Embracing the quantum future: fundamental training for UPT students

Introduction to key concepts and algorithms

Mihai Udrescu (UPT)

Making the headlines

IEEE Spectrum Electric Cooling Could Shrink Quantum Computers

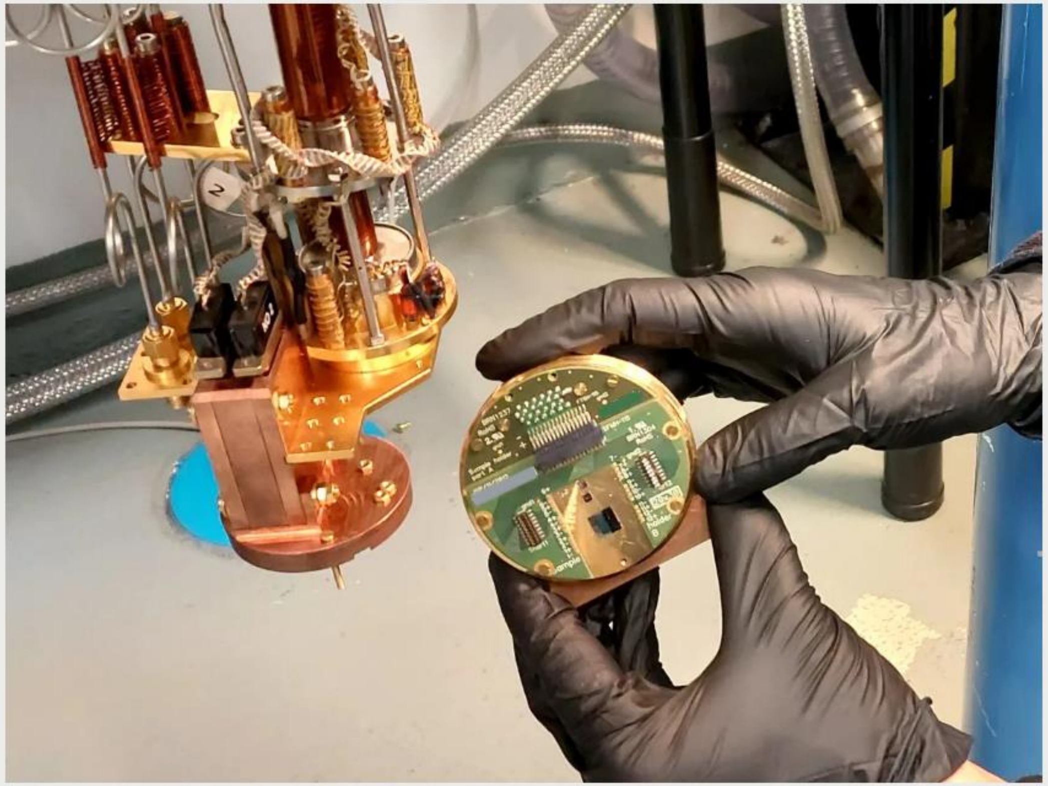
Type to search

NEWS | COMPUTING

Electric Cooling Could Shrink Quantum Computers ›

Vacuum-tube effect might simplify cryogenic chambers

BY CHARLES Q. CHOI | 12 SEP 2023 | 3 MIN READ



VTT's electronic refrigerator prototypes undergo cryogenic testing. VTT

BBC Sign in | Home | News | Sport | Reel | Worklife | Travel

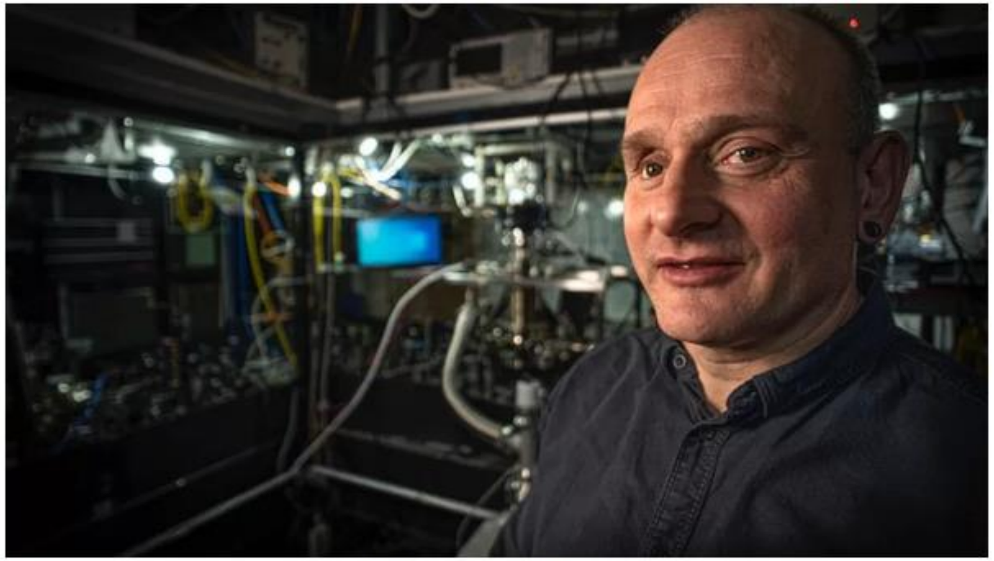
NEWS

Home | War in Ukraine | Climate | Video | World | UK | Business | Tech | Science | Entertainment & Arts

Science

Quantum breakthrough could revolutionise computing

8 February · Comments

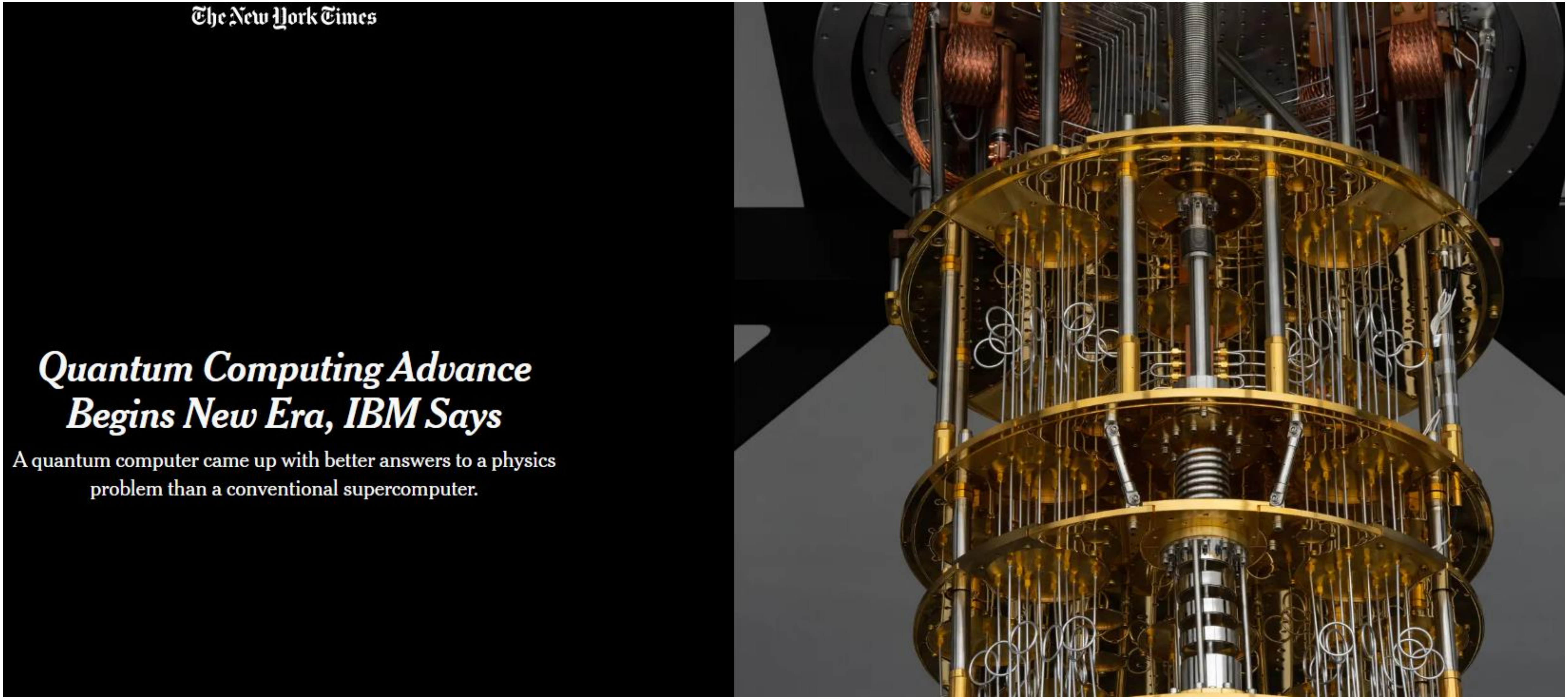


Twenty years ago Winfried Hensinger was told by other scientists that developing a powerful quantum computer was impossible. Now he has made the system behind him that he believes will prove them wrong

By Pallab Ghosh
Science correspondent

Scientists have come a step closer to making multi-tasking 'quantum' computers, far more powerful than even today's most advanced supercomputers.

Making the headlines


The New York Times

Quantum Computing Advance Begins New Era, IBM Says

A quantum computer came up with better answers to a physics problem than a conventional supercomputer.

