양자컴퓨팅 인공지능 SW 개발 전문인력 양성과정 - 기초

Day 2 : 양자알고리즘 개요

연세대학교 응용통계/통계데이터사이언스학과
박경덕 | dkd.park@yonsei.ac.kr

Course Outline

- Day 1
  - 양자 컴퓨팅 개요
  - 양자 역학 기초
  - 양자 회로 모델
  - Qiskit을 활용하는 양자 컴퓨팅 실습 기초
- Day 2
  - 양자 알고리즘 개요
  - Qiskit을 활용하는 양자 알고리즘 실습 기초
- Day 3
  - 양자 알고리즘 중급
  - Pennylane을 활용하는 양자 알고리즘 중급 실습

I. Quantum Mechanics Recap

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 qubits, we get $|ij\rangle$ with probability $\Pr(ij) = |\langle ij|\psi\rangle|^2 = |\alpha_{ij}|^2$.

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

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

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

- What about classical probabilistic algorithms?

<u>Example</u>: 2 bits

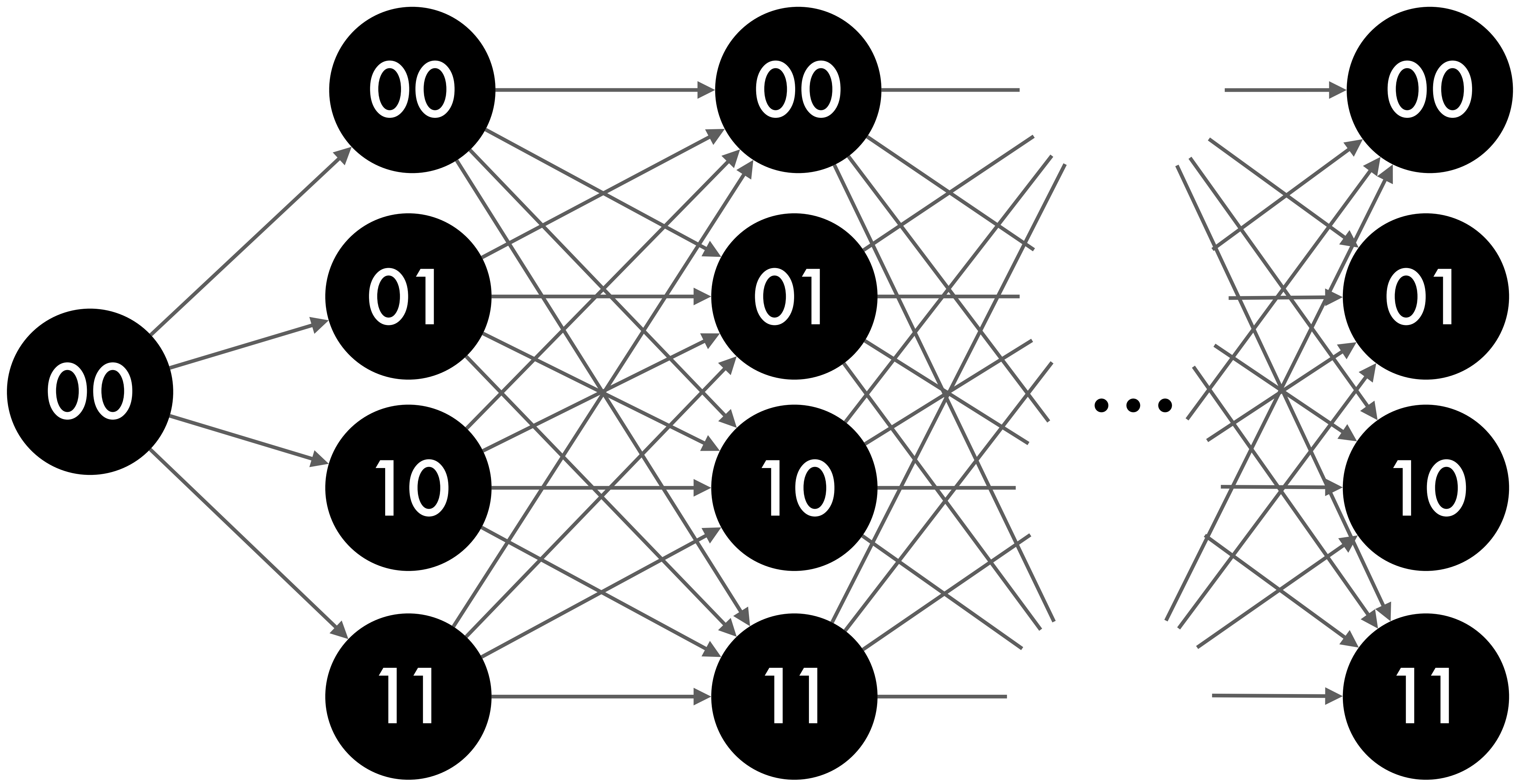
1st bit:

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

2nd bit:

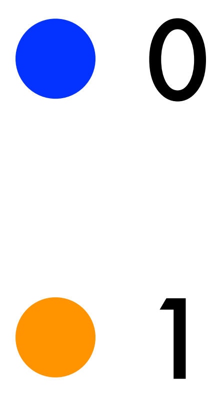
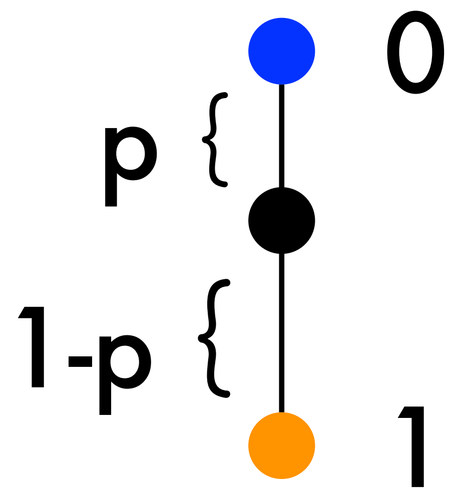
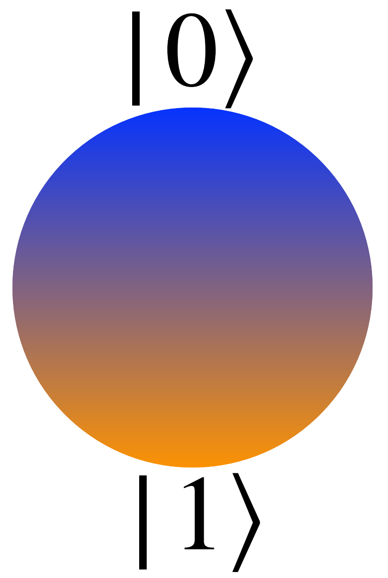
$$\begin{pmatrix} \Pr(0) \\ \Pr(1) \end{pmatrix} = \begin{pmatrix} q_0 \\ q_1 \end{pmatrix}$$

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



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

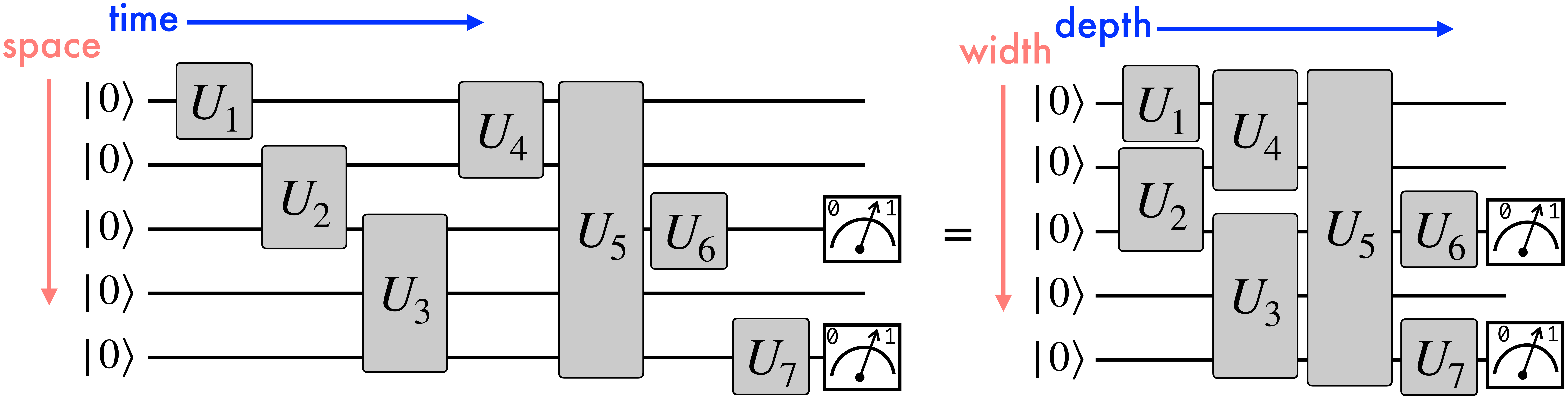
Summary: Bit, Pbit, Qubit

	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	$\Pr(0) = p$ $\Pr(1) = 1 - p$	$\Pr(0) = \vert\alpha\vert^2$ $\Pr(1) = \vert\beta\vert^2$
Evolution	Deterministic	Stochastic	Unitary

Quantum mechanics: a mathematical generalization of the probability theory

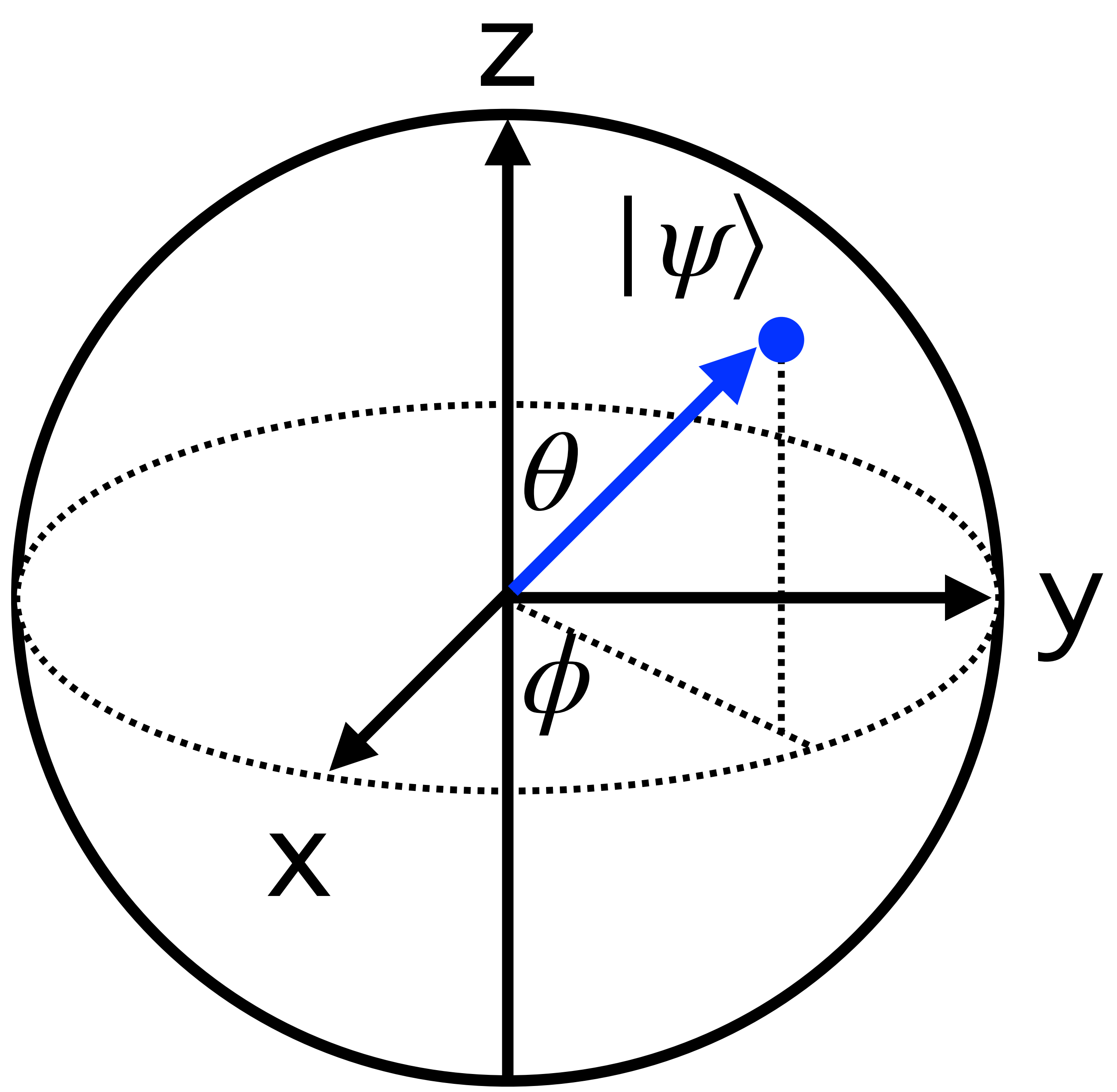
Elements of Quantum Circuit

- Quantum circuit: a reversible acyclic circuit of quantum gates



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.



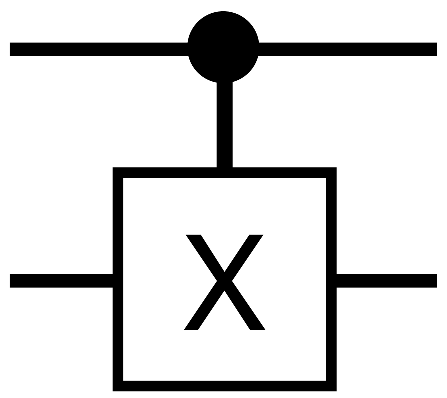
- A single qubit unitary operation can be represented as rotations on the Bloch sphere.

