NITHeP Mini-school on quantum computing

INTRODUCTION TO THE THEORY OF QUANTUM COMPUTING

Daniel K. Park | dkp.quantum@gmail.com

KAIST

Outline

Part I: What & Why

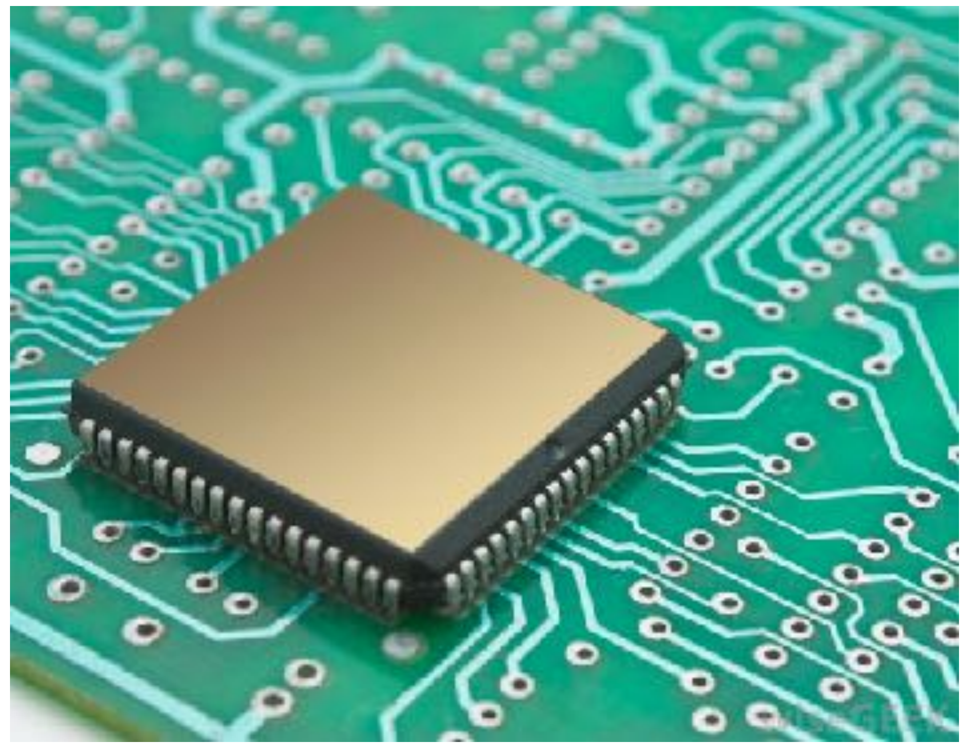
- Introduction & Background

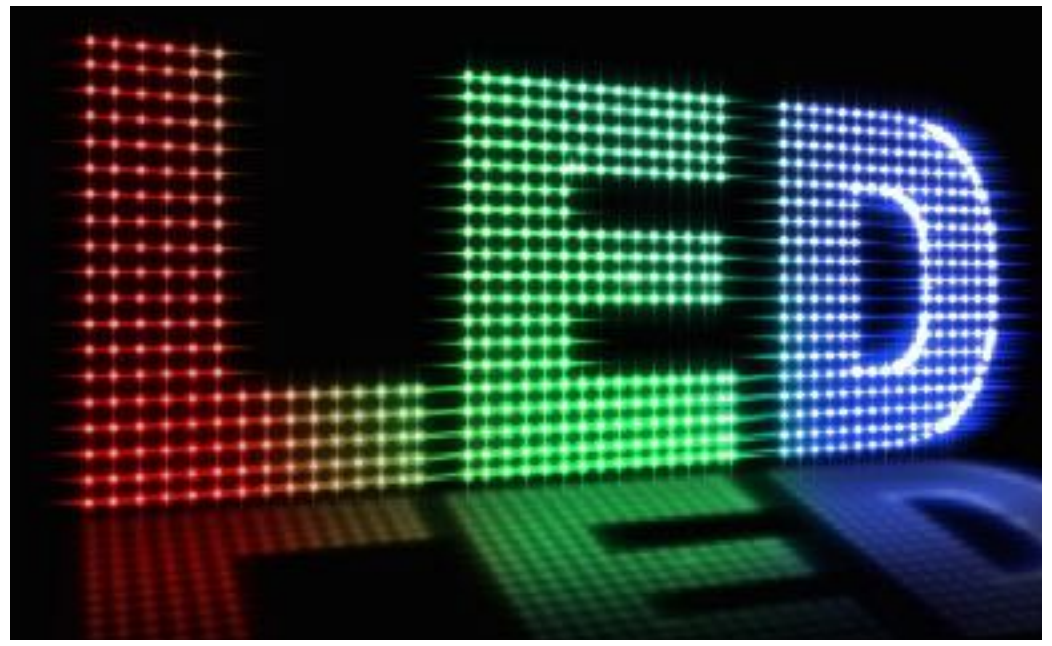
Part II: How

- Quantum Circuit
- Quantum Algorithms
- Quantum Error Correction

Quantum In Technology

Today






Future

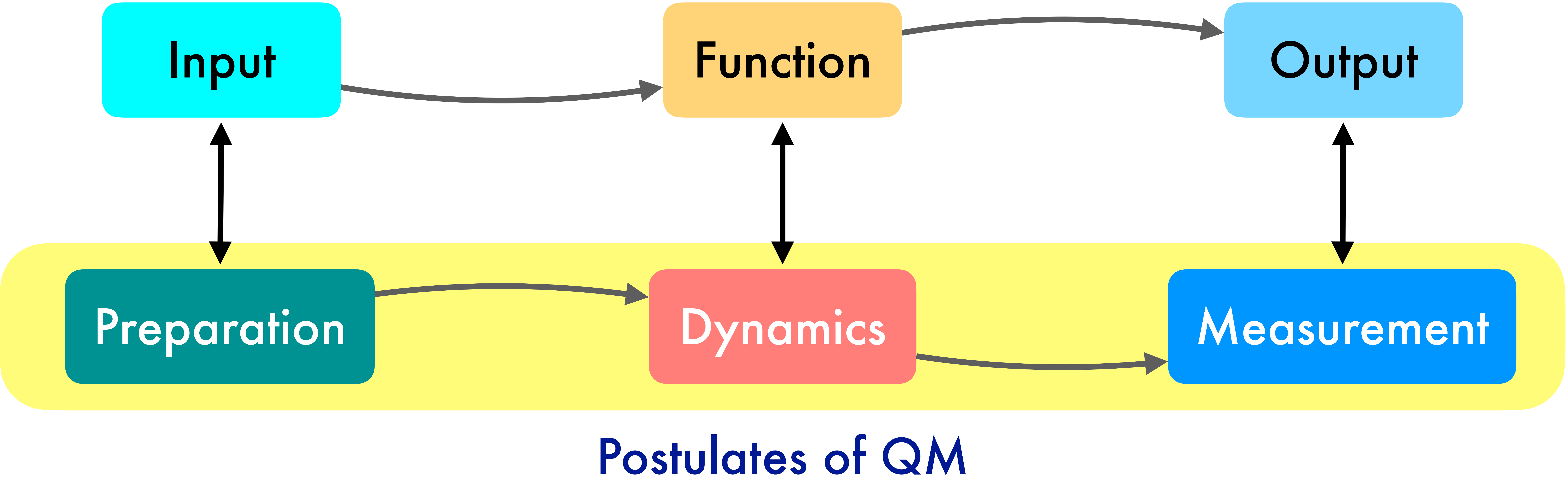
Use the laws of quantum physics for better

computation, communication, and sensing

Quantum Mechanics: Brief Review

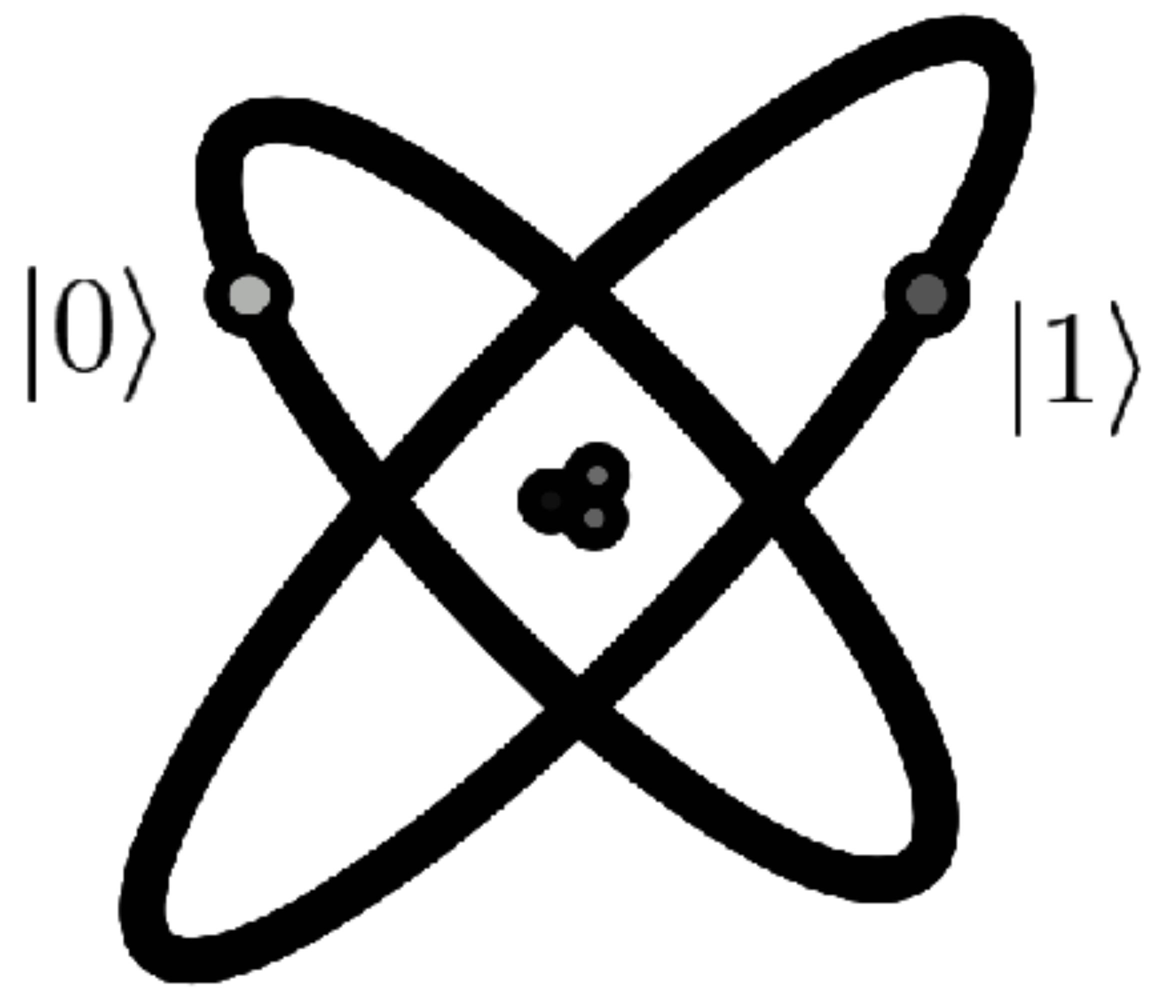
- Quantum Mechanics is a mathematical theory that describes nature at the microscopic/atomic scale.

