

Quantum Computing

- Week 6 (May 19-20, 2026)
- Topics:
 - Deutsch-Jozsa Problem
 - Entanglement
 - Pure states and mixed states

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: $\forall x \in \{0,1\}^n, f(x)$ is always a constant (0 or 1)
 - f is a *balanced* function: $\sum_{x \in \{0,1\}^n} f(x) = 2^{n-1}$ (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-1} (Check half of inputs)

Probabilistic algorithm (Check l inputs):

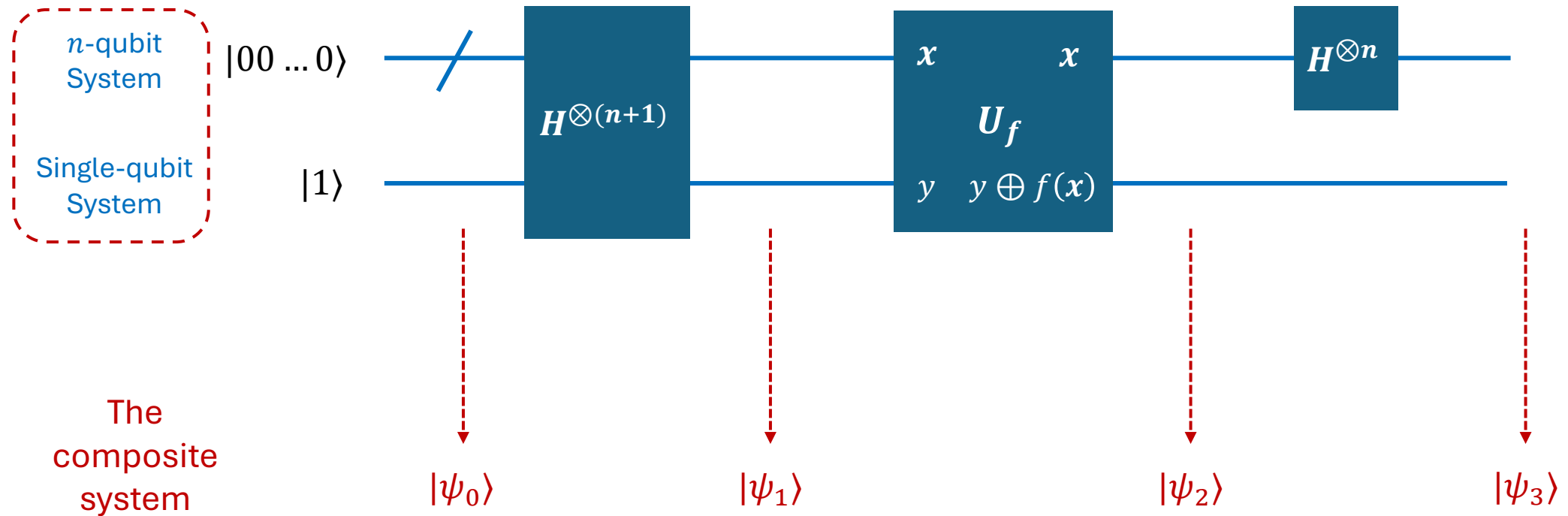
$l \ll 2^{n-1}$ times,

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

Can we do better?

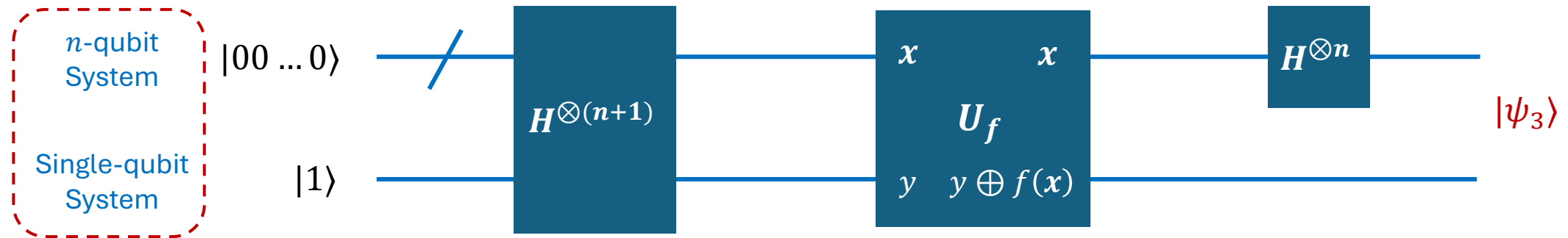
The Deutsch-Jozsa Algorithm

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



The Deutsch-Jozsa Algorithm

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

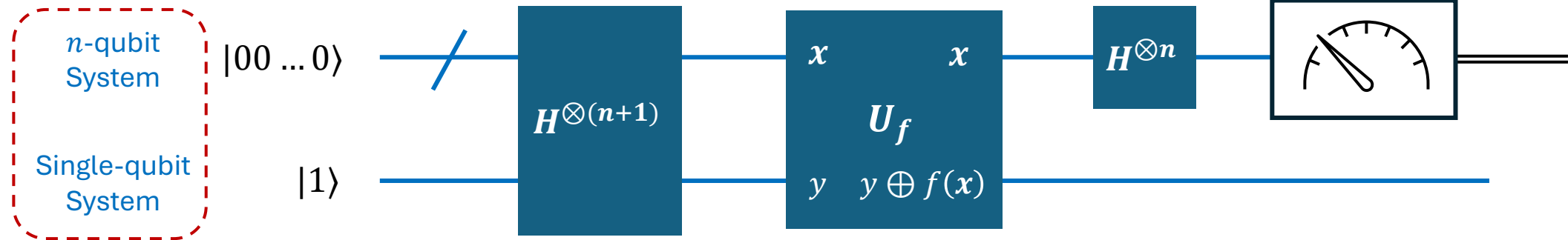


The composite system

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

The Deutsch-Jozsa Algorithm

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



The composite system

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

Measure the first n systems



The Deutsch-Jozsa Algorithm

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

Measure the first
 n -qubit system \mathbf{z}

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

The Deutsch-Jozsa Algorithm

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

Measure the first
 n -qubit system \mathbf{z}

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

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

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 \mathbf{z}

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

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

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

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 z

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

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

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

The Deutsch-Jozsa Algorithm

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

Measure the first
 n -qubit system \mathbf{z}

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

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

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

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

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

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

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

The Deutsch-Jozsa Algorithm

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

Measure the first
 n -qubit system z

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

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

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

Case $z = 00 \dots 0$:

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

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

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

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

The Deutsch-Jozsa Algorithm

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

Measure the first
 n -qubit system z

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

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

Case $z \neq 00 \dots 0$:

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

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

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

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

The Deutsch-Jozsa Algorithm

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

Measure the first n -qubit system z

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

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

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

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

The Deutsch-Jozsa Algorithm

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

Measure the first
 n -qubit system z

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

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

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

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

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

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

Probabilistic algorithm:

$l \ll 2^{n-1}$ 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: $\forall x \in \{0,1\}^n, f(x)$ is always a constant (0 or 1)
 - f is a *balanced* function: $\sum_{x \in \{0,1\}^n} f(x) = 2^{n-1}$ (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-1}

