A pedestrian introduction to quantum computing

Or quantum computing poorly explained by a dummy

jerome.milan (at) lix.polytechnique.fr

June 2010

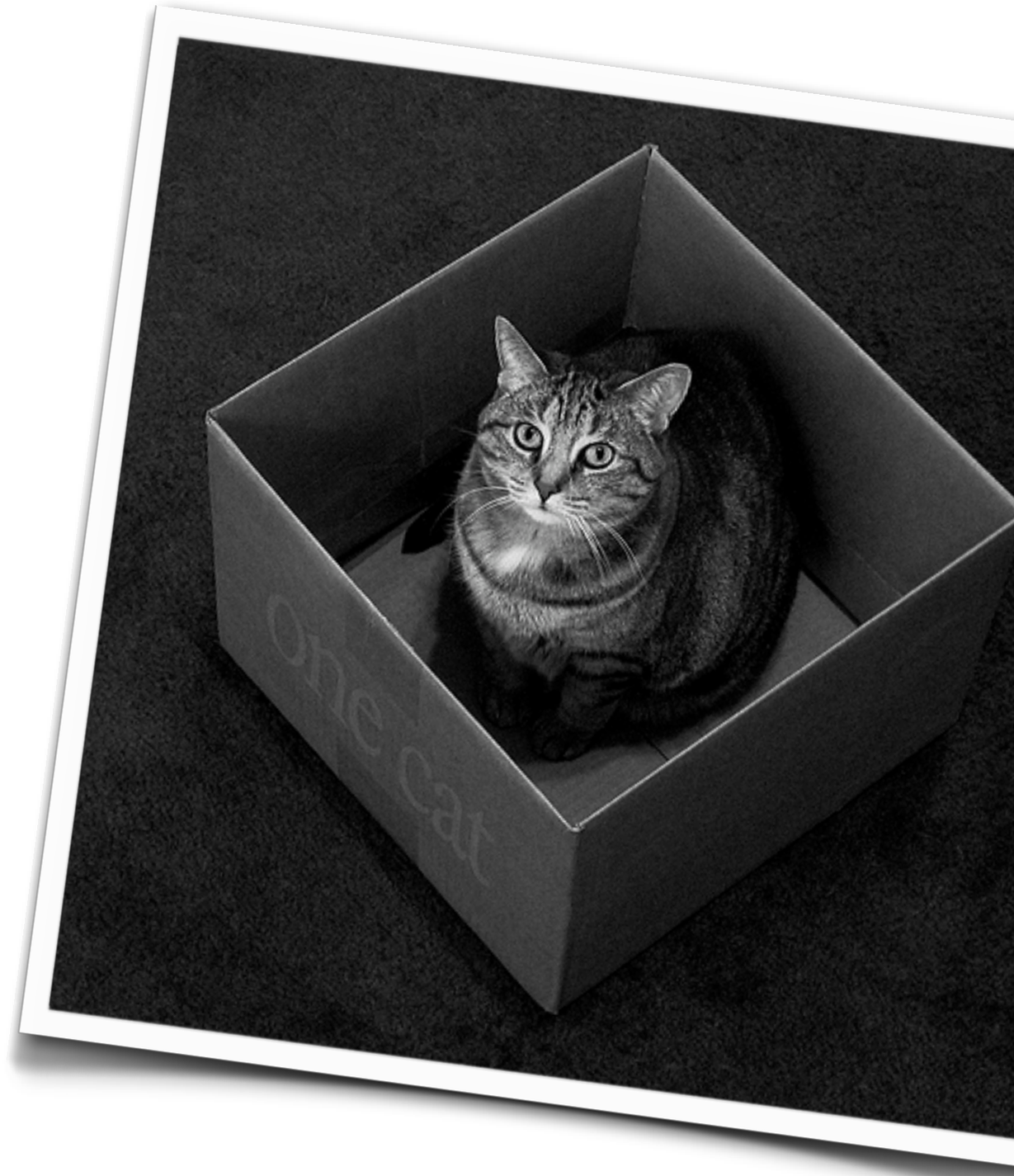
Outline

Quantum computation

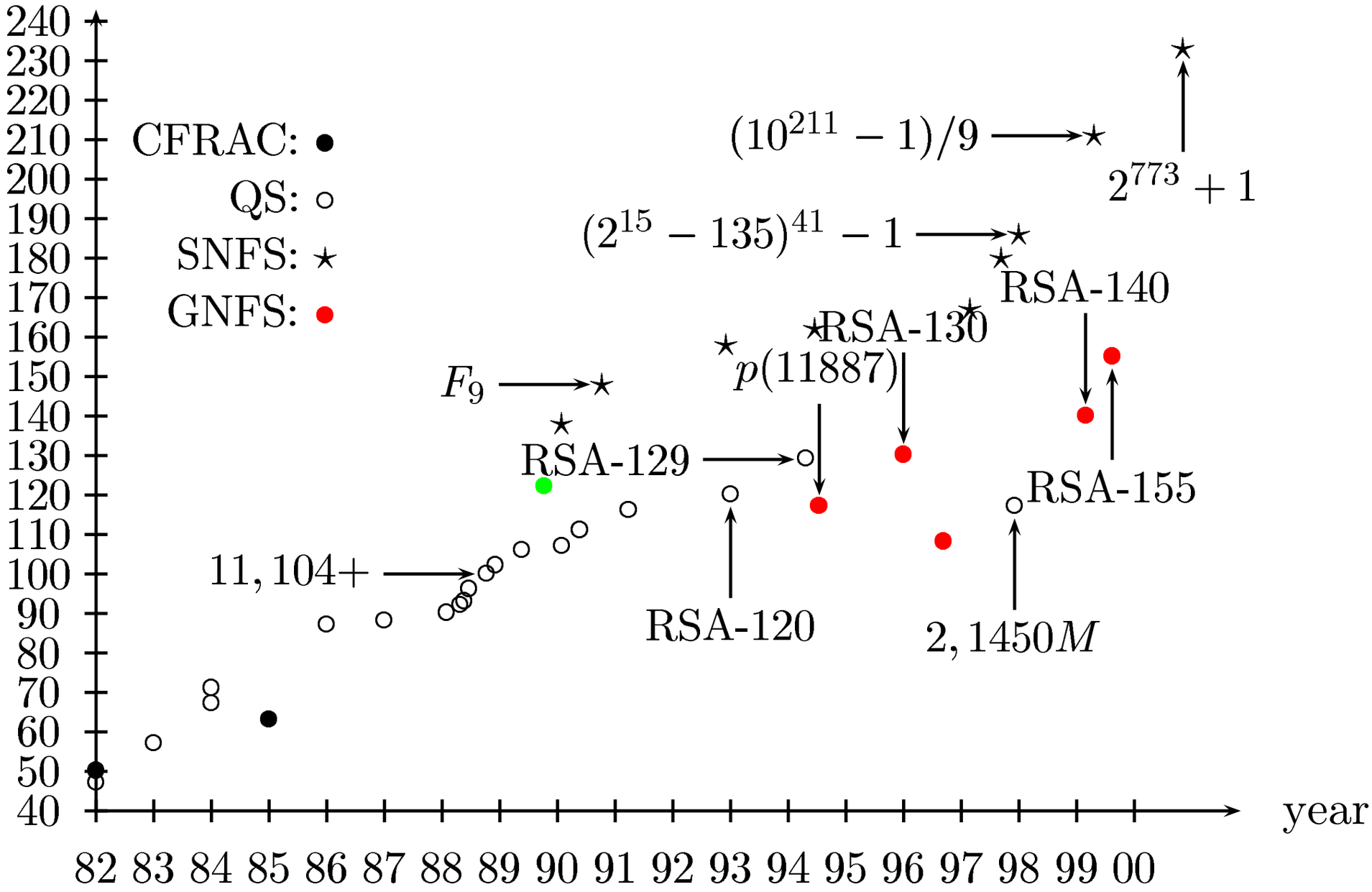
Shor's algorithm

Grover's algorithm

Quantum communication



Introduction – Factorization records



From "Thirty Years of Integer Factorization", F. Morain, 2001

Introduction – Factorization records

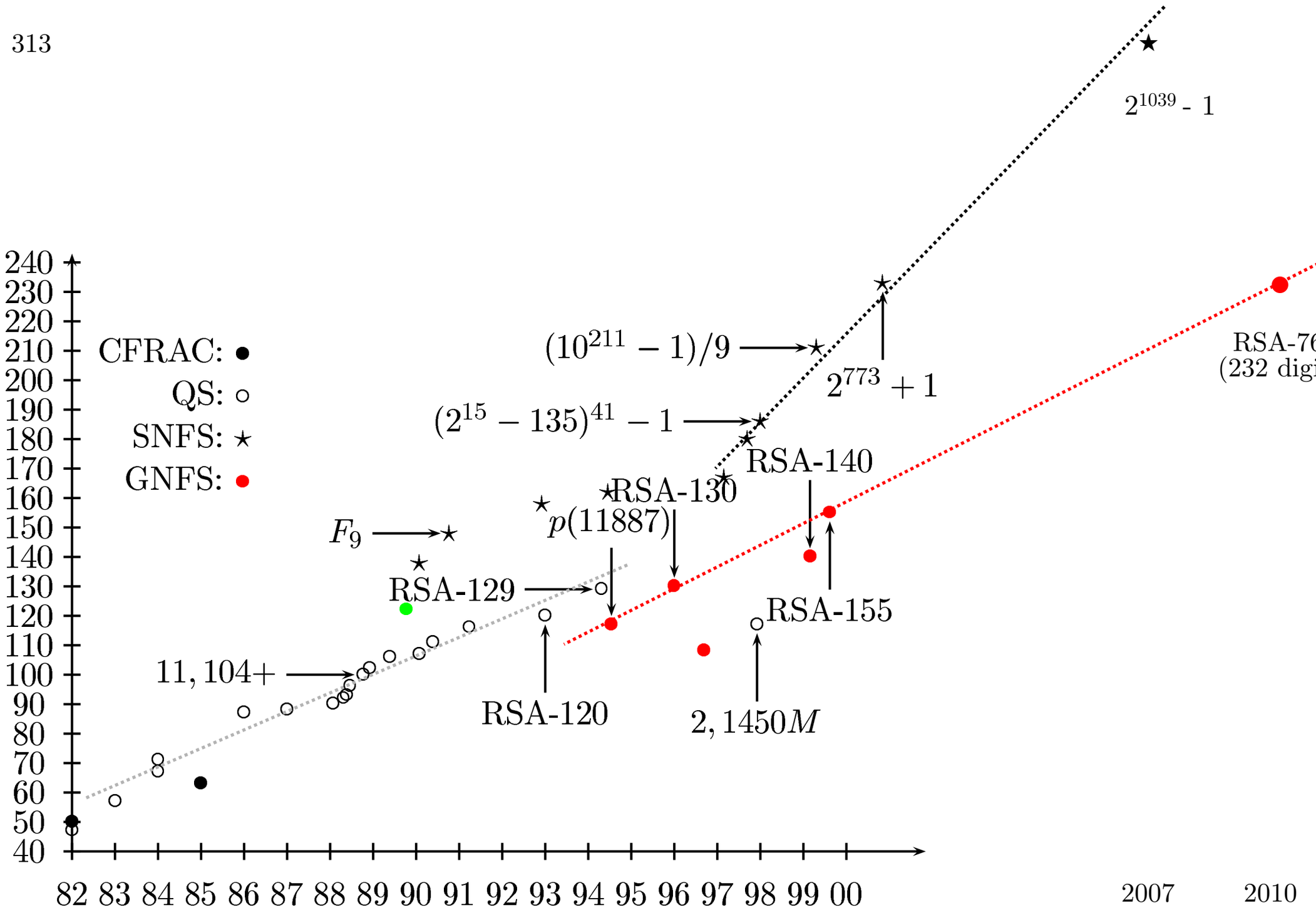
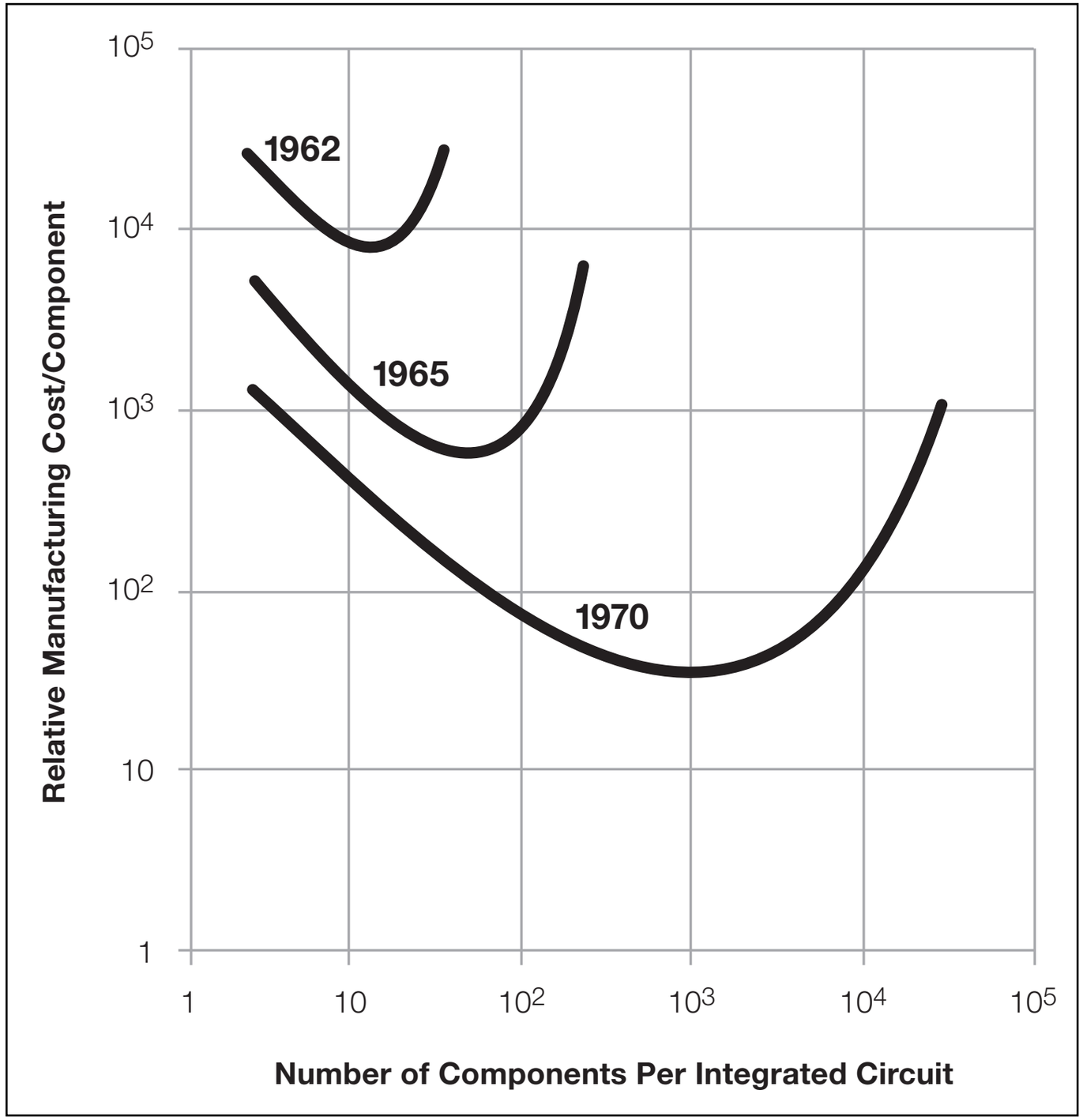


