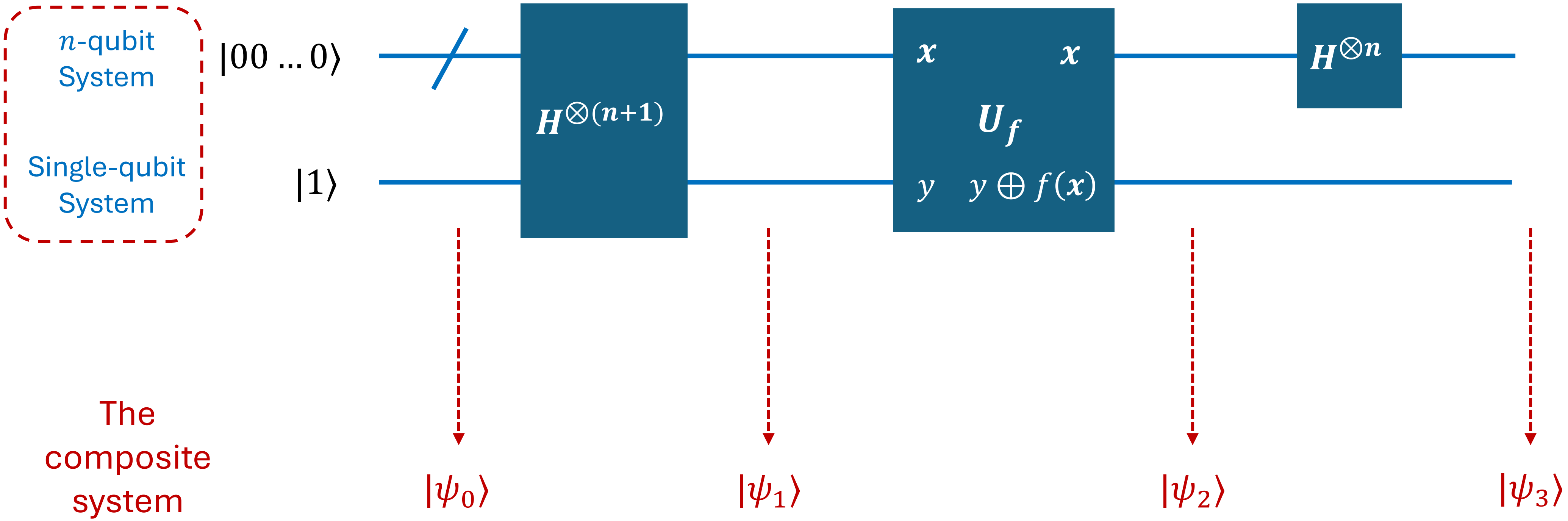
Quantum Computing

- Lectures 6 and 7 (May 21-22, 2025)

- Today:
  - Continue the Deutsch-Jozsa algorithm
  - Postulates of Quantum Computing

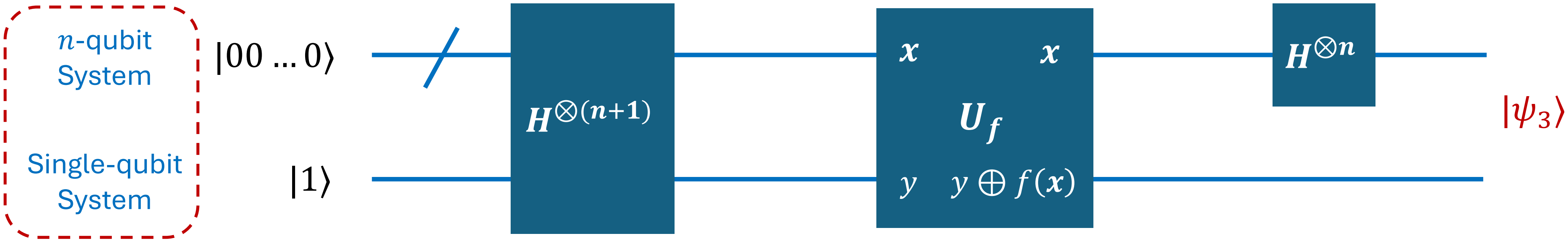
The Deutsch-Jozsa Algorithm

- Let $f: \{0,1\}^n \rightarrow \{0,1\}$ be a bit function…
- (Do it on the board)