Probabilistic algorithm:

$l \ll 2^{n-1}$ 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: $\forall x \in \{0,1\}^n, f(x)$ is always a constant (0 or 1)
 - f is a *balanced* function: $\sum_{x \in \{0,1\}^n} f(x) = 2^{n-1}$ (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: $\forall x \in \{0,1\}^n, f(x)$ is always a constant (0 or 1)
 - f is a *balanced* function: $\sum_{x \in \{0,1\}^n} f(x) = 2^{n-1}$ (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)

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
- 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

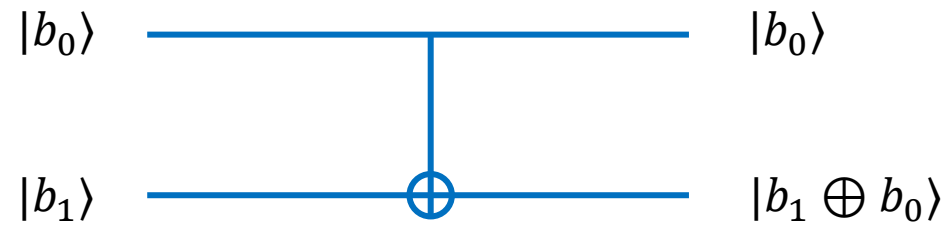
- Postulate 1: State space
- Postulate 2: Evolution and unitary transformation
- Postulate 3: Quantum Measurement
 - Projective measurement
- Postulate 4: Composite system

Postulates of Quantum Computing

- Postulate 1: State space (**isolated systems**)
- Postulate 2: Evolution and unitary transformation (**closed systems**)
- Postulate 3: Quantum Measurement
 - Projective measurement
- Postulate 4: Composite system

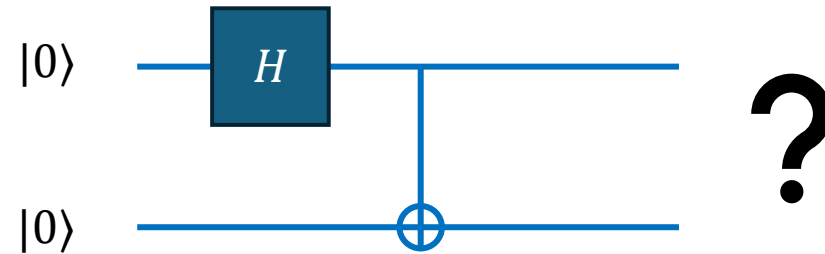
Controlled NOT Gate

- CNOT: If $b_0 = 0$, output b_1 ; Else, output $1 \oplus b_1$ (i.e., flip b_1 if $b_0 = 1$)



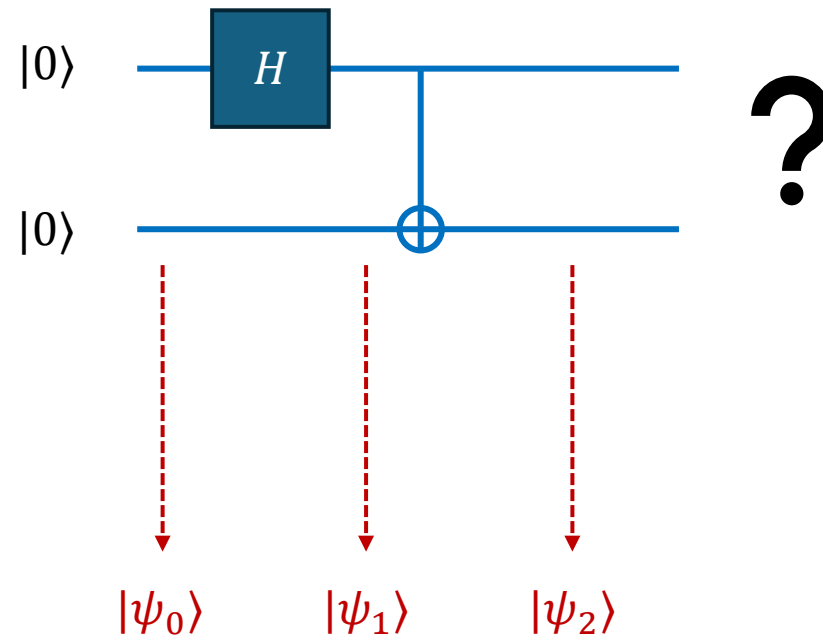
- $|00\rangle \rightarrow |00\rangle$
- $|01\rangle \rightarrow |01\rangle$
- $|10\rangle \rightarrow |11\rangle$
- $|11\rangle \rightarrow |10\rangle$

Controlled NOT Gate



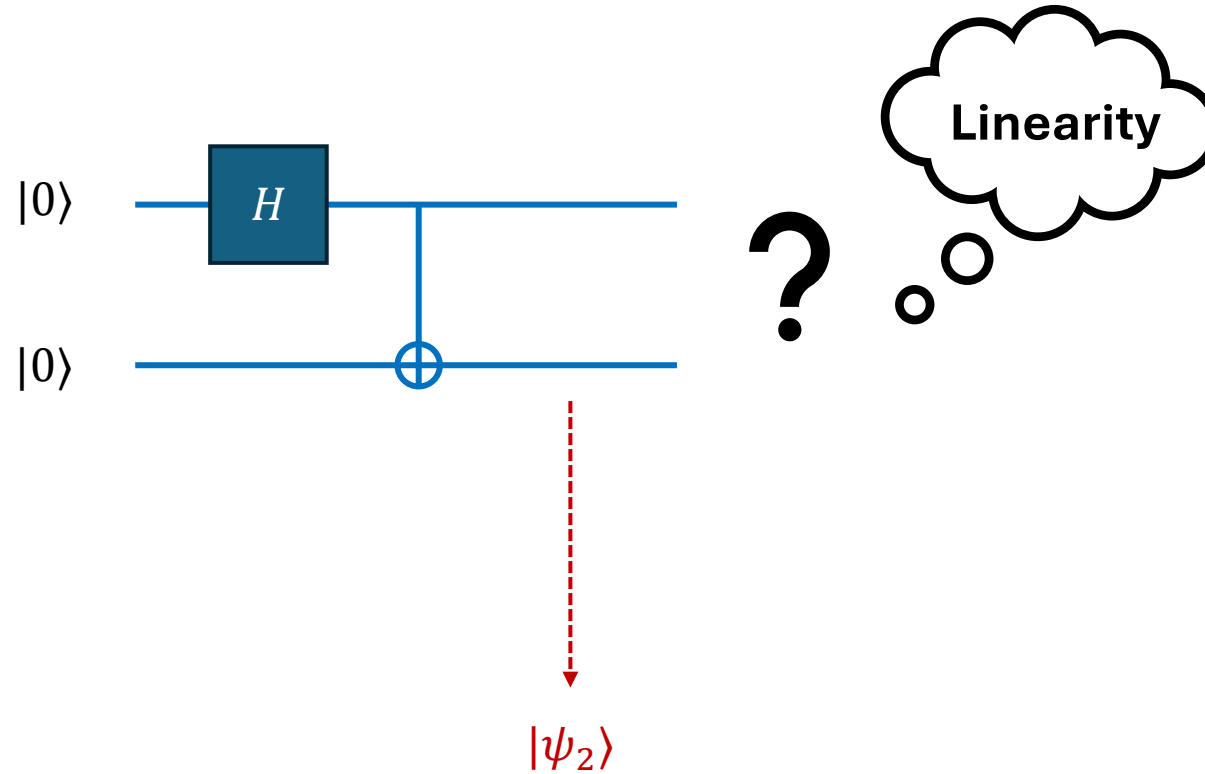
- $|00\rangle \rightarrow |00\rangle$
- $|01\rangle \rightarrow |01\rangle$
- $|10\rangle \rightarrow |11\rangle$
- $|11\rangle \rightarrow |10\rangle$