Making the headlines

AspenCore Network | About Us | Newsletters | Events | Webinars | White Papers | Advertise | Contact Us

embedded | Analysis | News | Technical Articles | Tutorials | Pro

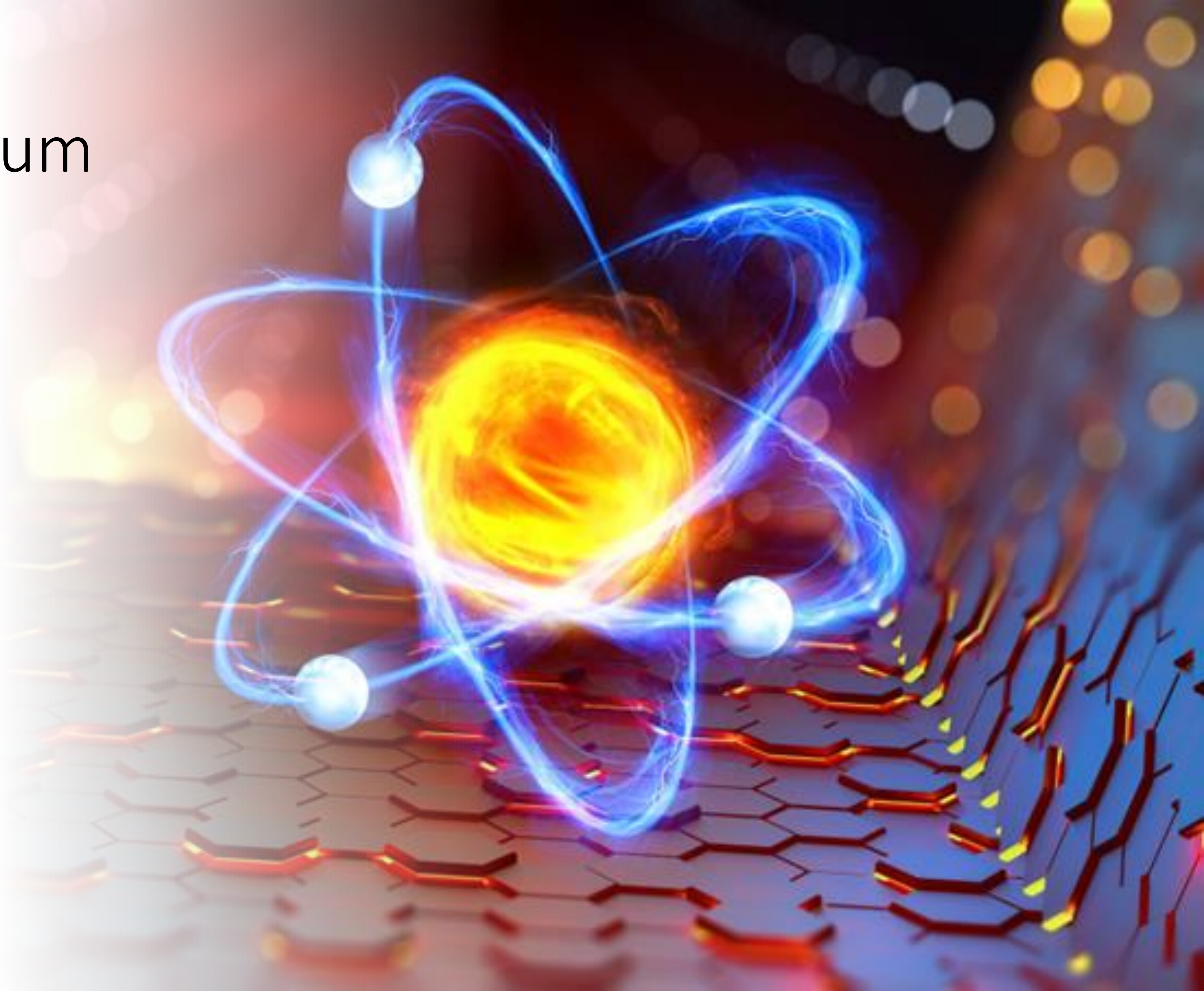
Applications

Dec 13, 2024 / 10:52 AM

Google’s Quantum Chip “Willow” Marks an Important Milestone in Quantum Computing

What is Quantum Computing?

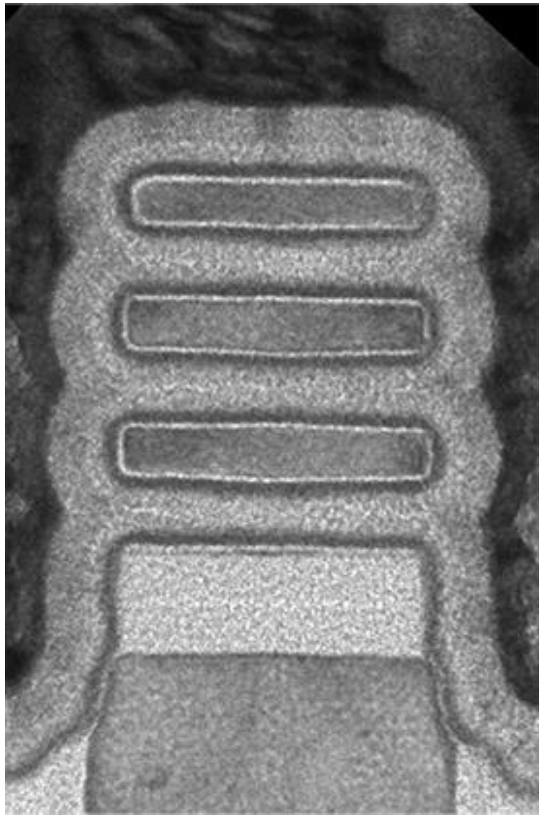
- Computation with coherent atomic-scale dynamics. [Lee Spector]
- Computation that takes advantage of quantum mechanical phenomena. [Wikipedia]
- A rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers. [ibm.com]



Why Quantum Computing?

SCALE

- Because the higher and higher integration scale will eventually lead to quantum computational devices
- IBM's 2 nm MOSFET (metal–oxide–semiconductor field-effect transistor) – 2024?
  - Size: 5 atoms
- Single atom transistor
  - M. Fuechsle et al., A single-atom transistor, Nature Nanotechnology 7: 242–246 (2012)
- Beyond atomic scale?

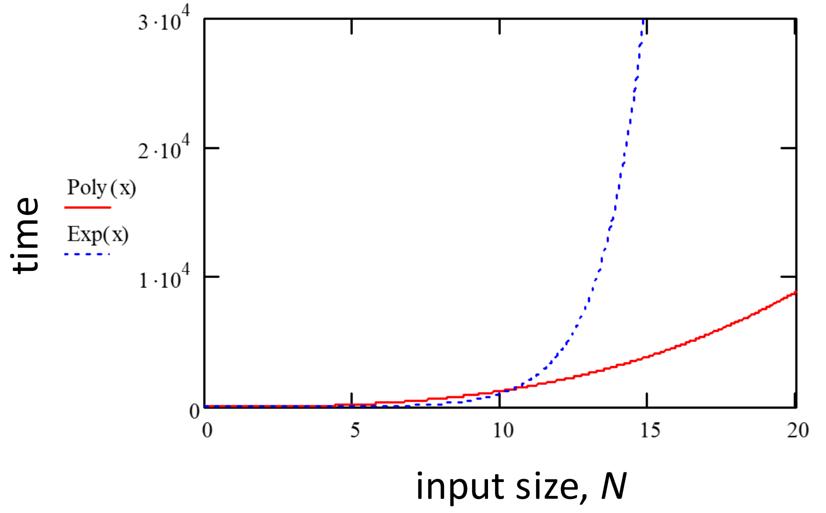


A 2 nm transistor.
Source: research.ibm.com

Why Quantum Computing?

COMPLEXITY

- Because the quantum algorithms are better than their classical counterparts
- Factoring large integers (Shor's algorithm) in $\mathcal{O}\left((\log N)^2(\log\log N)\right)$ time
  —polylogarithmic
  - Classical: NFS, $\mathcal{O}\left(e^{1.9(\log N)^{1/3}}(\log\log N)^{2/3}\right)$ time
  —subexponential
- Searching in unstructured search spaces (Grover's algorithm) in $\mathcal{O}\left(\sqrt{N}\right)$
  - Classical $\mathcal{O}(N)$
  —linear



Discrepancy between polynomial and exponential complexity

Exponential speedup impact

Factor a 5000-digit number

- On a classical computer (1ns/step)
  - The classical algorithm will require more than **5 trillion years**
  - The universe is ~10-16 billion years old

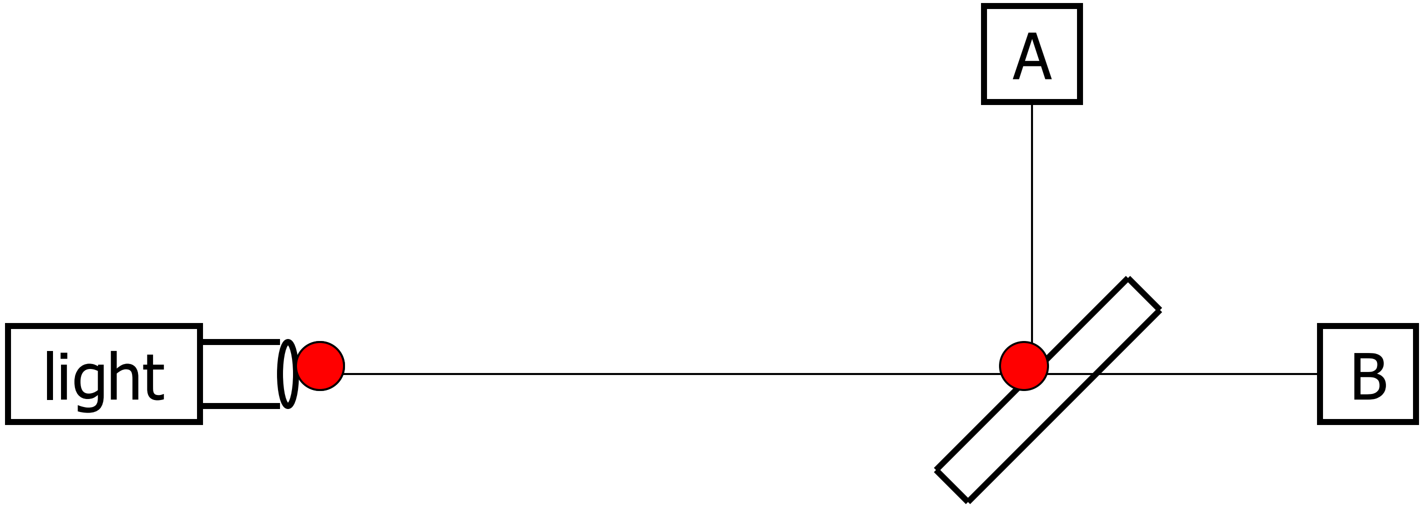
- On a quantum computer (1ns/step)
  - Shor's algorithm will require over **2 minutes**

The power of Quantum Computing

- In quantum systems **possibilities count**, even if they never happen!

