



NITHeP Mini-school on quantum computing

INTRODUCTION TO THE THEORY OF QUANTUM COMPUTING

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



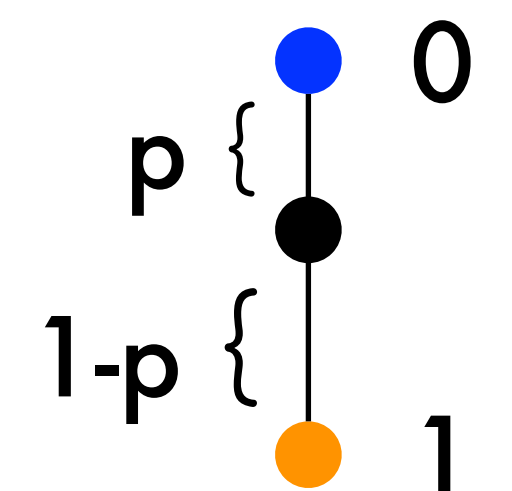
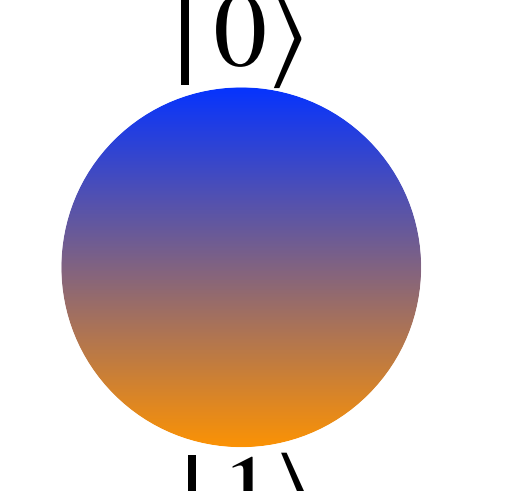
Part I: What & Why

- Introduction & Background

Part II: How

- Quantum Circuit
- **Quantum Algorithms**
- Quantum Error Correction

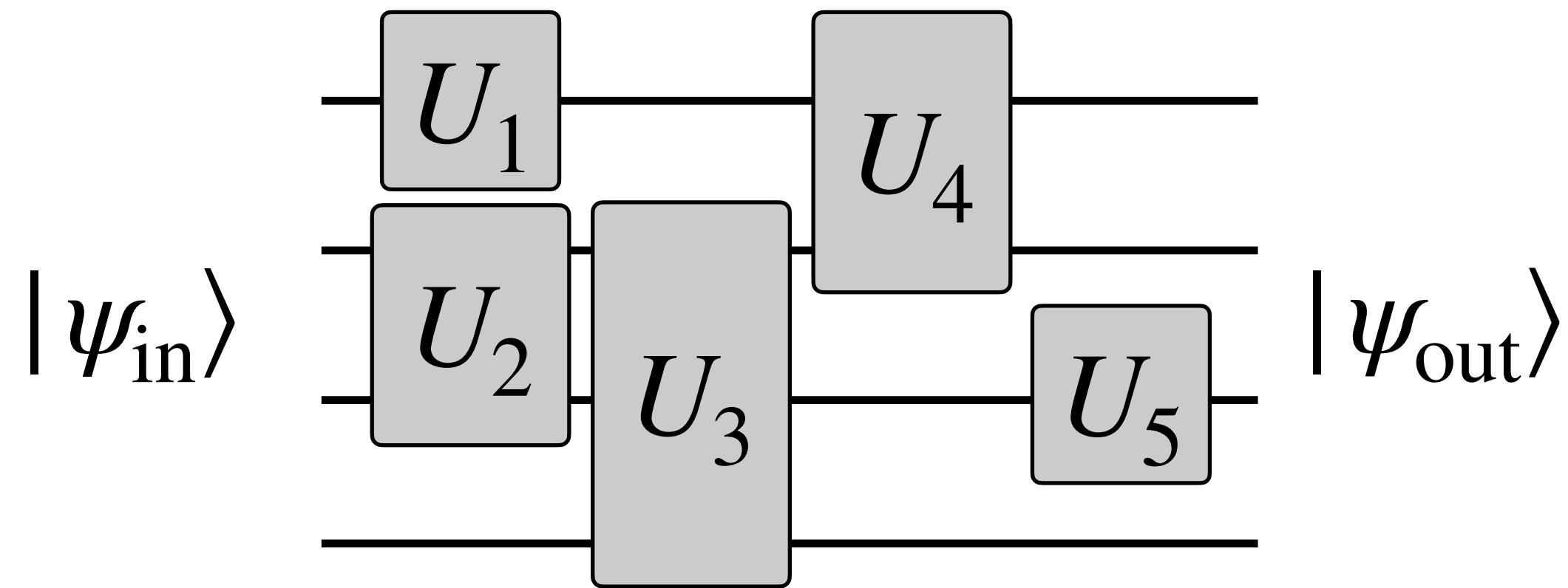
Summary: Bit, Pbit, Qubit

	bit	probabilistic bit	quantum bit
Pictorial Representation	<div><div>● 0</div><div>● 1</div></div>		
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