Controlled NOT Gate



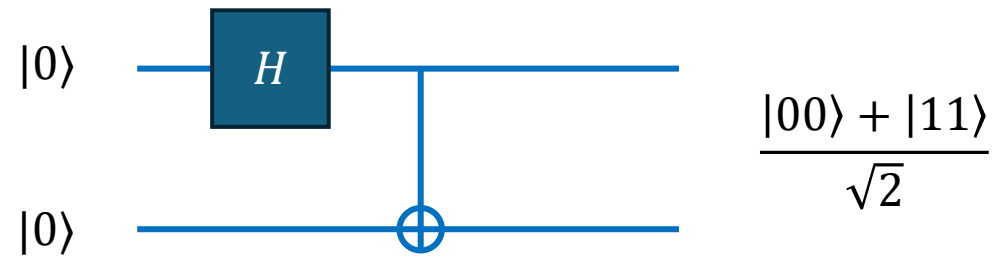
- $|00\rangle \rightarrow |00\rangle$
- $|01\rangle \rightarrow |01\rangle$
- $|10\rangle \rightarrow |11\rangle$
- $|11\rangle \rightarrow |10\rangle$

Controlled NOT Gate



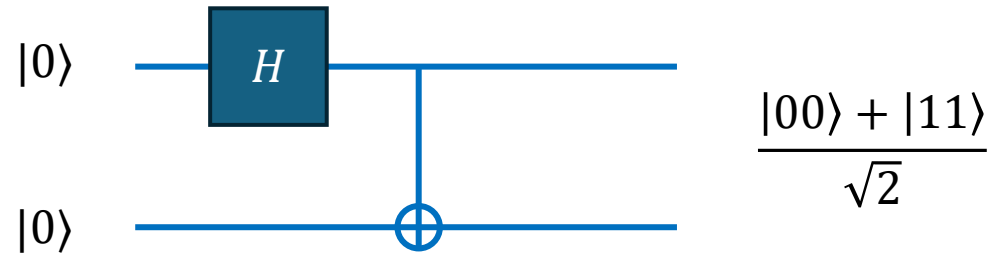
- $|00\rangle \rightarrow |00\rangle$
- $|01\rangle \rightarrow |01\rangle$
- $|10\rangle \rightarrow |11\rangle$
- $|11\rangle \rightarrow |10\rangle$

Controlled NOT Gate



- $|00\rangle \rightarrow |00\rangle$
- $|01\rangle \rightarrow |01\rangle$
- $|10\rangle \rightarrow |11\rangle$
- $|11\rangle \rightarrow |10\rangle$

Controlled NOT Gate



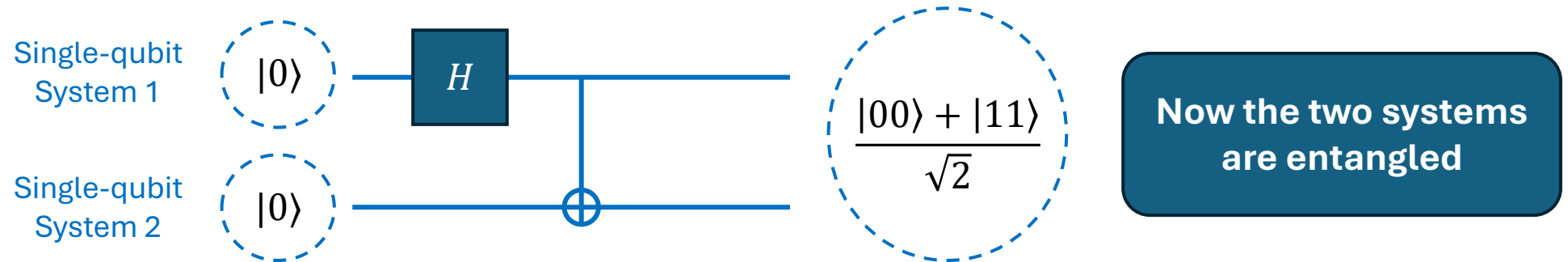
- $|00\rangle \rightarrow |00\rangle$
- $|01\rangle \rightarrow |01\rangle$
- $|10\rangle \rightarrow |11\rangle$
- $|11\rangle \rightarrow |10\rangle$



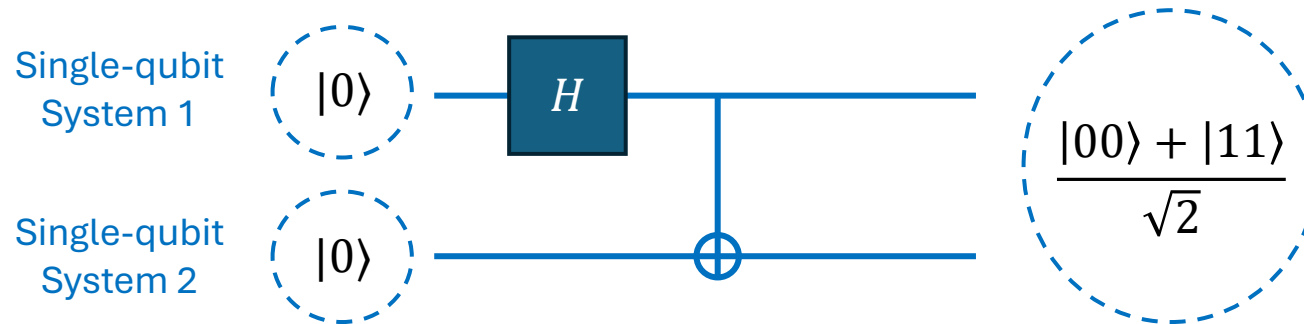
John Stewart Bell
(source: Wikipedia)

Bell state:
Impossible to be split into
a tensor product of two states
 $|\varphi_1\rangle \otimes |\varphi_2\rangle$