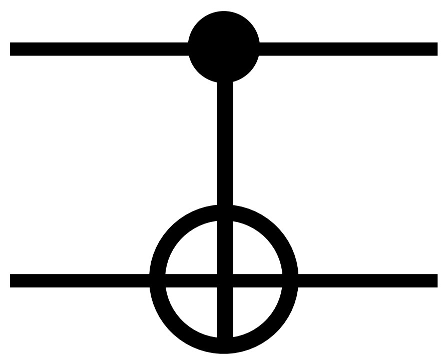
$$R_{\hat{n}}(\alpha) \equiv \exp\left(-i\frac{\alpha}{2}\hat{n}\cdot\vec{\sigma}\right), \quad \vec{\sigma} \in \{X, Y, Z\}$$

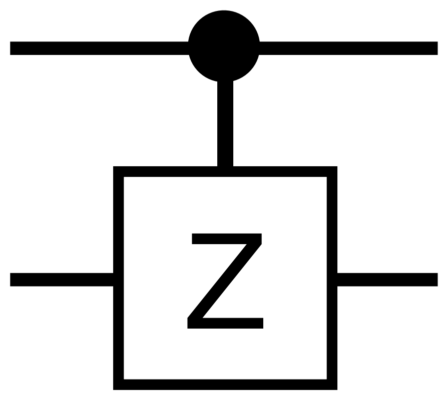
$$= \cos\left(\frac{\alpha}{2}\right)I - i\sin\left(\frac{\alpha}{2}\right)\hat{n}\cdot\vec{\sigma}$$

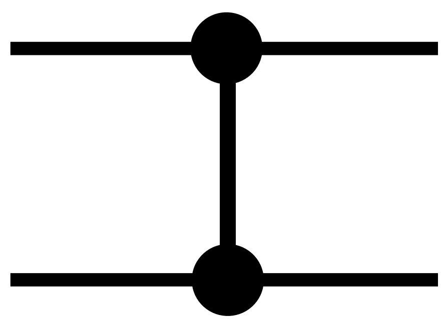
Two Qubit Entangling Gates

- 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:
  $CX = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$ & $CZ = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$

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

= 

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

= 

II. Basic Quantum Protocols

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

$$\begin{aligned} U_{copy}|\psi\rangle|0\rangle &= \alpha U_{copy}|\phi_1\rangle|0\rangle + \beta U_{copy}|\phi_2\rangle|0\rangle \\ &= \alpha|\phi_1\rangle|\phi_1\rangle + \beta|\phi_2\rangle|\phi_2\rangle \neq |\psi\rangle|\psi\rangle \end{aligned}$$

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

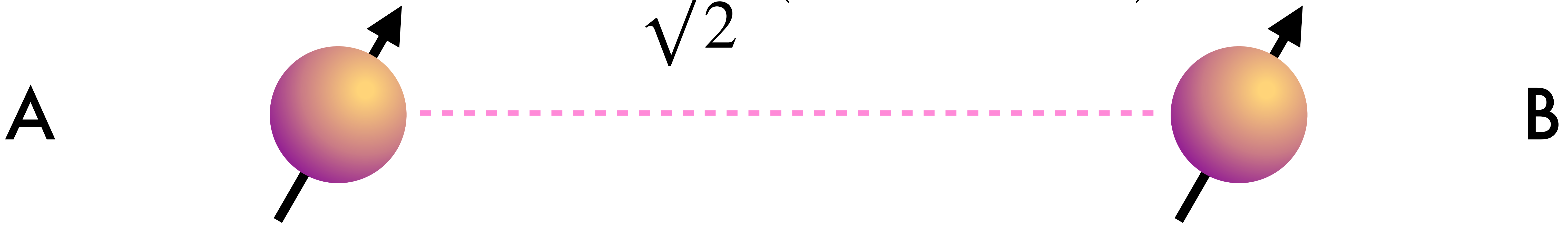
Superdense Coding

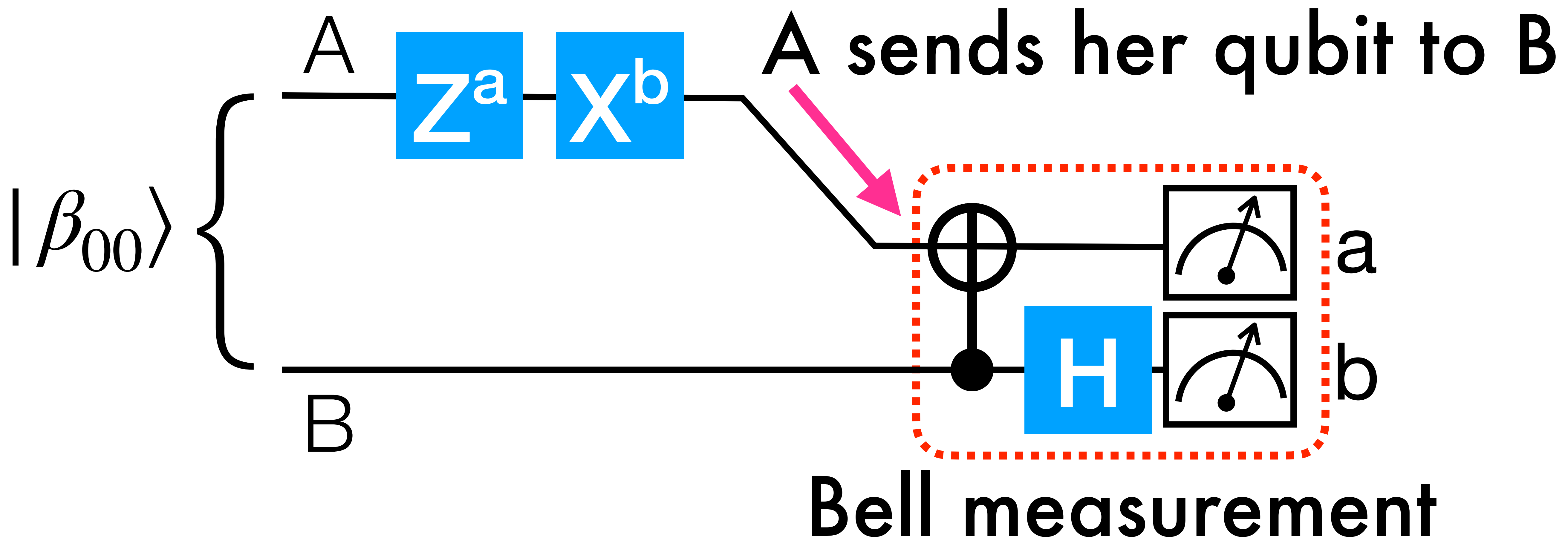
- How many classical bits of information can be sent with a qubit?
- By sending a qubit in $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, only one classical bit of information can be transmitted due to the quantum measurement postulate.
- Entanglement allows for 2 classical bits of information to be sent by sending only 1 qubit!

Superdense Coding

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

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





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

Quantum Teleportation

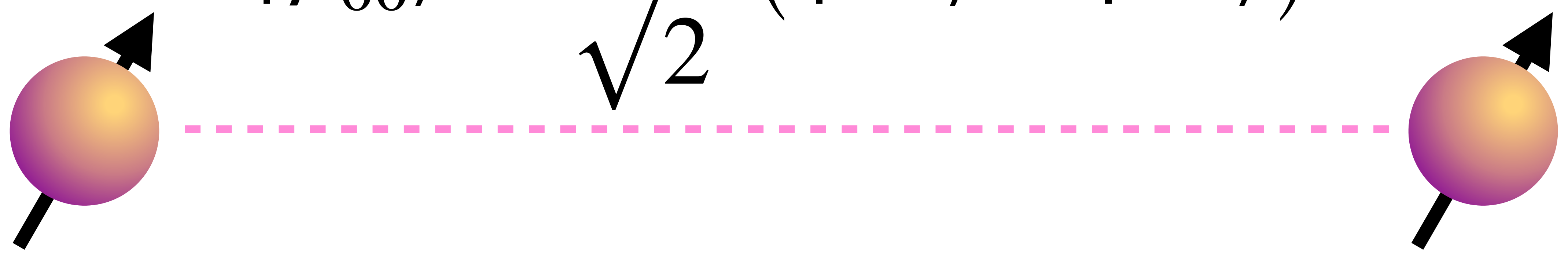
- How many classical bits should be sent in order to communicate the state of a qubit, i.e., $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$?
- At first glance, since $\alpha, \beta \in \mathbb{C}$ it seems that infinitely many bits are required.
- Entanglement allows for a quantum state to be sent by sending only 2 classical bits of information!

Quantum Teleportation

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

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

A $|\psi\rangle$



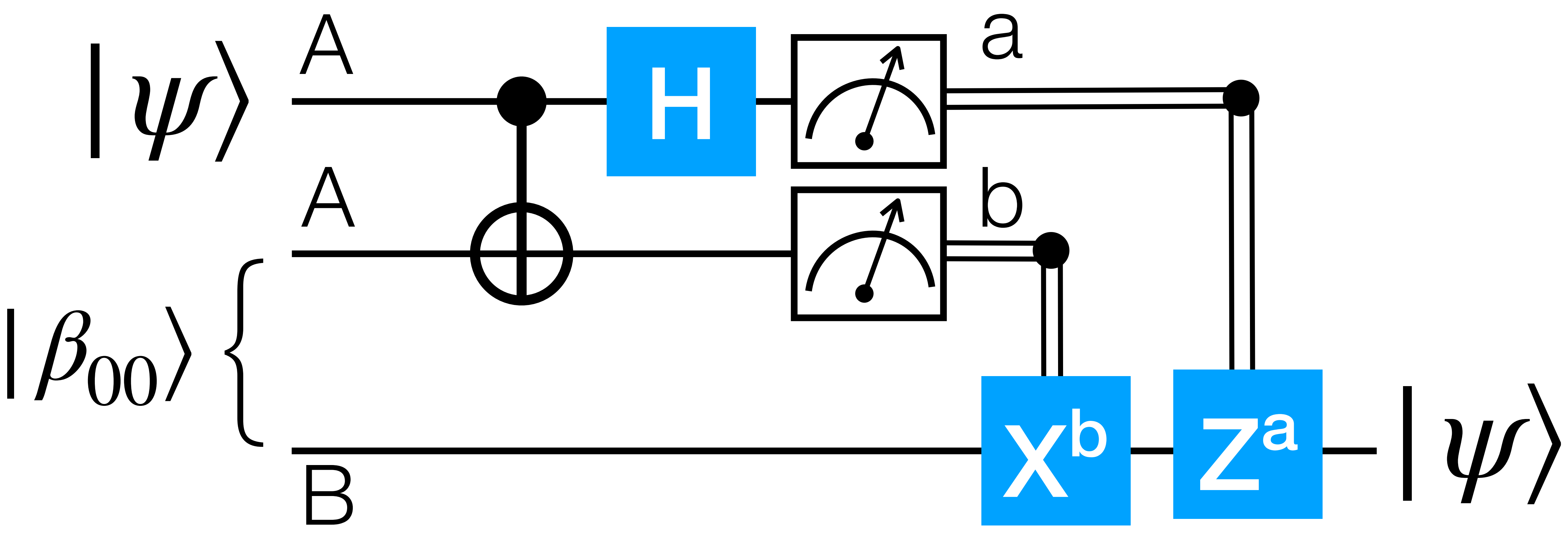
B

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

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

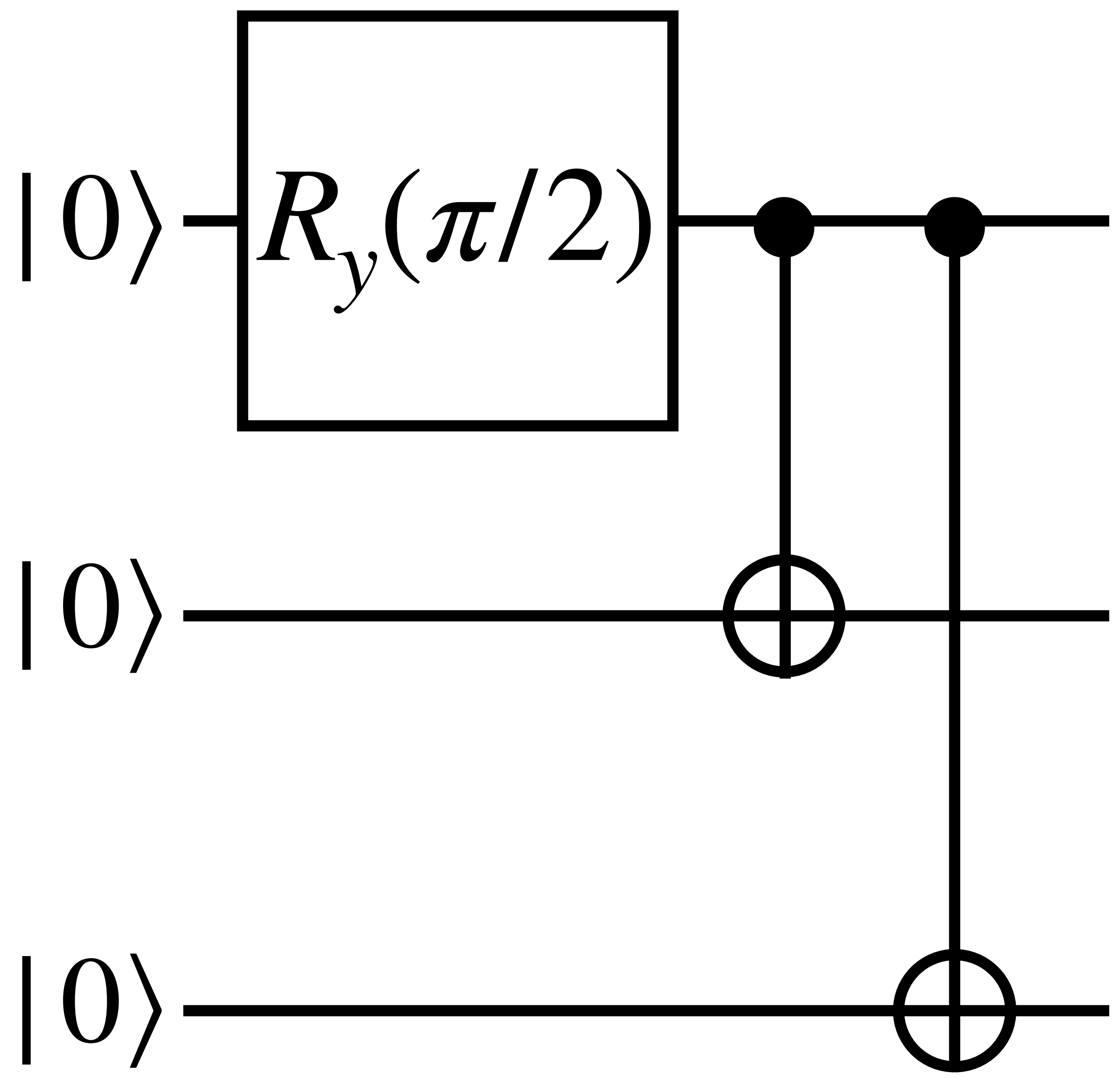
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