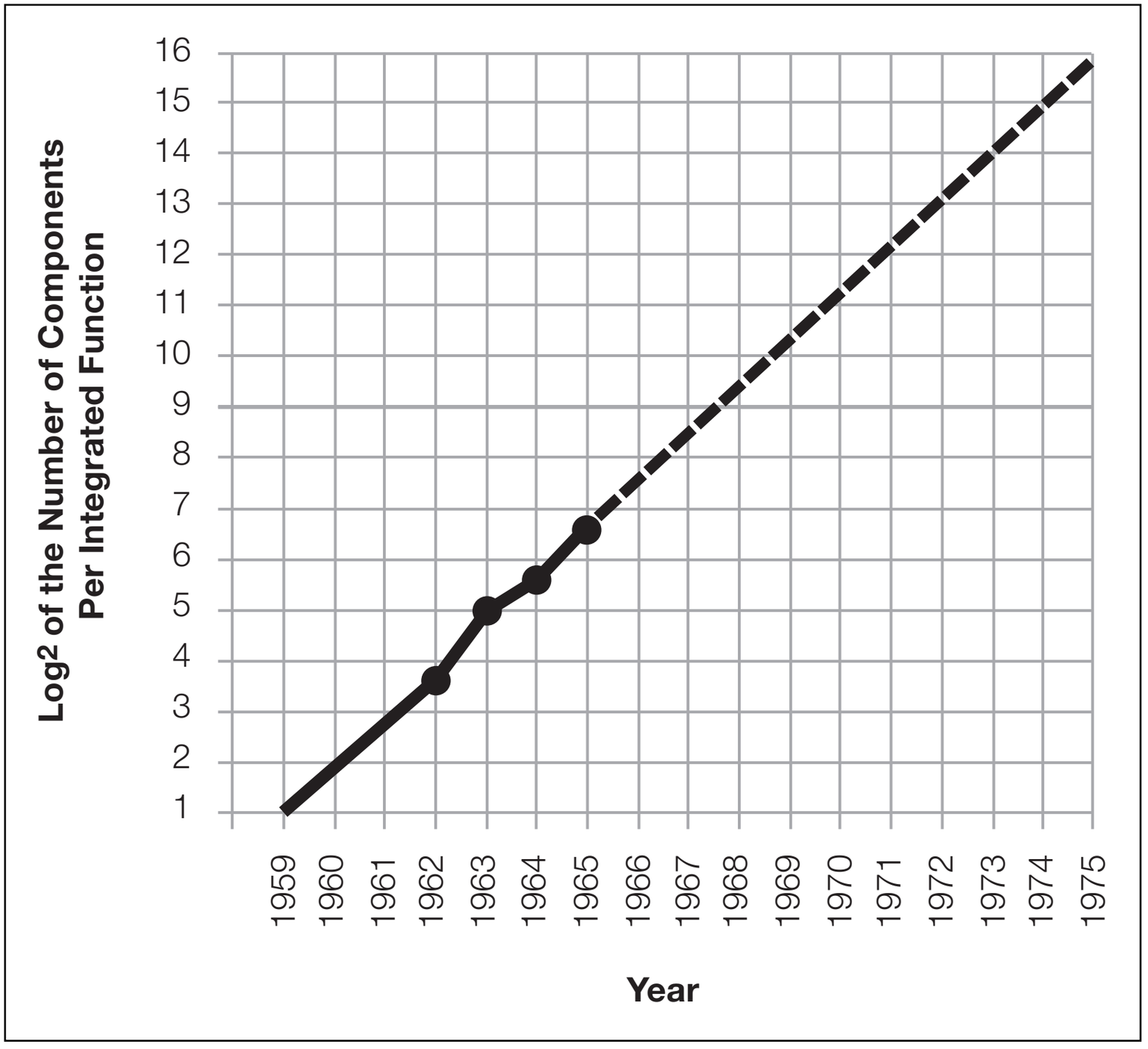
FIGURE 1. Size in bits of the factored numbers depending on the year.

Introduction – Moore's law



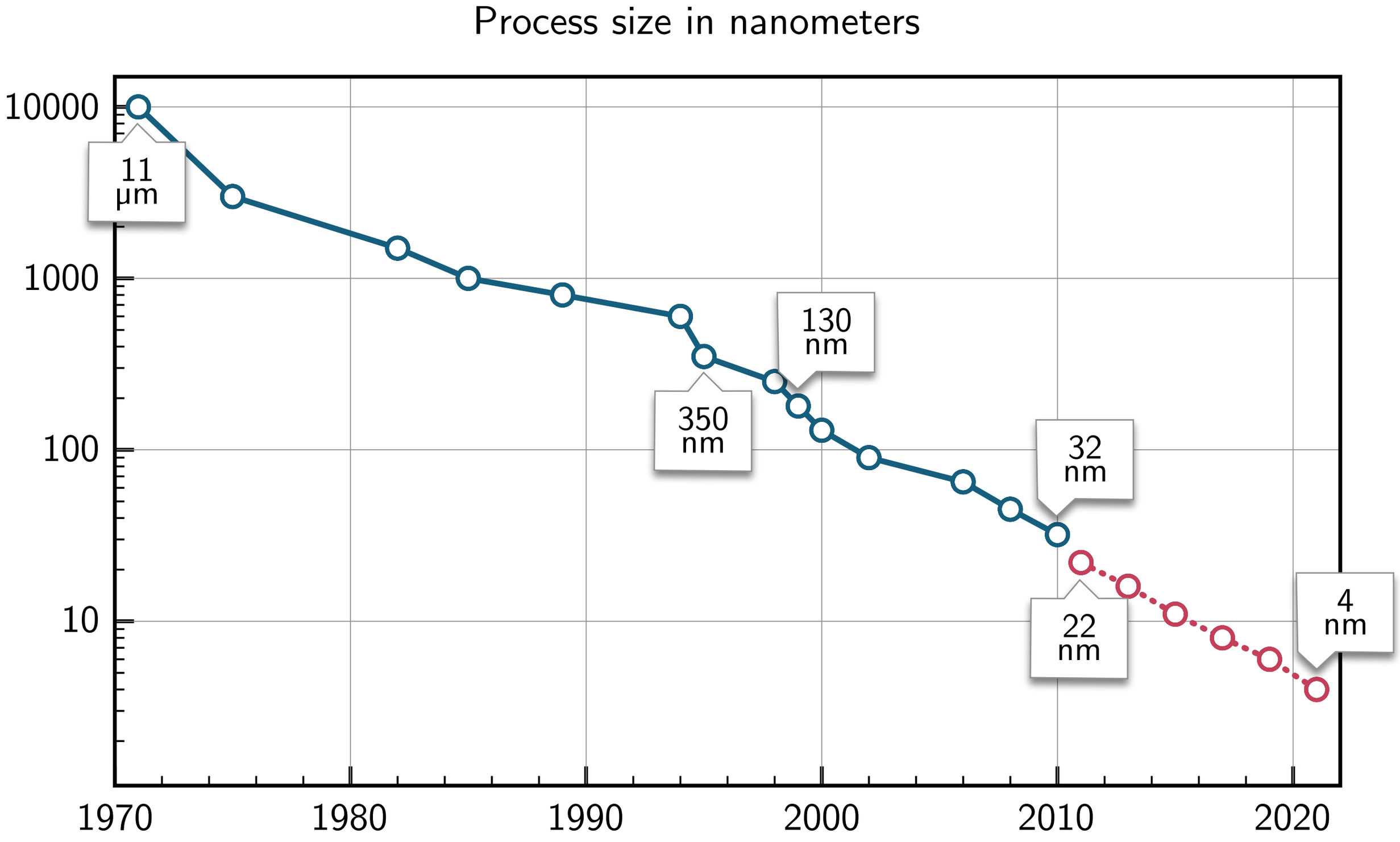
From "Cramming more components onto integrated circuits", Gordon E. Moore. Electronics, Volume 38, Number 8, April 19, 1965

Introduction – Moore's law

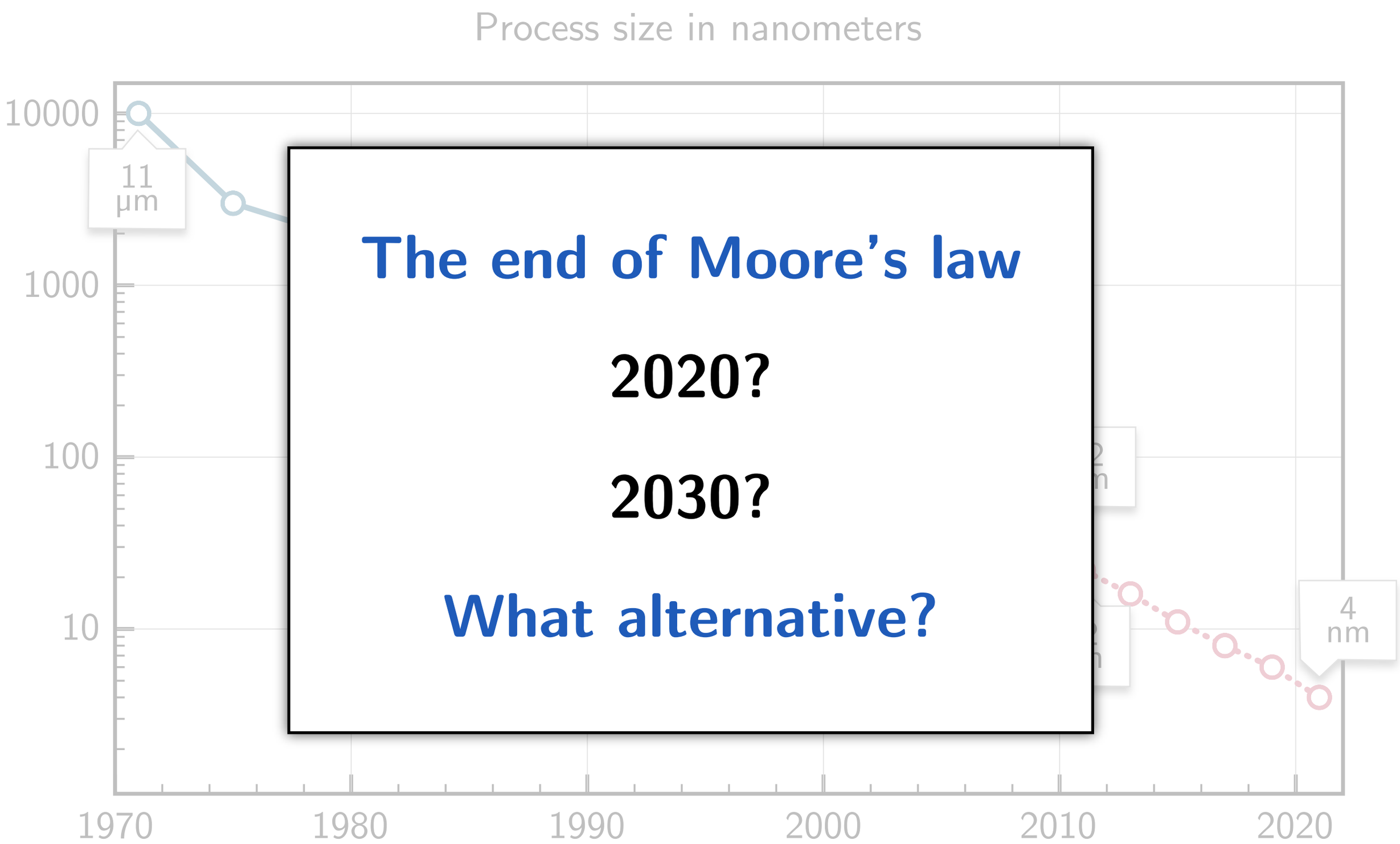


From "Cramming more components onto integrated circuits", Gordon E. Moore. Electronics, Volume 38, Number 8, April 19, 1965

Introduction – Moore's law



Introduction – Moore's law

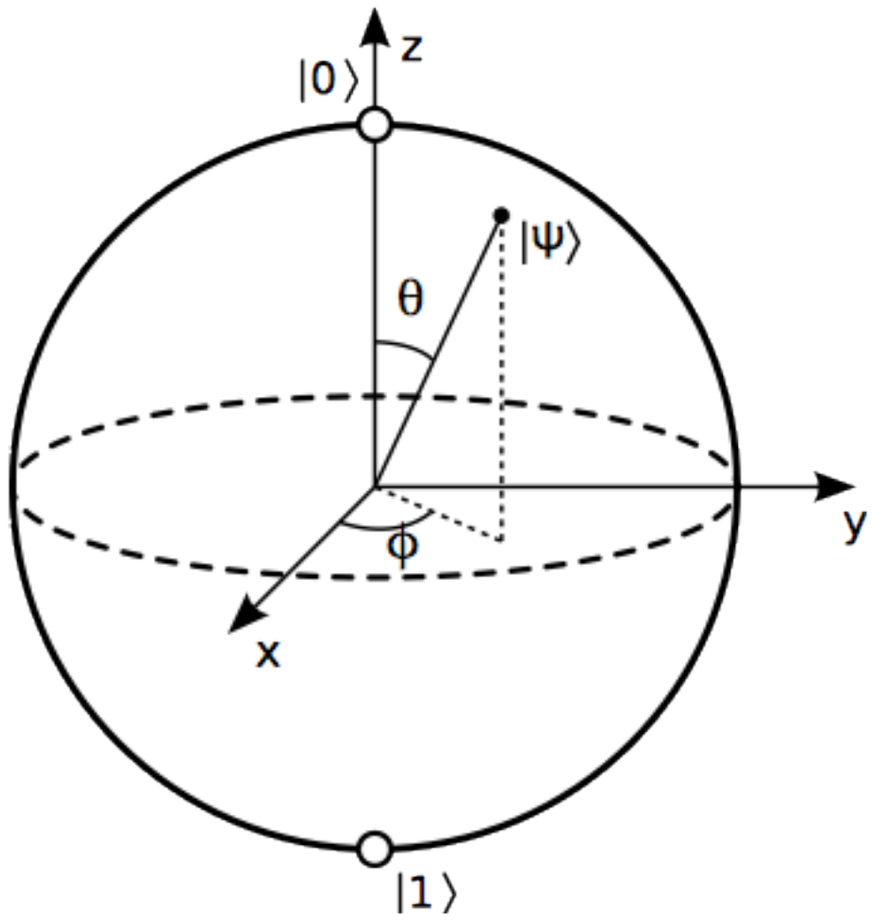


The quantum bit

- Classical bit is either
  - 0 or 1
- Quantum bit (qubit) can be
  - the eigenstates $|0\rangle$ or $|1\rangle$
  - or a superposition $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
    - $\alpha, \beta \in \mathbb{C}$ are probability amplitudes
    - $|\alpha|^2 + |\beta|^2 = 1$

The quantum bit

- Geometrical interpretation – the Bloch sphere



$$|\psi\rangle = cos(\theta/2)|0\rangle + e^{i\phi} sin(\theta/2)|1\rangle$$

Quantum bit register

- n classical bits $\longrightarrow$ vector in a $2n$ dimensional space $\mathbb{Z}_2^n$

$$(\text{reg3}) = a_0\ (001) + a_1\ (010) + a_2\ (100) \quad \text{with } a_i = 0 \text{ or } 1$$