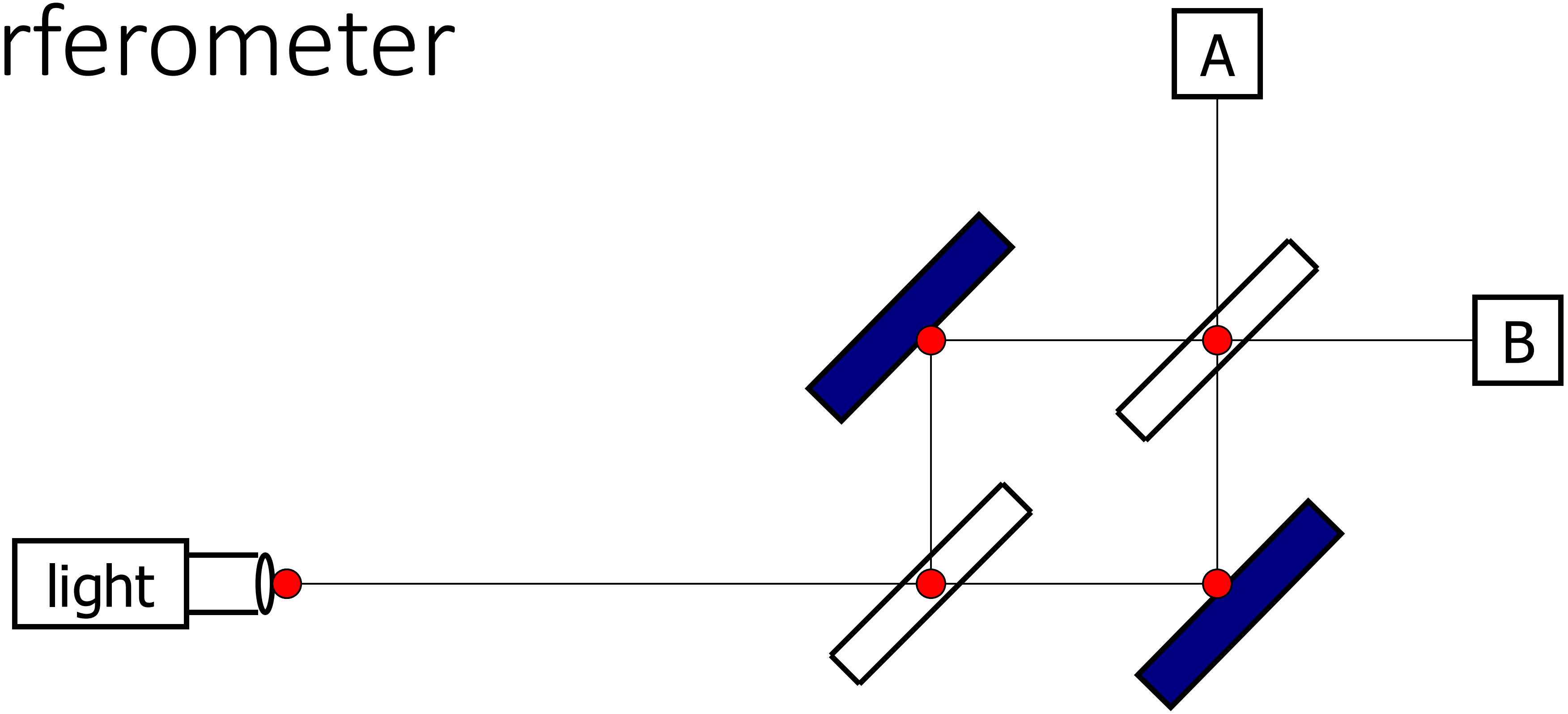
- Each of the **exponentially many** **possibilities** can be used to perform a part of that computation
  - **At the same time!**

Beam Splitter



- Photons leaving the light source
  - Half arrive at detector A;
  - Half arrive at detector B.

Interferometer

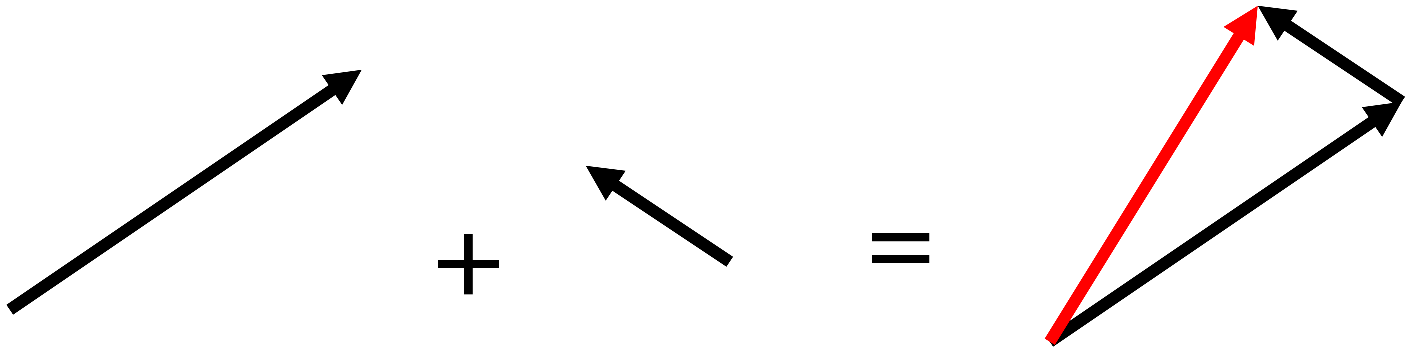


- Equal path lengths, rigid mirrors
- Only 1 photon in the apparatus at a time
- All of the photons leaving the light source arrive at detector B. WHY?

Possibilities count – computing interference

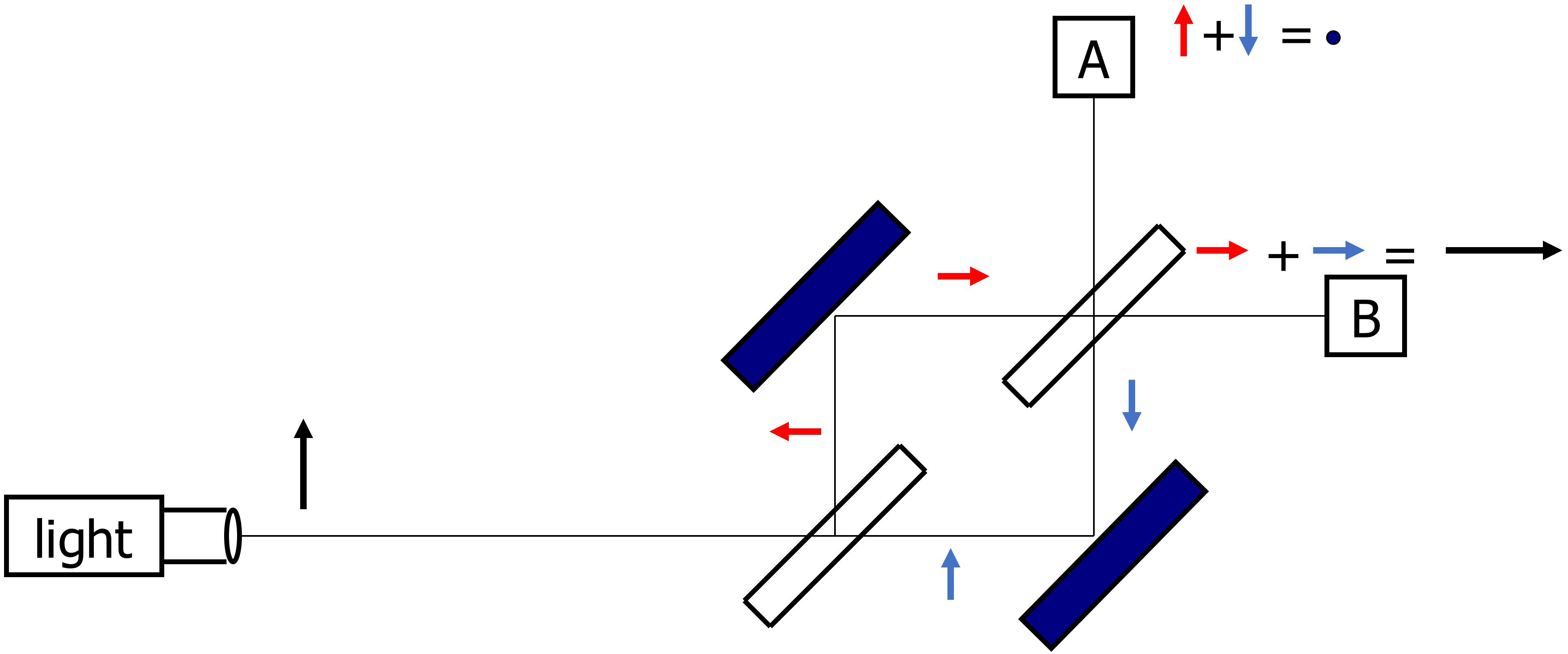
- “You will have to brace yourselves for this – not because is difficult to understand, but because it is absolutely ridiculous: All we do is draw little arrows on a piece of paper – that’s all!” – Richard Feynman
- Arrows for each possibility
- Arrows rotate; speed depends on frequency
- Arrows flip 180^o at mirrors, rotate 90^o counter-clockwise when reflected from beam splitters

Adding arrows



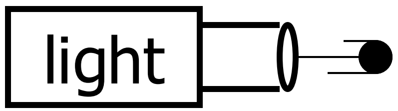
A	B	Sum
←	←	⟵
↖	↙	←
↑	↓	•
↗	↘	→
→	→	⟶
↘	↗	→
↓	↑	•
↙	↖	←
←	←	⟵

Possibilities count even if they do not happen



- The amplitudes can interfere constructively and destructively, even though each photon takes only one path
- The amplitudes at detector A interfere destructively; those at detector B interfere constructively