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

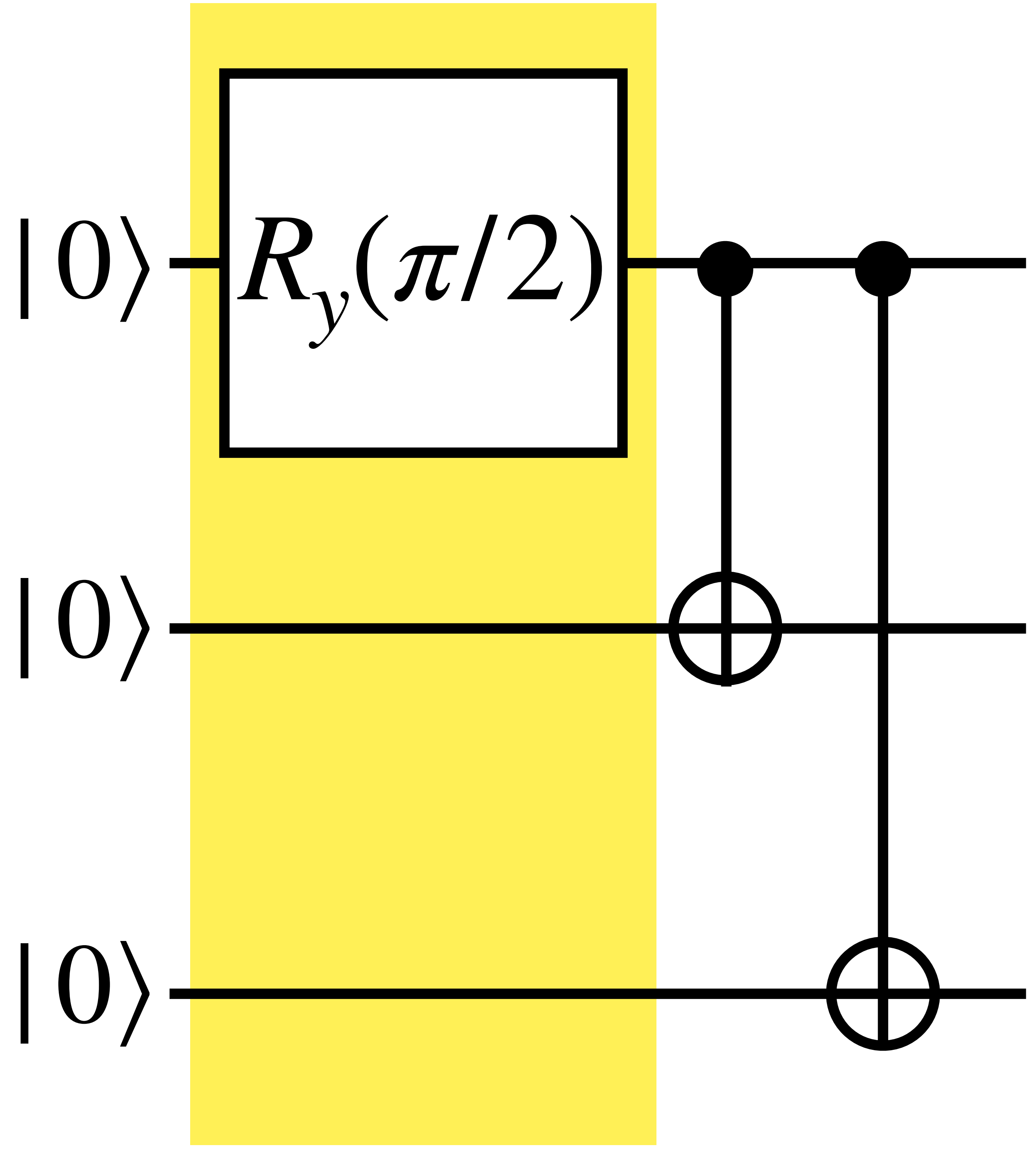


III. Basic Quantum Algorithms

Quantum Gate Examples



Quantum Gate Examples



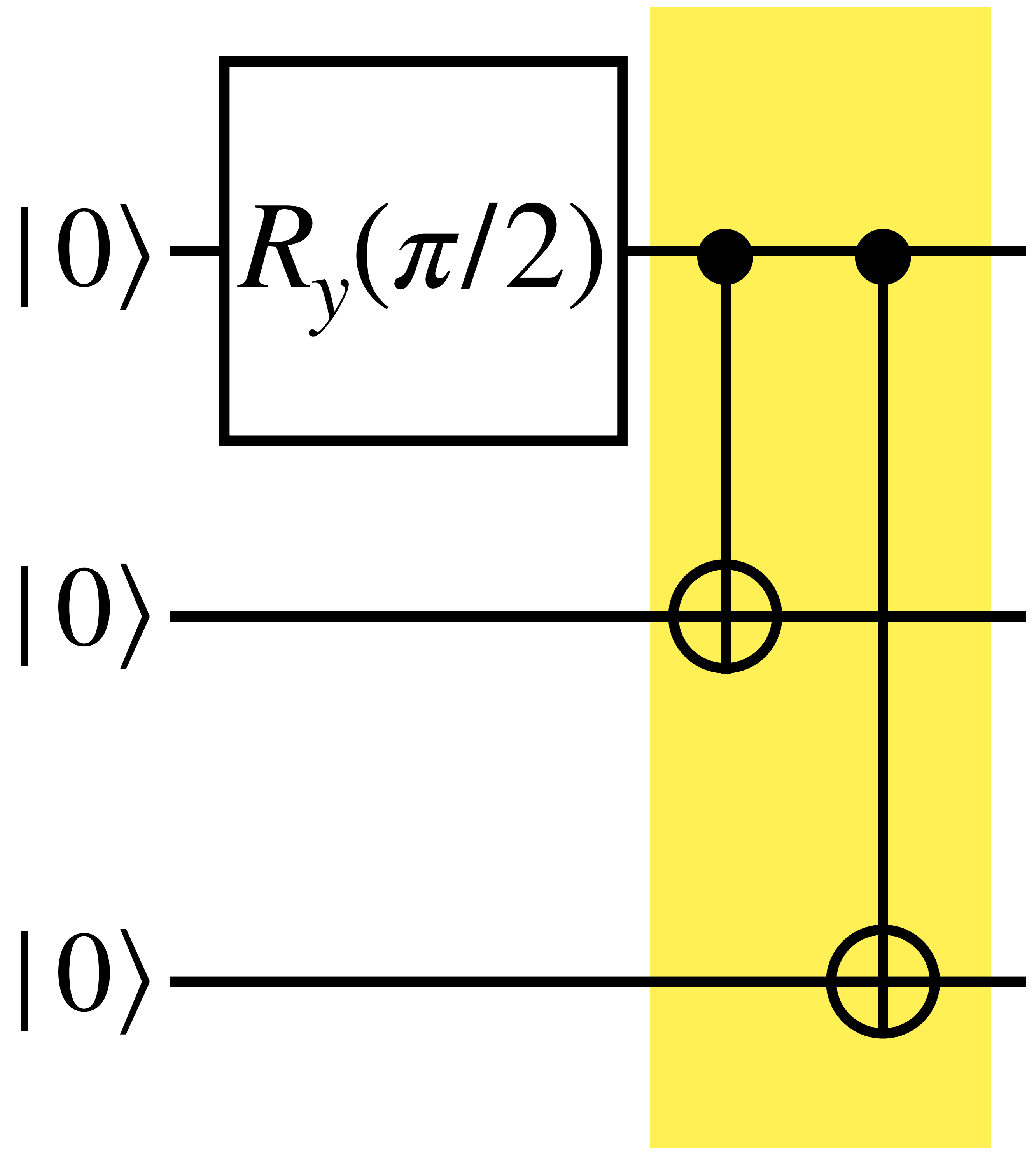
$$R_y(\pi/2)II|000\rangle = \Big((\cos(\pi/4)I - i\sin(\pi/4)\sigma_y)|0\rangle\Big)|00\rangle$$

$$= \left(\frac{1}{\sqrt{2}}I|0\rangle - i\frac{1}{\sqrt{2}}\sigma_y|0\rangle\right)|00\rangle$$

$$= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|00\rangle$$

Note: $R_y(\pi/2)II = R_y(\pi/2) \otimes I \otimes I$

Quantum Gate Examples

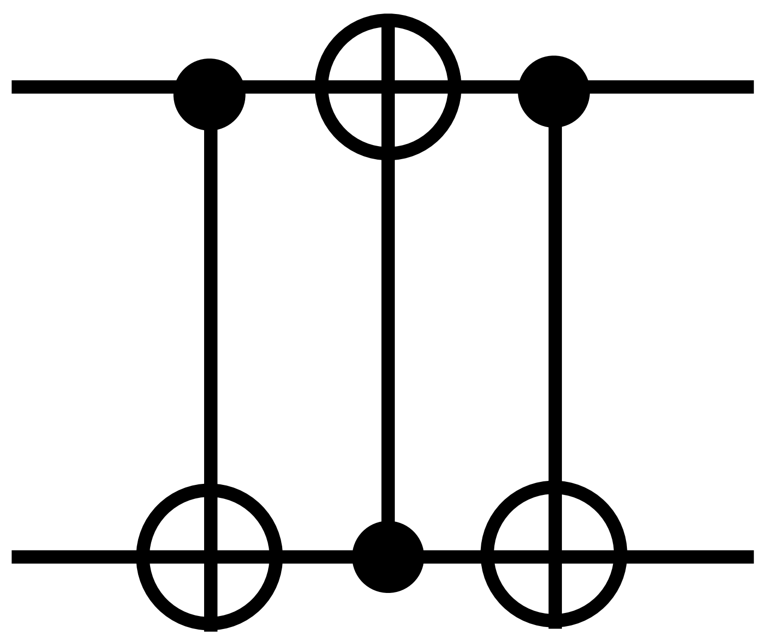


$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|00\rangle \to \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

Quantum Gate Examples

$a_0|0\rangle + a_1|1\rangle$

$b_0|0\rangle + b_1|1\rangle$

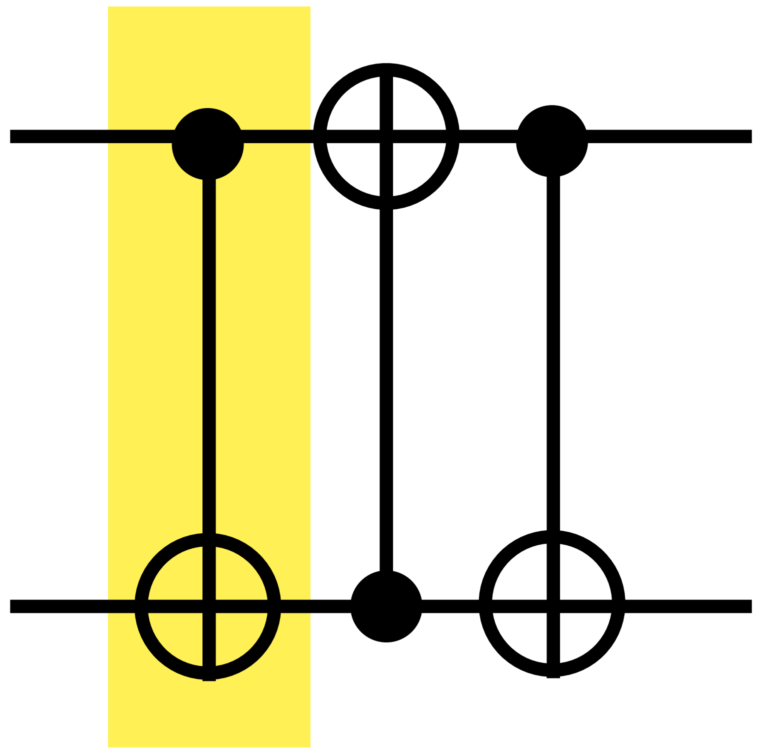


$a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle$

Quantum Gate Examples

$a_0|0\rangle + a_1|1\rangle$

$b_0|0\rangle + b_1|1\rangle$



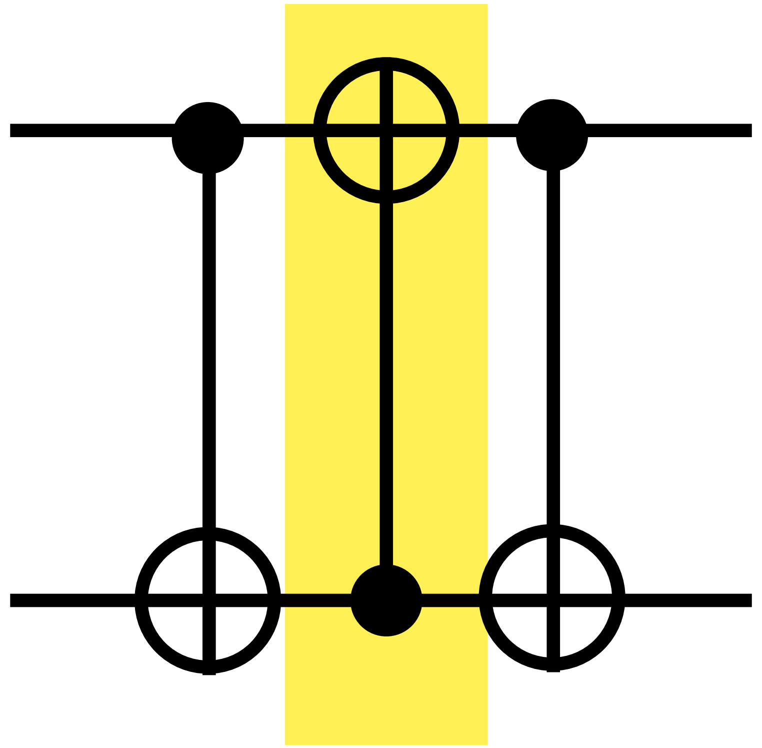
$$a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle$$

$$\rightarrow a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|11\rangle + a_1b_1|10\rangle$$