The Deutsch-Jozsa Algorithm

- Let $f: \{0,1\}^n \to \{0,1\}$ be a bit function…
- (Do it on the board)

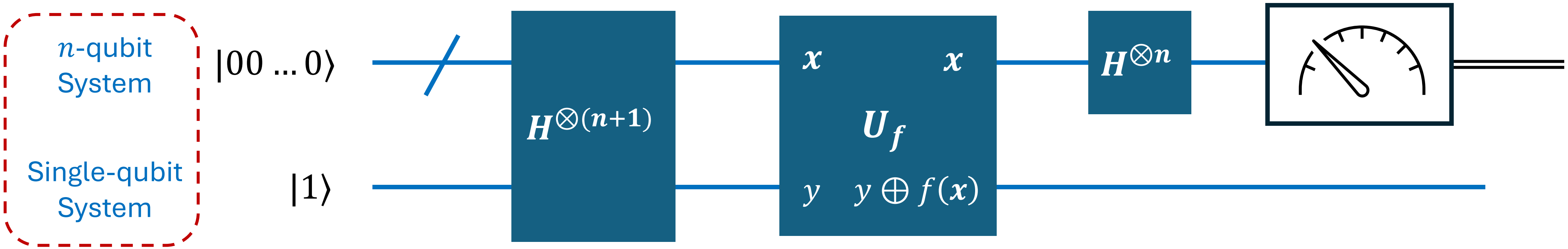


The composite system

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

The Deutsch-Jozsa Algorithm

- Let $f: \{0,1\}^n \to \{0,1\}$ be a bit function…
- (Do it on the board)



The composite system

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

Measure the first n systems ?

The Deutsch-Jozsa Algorithm

$$|\psi_3\rangle = \left(\sum_{\boldsymbol{z} \in \{0,1\}^n} \sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{\boldsymbol{x}^T \boldsymbol{z} + f(\boldsymbol{x})} |\boldsymbol{z}\rangle}{2^n} \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{\text{Measure the first } n\text{-qubit system}} \boldsymbol{z}$$

- What's the probability of $\boldsymbol{z} = 00 \dots 0$? What about $\boldsymbol{z} \neq 00 \dots 0$?

The Deutsch-Jozsa Algorithm

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

Measure the first n-qubit system $\Longrightarrow$ z

$$\sum_{x \in \{0,1\}^n} \frac{(-1)^{x^T z + f(x)}}{2^n}$$

- What's the probability of $z = 00 \dots 0$? What about $z \neq 00 \dots 0$?

The Deutsch-Jozsa Algorithm

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

Measure the first n-qubit system $\Longrightarrow$ z

- What's the probability of $z = 00 \ldots 0$? What about $z \neq 00 \ldots 0$?

$$\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}}{2^n} \qquad \sum_{x \in \{0,1\}^n} \frac{(-1)^{x^T z + f(x)}}{2^n}$$

The Deutsch-Jozsa Algorithm

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

Measure the first n-qubit system $\Longrightarrow$ $\boldsymbol{z}$

- What's the probability of $\boldsymbol{z} = 00 \ldots 0$? What about $\boldsymbol{z} \neq 00 \ldots 0$?

$$\sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{f(\boldsymbol{x})}}{2^n} \qquad \sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{\boldsymbol{x}^T \boldsymbol{z} + f(\boldsymbol{x})}}{2^n}$$

- What if f is a *constant* function: $\forall \boldsymbol{x} \in \{0,1\}^n, f(\boldsymbol{x}) = 0$? Or $f(\boldsymbol{x}) = 1$?

- What if f is a *balanced* function: $\sum_{\boldsymbol{x} \in \{0,1\}^n} f(\boldsymbol{x}) = \mathbf{2^{n-1}}$

The Deutsch-Jozsa Algorithm

$$|\psi_3\rangle = \left(\sum_{\boldsymbol{z} \in \{0,1\}^n} \sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{\boldsymbol{x}^T \boldsymbol{z} + f(\boldsymbol{x})} |\boldsymbol{z}\rangle}{2^n}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{\text{Measure the first } n\text{-qubit system}} \boldsymbol{z}$$

- What's the probability of $\boldsymbol{z} = 00 \dots 0$? What about $\boldsymbol{z} \neq 00 \dots 0$?

$$\sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{f(\boldsymbol{x})}}{2^n} \qquad \sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{\boldsymbol{x}^T \boldsymbol{z} + f(\boldsymbol{x})}}{2^n}$$

Case $\boldsymbol{z} = 00 \dots 0$:

- What if f is a *constant* function: $\forall \boldsymbol{x} \in \{0,1\}^n, f(\boldsymbol{x}) = 0$? Or $f(\boldsymbol{x}) = 1$?