Quantum Entanglement



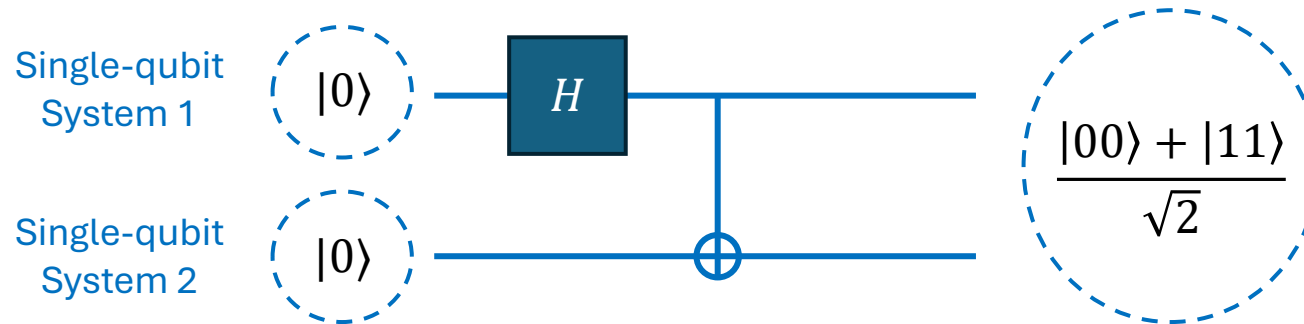
Quantum Entanglement



Now the two systems are entangled

Pure state: Can be described by a state vector
Mixed state: Cannot ...

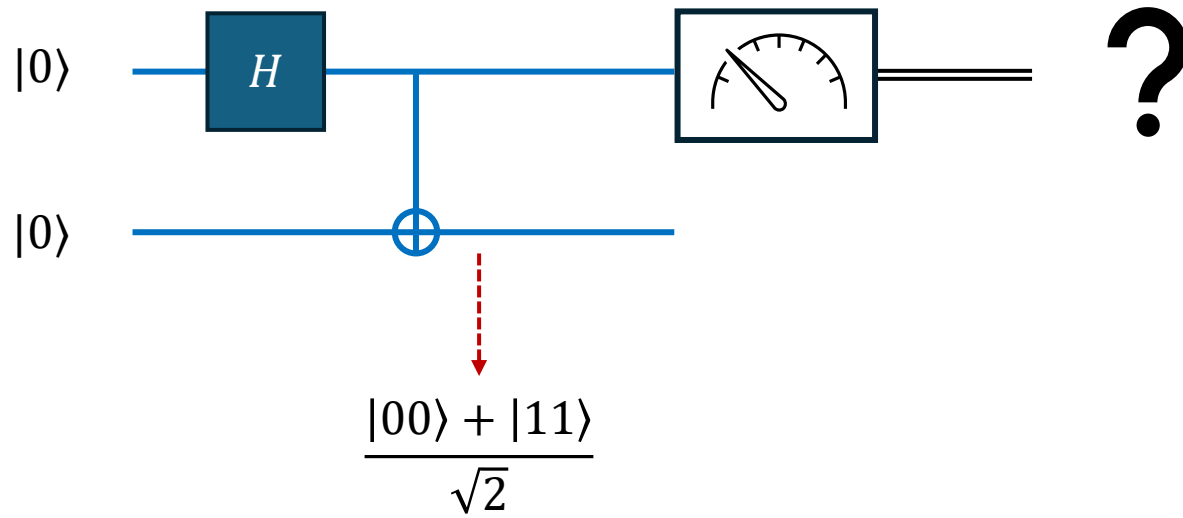
Quantum Entanglement



Small Exercise: (pure or mixed)

1. The initial state of system 1 is ____.
2. The states of system 1 and 2 (after H and CNOT) are ____.
3. The state of the total system (after H and CNOT) is ____.

Partial Measurement on Entangled States



Partial Measurement on Entangled States

- Formalizing Partial Measurement
 - Let's focus on the computational basis
 - General measurement: $\{M_m\}_m \rightarrow \{M_m \otimes I\}_m$
 - Projective measurement: $\mathbf{M} = \sum_m m\mathbf{P}_m \rightarrow \mathbf{M} \otimes \mathbf{I} = (\sum_m m\mathbf{P}_m) \otimes \mathbf{I} = \sum_m m(\mathbf{P}_m \otimes \mathbf{I})$

Partial Measurement on Entangled States

- **Spectral decomposition (simplified):**

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

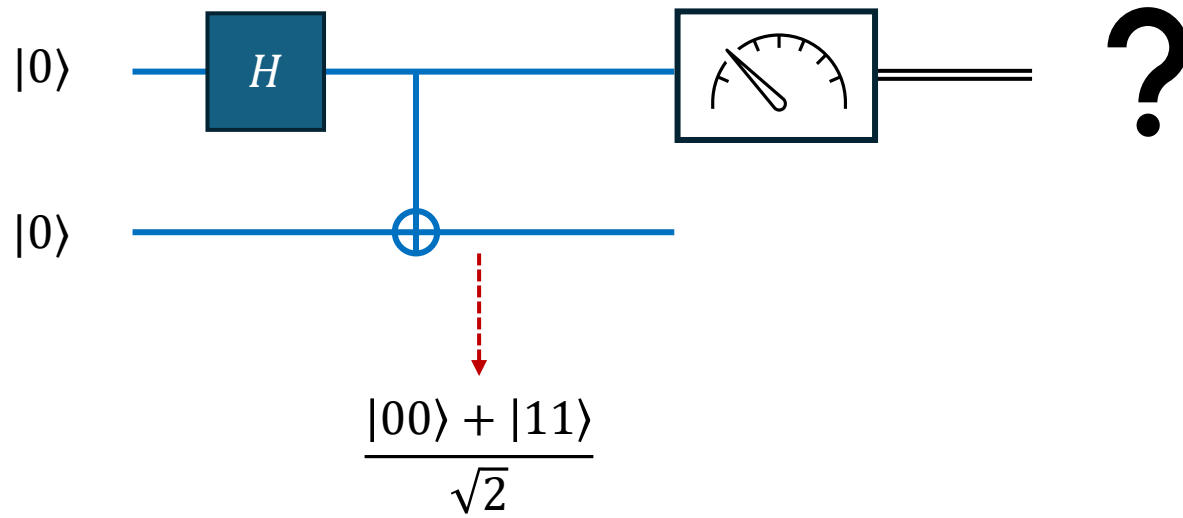
$$M = \sum_{\lambda} \lambda P_{\lambda}$$

- λ represents an eigenvalue of M (also indexes the projectors)
- P_{λ} represents the projector onto the λ eigenspace, $P_{\lambda}^2 = P_{\lambda}$
- P_{λ} itself is also Hermitian, i.e., $P_{\lambda} = P_{\lambda}^\dagger$
- $\sum_{\lambda} P_{\lambda} = I$
- $P_{\lambda}^\dagger P_{\lambda'} = \delta_{\lambda,\lambda'} (= 1 \text{ if } \lambda = \lambda', \text{ otherwise } = 0)$