- n qubits $\longrightarrow$ vector in a 2^n dimensional space $\mathcal{H}_2^{\otimes n} = \mathcal{H}_2 \otimes ... \otimes \mathcal{H}_2$

$$\begin{aligned} |\psi_{\text{reg3}}\rangle \quad = \quad & a_0\ |000\rangle + a_1\ |001\rangle + a_2\ |010\rangle + \\ & a_3\ |011\rangle + a_4\ |100\rangle + a_5\ |101\rangle + \\ & a_6\ |110\rangle + a_7\ |111\rangle \qquad\qquad \text{with} \quad \sum_i |a_i|^2 = 1 \end{aligned}$$

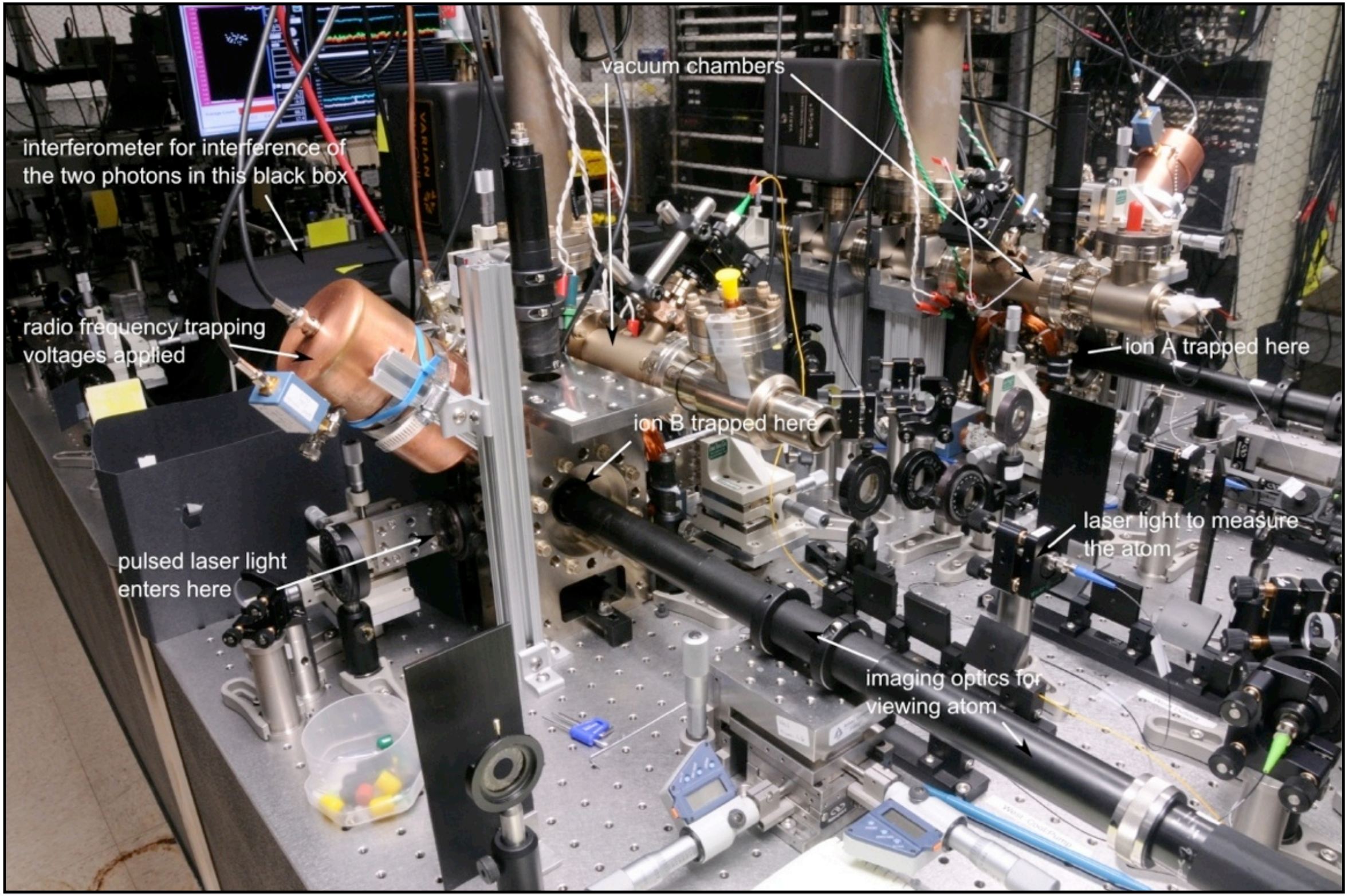
- Number of dimensions grows exponentially
  - Extra states — the entangled states

Quantum bit implementations

- Non exhaustive list

Physical system	Qubit state
Photon	Polarization
Electron or nucleus	Spin
Trapped ion	Electronic state
Molecule under NMR	Collective spin
Quantum dot	Charge or spin
Flux qubit	Charge

A quantum "computer"



http://cdn.physorg.com/newman/gfx/news/hires/teleportationapparatus1.jpg

The quantum collapse

- Measuring a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ yields
  - $|0\rangle$ with probability $|\alpha|^2$
  - $|1\rangle$ with probability $|\beta|^2$

- Measurement destroys initial state
  - Collapse into one of the eigenstate

- No cloning theorem
  - Arbitrary unknown state can not be duplicated

Quantum computations

- Temporal evolution – the Schrödinger equation

$$i\hbar \, \frac{\mathrm{d}}{\mathrm{dt}} |\psi(t)\rangle = H(t) \, |\psi(t)\rangle$$

- This implies $|\psi(t)\rangle = U(t, t_0) \, |\psi(t_0)\rangle$ with U a unitary operator

- A quantum program ≡ unitary matrix M_{prog}

$$|\psi_{out}\rangle = \mathrm{M}_{prog} \, |\psi_{in}\rangle$$

An example: the Walsh-Hadamar transform

- Hadamar gate defined by

$$\mathsf{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\mathsf{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\mathsf{M}_\mathsf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

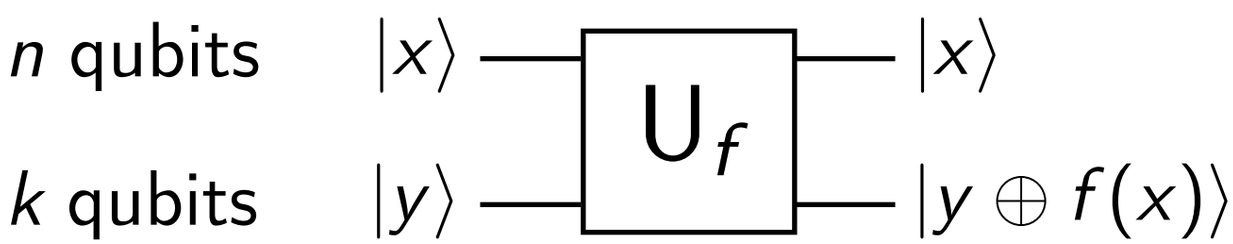
- Walsh-Hadamar transform on a n qubit register

$$\begin{aligned} \mathsf{H}_n(|00\ \ldots\ 0\rangle) &= (\mathsf{M}_\mathsf{H} \otimes \ldots \otimes \mathsf{M}_\mathsf{H})(|00\ldots0\rangle) \\ &= \frac{1}{\sqrt{2^n}}\ (\ (|0\rangle + |1\rangle) \otimes \ldots \otimes\ \ (|0\rangle + |1\rangle)\ ) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \end{aligned}$$

- n Hadamar gates $\rightarrow$ superposition of all possible 2^n states

The quantum parallelism

- Given a gate $\mathsf{U}_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$



- Combined with Walsh-Hadamar

$$\begin{aligned} \mathsf{U}_f \mathsf{H}_n |\vec{0}_n, \vec{0}_k\rangle &= \mathsf{U}_f \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, \vec{0}_k\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle \end{aligned}$$

- n Hadamar gates + one $\mathsf{U}_f \rightarrow$ superposition of all possible $f(x)$

Quantum algorithms

- Quantum parallelism can lead to exponential speed-up
- Problem – quantum collapse
  - How to measure the result?
    - Use tricks to get result with high probability
- Roughly speaking, two main algorithms (+ derivatives)
  - 1996 – Grover's algorithm (search within N elements in $O(\sqrt{N})$)
  - 1994 – Shor's algorithm (integer factorization & discrete log)
    - Integer factorization in polynomial time

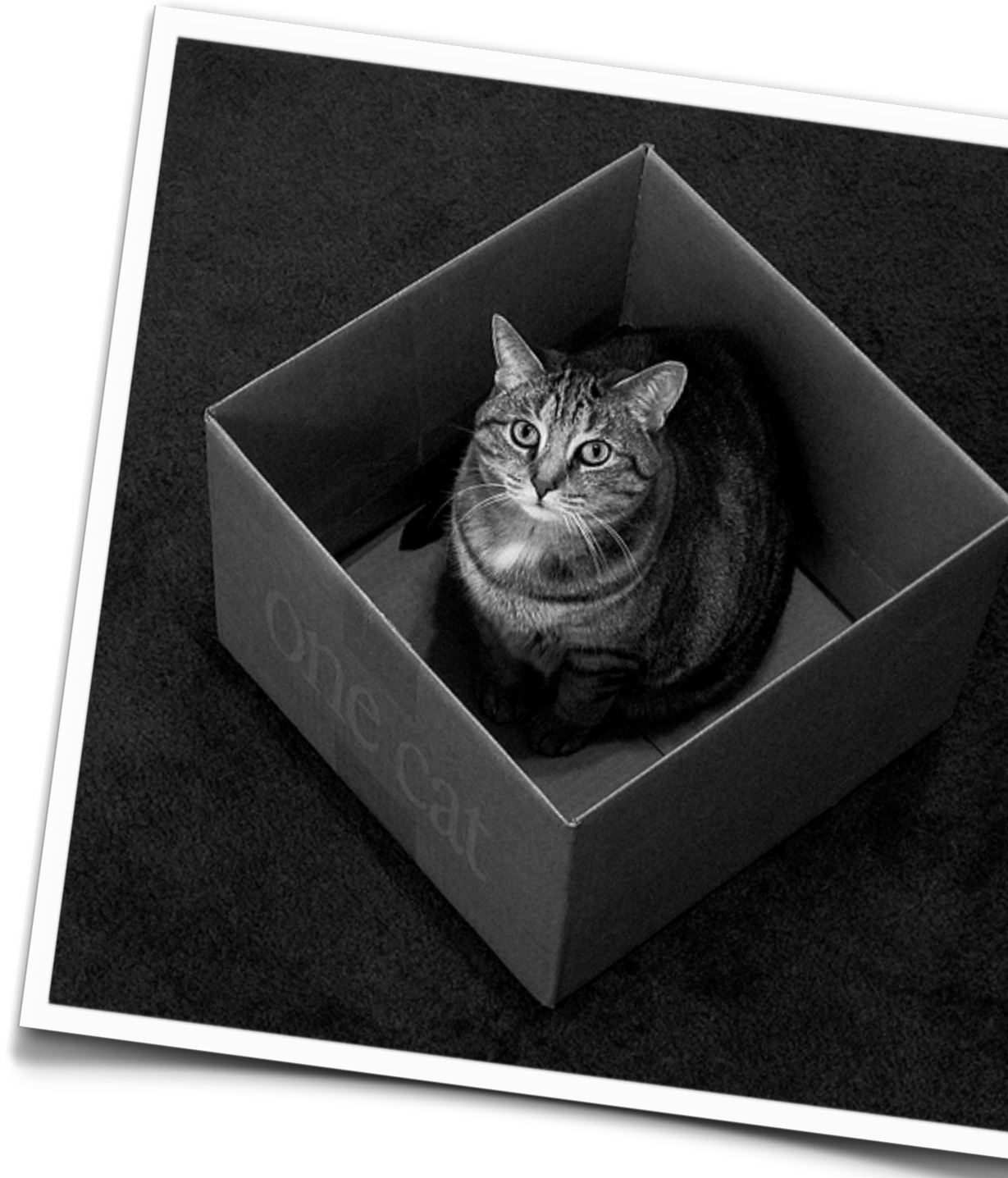
Outline

Quantum computation

Shor's algorithm

Grover's algorithm

Quantum communication



Shor's factoring algorithm – overview

- Runs in polynomial time – $O((\log N)^3(\log\log N)(\log\log\log N))$
- Basic idea – reduce factoring to period-finding problem

Shor's factoring algorithm

Input: integer N to factor of size $n = \lceil \log_2 N \rceil$
Output: a factor p of N

1. Choose base:

Pick $x \in \mathbb{Z}$ coprime to N

2. Find period: this is the quantum part

Find the period r of f given by $f(y) = x^y \bmod N$

3. Deduce factor:

If r is even then since $x^r = 1 \bmod N$

$$p = \gcd(x^{r/2} - 1, N) \text{ or } p = \gcd(x^{r/2} + 1, N)$$

Shor's algorithm – the quantum part

- Let $Q = 2^q$ such that $N^2 \leq Q \leq 2N^2$
- Start with $|\psi\rangle = |\mathrm{reg}_q, \mathrm{reg}_n\rangle = |\vec{0}_q, \vec{0}_n\rangle$

$$|\psi\rangle \quad = \quad \mathrm{M}_f \ \mathrm{H}_q \ |\vec{0}_q, \vec{0}_n\rangle \ = \ \mathrm{M}_f \ \frac{1}{\sqrt{Q}} \ \sum_{a=0}^{Q-1} \ |a, \vec{0}_n\rangle$$

$$= \quad \frac{1}{\sqrt{Q}} \ \sum_{a=0}^{Q-1} \ |a, f(a)\rangle$$

  - All $f(a)$ computed with one application of M_f

- Measure $|\mathrm{reg}_n\rangle$ only $\rightarrow$ gives a result v

$$|\psi\rangle = \frac{1}{\sqrt{\#A}} \sum_{a \in A} |a, v\rangle \quad \text{where } A = \{y | f(y) = v\}$$

Shor's algorithm – the quantum part

- $|\psi\rangle = \frac{1}{\sqrt{\#A}} \sum_{a \in A} |a, v\rangle$ with $|a\rangle = |a_0 + kr\rangle$
- Quantum Fourier Transform on d qubit register

$$\text{QFT} \;:\; |x\rangle \;\mapsto\; \frac{1}{\sqrt{2^d}} \sum_{y=0}^{2^d-1} \omega^{xy} \; |y\rangle \qquad \text{with} \;\; \omega = \exp(2\pi i/2^d)$$