- Quantum Computing consists of:

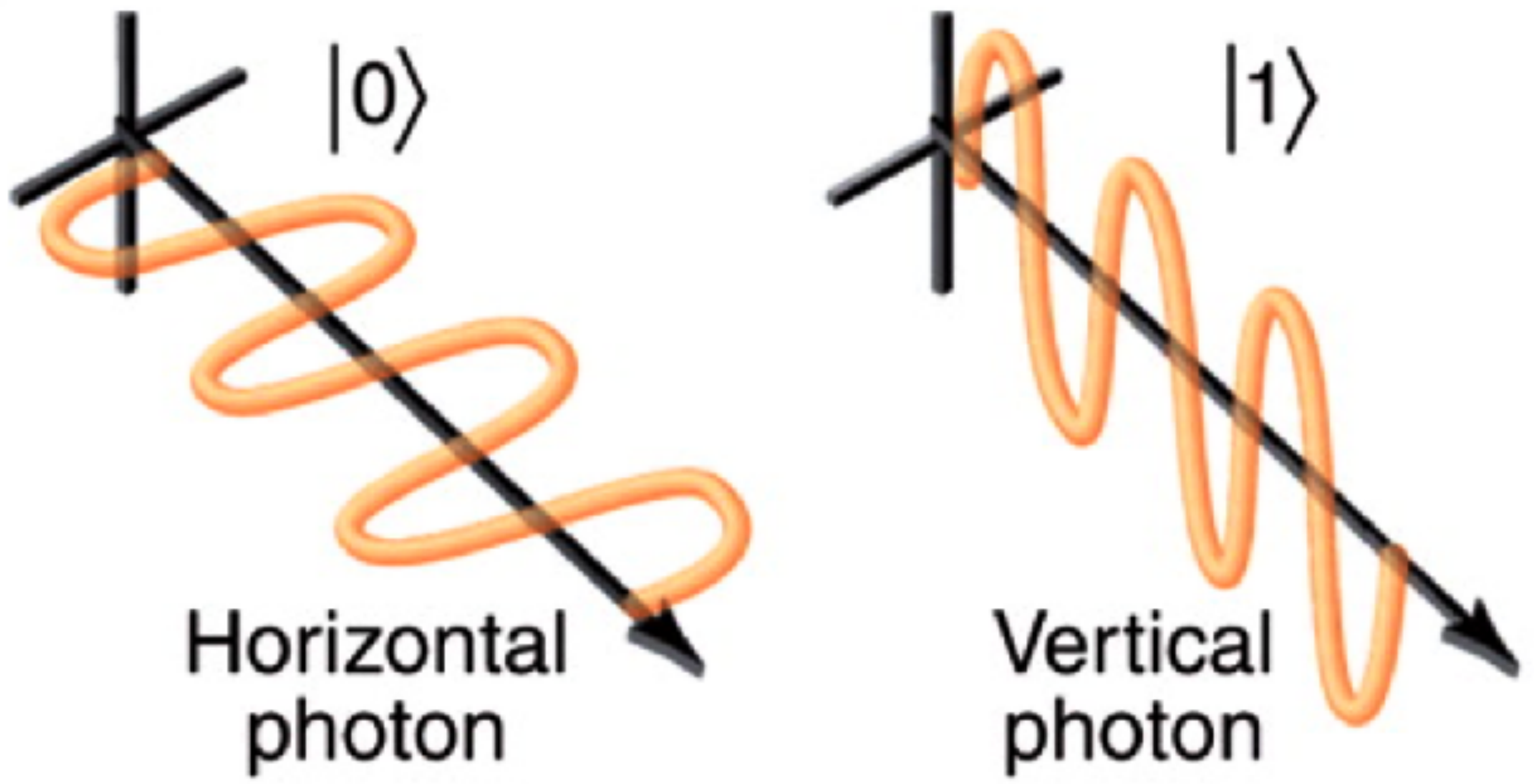


Abstraction: Qubit

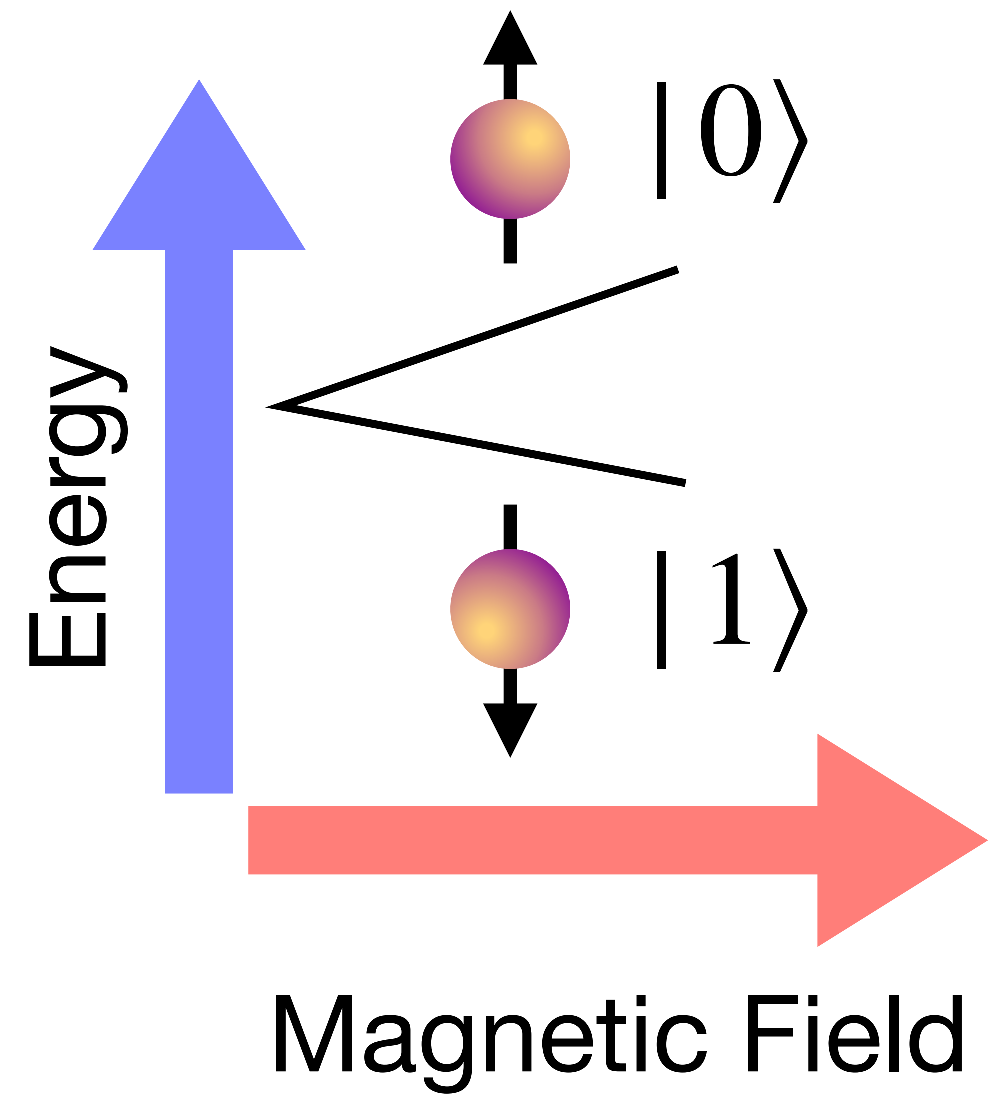
- Bit vs Qubit: Qubit is a unit of quantum information.
- Usually a two level quantum system
- Examples:



Quantum Computation and Quantum Information (2000)



Optical Quantum Computing, Science, **318,** 1567-1570 (2007)

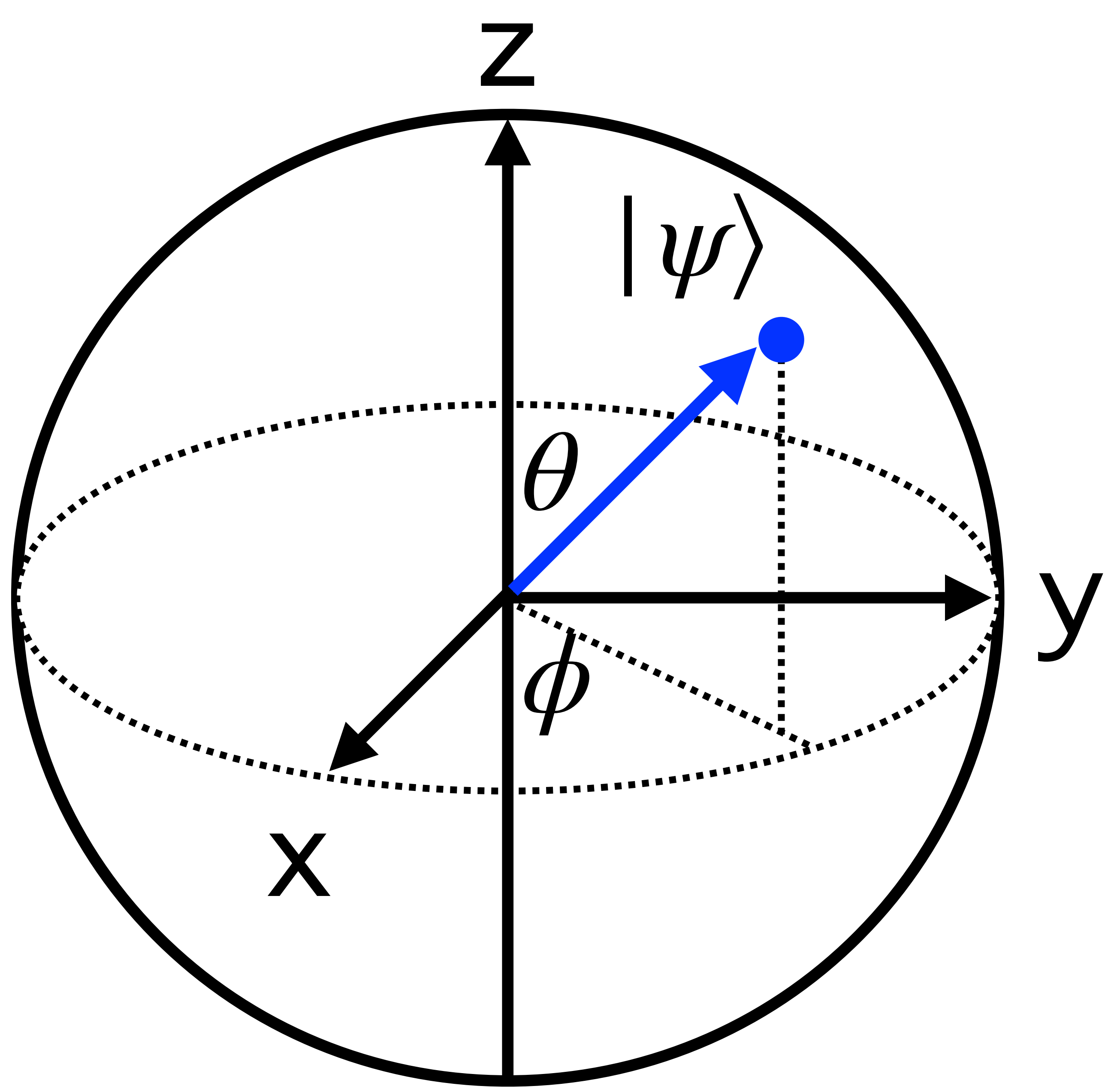


Bloch Sphere Representation

- For a single qubit, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

- Since $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$, $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$.