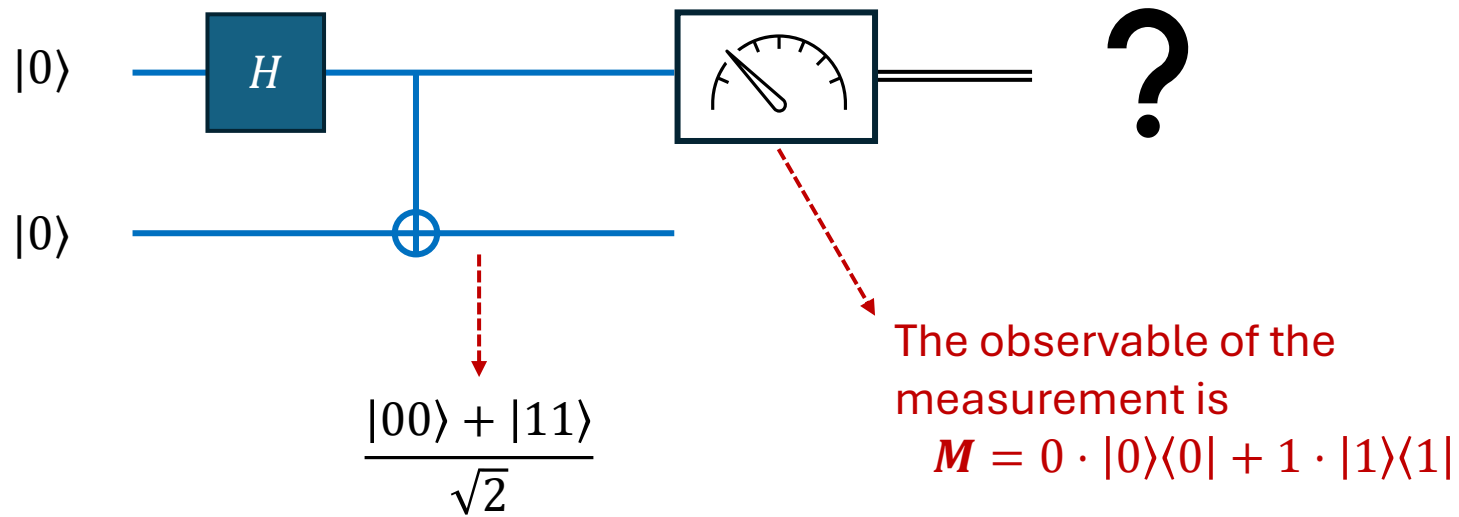
Partial Measurement on Entangled States

- Formalizing Partial Measurement
 - Let's focus on the computational basis
 - General measurement: $\{M_m\}_m \rightarrow \{M_m \otimes I\}_m$
 - Projective measurement: $\mathbf{M} = \sum_m m\mathbf{P}_m \rightarrow \mathbf{M} \otimes \mathbf{I} = (\sum_m m\mathbf{P}_m) \otimes \mathbf{I} = \sum_m m(\mathbf{P}_m \otimes \mathbf{I})$
- Important notes:
 - $\{M_m \otimes I\}_m$ still satisfies the completeness equation
 - $\mathbf{M} \otimes \mathbf{I}$ is still an observable
- Example (Exercise):
 - Partial measurement on the state $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$

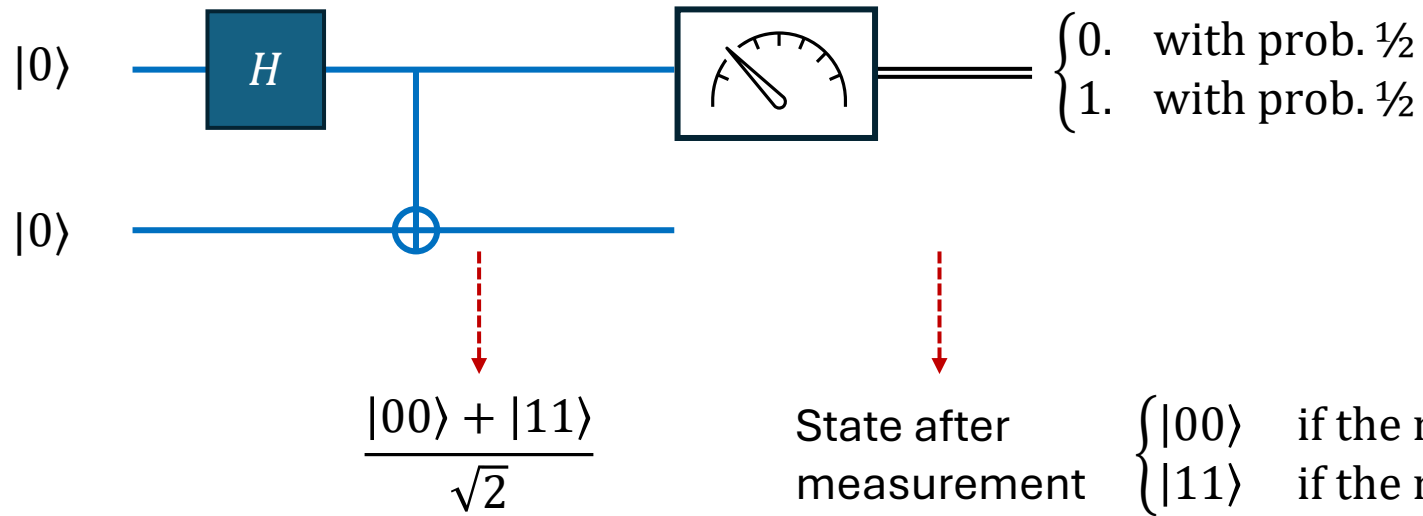
Partial Measurement on Entangled States



Partial Measurement on Entangled States

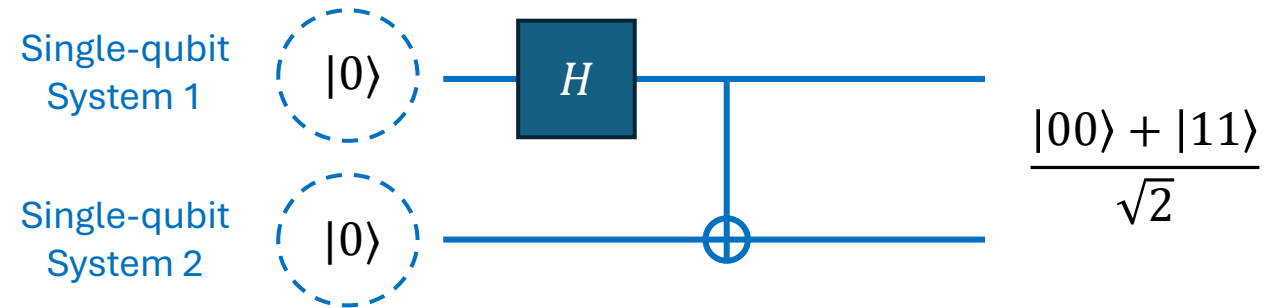


Partial Measurement on Entangled States



For entangled states,
partial measurement
leads to global collapse

Action at a Distance (Fernwirkung)



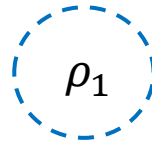
Action at a Distance



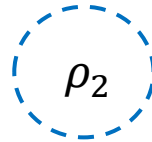
Very long distance (e.g., 10 light-years)