Quantum Gate Examples

$a_0|0\rangle + a_1|1\rangle$

$b_0|0\rangle + b_1|1\rangle$



$$a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle$$

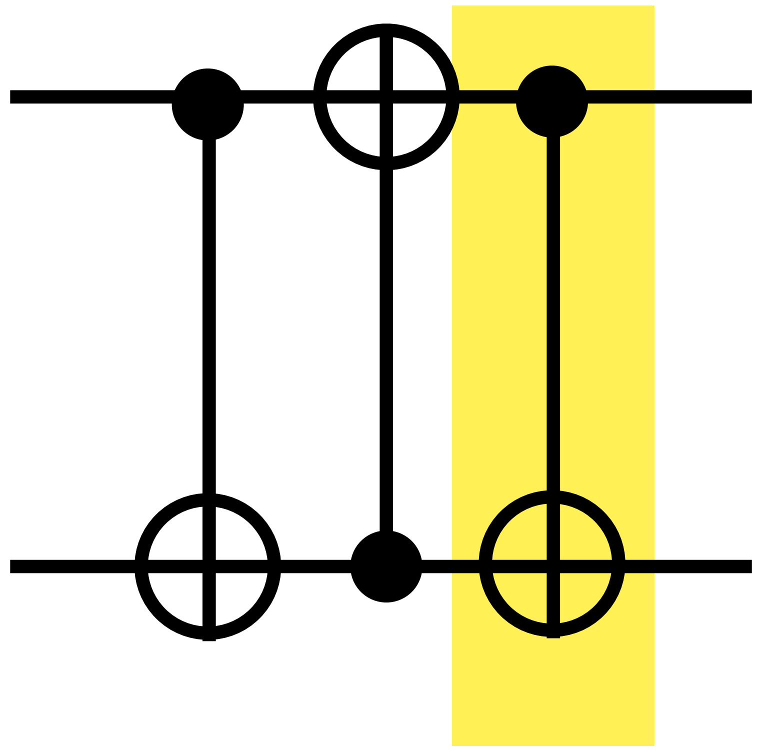
$$\rightarrow a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|11\rangle + a_1b_1|10\rangle$$

$$\rightarrow a_0b_0|00\rangle + a_0b_1|11\rangle + a_1b_0|01\rangle + a_1b_1|10\rangle$$

Quantum Gate Examples

$a_0|0\rangle + a_1|1\rangle$

$b_0|0\rangle + b_1|1\rangle$



$$a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle$$

$$\rightarrow a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|11\rangle + a_1b_1|10\rangle$$

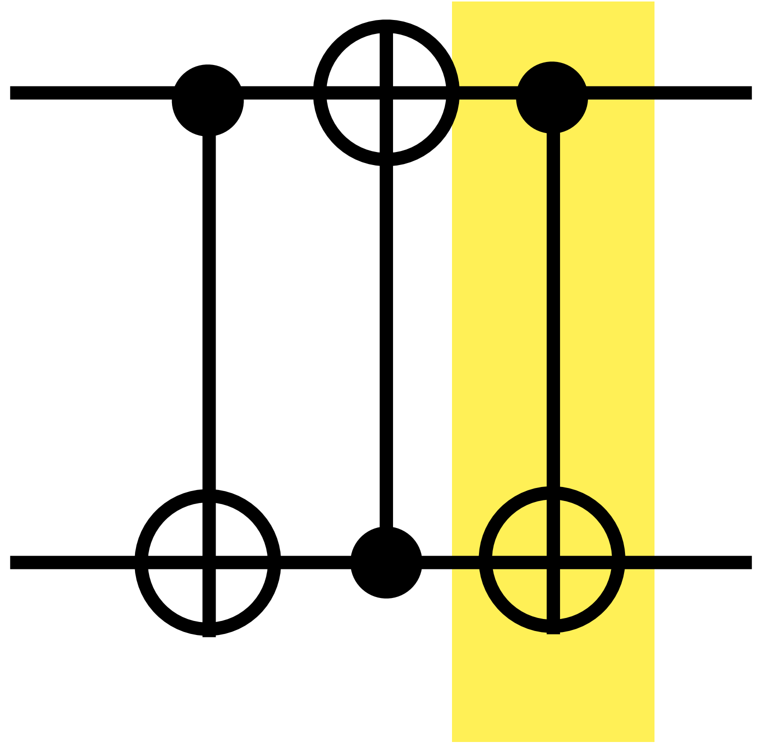
$$\rightarrow a_0b_0|00\rangle + a_0b_1|11\rangle + a_1b_0|01\rangle + a_1b_1|10\rangle$$

$$\rightarrow a_0b_0|00\rangle + a_0b_1|10\rangle + a_1b_0|01\rangle + a_1b_1|11\rangle$$

Quantum Gate Examples

$a_0|0\rangle + a_1|1\rangle$

$b_0|0\rangle + b_1|1\rangle$



$$a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle$$

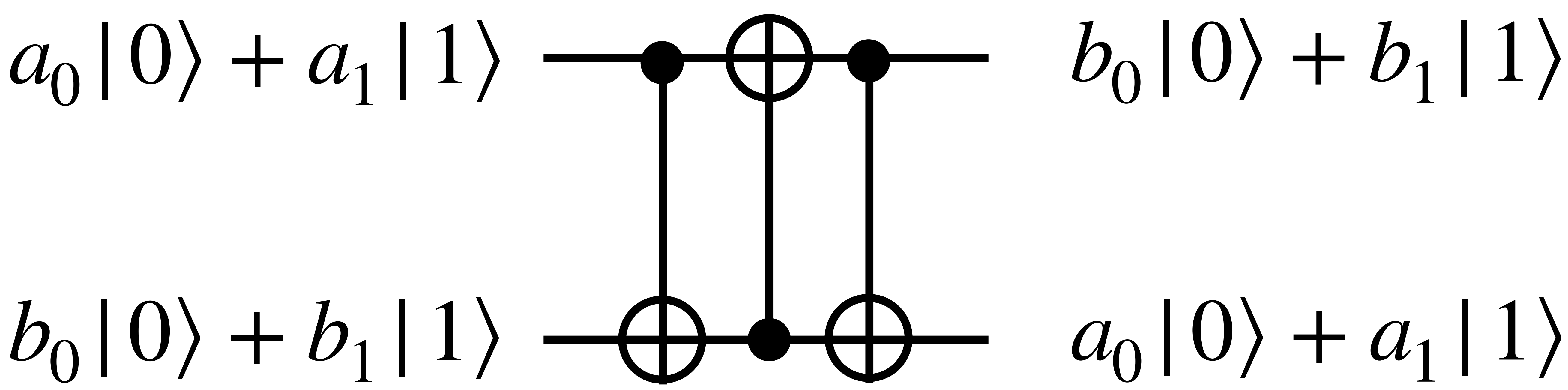
$$\to a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|11\rangle + a_1b_1|10\rangle$$

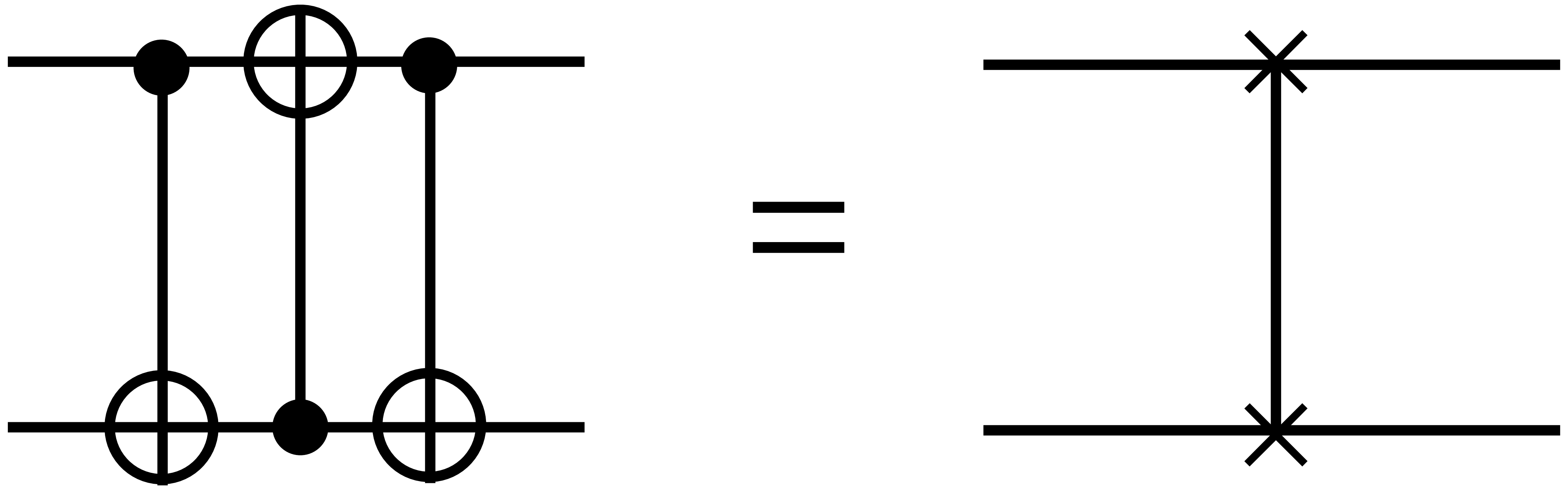
$$\to a_0b_0|00\rangle + a_0b_1|11\rangle + a_1b_0|01\rangle + a_1b_1|10\rangle$$

$$\to a_0b_0|00\rangle + a_0b_1|10\rangle + a_1b_0|01\rangle + a_1b_1|11\rangle$$

