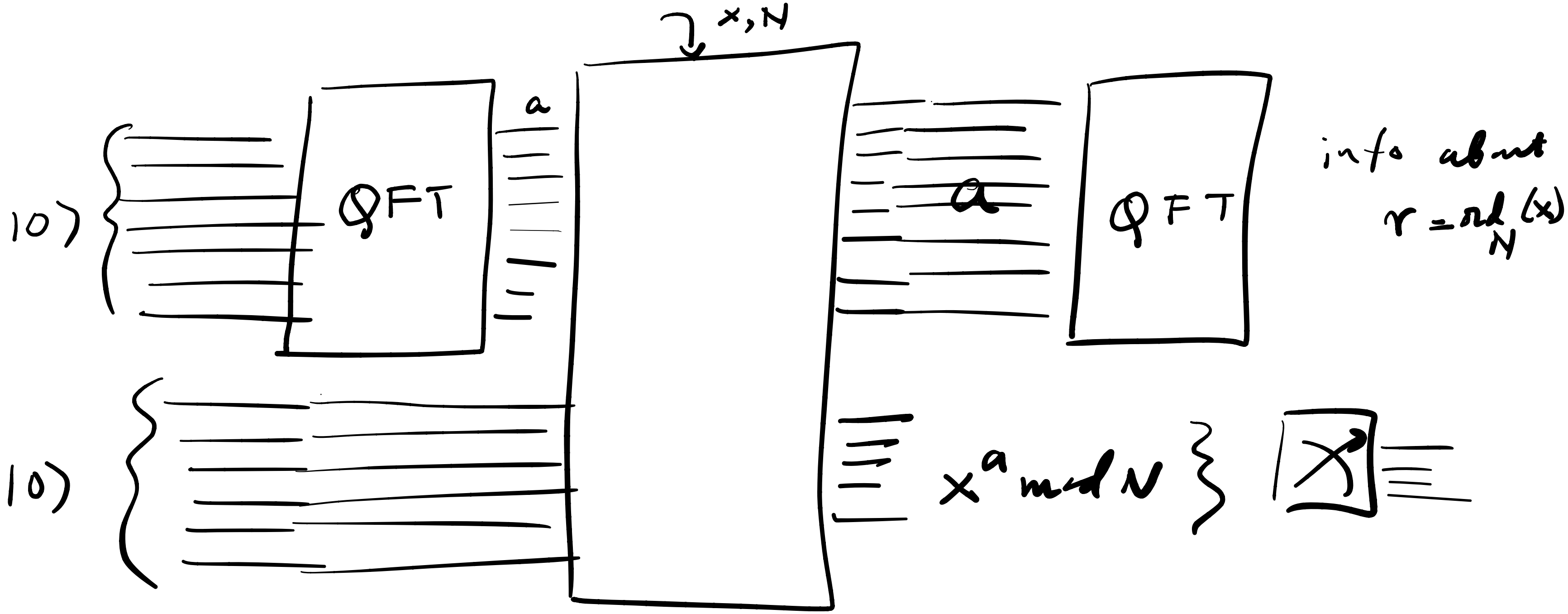
$|0\rangle$

$x = 2$

$\frac{1}{\sqrt{M}} \quad |0\rangle|x^0 \bmod N\rangle + |1\rangle|x^1 \bmod N\rangle + \dots + |M-1\rangle x^{M-1} \bmod N$

$\left.\begin{array}{l} x^0 = 1 \\ x^1 = x \\ x^2 = x^2 \\ \vdots \\ x^{r-1} \end{array}\right\}$

$\left.\begin{array}{l} x^r = 1 \\ x^{r+1} = x \\ \vdots \end{array}\right\}$



x, N
a
$|0\rangle$
QFT
a
QFT
info about
$r = \text{ord}_N(x)$
$|0\rangle$
$x^a \bmod N$