Quantum circuits and Quantum Algorithms

Dung Nguyen

Brown University

DARTMOUTH

Quantum Winter School 2020

BROWN PHYSICS

Content

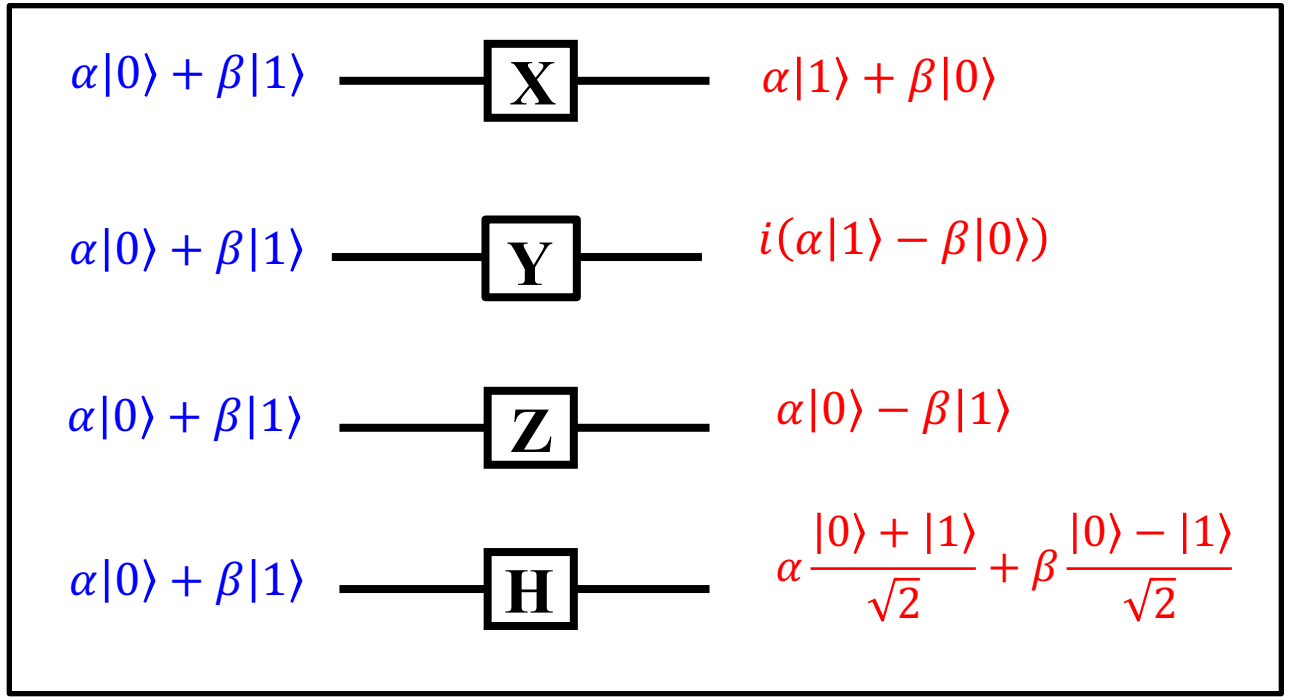
- ❑Universal quantum gates (Solovay-Kitaev theorem)
- ❑ Quantum circuits
- ❑Quantum parallelism.
- ❑ Deutsch & Deutsch-Jozsa algorithm

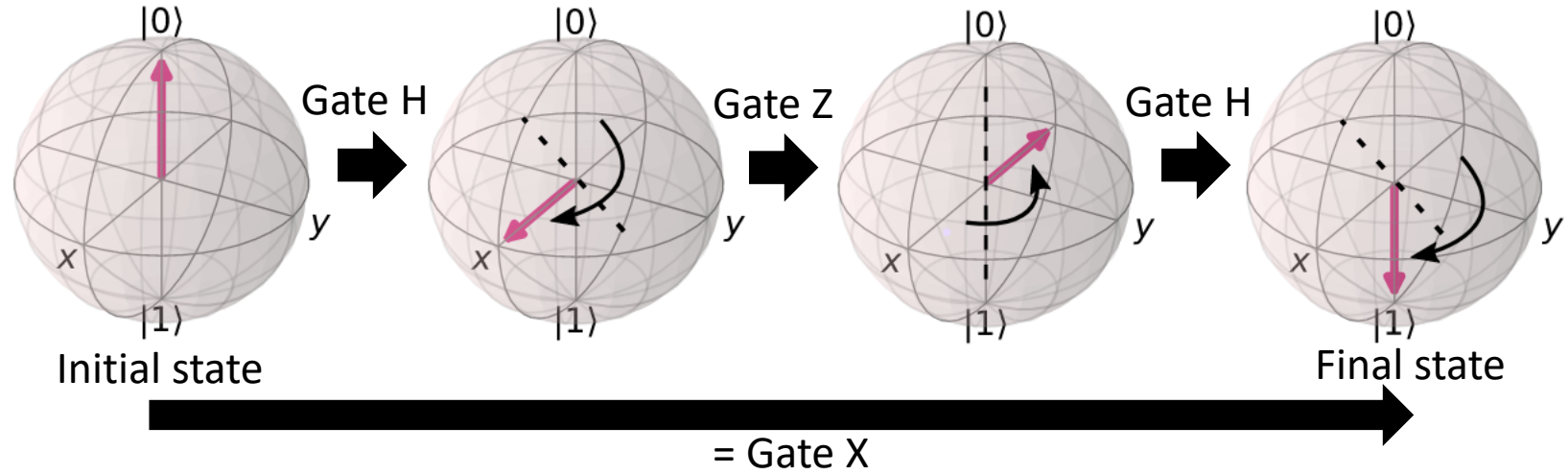
Appendix:

- ❑BB84 protocol: An example of quantum cryptography
- ❑No-cloning theorem
- ❑Quantum communication
- ❑Grover’s algorithm

Universal quantum gates

Universal single qubit gates





- We know that any unitary transformation in 2 dimensions (1-qubit gate) can be decomposed in to Euler rotations

Rotation around Z-axis — Rotation around Y-axis — Rotation around Z-axis

Overall phase

$$U = e^{i\alpha} \begin{bmatrix} e^{\frac{i\beta}{2}} & 0 \\ 0 & e^{-\frac{i\beta}{2}} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{\frac{i\delta}{2}} & 0 \\ 0 & e^{-\frac{i\delta}{2}} \end{bmatrix}$$

- So with any unitary transformation, can we built it up from 4 elementary gates? Not really, since $\alpha, \beta, \gamma, \delta$ are real numbers, we still need infinite number of elementary gates to built up exactly any unitary transformation.
- However with in an approximation

$$|\mathrm{U}|\psi> - U_{built}|\psi>|^2 \leq \epsilon$$

where U_{built} is the transformation built from elementary quantum gates.

We need only some certain special fixed elementary rotations $\lambda_\alpha, \lambda_\beta, \lambda_\gamma, \lambda_\delta$, and the price is we need more than 4 gates to build up U_{built}.

- For an arbitrary real number α, and a fixed irrational number $\tilde{\lambda}_\alpha$, we always can find a integer number m such that

$$\left| e^{i\alpha} - e^{i\, m\tilde{\lambda}_\alpha \pi} \right| < \epsilon$$

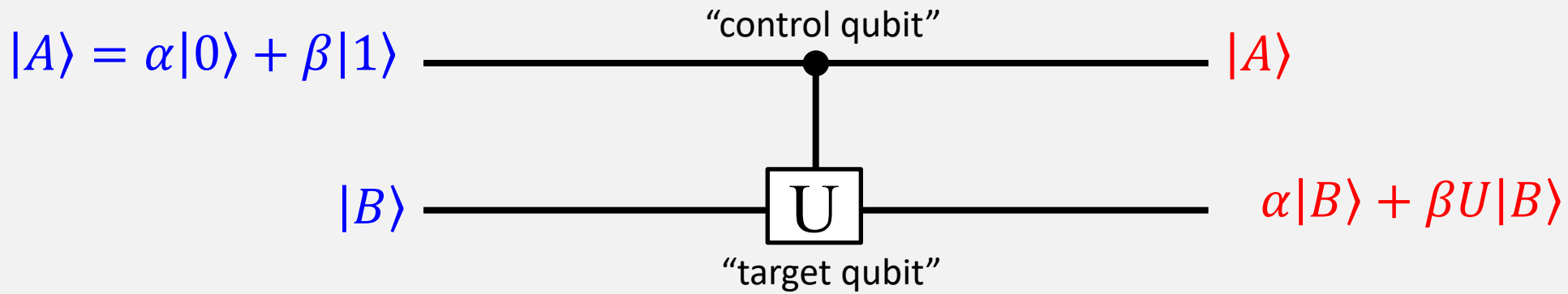
- Thus an $e^{i\alpha}$ gate can be built up (approximately) from m $e^{i\tilde{\lambda}_\alpha \pi}$ gates ($\lambda_\alpha = \tilde{\lambda}_\alpha \pi$).
- We can argue similarly for other rotations $\lambda_\beta, \lambda_\gamma, \lambda_\delta$.
- This is just an example to show that we can have a set of universal single qubit gates. In practice, we may use different set of gates as the universal single qubit gates.

Note : To archive a general 1-qubit unitary operator, one needs only a set of 2 universal gates, for example, a rotation about the x-axis with angle α and a rotation about the y-axis with angle β such that both α and β are irrational multiples of π.

How about multiple-qubits gates?

2-qubit controlled gate

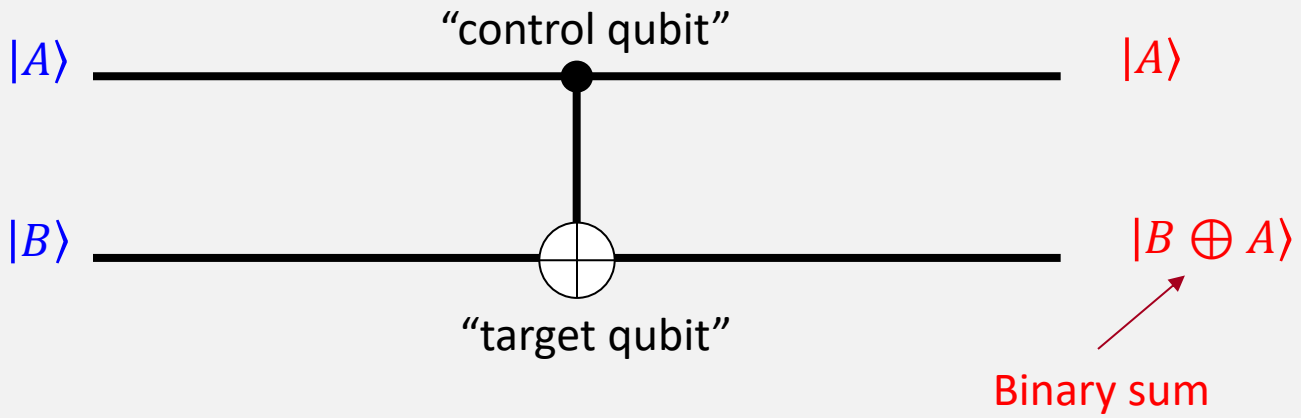
Let U be a 1-qubit gate, the 2-qubit gate "Controlled U" is defined by:



➡ We apply the operation U on the target qubit when ever the control qubit is $|1\rangle$

2-qubit quantum gate: CNOT gate

CNOT (Controlled NOT gate) is the reversible version of classical **XOR**:



$$\text{CNOT}|A, B\rangle = |A, B \oplus A\rangle$$

$$\text{CNOT}|00\rangle = |00\rangle$$
$$\text{CNOT}|01\rangle = |01\rangle$$
$$\text{CNOT}|10\rangle = |11\rangle$$
$$\text{CNOT}|11\rangle = |10\rangle$$

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

You know how does CNOT act on a general (superposition) state from this definition.

(In the computational basis) CNOT gate flips the « target qubit » if the value of the « control qubit » = 1

Universal quantum gates

- We can prove that any multiple qubits transformation can be constructed from CNOT gates and single qubit gates.
- For an approximation ϵ, any multiple qubits gate can be built from CNOT gate, Hadamard gate and $R_{\frac{\pi}{4}}$ gate.
- Thus we have CNOT gate, Hadamard gate and $R_{\frac{\pi}{4}}$ gate are a set of universal gates for multiple qubits.
- We have quantum Church-Turing thesis:

  One can use an universal quantum computer to simulate other quantum computers.