$\sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{f(\boldsymbol{x})}}{2^n} = 1$ or -1

- What if f is a *balanced* function: $\sum_{\boldsymbol{x} \in \{0,1\}^n} f(\boldsymbol{x}) = \mathbf{2^{n-1}}$

The Deutsch-Jozsa Algorithm

$$|\psi_3\rangle = \left(\sum_{z\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} \frac{(-1)^{x^T z + f(x)} |z\rangle}{2^n} \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow[\text{n-qubit system}]{\text{Measure the first}} z$$

- What's the probability of $z = 00\ldots0$? What about $z \neq 00\ldots0$?

$$\sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}}{2^n} \qquad \sum_{x\in\{0,1\}^n} \frac{(-1)^{x^T z + f(x)}}{2^n}$$

Case $z = 00\ldots0$:

- What if f is a *constant* function: $\forall x \in \{0,1\}^n, f(x) = 0$? Or $f(x) = 1$?

$\sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}}{2^n} = 1$ or -1

- What if f is a *balanced* function: $\sum_{x\in\{0,1\}^n} f(x) = \mathbf{2^{n-1}}$

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

The Deutsch-Jozsa Algorithm

$$|\psi_3\rangle = \left(\sum_{\boldsymbol{z} \in \{0,1\}^n} \sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{\boldsymbol{x}^T\boldsymbol{z}+f(\boldsymbol{x})} |\boldsymbol{z}\rangle}{2^n} \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow[\text{n-qubit system}]{\text{Measure the first}} \boldsymbol{z}$$

- What's the probability of $\boldsymbol{z} = 00 \ldots 0$? What about $\boldsymbol{z} \neq 00 \ldots 0$?

$$\sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{f(\boldsymbol{x})}}{2^n} \qquad \sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{\boldsymbol{x}^T\boldsymbol{z}+f(\boldsymbol{x})}}{2^n}$$

- What if f is a *constant* function: $\forall \boldsymbol{x} \in \{0,1\}^n, f(\boldsymbol{x}) = 0$? Or $f(\boldsymbol{x}) = 1$?
- What if f is a *balanced* function: $\sum_{\boldsymbol{x} \in \{0,1\}^n} f(\boldsymbol{x}) = \boldsymbol{2^{n-1}}$

Case $\boldsymbol{z} \neq 00 \ldots 0$:

$$\sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{\boldsymbol{x}^T\boldsymbol{z}+f(\boldsymbol{x})}}{2^n} = 0$$

$$\sum_{\boldsymbol{x} \in \{0,1\}^n} \frac{(-1)^{\boldsymbol{x}^T\boldsymbol{z}+f(\boldsymbol{x})}}{2^n} \neq 0$$

The Deutsch-Jozsa Algorithm

$$|\psi_3\rangle = \left(\sum_{z \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} \frac{(-1)^{x^T z + f(x)} |z\rangle}{2^n} \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow[]{\text{Measure the first } n\text{-qubit system}} z$$

- What if f is a *constant* function: $\forall x \in \{0,1\}^n, f(x) = 0$? Or $f(x) = 1$?

$$|\psi_3\rangle = \pm|0 \ldots 0\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

- What if f is a *balanced* function: $\sum_{x \in \{0,1\}^n} f(x) = 2^{n-1}$

$$|\psi_3\rangle = \left(\frac{-1}{\sqrt{2^n}} |0 \ldots 0\rangle + (\cdots) \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

The Deutsch-Jozsa Algorithm

$$|\psi_3\rangle = \left(\sum_{z \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} \frac{(-1)^{x^T z + f(x)} |z\rangle}{2^n} \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow[\text{n-qubit system}]{\text{Measure the first}} z$$