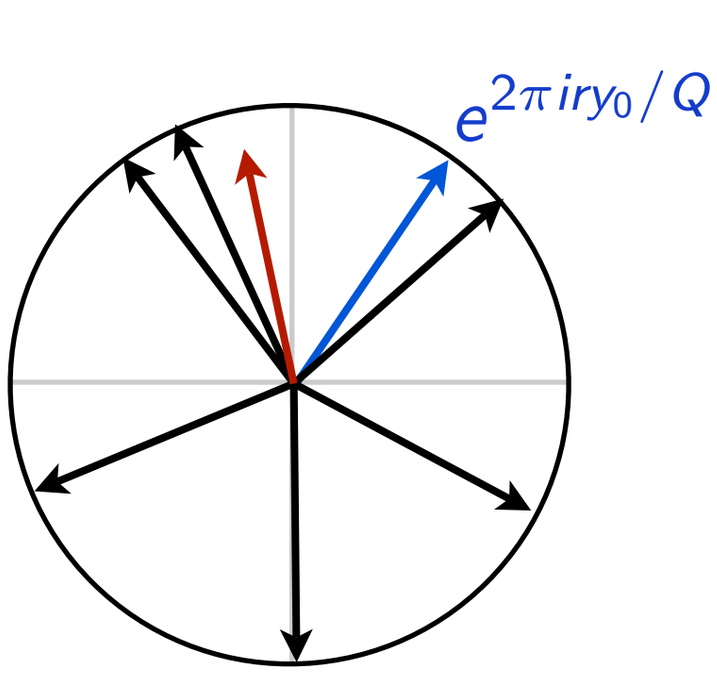
- QFT $|\psi\rangle$ $= \frac{1}{\sqrt{\#A}} \sum_{a \in A} \frac{1}{\sqrt{Q}} \sum_{y=0}^{Q-1} \omega^{ay} |y, v\rangle$

$$= \frac{1}{\sqrt{Q\#A}} \sum_{y=0}^{Q-1} \exp(2\pi i a_0 y/Q) \sum_{k=0}^{\#A-1} \exp(2\pi i k r y/Q) |y, v\rangle$$

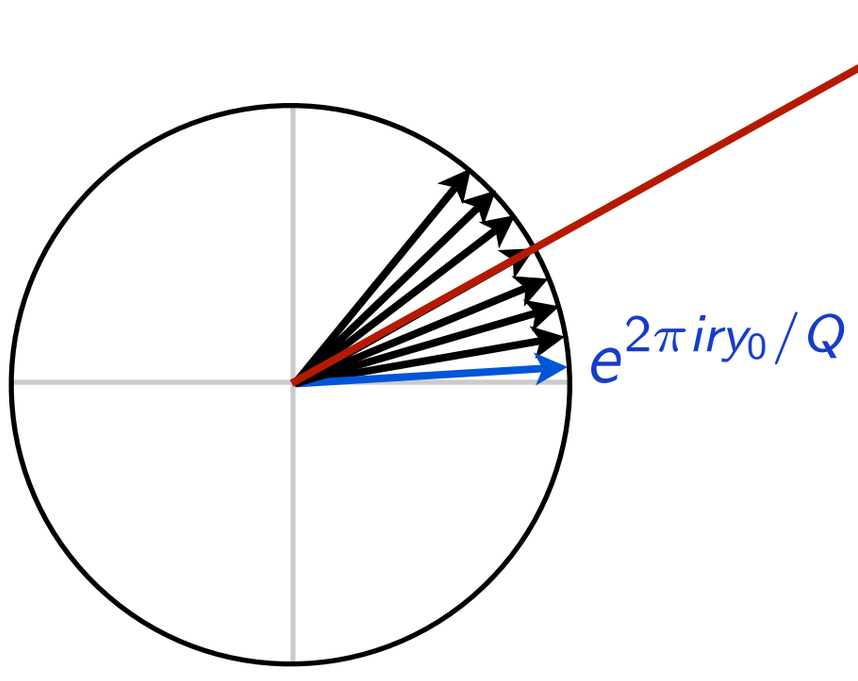
- $Prob(y = y_0) = \frac{\#A}{Q} \left| \frac{1}{\#A} \sum_{k=0}^{\#A-1} \exp(2\pi i k r y_0/Q) \right|^2$

Shor's algorithm – the quantum part

- $Prob(y = y_0) = \frac{\#A}{Q} \left| \frac{1}{\#A} \sum_{k=0}^{\#A-1} \exp(2\pi i k r y_0 / Q) \right|^2$
  - Quantum interferences
    - $Prob(y = y_0)$ is higher as ry_0/Q is closer to an integer



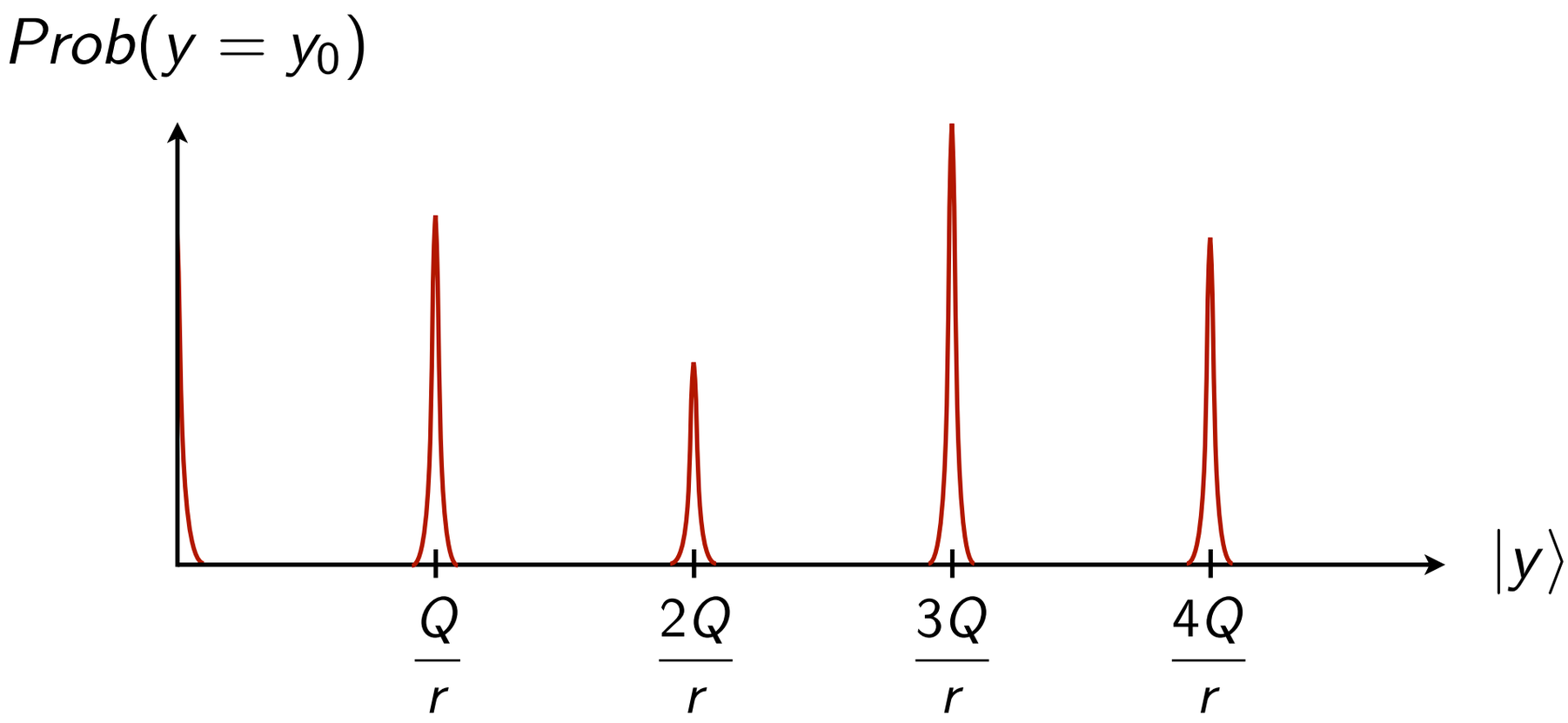
Destructive interferences



Constructive interferences for

$$\left| \frac{y_0}{Q} - \frac{k}{r} \right| \leq \frac{1}{2Q}$$

Shor's algorithm – the quantum part



- Mesure first register $\rightarrow$ $y_0 \approx k\frac{Q}{r}$ with high probability
  - $\frac{y_0}{Q} \approx \frac{k}{r}$
  - Find r knowing y_0 and Q ?

Shor's algorithm – deducing the order

- Remember $\left|\frac{y_0}{Q} - \frac{k}{r}\right| \leq \frac{1}{2Q}$ and $r < N$
- Use continued fractions to find k^* and r^* from y_0, Q
  - There is only one such fraction iff $Q \geq N^2$
  - r^* is the period iff $\gcd(k^*, r^*) = 1$
  - r^* is a factor of the period otherwise
  - Repeat quantum part if needed
    - At most $O(\log \log r)$ times

Shor's algorithm – it works!

- Nature 414 (6866): 883–887 (2001)

Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance

Lieven M. K. Vandersypen*†, Matthias Steffen*†, Gregory Breyta*, Costantino S. Yannoni*, Mark H. Sherwood* & Isaac L. Chuang*†

** IBM Almaden Research Center, San Jose, California 95120, USA*
† Solid State and Photonics Laboratory, Stanford University, Stanford, California 94305-4075, USA

The number of steps any classical computer requires in order to find the prime factors of an *l*-digit integer *N* increases exponentially with *l*, at least using algorithms known at present[1]. Factoring large integers is therefore conjectured to be intractable classically, an observation underlying the security of widely used cryptographic codes[1,2]. Quantum computers[3], however, could factor integers in only polynomial time, using Shor's quantum factoring algorithm[4–6]. Although important for the study of quantum computers[7], experimental demonstration of this algorithm has proved elusive[8–10]. Here we report an implementation of the simplest instance of Shor's algorithm: factorization of $N = 15$

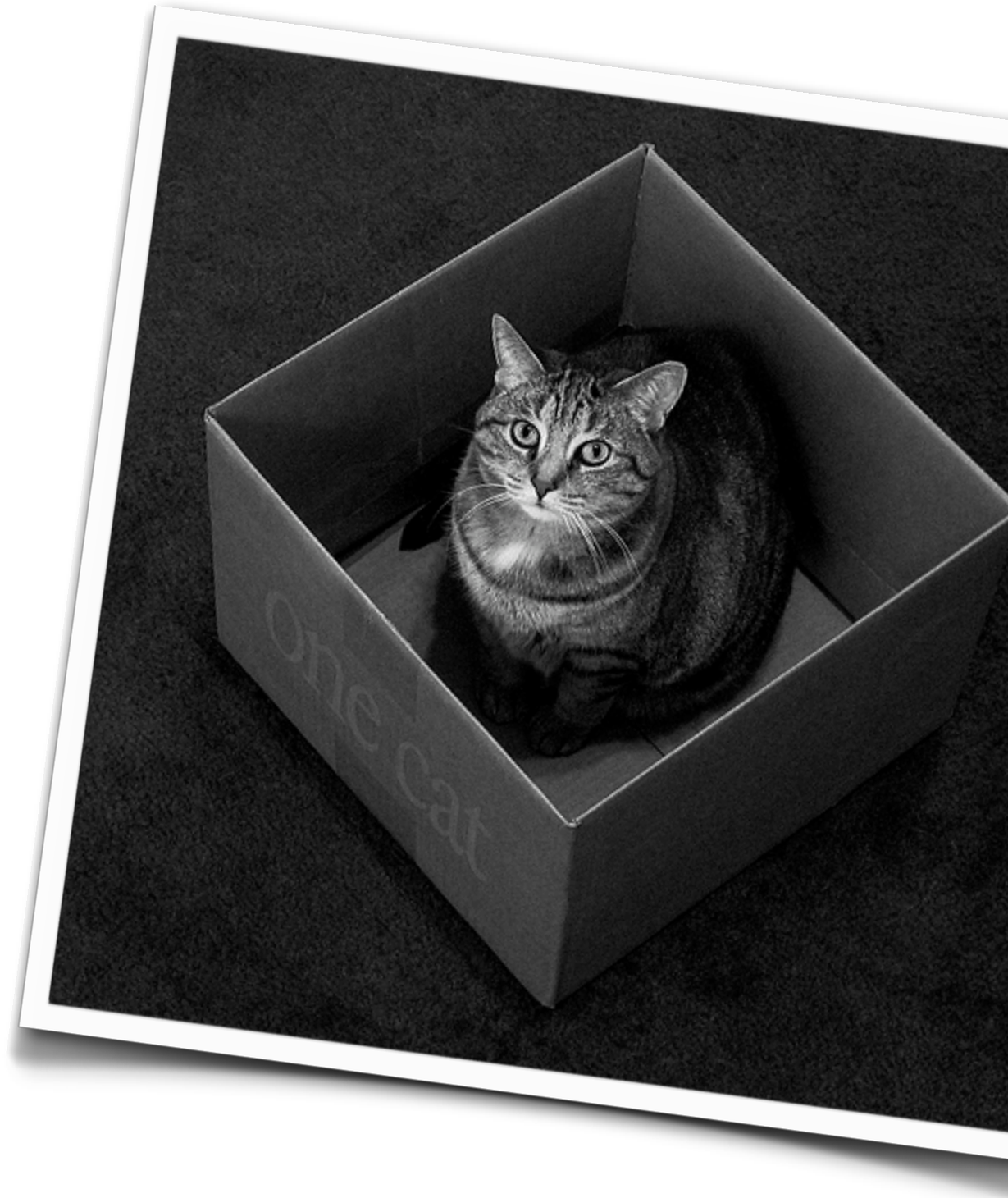
Outline

Quantum computation

Shor's algorithm

Grover's algorithm

Quantum communication



Grover's algorithm

- Unstructured search
  - Find one element within N elements in $O(\sqrt{N})$
    - Classically in $O(N)$
  - Quadratic speed-up

- Akin to inverting a function f
  - $N = 2^n$ entries $[0 \ldots N-1]$
  - Find the unique x_0 such that $f(x_0) = 1$

Grover's algorithm

- Start with a superposition of $N = 2^n$ states (n qubit register)

$$\begin{aligned} |\psi_0\rangle &= \mathsf{H}_n|\vec{0}_n\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \end{aligned}$$

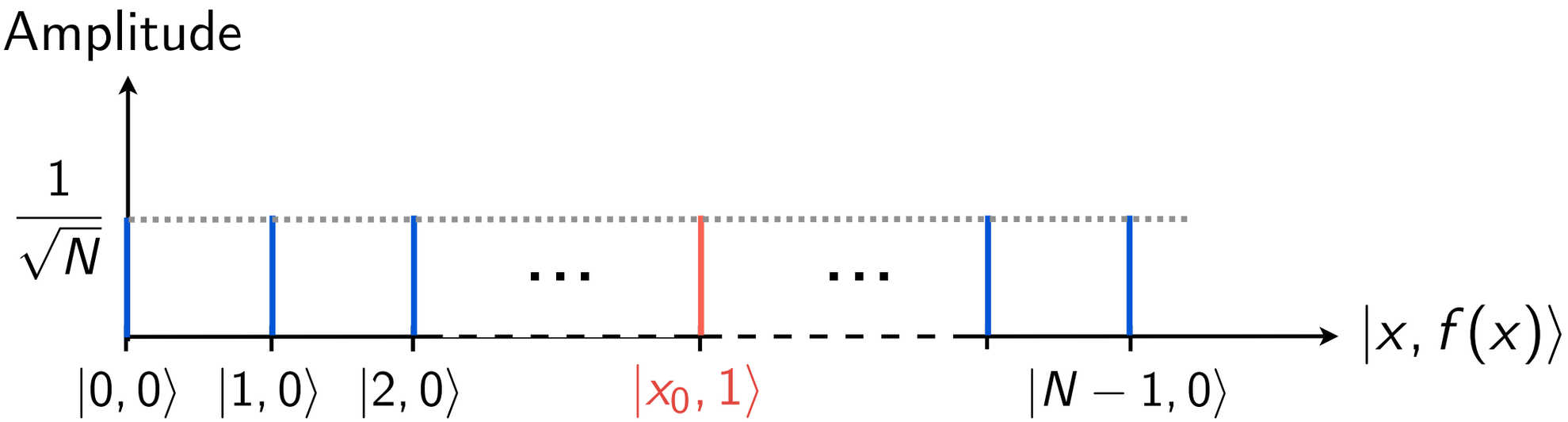
- Apply f transform

$$|\psi\rangle = \mathsf{U}_f|\psi_0, 0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, f(x)\rangle$$