Single-qubit
System 1

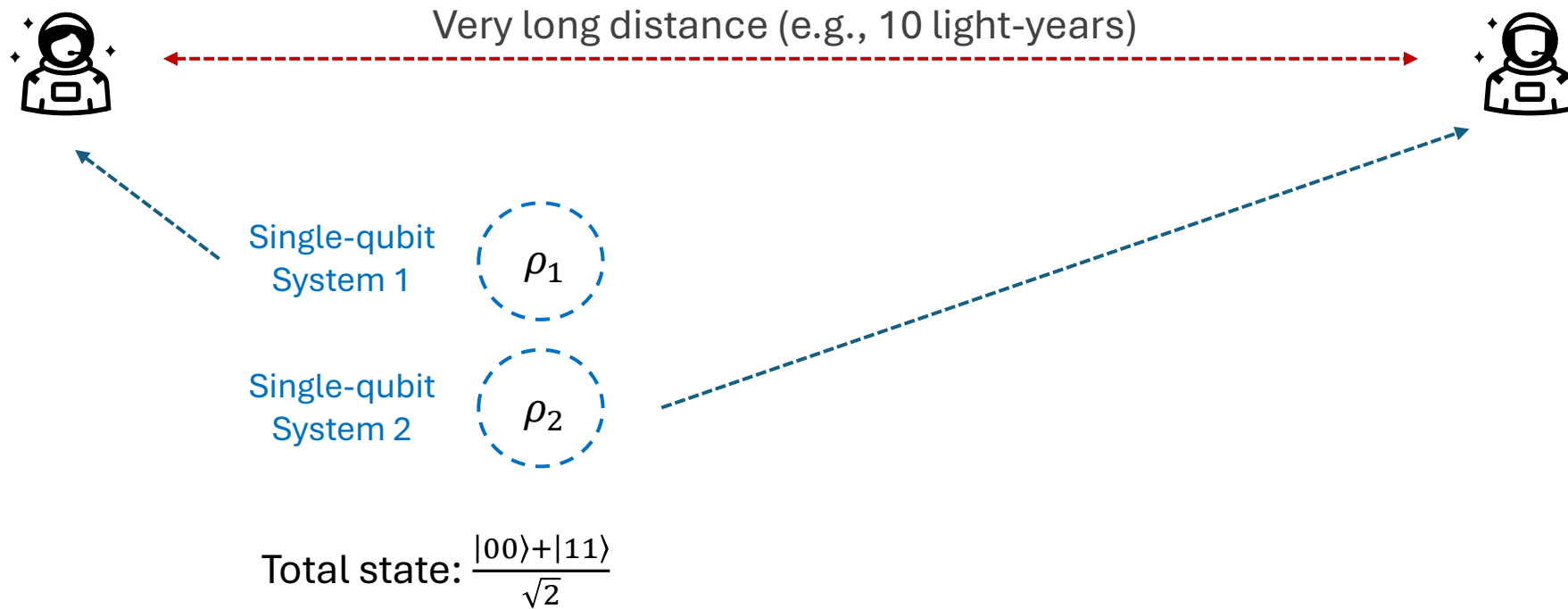


Single-qubit
System 2

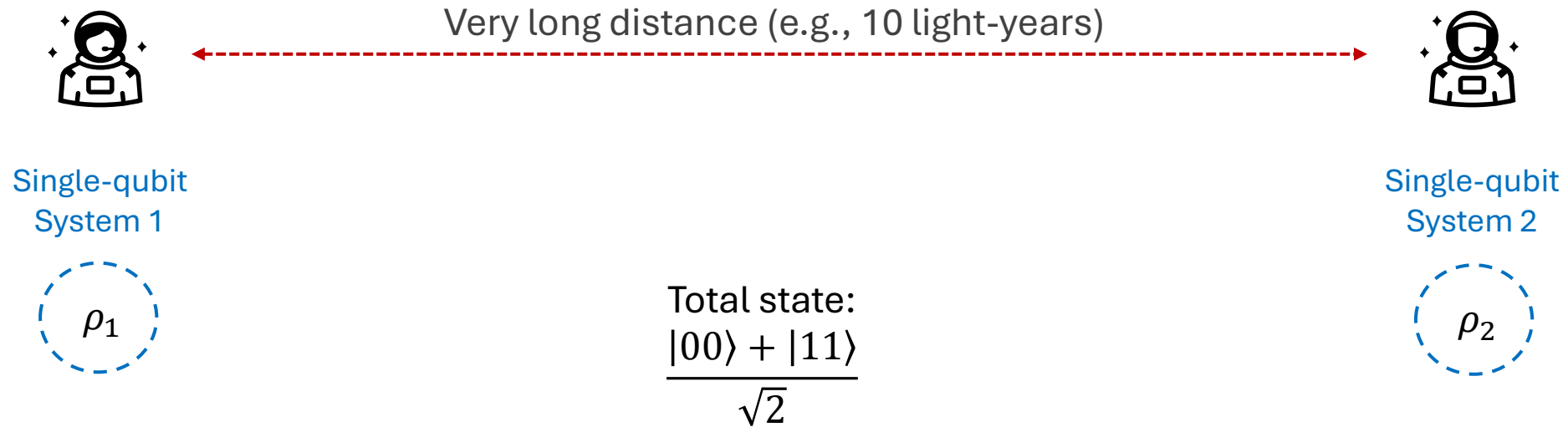


Total state: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

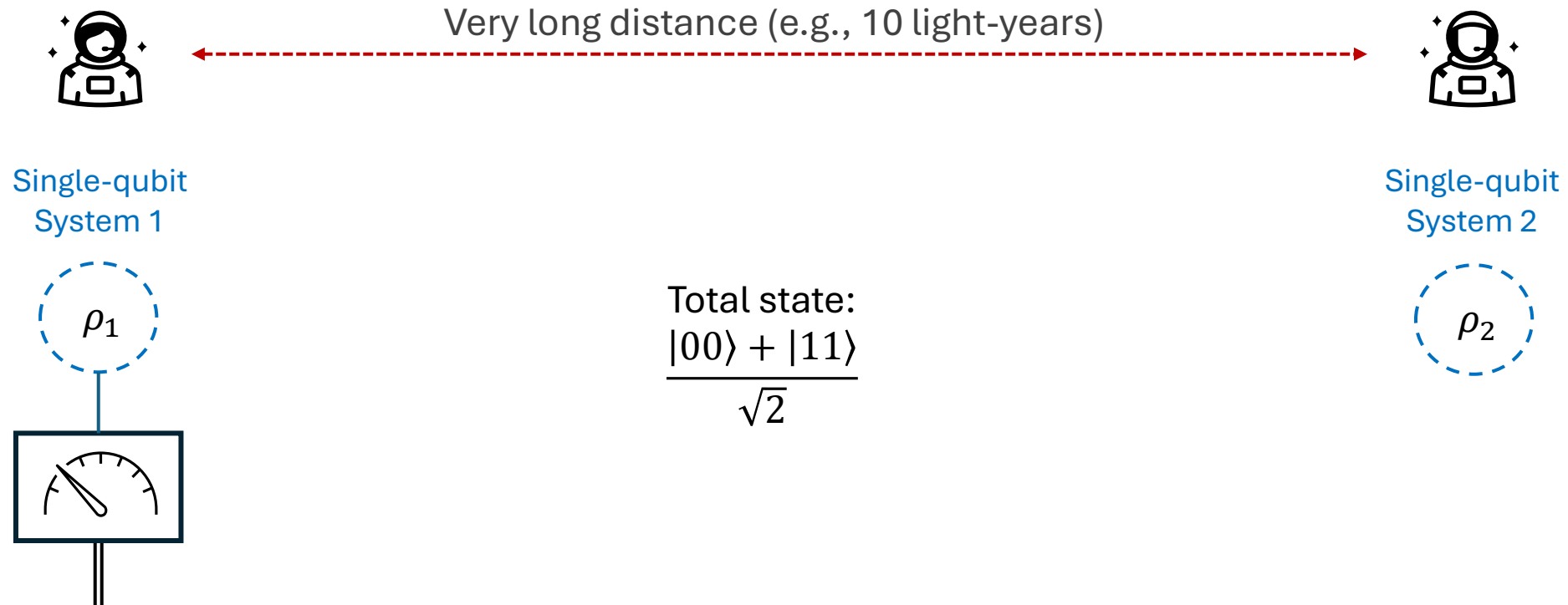
Action at a Distance



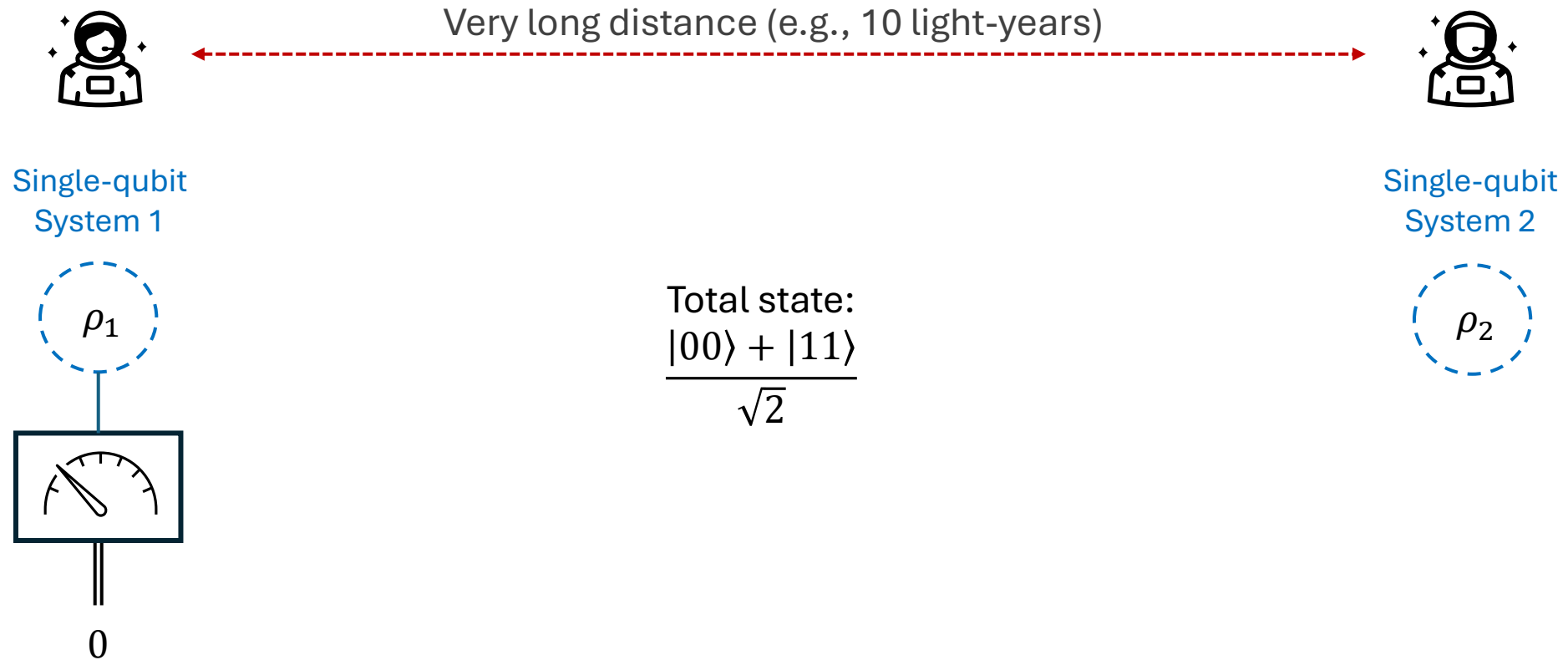
Action at a Distance



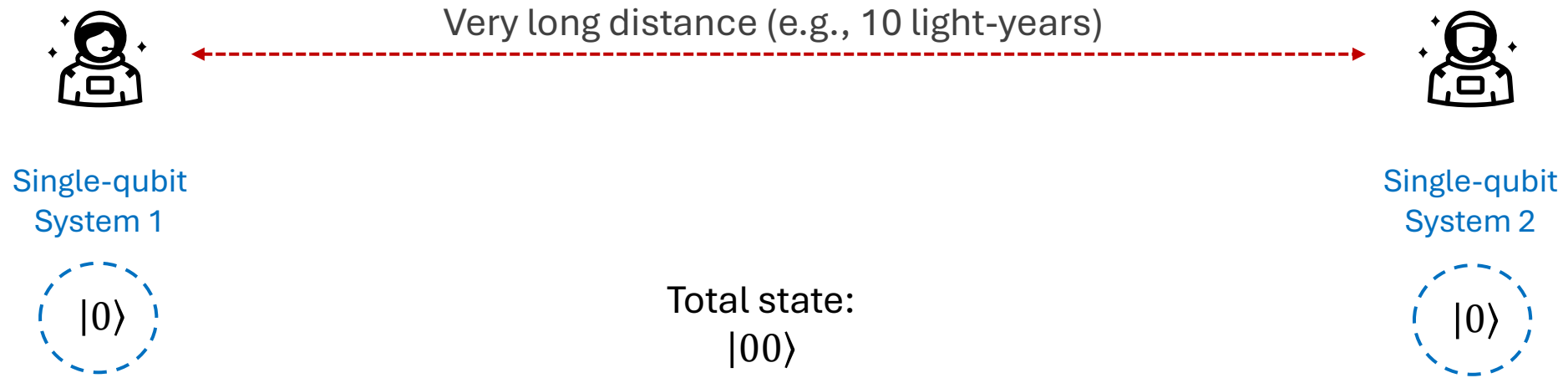
Action at a Distance



Action at a Distance

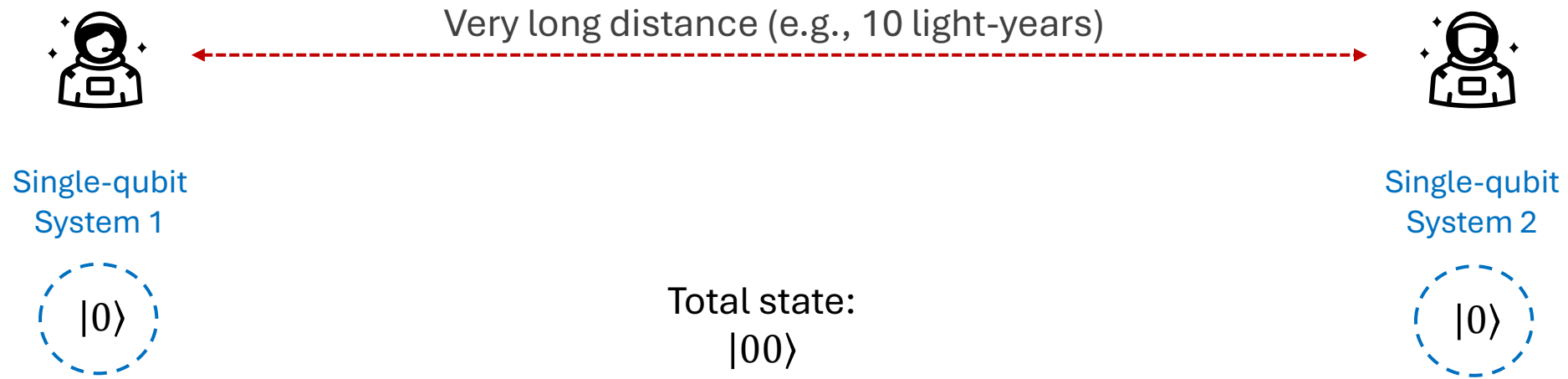