- The numbers θ and ϕ define a point on the unit three-dimensional sphere.



- A single qubit unitary operation can be represented as rotations on the Bloch sphere.

$$R_{\hat{n}}(\alpha) \equiv \exp\left(-i\frac{\alpha}{2}\hat{n}\cdot\vec{\sigma}\right), \quad \vec{\sigma} \in \{X, Y, Z\}$$

$$= \cos\left(\frac{\alpha}{2}\right)I - i\sin\left(\frac{\alpha}{2}\right)\hat{n}\cdot\vec{\sigma}$$

Revisit Mach-Zehnder Interferometer

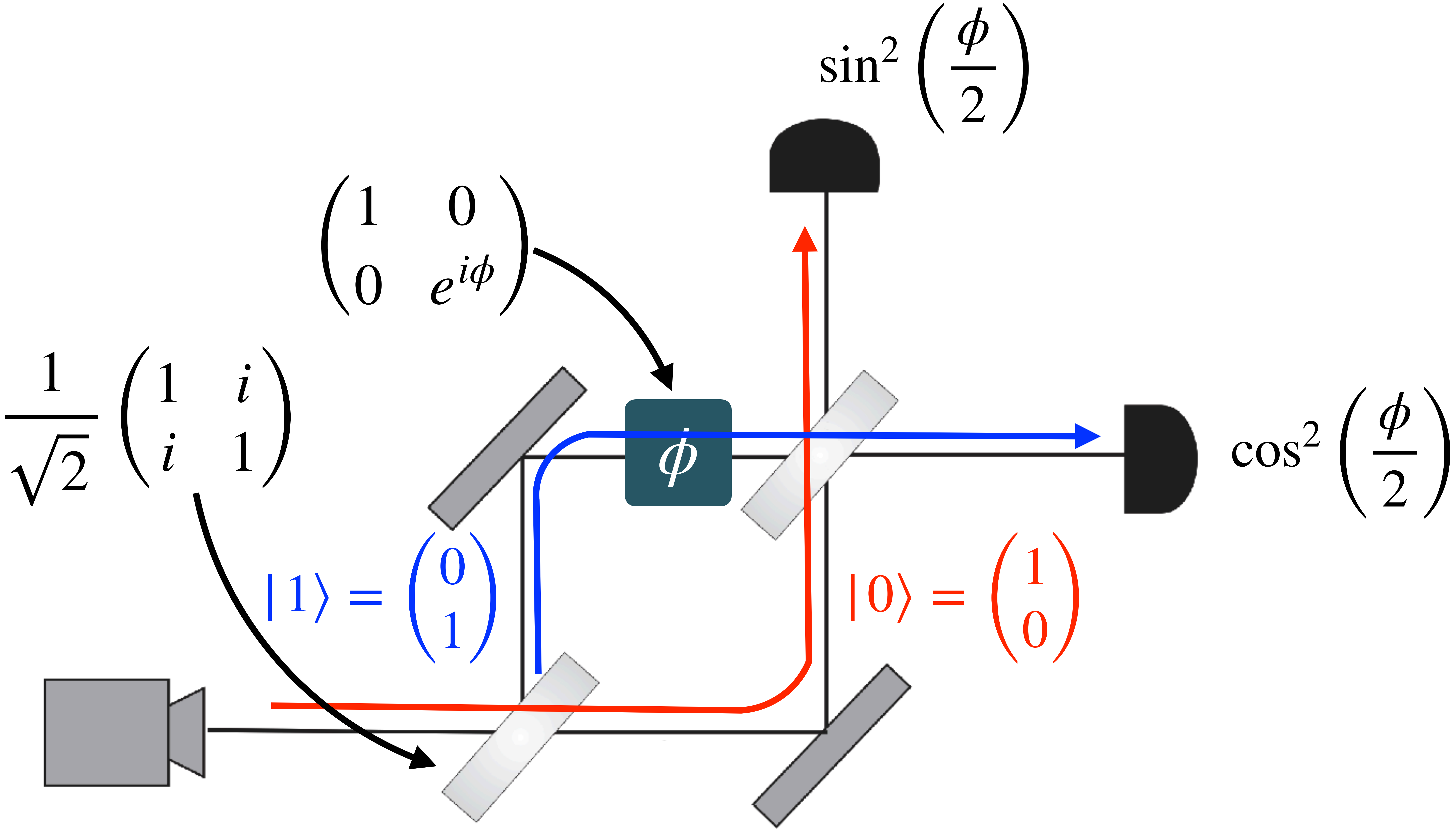


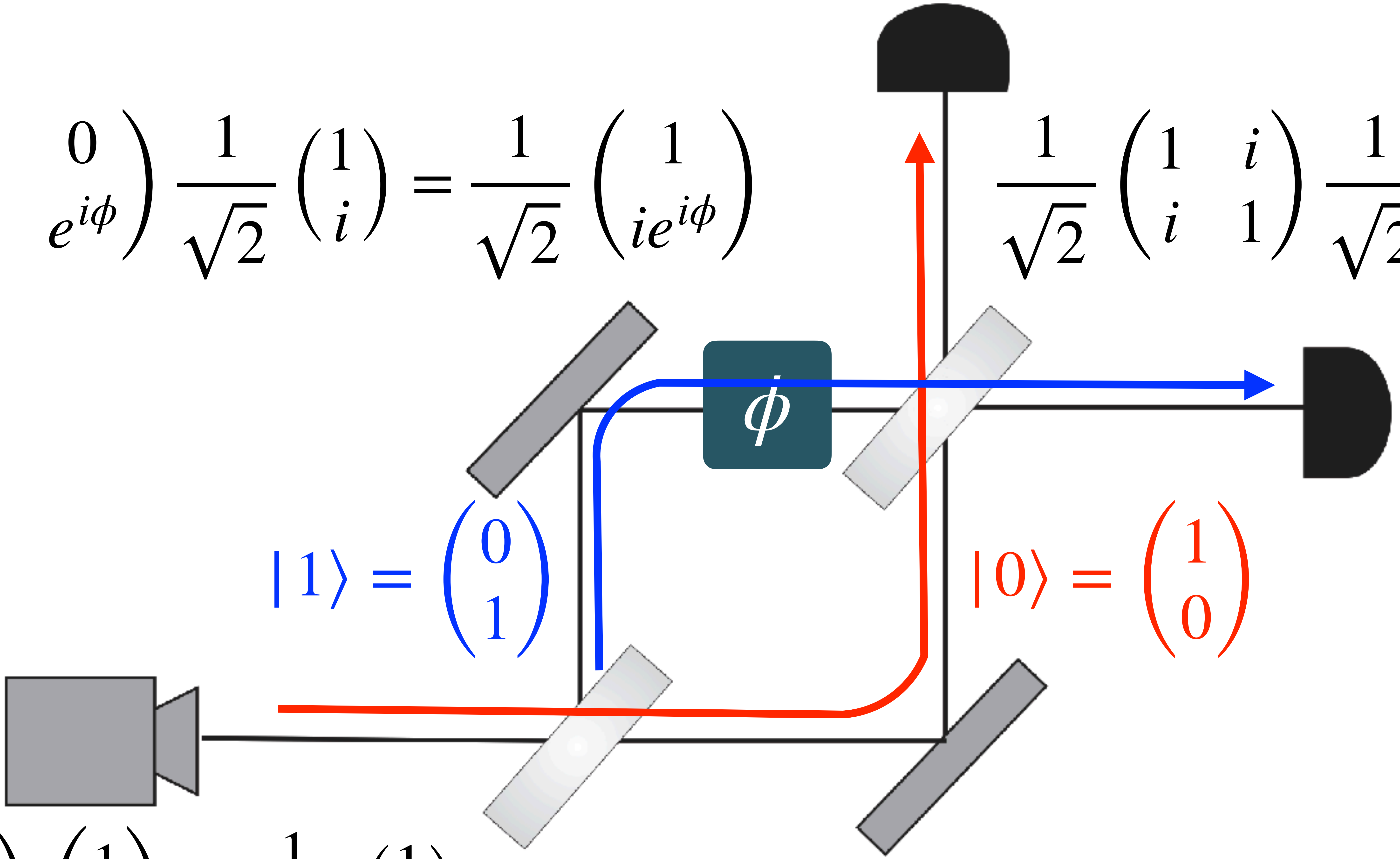
Figure from An Introduction to Quantum Computing (2007)

Revisit Mach-Zehnder Interferometer

$$\sin^2\left(\frac{\phi}{2}\right)$$

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ ie^{i\phi} \end{pmatrix}$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ ie^{i\phi} \end{pmatrix} = ie^{i\frac{\phi}{2}} \begin{pmatrix} -\sin\left(\frac{\phi}{2}\right) \\ \cos\left(\frac{\phi}{2}\right) \end{pmatrix}$$



$$\cos^2\left(\frac{\phi}{2}\right)$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$$

Figure from An Introduction to Quantum Computing (2007)

Postulates of QM: Composite System

The state space of a composite physical system is the tensor product space $\mathscr{H}_1 \otimes \ldots \otimes \mathscr{H}_n$ of the state spaces of the component subsystems $\mathscr{H}_1, \ldots, \mathscr{H}_n$.

<u>Example</u>: $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle \qquad |\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$

Concatenate:

$$\alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle = \begin{pmatrix} \alpha_1\alpha_2 \\ \alpha_1\beta_2 \\ \beta_1\alpha_2 \\ \beta_1\beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \\ \beta_1 \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}$$

$$|\psi_1\rangle \otimes |\psi_2\rangle = \left(\alpha_1|0\rangle + \beta_1|1\rangle\right) \otimes \left(\alpha_2|0\rangle + \beta_2|1\rangle\right)$$

Entanglement

- Some composite quantum states cannot be written in the product form, i.e. $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_m\rangle$

Example: $|\Phi_{00}\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$ cannot written as $|\psi_1\rangle \otimes |\psi_2\rangle$

- A quantum state that can be written in the product form is separable.
- A quantum state that is not separable is entangled.
- Entanglement describes correlations between quantum systems that cannot be described with classical physics.

Composite system: Measurement

General two-qubit state: $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, $\sum |\alpha_{ij}|^2 = 1$

If we measure both bits, we get $|ij\rangle$ with probability $|\alpha_{ij}|^2$.

What if we just measure one of them, e.g. the first qubit?

Rewrite: $$\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}\,|0\rangle\left(\frac{\alpha_{00}|0\rangle + \alpha_{01}|1\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}\right) + \sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}\,|1\rangle\left(\frac{\alpha_{10}|0\rangle + \alpha_{11}|1\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}\right)$$

What if we just throw away one of them, e.g. the first qubit?