A photon-triggered bomb

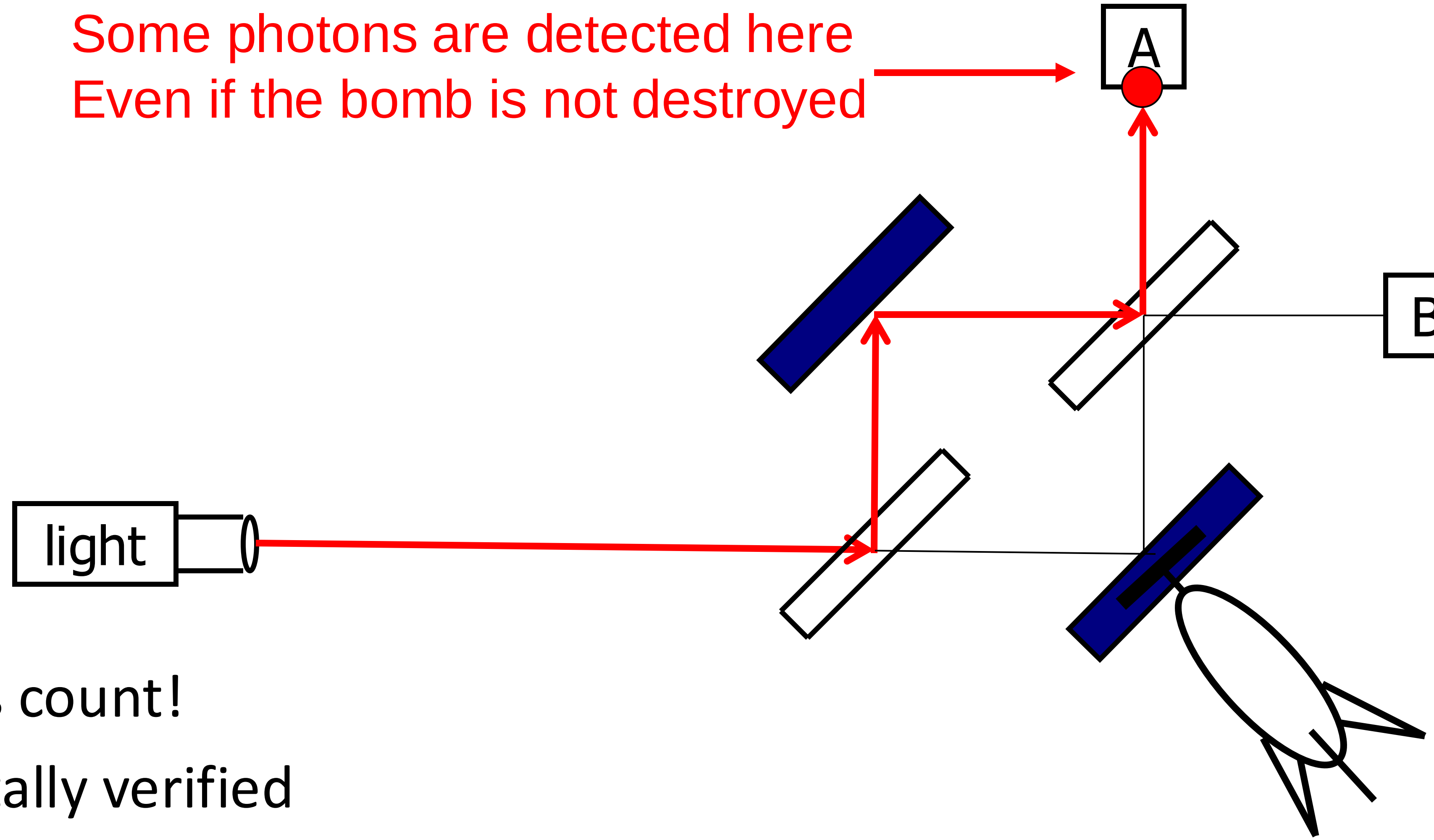


- A mirror is mounted on a plunger on the bomb’s nose
- A single photon hitting the mirror depresses the plunger and explodes the bomb

Bomb problem

- Some plunger are stuck, producing duds
- How can you find a good, unexploded bomb?

Elitzur-Vaidman bomb test



- Possibilities count!
- Experimentally verified
- Can be enhanced to reduce or eliminate bomb loss

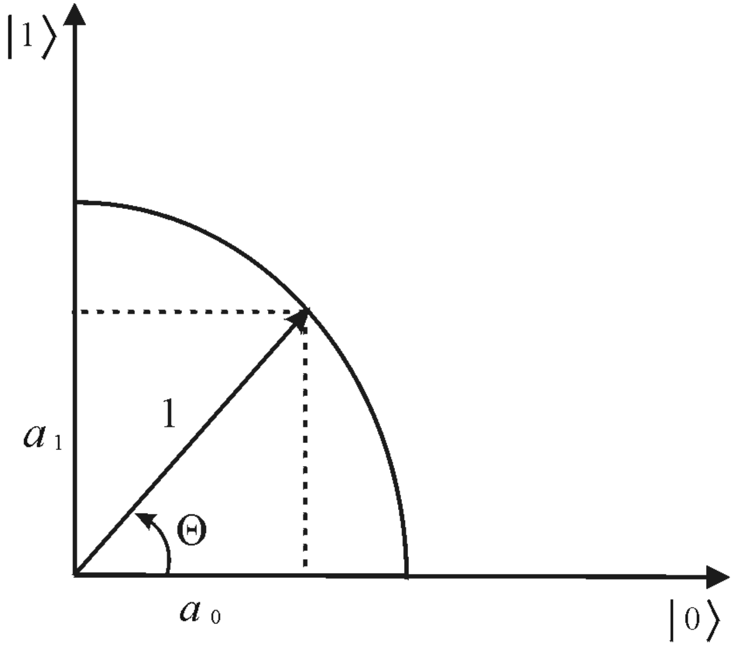
Quantum states

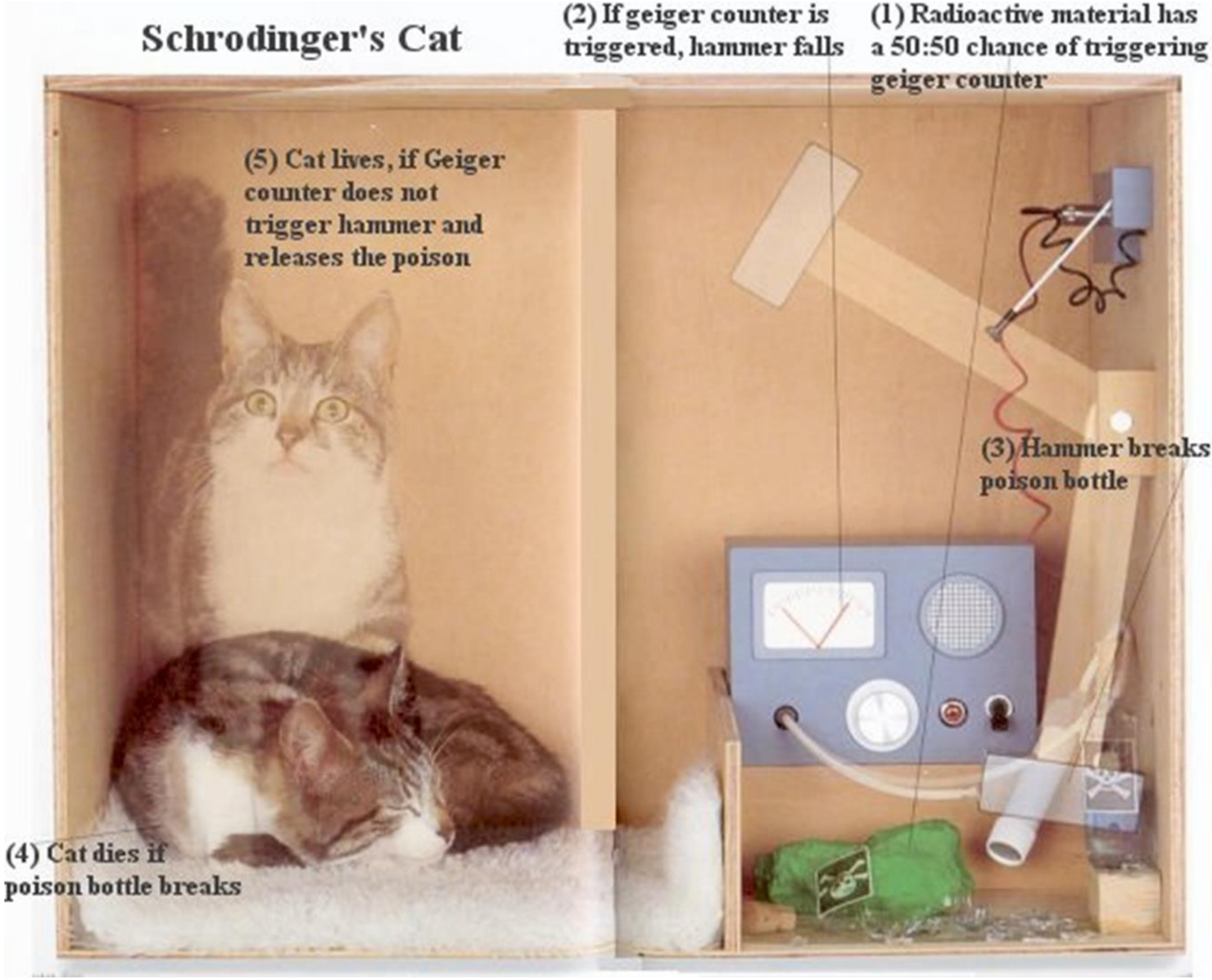
QUBIT

$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$; $a_0, a_1 \in \mathbb{C}$

Basis $\rightarrow \{|0\rangle, |1\rangle\}$

Measurement $\rightarrow |0\rangle$ or $|1\rangle$





Quantum register

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i\,|i\rangle, \text{with } \sum_{\mathrm{i}=0}^{2^n-1} |a_i|^2 = 1$$

$$|\psi\rangle = \sum_{c_0 c_1 \dots c_{n-1} \in \mathbb{B}^n} a_{c_0 c_1 \dots c_{n-1}} |c_0 c_1 \dots c_{n-1}\rangle, \text{ where } \sum_{c_0 c_1 \dots c_{n-1} \in \mathbb{B}^n} \left|a_{c_0 c_1 \dots c_{n-1}}\right|^2 = 1$$

$$\left|\psi_{2-qubit}\right\rangle = a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle, \text{ where } \sum_{i=0}^{3} |a_i|^2 = 1$$