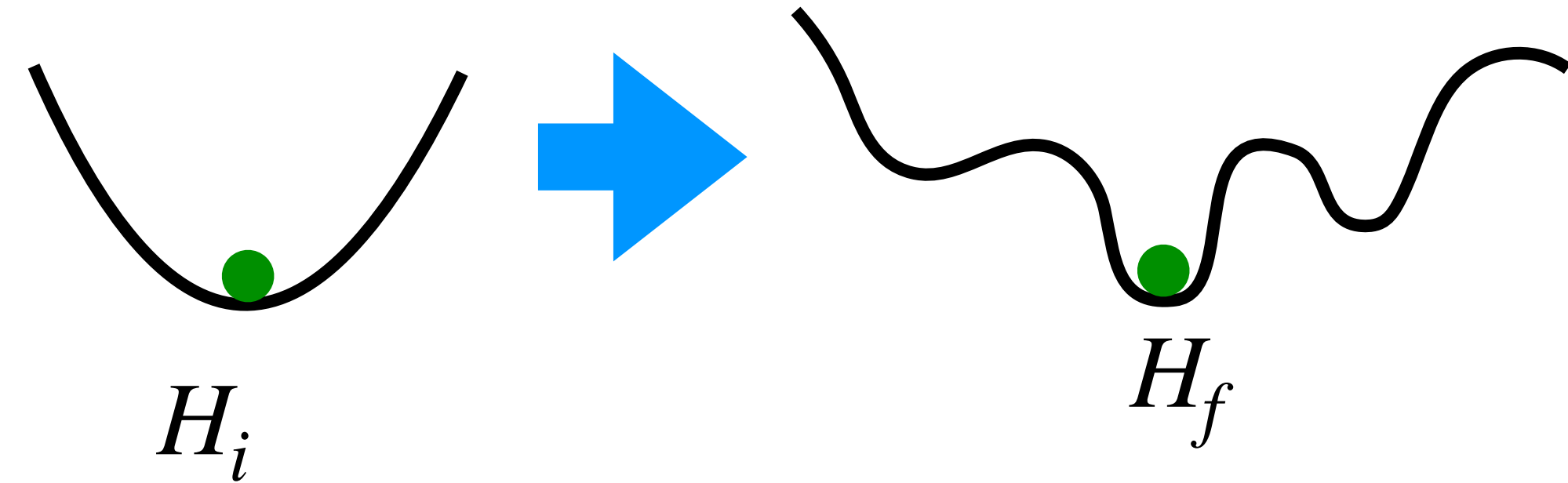
Example Models of Quantum Computing

Circuit-based QC

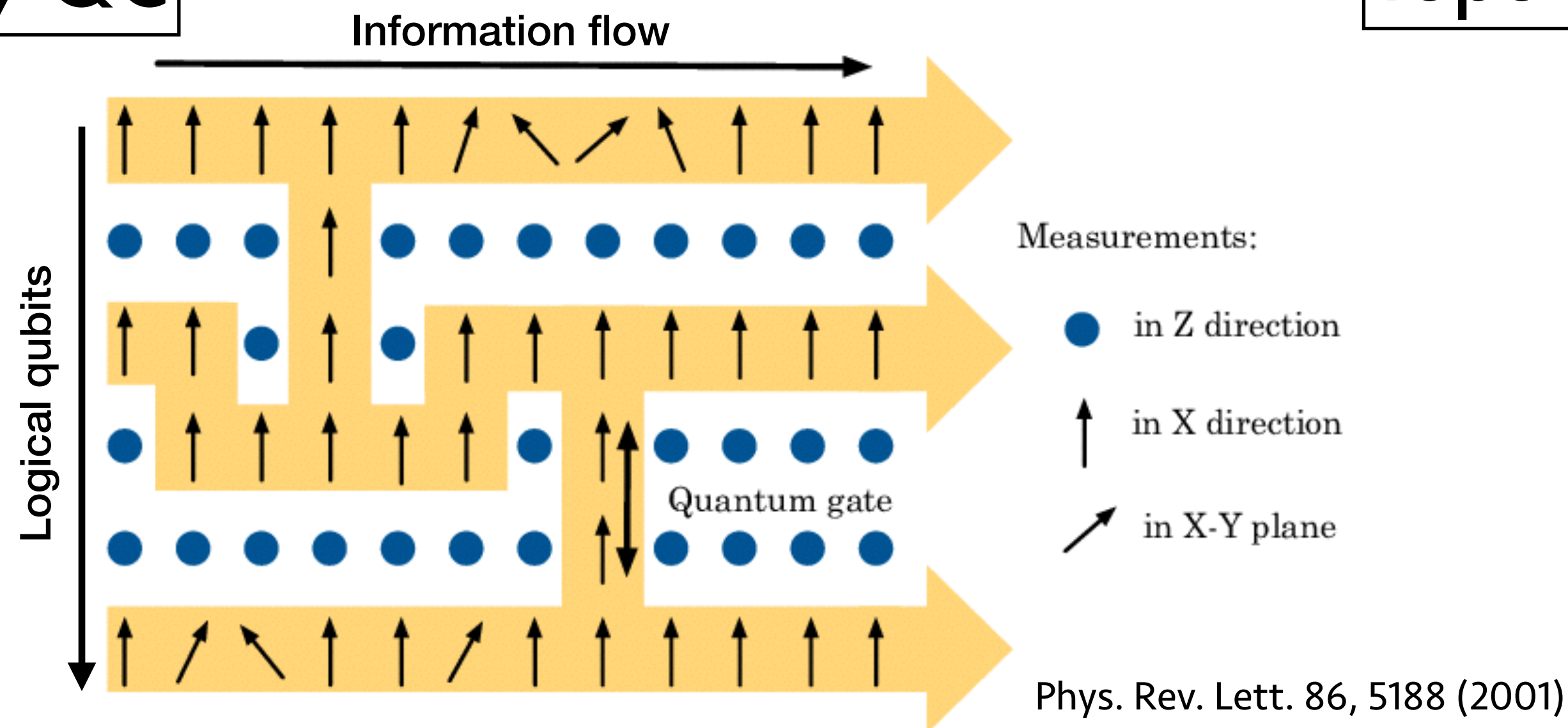


Adiabatic QC

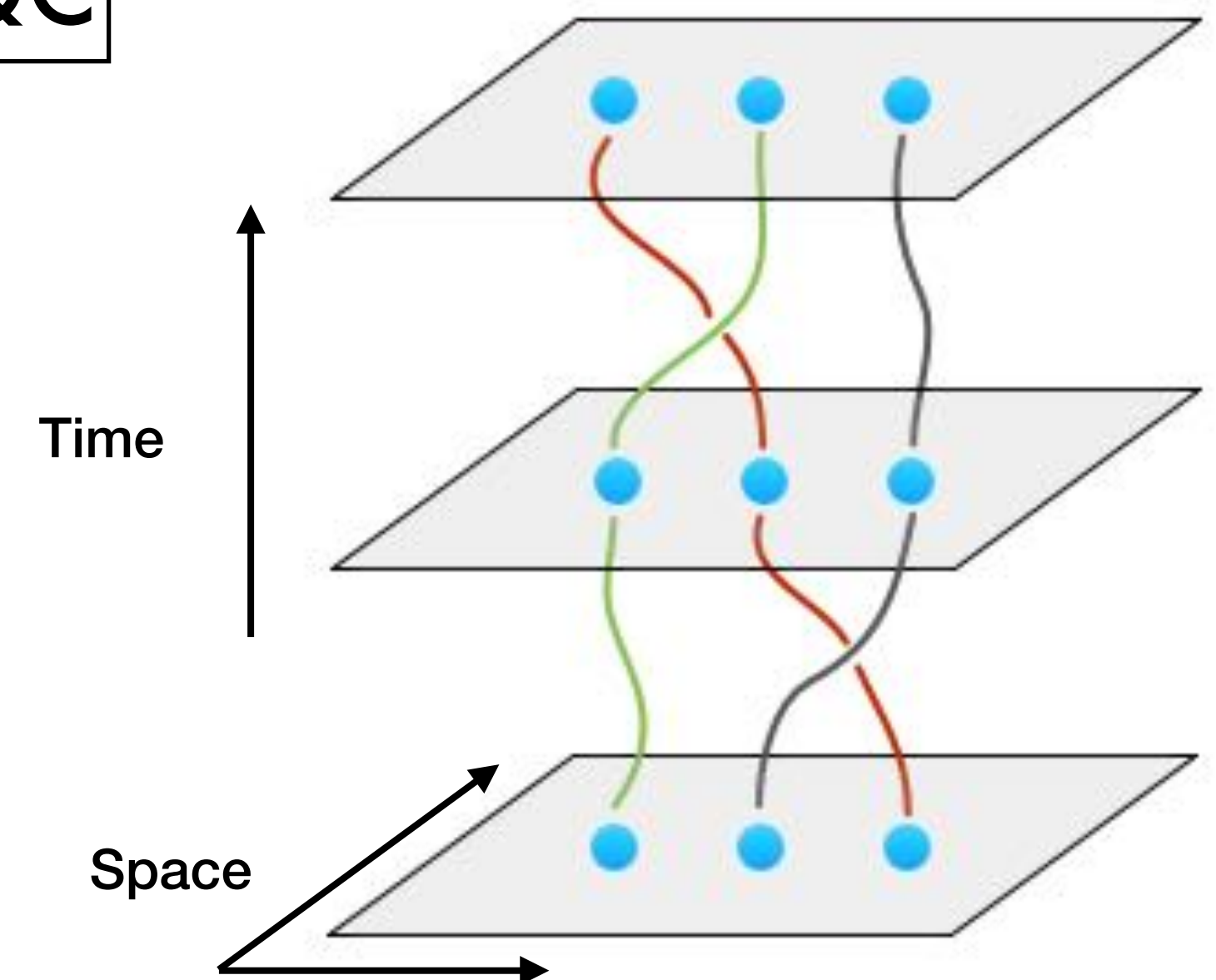
$$H(t) = (1 - t)H_i + tH_f$$



1-way QC



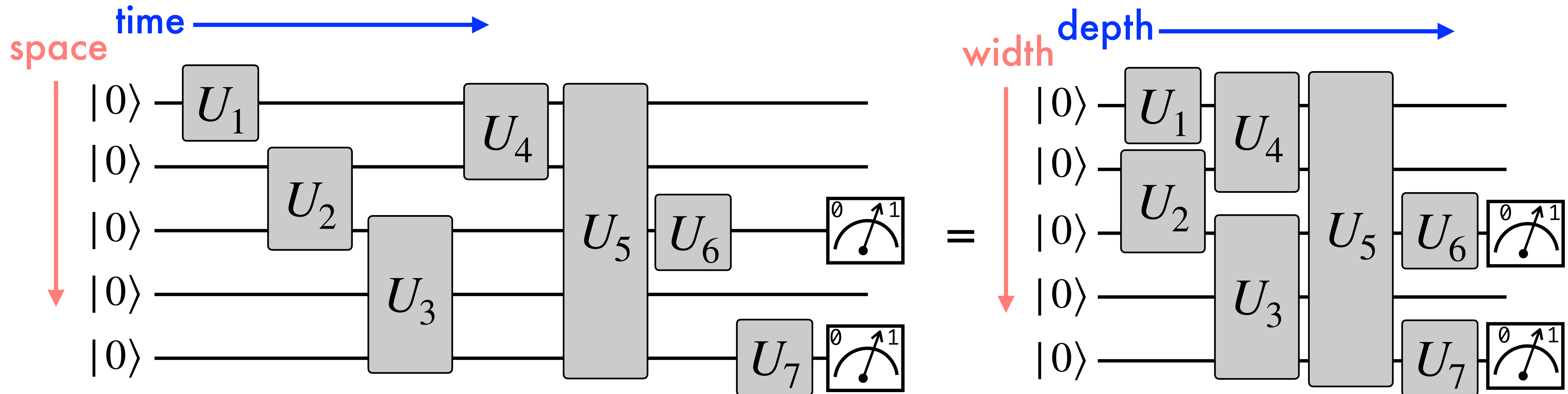
Topological QC



Elements of Quantum Circuit



- Quantum circuit: a reversible acyclic circuit of quantum 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.

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

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \boxed{X} \text{---} \end{array} = \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \oplus \text{---} \end{array}$$

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \boxed{Z} \text{---} \end{array} = \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \text{---} \bullet \text{---} \end{array}$$

No Cloning

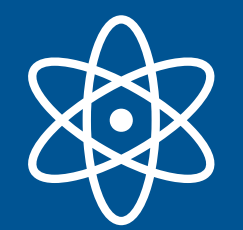
- Is it possible to copy an unknown quantum state?
- The answer is...NO! (due to the linearity of QM)



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

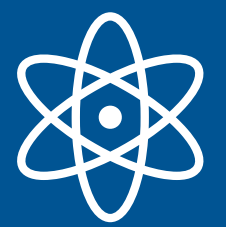
$$\begin{aligned} \text{Let } |\psi\rangle = \alpha |\phi_1\rangle + \beta |\phi_2\rangle \quad \longrightarrow \quad U_{copy} |\psi\rangle |0\rangle &= \alpha U_{copy} |\phi_1\rangle |0\rangle + \beta U_{copy} |\phi_2\rangle |0\rangle \\ &= \alpha |\phi_1\rangle |\phi_1\rangle + \beta |\phi_2\rangle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