- What if f is a *constant* function: $\forall x \in \{0,1\}^n, f(x) = 0$? Or $f(x) = 1$?

$$|\psi_3\rangle = \pm |0 \dots 0\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

The measurement outcome is always $z = 0 \dots 0$

- What if f is a *balanced* function: $\sum_{x \in \{0,1\}^n} f(x) = 2^{n-1}$

$$|\psi_3\rangle = \left(\frac{-1}{\sqrt{2^n}} |0 \dots 0\rangle + (\cdots) \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

The measurement outcome is $z = 0 \dots 0$ with probability $\frac{1}{2^n}$

The Deutsch-Jozsa Problem

- Constant-vs-balanced problem
- Let $f: \{0,1\}^n \rightarrow \{0,1\}$ be a bit function such that it is in either two cases:
  - f is a *constant* function: $\forall \boldsymbol{x} \in \{0,1\}^n, f(\boldsymbol{x})$ is always a constant (0 or 1)
  - f is a *balanced* function: $\sum_{\boldsymbol{x} \in \{0,1\}^n} f(\boldsymbol{x}) = \mathbf{2^{n-1}}$ (i.e., outputs 0 for half the inputs, and 1 for the other half)

- To decide whether f is constant or balanced, **how many times** must we evaluate f?

The Deutsch-Jozsa Problem

- Constant-vs-balanced problem
- Let $f: \{0,1\}^n \rightarrow \{0,1\}$ be a bit function such that it is in either two cases:
  - f is a *constant* function: $\forall \boldsymbol{x} \in \{0,1\}^n, f(\boldsymbol{x})$ is always a constant (0 or 1)
  - f is a *balanced* function: $\sum_{x \in \{0,1\}^n} f(\boldsymbol{x}) = \boldsymbol{2^{n-1}}$ (i.e., outputs 0 for half the inputs, and 1 for the other half)

- To decide whether f is constant or balanced, **how many times** must we evaluate f?

Classical Computer

Worst-case: 2^n

Probabilistic algorithm:

$l \ll 2^n$ times,

with a failure rate of $\frac{1}{2^l}$

The Deutsch-Jozsa Problem

- Constant-vs-balanced problem
- Let $f: \{0,1\}^n \rightarrow \{0,1\}$ be a bit function such that it is in either two cases:
  - f is a *constant* function: $\forall \boldsymbol{x} \in \{0,1\}^n, f(\boldsymbol{x})$ is always a constant (0 or 1)
  - f is a *balanced* function: $\sum_{x \in \{0,1\}^n} f(\boldsymbol{x}) = \mathbf{2^{n-1}}$ (i.e., outputs 0 for half the inputs, and 1 for the other half)

- To decide whether f is constant or balanced, **how many times** must we evaluate f?

Classical Computer
Worst-case: 2^n
Probabilistic algorithm:
$l \ll 2^n$ times,
with a failure rate of $\frac{1}{2^l}$

Quantum Computer:
Evaluate **once**,
with a failure rate $\frac{1}{2^n}$

The Deutsch-Jozsa Problem

- Constant-vs-balanced problem
- Let $f:\{0,1\}^n \rightarrow \{0,1\}$ be a bit function such that it is in either two cases:
  - f is a *constant* function: $\forall \boldsymbol{x} \in \{0,1\}^n, f(\boldsymbol{x})$ is always a constant (0 or 1)
  - f is a *balanced* function: $\sum_{x\in\{0,1\}^n} f(\boldsymbol{x}) = \boldsymbol{2^{n-1}}$ (i.e., outputs 0 for half the inputs, and 1 for the other half)

- To decide whether f is constant or balanced, **how many times** must we evaluate f?

Classical Computer:

Probabilistic algorithm: l times, with a failure rate of $\frac{1}{2^l}$

Quantum Computer:

Evaluate **once**, with a failure rate $\frac{1}{2^n}$

Quantum Supremacy

The Deutsch-Jozsa Problem

- Constant-vs-balanced problem
- Let $f: \{0,1\}^n \rightarrow \{0,1\}$ be a bit function such that it is in either two cases:
  - f is a *constant* function: $\forall \boldsymbol{x} \in \{0,1\}^n, f(\boldsymbol{x})$ is always a constant (0 or 1)
  - f is a *balanced* function: $\sum_{x \in \{0,1\}^n} f(\boldsymbol{x}) = \boldsymbol{2^{n-1}}$ (i.e., outputs 0 for half the inputs, and 1 for the other half)

- To decide whether f is constant or balanced, **how many times** must we evaluate f?