$$= (b_0|0\rangle + b_1|1\rangle) \otimes (a_1|0\rangle + a_1|1\rangle)$$

Quantum Gate Examples



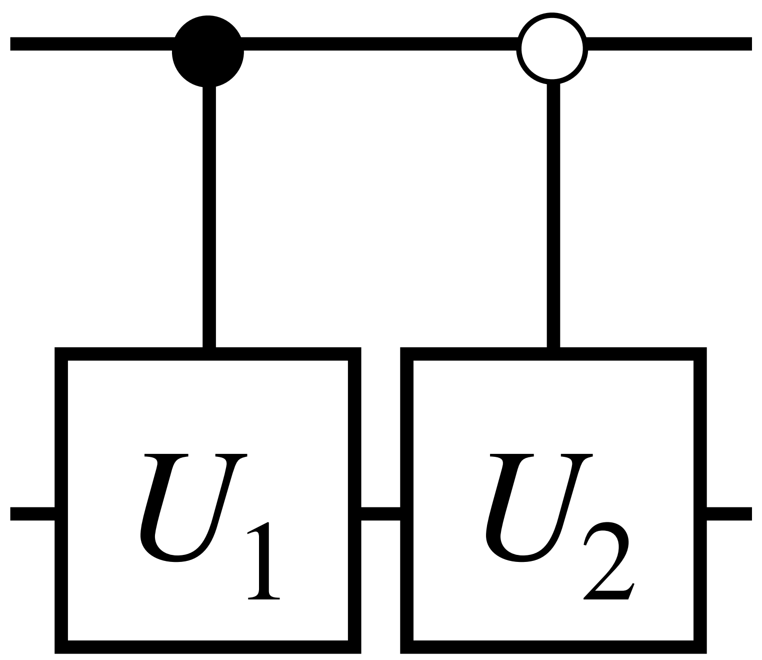


Swap gate

Quantum Gate Examples

$$a_0|0\rangle + a_1|1\rangle$$

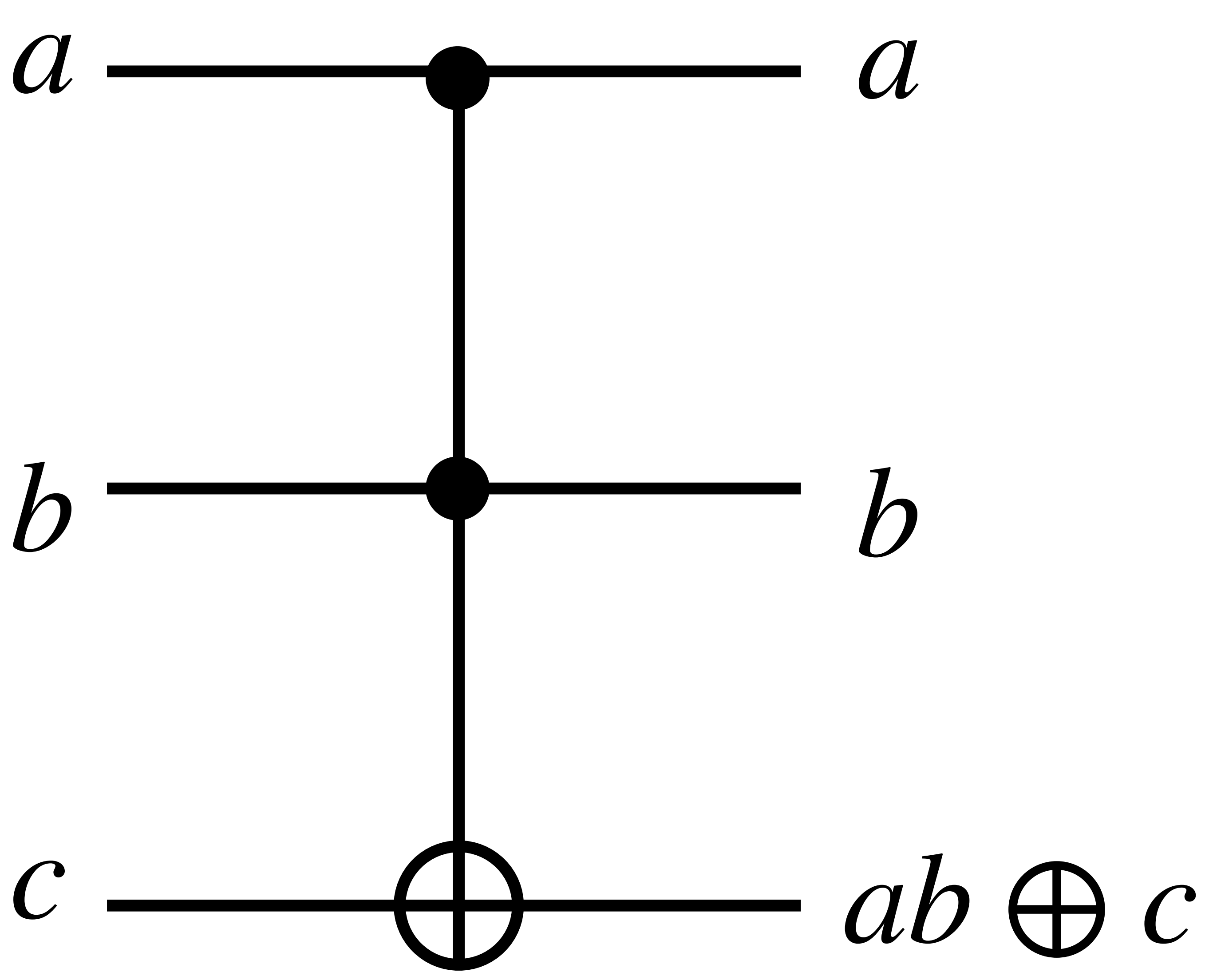
$$b_0|0\rangle + b_1|1\rangle$$



$$a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle$$

$$\rightarrow a_0b_0I|0\rangle U_2|0\rangle + a_0b_1I|0\rangle U_2|1\rangle + a_1b_0I|1\rangle U_1|0\rangle + a_1b_1I|1\rangle U_1|1\rangle$$

Quantum Gate Examples

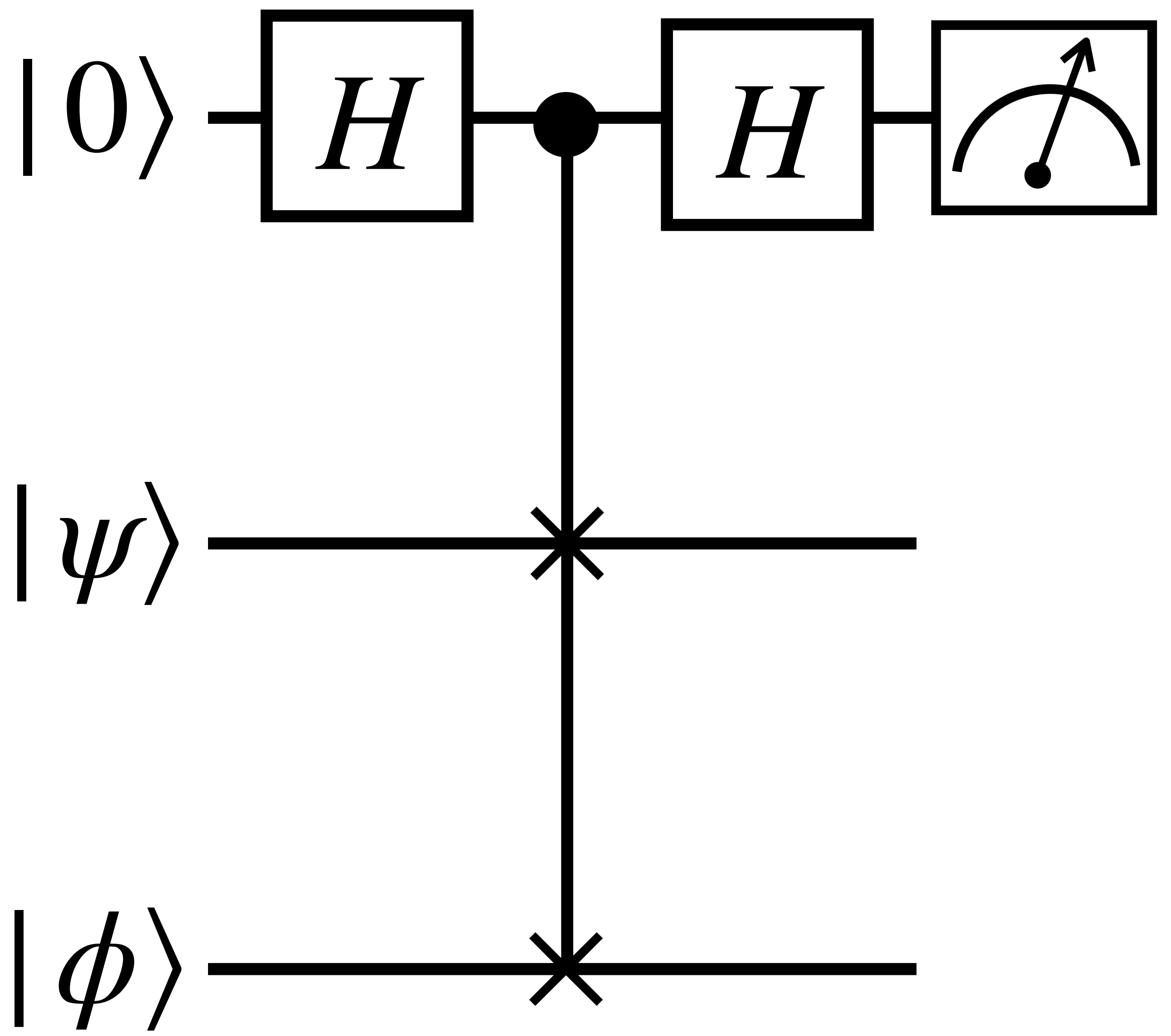


$$\frac{1}{\sqrt{8}}\sum_{a,b,c\in\{0,1\}}|a\rangle|b\rangle|c\rangle \rightarrow \frac{1}{\sqrt{8}}\sum_{a,b,c\in\{0,1\}}|a\rangle|b\rangle|ab\oplus c\rangle$$