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



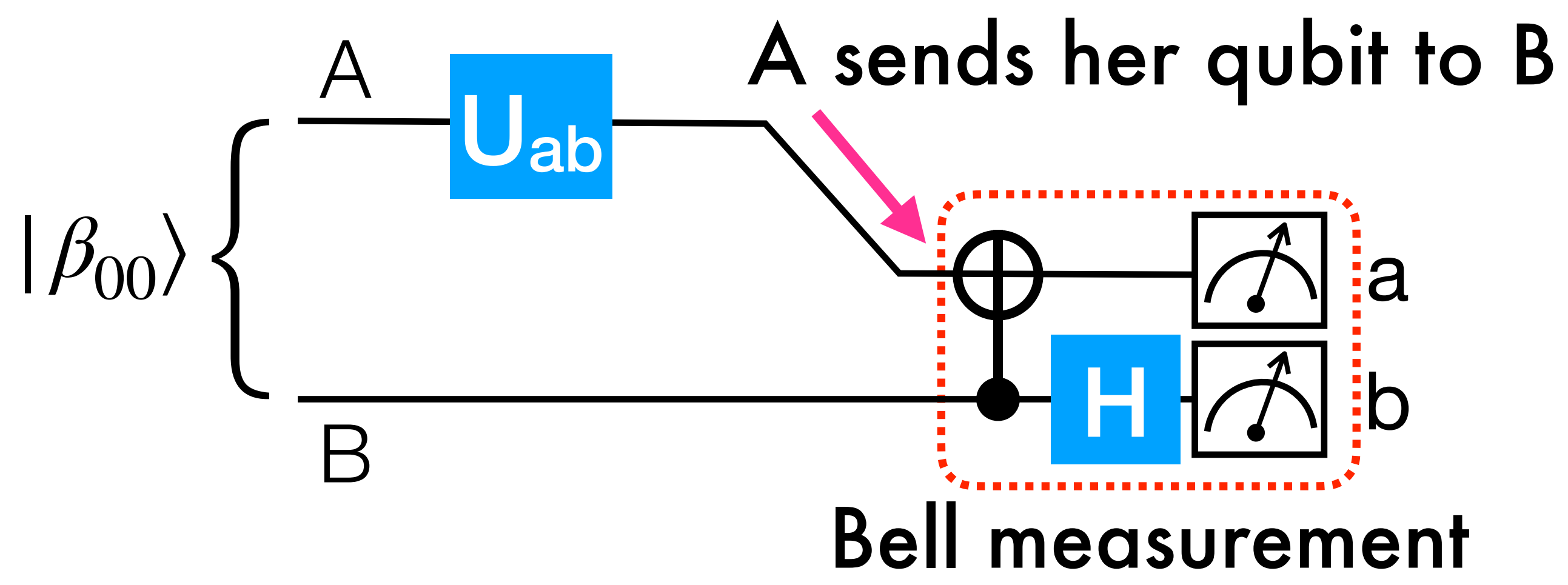
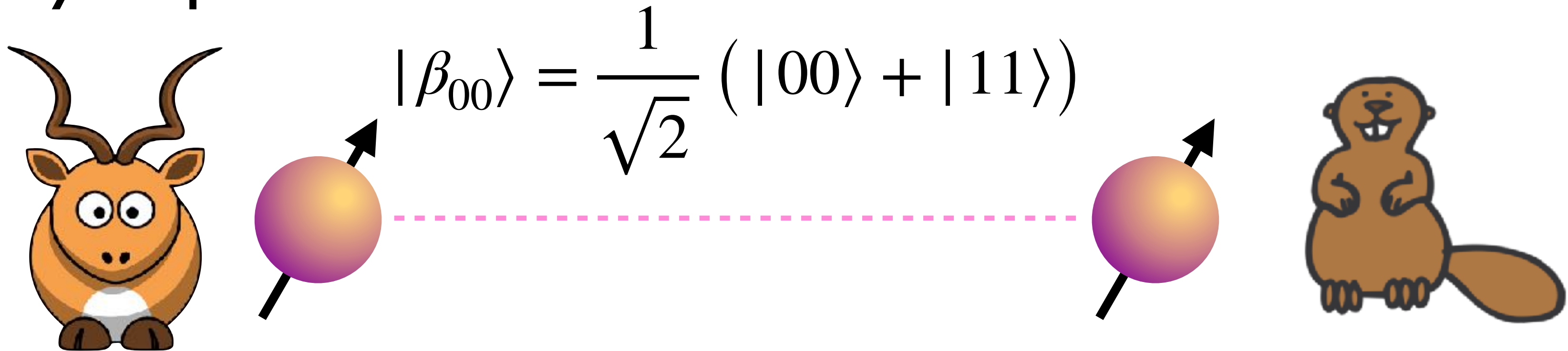
Elementary Q. Protocol: Superdense Coding

- 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!

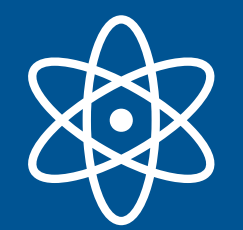


Elementary Q. Protocol: Superdense Coding

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

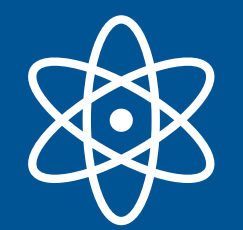


U_{ab}	B receives	B measures
I	$(00\rangle + 11\rangle)/\sqrt{2}$	00
X	$(01\rangle + 10\rangle)/\sqrt{2}$	01
Z	$(00\rangle - 11\rangle)/\sqrt{2}$	10
ZX	$(01\rangle - 10\rangle)/\sqrt{2}$	11



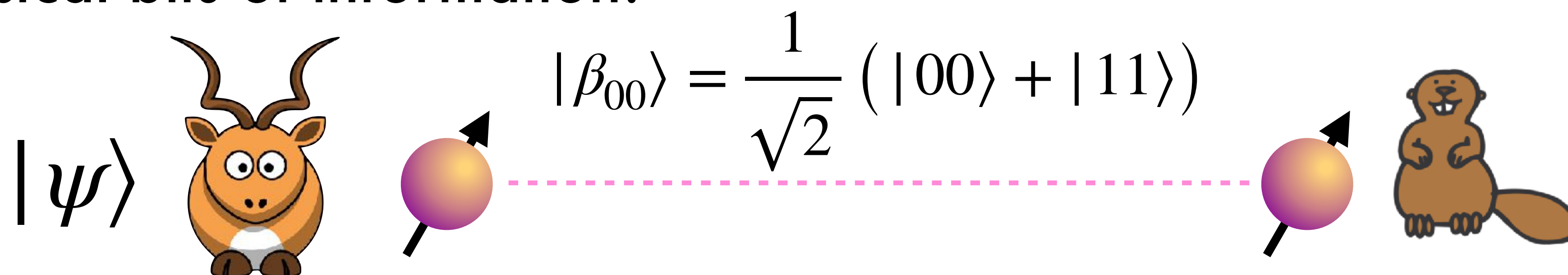
Elementary Q. Protocol: Quantum Teleportation

- 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!

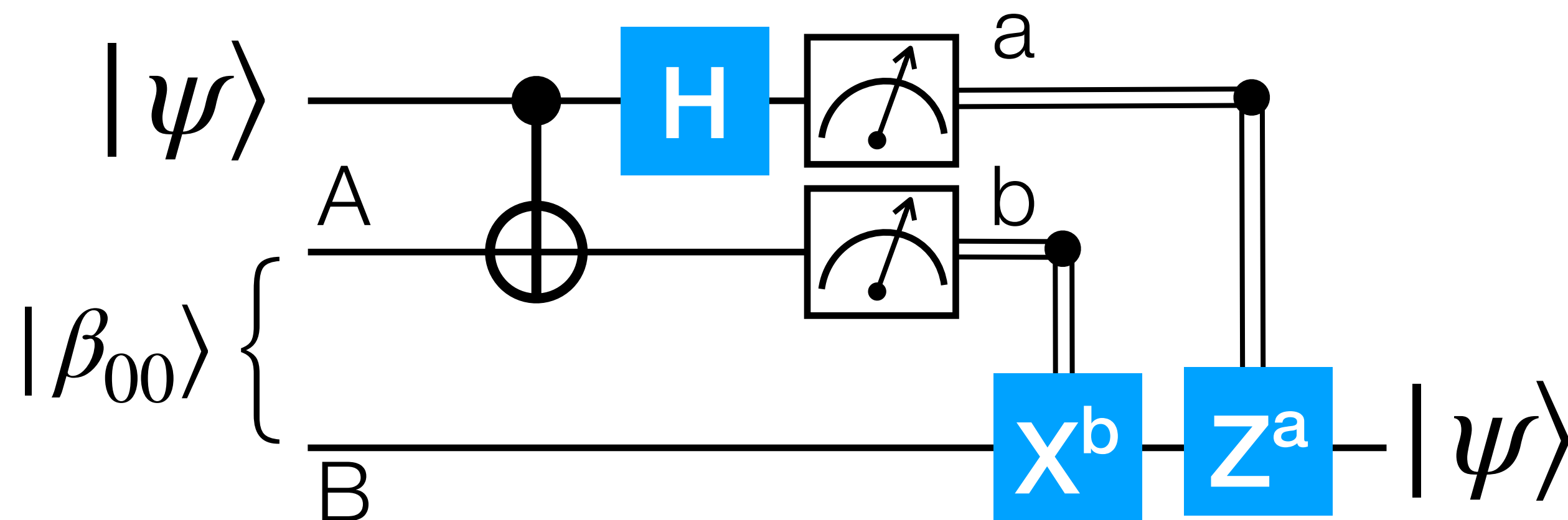


$$|\psi\rangle |\beta_{00}\rangle = (|\beta_{00}\rangle |\psi\rangle + |\beta_{01}\rangle X |\psi\rangle + |\beta_{10}\rangle Z |\psi\rangle + |\beta_{11}\rangle XZ |\psi\rangle) / 2$$