Classical Computer:

Probabilistic algorithm: l times, with a failure rate of $\frac{1}{2^l}$

Quantum Computer:

Evaluate **once**, with a failure rate $\frac{1}{2^n}$

Quantum Supremacy

But wait…What's **the practical application** of the Deutsch-Jozsa problem?

Quantum-Classical Separation Problems

- The Deutsch–Jozsa problem has no known practical application
- It is an early example of quantum supremacy, illustrating (or suggesting) the theoretical **separation between quantum and classical computation** (e.g., BPP vs BQP)

Quantum-Classical Separation Problems

- The Deutsch–Jozsa problem has no known practical application
- It is an early example of quantum supremacy, illustrating (or suggesting) the theoretical separation between quantum and classical computation (e.g., BPP vs BQP)

- Similar quantum-classical separation problems:
  - Simon's problem (exercise or homework, TBD)
  - Random Circuit Sampling

Quantum-Classical Separation Problems

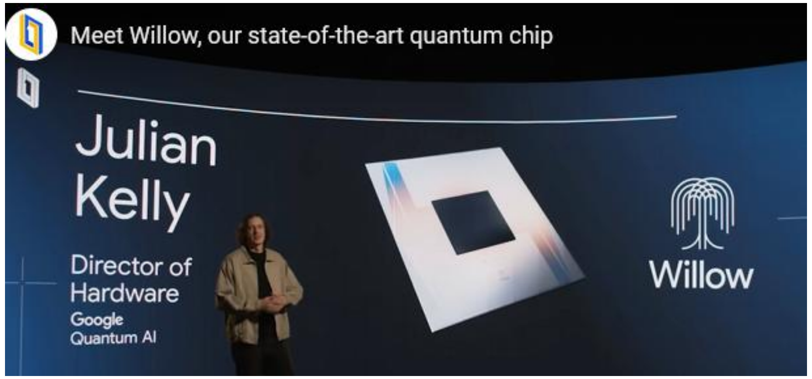
- The Deutsch–Jozsa problem has no known practical application
- It is an early example of quantum supremacy, illustrating (or suggesting) the theoretical separation between quantum and classical computation (e.g., BPP vs BQP)

- Similar quantum-classical separation problems:
  - Simon’s problem
  - Random Circuit Sampling (Google’s Sycamore and Willow)

Google says an advanced computer has achieved "quantum supremacy" for the first time, surpassing the performance of conventional devices.

The technology giant's Sycamore quantum processor was able to perform a specific task in 200 seconds that would take the world's best supercomputer 10,000 years to complete.

BBC News, 2019



Google quantum AI, 2024

Quantum-Classical Separation Problems

- The Deutsch–Jozsa problem has no known practical application
- It is an early example of quantum supremacy, illustrating (or suggesting) the theoretical separation between quantum and classical computation (e.g., BPP vs BQP)

- Similar quantum-classical separation problems:
  - Simon's problem
  - Random Circuit Sampling
  - Forrelation, Boson Sampling, …

Quantum-Classical Separation Problems

- The Deutsch–Jozsa problem has no known practical application
- It is an early example of quantum supremacy, illustrating (or suggesting) the theoretical separation between quantum and classical computation (e.g., BPP vs BQP)

- Similar quantum-classical separation problems:
  - Simon’s problem
  - Random Circuit Sampling
  - Forrelation, Boson Sampling, …
- Separation problems that have **practical use**:
  - Hidden subgroup problem (Discrete logarithm, Factoring): Shor’s algorithm
- No quantum supremacy, but **quantum acceleration**
  - Unstructured search problem: Grover’s search algorithm

Postulates of Quantum Computing

"Don't be surprised if the motivation for the postulates is not always clear; even to experts the basic postulates of quantum mechanics appear surprising..." from [NC00]

Postulates of Quantum Computing

- First postulate: State space

> **Postulate 1**: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.
>
> from [NC00]