Probabilistic mixture of states ➞ Mixed State

Example: $|\Phi_{00}\rangle = \dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$

Throwing away one qubit leaves the other in a completely random state

Comparison to Classical Deterministic Bits

- The values of a two-state system are labeled with 0 or 1
- n two-state systems have 2^n possible values, labeled with binary strings. For example, $n = 3$: 000, 001, 010, 011, 100, 101, 110, 111.
- More redundant representation:

$$\underbrace{000\ldots0}_{n} = \left.\begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right\} 2^n \quad 000\ldots1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \ldots \quad 11\ldots10 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix} \quad 11\ldots11 = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

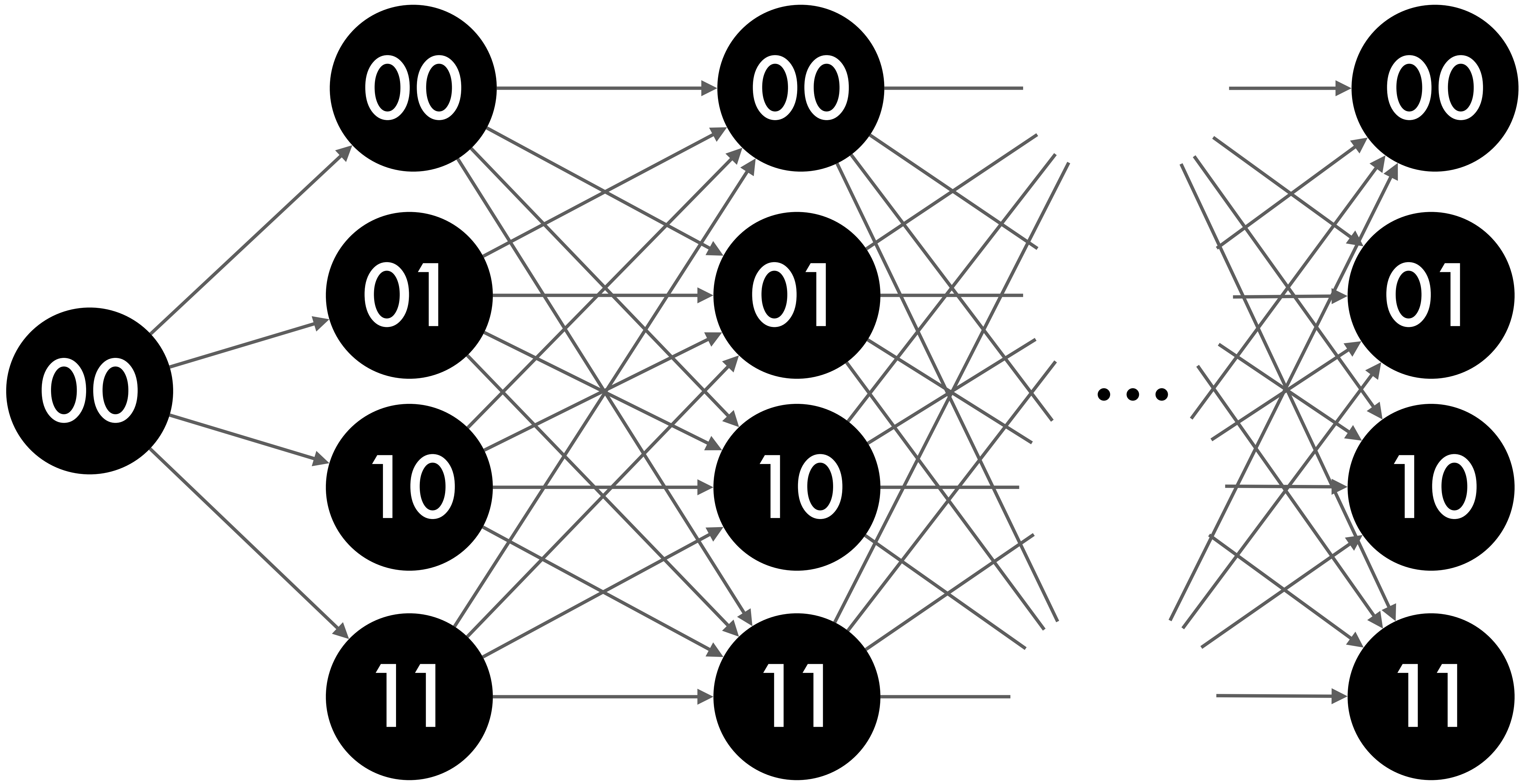
Comparison to Classical Probabilistic Bits

<u>Example</u>: 2 bits

1st bit: $\begin{pmatrix} \Pr(0) \\ \Pr(1) \end{pmatrix} = \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$

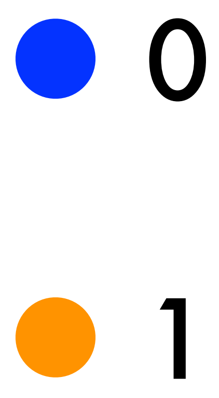
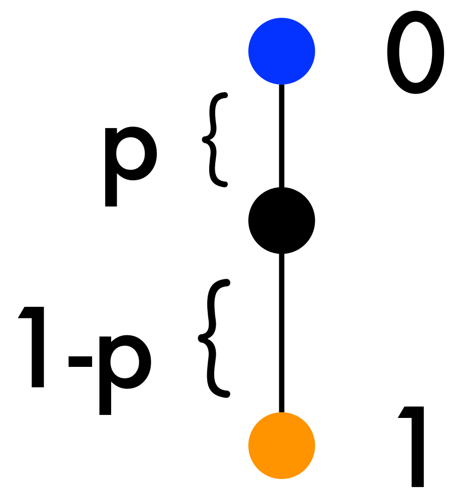
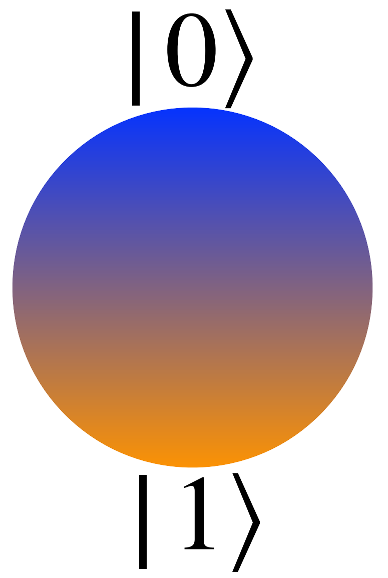
2nd bit: $\begin{pmatrix} \Pr(0) \\ \Pr(1) \end{pmatrix} = \begin{pmatrix} q_0 \\ q_1 \end{pmatrix}$

$$\begin{pmatrix} \Pr(00) \\ \Pr(01) \\ \Pr(10) \\ \Pr(11) \end{pmatrix} = \begin{pmatrix} p_0 q_0 \\ p_0 q_1 \\ p_1 q_0 \\ p_1 q_1 \end{pmatrix} = \begin{pmatrix} p_0 \\ p_1 \end{pmatrix} \otimes \begin{pmatrix} q_0 \\ q_1 \end{pmatrix}$$



$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \longrightarrow \begin{pmatrix} p_{1,00} \\ p_{1,01} \\ p_{1,10} \\ p_{1,11} \end{pmatrix} \longrightarrow \begin{pmatrix} p_{2,00} \\ p_{2,01} \\ p_{2,10} \\ p_{2,11} \end{pmatrix} \longrightarrow \cdots \longrightarrow \begin{pmatrix} p_{k,00} \\ p_{k,01} \\ p_{k,10} \\ p_{k,11} \end{pmatrix}$$

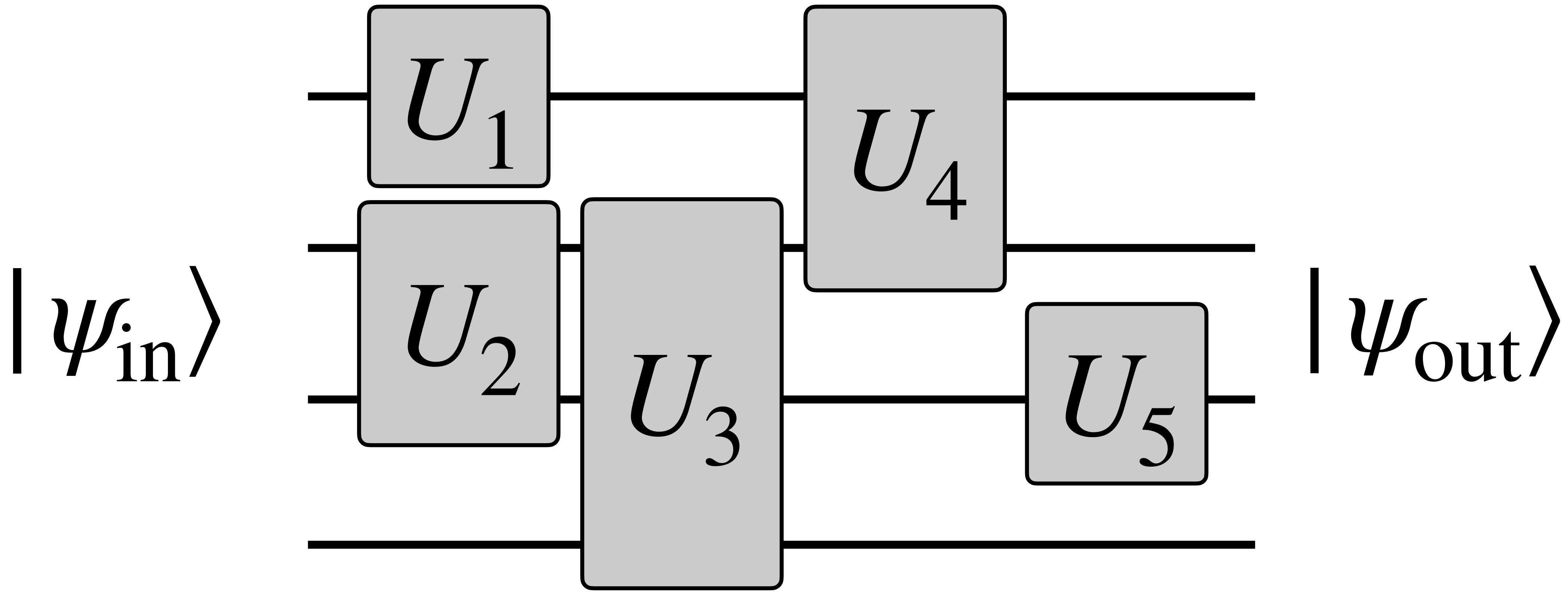
Summary: Bit, Pbit, Qubit

	bit	probabilistic bit	quantum bit
Pictorial Representation			
Vector Representation	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} p \\ 1-p \end{pmatrix}, p \in \mathbb{R}_+$	$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \alpha, \beta \in \mathbb{C}$
Observation	0	$\Pr(0) = p$ $\Pr(1) = 1-p$	$\Pr(0) = \|\alpha\|^2$ $\Pr(1) = \|\beta\|^2$
Evolution	Deterministic	Stochastic	Unitary