Quantum register example

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} = \left\{\begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\right\}$$

$$|\psi_{2-qubit}\rangle = \begin{bmatrix}a_0\\a_1\\a_2\\a_3\end{bmatrix}, \text{where } \sum_{i=0}^{3} |a_i|^2 \quad = 1$$

$$|\psi_A\psi_B\rangle = |\psi_A\rangle \otimes |\psi_B\rangle = \begin{bmatrix}a_{A0}\\a_{A1}\end{bmatrix} \otimes \begin{bmatrix}a_{B0}\\a_{B1}\end{bmatrix} = \begin{bmatrix}a_{A0}\cdot a_{B0}\\a_{A0}\cdot a_{B1}\\a_{A1}\cdot a_{B0}\\a_{A1}\cdot a_{B1}\end{bmatrix}$$

$$|\psi_A\rangle = a_{A0}|0\rangle + \ a_{A1}|1\rangle = \begin{bmatrix}a_{A0}\\a_{A1}\end{bmatrix}$$

$$|\psi_B\rangle = a_{B0}|0\rangle + \ a_{B1}|1\rangle = \begin{bmatrix}a_{B0}\\a_{B1}\end{bmatrix}$$

$$|\psi_A\psi_B\rangle = |\psi_A\rangle \otimes |\psi_B\rangle = a_{A0}a_{B0}|00\rangle + \ a_{A0}a_{B1}|01\rangle + a_{A1}a_{B0}|10\rangle + a_{A1}a_{B1}|11\rangle \in \boldsymbol{\mathcal{H}}^4$$

Tensor product

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i\,|i\rangle, \text{ with } \sum_{i=0}^{2^n-1} |a_i|^2 = 1$$

$$|\psi\rangle \otimes |\phi\rangle = |\psi\phi\rangle = \sum_{i=0}^{2^n-1}\sum_{j=0}^{2^m-1} a_i b_j |i,j\rangle$$

$$|\phi\rangle = \sum_{i=0}^{2^m-1} b_i\,|i\rangle, \text{ with } \sum_{i=0}^{2^m-1} |b_i|^2 = 1$$

$$|\psi\rangle \otimes |\phi\rangle = |\psi\phi\rangle = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{2^n-1} \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{2^m-1} \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ \vdots \\ a_0 b_{2^m-1} \\ \vdots \\ a_{2^n-1} b_0 \\ \vdots \\ a_{2^n-1} b_{2^m-1} \end{bmatrix}$$

Unitary transformations

- Transforms a basis state into a superposition
- Parallel transform of all superposed states
- All transformations are reversible
- Unitary: $U \cdot U^{\dagger} = I$
- Implemented with quantum gates

$$U = \begin{bmatrix} u_{00} & \cdots & u_{0,2^n-1} \\ \vdots & \ddots & \vdots \\ u_{2^n-1,0} & \cdots & u_{2^n-1,2^n-1} \end{bmatrix}$$

$$U|\psi\rangle = U \sum_{i=0}^{2^n-1} a_i \, |i\rangle = \sum_{i=0}^{2^n-1} U a_i |i\rangle$$

$$U = \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} |x\rangle \cdot u_{xy} \cdot \langle y|, \text{ where } \sum_{i=0}^{2^n-1} u_{ix}^* \cdot u_{iy} = \delta_{xy}$$

Universal quantum gate sets

- Deutsch

Universal gate

$$D(\theta) : |x, y, z\rangle \Rightarrow \begin{cases} i\cos\theta|x, y, z\rangle + \sin\theta|x, y, 1 - z\rangle & x = y = 1 \\ |x, y, z\rangle & \text{otherwise} \end{cases}$$

- Di Vincenzo

$$U_2(\omega, \alpha, \beta, \varphi) = \mathrm{e}^{-\mathrm{i}\varphi} \begin{bmatrix} \mathrm{e}^{\mathrm{i}\alpha}\cos\omega & -\mathrm{e}^{-\mathrm{i}\varphi}\sin\omega \\ \mathrm{e}^{\mathrm{i}\varphi}\sin\omega & \mathrm{e}^{-\mathrm{i}\alpha}\cos\omega \end{bmatrix}$$

$$XOR = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Universal gate set

Quantum gates

- Pseudo-classical operators

$$PC|\psi\rangle = PC\sum_{i=0}^{2^n-1} a_i\,|i\rangle = \sum_{i=0}^{2^n-1} a_i|p(i)\rangle$$

$p(k)$ is a permutation over the basis states

- $XOR: |x, y\rangle \rightarrow |x, x \oplus y\rangle$

$\boxed{1}0 \quad \boxed{1}1$

$$XOR = \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} & \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} & \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} \end{array}$$

- Toffoli Gate:

$TOFF: |x, y, z\rangle \rightarrow |x, y, (x{\cdot}y) \oplus z\rangle$

$\boxed{11}0 \quad \boxed{11}1$

$$TOFF|\psi\rangle = \begin{array}{c} \begin{array}{cccccccc} & & & & & & 110 & \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ 111 \end{array} = \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_7 \\ a_6 \end{bmatrix}$$

Quantum gates

- Hadamard

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

$$\begin{aligned} |\Psi\rangle &= H \otimes H \otimes \cdots H|00\ldots 0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \cdots \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2^{\frac{n}{2}}}(|00\cdots 00\rangle + |00\cdots 01\rangle + \cdots |11\cdots 11\rangle) \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{i=0}^{2^n-1} |i\rangle \end{aligned}$$

- Conditional not

$$CNOT_{(n+1)-qubit}: |x_0, x_1 \ldots, x_{n-1}, z\rangle \rightarrow \left|x_0, x_1 \ldots, x_{n-1}, \left(\Lambda_{i=0}^{n-1} x_i\right) \otimes z\right\rangle$$

$$CNOT = \begin{bmatrix} 1 & 0 & \cdots & & & 0 \\ 0 & 1 & & & & \\ \vdots & & \ddots & & & \vdots \\ & & & 1 & 0 & 0 \\ & & & 0 & 0 & 1 \\ 0 & & \cdots & 0 & 1 & 0 \end{bmatrix}$$

- Conditional phase shift

$$P(\varepsilon)|c_0 c_1 \ldots c_{n-1}\rangle \rightarrow \begin{cases} e^{i\varepsilon}|c_0 c_1 \ldots c_{n-1}\rangle, if\ c_0 c_1 \ldots c_{n-1} = 11\cdots 1 \\ |c_0 c_1 \ldots c_{n-1}\rangle, otherwise \end{cases}$$

$$P_{n-qubit}(\varepsilon) = \begin{bmatrix} 1 & 0 & 0 & \cdots & & 0 \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ \vdots & & & \ddots & & \vdots \\ & & & & 1 & 0 \\ 0 & & & \cdots & 0 & e^{i\varepsilon} \end{bmatrix}$$

Interference

$$H: \begin{cases} |0\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$$

$$H \cdot H: |0\rangle \rightarrow H: \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] = |0\rangle$$

$$H \cdot H: |1\rangle \rightarrow H: \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \rightarrow \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) - \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] = |1\rangle$$

$$H \cdot H: |0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

$$H \cdot H: |1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}}\begin{bmatrix} +1 \\ -1 \end{bmatrix} \rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

Other important features

- Entanglement

$$|\rho\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

$\neg\exists\ |x\rangle, |y\rangle$ s. t. $|\rho\rangle = |x\rangle \otimes |y\rangle$

- Cloning impossibility

For $|\psi\rangle = a_0|0\rangle + a_1|1\rangle$, $\neg\exists\ U$ and $\neg\exists\ |x\rangle$ so that

$$U: (|\psi\rangle \otimes |x\rangle) = |\psi\rangle \otimes |\psi\rangle$$

The Einstein-Podolsky-Rosen paradox

- Is quantum theory incomplete?
- A theory of a system must have
  - **Realism**: observables characterized by definite values are independent on the measurement performed on the system
  - **Localism**: there is no action at the distance
- Bohm's interpretation of EPR – Alice and Bob receive a pair of particles (Bell state)

$$|\rho\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$$

- Alice and Bob measure the spins of their respective particles
- Assumption of reality and locality => Alice's measurement result will not affect the result of Bob's measurement

The Einstein-Podolsky-Rosen paradox

- Assumption of reality and locality => Alice's measurement result will not affect the result of Bob's measurement

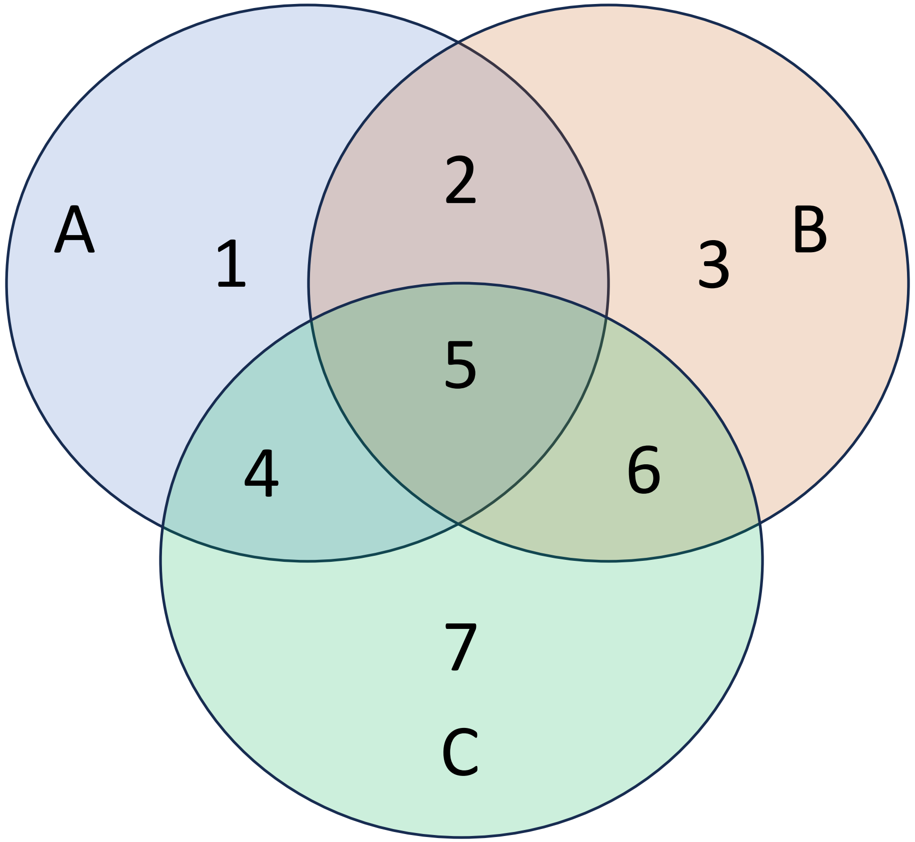
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$$