Toffoli gate

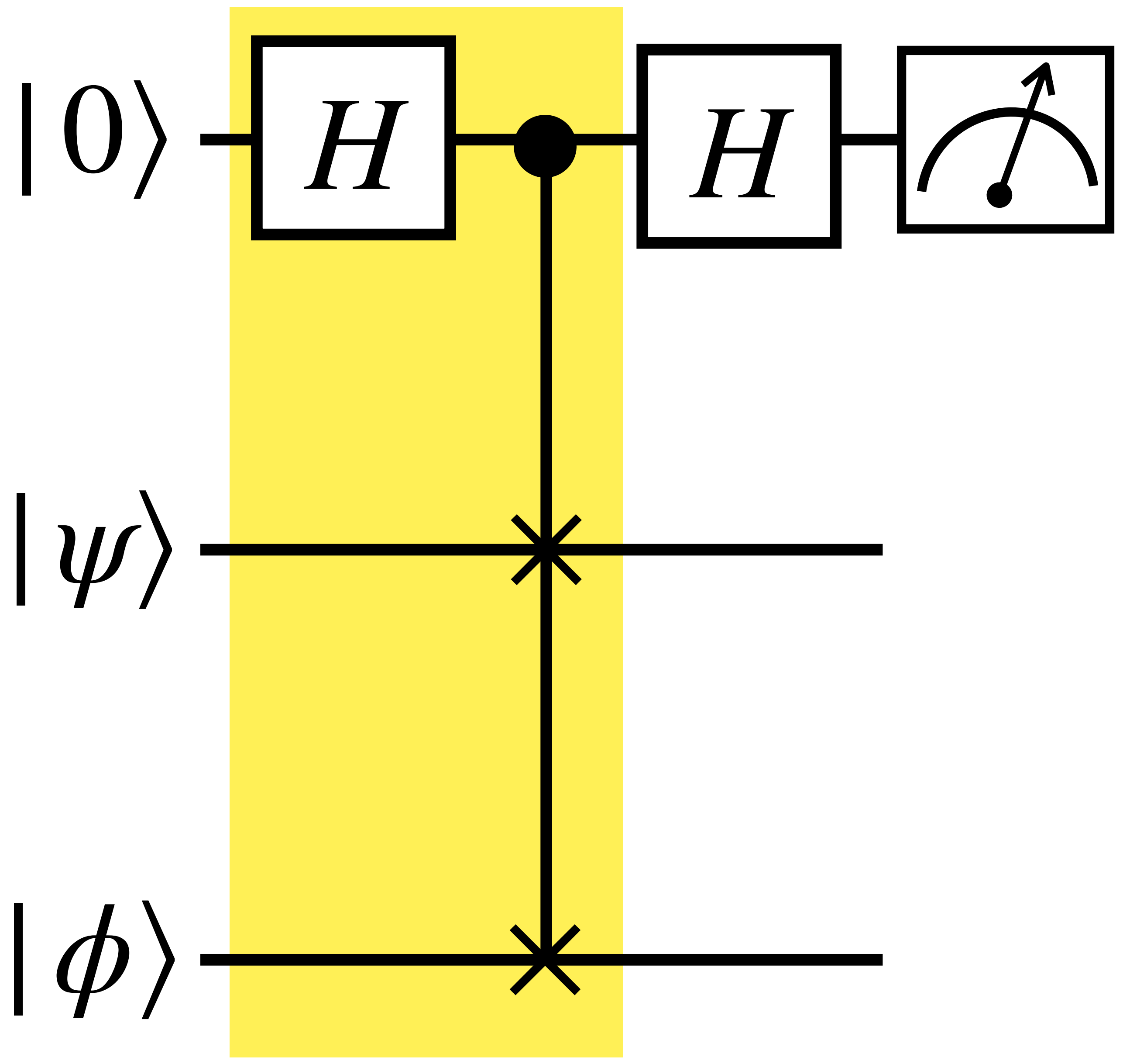
Inner Product Calculation

- Swap test



Inner Product Calculation

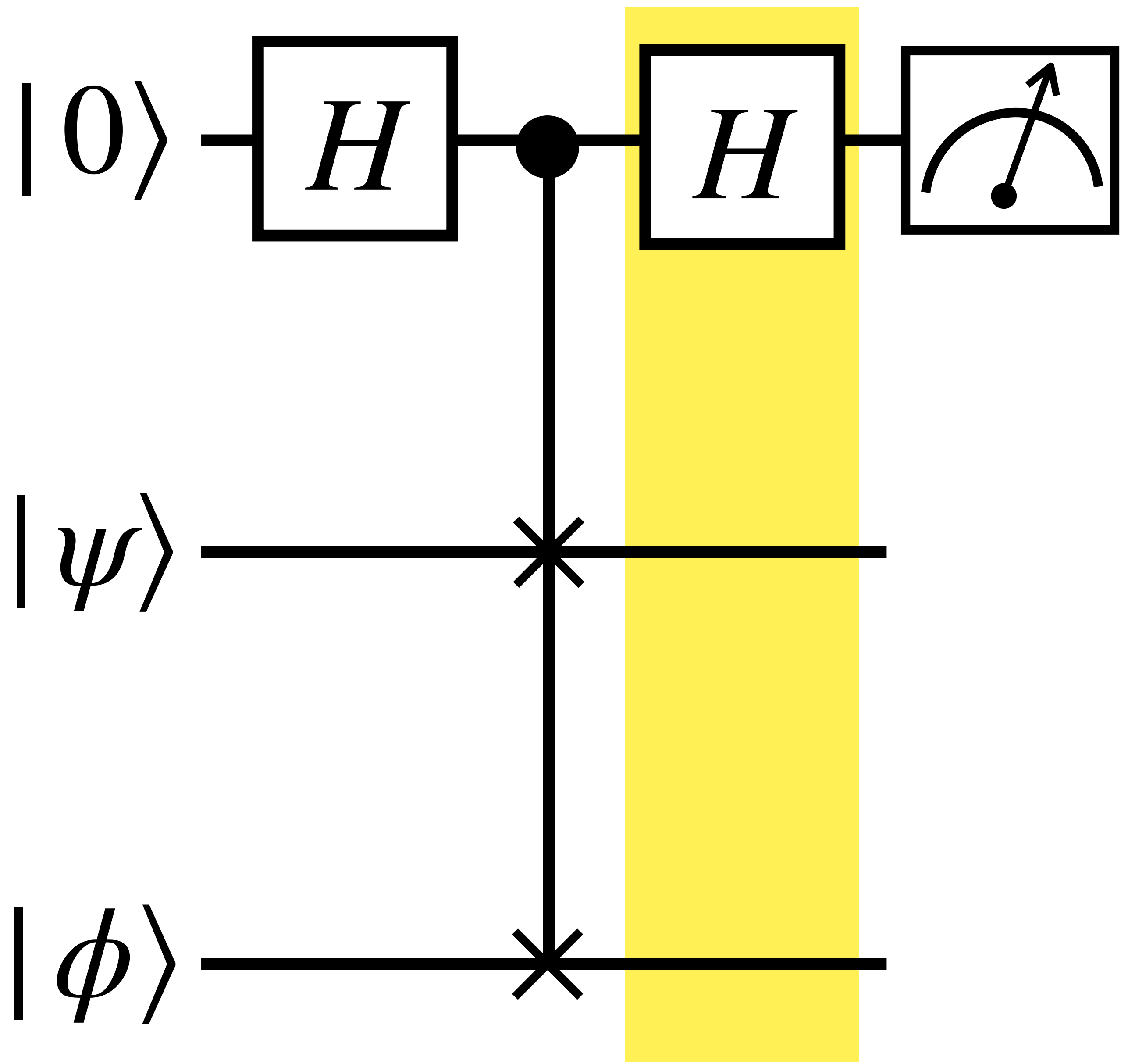
- Swap test



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

Inner Product Calculation

- Swap test

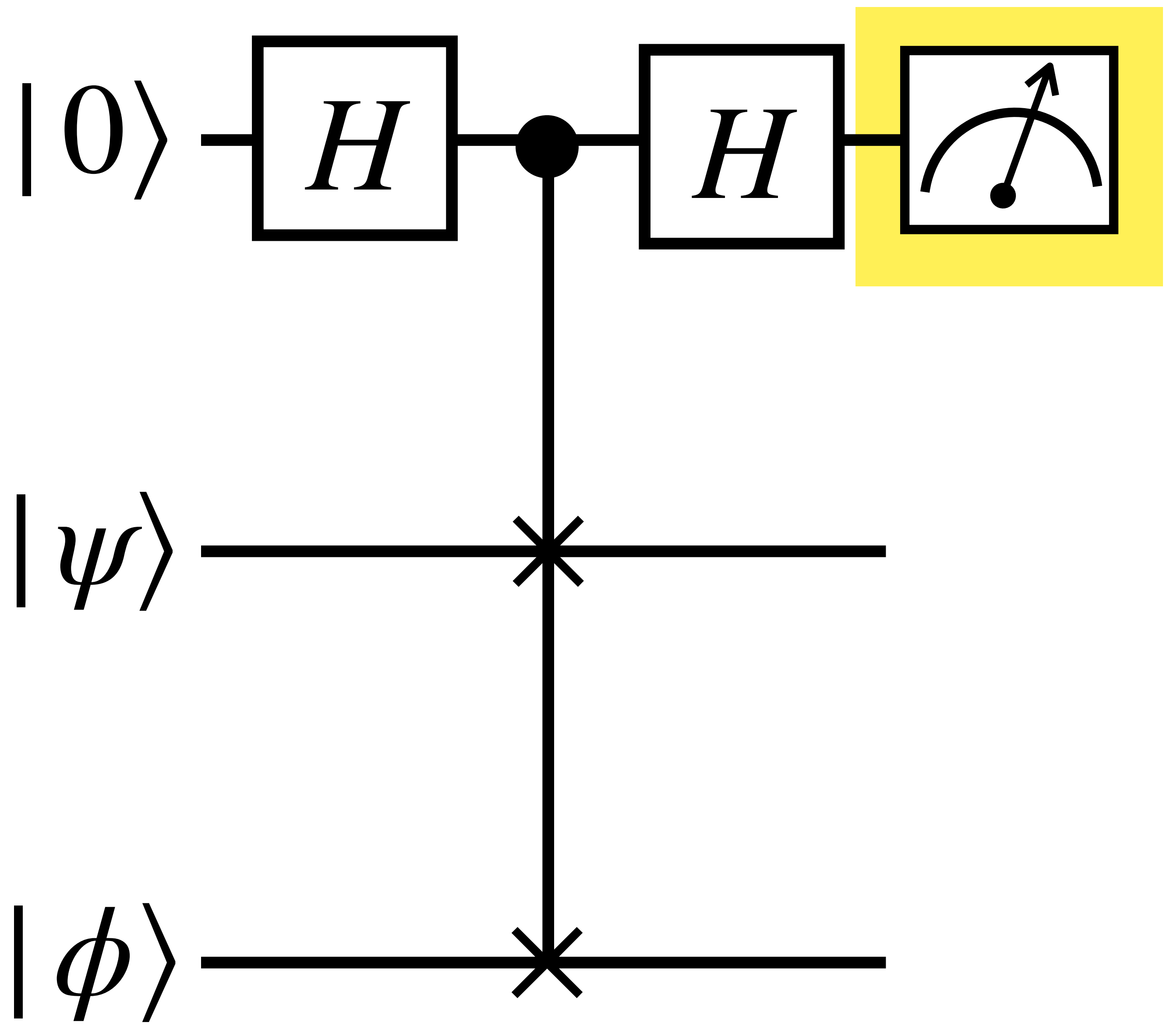


$$\frac{|0\rangle|\psi\rangle|\phi\rangle + |1\rangle|\phi\rangle|\psi\rangle}{\sqrt{2}}$$

$$\rightarrow \frac{|0\rangle(|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle) + |1\rangle(|\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle)}{2}$$

Inner Product Calculation

- Swap test



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

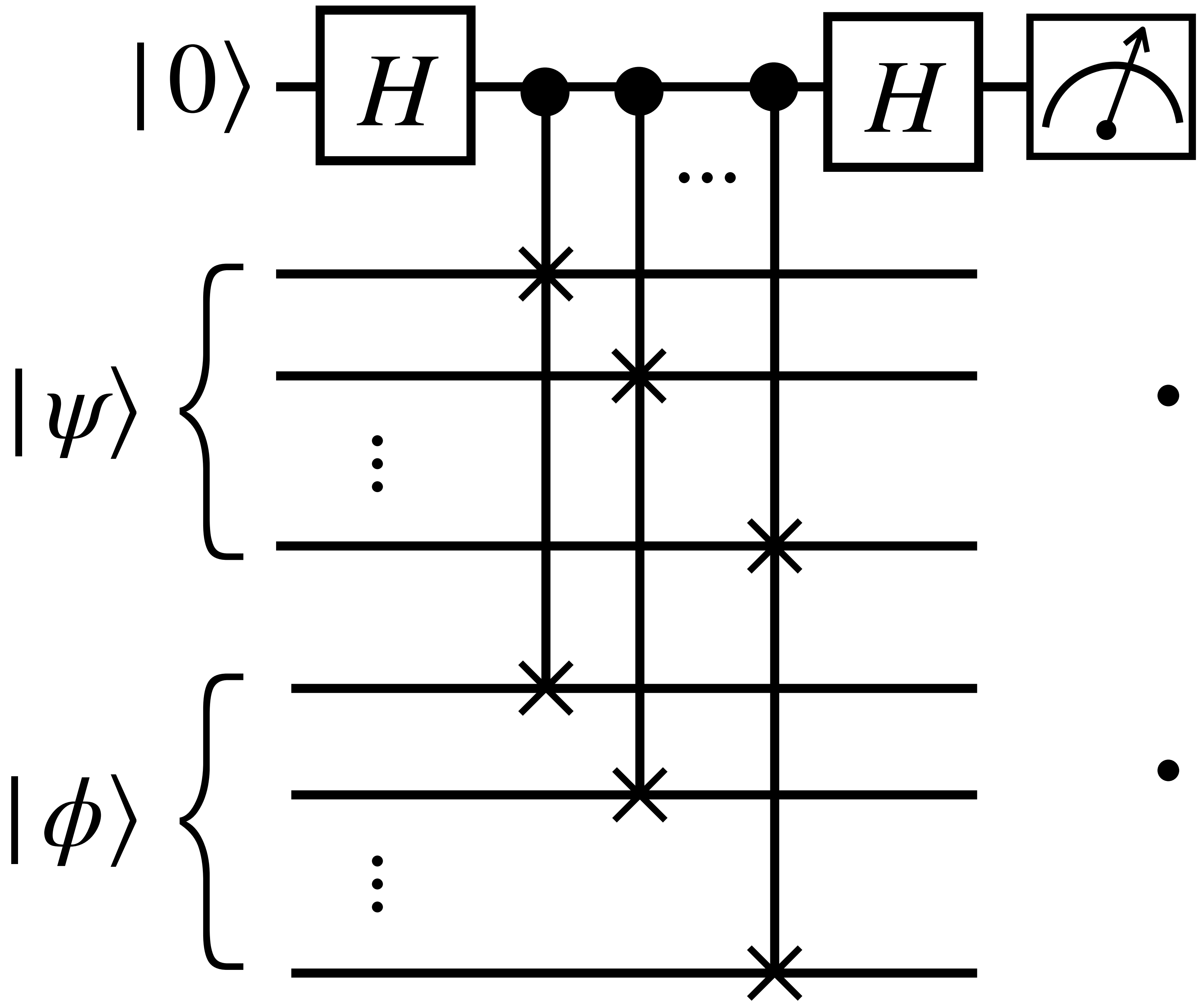
$$\rightarrow \frac{|0\rangle(|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle) + |1\rangle(|\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle)}{2}$$

$$\Pr(0) = \frac{1 + |\langle\psi|\phi\rangle|^2}{2} \qquad \Pr(1) = \frac{1 - |\langle\psi|\phi\rangle|^2}{2}$$

$$\langle Z\rangle = \Pr(0) - \Pr(1) = |\langle\psi|\phi\rangle|^2$$

Inner Product Calculation

- Swap test for multiple-qubit states $|\psi\rangle, |\phi\rangle \in \mathbb{C}^{2^n}$



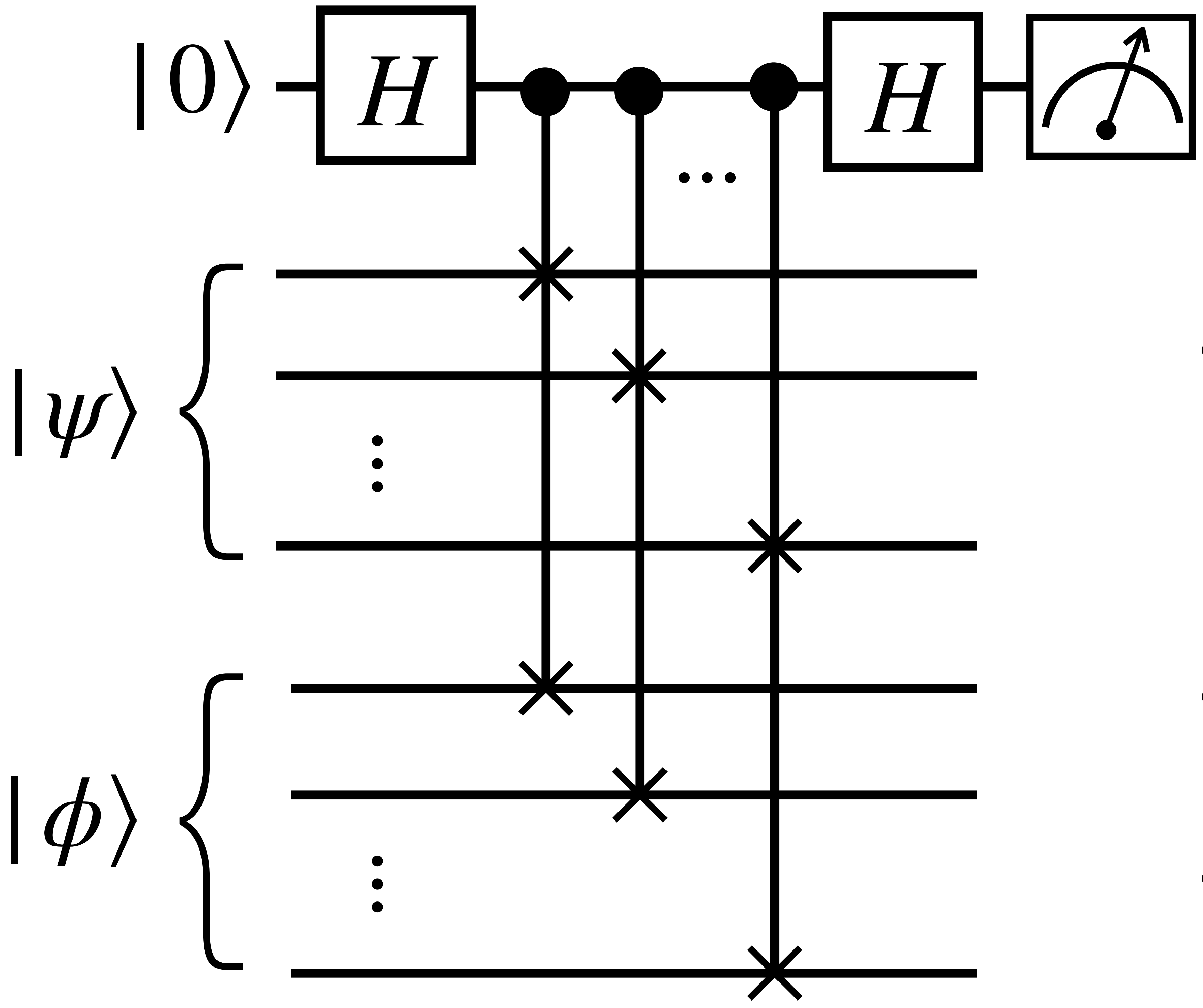
$$\langle Z \rangle = \Pr(0) - \Pr(1) = |\langle \psi | \phi \rangle|^2$$

- Inner product between two 2^n dimensional complex vectors can be evaluated n controlled-swap gates & 2 Hadamard gates.