- We would like to measure $|x_0, 1\rangle$ with high probability

Grover's algorithm

- As is, only 1 over N chance to measure $|x_0, 1\rangle$

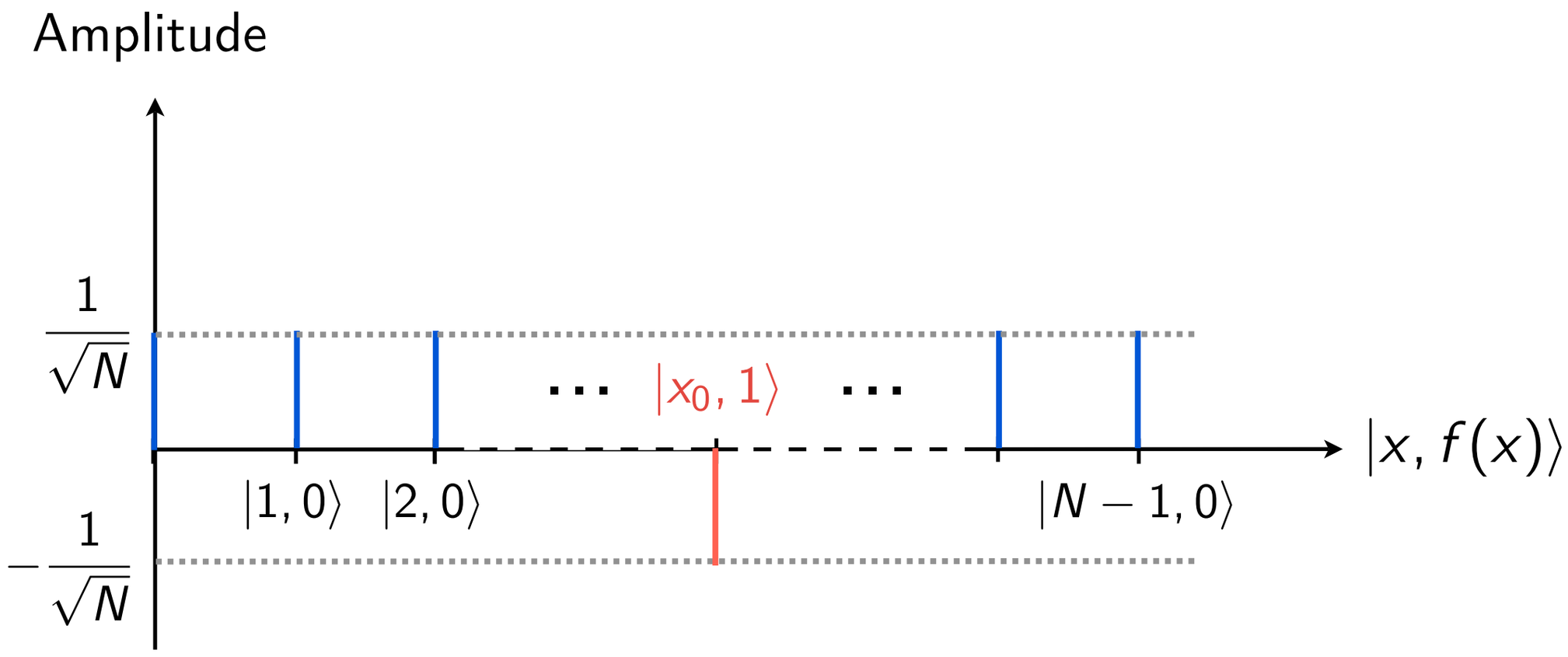


- Amplify that probability with two transforms
  - Phase inversion
  - Inversion about average

  } Grover iteration

Grover iteration — Phase inversion

- Inverse phase of amplitude for $|x_0, 1\rangle$



- Is this possible with a unitary transform?
  - Yes!

Grover iteration — Phase inversion

- We showed that $\mathsf{U}_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$ is a unitary transform
  - Now take $|y_0\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$ and $f(x) = 0$ or 1

$$\mathsf{U}_f|x, y_0\rangle = |x\rangle \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}$$

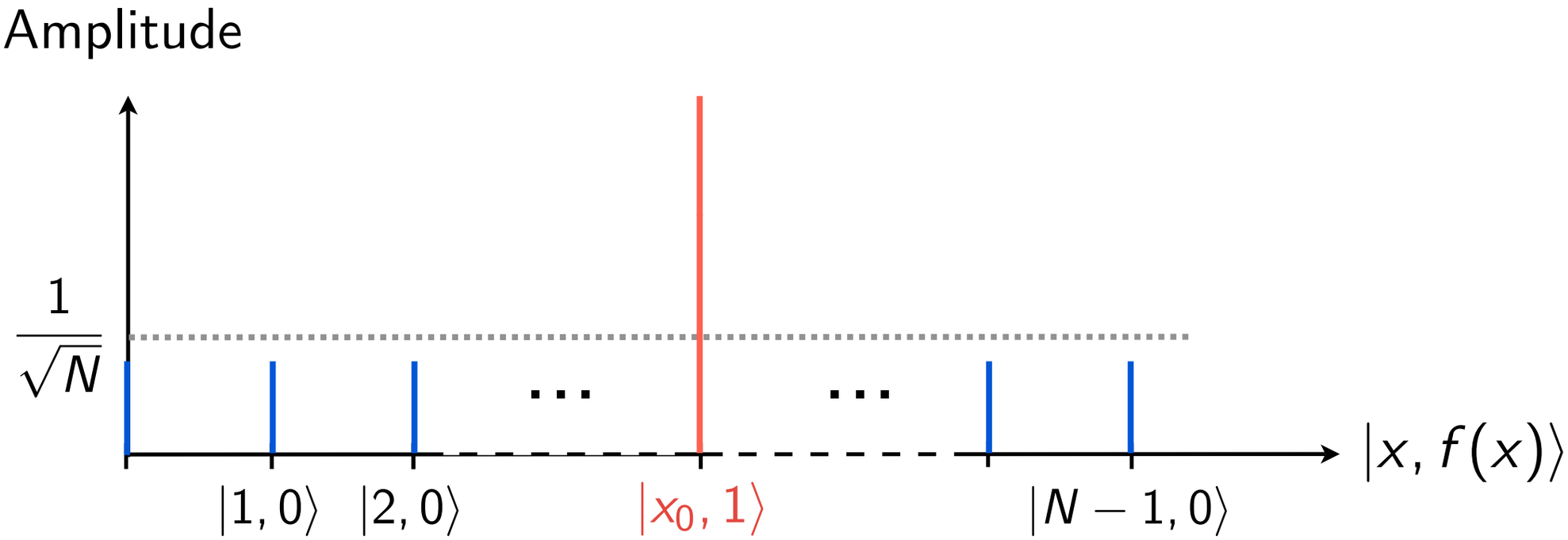
$$(-1)^{f(x)}|x, y_0\rangle$$

- We obtain the phase-inversion transform

$$\mathsf{U}_i|x\rangle = \mathsf{U}_f|x, y_0\rangle$$

Grover iteration — Inversion / average

- Inverse about average of amplitude for $|x_0, 1\rangle$



- Is this possible with a unitary transform?
  - Yes!

Grover iteration — Inversion / average

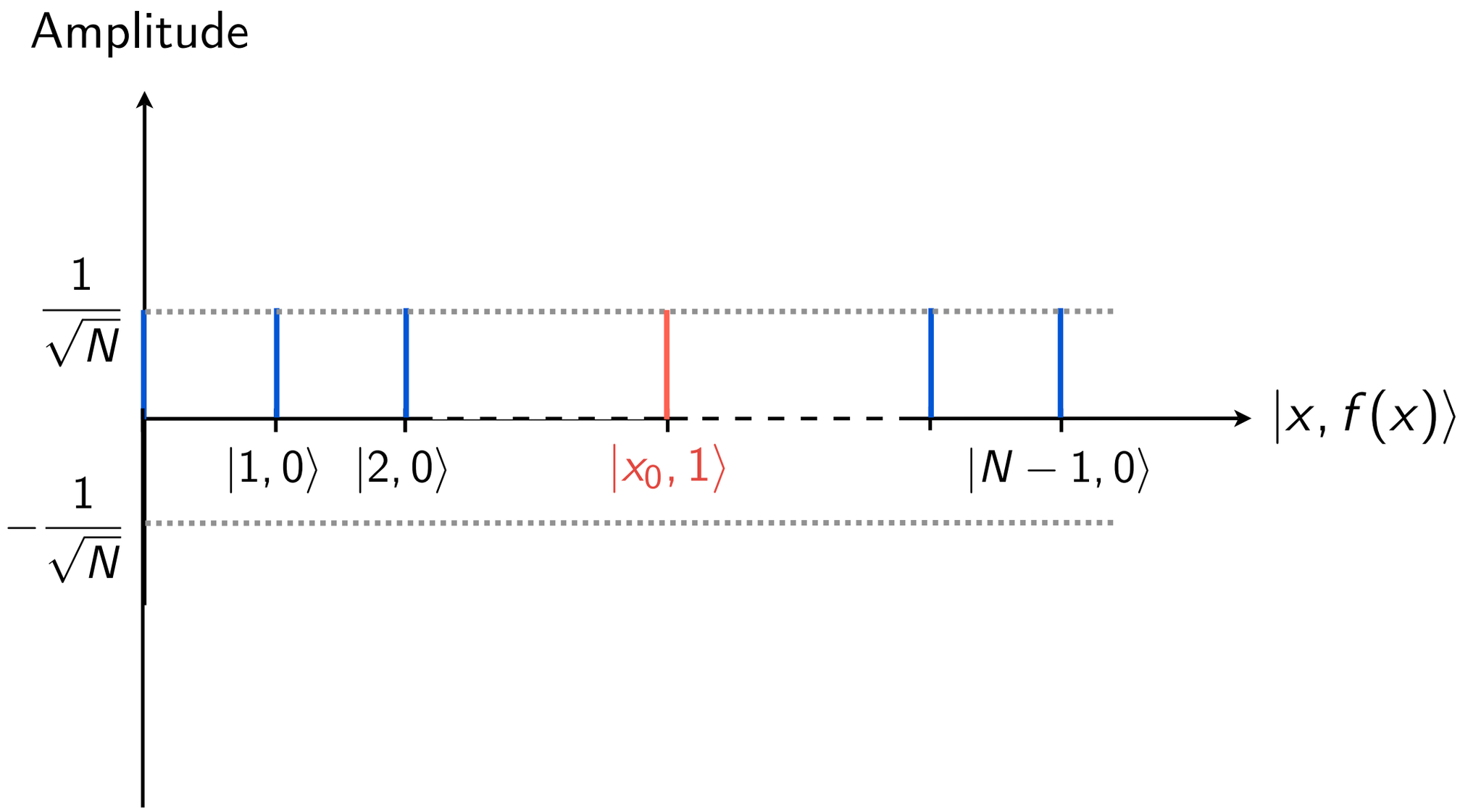
- Inversion about average operator U_a given by matrix M_a

$$\mathsf{M}_a = -I + 2P \qquad \text{with } P = \frac{1}{N}\begin{pmatrix} 1 & \dots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \dots & 1 \end{pmatrix}$$

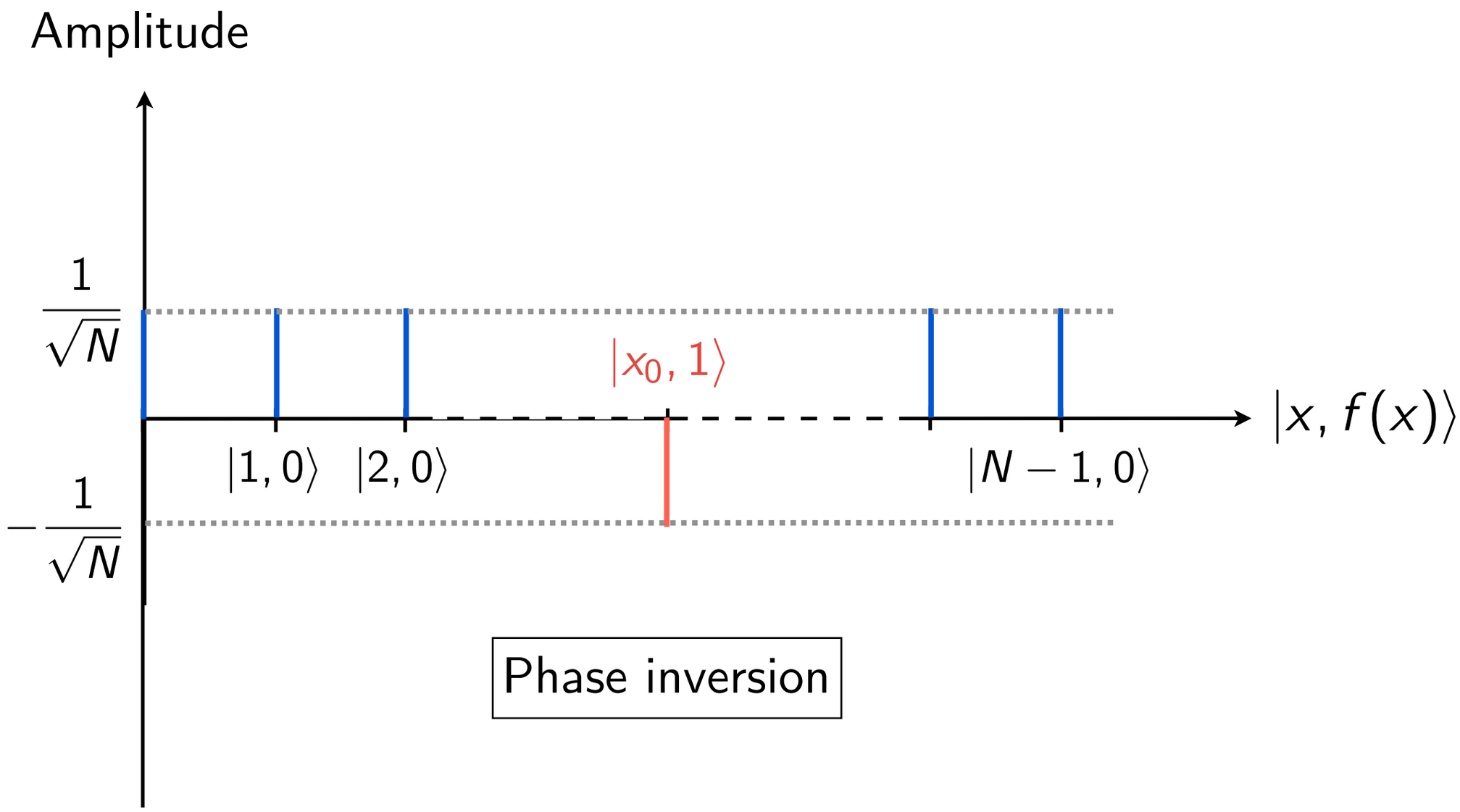
- Indeed $\begin{aligned} \mathsf{M}_a\vec{v} &= -\vec{v} + 2\vec{A} \\ &= \vec{A} + (\vec{A} - \vec{v}) \end{aligned}$