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

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

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



Quantum Mechanics for Computing

1 qubit

$$\alpha_1 |0\rangle$$

$$\alpha_2 |1\rangle$$

2 qubits

$$\alpha_1 |00\rangle$$

$$\alpha_2 |01\rangle$$

$$\alpha_3 |10\rangle$$

$$\alpha_4 |11\rangle$$

3 qubits

$$\alpha_1 |000\rangle \quad \alpha_2 |001\rangle \quad \alpha_3 |010\rangle \quad \alpha_4 |011\rangle \quad \alpha_5 |100\rangle \quad \alpha_6 |101\rangle \quad \alpha_7 |110\rangle \quad \alpha_8 |111\rangle$$

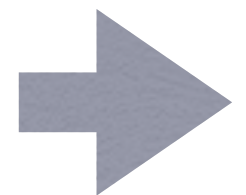
\vdots

\vdots

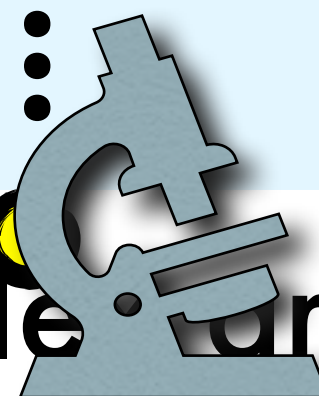
\vdots

\vdots

70 qubits



Process $\sim 10^9$ amplitudes in parallel



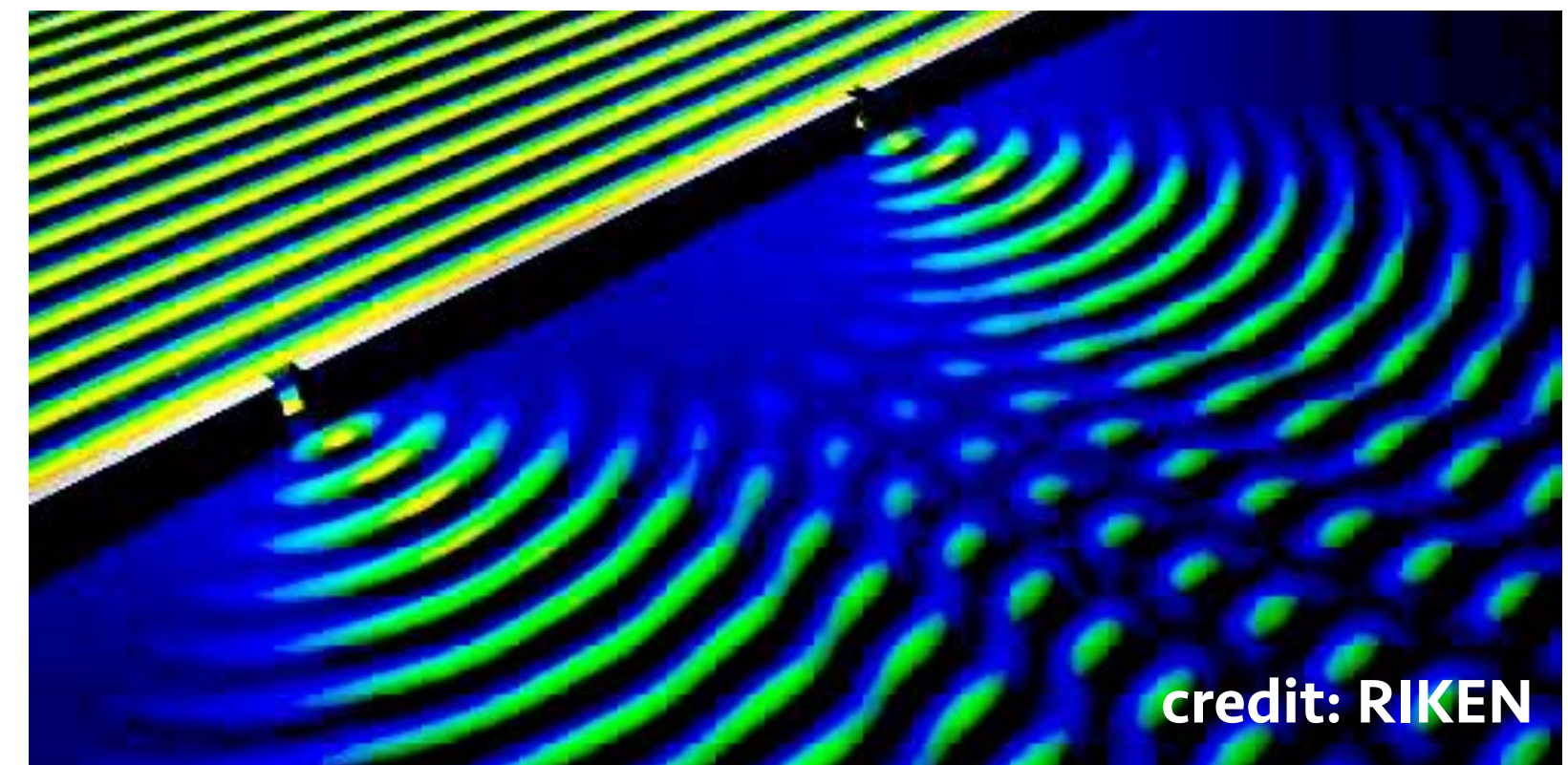
$\rightarrow \sim 10^9$ terabytes

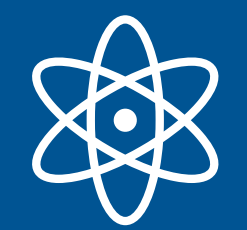
But there is an enemy...

Measurement destroys quantum superposition!



SOLUTION: Quantum Interference!





Elementary Q. Algorithm: The Deutsch-Jozsa Problem

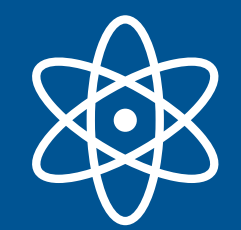
Input: A black-box for computing an unknown function $f : \{0,1\}^n \rightarrow \{0,1\}$.

Promise: f is either a constant or a balanced function.

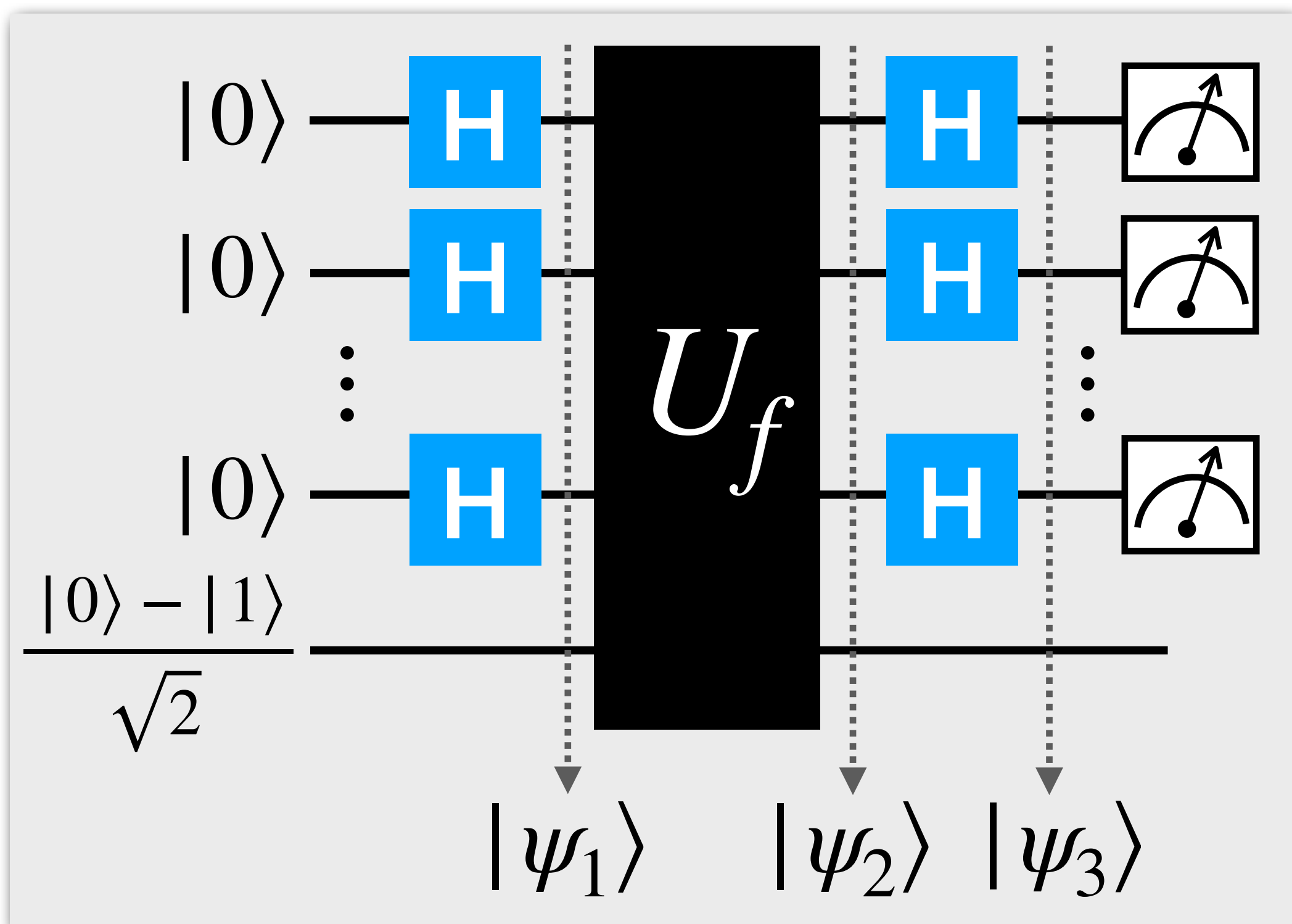
- Constant: $f(x)$ is the same for all $x \in \{0, 1\}^n$.
- Balanced: $f(x) = 0$ for $1/2$ of the input strings, and $f(x) = 1$ otherwise.