- If Alice obtains $|0\rangle$ with probability 0.5 => Bob obtains $|1\rangle$ with probability 1
- If Alice obtains $|1\rangle$ with probability 0.5 => Bob obtains $|0\rangle$ with probability 1
- Alice's measurement influences the outcome of Bob's measurement
- Quantum mechanics is a nonlocal theory => EPR paradox

Bell inequality

A not B + B not C ≥ A not C

1 + 4 + **2** + 3 ≥ 1 + 2



CHSH Bell inequality

- A tool to invalidate the assumptions of the EPR paradox
- Charlie prepares a system of 2 particles in a given state, many times
- Charlie sends 1 particle to Alice, 1 particle to Bob (at a distant location)
- Alice and Bob measure their particles and repeat this experiment many times
- Alice can measure 2 observables on her particle: A_1 and A_2
- Bob measures 2 observables on his particle: B_1 and B_2
- We encode the outcomes (considered binary) as 1 and -1
- Alice and Bob chose randomly which of the 2 observables to measure
- Alice and Bob perform measurement simultaneously
- Assumption: the measurement of an observer cannot disturb the outcome of the other observer (they are situated at a distance)

CHSH Bell inequality

We can state

$A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2 = (A_1 + A_2)B_1 + (A_1 - A_2)B_2$

But $A_1 = \pm 1$ and $A_2 = \pm 1$, so $A_1 + A_2 = 0$ or $A_2 - A_1 = 0$

$\Rightarrow A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2 = \pm 2$

$p(a_1,a_2,b_1,b_2) \in [0, 1]$; $A_1 = a_1$, $A_2 = a_2$, $B_1 = b_1$, $B_2 = b_2$

$$\sum_{a_1,a_2,b_1,b_2} p(a_1,a_2,b_1,b_2) = 1$$

CHSH Bell inequality

The mean of A_1B_1 is $$E(A_1B_1) = \sum_{a_1,a_2,b_1,b_2} p(a_1,a_2,b_1,b_2)\, a_1b_1$$

$$E(A_1B_1 + A_2B_1 + A_2B_2 - A_1B_2) = \sum_{a_1,a_2,b_1,b_2} p(a_1,a_2,b_1,b_2)\,(a_1b_1+a_2b_1+a_2b_2-a_1b_2) \le 2 \sum_{a_1,a_2,b_1,b_2} p(a_1,a_2,b_1,b_2) = 2$$

$$E(A_1B_1 + A_2B_1 + A_2B_1 - A_1B_2) = E(A_1B_1) + E(A_2B_1) + E(A_2B_2) - E(A_1B_2) \le 2$$

But if the state prepared by Charlie is $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)$

then $< A_1B_1 > + < A_2B_1 > + < A_2B_2 > - < A_1B_2 > \; = \; 2\sqrt{2}$

=> CHSH-Bell inequality is violated and EPR assumption of realism is wrong

Quantum functions

- Pseudo-classic operator *f* over *n* input qubits and *m* output qubits:

$$F_{n,m}: |k\rangle \otimes |0\rangle = |k, 0\rangle \to |k, f(k)\rangle = |k\rangle \otimes |f(k)\rangle$$

- Could be applied over a superposition:

$$F: \frac{1}{2^{\frac{n}{2}}} \sum_{i=0}^{2^n-1} |i\rangle\,|0\rangle \to \frac{1}{2^{\frac{n}{2}}} \sum_{i=0}^{2^n-1} |i\rangle\,|f(i)\rangle$$

- Measurement (input register)

$$\frac{1}{2^{\frac{n}{2}}} \sum_{i=0}^{2^n-1} |i\rangle\,|f(i)\rangle \xrightarrow{\text{measurement}} |q\rangle|f(q)\rangle$$

- Measurement (output register) and $f(j_0) = \mathrm{f}(j_1) = \ldots = \mathrm{f}(j_{w\text{-}1}) = q$

$$\frac{1}{2^{\frac{n}{2}}} \sum_{i=0}^{2^n-1} |i\rangle\,|f(i)\rangle \xrightarrow{\text{measurement}} \frac{1}{\sqrt{w}} \sum_{i=0}^{w-1} |j_i\rangle|q\rangle$$

Grover's algorithm

- We consider that the problem has k solutions, $1 \le k \le n$
- We can reduce his problem to a decision problem, thus

$$f_d(x) = \begin{cases} 0 & \text{if } x \text{ is not the solution} \\ 1 & \text{if } x \text{ is the solution} \end{cases}$$

- In this context, we can define a quantum oracle as

$$U_O: \underbrace{|x\rangle}_{\text{Index quregister}} \underbrace{|u\rangle}_{\text{Oracle quregister}} \mapsto |x\rangle |f_d(x) \oplus u\rangle$$

- If $|u\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, because $NOT: \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \mapsto (-1)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

- We have:

$$U_O: |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \mapsto (-1)^{f_d(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The Oracle

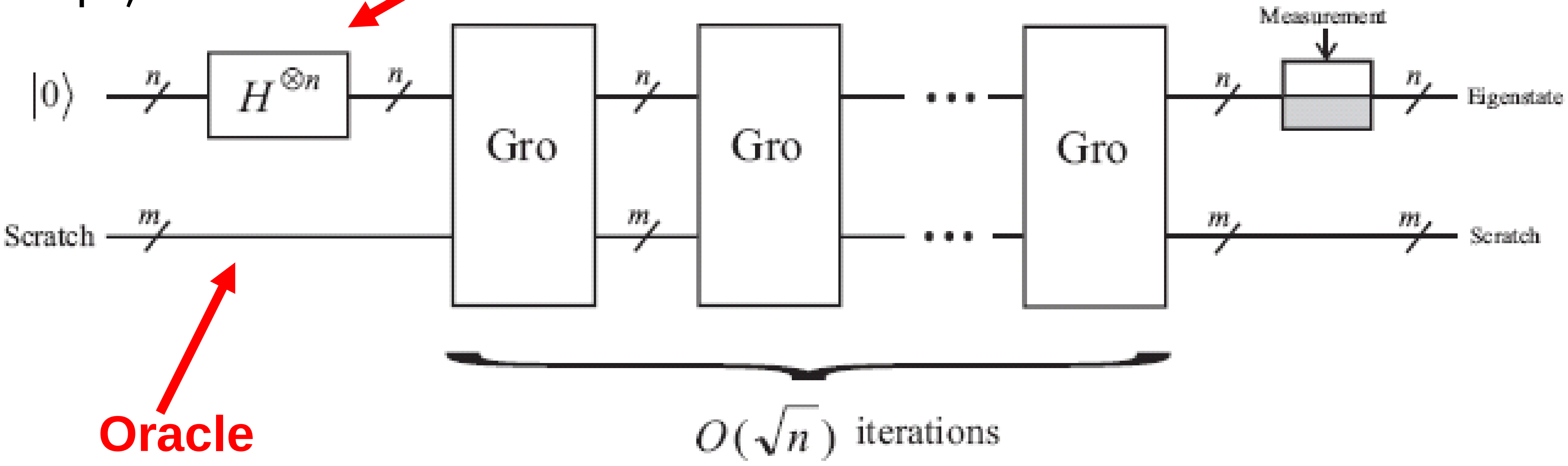
"Marks the Solution"

Grover's algorithm

$$|\psi_i\rangle = H^{\otimes n}|00\ldots0\rangle \mapsto \frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{n-1}|x\rangle$$