- It is one of the conclusions of Solovay-Kitaev theorem

Robert M. Solovay
1938
American Mathematician

Alexei Kitaev
1963
Russian-American Physicist

$$R_{\frac{\pi}{4}} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$$

Remark : An example of classical version of Church-Turing thesis is famous recently.
One can use an ARM processor (Apple's M1 processor) to simulate x86 processors (Intel's Core-i or AMD's Ryzen).
(And vice versa of course-simulating an android phone (ARM) on your PC (x86))

Summary I:

- We now see that one can build up any multiple qubits operator with universal quantum gates.
- Quantum gate is the most essential element of a quantum circuit that we will discuss subsequently.
- We will assume that we can construct (approximately) any unitary operation.

LOGIC CIRCUITS:

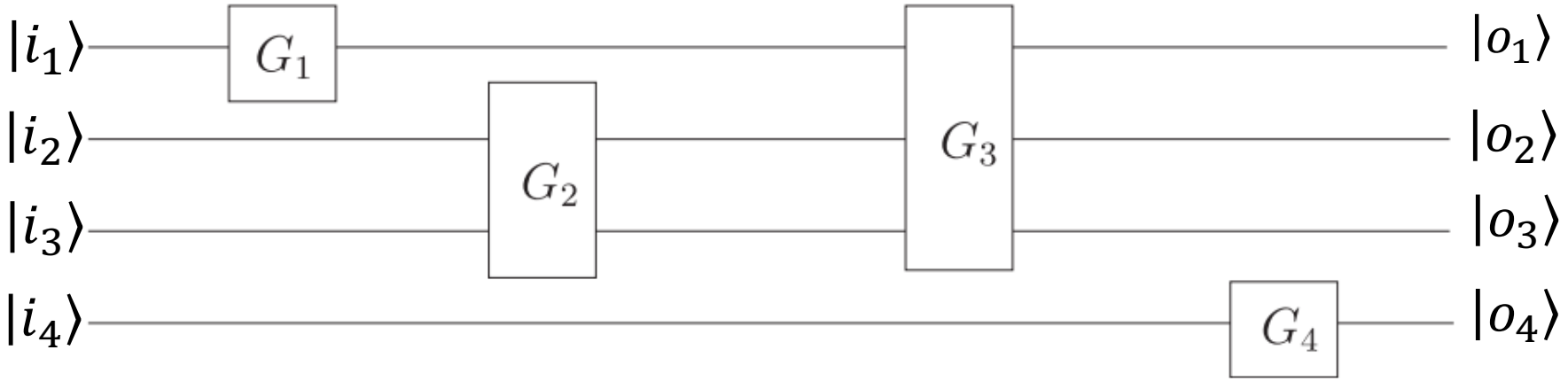
Classical VS Quantum

Logic circuit: update to "quantum"

SAME
SAME
BUT
DIFFERENT

- Made up of wires and logic gates
- Information spreads from the left → right on horizontal lines
- Acyclic (no loops)

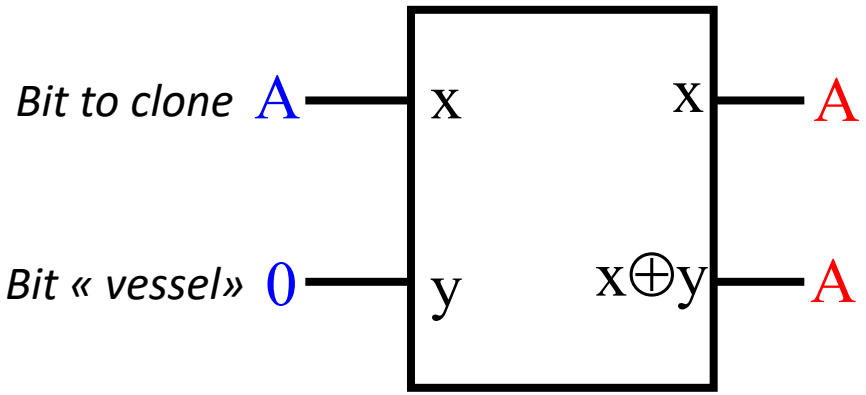
- Bits are superposition states $|a\rangle = \alpha|0\rangle + \beta|1\rangle$
- Reversible (a classical circuit is not necessary to be reversible)



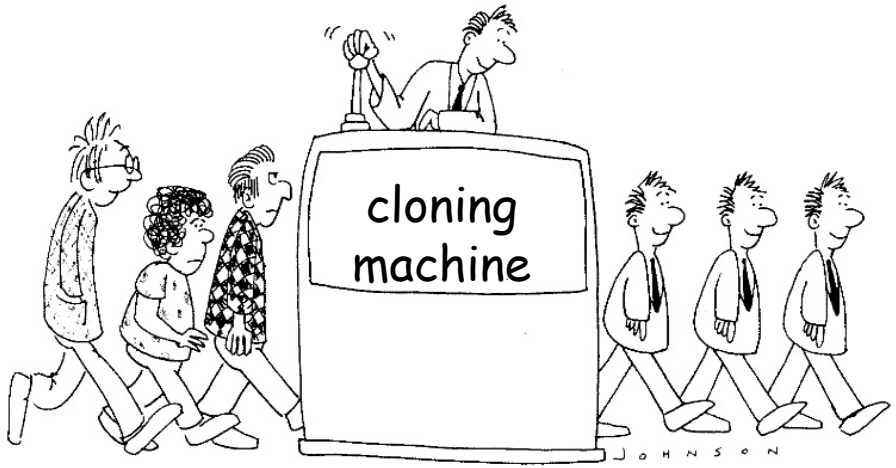
Remark: (I assume) The decoherence processes can be neglected so that the circuit is reversible (i.e. closed). All the operations must last much shorter than the system (de)-coherence time.

Clone circuit

The logic circuit to clone a classic bit (Fan out):



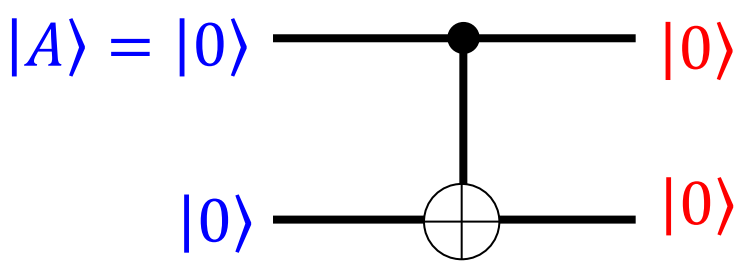
Classical version of CNOT

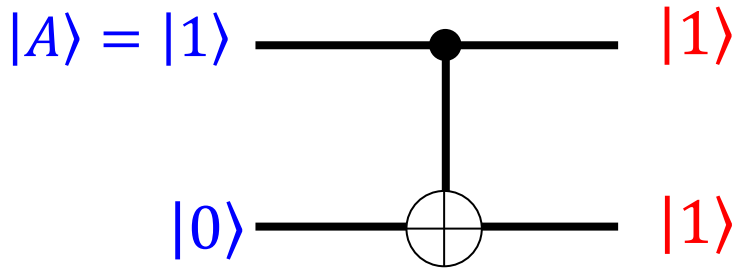


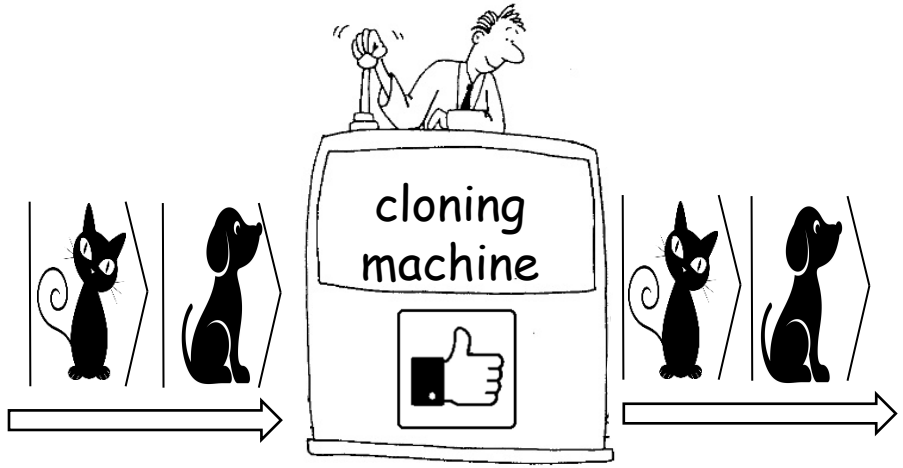
Does the quantum version allow quantum cloning to be carried out? $|A\rangle|0\rangle \xrightarrow{?} |A\rangle|A\rangle$

Quantum cloning with CNOT

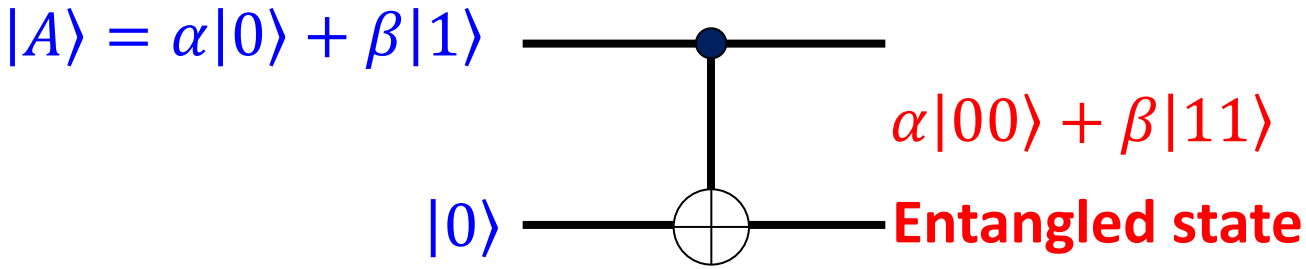
Seems to work fine like the classic version if the inputs are basis states

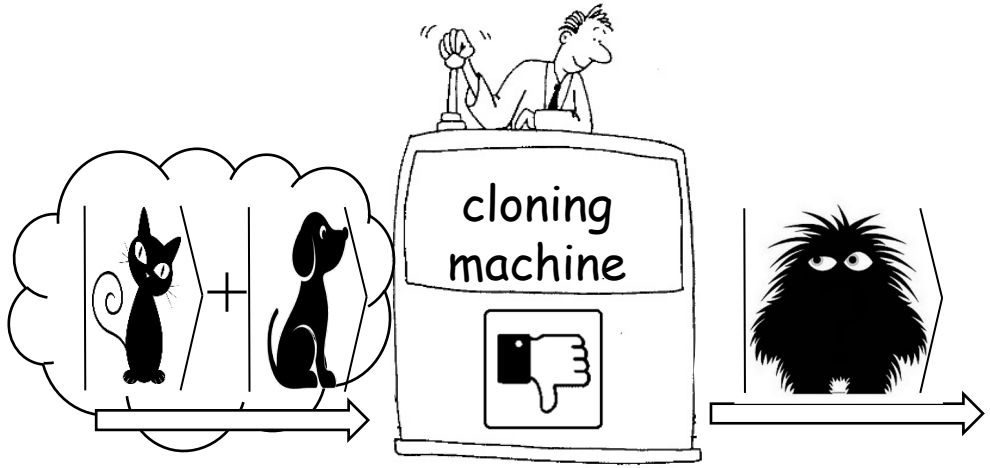






But when we try to clone a quantum superposition state ...