Problem: Determine whether f is constant or balanced by making queries to f .

- Classical: Try more than $1/2$ of all possible input $\Rightarrow 2^{n-1} + 1$ queries.
- Quantum: 1 query will solve the problem.



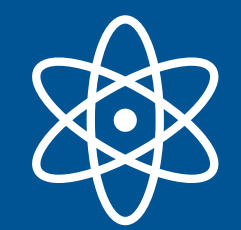
Elementary Q. Algorithm: The Deutsch-Jozsa Problem



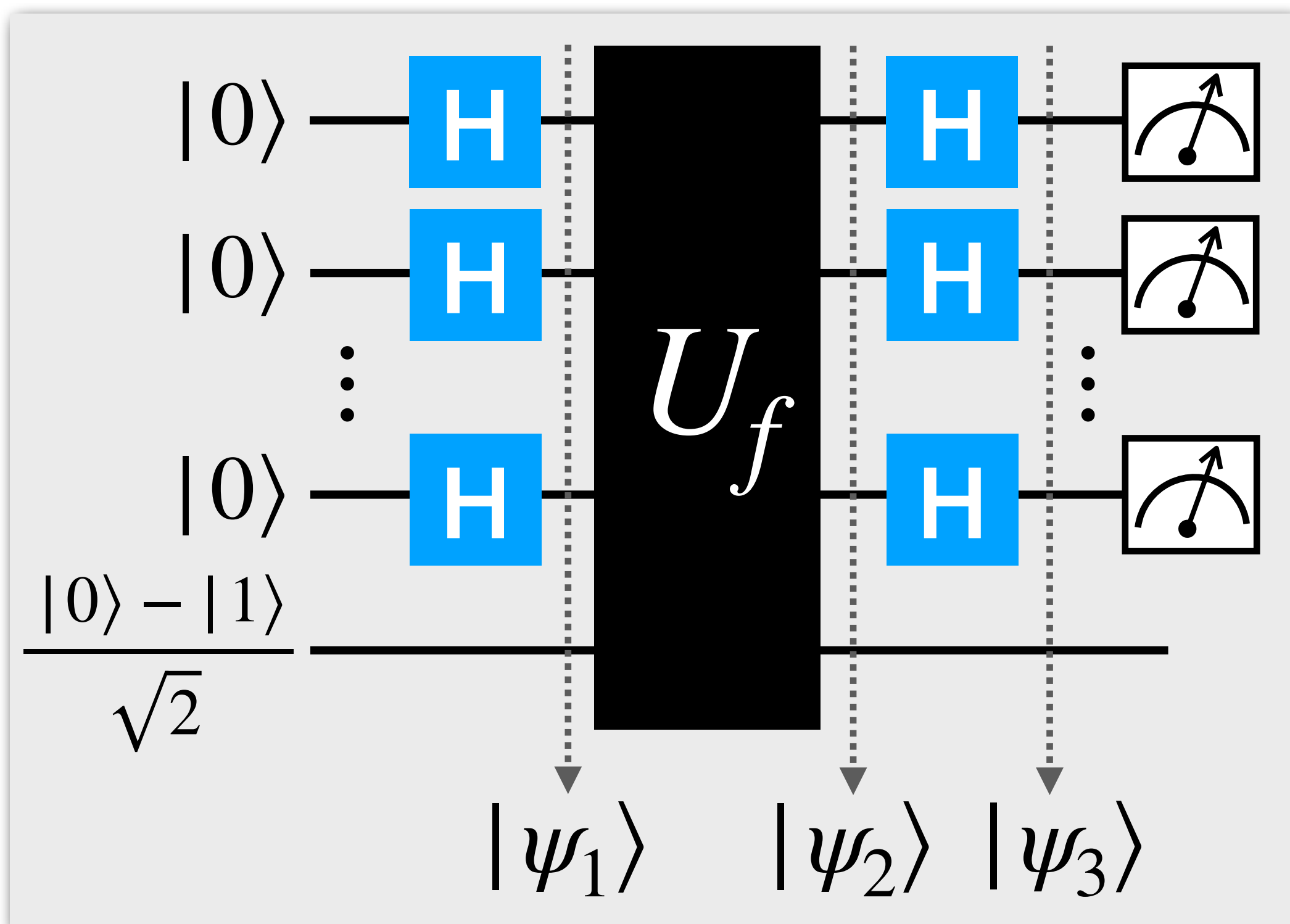
$$H^{\otimes n} |0\rangle^{\otimes n} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

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

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



Elementary Q. Algorithm: The Deutsch-Jozsa Problem



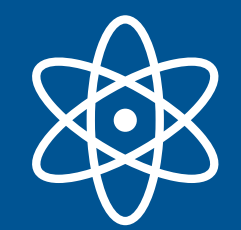
Recall $f(x) \in \{0,1\}$

$$|x\rangle \left(\frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \right) = \overset{\text{phase kick-back}}{(-1)^{f(x)}} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

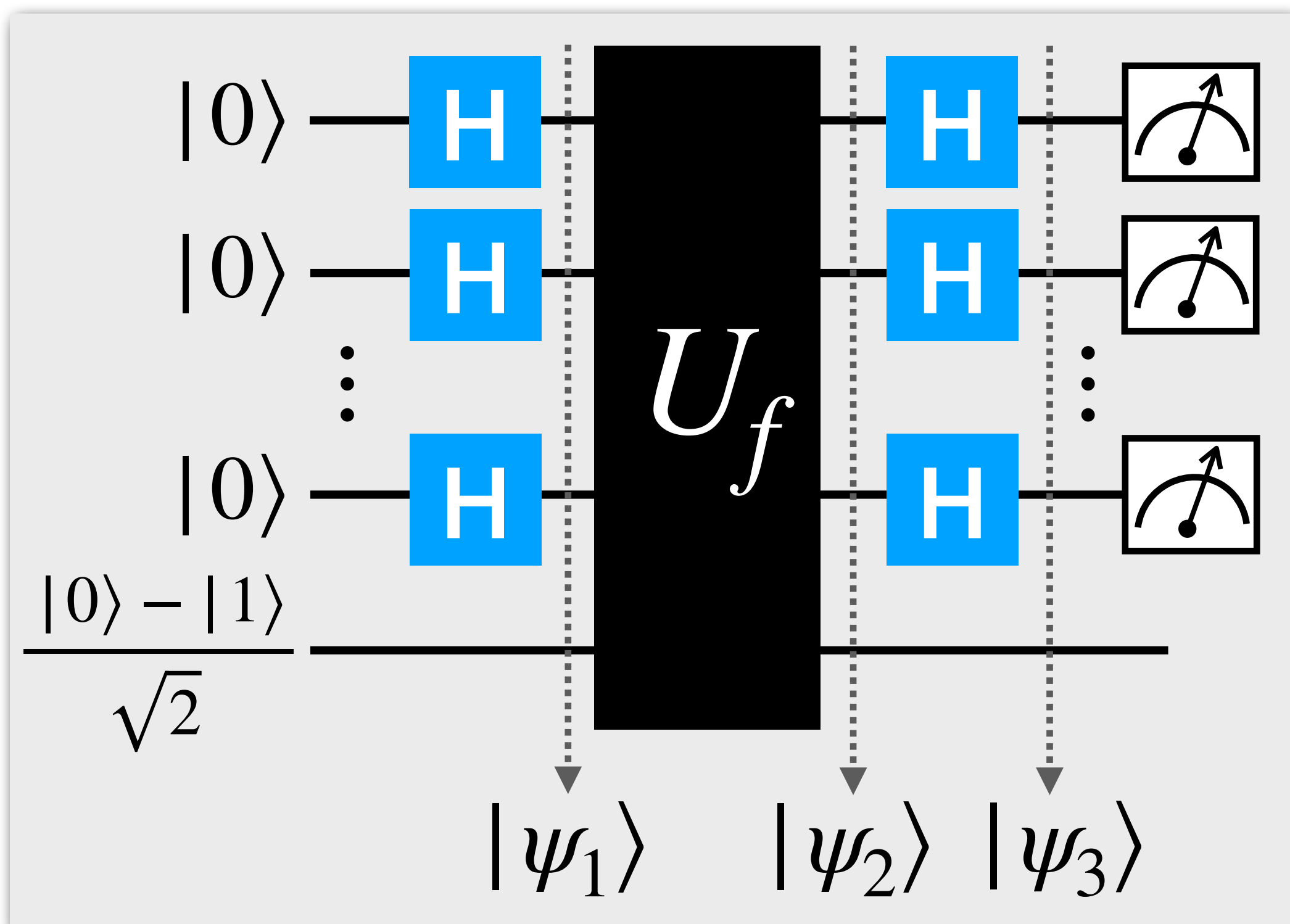
$$\therefore |\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

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

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



Elementary Q. Algorithm: The Deutsch-Jozsa Problem



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

Measure

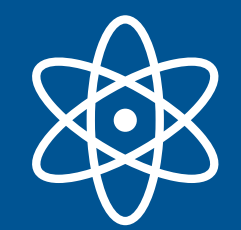
Consider $|z\rangle = |0\rangle^{\otimes n}$

The amplitude is $\alpha_0 = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}$

If $f(x)$ is **constant**, $\alpha_0 = +1$ or $\alpha_0 = -1$. Therefore, $|\alpha_0|^2 = 1$.