- M_a is unitary
  - Since $P^2 = P$ then $\mathsf{M}_a^2 = I - 4P + 4P^2 = I$

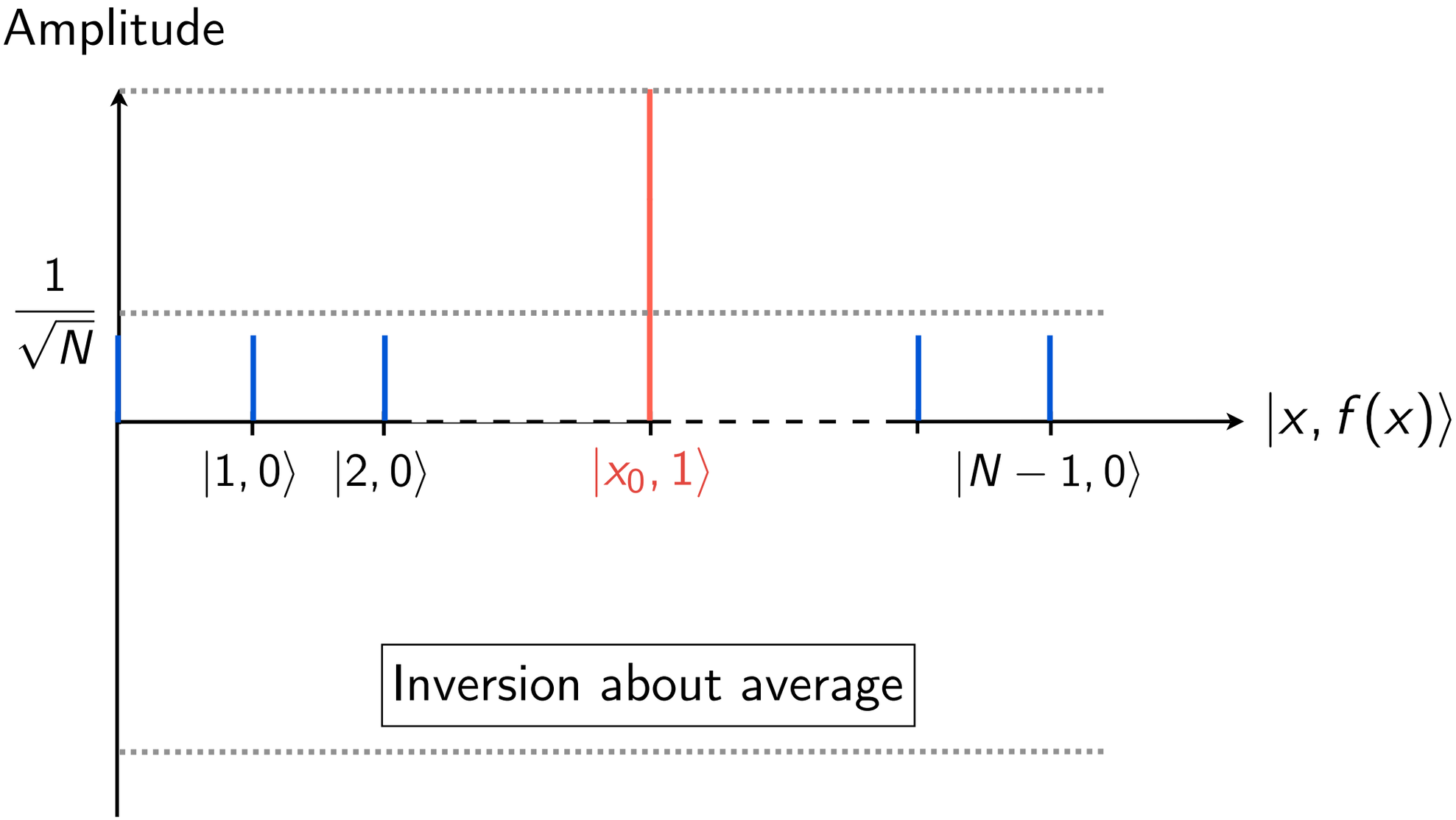
Grover iteration — Effect on amplitudes



Grover iteration — Effect on amplitudes



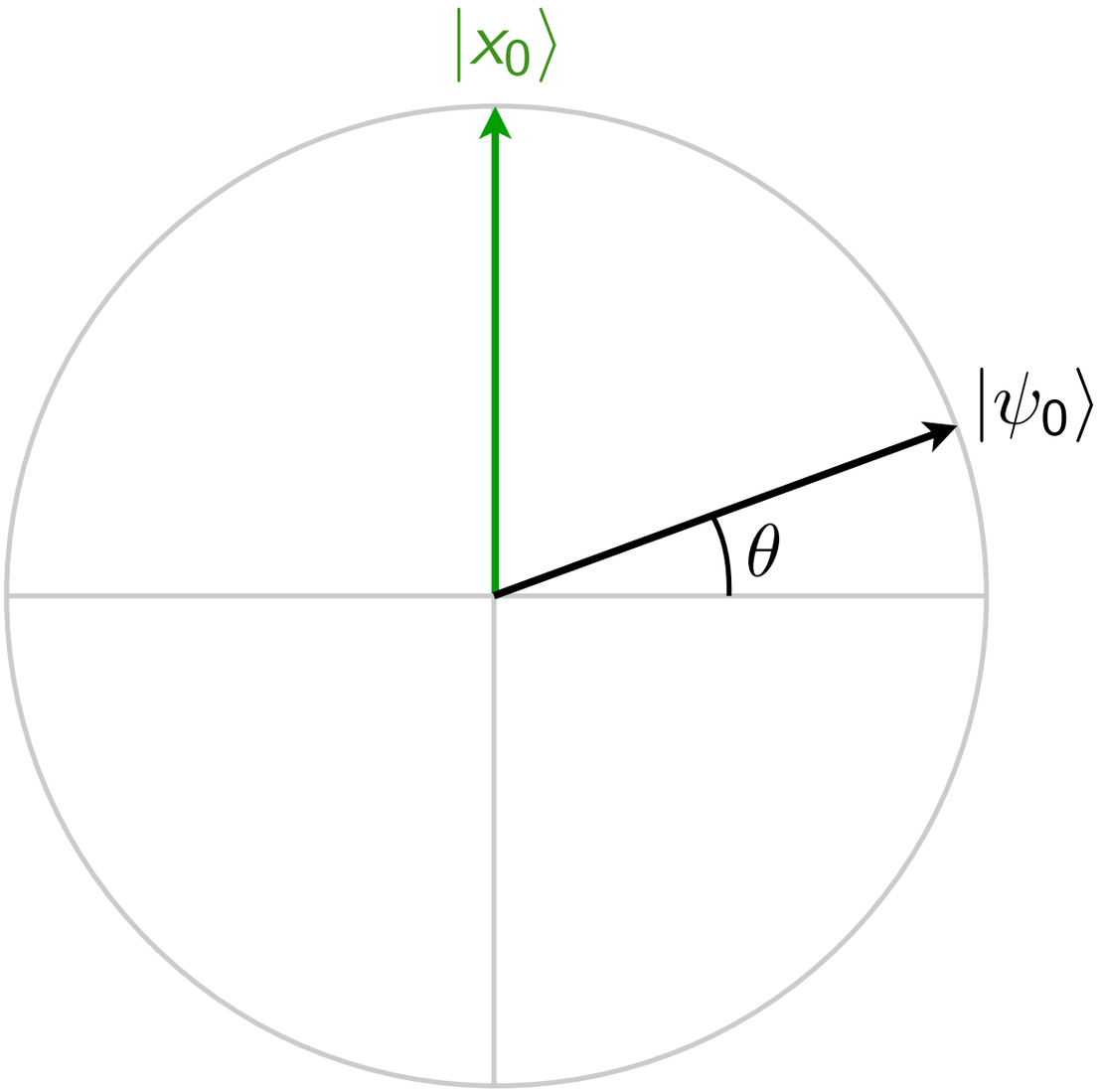
Grover iteration — Effect on amplitudes



Grover's algorithm — geometrical interpretation

- Initial state $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq x_0} |x\rangle + \frac{1}{\sqrt{N}} |x_0\rangle$

- As a vector in the space spawned by $|x_0\rangle$ and $|\psi_0\rangle$



$$\langle \psi_0 | x_0 \rangle = \frac{1}{\sqrt{N}}$$

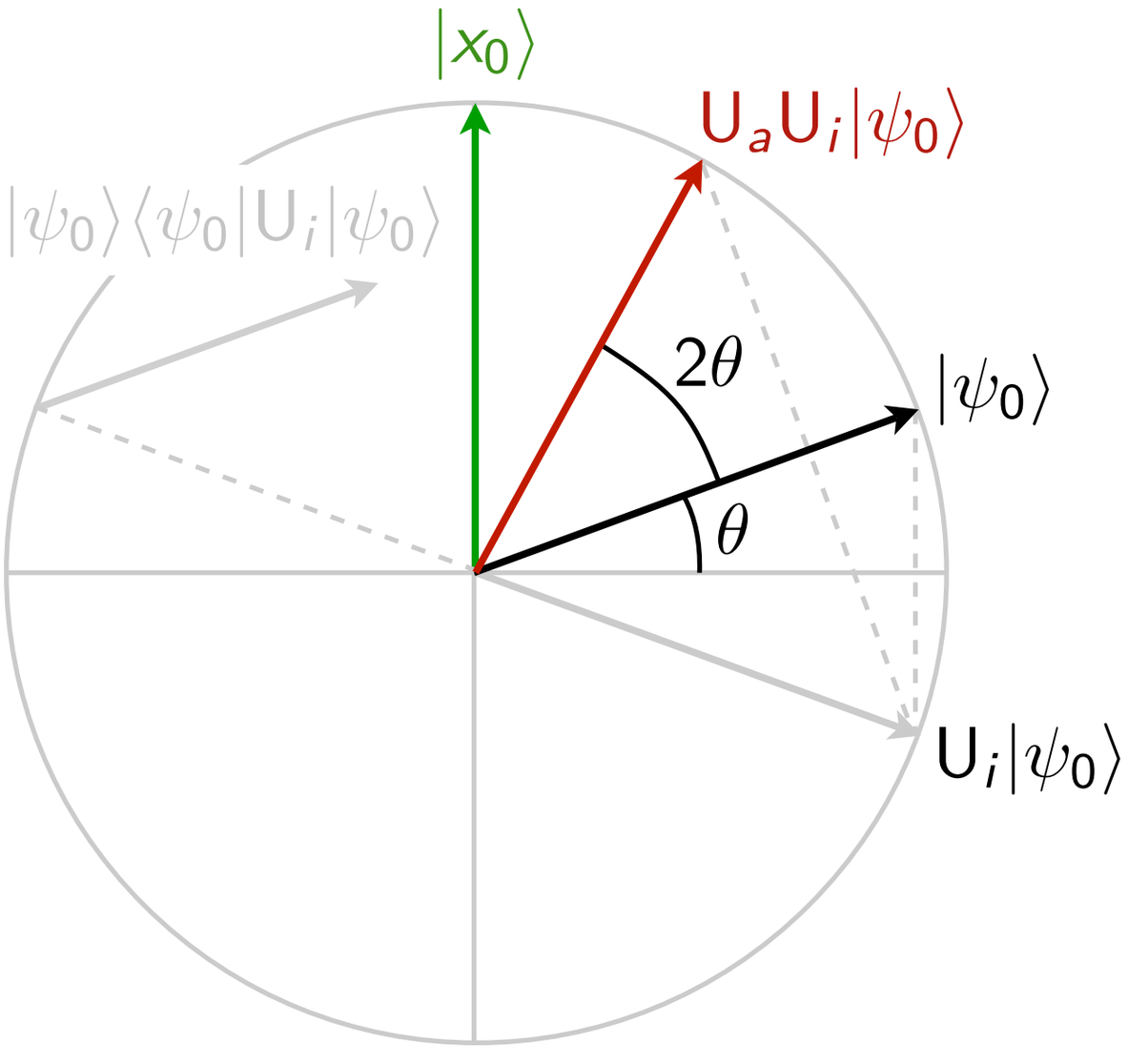
$$sin\ \theta = \frac{1}{\sqrt{N}}$$

$$\theta \to \frac{1}{\sqrt{N}} \quad \text{as} \quad N \to \infty$$

Grover's algorithm — geometrical interpretation

- Initial state $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq x_0} |x\rangle + \frac{1}{\sqrt{N}} |x_0\rangle$

- As a vector in the space spawned by $|x_0\rangle$ and $|\psi_0\rangle$



phase inversion U_i

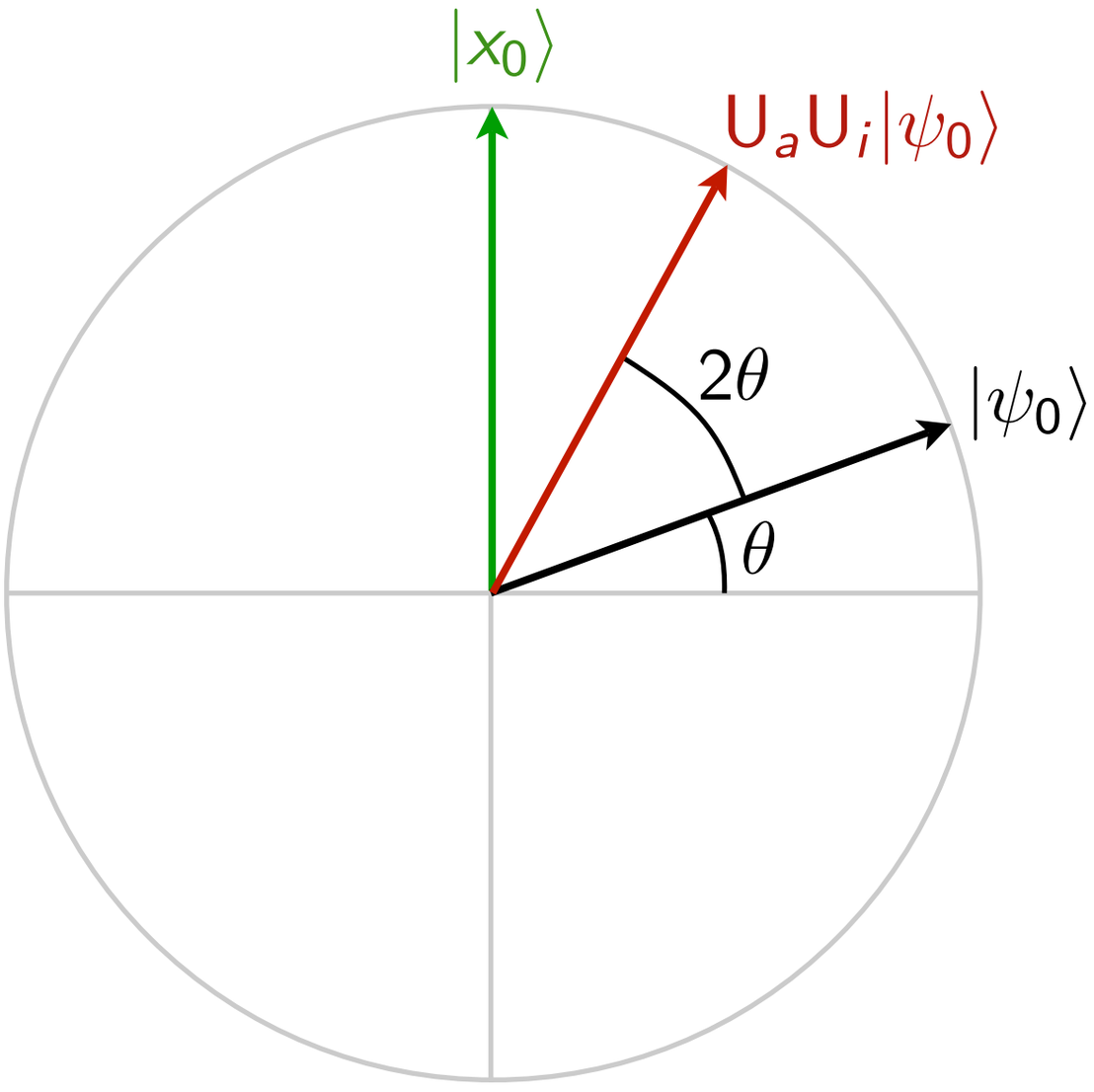
$$U_i|\psi_0\rangle = |\psi_0\rangle - \frac{2}{\sqrt{N}}|x_0\rangle$$

inversion about average U_a

$$U_a U_i|\psi_0\rangle = (2|\psi_0\rangle\langle\psi_0| - I)U_i|\psi_0\rangle$$

Grover's algorithm — geometrical interpretation

- Initial state $|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq x_0} |x\rangle + \frac{1}{\sqrt{N}} |x_0\rangle$
- As a vector in the space spawned by $|x_0\rangle$ and $|\psi_0\rangle$