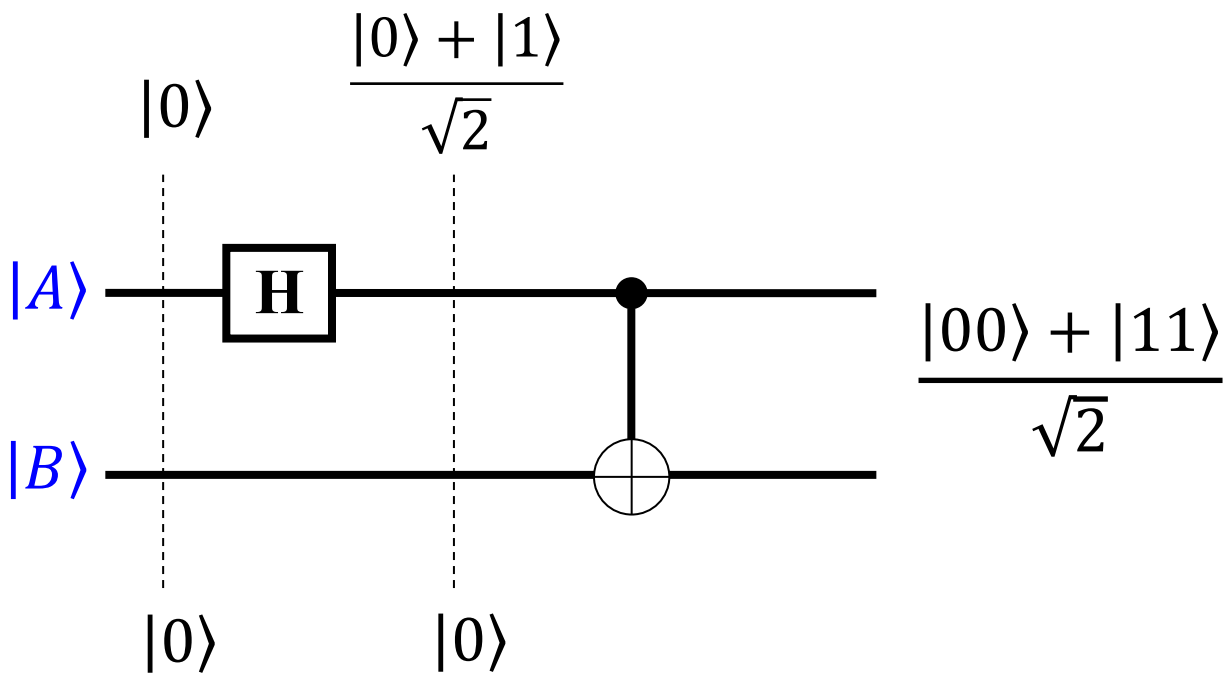




There is the "no-cloning theorem" which implies that one can't copy a general quantum state (Appendix)

Due to "no-cloning theorem" , one can't easily steal your quantum information (see the quantum communication section in the Appendix).

Entanglement cicuit: Creating Bell's state



$\|A\rangle$	$\|B\rangle$	Output
$\|0\rangle$	$\|0\rangle$	$\frac{\|00\rangle + \|11\rangle}{\sqrt{2}}$
$\|0\rangle$	$\|1\rangle$	$\frac{\|01\rangle + \|10\rangle}{\sqrt{2}}$
$\|1\rangle$	$\|0\rangle$	$\frac{\|00\rangle - \|11\rangle}{\sqrt{2}}$
$\|1\rangle$	$\|1\rangle$	$\frac{\|01\rangle - \|10\rangle}{\sqrt{2}}$

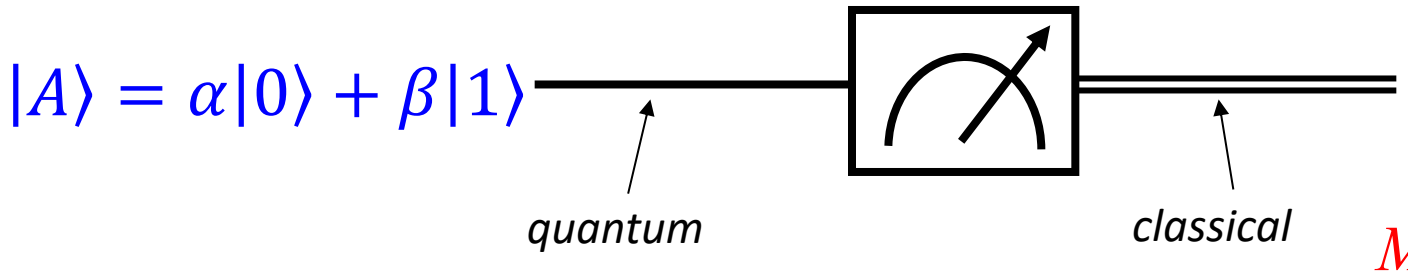
The basis to describe the entangled states of 2 qubits

CIRCUITS WITH MEASUREMENTS

We can have the combination of quantum gates and quantum measurements in a quantum circuit

Implementation of "quantum measurements"

Result of a measurement on a qubit gives a classical bit value in with a probability



M (classic bit represents the result of the measurement)

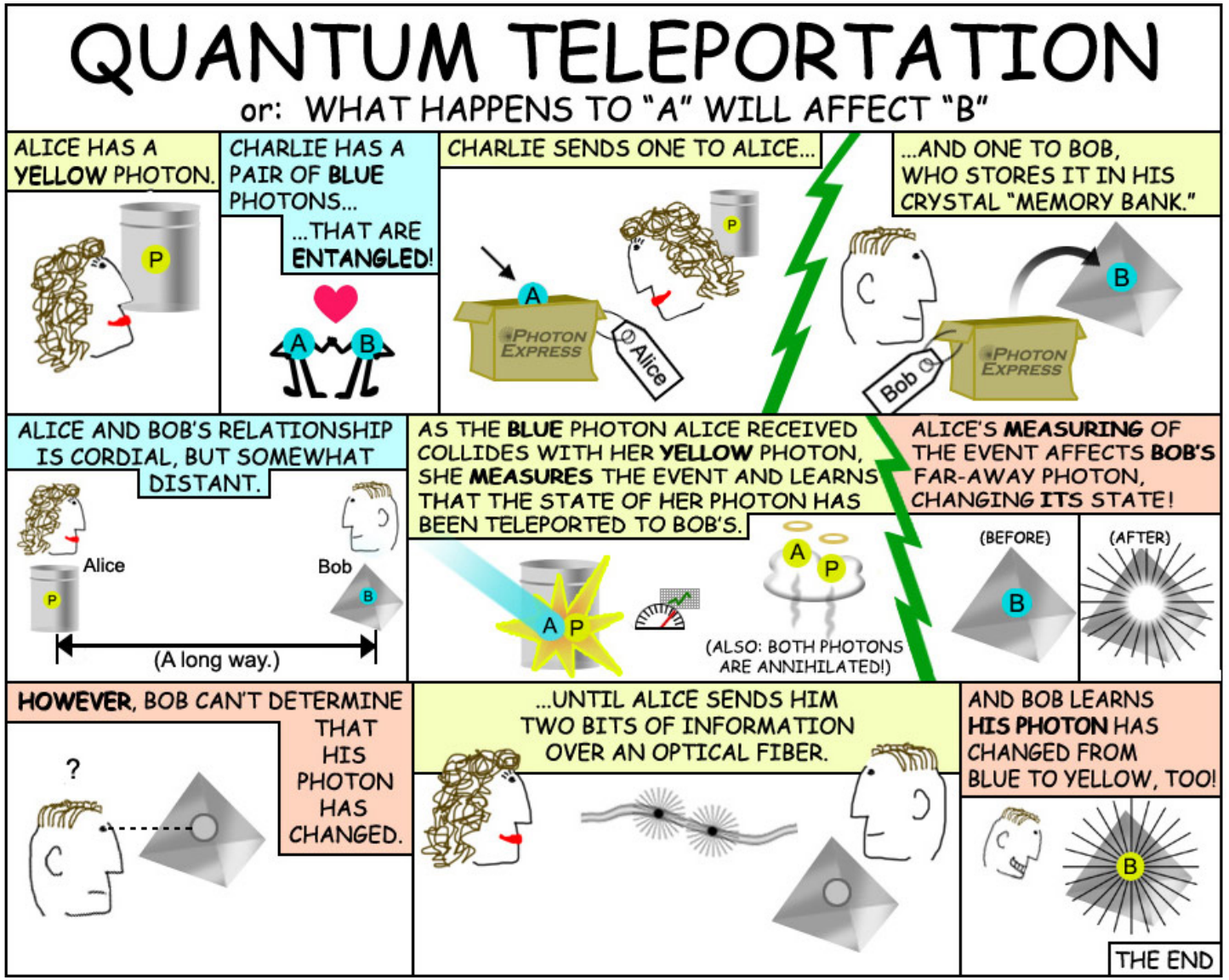
$M = 0$ with prob. $|\alpha|^2$

$M = 1$ with prob. $|\beta|^2$

Note : The measurement is always carried out in a chosen basis $\{|0\rangle, |1\rangle\}$.

Question: - What about the coherent? (on the measured line, and also the unmeasured lines)

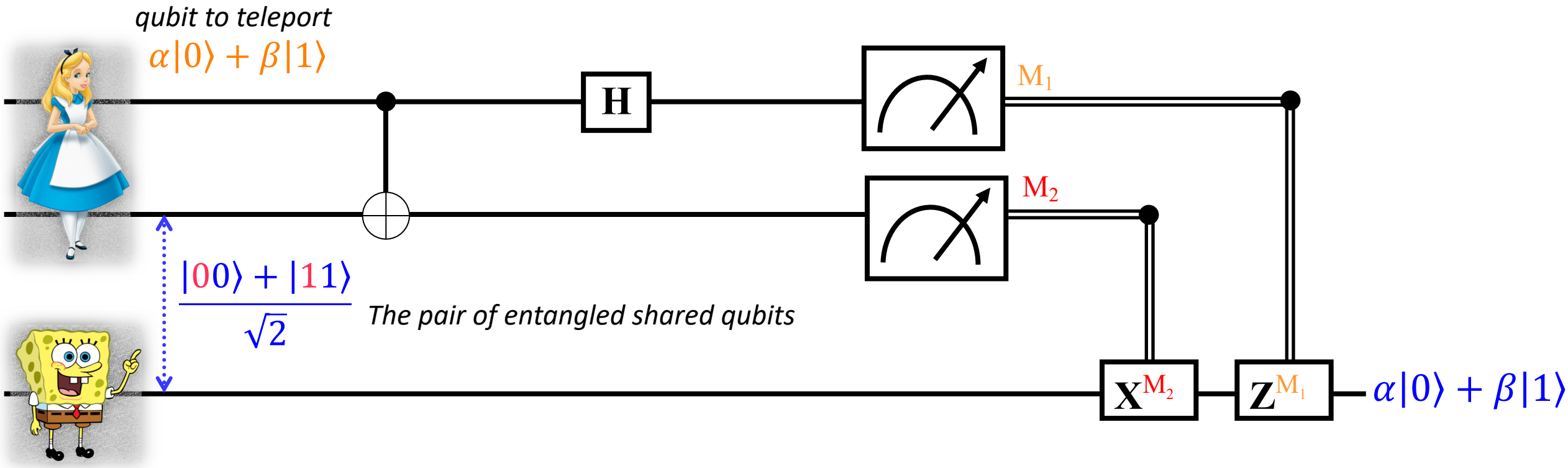
Quantum teleportation: in a nutshell



Allice wants to send a quantum bit to Bob safely.

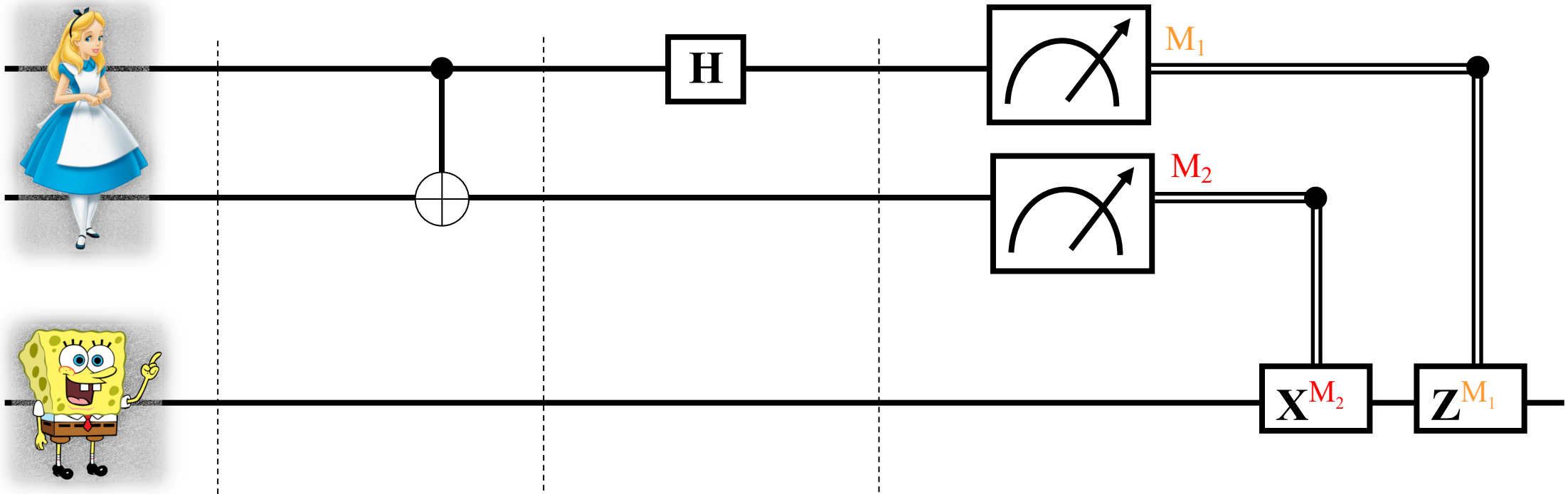
1. A and B qubits are entangled, one is sent to Bob and one is sent to Alice.
2. P is the qubit that Alice wants to teleport
3. Alice measures the value of (A,P)
   → 2 qubit becomes classical
   → reports the measurement result to Bob
4. Bob performs a 1 qubit operation on B based on Alice's result

Quantum teleport: implementation



We will demonstrate in the following how this implementation works ...