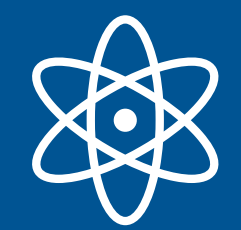
If $f(x)$ is **balanced**, $1/2$ of the terms are $+1$ and $1/2$ are -1 . Therefore, $|\alpha_0|^2 = 0$.

Therefore, the Deutsch-Jozsa problem can be solved with 1 query!



The Deutsch-Jozsa Problem: Summary & Remarks

- The goal was not to learn the unknown function itself, but to learn its property, i.e. constant or balanced.
- Deterministic classical algorithm requires $2^{n-1} + 1$ queries in the worst case.
- Quantum algorithm solves the problem with only 1 query:
Quantum superposition & constructive or destructive interference.
- For probabilistic classical algorithm, the error probability can be reduced to 2^{-n} with only $n + 1$ queries. Thus, for a constant success probability, only a constant number of queries is required.



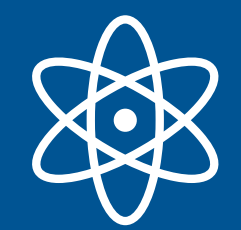
Elementary Q. Algorithm: Simon's Problem

Input: A black-box for computing an unknown function $f: \{0,1\}^n \rightarrow \{0,1\}^m$.

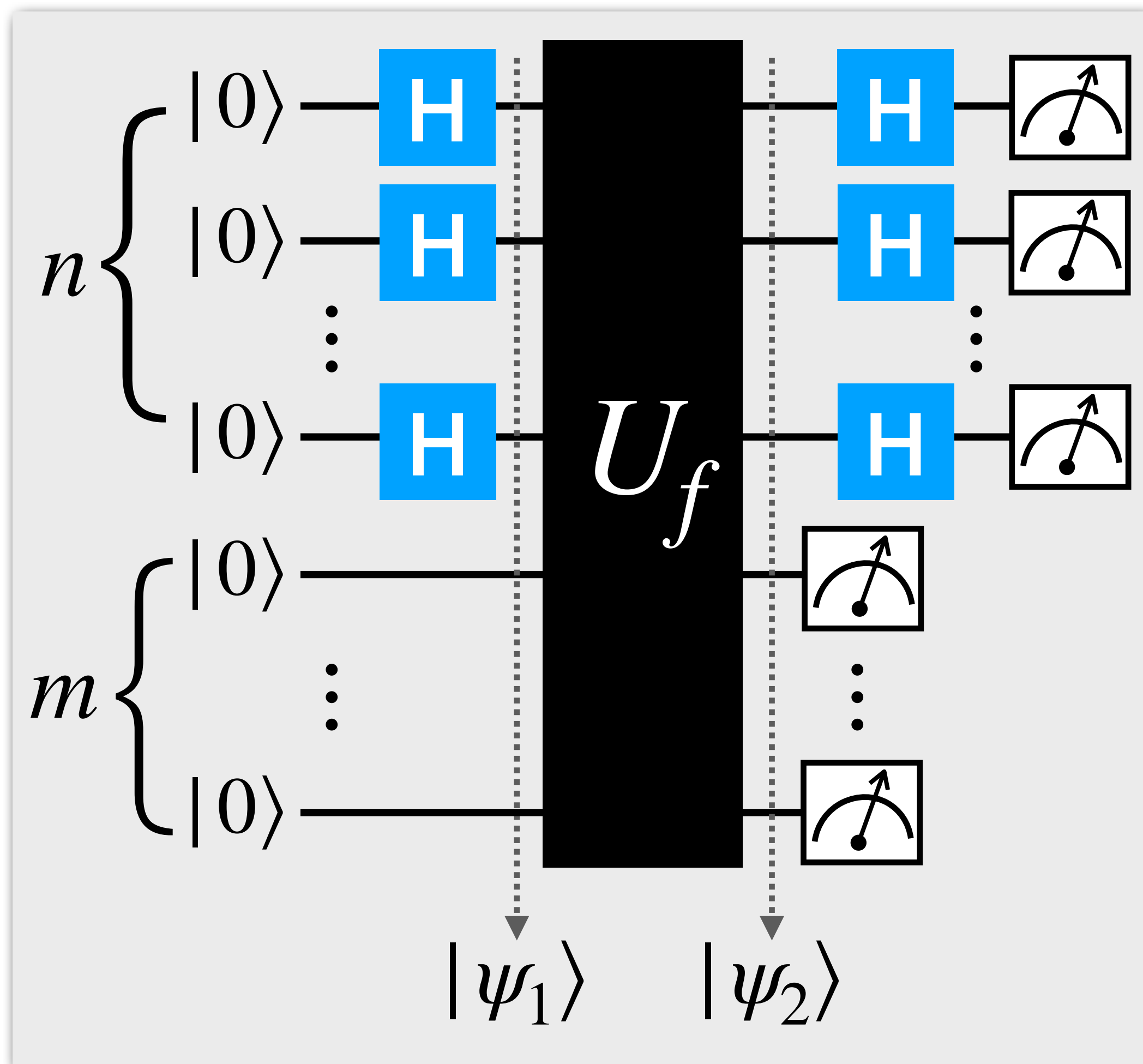
Promise: There is some $s \in \{0, 1\}^n$ such that $f(x) = f(x')$ iff $x = x' \oplus s$.

Problem: Determine s by making queries to f .

- Classical algorithm: Query a random x , repeat until we find $x_i \neq x_j$ such that $f(x_i) = f(x_j)$. Output $x_i \oplus x_j$.
- This uses about $\sqrt{2^n}$ queries.
- Quantum algorithm: Query many times & post process



Elementary Q. Algorithm: Simon's Problem



$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$

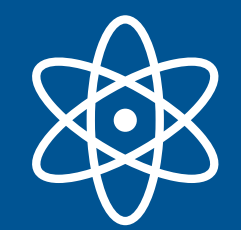
$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |0\rangle^{\otimes m}$$

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

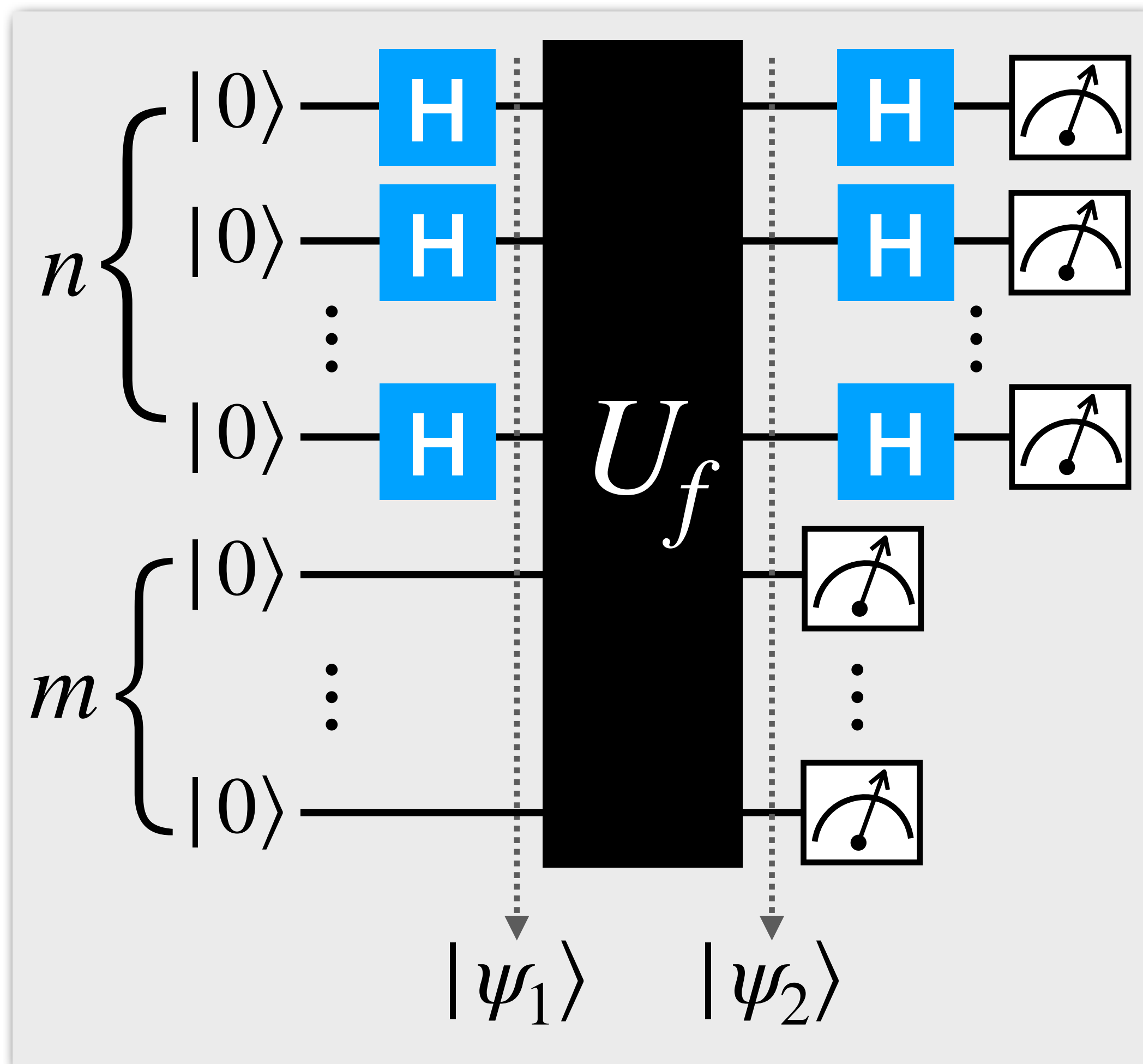
$$= \frac{1}{\sqrt{2^{n-1}}} \sum_{x \in \Gamma} \frac{|x\rangle + |x \oplus s\rangle}{\sqrt{2}} \otimes |f(x)\rangle^{\otimes m},$$

where $\Gamma \subset \{0,1\}^n$

After measuring the second registers $|\psi_2\rangle \rightarrow \frac{|x\rangle + |x \oplus s\rangle}{\sqrt{2}} \otimes |f(x)\rangle^{\otimes m}$