Quantum mechanics: a mathematical generalization of the probability theory

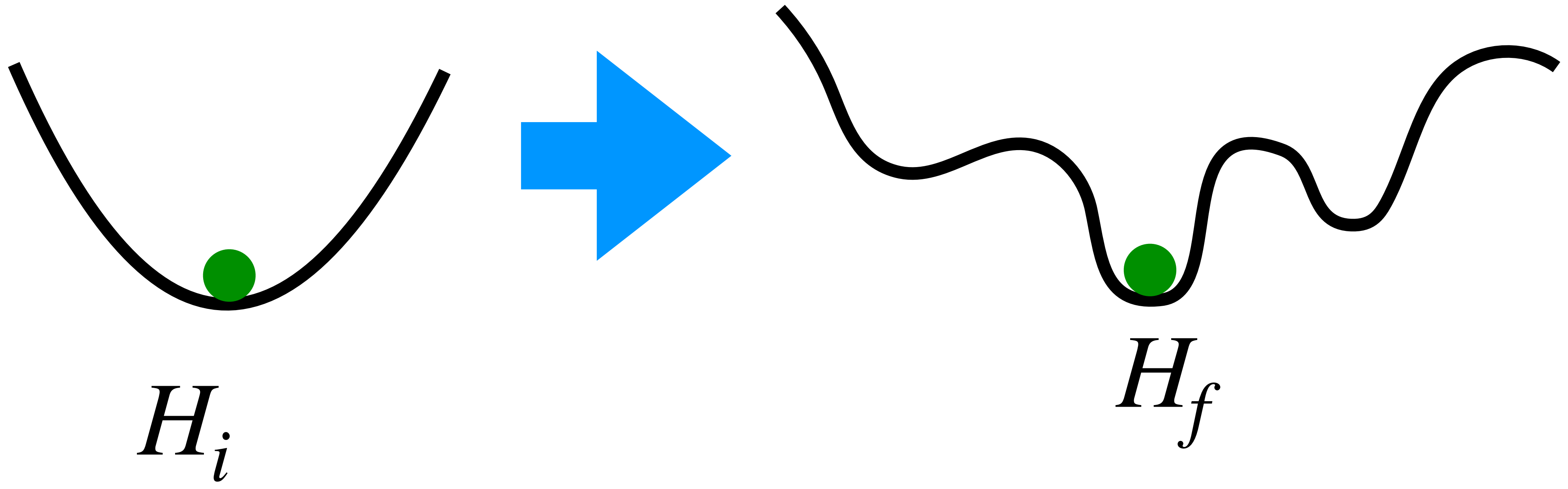
Example Models of Quantum Computing

Circuit-based QC

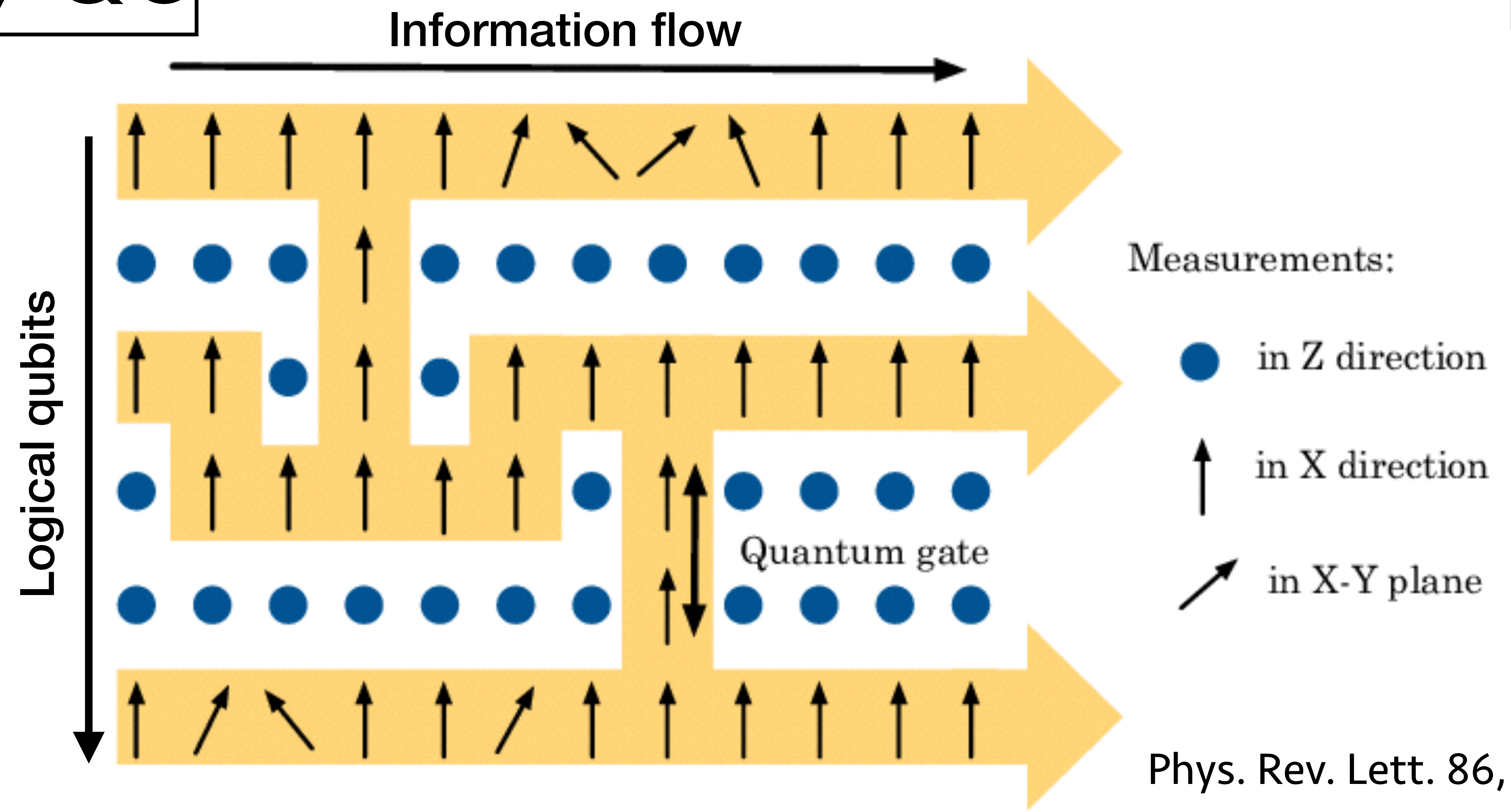


Adiabatic QC

$$H(t) = (1-t)H_i + tH_f$$

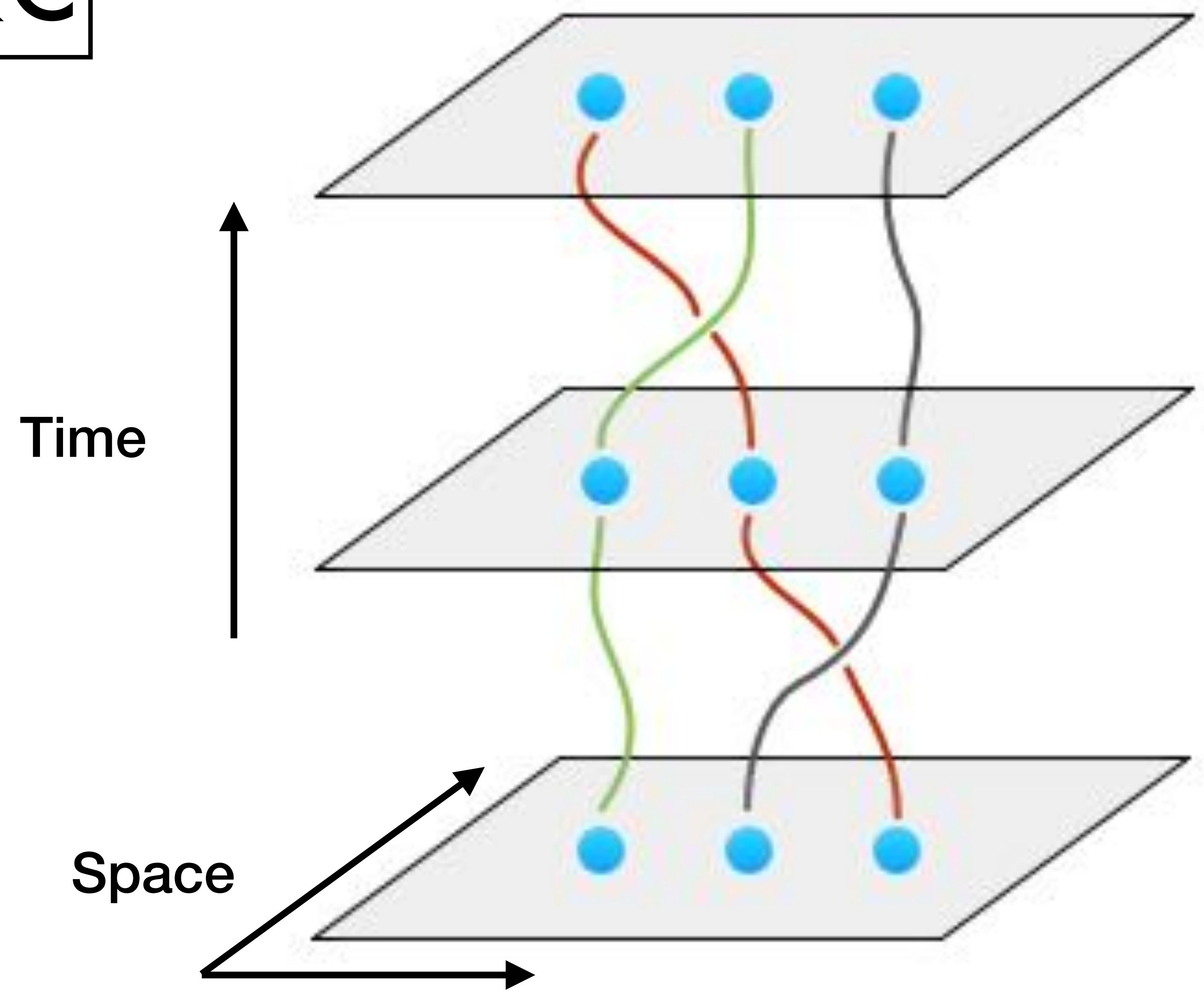


1-way QC



Phys. Rev. Lett. 86, 5188 (2001)

Topological QC

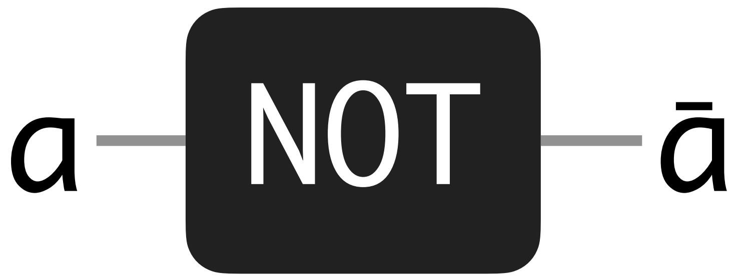


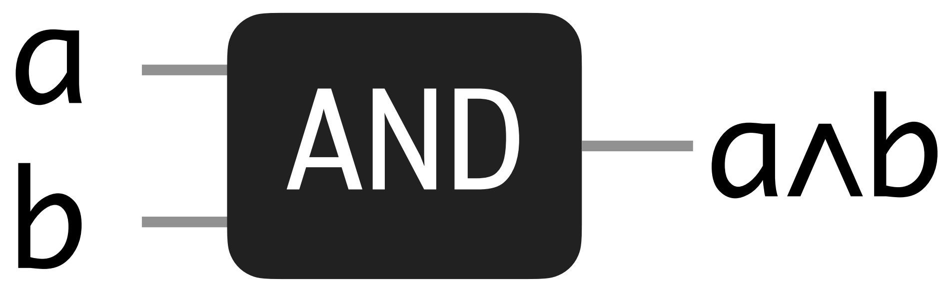
II. Quantum Circuit

Classical Circuits

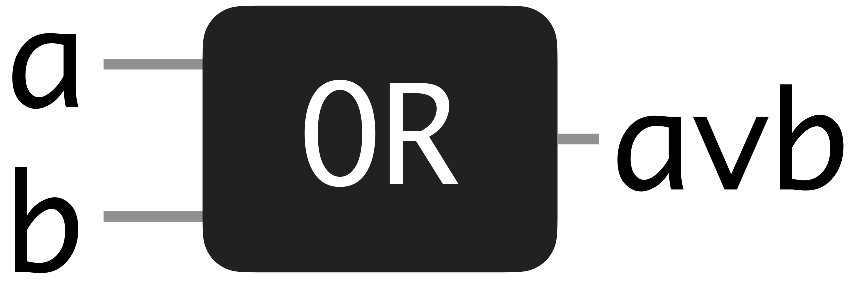
- Circuit model is a useful model for describing transformations on data in terms of basic operations called gates.
- An easy way to formalize the notion of computational efficiency
- Closely tied to the physical implementation of a computation.

