Quantum Computation (484)

Mario Berta, Herbert Wiklicky

m.berta@imperial.ac.uk
Autumn 2018

About myself

- Background:
  - PhD in theoretical Physics ETH Zurich
  - 4 years postdoctoral researcher at Caltech
  - joined Imperial one year ago
- Research area:
  - Quantum information processing, theoretical computer science
  - Quantum cryptography and quantum communication theory
- Interested in connections to mathematical physics, through matrix analysis and optimization theory
- More information: marioberta.info

Organisational

- Material: marioberta.info/teaching/
- Same structure as first part of Herbert Wiklicky
- Lectures:
  - Tuesday 4pm – 5pm in Huxley 140
  - Friday 9am – 11am in Huxley 130
- Tutorials with Francesco Borderi:
  - Tuesday 5pm – 6pm in Huxley 140
- Coursework test (7.5% towards final mark, I think):
  - Tuesday 27/11 4pm – 5pm in Huxley 140
- Exam:
  - Monday 10/12, 2 hours (not sure if confirmed yet)
- I am on Piazza + Panopto should be running?
- Special thanks to Herbert Wiklicky

Overview

- Already covered material:
  - Basics
  - Quantum circuit model
  - No cloning theorem
  - Quantum key distribution
  - Deutsch problem
- Quantum teleportation
- Quantum algorithms:
  - Computational complexity
  - Deutsch-Jozsa problem
  - Simon's problem
  - Grover's algorithm
  - Shor's algorithm
- Quantum error correction (very basics, if time permits)

Quantum Teleportation

We know that it is impossible to clone, i.e. **duplicate** a qubit.

however

It is possible to **teleport** qubits, i.e. to transfer the state of an arbitrary qubit to another qubit.

It is essential to exploit **entanglement** for this process.

Quantum Teleportation

PHYSICAL REVIEW
LETTERS

VOLUME 70 | 29 MARCH 1993 | NUMBER 13

Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels

Charles H. Bennett,[1] Gilles Brassard,[2] Claude Crépeau,[2,3]
Richard Jozsa,[2] Asher Peres,[4] and William K. Wootters[5]
[1] *IBM Research Division, T.J. Watson Research Center, Yorktown Heights, New York 10598*
[2] *Département IRO, Université de Montréal, C.P. 6128, Succursale "A", Montréal, Québec, Canada H3C 3J7*
[3] *Laboratoire d'Informatique de l'École Normale Supérieure, 45 rue d'Ulm, 75230 Paris CEDEX 05, France*[a]
[4] *Department of Physics, Technion–Israel Institute of Technology, 32000 Haifa, Israel*
[5] *Department of Physics, Williams College, Williamstown, Massachusetts 01267*
(Received 2 December 1992)

An unknown quantum state $|\phi\rangle$ can be disassembled into, then later reconstructed from, purely classical information and purely nonclassical Einstein-Podolsky-Rosen (EPR) correlations. To do so the sender, "Alice," and the receiver, "Bob," must prearrange the sharing of an EPR-correlated pair of particles. Alice makes a joint measurement on her EPR particle and the unknown quantum system, and sends Bob the classical result of this measurement. Knowing this, Bob can convert the state of his EPR particle into an exact replica of the unknown state $|\phi\rangle$ which Alice destroyed.

Bell States

For **one** qubit we have the standard base $\{|0\rangle, |1\rangle\}$, and also a non-standard base $\{|+\rangle, |-\rangle\}$.

For **two** qubits we have the standard base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ and a non-standard base made up by Bell States:

$$
\begin{aligned}
|\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \\
|\phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)
\end{aligned}
$$

Base Change

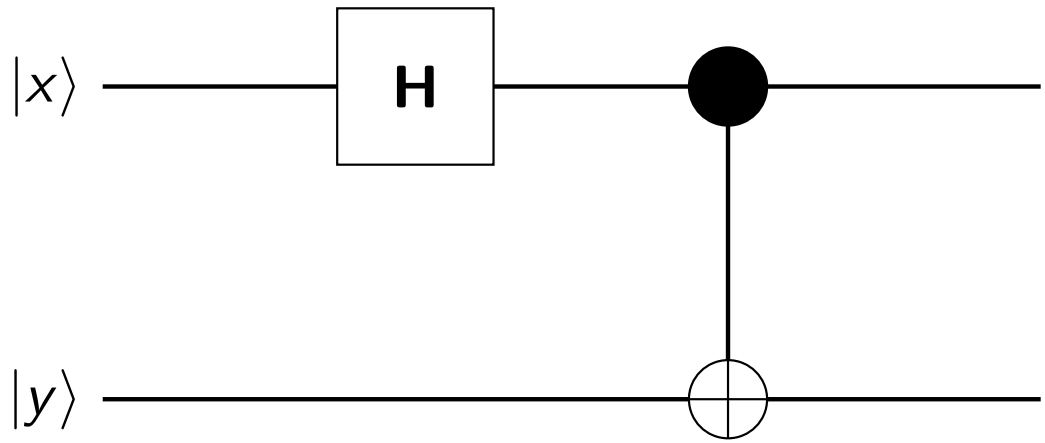
We can express the standard base in terms of Bell states:

$$
\begin{aligned}
|00\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle) \\
|01\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle) \\
|10\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle - |\psi^-\rangle) \\
|11\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle)
\end{aligned}
$$

Note that the four Bell states are entangled, i.e. can only be represented as linear combinations.

"Computing" Bell States

We can construct Bell states from standard base states using the Hadamard gate (similar to the one qubit case).

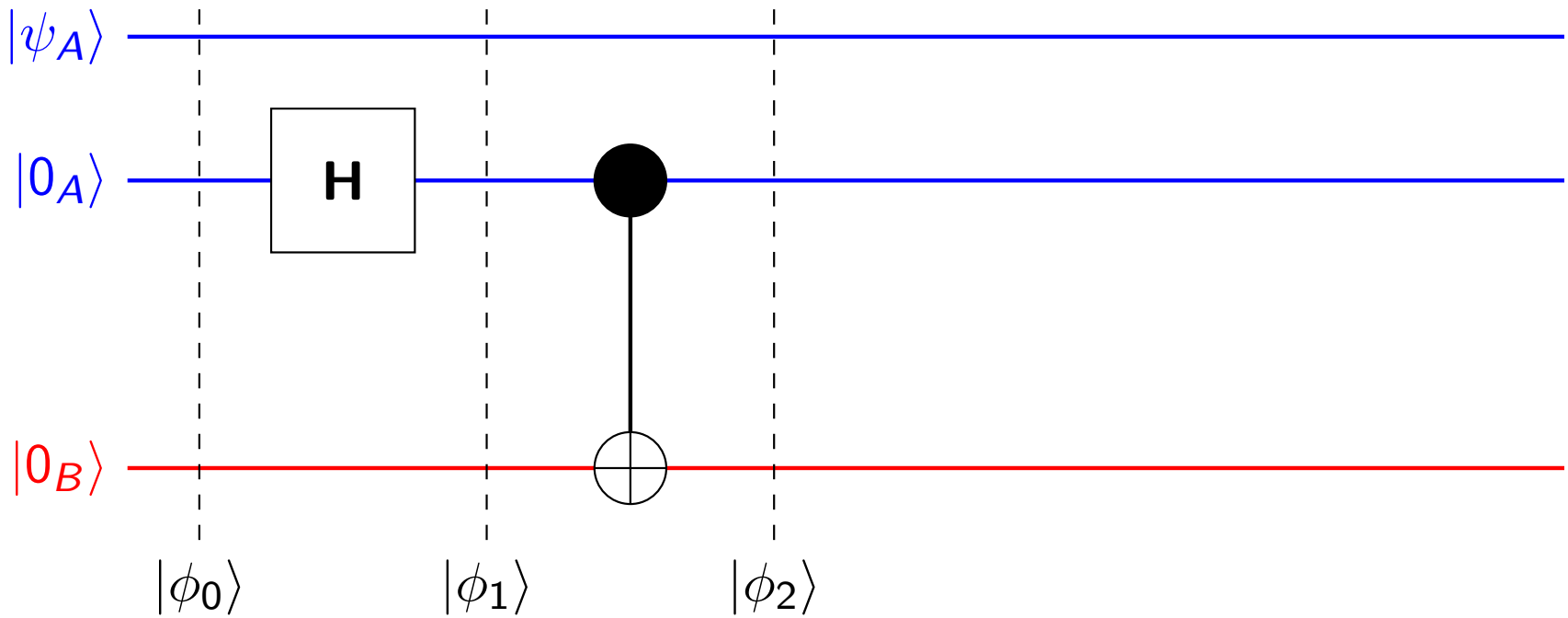


$$|00\rangle \mapsto \left|\phi^+\right\rangle \qquad |01\rangle \mapsto \left|\psi^+\right\rangle \qquad |10\rangle \mapsto \left|\phi^-\right\rangle \qquad |11\rangle \mapsto \left|\psi^-\right\rangle$$

$$|\beta_{00}\rangle = \left|\phi^+\right\rangle \qquad |\beta_{01}\rangle = \left|\psi^+\right\rangle \qquad |\beta_{10}\rangle = \left|\phi^-\right\rangle \qquad |\beta_{11}\rangle = \left|\psi^-\right\rangle$$

Step 1: Entangled Bell State

Create two qubits which are entangled in state $|\phi^+\rangle$. One of these, one qubit is given to Alice – who also is in charge of another (unknown) qubit $|\psi\rangle$ – the other to Bob.