Action at a Distance



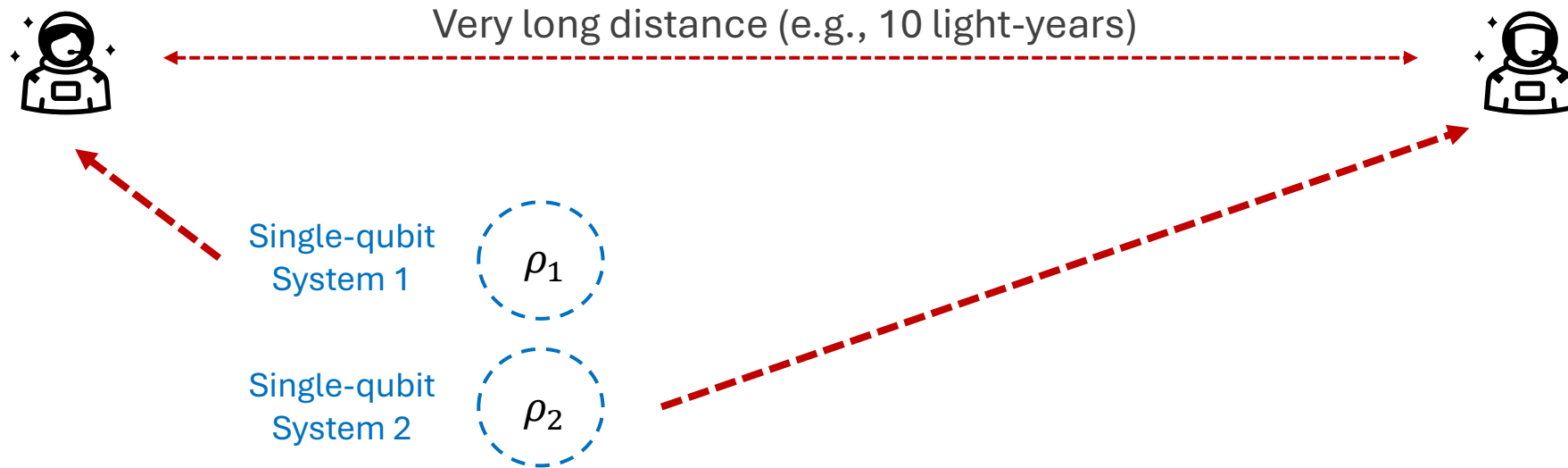
- “spukhafte Fernwirkung”

Action at a Distance



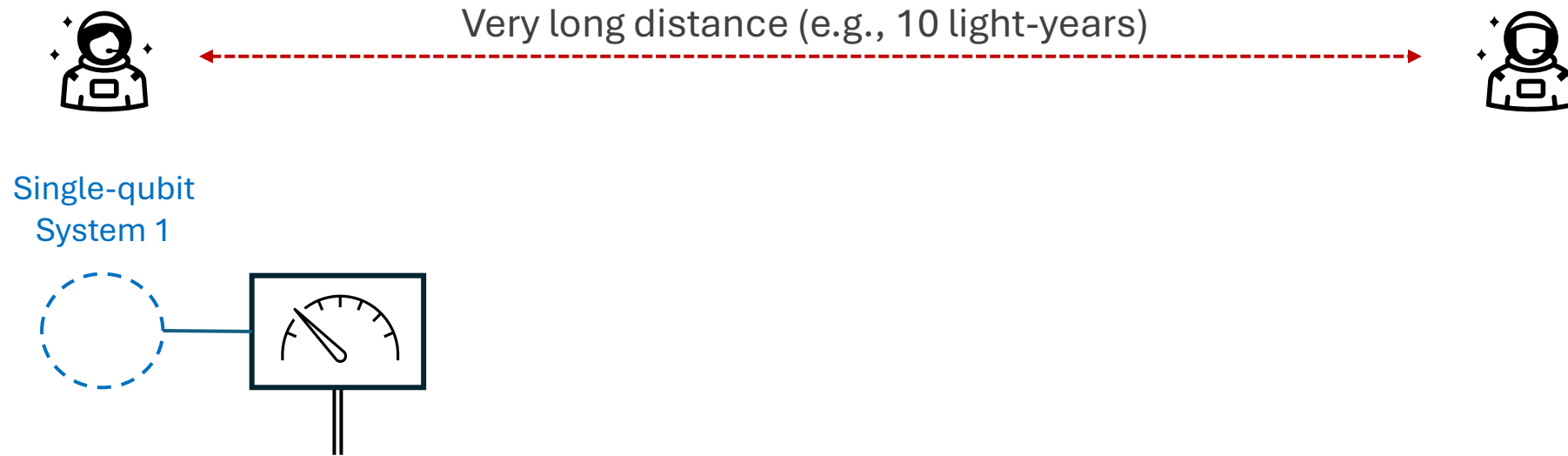
- “spukhafte Fernwirkung”
- A quick question: Is it a faster-than-light **communication**?

Action at a Distance



- “spukhafte Fernwirkung”
- A quick question: Is it a faster-than-light **communication**? **No**
 - They require some pre-shared entangled states

Action at a Distance



- “spukhafte Fernwirkung”
- A quick question: Is it a faster-than-light **communication**? **No**
 - They require some pre-shared entangled states
 - We cannot control the measurement output (i.e., random bit)
 - The receiver has no idea if its system has been measured

Next Week

- Superdense coding (...one qubit “encodes” two classical bits...)
- Quantum teleportation (...transfer one qubit via sending two classical bits...)