<u>Examples</u>:

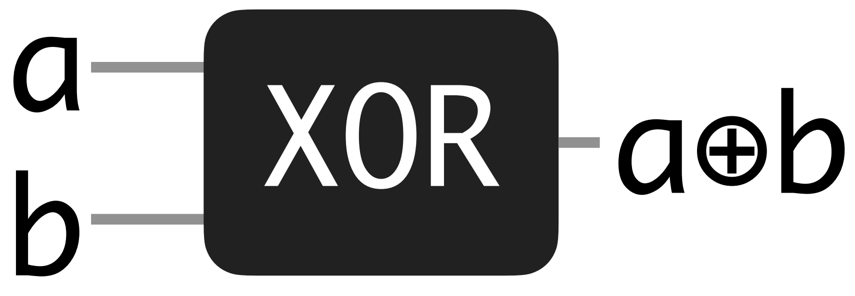


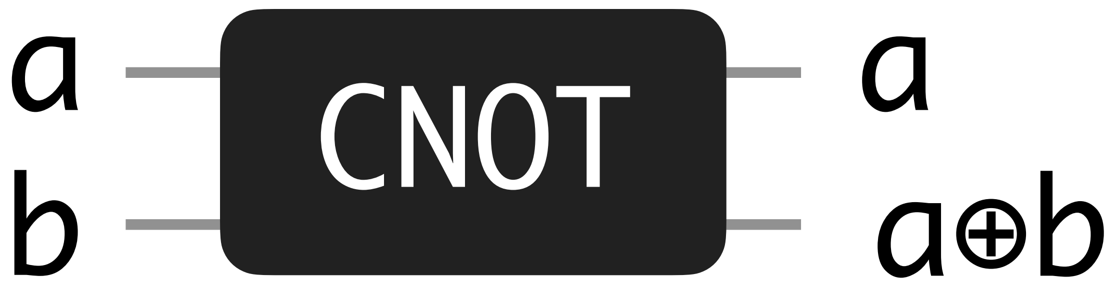


a	b	avb
0	0	0
0	1	1
1	0	1
1	1	1



a	b	a∧b
0	0	0
0	1	0
1	0	0
1	1	1

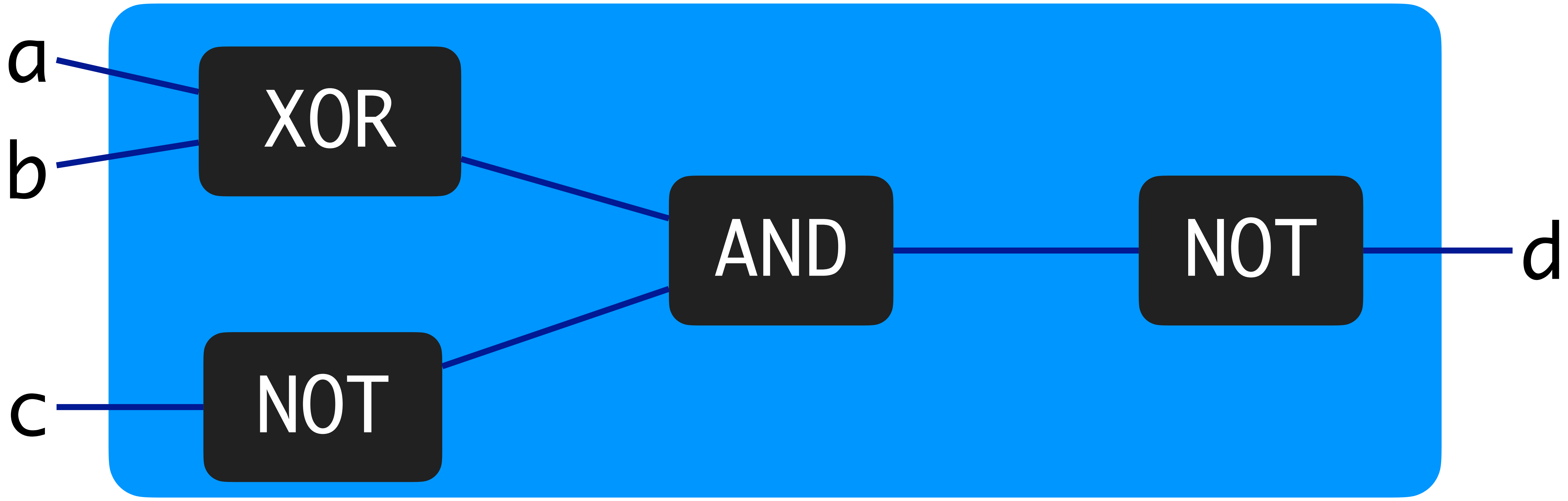




Classical Circuits & Universality

- Gates are glued together to make circuits (arrays of gates), which compute Boolean functions

$x \in \{0,1\}^3$

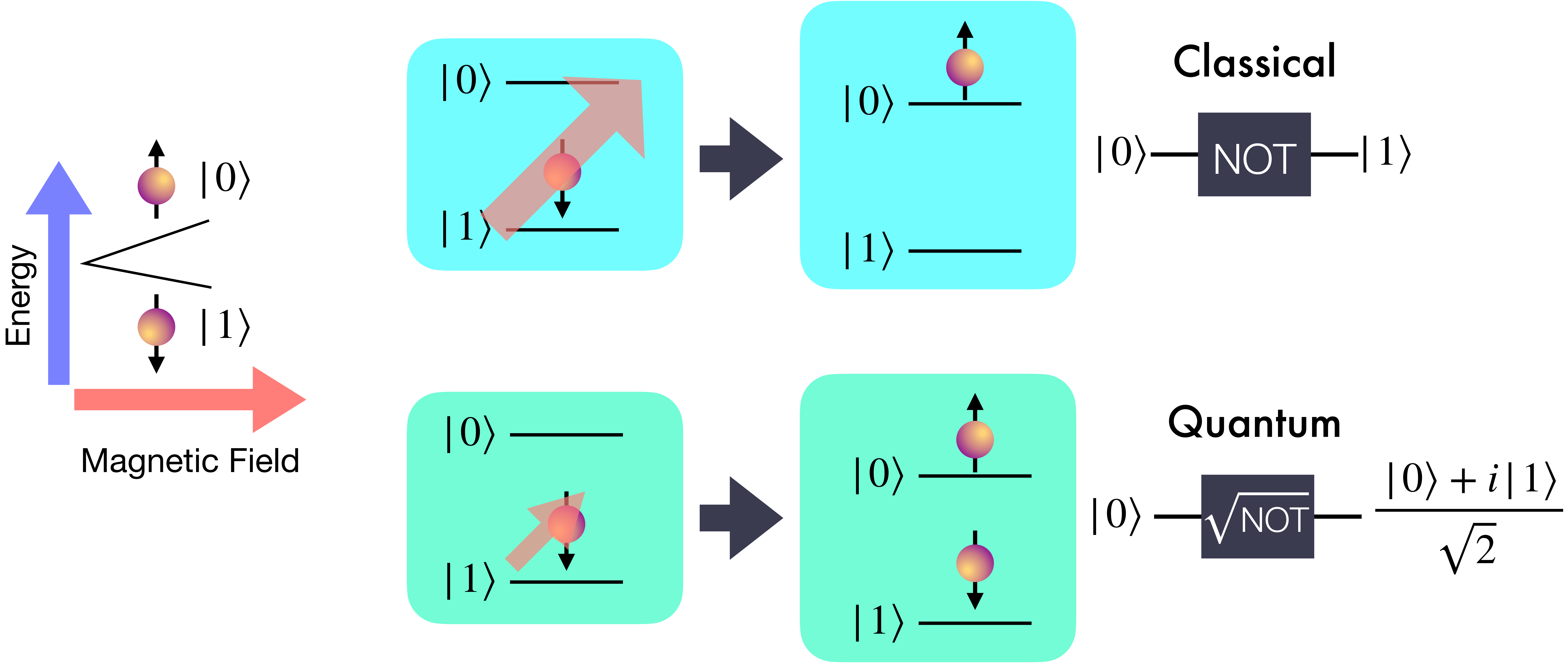


$f(x) \in \{0,1\}$

- A set of gates is universal for classical computation, if for any Boolean function f, a circuit can be constructed for computing f using only gates from that set.