- But the circuit has to be repeated many times to estimate the expectation value.

Inner Product Calculation

- Swap test for multiple-qubit states $|\psi\rangle, |\phi\rangle \in \mathbb{C}^{2^n}$

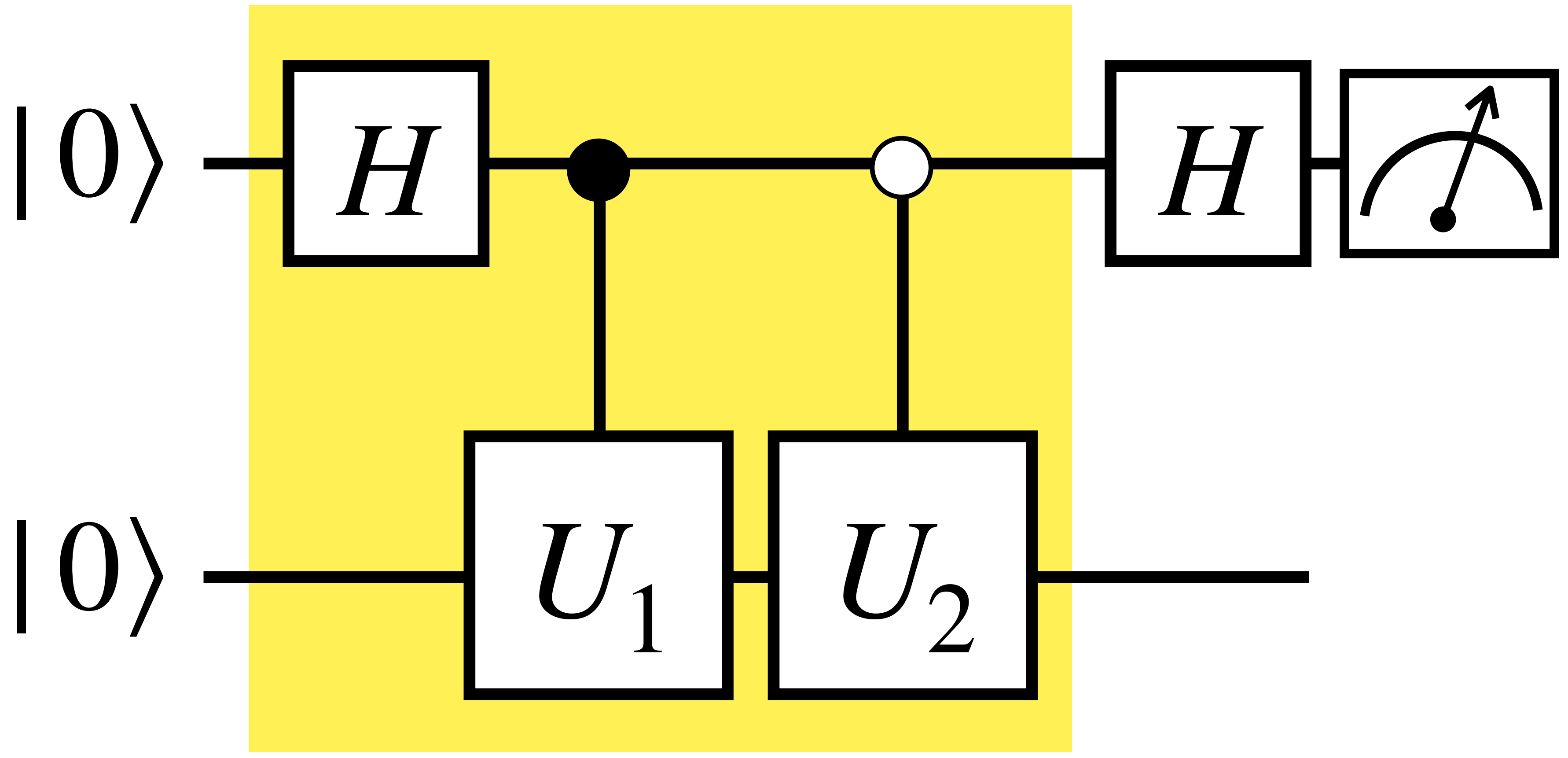


$$\langle Z \rangle = \Pr(0) - \Pr(1) = |\langle \psi | \phi \rangle|^2$$

- Chebyshev Inequality: $\Pr(|X - \mu| \geq \epsilon) \leq \dfrac{\sigma^2}{k\epsilon^2}$,
  where μ is obtained from k repetitions.
- Variance: $\sigma^2 = \langle Z^2 \rangle - \langle Z \rangle^2 = 1 - |\langle \psi | \phi \rangle|^4$.
- To bound the error probability to some constant:
  $k \propto \dfrac{1 - |\langle \psi | \phi \rangle|^4}{\epsilon^2}$.

Inner Product Calculation

- Real part of the inner product: Hadamard test



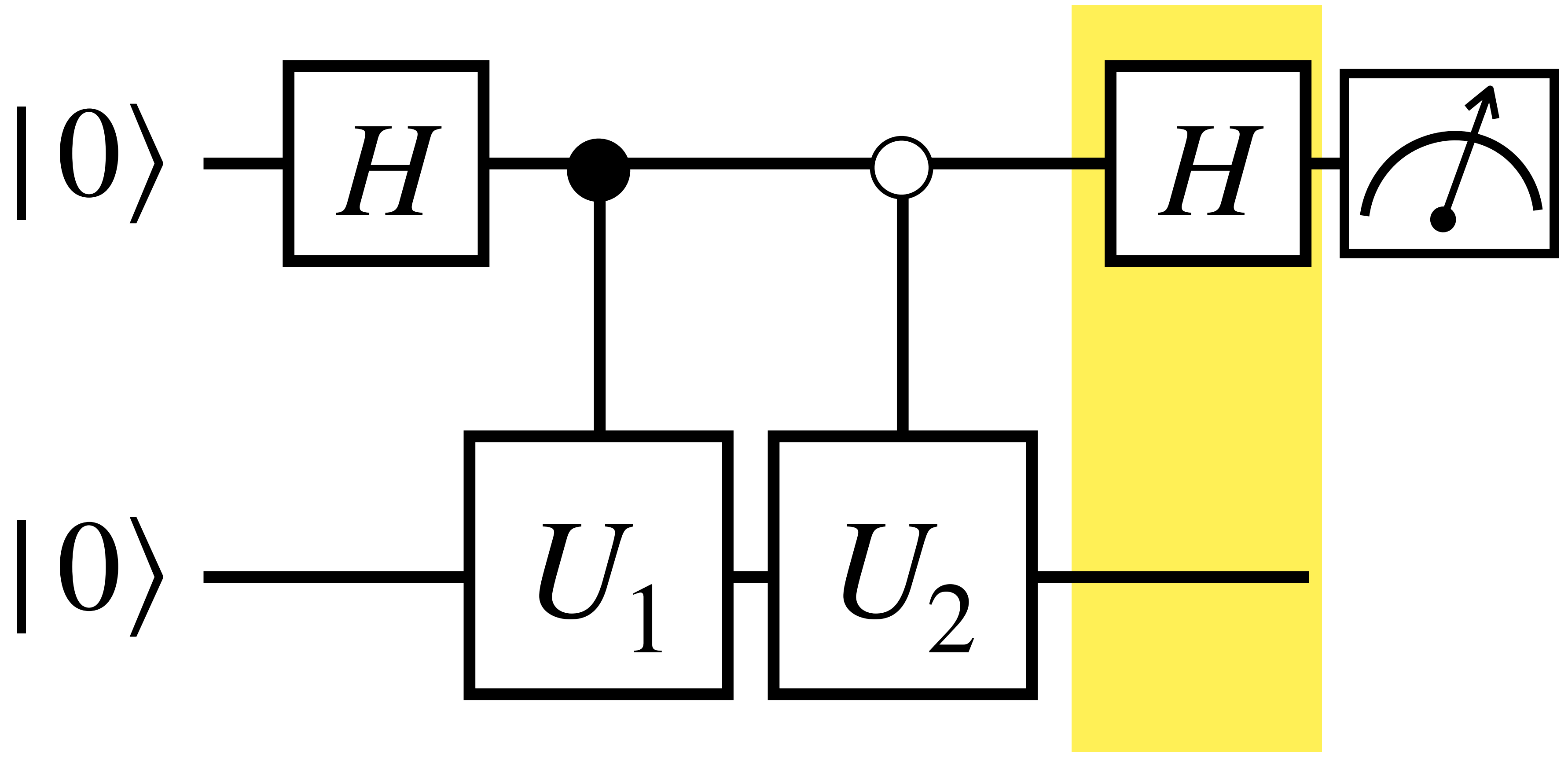
$$\frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle|\phi\rangle\right)$$

$$U_1|0\rangle = |\phi\rangle$$

$$U_2|0\rangle = |\psi\rangle$$

Inner Product Calculation

- Real part of the inner product: Hadamard test



$$\frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle|\phi\rangle\right)$$

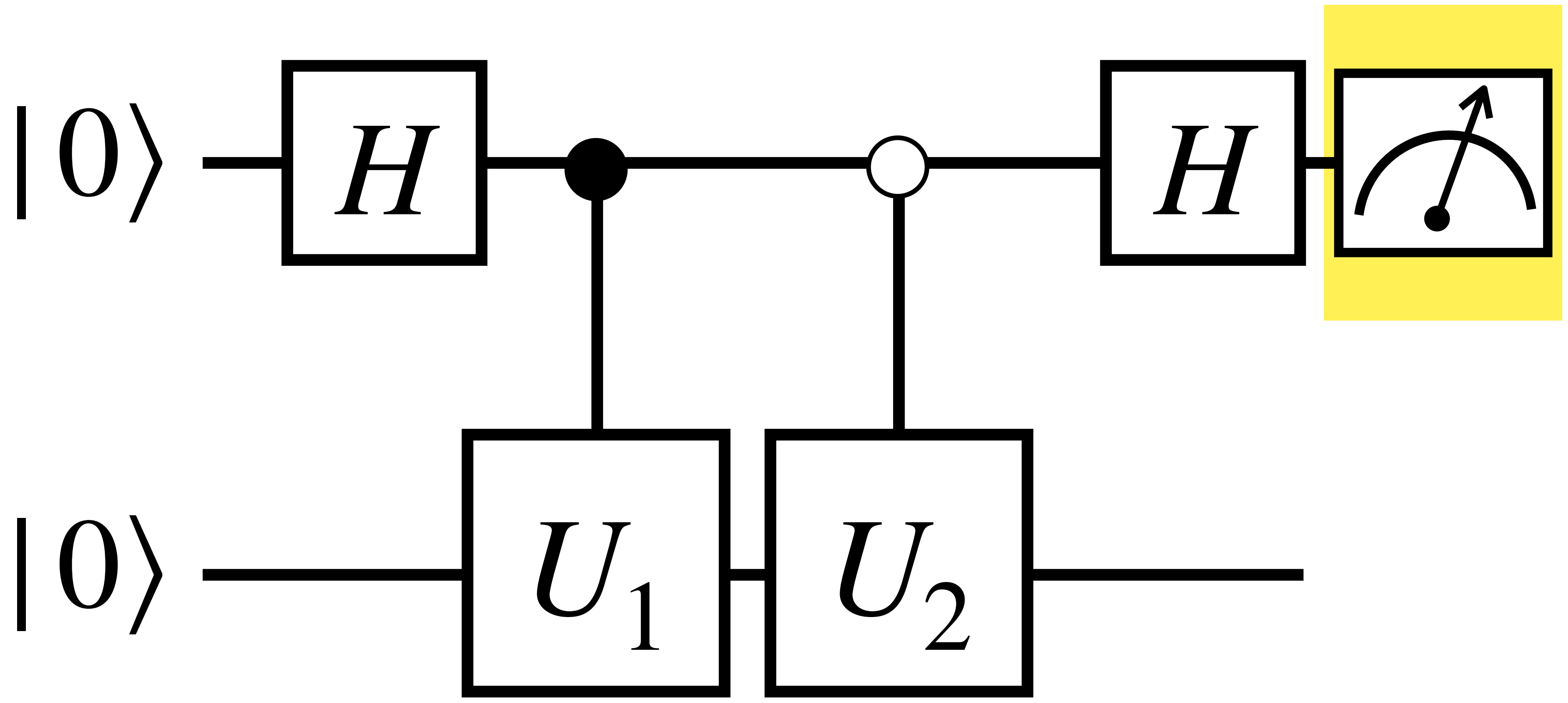
$$\to \frac{1}{2}\Big(|0\rangle\left(|\psi\rangle + |\phi\rangle\right) + |1\rangle\left(|\psi\rangle - |\phi\rangle\right)\Big)$$

$$U_1|0\rangle = |\phi\rangle$$

$$U_2|0\rangle = |\psi\rangle$$

Inner Product Calculation

- Real part of the inner product: Hadamard test



$$\frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle|\phi\rangle\right)$$

$$\rightarrow \frac{1}{2}\Big(|0\rangle\big(|\psi\rangle + |\phi\rangle\big) + |1\rangle\big(|\psi\rangle - |\phi\rangle\big)\Big)$$

$$U_1|0\rangle = |\phi\rangle$$

$$U_2|0\rangle = |\psi\rangle$$

$$\Pr(0) = \frac{1 + \Re\left(\langle\psi|\phi\rangle\right)}{2} \qquad \Pr(1) = \frac{1 - \Re\left(\langle\psi|\phi\rangle\right)}{2}$$

$$\langle Z\rangle = \Pr(0) - \Pr(1) = \Re\left(\langle\psi|\phi\rangle\right)$$

Computational Cost

- How do we estimate the computational cost?
- In practice,
  - Gates and/or circuit depth after compilation to specific hardware.
  - Gate and/or circuit depth with respect to logical qubits & logical gates.
  - Actual runtime = (circuit depth x gate time + reset) x repetition + some other stuff.
  - Number of qubits (circuit width).
- Can we abstract away hardware-specific implementation details and estimate the intrinsic computational cost of the algorithm?
  - Oracle model & Query complexity ← Many early quantum algorithms are based on it.