Postulates of Quantum Computing

- First postulate: State space

> **Postulate 1:** Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.
>
> from [NC00]

- Keywords:
  - **Isolated system**
  - **Hilbert space**: Complex inner product linear space (e.g., $\mathbb{C}^{2^n}$)
  - The state of a system is completely described by a **state vector**
  - A state vector is a **unit vector of** the Hilbert space

Example:
$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$

Postulates of Quantum Computing

- First postulate: State space

> **Postulate 1:** Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.
>
> from [NC00]

- Keywords:
  - **Isolated system: (Informally,) Not entangled with other systems…**
  - **Hilbert space**: Complex inner product linear space (e.g., $\mathbb{C}^{2^n}$)
  - The state of a system is completely described by a **state vector**
  - A state vector is a **unit vector of** the Hilbert space

Example:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Postulates of Quantum Computing

- Second postulate: Evolution

Postulate 2: The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle .$$

from [NC00]

- Keywords:
  - **Closed system**
  - **Unitary transformation**

Postulates of Quantum Computing

- Second postulate: Evolution

Postulate 2: The evolution of a *closed* quantum system is described by a *unitary transformation*. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U|\psi\rangle .$$

from [NC00]

- Keywords:
  - **Closed system: Not interacting with other systems**
  - **Unitary transformation**

Postulates of Quantum Computing

- Second postulate (using Schrodinger's equation): Evolution

Postulate 2′: The time evolution of the state of a closed quantum system is described by the *Schrödinger equation*,

$$i\hbar\frac{d|\psi\rangle}{dt} = H|\psi\rangle.$$

In this equation, $\hbar$ is a physical constant known as *Planck's constant* whose value must be experimentally determined. The exact value is not important to us. In practice, it is common to absorb the factor $\hbar$ into H, effectively setting $\hbar = 1$. H is a fixed Hermitian operator known as the *Hamiltonian* of the closed system.

from [NC00]

Postulates of Quantum Computing

- Fourth postulate: Composite system:

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$. from [NC00]

Postulates of Quantum Computing

- Fourth postulate: Composite system:

Postulate 4: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$. from [NC00]

- Keywords:
  - **Tensor product**
  - State space of the whole system: **Tensor product of the Hilbert spaces** of each component system
  - State vector of the whole system: **Tensor product of the state vector** of each component system