- NAND, FANOUT is universal

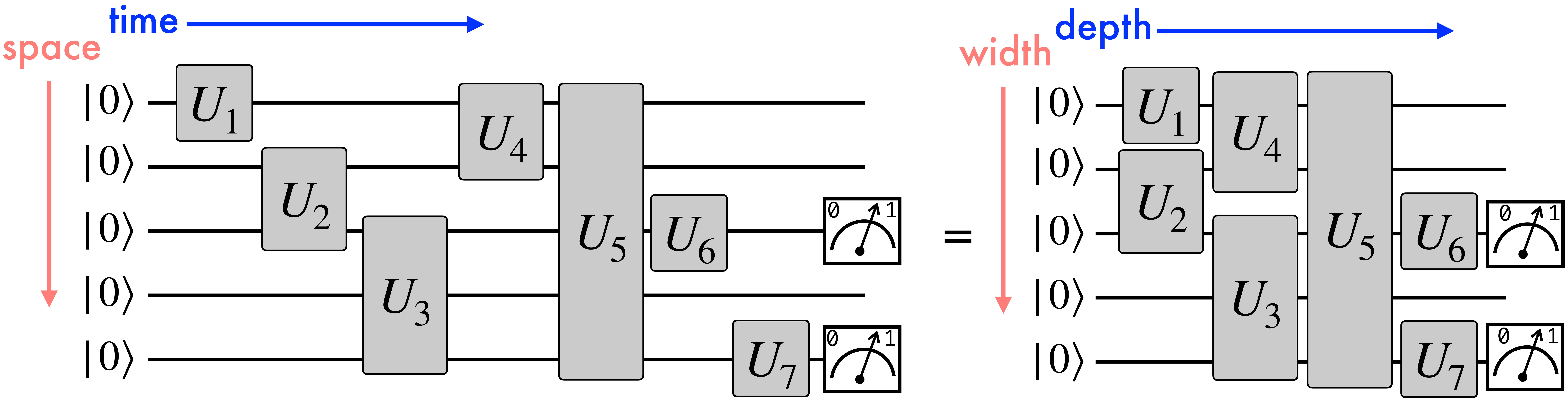
Classical gate vs Quantum gate



Elements of Quantum Circuit

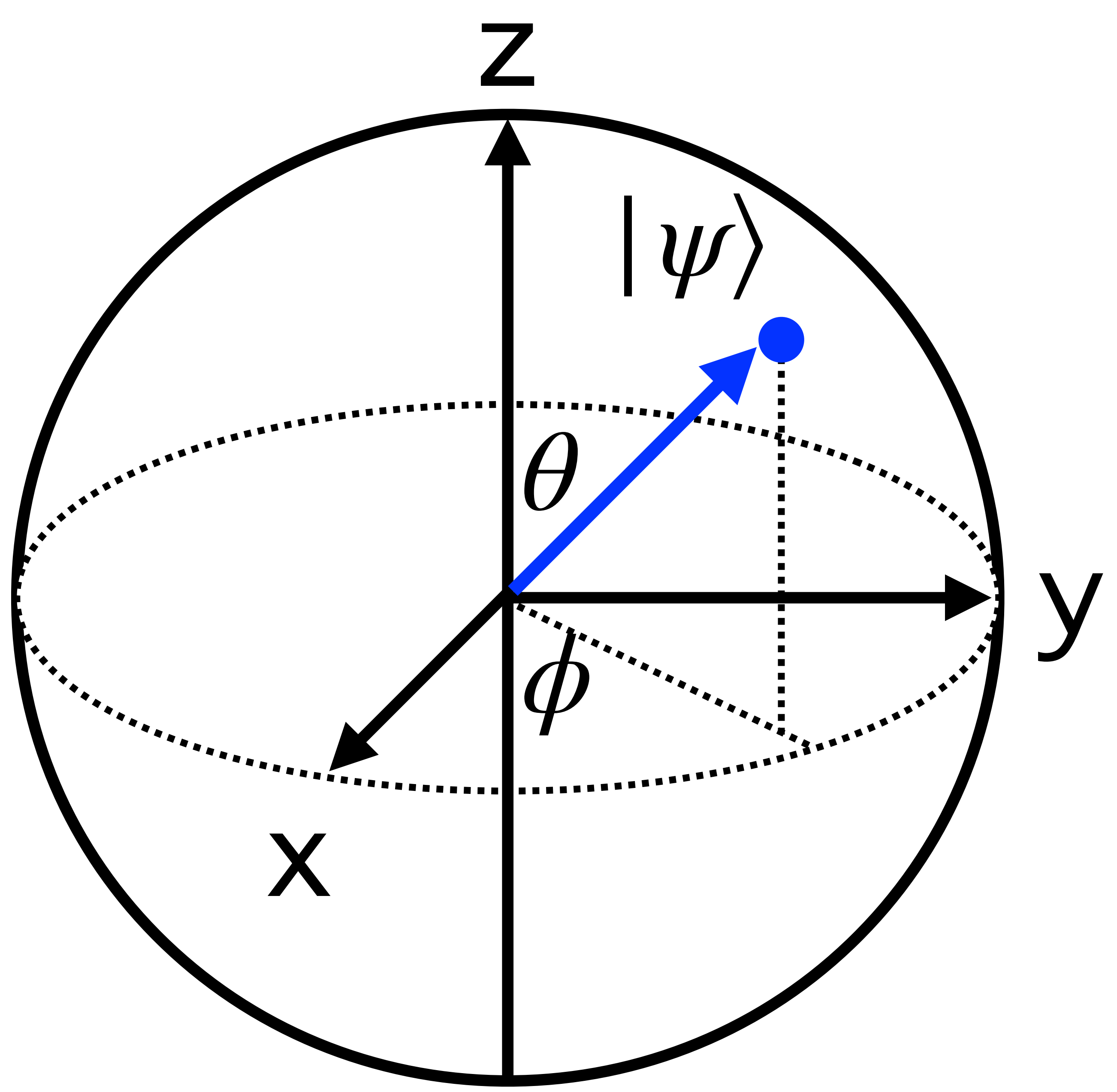
Preparation → Dynamics → Measurement

- Quantum circuit: a reversible acyclic circuit of quantum gates



Bloch Sphere Representation for 1-Qubit Gate

- For a single qubit, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
- Since $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$, $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$.
- The numbers θ and ϕ define a point on the unit three-dimensional sphere.



- A single qubit unitary operation can be represented as rotations on the Bloch sphere.

$$R_{\hat{n}}(\alpha) \equiv \exp\left(-i\frac{\alpha}{2}\hat{n}\cdot\vec{\sigma}\right), \quad \vec{\sigma} \in \{X, Y, Z\}$$

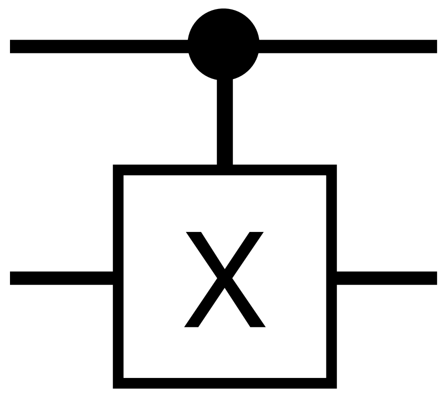
$$= \cos\left(\frac{\alpha}{2}\right)I - i\sin\left(\frac{\alpha}{2}\right)\hat{n}\cdot\vec{\sigma}$$

Two Qubit Entangling Gates

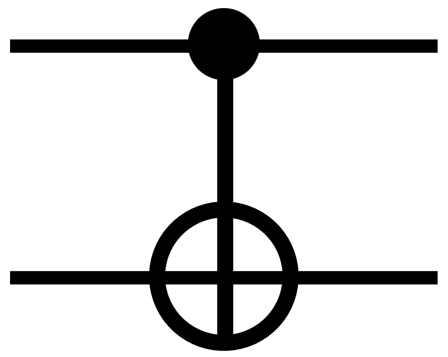
- Must be able to transform $|\psi_1\rangle \otimes |\psi_2\rangle \rightarrow |\Psi_{12}\rangle$, where $|\Psi_{12}\rangle$ is entangled
- What about $\left(U_1 \otimes U_2\right)|\psi_1\rangle \otimes |\psi_2\rangle$?
- By linearity, $\left(U_1 \otimes U_2\right)|\psi_1\rangle \otimes |\psi_2\rangle = (U_1|\psi_1\rangle) \otimes (U_2|\psi_2\rangle)$: Remains separable.
- Entangling gate examples:

  $CX = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$, $CZ = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$

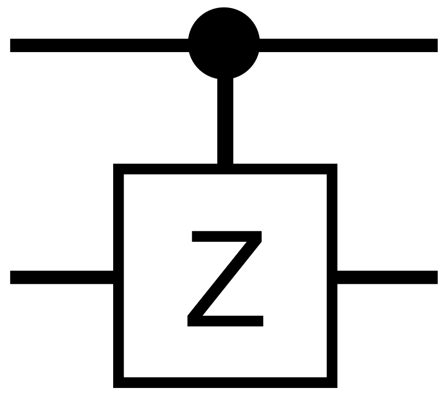
$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} =$$



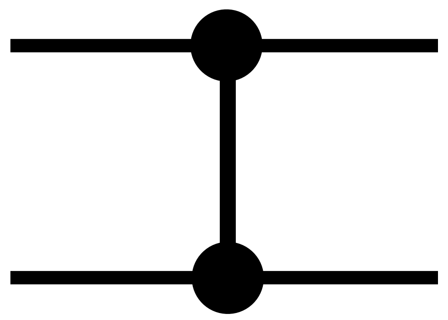
=



$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} =$$



=



Universal Set of Quantum Gates

A set of gates G is said to be universal if any n-qubit unitary operator can be approximated to arbitrary accuracy by a quantum circuit using only gates from G.

- A set composed of any two-qubit entangling gate, together with all one-qubit gates, is universal
- This is a bit of an overkill: Good approximation suffices.
- Need access to an infinite number of single-qubit gates.

Universal Set of Quantum Gates

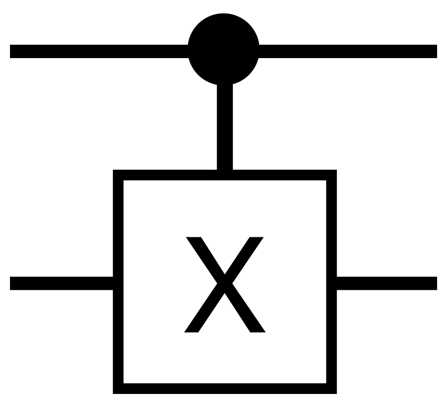
A set of gates G is said to be universal if any n-qubit unitary operator can be approximated to arbitrary accuracy by a quantum circuit using only gates from G.

- Can we achieve universality with a finite set of gates?

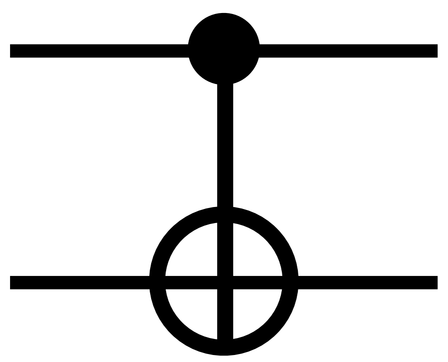
➡ YES: For any number of qubits, $G = \{H, T, CX\}$ is a universal set of gates.