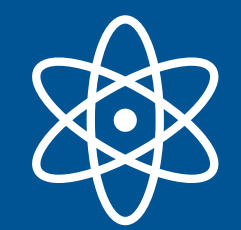


Elementary Q. Algorithm: Simon's Problem

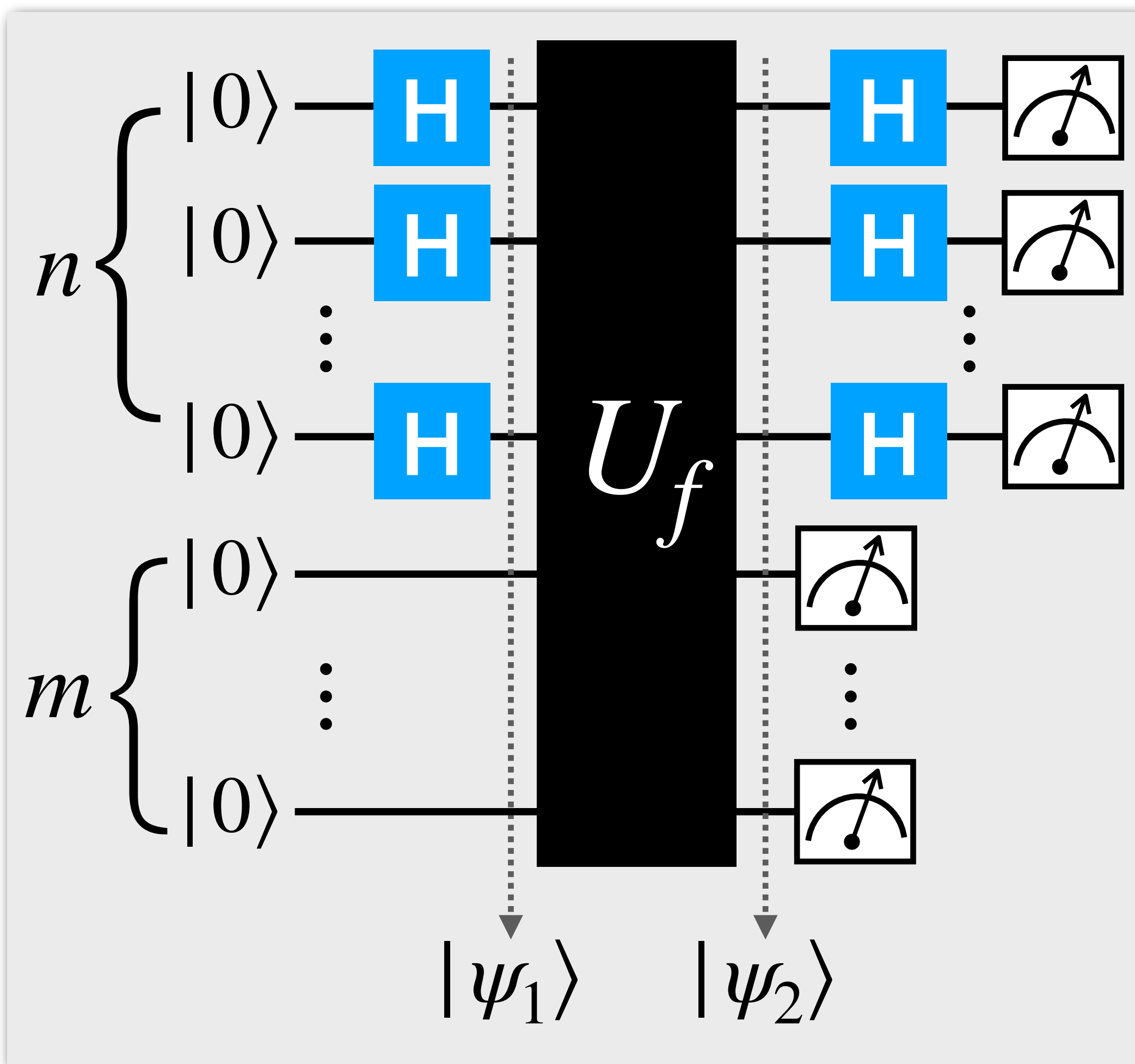


$$\begin{aligned} & H^{\otimes n} \left(\frac{|x\rangle + |x \oplus s\rangle}{\sqrt{2}} \right) \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{z \in \{0,1\}^n} \left[(-1)^{x \cdot z} + (-1)^{(x \oplus s) \cdot z} \right] |z\rangle \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} \underbrace{\left[1 + (-1)^{s \cdot z} \right]}_{\text{Non-zero only when } s \cdot z = 0} |z\rangle \end{aligned}$$

Measurement gives a random z orthogonal to s (i.e. $z \cdot s = 0$)



Elementary Q. Algorithm: Simon's Problem



A random z orthogonal to s (i.e. $z \cdot s = 0$)

1. Repeat k times and get $z_1, z_2, \dots, z_k \in \{0,1\}^n$.
2. Solve a system of k linear equations for s :

$$z_1 \cdot s = 0, \quad z_2 \cdot s = 0, \quad \dots, \quad z_k \cdot s = 0$$

- $k = O(n)$ suffices to provide a unique solution with a high (constant) probability.

$O(n)$ queries & $O(n^3)$ for post-processing

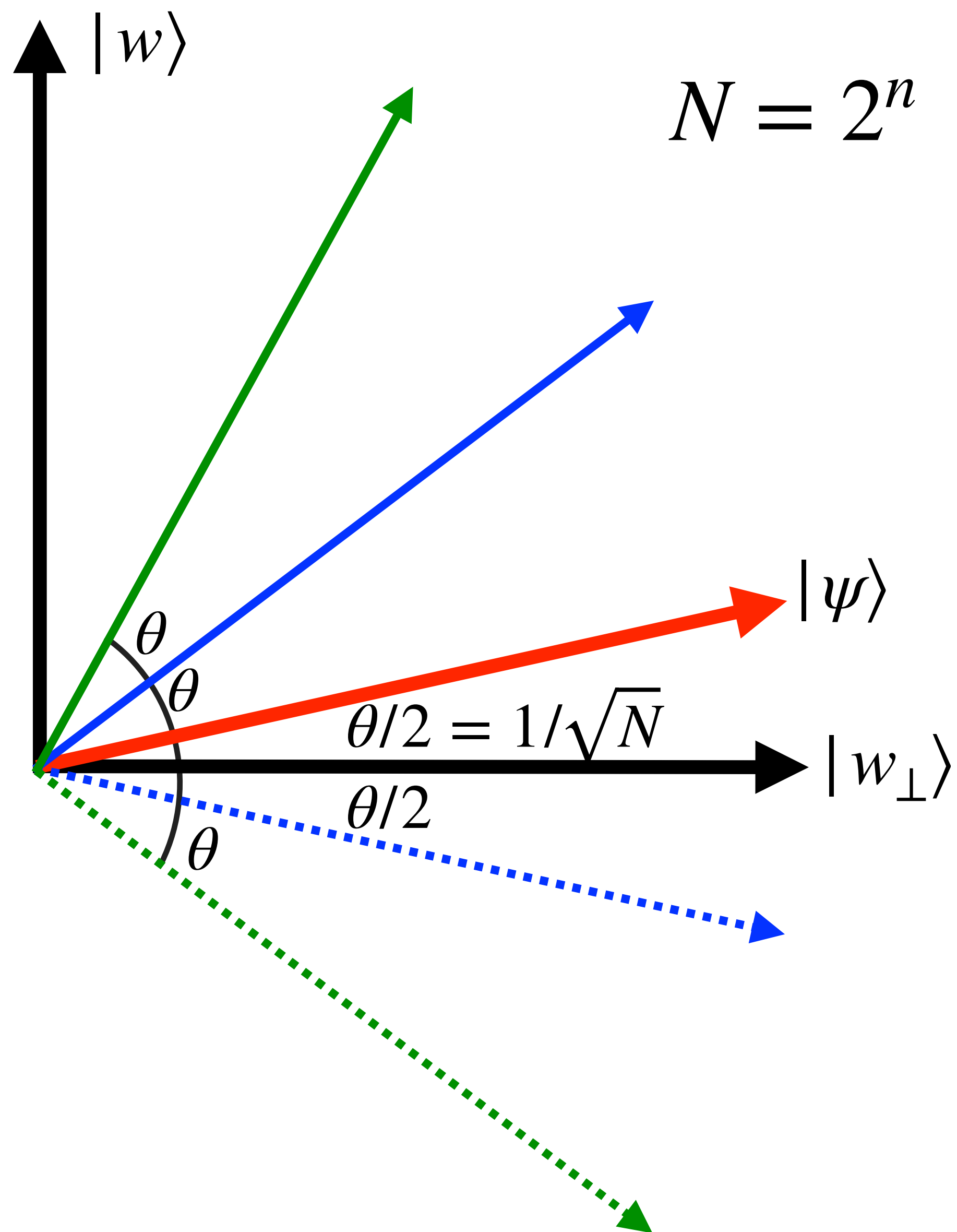
Grover's Search Algorithm

Input: A black-box U_f for computing an unknown function $f: \{0,1\}^n \rightarrow \{0,1\}$.