One Grover iteration $U_a U_i$

Rotates $|\psi_0\rangle$ counterclockwise by 2θ towards $|x_0\rangle$

Number of iterations k

$$2k\theta + \theta = \frac{\pi}{2}$$

$$k = \left\lceil \frac{\pi}{4\theta} - \frac{1}{2} \right\rfloor \rightarrow \left\lceil \frac{\pi}{4} \sqrt{N} \right\rfloor$$

Grover's algorithm

- Repeat phase & average inversion about $\frac{\pi}{4}\sqrt{2^n}$ times
  - Failure rate $\simeq \frac{1}{N}$
- Grover's algorithm shown to be optimal

- Generalization known as amplitude amplification algorithm
  - Case with several solutions
  - Find global minimum of a function
  - Evaluation of special integrals

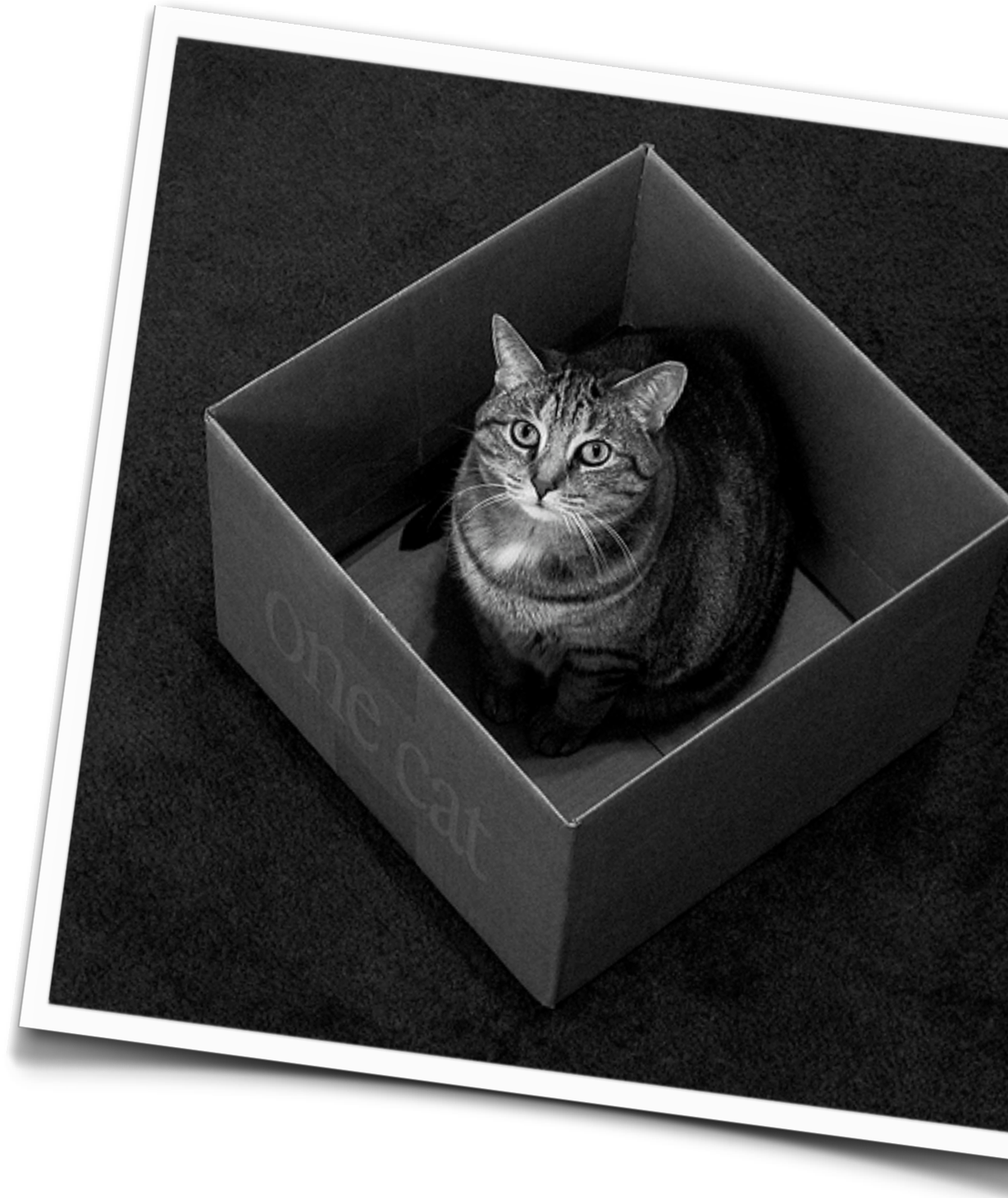
Outline

Quantum computation

Shor's algorithm

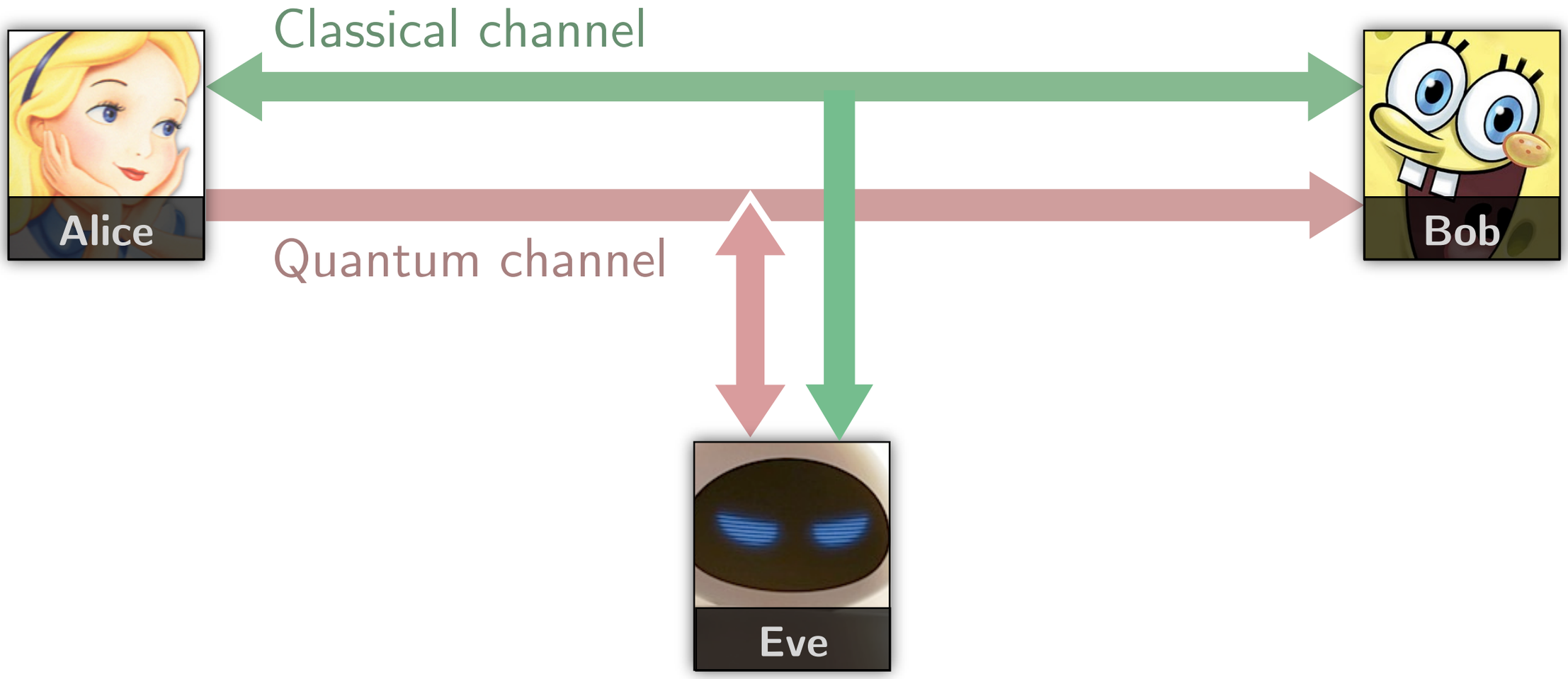
Grover's algorithm

Quantum communication

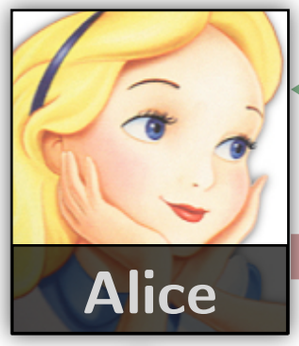


Quantum Key Distribution

- Simplest example: BB84 [Bennet & Brassard, 1984]
  - Relies on no-cloning theorem and quantum collapse



BB84 – Key Distribution



3 Choose random basis and measures qubits

2 Sends random bits in random bases

Basis reconciliation

4

1 Uses two basis at random

$0 : |\downarrow\rangle$

$1 : |\rightarrow\rangle$

or

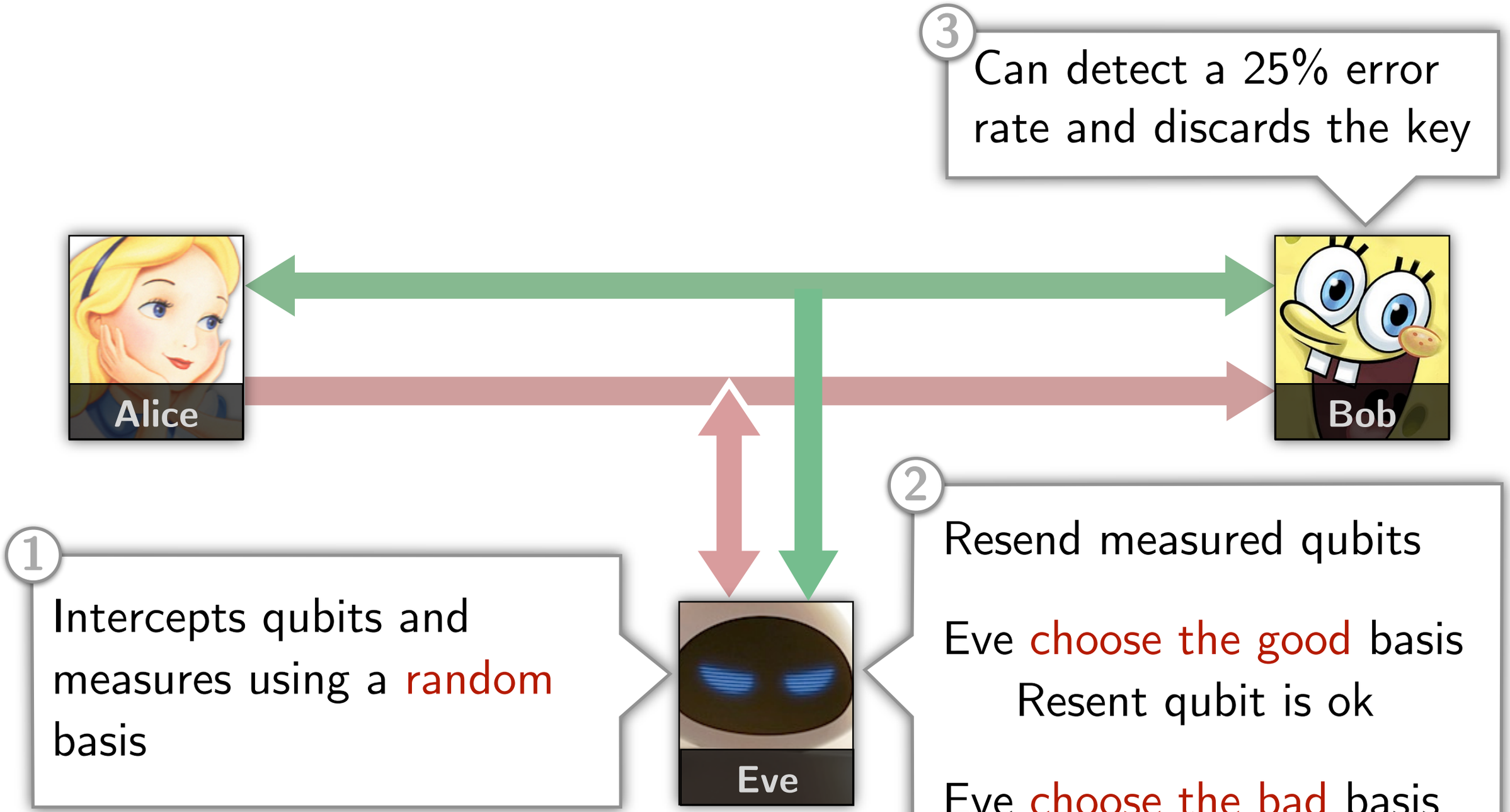
$0 : |\nwarrow\rangle$

$1 : |\nearrow\rangle$

Alice & Bob agreed on 50% of all bits transmitted.

This is their key!