Postulates of Quantum Computing

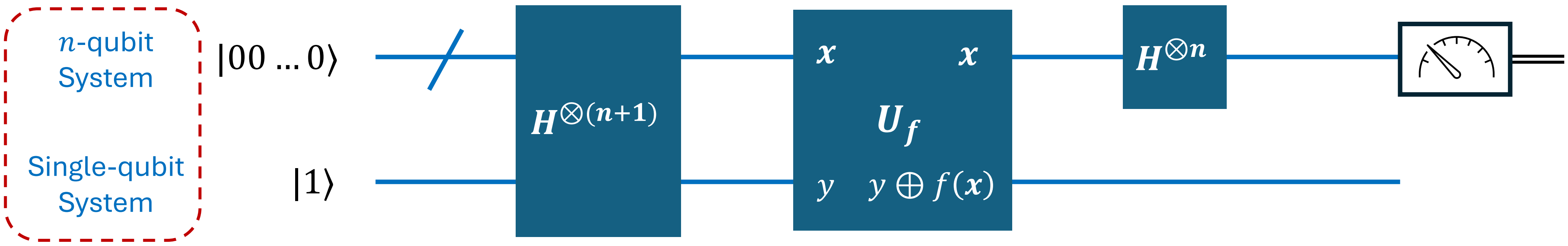
- Third postulate: Quantum measurement

- Do it on the board

- Measurement **in the computational basis**
- **Partial measurement**

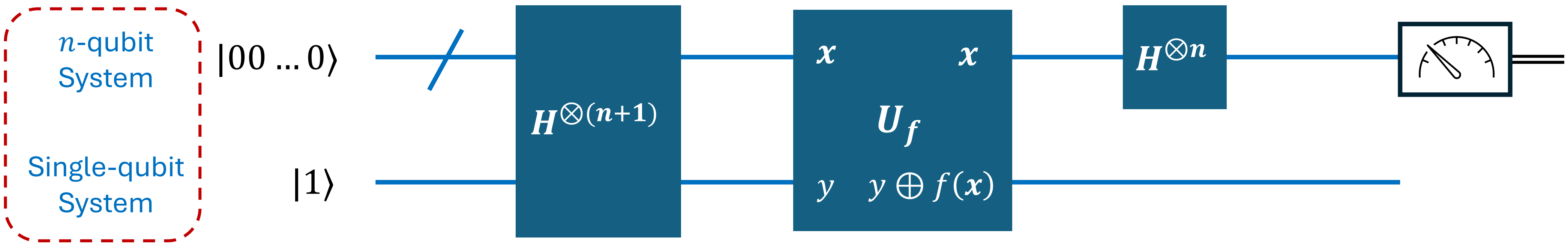
Postulates of Quantum Computing

- Illustrating the Quantum Postulates through the Deutsch–Jozsa Algorithm



Postulates of Quantum Computing

- Illustrating the Quantum Postulates through the Deutsch–Jozsa Algorithm



(A student's question)
Why **isn't** the final state of the first n-qubit system $|00 \ldots 0\rangle$?

Postulates of Quantum Computing

- Third postulate: Quantum measurement

- Measurement in the computational basis
- Partial measurement

- **Collapse: The state after measurement** $|\phi\rangle \longrightarrow \frac{M_m|\phi\rangle}{\sqrt{\langle\phi|M_m^\dagger M_m|\phi\rangle}}$

Quantum Measurement

- Let $\{M_m\}_m$ be a set of matrices describing some quantum measurement

- Let $|\phi\rangle$ be a quantum state, perform the same measurement $\{M_m\}_m$ on $|\phi\rangle$ **twice**

$$|\phi\rangle \longrightarrow \frac{M_m|\phi\rangle}{\sqrt{\langle\phi|M_m^\dagger M_m|\phi\rangle}} \longrightarrow \textbf{?}$$

(with probability
$p(m) = \langle\phi|M_m^\dagger M_m|\phi\rangle$)

Quantum Measurement

- Let $\{M_m\}_m$ be a set of matrices describing some quantum measurement

- Let $|\phi\rangle$ be a quantum state, perform the same measurement $\{M_m\}_m$ on $|\phi\rangle$ **twice**

$$|\phi\rangle \longrightarrow \frac{M_m|\phi\rangle}{\sqrt{\langle\phi|M_m^\dagger M_m|\phi\rangle}} \longrightarrow ?$$

(with probability
$p(m) = \langle\phi|M_m^\dagger M_m|\phi\rangle$)

We need more restrictions to achieve **"Stability"**

Projective Measurement

- Projective measurements: A special class of measurements

Projective Measurement

- Some Linear Algebra – **Projector and Eigenspace**:
  - A matrix $\boldsymbol{P}$ is a projector (or projection operator) if $\boldsymbol{P}^2 = \boldsymbol{P}$
  - For any vector $\boldsymbol{x}$, $\boldsymbol{P}^n\boldsymbol{x} = \boldsymbol{P}^{n-1}\boldsymbol{x} = \cdots = \boldsymbol{P}\boldsymbol{x}$

  - **Eigenvalues** and **Eigenvectors**: $\boldsymbol{A}\boldsymbol{x} = \lambda\boldsymbol{x}$
  - A matrix (linear operator) may have **multiple eigenvalues**
  - Each eigenvalue may have **multiple linearly independent eigenvectors**

  - Let $\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_m\}$ denote a *maximal set* of linearly independent eigenvectors of λ (i.e., $\boldsymbol{A}\boldsymbol{x}_i = \lambda\boldsymbol{x}_i$)
  - We say $\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_m\}$ **span the eigenspace** of $\boldsymbol{A}$ with eigenvalue λ

  - Given such $\{\boldsymbol{x}_1, \dots, \boldsymbol{x}_m\}$, the **Gram-Schmidt process** gives us an **orthogonal basis of the eigenspace**
  - Given an orthogonal basis, we can easily compute the **projector onto this eigenspace**

Projective Measurement

- Some Linear Algebra – **Spectral decomposition (simplified)**:

  Any Hermitian operator $\boldsymbol{M}$ (i.e., $\boldsymbol{M} = \boldsymbol{M}^{\dagger}$) can be written as:

$$\boldsymbol{M} = \sum_{\lambda} \lambda \boldsymbol{P}_{\lambda}$$

  - λ represents an eigenvalue of $\boldsymbol{M}$
  - $\boldsymbol{P}_{\lambda}$ represents the projector onto the λ eigenspace
  - $\boldsymbol{P}_{\lambda}$ itself is also Hermitian, i.e., $\boldsymbol{P}_{\lambda} = \boldsymbol{P}_{\lambda}^{\dagger}$

  - Examples (show on the board)...