Quantum teleportation: before measurements



$$(\alpha|0\rangle + \beta|1\rangle)\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$\alpha|0\rangle\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \beta|1\rangle\frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

$$\alpha\frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|00\rangle + |11\rangle}{\sqrt{2}} + \beta\frac{|0\rangle - |1\rangle}{\sqrt{2}}\frac{|10\rangle + |01\rangle}{\sqrt{2}}$$

$$= \frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle) + \frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle) + \frac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle)$$

Quantum teleportation: after measurements

The quantum state before measurement:

$$\frac{1}{2}|00\rangle(\alpha|0\rangle+\beta|1\rangle)+\frac{1}{2}|01\rangle(\alpha|1\rangle+\beta|0\rangle)+\frac{1}{2}|10\rangle(\alpha|0\rangle-\beta|1\rangle)+\frac{1}{2}|11\rangle(\alpha|1\rangle-\beta|0\rangle)$$

Once Alice has measured her qubits, these bits become classical $\{M_1, M_2\}$.
But Bob's qubit (still intact) remains quantum and can still be manipulated in a coherent way

If Alice measures		Bob will get	Bob will apply	and finally gets
M_1	M_2			
0	0	$\alpha\|0\rangle+\beta\|1\rangle$	$\mathbf{I}$	$\alpha\|0\rangle+\beta\|1\rangle$
0	1	$\alpha\|1\rangle+\beta\|0\rangle$	$\mathbf{X}$	
1	0	$\alpha\|0\rangle-\beta\|1\rangle$	$\mathbf{Z}$	
1	1	$\alpha\|1\rangle-\beta\|0\rangle$	$\mathbf{Y}=\mathbf{ZX}$	

Summary II:

- ❑We've seen the differences between quantum circuits and classical circuits.
- ❑We've seen some simple applications of quantum circuits in quantum information.
- ❑We will use quantum circuits to implement quantum algorithms.
- ❑Quantum teleportation is not quantum cloning (no quantum copy) because Allice's qubit dies after the measurement.

QUANTUM PARALLELISM

the Quantum Oracle and Deutsch's algorithm

Quantum parallelism

Quantum parallelism is one aspect of the quantum computer that allows a function ***f(x)*** to be evaluated for different values of ***x***, simultaneously.

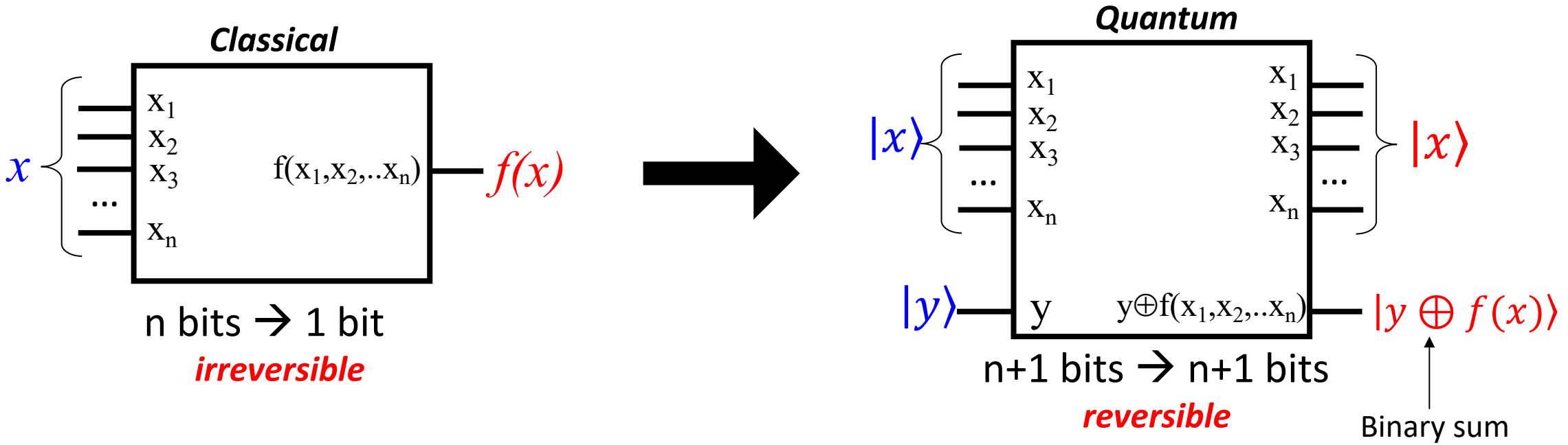
We will illustrate a quantum parallelism:

Simultaneously calculate the function ***f(0)*** and ***f(1)*** for a given binary function ***f***

Logic circuit to implement a binary function

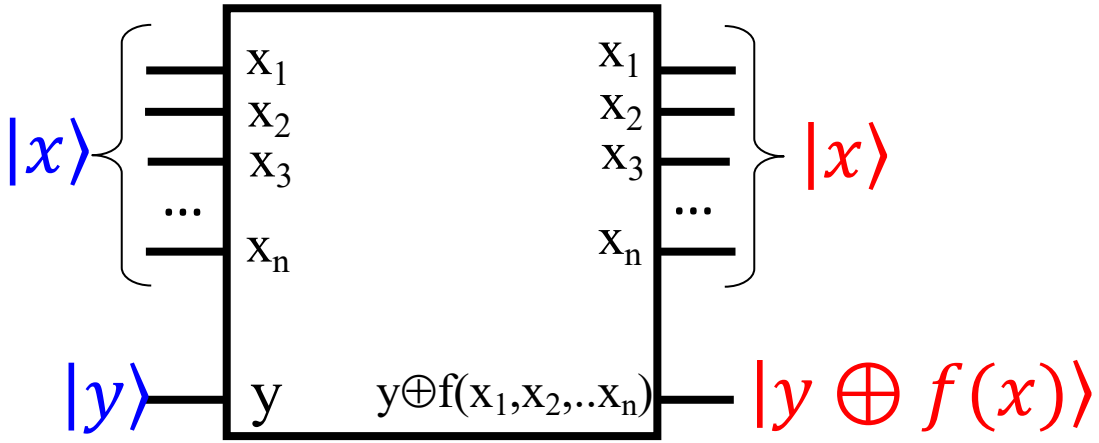
- Let's consider a binary function $f: \{0,1\}^n \mapsto \{0,1\}$

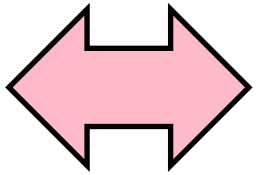
- The logic circuit to realize the function *f*:

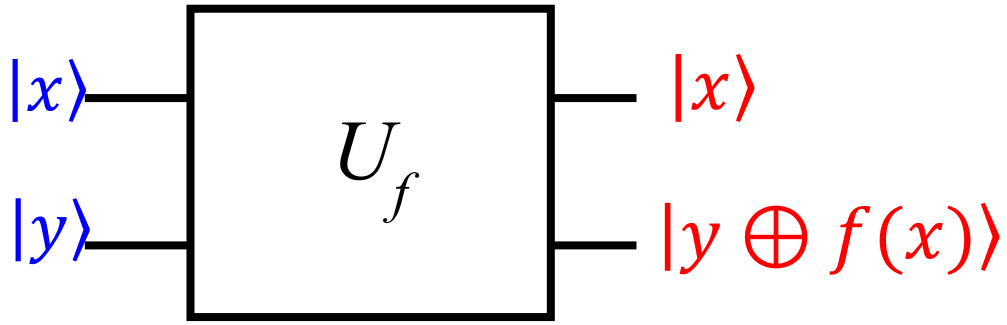


We can easily understand the quantum version with $|x\rangle$ is a basis state ($|x_i\rangle = \{|1\rangle, |0\rangle\}$) and also $|y\rangle = \{|1\rangle, |0\rangle\}$. The operation on a general (superposition) multi-qubits state can be obtained using linear algebra.

Quantum operator to realize a binary function







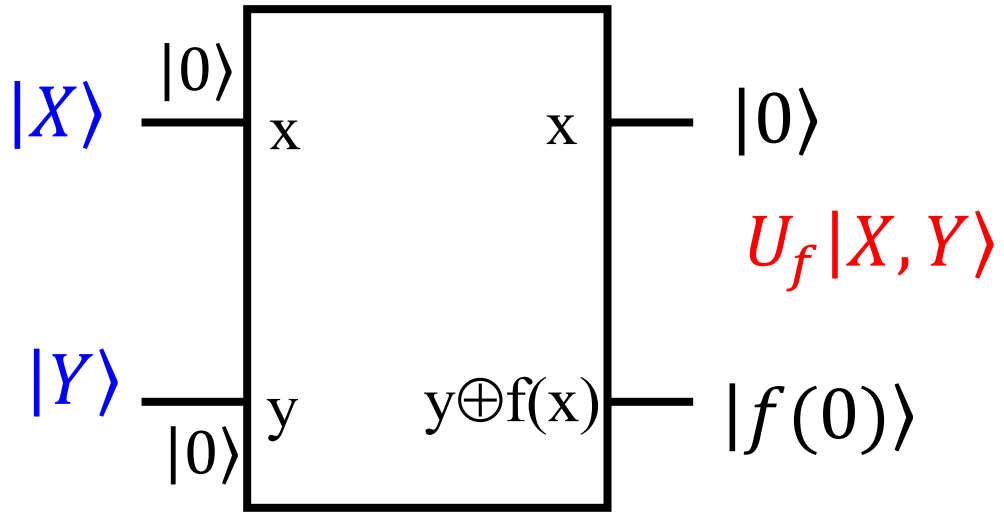
$$U_f: |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$$

The operator U_f is called: "quantum black box" or "quantum oracle"

Questions: - Show that $U_f.U_f = I$

- Prove that U_f is unitary (so that it is a valid quantum operation)

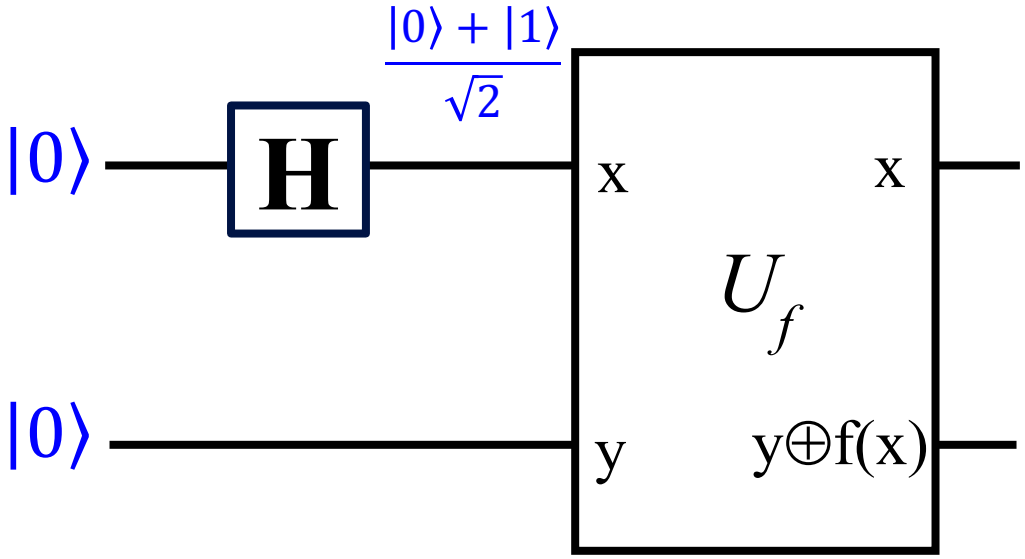
The quantum oracle with n = 1



$\|X\rangle$	$\|Y\rangle$	Output
$\|0\rangle$	$\|0\rangle$	$\|0, f(0)\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0,1 \oplus f(0)\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1, f(1)\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1,1 \oplus f(1)\rangle$

For each "question", only one "Response" f (0) or f (1) is evaluated.