Oracle Model

- How many times should we query an oracle (or a black-box) to learn something about a Boolean function $f(x)$?

Membership oracle $x \longrightarrow \blacksquare \longrightarrow f(x)$

Example oracle $\blacksquare \longrightarrow \big(x, f(x)\big),\ x \sim p(x)$

Quantum membership oracle $|x\rangle\,|y\rangle \longrightarrow \blacksquare \longrightarrow |x\rangle\,|y \oplus f(x)\rangle$

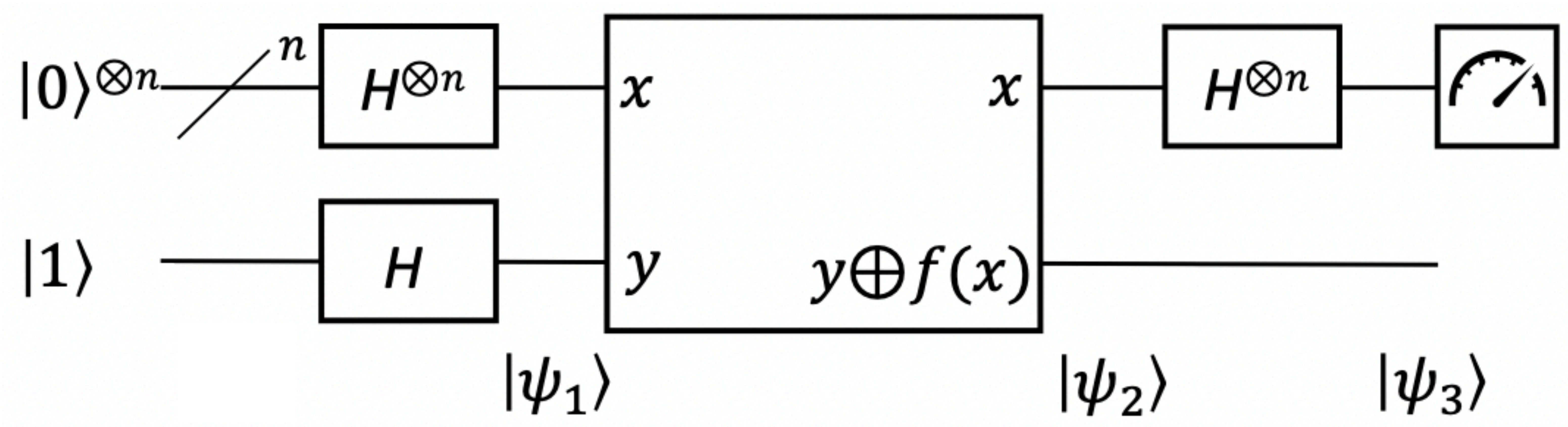
Quantum example oracle $|0\ldots0\rangle \longrightarrow \blacksquare \longrightarrow \sum_{x \in \{0,1\}^n} \sqrt{p(x)}\,|x\rangle\,|f(x)\rangle$

Deutsch-Jozsa Algorithm

- Input: An oracle that computes an unknown function $f : \{0,1\}^n \to \{0,1\}$.
- Promise: f is either constant or balanced.
  - Constant: Same output for all $x \in \{0,1\}^n$.
  - Balanced: $f(x)$ is 0 for half of the possible values of x, and 1 for the other half.
- Problem: Determine whether $f(x)$ is constant or balanced by making queries to the oracle with an input x.
- Classical oracle: $\dfrac{2^n}{2} + 1$ queries to solve the problem with certainty.
- Quantum oracle: Query only once!

Deutsch-Jozsa Algorithm

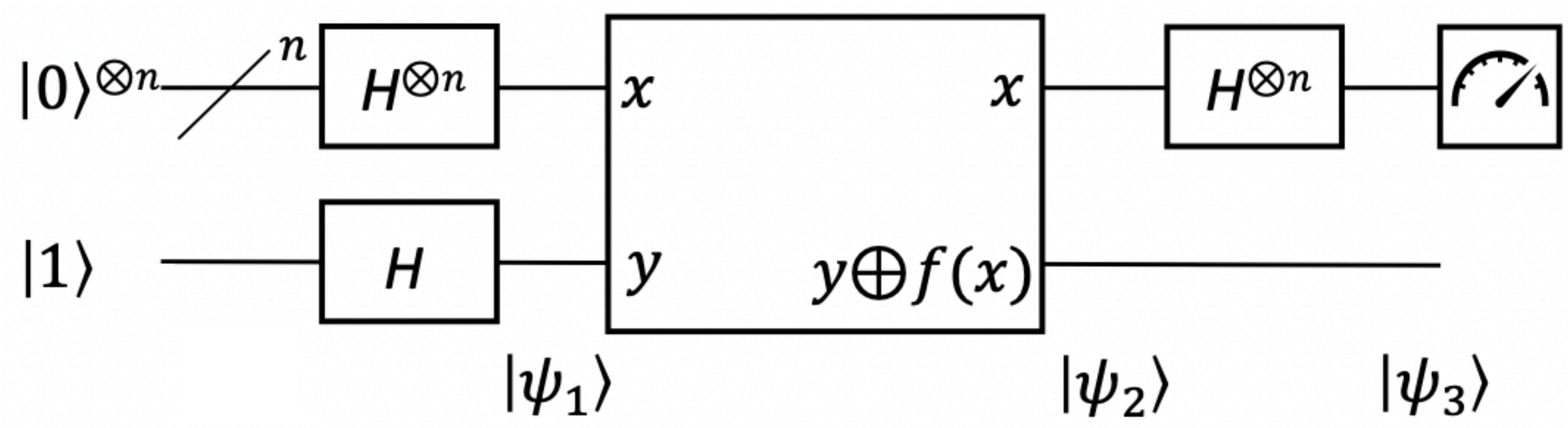
- The quantum circuit for the Deutsch-Jozsa algorithm:



$$|\psi_1\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}}|x\rangle \otimes (|0\rangle - |1\rangle)$$

Deutsch-Jozsa Algorithm

- The quantum circuit for the Deutsch-Jozsa algorithm:

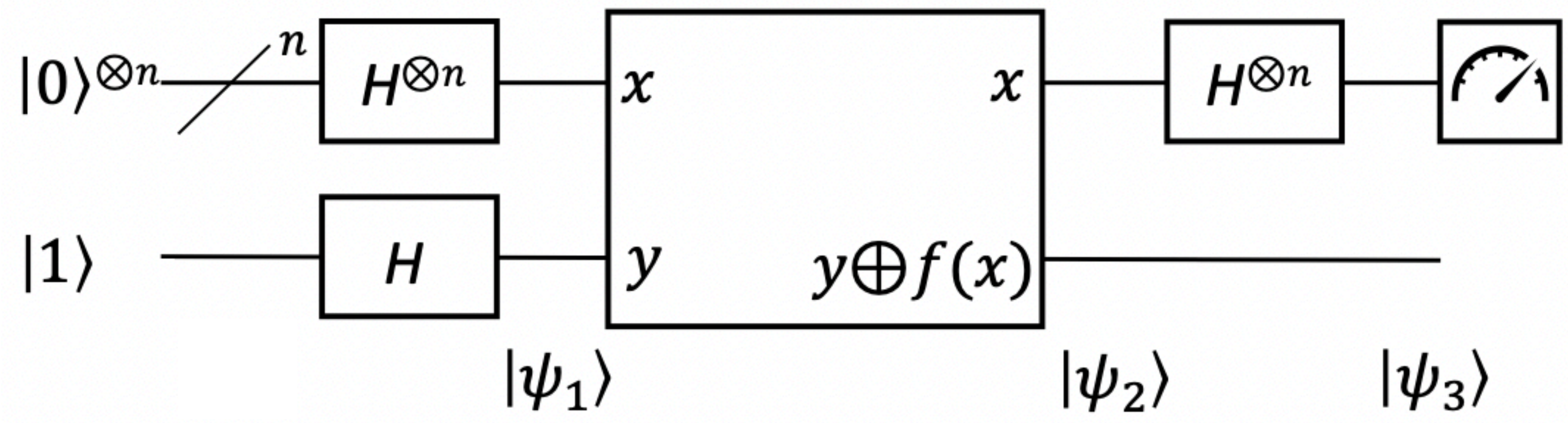


$$|\psi_2\rangle = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} |x\rangle \otimes (|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)$$

$$= \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} |x\rangle \otimes (|f(x)\rangle - |1 \oplus f(x)\rangle)$$

Deutsch-Jozsa Algorithm

- The quantum circuit for the Deutsch-Jozsa algorithm:



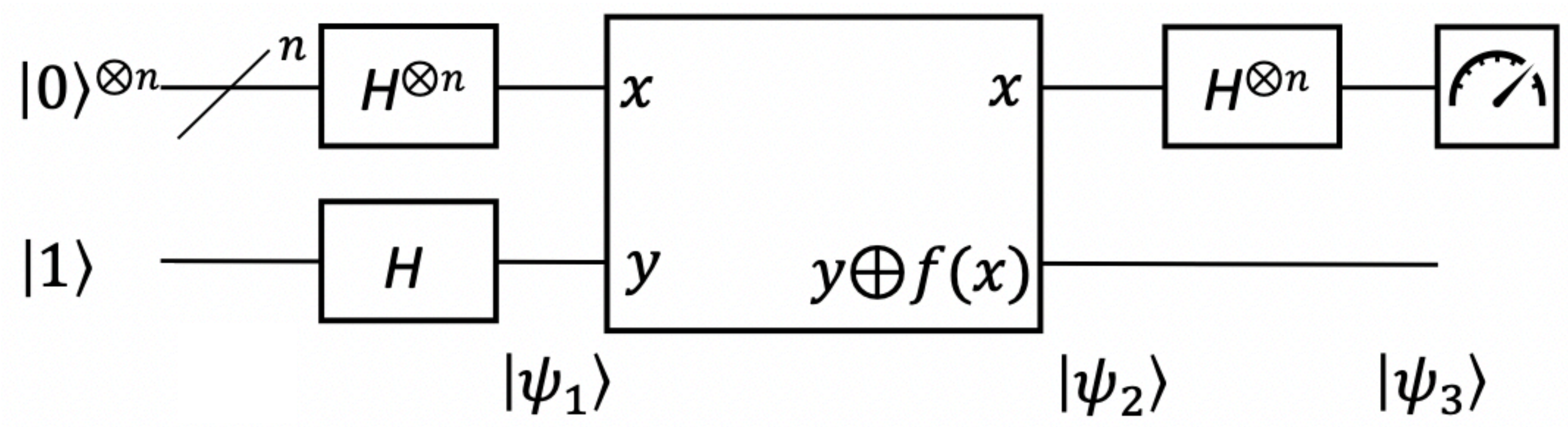
$$|\psi_2\rangle = \begin{cases} \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} |x\rangle \otimes (|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} |x\rangle \otimes (|1\rangle - |0\rangle) & \text{if } f(x) = 1 \end{cases}$$

$$\therefore |\psi_2\rangle = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} (-1)^{f(x)} |x\rangle |-\rangle$$

phase kick-back

Deutsch-Jozsa Algorithm

- The quantum circuit for the Deutsch-Jozsa algorithm:



For $x \in \{0,1\}^n$, $H^{\otimes n}|x\rangle = \dfrac{1}{\sqrt{2^n}} \displaystyle\sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle$

$$|\psi_3\rangle = \sum_{x \in \{0,1\}^n} \sum_{z \in \{0,1\}^n} \frac{1}{2^n} (-1)^{x \cdot z + f(x)} |z\rangle |-\rangle$$

Deutsch-Jozsa Algorithm

$$|\psi_3\rangle = \sum_{x\in\{0,1\}^n} \sum_{z\in\{0,1\}^n} \frac{1}{2^n}(-1)^{x\cdot z+f(x)}|z\rangle|-\rangle$$

- When $f(x)$ is constant:
  - When $|z\rangle = |0\rangle^{\otimes n}$, its amplitude is $\sum_{x\in\{0,1\}^n} \frac{1}{2^n}(-1)^{f(x)} = \pm 1$.
  - Therefore, $|z\rangle = |0\rangle^{\otimes n}$ with measured with probability 1.
- When $f(x)$ is balanced:
  - For $|z\rangle = |0\rangle^{\otimes n}$, its amplitude is $\sum_{x\in\{0,1\}^n} \frac{1}{2^n}(-1)^{f(x)} = 0$. Why?

Deutsch-Jozsa Algorithm

- Deterministic classical algorithm would require $2^{n-1} + 1$ queries in the worst case..
- Quantum algorithm requires only 1 query, achieved by exploiting quantum superposition & interference.
- What if we allow for some error probability?
  - If $f(x)$ is balanced, the probability of getting $f(x) = 0$ (or equivalently, $f(x) = 1$) is 1/2. Thus, the probability to get the same bit k times is $2/2^k$.
  - Therefore, for a randomized algorithm, the probability to guess incorrectly scales inverse exponentially with the number of queries k.
- If $f(x)$ is balanced with a probability of $1/2$ and constant with a probability of $1/2$, then the probability to success after k queries is $1 - 2^{-k}$.