Initial state

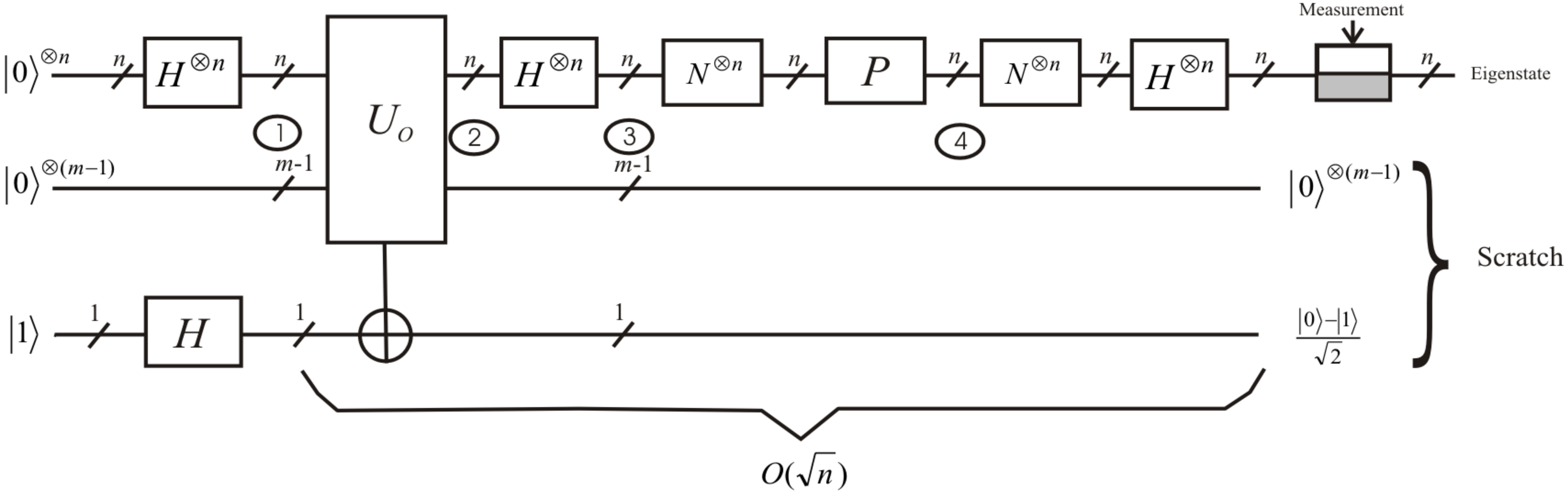
$|0\rangle^{\otimes n}$

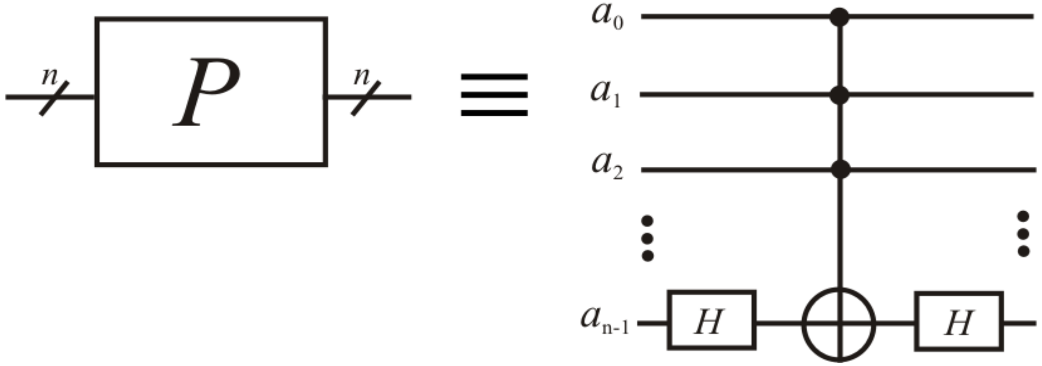


Oracle Workspace

$|0\rangle^{\otimes (m-1)}|1\rangle$

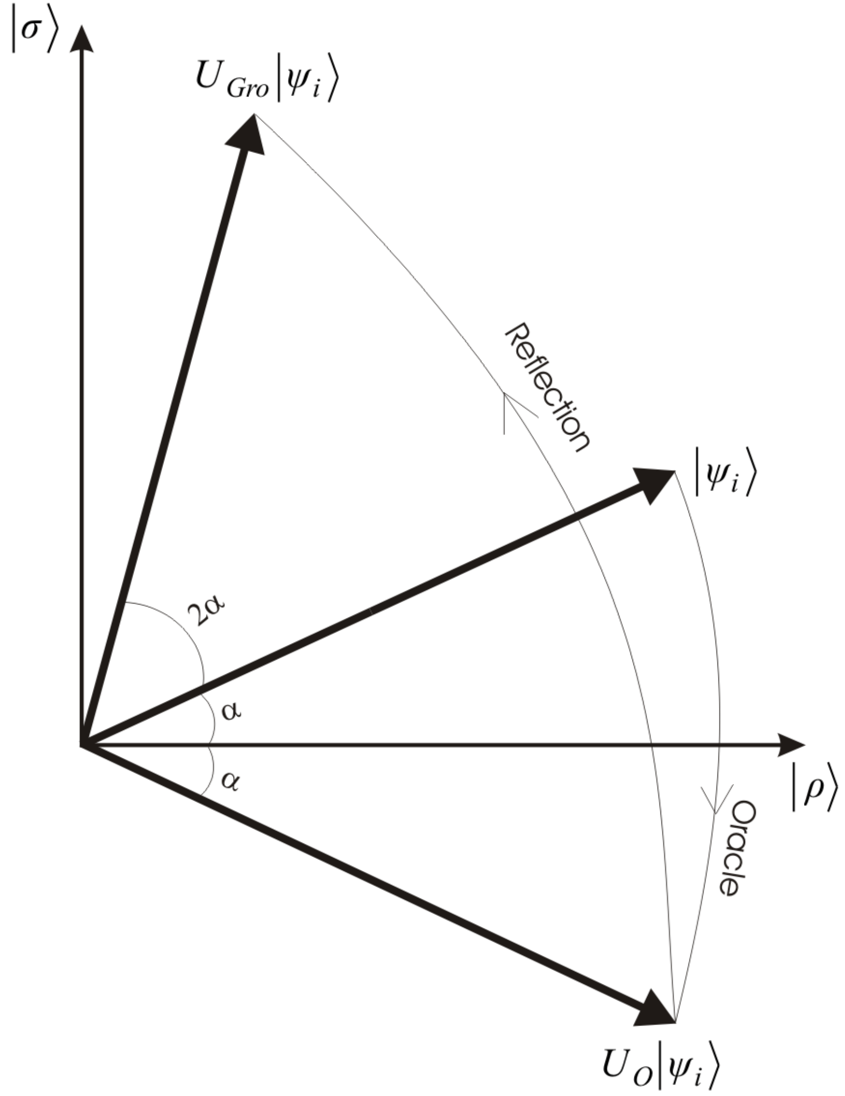
Grover (Gro) circuit





$$U_{Gro} = (2|\psi_i\rangle\langle\psi_i| - I)U_O$$

Grover's algorithm



New basis: $\{|\rho\rangle, |\sigma\rangle\}$

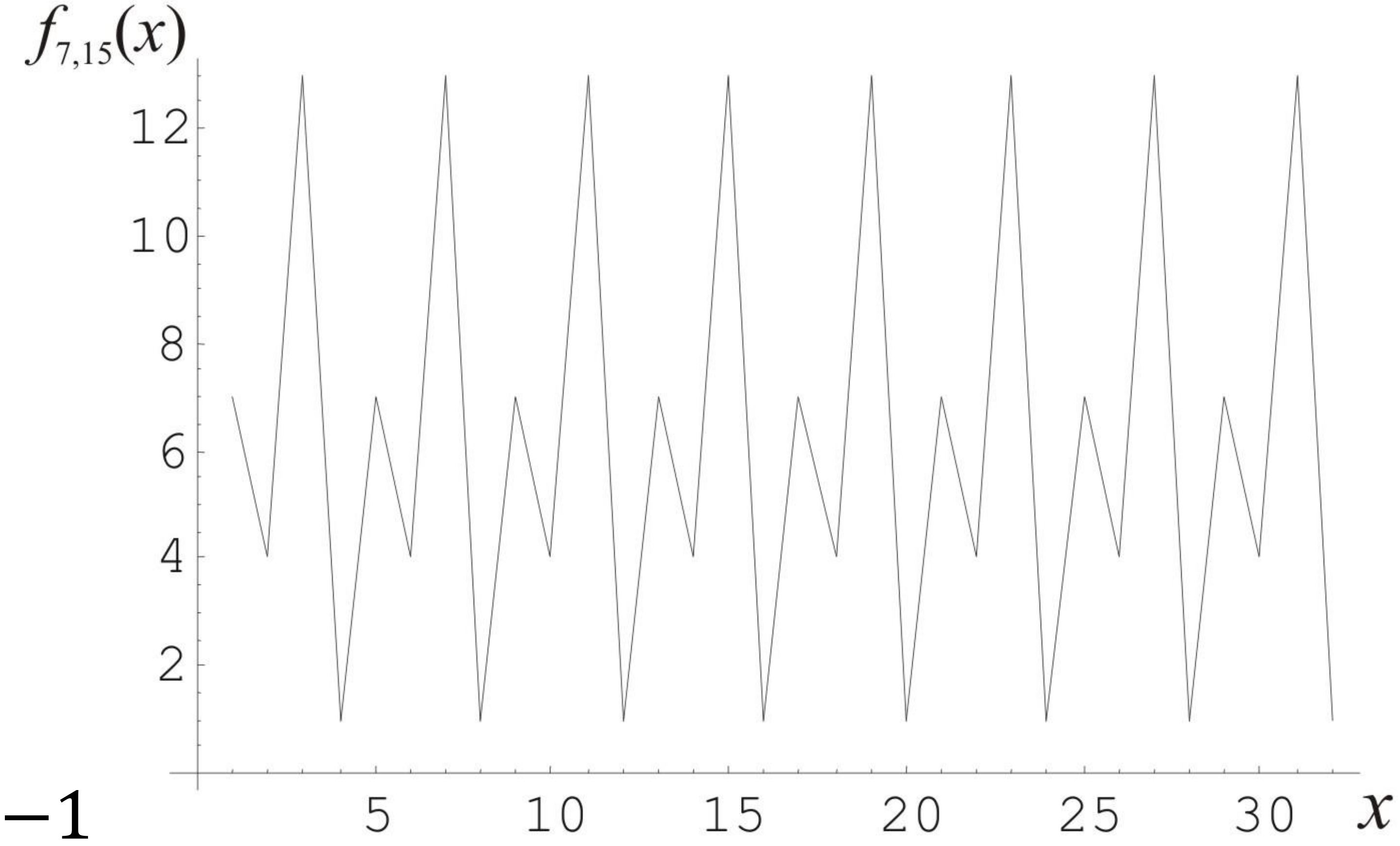
$$|\rho\rangle = \frac{1}{\sqrt{n-k}} \sum_{x \in \bar{S}} |x\rangle \qquad |\sigma\rangle = \frac{1}{\sqrt{k}} \sum_{x \in S} |x\rangle$$

Iterations: $q \leq \left\lceil \frac{\pi}{4} \sqrt{\frac{n}{k}} \right\rceil$

$$O\left(\sqrt{\frac{n}{k}}\right)$$

Shor's algorithm

- Step 1: $|\psi_1\rangle = |\psi_i\rangle|\psi_o\rangle = |0\rangle^{\otimes 2L}|0\rangle^{\otimes 2L}$
- Step 2: $$|\psi_2\rangle = \left(\frac{1}{2^L}\sum_{i=0}^{2^{2L}-1}|i\rangle\right)|0\rangle$$
- Step 3: $$|\psi_3\rangle = \frac{1}{2^L}\sum_{i=0}^{2^{2L}-1}|i\rangle\,|f(i)\rangle$$
  - f is periodic
  $$f_{a,N}(x) = a^x \bmod N$$
  - factors:
  $$\gcd\left(a^{\frac{r}{2}} \pm 1, N\right), r \bmod N \neq -1$$