The quantum oracle with n = 1: quantum parallelism



$$\frac{U_f|00\rangle}{\sqrt{2}} + \frac{U_f|10\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}(|0, f(0)\rangle + |1, f(1)\rangle)$$

$f(0)$ and $f(1)$ are calculated simultaneously

n qubits

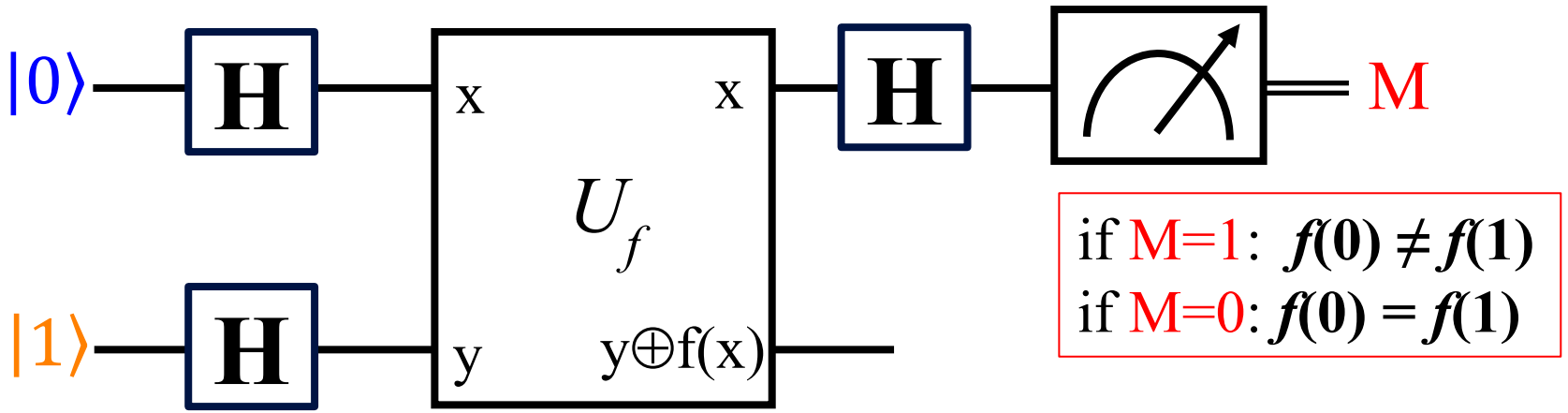
A quantum circuit can simultaneously follow $\mathbf{2^n}$ classical paths

Deutsch's algorithm: the first quantum algorithm

Problem:

Let an oracle (a black box) defined by the binary function $f(x)$: $\{0,1\} \rightarrow \{0,1\}$.
→ with **just one question**, how do we know if $f(0)=f(1)$ or $f(0)\neq f(1)$?

➡ Deutsch's proposal (1985)



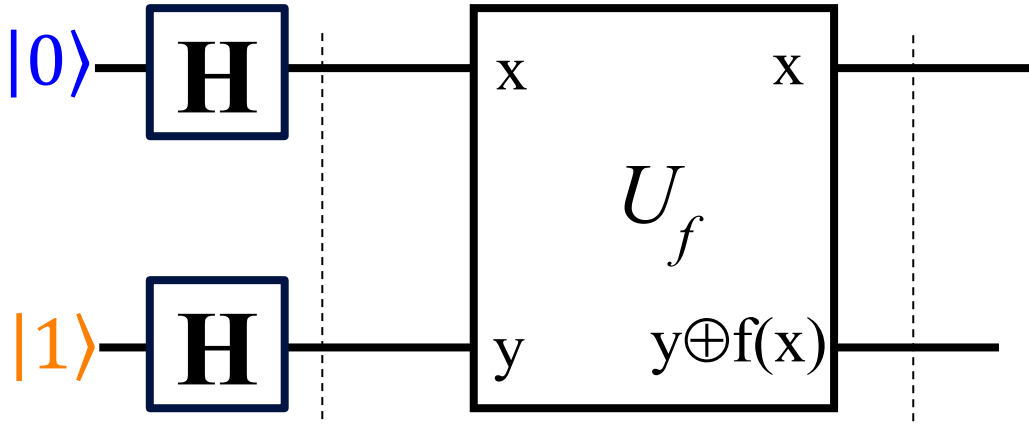
if M=1: $f(0) \neq f(1)$
if M=0: $f(0) = f(1)$

David Deutsch
(1953)

- Anecdote 1: Deutsch is an advocate of the multiverse interpretation of quantum mechanics proposed by Everett.
- Anecdote 2: Deutsch is falsely mentioned by the character Tony Stark in the movie Avenger End game :

"Quantum fluctuation messes with the Planck scale, which then triggers the Deutsch Proposition. Can we agree on that?"

Deutsch algorithm: step-by-step analysis



$$\frac{1}{\sqrt{2}}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right]$$

$$\frac{1}{2}\left[(-1)^{f(0)} + (-1)^{f(1)}\right]|0\rangle$$
$$\frac{1}{2}\left[(-1)^{f(0)} - (-1)^{f(1)}\right]|1\rangle$$

➡ if M=1: $f(0) \neq f(1)$
if M=0: $f(0) = f(1)$

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$= |0\rangle\frac{|0\rangle - |1\rangle}{2} + |1\rangle\frac{|0\rangle - |1\rangle}{2}$$

$$|0\rangle\frac{|f(0)\rangle - |1\oplus f(0)\rangle}{2}$$
$$+|1\rangle\frac{|f(1)\rangle - |1\oplus f(1)\rangle}{2}$$

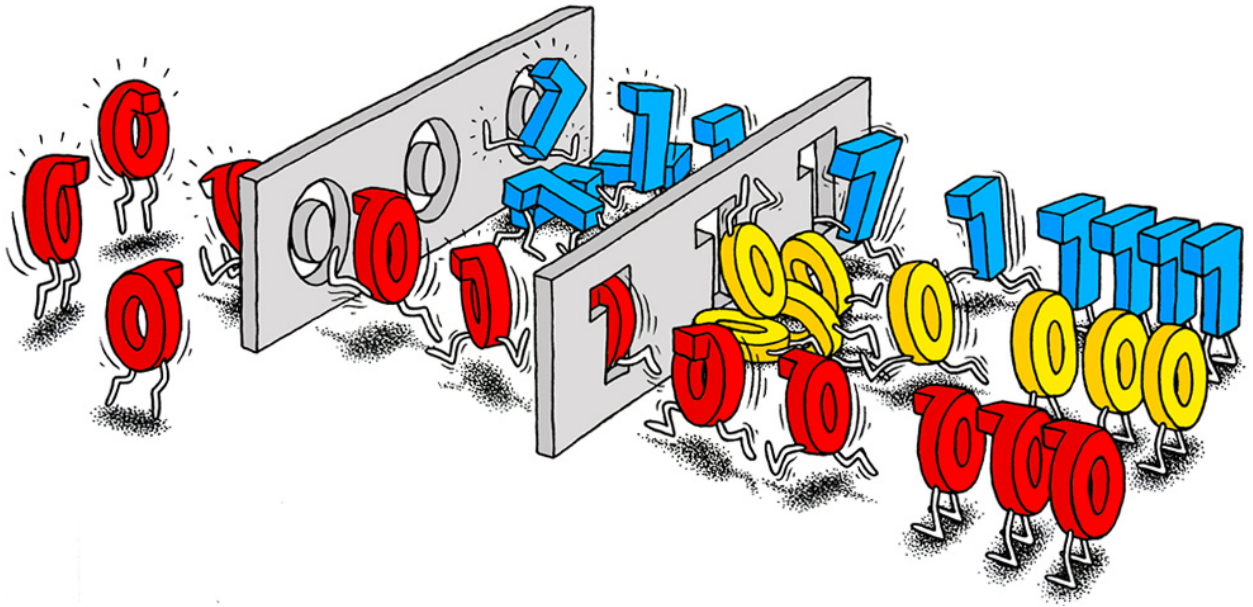
$$= \frac{1}{2}\sum_{x=0}^{1}|x\rangle\underbrace{(|f(x)\rangle - |1\oplus f(x)\rangle)}_{\begin{cases} f(x)=0: & |0\rangle - |1\rangle \\ f(x)=1: & |1\rangle - |0\rangle \end{cases}} = \frac{1}{2}\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

Summary III:

- The power of quantum computation is quantum parallelism.
- **Quantum parallelism is a consequence of quantum superposition**:

  the quantum circuit can simultaneously evaluate several classical paths.
- We will use quantum parallelism for multiple-qubits algorithms.

MULTI-QUBITS



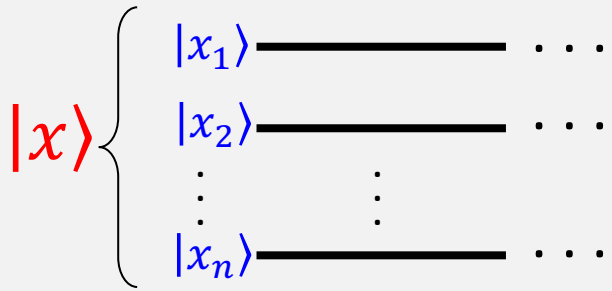
Binary / computational basis

« computational basis » = **The basis of the measuring device**

1 qubit → 2 states: $|0\rangle, |1\rangle$

No quantum superposition!

n qubits → $\boxed{N = 2^n}$ linear independent states: $|x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle = |x_1 x_2 x_3 \ldots . x_n\rangle$ with $x_j \in \{0,1\}$



$|0..000\rangle, |0..001\rangle, |0..010\rangle, \ldots . , |1..111\rangle$

$\underbrace{\quad}_{|0\rangle} \quad \underbrace{\quad}_{|1\rangle} \quad \underbrace{\quad}_{|2\rangle} \quad \underbrace{\quad}_{|N-1\rangle}$

$|x\rangle$ with $\boxed{x = 2^{n-1}x_1 + 2^{n-2}x_2 + \ldots + 2^0 x_n}$

Hadamard / superposition basis : definition

The Hadamard / superposition basis is defined by:

n bits $\rightarrow \boxed{N = 2^n}$ basis states:

Binary basis: $|x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle = |x\rangle$

$$H^{\otimes n} \rightarrow \boxed{\prod_{j=1}^{n} \left\{ \frac{|0\rangle + (-1)^{x_j}|1\rangle}{\sqrt{2}} \right\}}$$

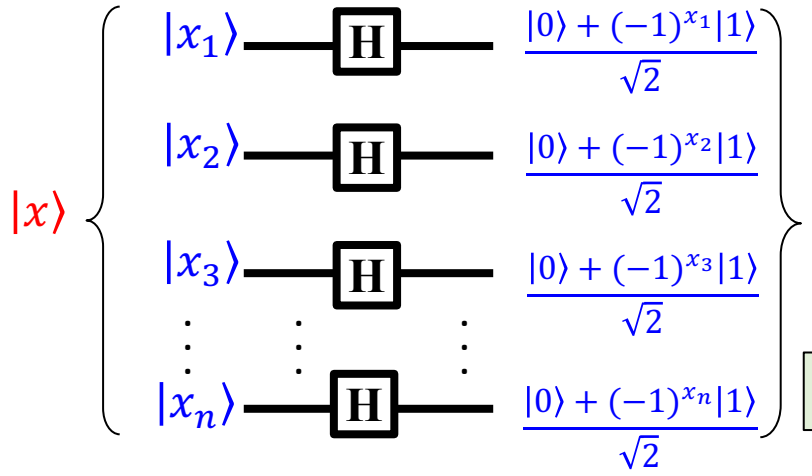
Hadamard basis

Tensor product

with $x_j \in \{0,1\}$

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

Balanced Quantum superposition !!!