Problem: Find an input $x \in \{0,1\}^n$ such that $f(x) = 1$ (without loss of generality, assume there's exactly one solution $x = w$).

- There's no structure in the problem. Thus, classically, with k queries, the success probability is $\frac{k+1}{2^n}$.
- Quantum computer can perform **quadratically** faster.

Grover's Search Algorithm



$$N = 2^n$$

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = \sqrt{\frac{N-1}{N}} |w_{\perp}\rangle + \sqrt{\frac{1}{N}} |w\rangle$$

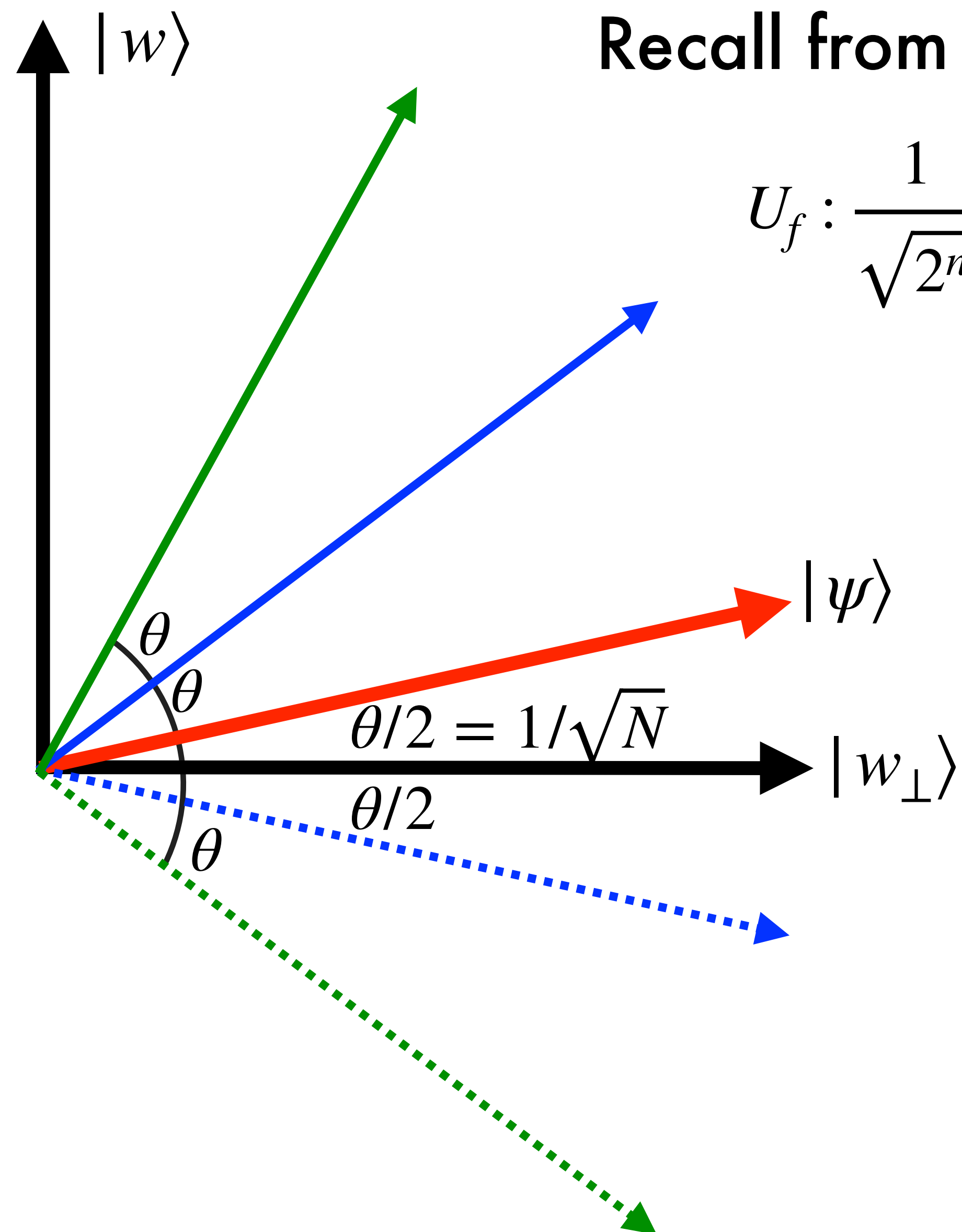
- Reflection around $|w_{\perp}\rangle$: $U_f = I - 2|w\rangle\langle w|$.
- Reflection around $|\psi\rangle$: $V = 2|\psi\rangle\langle\psi| - I$.
- The product of two reflections is a rotation. Thus the state remains in this plane.

$$(VU_f)^k |\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right) |w_{\perp}\rangle + \sin\left(\frac{2k+1}{2}\theta\right) |w\rangle$$

$$\sin\left(\frac{2k+1}{2}\theta\right) \approx 1 \rightarrow \frac{2k+1}{2}\theta \approx \pi/2$$

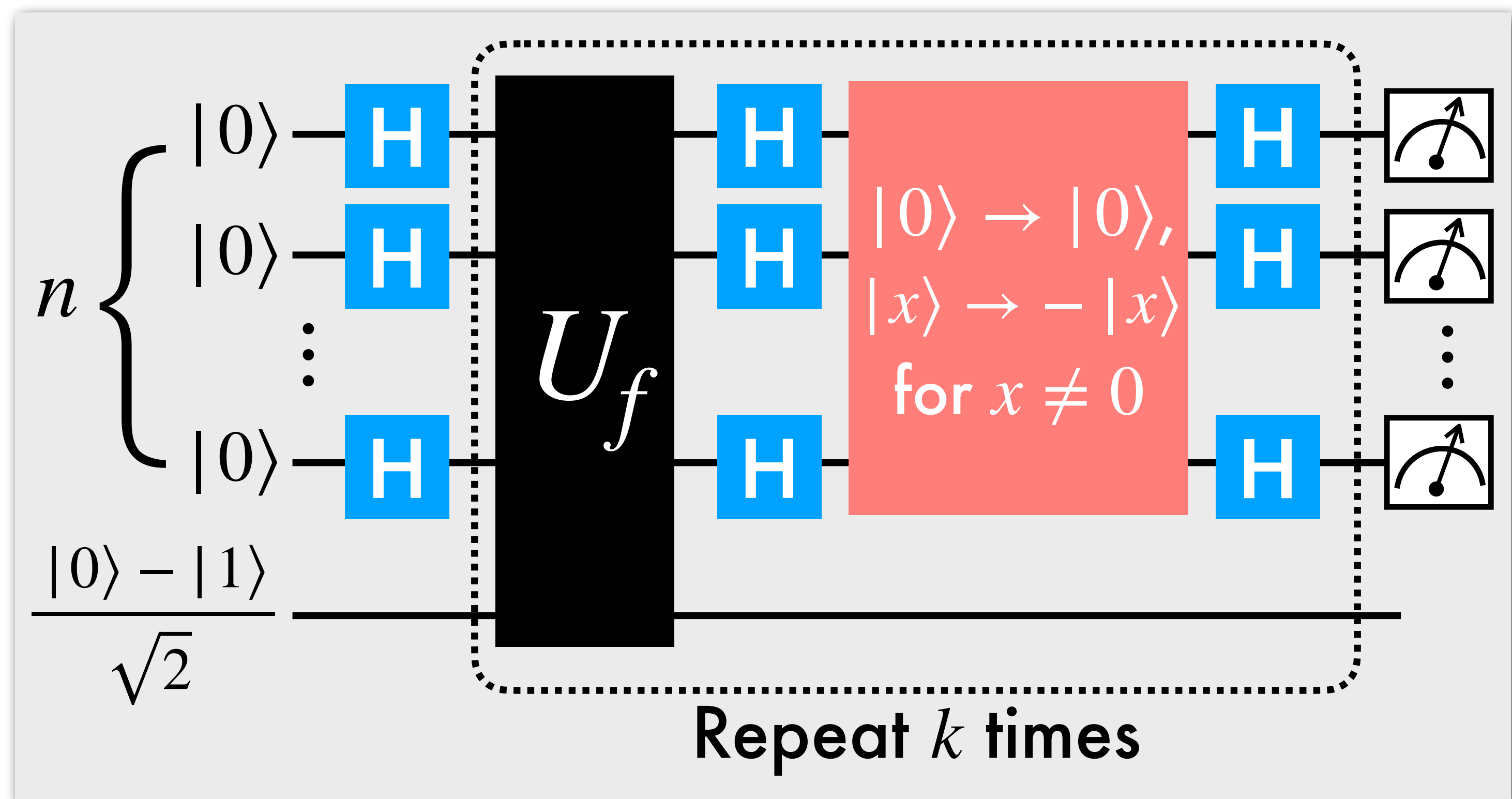
$$\rightarrow k = O(\sqrt{N})$$

Grover's Search Algorithm



Recall from Deutsch-Jozsa algorithm: $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$

$$U_f : \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \rightarrow \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$



- **Elementary quantum protocols:**
 - Quantum entanglement provides the advantage.
- **Quantum Algorithms:**
 - Given a problem with certain structure, engineer quantum interference to achieve quantum speedup.
 - Quadratic speedup can be achieved for unstructured search.