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

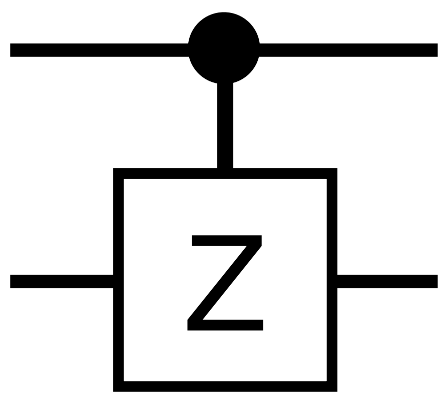
$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$ =



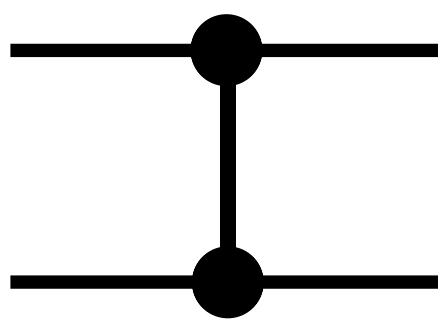
=



$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$ =



=



No Cloning

- Is it possible to copy an unknown quantum state?
- The answer is...NO! (due to the linearity of QM)

If copying is possible, then $U_{copy}|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$

Let $|\psi\rangle = \alpha|\phi_1\rangle + \beta|\phi_2\rangle \Rightarrow U_{copy}|\psi\rangle|0\rangle = \alpha U_{copy}|\phi_1\rangle|0\rangle + \beta U_{copy}|\phi_2\rangle|0\rangle$

$$= \alpha|\phi_1\rangle|\phi_1\rangle + \beta|\phi_2\rangle|\phi_2\rangle \neq |\psi\rangle|\psi\rangle$$

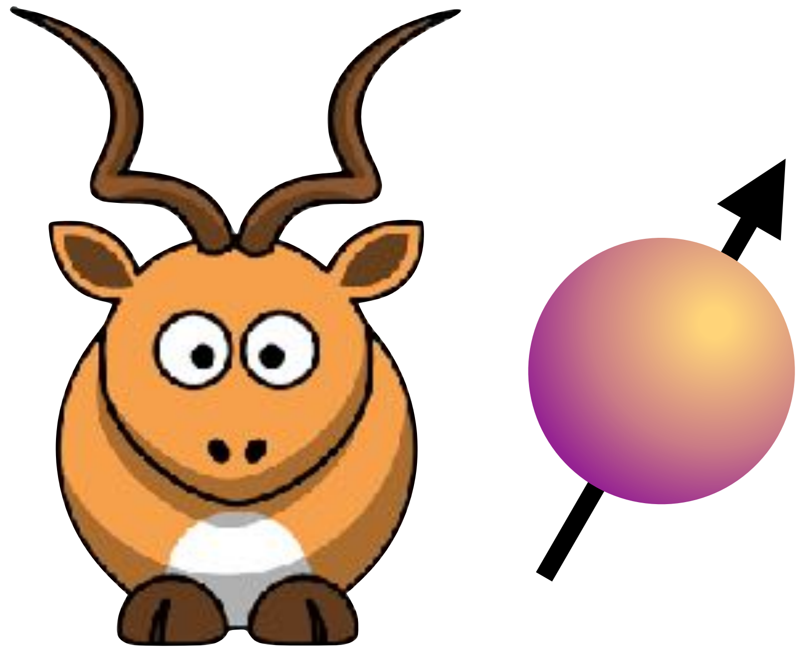
Important in quantum communication, quantum cryptography, quantum error correction, etc.!

Elementary Q. Protocol: Superdense Coding

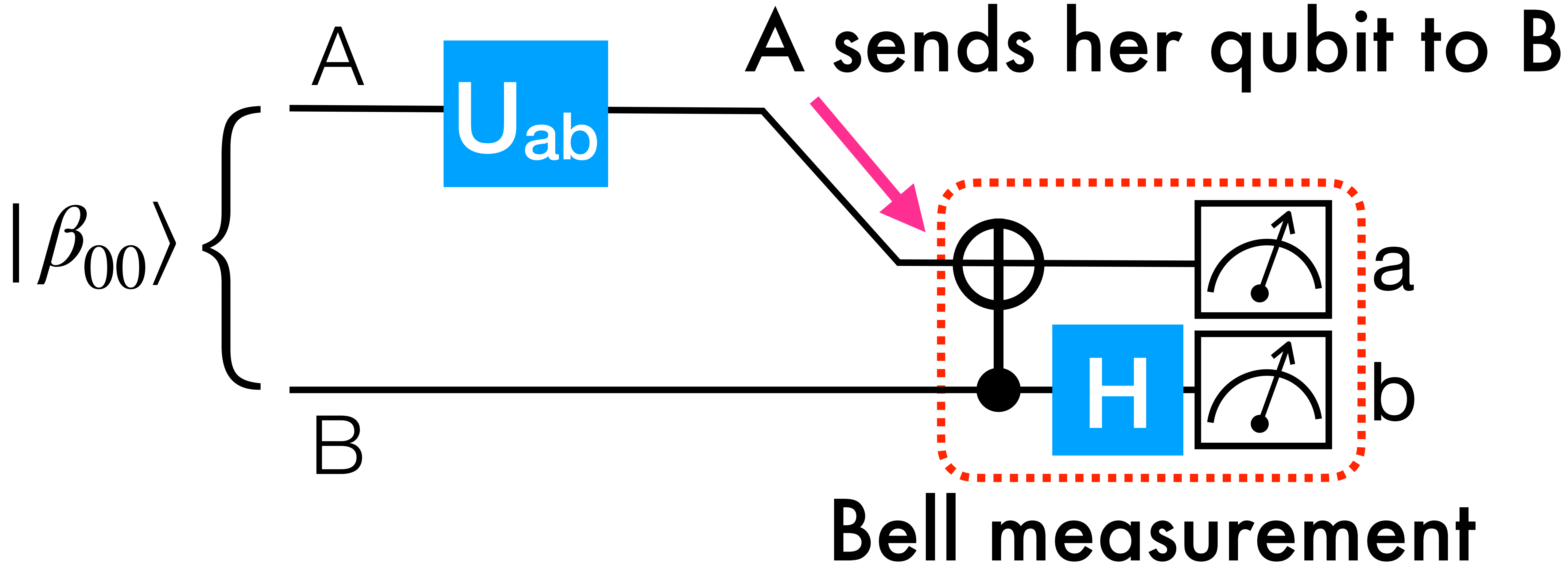
- How many classical bits of information can be sent with a qubit?
- By sending a qubit in $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, only one classical bit of information can be transmitted due to the quantum measurement postulate & no cloning theorem.
- Entanglement allows for 2 classical bits of information to be sent by sending only 1 qubit!

Elementary Q. Protocol: Superdense Coding

- Entanglement allows for 2 classical bits of information to be sent by sending only 1 qubit!



$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$



U_{ab}	B receives	B measures
I	$(\|00\rangle + \|11\rangle)/\sqrt{2}$	00
X	$(\|01\rangle + \|10\rangle)/\sqrt{2}$	01
Z	$(\|00\rangle - \|11\rangle)/\sqrt{2}$	10
ZX	$(\|01\rangle - \|10\rangle)/\sqrt{2}$	11

Elementary Q. Protocol: Quantum Teleportation

- How many classical bits should be sent in order to communicate the state of a qubit, i.e., $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$?

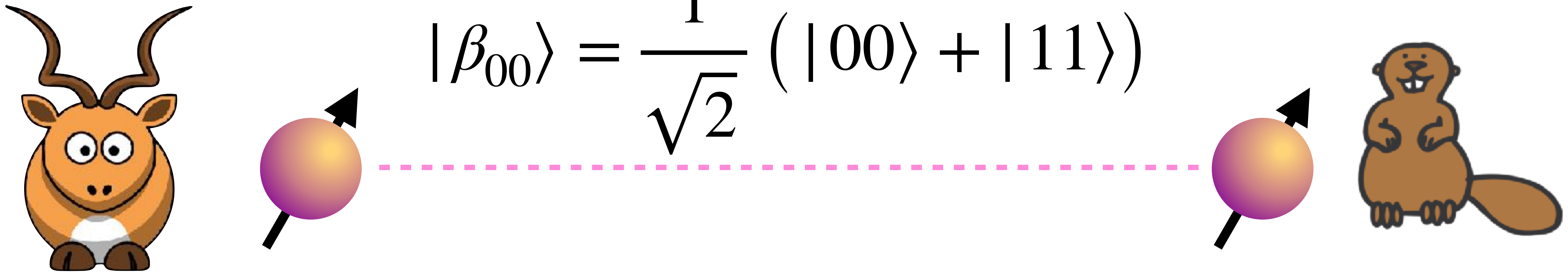
- At first glance, since $\alpha, \beta \in \mathbb{C}$ it seems that infinitely many bits are required.

- Entanglement allows for a quantum state to be sent by sending only 2 classical bits of information!

Elementary Q. Protocol: Quantum Teleportation

- Entanglement allows for a quantum state to be sent by sending only 2 classical bits of information!

$$|\psi\rangle$$



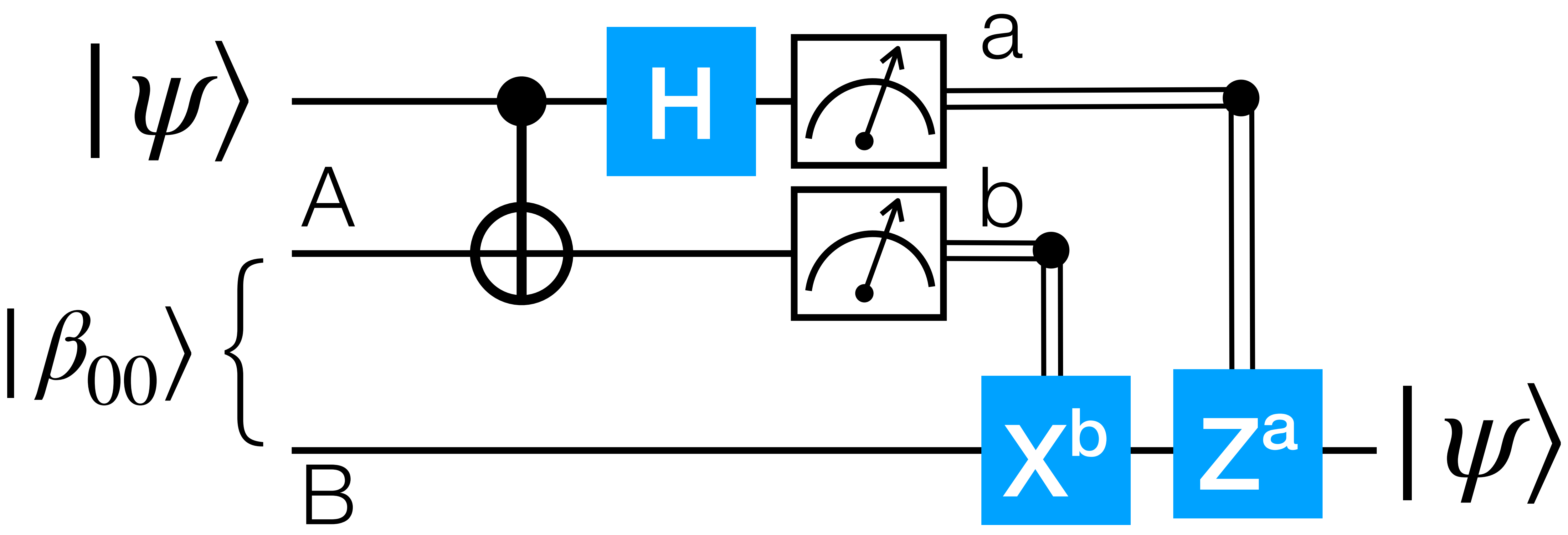
$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\psi\rangle|\beta_{00}\rangle = \left(|\beta_{00}\rangle|\psi\rangle + |\beta_{01}\rangle X|\psi\rangle + |\beta_{10}\rangle Z|\psi\rangle + |\beta_{11}\rangle XZ|\psi\rangle\right)/2$$

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$



Summary

- **Quantum computing:**
  Mathematical generalization of the probability theory.
- **Quantum circuit:**
  Useful for describing transformations of quantum data in terms gates.
- **Universality:**
  Finite set of gates can approximate any transformation.
- **Elementary quantum protocols:**
  Quantum entanglement provides the advantage.