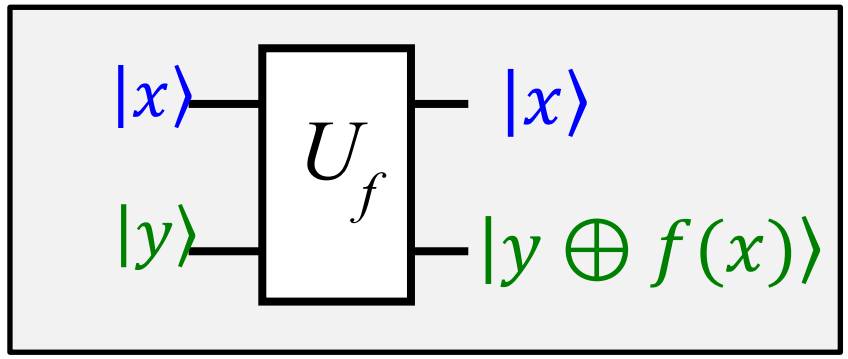
$$\boxed{\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} (-1)^{x \cdot y} |y\rangle}$$

With $x \cdot y$ is the scalar product $\sum_i x_i y_i$

Question: Prove this expression

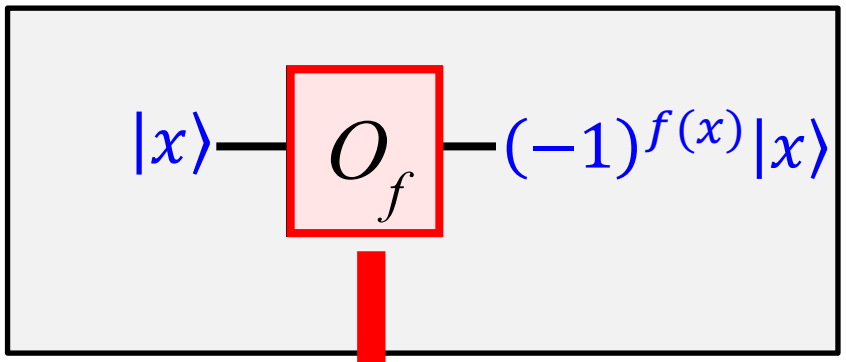
Phase Oracle: The Ultimate Quantum Oracle

Quantum bit oracle



More practical

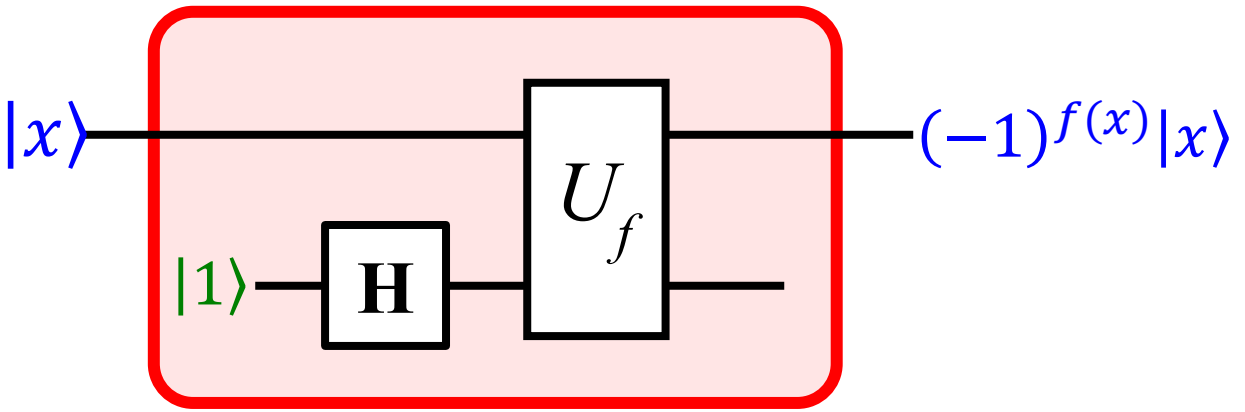
Quantum phase oracle



$$f: \{0,1\}^n \mapsto \{0,1\}$$

$|x\rangle = |x_1 x_2 x_3 \ldots x_n\rangle$ with $x_j \in \{0,1\}$

$|y\rangle = \{|1\rangle, |0\rangle\}$

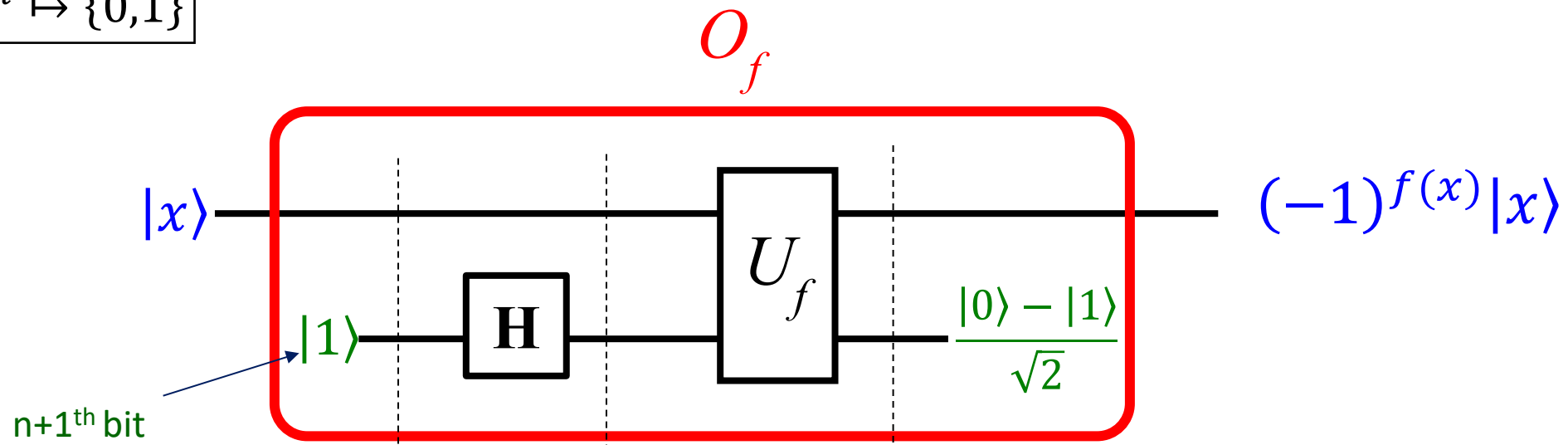


Questions: - *Show that $O_f.O_f = I$*
- *Prove that O_f is unitary*

Phase oracle: how does it work?

$|x\rangle = |x_1 x_2 x_3 \ldots x_n\rangle$ with $x_j \in \{0,1\}$

$f: \{0,1\}^n \mapsto \{0,1\}$



$|x\rangle|1\rangle$

$|x\rangle \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = (-1)^{f(x)}|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$$\begin{cases} \text{if } f(x) = 0: & \frac{|0\rangle - |1\rangle}{\sqrt{2}} \\ \text{if } f(x) = 1: & \frac{|1\rangle - |0\rangle}{\sqrt{2}} \end{cases}$$

DEUTSCH – JOZSA ALGORITHM

Deutsch-Jozsa algorithm: constant or balanced?

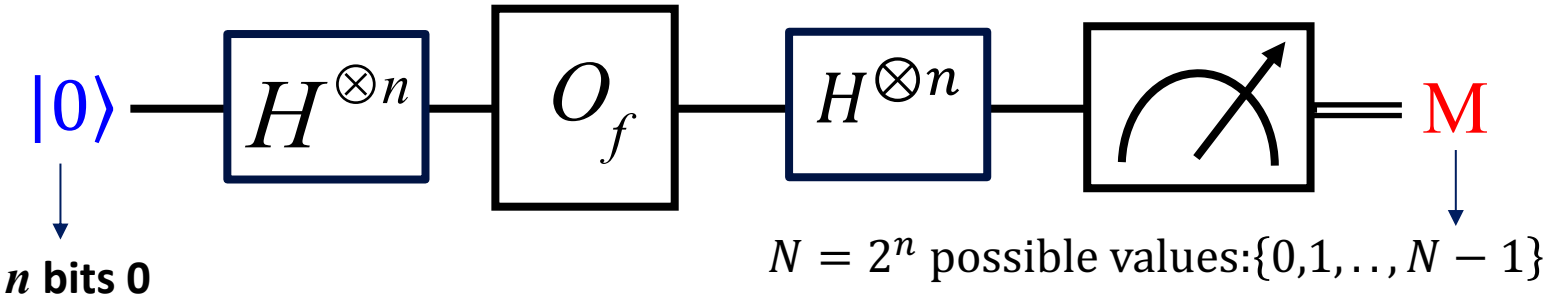
Problem:

Consider an oracle (a black box) defined by a function $f(x)$: $\{0,1\}^n \rightarrow \{0,1\}$.

- Knowing that ***f*** **is: either constant** (the output is 0 or 1 for all inputs)
- **or is balanced** (the output is 0 in half of the cases, 1 in the others).

With just **one question**, how can we tell if ***f*** **is constant or balanced**?

Deutsch-Jozsa's proposal (1992) :



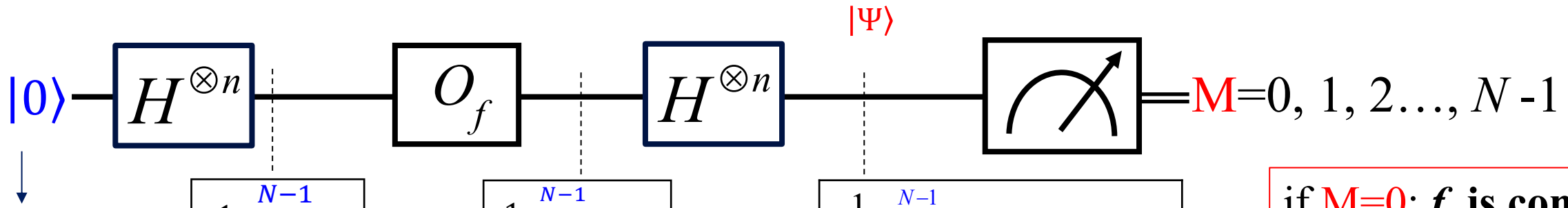
David Deutsch

Richard Jozsa

if M≠0: ***f*** **is balanced**
if M=0: ***f*** **is constant**

Deutsch-Jozsa Algorithm: Step-by-Step Analysis

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}(-1)^{x\cdot y}|y\rangle$$



if M=0: ***f*** **is constant**
if M≠0: ***f*** **is balanced**

$$= \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}(-1)^{f(y)}|y\rangle \qquad = \frac{1}{N}\sum_{y=0}^{N-1}(-1)^{f(y)}\sum_{x=0}^{N-1}(-1)^{x\cdot y}|x\rangle$$

$$\langle 0|\Psi\rangle = \frac{1}{N}\sum_{y=0}^{N-1}(-1)^{f(y)}$$

n **bits 0**

$$\begin{cases} f \text{ is constant}: & \langle 0|\Psi\rangle = \pm 1 \\ f \text{ is balanced}: & \langle 0|\Psi\rangle = 0 \end{cases}$$

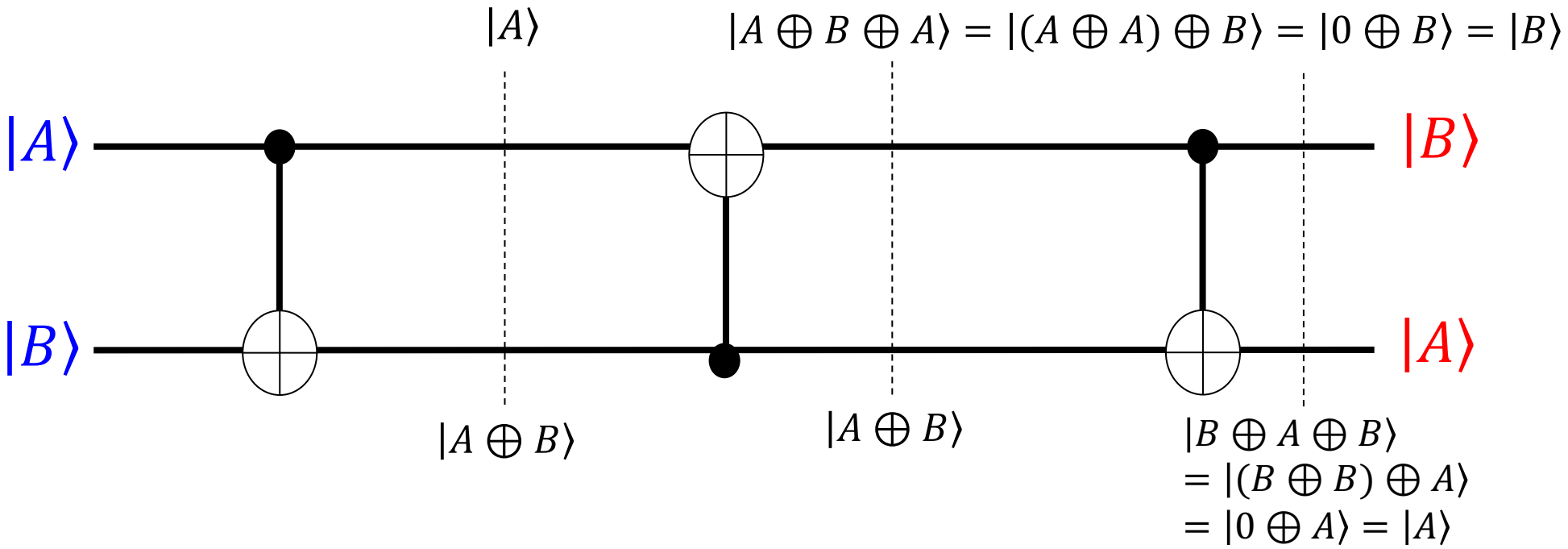
Summary

- **Quantum version of Church-Turing thesis (Solovey-Kiatev theorem)**
- **Quantum circuits differ fundamentally from classical circuits.**
- **Quantum parallelism** is the origin of **quantum algorithms** with the Oracle. This is a common concept to most quantum algorithms.
- We have seen the Deutsch-Jozsa's algorithm: the very first and simplest quantum algorithm using quantum parallelism.