Shor’s algorithm

- Step 4: output register measurement

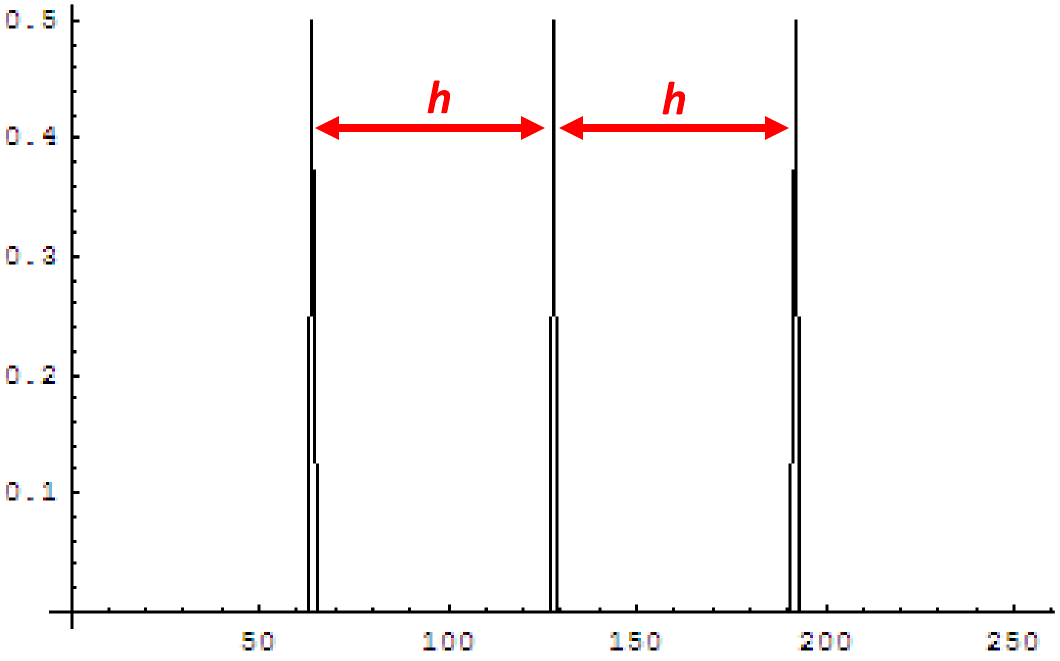
$$|\psi_4\rangle = \sqrt{\left\lceil \frac{r}{2^{2L}} \right\rceil} \sum_{i=0}^{\left\lceil \frac{2^{2L}}{r} \right\rceil - 1} |r \cdot i + b\rangle |m\rangle$$

Result	Post-measure state	Offset
1	$\xi(\lvert 0\rangle + \lvert 4\rangle + \lvert 8\rangle + \ldots)\lvert 1\rangle$	0
4	$\xi(\lvert 3\rangle + \lvert 7\rangle + \lvert 11\rangle + \ldots)\lvert 4\rangle$	3
7	$\xi(\lvert 1\rangle + \lvert 5\rangle + \lvert 9\rangle + \ldots)\lvert 7\rangle$	1
13	$\xi(\lvert 2\rangle + \lvert 6\rangle + \lvert 10\rangle + \ldots)\lvert 13\rangle$	2

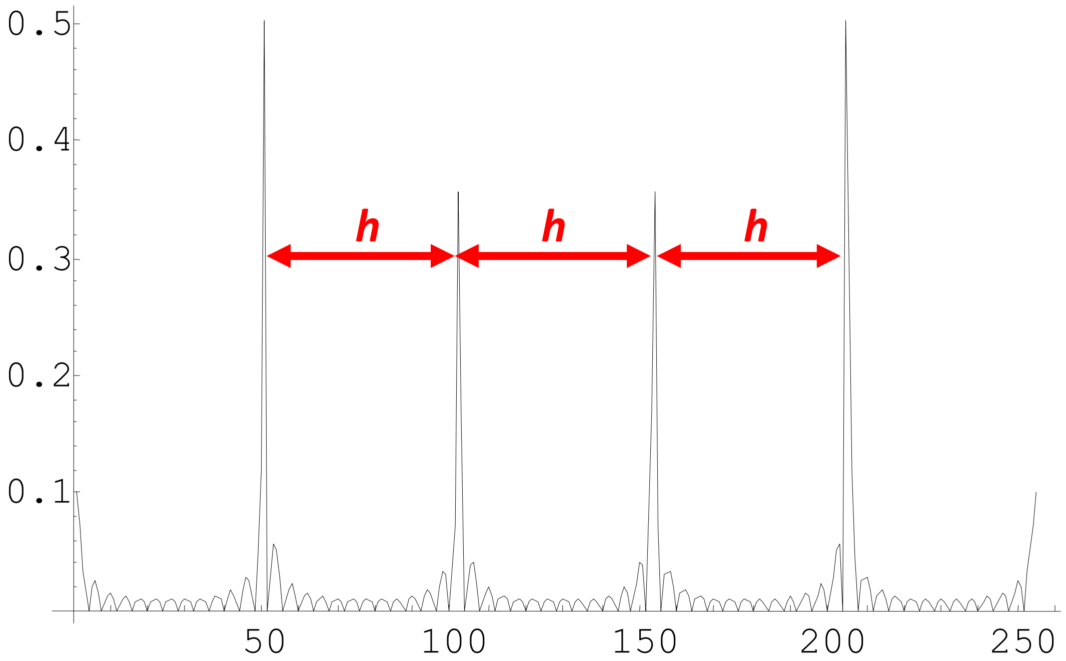
Shor's algorithm (QFFT)

- Step 5: offset removal $|\psi_5\rangle = U_{DFT}|\psi_4\rangle$
  - input register measurement: *h*
  - $h/2^{2L}=a_1/a_2$ is approximated with continued fractions

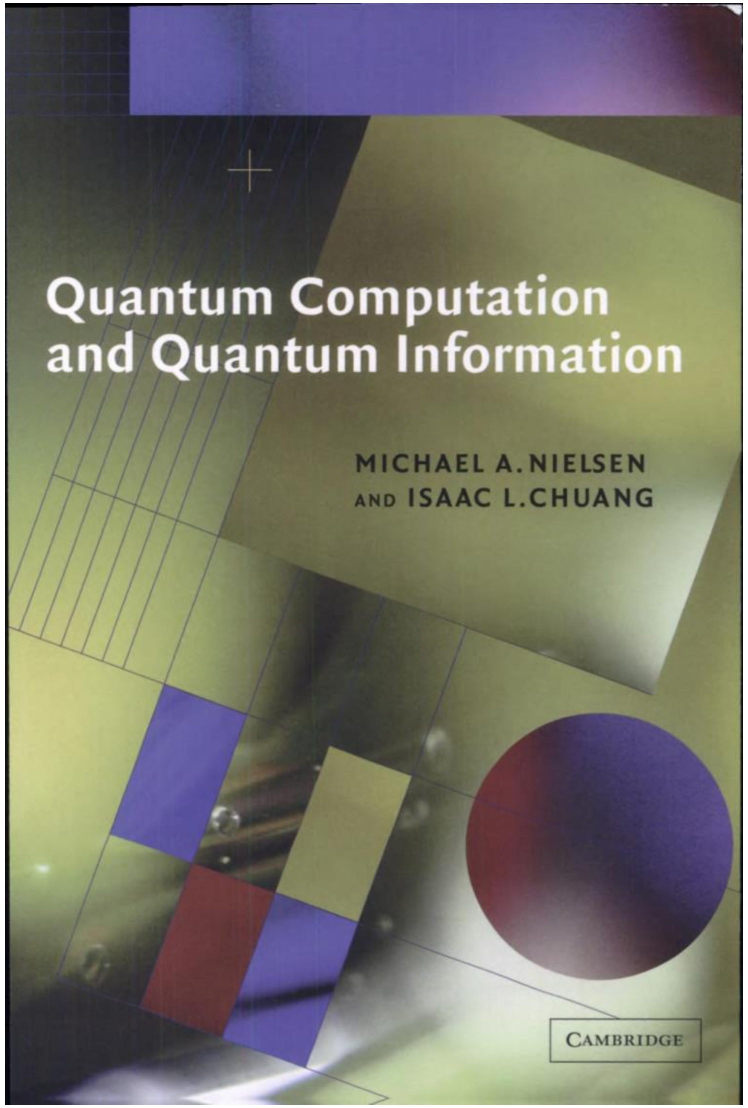
r divides 2^{2L}, peak distance $2^{2L}/r$

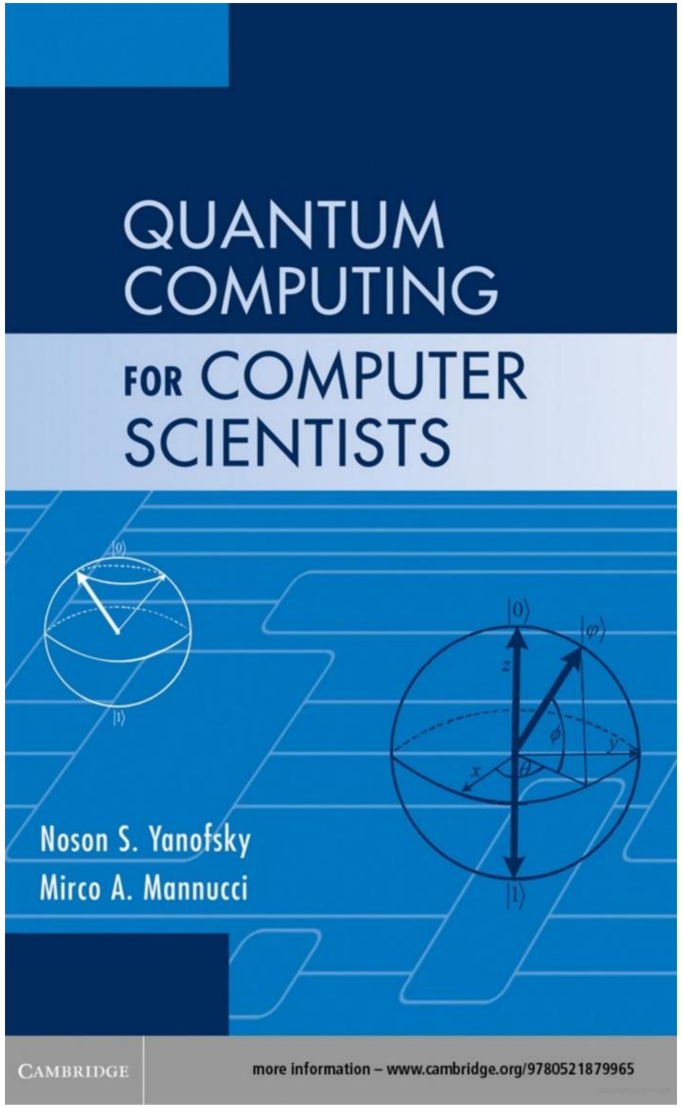


r does not divide 2^{2L}, distinct peak distance $\lceil 2^{2L}/r \rceil$



Books


Quantum Computation and Quantum Information
MICHAEL A. NIELSEN
AND ISAAC L. CHUANG
CAMBRIDGE


QUANTUM COMPUTING
FOR COMPUTER SCIENTISTS
Noson S. Yanofsky
Mirco A. Mannucci
CAMBRIDGE
more information – www.cambridge.org/9780521879965