BB84 – Intercept-resend strategy



Intermezzo – Quantum entanglement

- Entanglement — subsystem cannot be taken in isolation
  - Non-classical correlations between constituents of the system
- Formally, subsystem a and b are entangled if $|\psi_{ab}\rangle \neq |\psi_a\rangle \otimes |\psi_b\rangle$
- Simplest example: an EPR pair [Einstein-Podolsky-Rosen]
  - $|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
    - Non-local correlations $\longrightarrow$ subluminal communication
      - Einstein: Spooky action at a distance
- Deep philosophical implication
  - No consensus on the interpretation of Quantum Mechanics

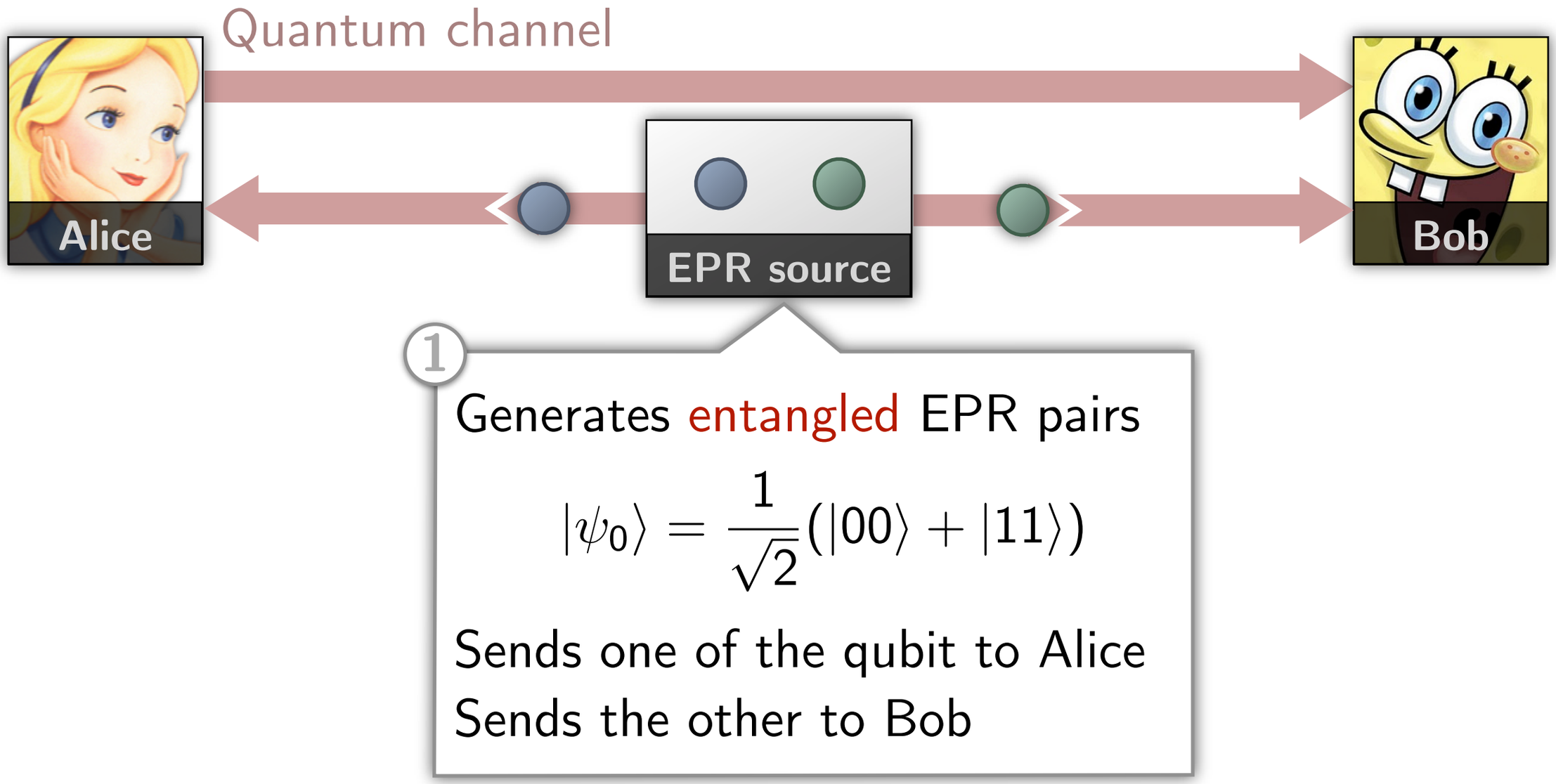
Dense coding

- [Bennett & Wiesner, 1992]
- Uses entanglement to send one qubit & extract two classical bits
- Needs a source of EPR pairs
  - $|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Five unitary transforms

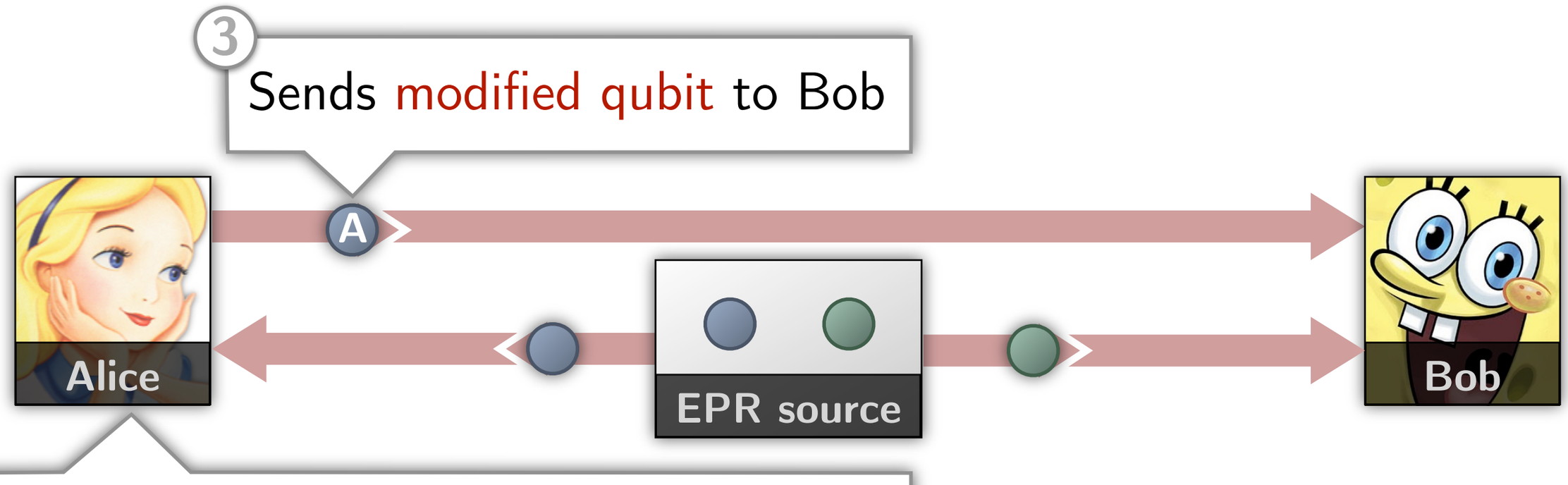
$$
\begin{array}{lcl}
I & : & |0\rangle \rightarrow |0\rangle \\
 & & |1\rangle \rightarrow |1\rangle
\end{array}
\qquad
\begin{array}{lcl}
X & : & |0\rangle \rightarrow |1\rangle \\
 & & |1\rangle \rightarrow |0\rangle
\end{array}
\qquad
\begin{array}{lcl}
C_{not} & : & |00\rangle \rightarrow |00\rangle \\
 & & |01\rangle \rightarrow |01\rangle \\
 & & |10\rangle \rightarrow |11\rangle \\
 & & |11\rangle \rightarrow |10\rangle
\end{array}
$$

$$
\begin{array}{lcl}
Y & : & |0\rangle \rightarrow -|1\rangle \\
 & & |1\rangle \rightarrow |0\rangle
\end{array}
\qquad
\begin{array}{lcl}
Z & : & |0\rangle \rightarrow |0\rangle \\
 & & |1\rangle \rightarrow -|1\rangle
\end{array}
$$

Dense coding



Dense coding



Encodes two classical bits via
local transforms on her qubit

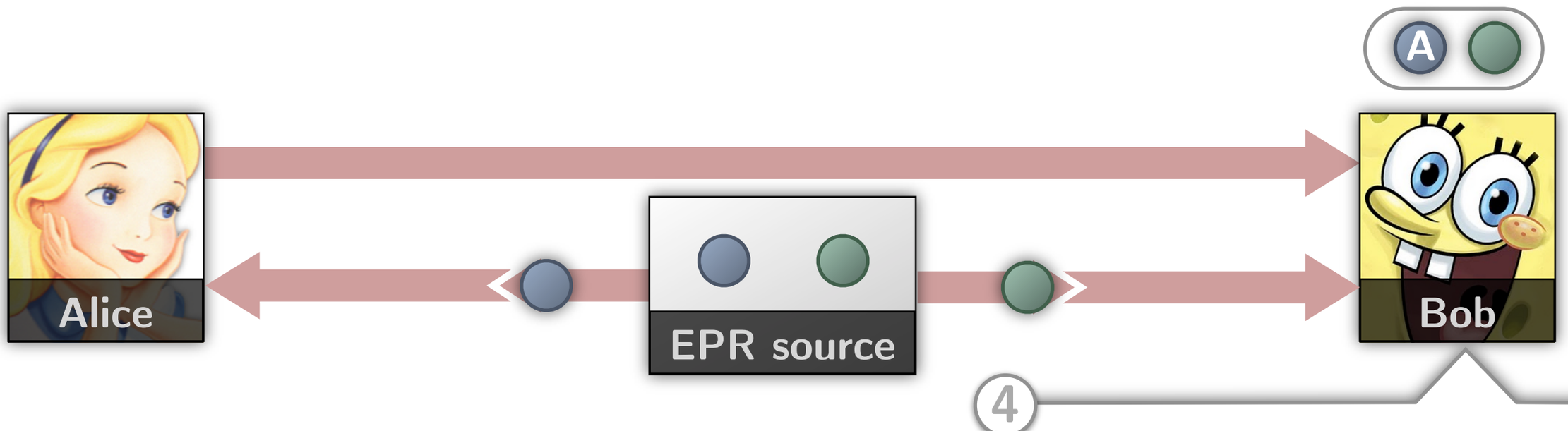
$$0 \to (X \otimes I)|\psi_0\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$

$$1 \to (X \otimes I)|\psi_0\rangle = (|10\rangle + |01\rangle)/\sqrt{2}$$

$$2 \to (Y \otimes I)|\psi_0\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$$

$$3 \to (Z \otimes I)|\psi_0\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$$

Dense coding



4

Applies C_{not}

$$0 \rightarrow (|00\rangle + |10\rangle)/\sqrt{2}$$

$$1 \rightarrow (|11\rangle + |01\rangle)/\sqrt{2}$$

$$2 \rightarrow (|01\rangle - |11\rangle)/\sqrt{2}$$

$$3 \rightarrow (|00\rangle - |10\rangle)/\sqrt{2}$$

5

Measures second qubit

$$|0\rangle_B \rightarrow 0 \text{ or } 3$$

$$|1\rangle_B \rightarrow 1 \text{ or } 2$$

This does not disturb the state!

Dense coding

6

Hadamar on first qubit

$|0\rangle_A \longrightarrow 0$ or 1

$|1\rangle_A \longrightarrow 2$ or 3

After step 5

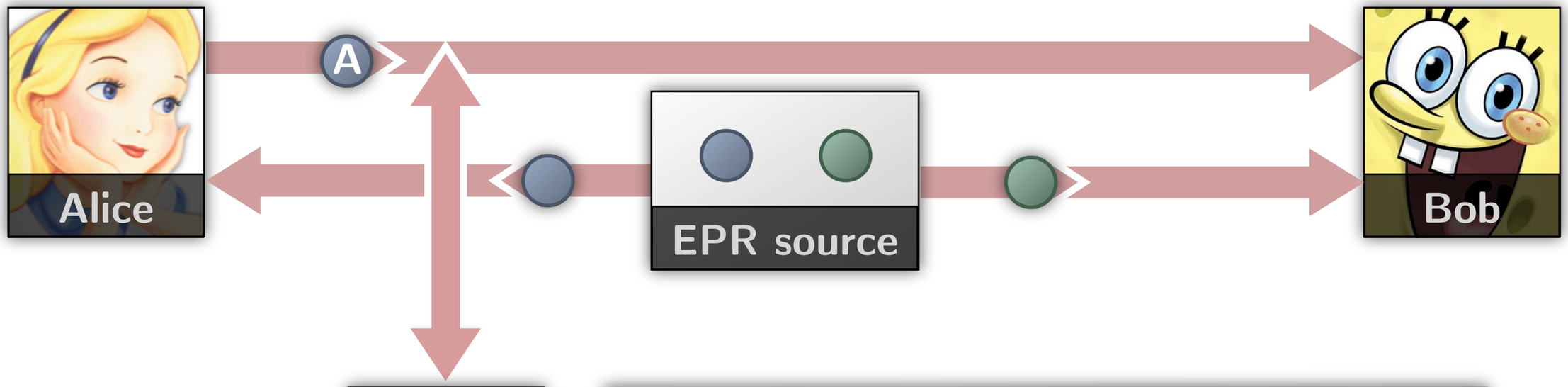
$0 \longrightarrow (|00\rangle + |10\rangle)/\sqrt{2}$

$1 \longrightarrow (|11\rangle + |01\rangle)/\sqrt{2}$

$2 \longrightarrow (|01\rangle - |11\rangle)/\sqrt{2}$

$3 \longrightarrow (|00\rangle - |10\rangle)/\sqrt{2}$

Dense coding

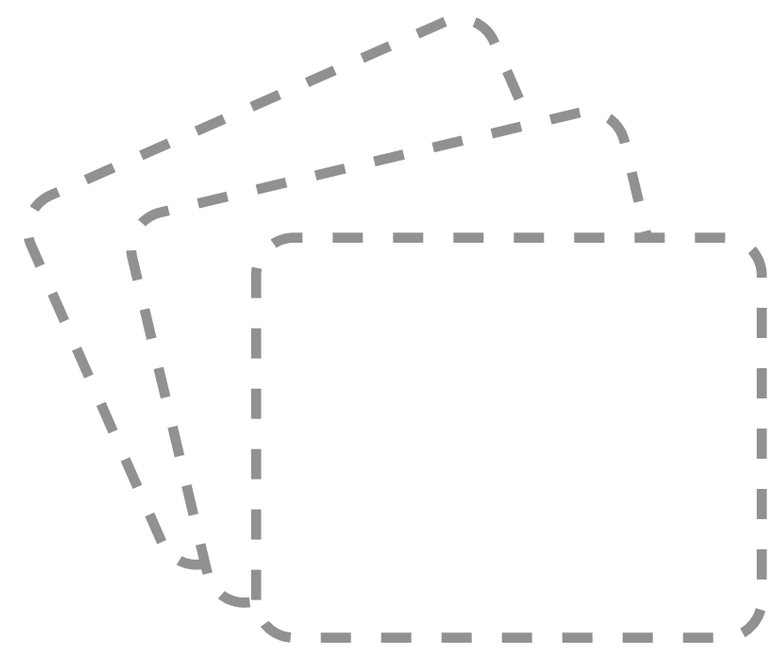


No information from a single qubit.

Information comes from correlations between Alice and Bob's qubits.

Quantum teleportation

Error – Slides have been teleported to a parallel universe*



*Actually they have not been written due to lack of motivation and suitable temporal window

References

Thirty Years of Integer Factorization
François Morain
http://algo.inria.fr/seminars/sem00-01/morain.ps

Cramming more components onto integrated circuits
G.E. Moore
Electronics, Volume 38, Number 8, April 19, 1965

An Introduction to Quantum Computing for Non-Physicists
E. Rieffel & W. Polak
http://arxiv.org/abs/quant-ph/9809016v2

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer
Peter Shor
http://arxiv.org/pdf/quant-ph/9508027v2

A fast quantum mechanical algorithm for database search
Lov K. Grover
http://arxiv.org/abs/quant-ph/9605043

References

Quantum Cryptography: Public Key Distribution and Coin Tossing
C.H. Bennett & G. Brassard
Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, December 1984, pp 175-179.

Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states
C.H. Bennett & S.J. Wiesner
Phys. Rev. Lett. 69, 2881–2884 (1992)