Projective Measurement

- Projective measurements: A special class of measurements
- (Do it on the board)

- Keywords
  - **Observable $\boldsymbol{M} = \sum_m m\boldsymbol{P}_m$** is a *Hermitian matrix*
    - m represents an eigenvalue of $\boldsymbol{M}$**,** and it is also used to **label a measurement outcome**
    - $\boldsymbol{P}_m$ represents the projector onto the m eigenspace
    - $\boldsymbol{P}_m$ is also Hermitian
  - Measurement outcome **correspond to the eigenvalues**
    - e.g., $p(m) = \langle\phi|P_m|\phi\rangle$
  - The state after measurement: $|\phi\rangle \rightarrow \frac{P_m|\phi\rangle}{\sqrt{p(m)}}$

Projective Measurement

- Projective measurements: A special class of measurements

- Relation to Postulate 3:
  - $\boldsymbol{M} = \sum_m m\boldsymbol{P}_m$, but $\sum_m \boldsymbol{P}_m = \boldsymbol{I}$, so the completeness condition holds
  - Note: An eigenvalue of an observable just **represents a possible outcome (i.e., a label), but not the probability or physical meaning by itself**

- Examples: $|0\rangle\langle 0| = 1 \cdot |0\rangle\langle 0| + 0 \cdot |1\rangle\langle 1|$ and $|1\rangle\langle 1| = 0 \cdot |0\rangle\langle 0| + 1 \cdot |1\rangle\langle 1|$
  - Both can be used to represent measurement in the computational basis

Projective Measurement

- Let $\boldsymbol{M} = \sum_m m\boldsymbol{P}_m$ be an observable
- Let $|\phi\rangle$ be a quantum state, perform the same projective measurement $\boldsymbol{M}$ on $|\phi\rangle$ **twice**

Projective Measurement

- Let $\boldsymbol{M} = \sum_m m\boldsymbol{P}_m$ be an observable
- Let $|\phi\rangle$ be a quantum state, perform the same projective measurement $\boldsymbol{M}$ on $|\phi\rangle$ **twice**

$$|\phi\rangle \longrightarrow \frac{P_m|\phi\rangle}{\sqrt{\langle\phi|P_m|\phi\rangle}} \longrightarrow \textbf{?}$$

(with probability
$p(m) = \langle\phi|P_m|\phi\rangle$)

Projective Measurement

- Let $\boldsymbol{M} = \sum_m m\boldsymbol{P}_m$ be an observable
- Let $|\phi\rangle$ be a quantum state, perform the same projective measurement $\boldsymbol{M}$ on $|\phi\rangle$ **twice**

$$|\phi\rangle \longrightarrow \frac{P_m|\phi\rangle}{\sqrt{\langle\phi|P_m|\phi\rangle}} \longrightarrow \frac{P_m|\phi\rangle}{\sqrt{\langle\phi|P_m|\phi\rangle}}$$

(with probability $p(m) = \langle\phi|P_m|\phi\rangle$)

(with probability 1)

Non-Projective Measurement

- Let $\{M_m\}_m$ be a set of matrices describing some quantum measurement

- General measurement (Postulate 3): $M_m^\dagger M_m$ is not necessarily a projector.
  - **Non-projective measurement:** $M_m^\dagger M_m$ is not a projector
  - Cannot guarantee that the same result will be reproduced if the same measurement is repeated

- Used in various quantum information-processing protocols
  - But will not be not covered in this course

References

- [NC00]: Sections 1.4.4, 2.2
- [KLM07]: Chapter 3, Sections 6.4.

Next Week

- Entanglement
- Pure state and mixed state
- Partial measurement

- **No lecture next Thursday** (Ascension Day, May 29)