Thank you and have fun!

Appendix

Exchange circuit: qubit swapping



No-cloning theorem

We can not do quantum copy on a qubit

❑*Proof:*

If we can find an unitary operator C (clone operator) such that with any normalized qubit state $|\psi>$, we have

$$C|\psi>_1|e_0>_2 = |\psi>_1|\psi>_2$$

$$\rightarrow <e_0|<\psi|C^\dagger C|\varphi>|e_0> = <e_0|<\psi|\varphi>|e_0>$$

$$\rightarrow <\psi|\varphi>_1<\psi|\varphi>_2 = <\psi|\varphi>_1<e_0|e_0> = <\psi|\varphi>$$

Thus we have

$$<\psi|\varphi>^2 = <\psi|\varphi>$$

This can not be true for general state.

BB84 protocol: An example of quantum cryptography

Key exchange on the quantum channel of the BB84 protocol:

-Alice **randomly** chooses between the basis $\{\leftrightarrow,\updownarrow\}$ and $\{\nearrow,\nwarrow\}$ to **Send** her bits **one by one**

-Bob **randomly** chooses between the basis $\{\leftrightarrow,\updownarrow\}$ and $\{\nearrow,\nwarrow\}$ to **Measure** his bits **one by one**

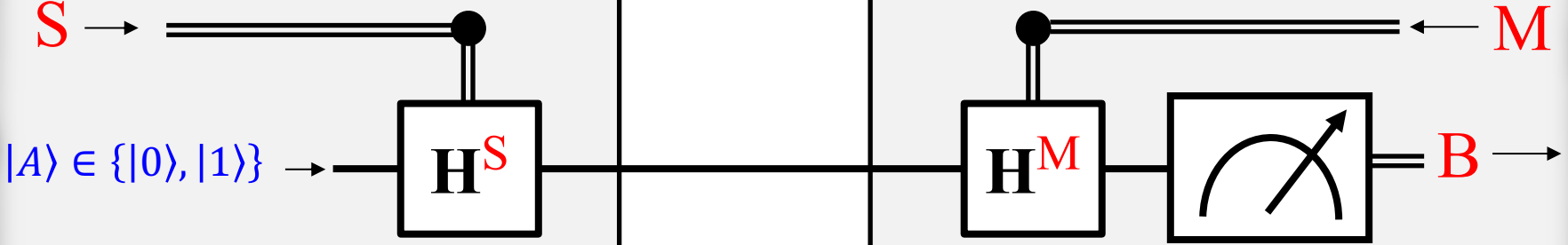
Binary basis $\begin{cases} |\leftrightarrow\rangle \equiv |0\rangle \\ |\updownarrow\rangle \equiv |1\rangle \end{cases}$

Hadamard *basis* $\begin{cases} |\nearrow\rangle \equiv \dfrac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |\nwarrow\rangle \equiv \dfrac{|0\rangle - |1\rangle}{\sqrt{2}} \end{cases}$

After the measurement, Bod and Alice compare (publicly) **S** and **M**, then save the sent and measured bits if **S=M**

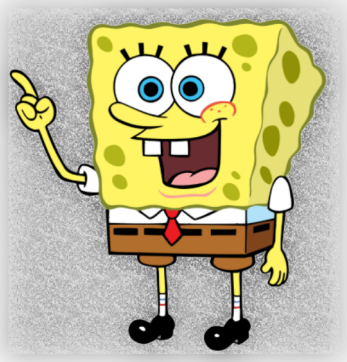
$S = 0$: send with $\{\leftrightarrow,\updownarrow\}$

$S = 1$: send with $\{\nearrow,\nwarrow\}$



$M = 0$: measure with $\{\leftrightarrow,\updownarrow\}$

$M = 1$: measure with $\{\nearrow,\nwarrow\}$



Quantum Communication

- We can use quantum entanglement to send the decode key for classical cryptography.

- If Alice want to share with Bob a secret key that they can use latter to decode the information. However they worry about Eva, who can steal their key.
- Alice prepare a entanglement state

$$|\phi^+> = \frac{|00> + |11>}{\sqrt{2}}$$

- And send one of qubit to Bob
- Then Alice and Bob do the measurement on their qubit in Z and X, if they have 100% correlation, they know that they share an entanglement pair of qubit.

Quantum Communication

- Since Eva can interfere with the system, the state of the three is

$$|\Phi\rangle_{ABE} = \frac{1}{\sqrt{2}}\left(\begin{array}{c} |00\rangle_{AB}|e_{00}\rangle_E + |01\rangle_{AB}|e_{01}\rangle_E \\ +|10\rangle_{AB}|e_{10}\rangle_E + |11\rangle_{AB}|e_{11}\rangle_E + \end{array} \right)$$

- But the measurement in Z direction are correlated, thus the state should be

$$|\Phi\rangle_{ABE} = \frac{1}{\sqrt{2}}\left(\quad |00\rangle_{AB}|e_{00}\rangle_E + |11\rangle_{AB}|e_{11}\rangle_E + \right)$$

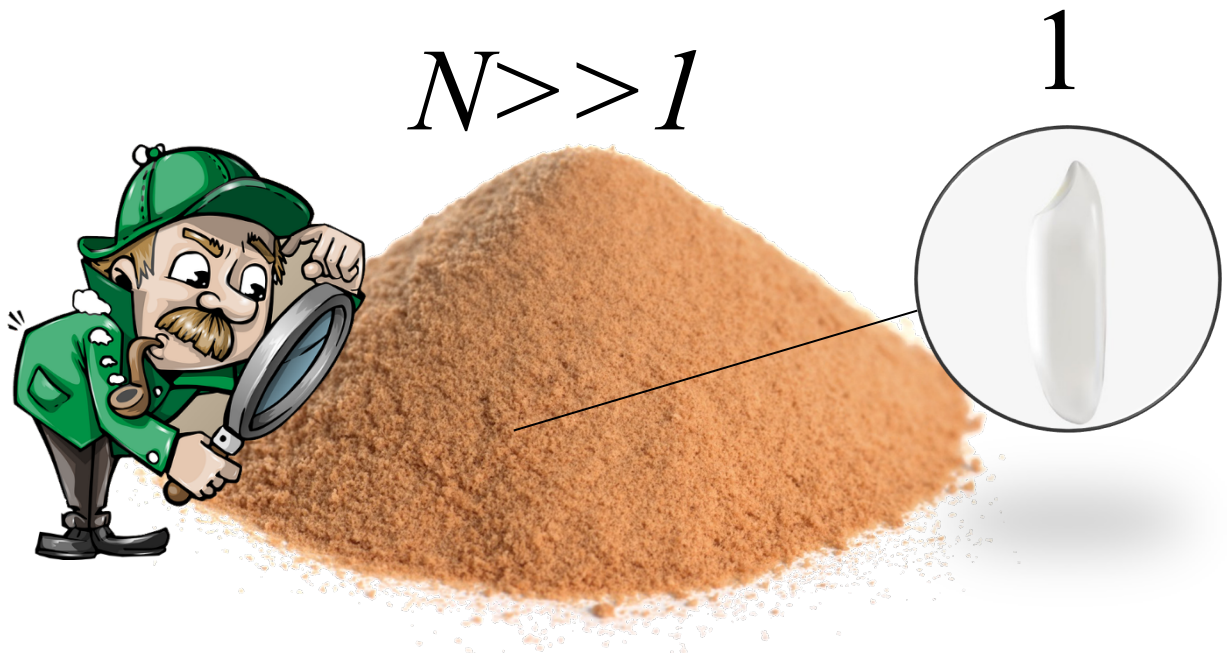
- Furthermore, the measurement in X direction are correlated, thus the state should be

$$|\Phi\rangle_{ABE} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB} \right)|e\rangle_E = |\phi^+\rangle_{AB}|e\rangle_E$$

- So they know that Eva's state is uncorrelated with their entanglement pairs. They can use their shared entanglement pairs to generate random key latter.

GROVER ALGORITHM

Looking for a grain of rice in a sand dune



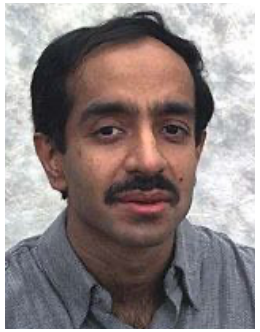
Search in an unstructed data base

Problem:

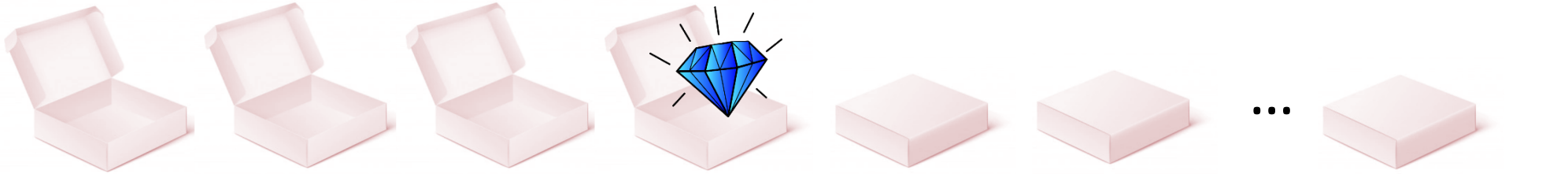
Let an oracle (an black box) defined by a binary function $f(x)$: $\{0,1\}^n \rightarrow \{0,1\}$.

Know that $f(x) = 0$ except for a special value a at which $f(a) = 1$

→ Find a ?



Lov Grover



➡ **Classical Algorithm:** $O(N)$

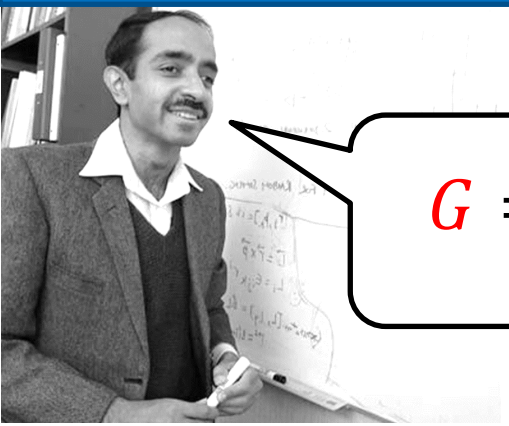
We test the input of function ***f one by one***:

- **Best case: 1 question**
- **Worst case: $N=2^n$ questions**

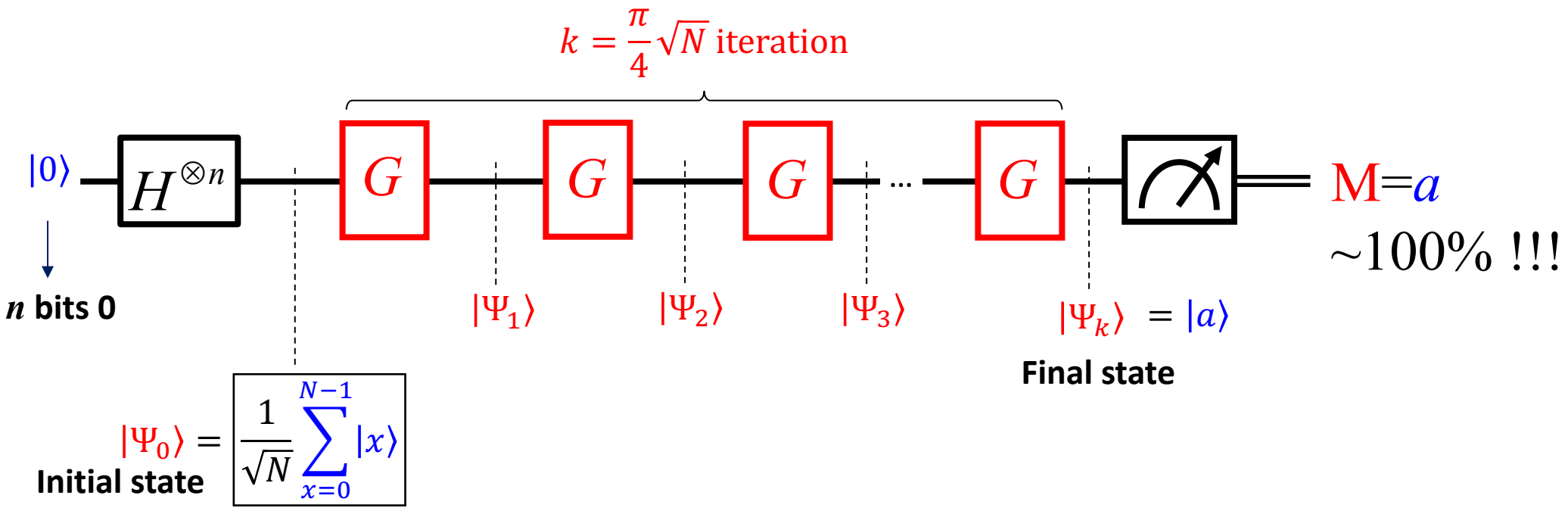
} **On average: ~ $N/2$**

➡ **Quantum Algorithm proposed in 1996 by Grover:** $O(\sqrt{N})$

Grover's circuit and Grover's operator

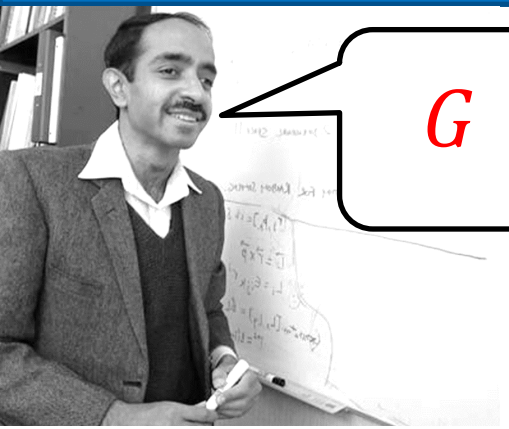


$$G = (2|\Psi_0\rangle\langle\Psi_0| - I).O_f$$



Note: The starting point of the Grover algorithm is the same as the starting point of the Deutsch-Jozsa algorithm

Grover's decomposition



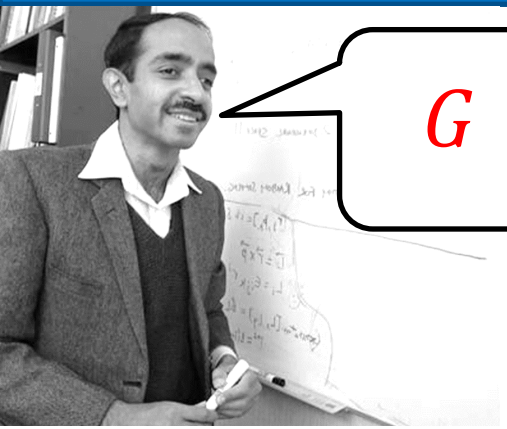
$$G = W.O_f$$

with $W = 2|\Psi_0\rangle\langle\Psi_0| - I$ and $O_f = I - 2|a\rangle\langle a|$

$$|x\rangle \boxed{O_f} (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle \text{ if } x \neq a \\ -|a\rangle \text{ if } x = a \end{cases}$$

$$\begin{cases} f(x) = 0 \text{ if } x \neq a \\ f(x) = 1 \text{ if } x = a \end{cases}$$

Grover's Hilbert subspace



$$G = W.O_f$$ with $$\boxed{W = 2|\Psi_0\rangle\langle\Psi_0| - I}$$ and $$\boxed{O_f = I - 2|a\rangle\langle a|}$$

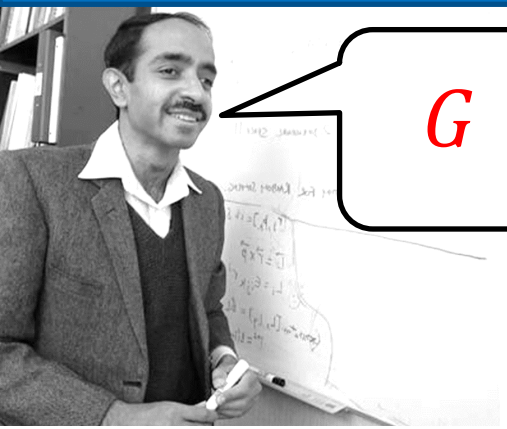
or $$\boxed{|\Psi_0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|y\rangle} \rightarrow \boxed{\langle a|\Psi_0\rangle = \frac{1}{\sqrt{N}}}$$

$$\rightarrow \begin{cases} W|\Psi_0\rangle = |\Psi_0\rangle \\ W|a\rangle = \frac{2}{\sqrt{N}}|\Psi_0\rangle - |a\rangle \end{cases} \text{ and } \begin{cases} O_f|\Psi_0\rangle = |\Psi_0\rangle - \frac{2}{\sqrt{N}}|a\rangle \\ O_f|a\rangle = -|a\rangle \end{cases}$$

➡ With the initial state $|\Psi_0\rangle$, iteration of W and O_f always give a linear combination of $|\Psi_0\rangle$ and $|a\rangle$ with real coefficients

➡ $|\Psi_{1,2,..k}\rangle$ is the two dimensional sub Hilbert space generated by $|\Psi_0\rangle$ and $|a\rangle$

Action of Grover's operator on Grover' Hilbert subspace



$$G = W.O_f$$

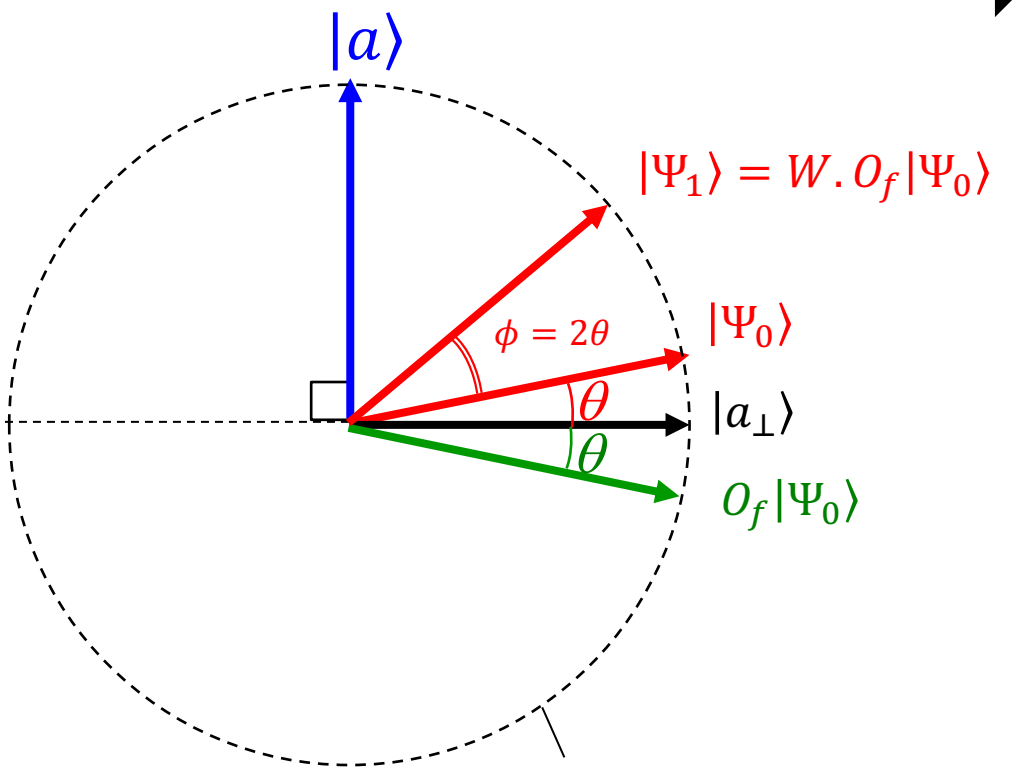
with $W = 2|\Psi_0\rangle\langle\Psi_0| - I$ and $O_f = I - 2|a\rangle\langle a|$

Reflection about $|\Psi_0\rangle$

Reflection about $|a_\perp\rangle$

G = composition of two refections in the plane of Hilbert subspace

= **1 *one rotation* with angle ϕ**



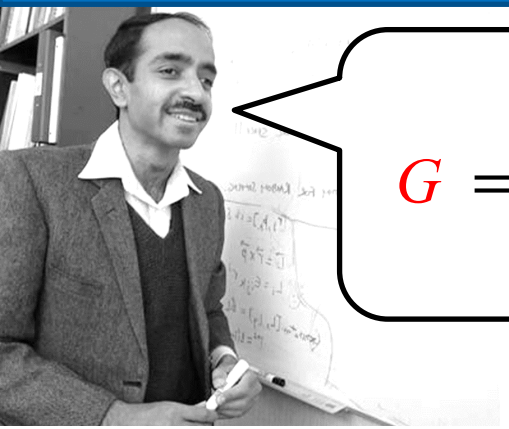
$$\phi = 2\theta$$

We know that: $\sin\theta = \langle a|\Psi_0\rangle = \frac{1}{\sqrt{N}} << 1$

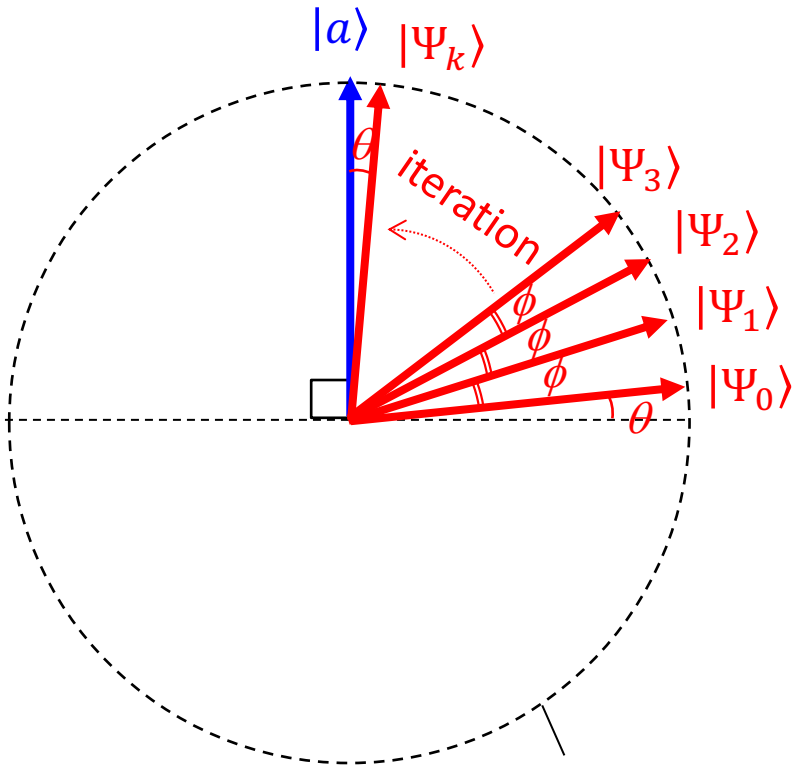
$$\phi \approx \frac{2}{\sqrt{N}}$$

2 – dimentional Hilbert subspace generated by $|\Psi_0\rangle$ and $|a\rangle$

The sequence of state in Grover's circuit



G = **1 rotation with angle** $\boxed{\phi = 2\theta \approx \frac{2}{\sqrt{N}}}$



2 − dimentional Hilbert subspace generated by $|\Psi_0\rangle$ and $|a\rangle$

At the end of $k \sim \left[\frac{\pi/2}{\phi}\right] \sim \left[\frac{\pi}{4}\sqrt{N}\right]$ iterations,
the final state $|\psi_k\rangle$ is within "distance" θ from $|a\rangle$

A measurement of this state gives $M = a$ with a probability:

$$\|\langle a|\Psi_k\rangle\|^2 \geq (\cos\theta)^2 = 1 - (\sin\theta)^2 = \frac{N-1}{N} \sim 1\,00\%$$