Step 1: States

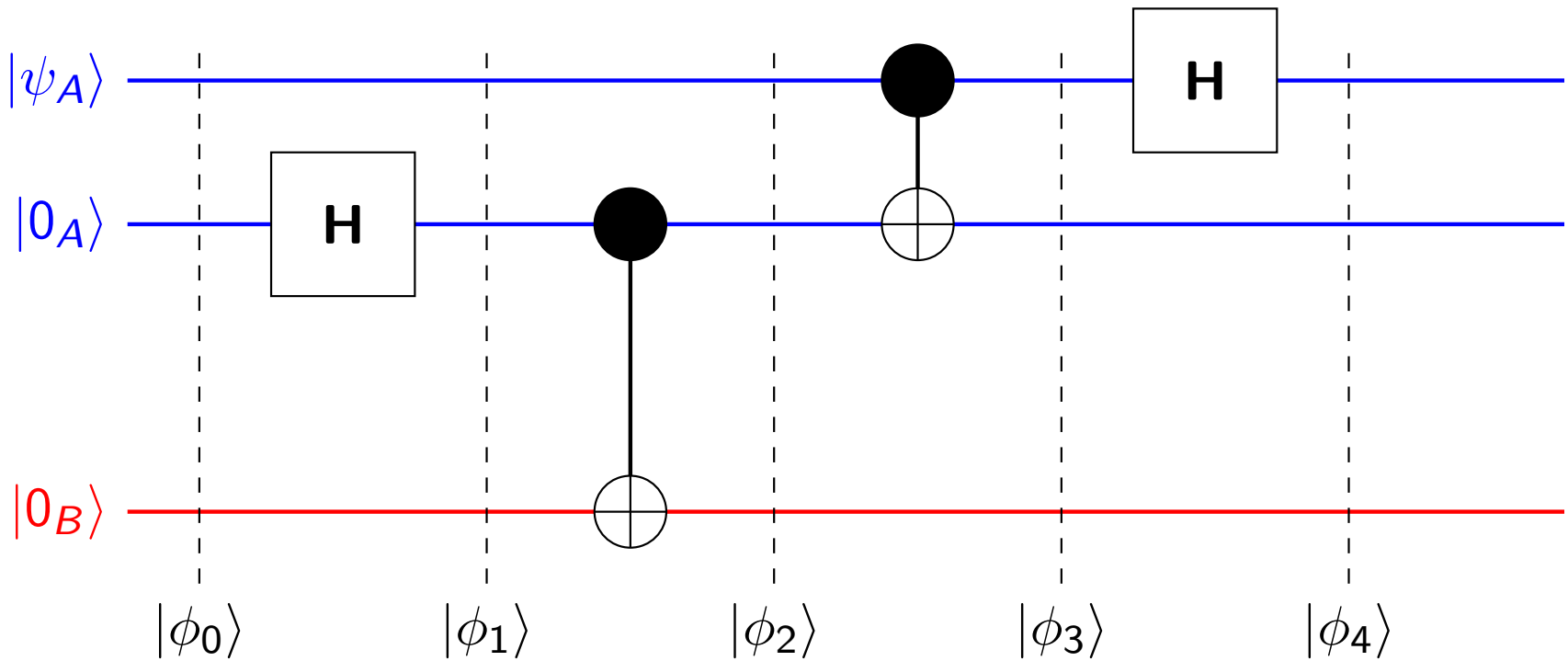
$$|\phi_0\rangle = |\psi\rangle \otimes |0\rangle \otimes |0\rangle$$

$$|\phi_1\rangle = |\psi\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$$

$$\begin{aligned}
|\phi_2\rangle &= |\psi\rangle \otimes \left|\phi^+\right\rangle \\
&= |\psi\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= \frac{1}{\sqrt{2}}(\alpha\,|0\rangle(|00\rangle + |11\rangle) + \beta\,|1\rangle(|00\rangle + |11\rangle))
\end{aligned}$$

Step 2: Entangle $|\psi\rangle$

On Alice's side we entangle the unknown qubit $|\psi\rangle$ with her qubit in the Bell state $|\phi^+\rangle$.



Step 2: States

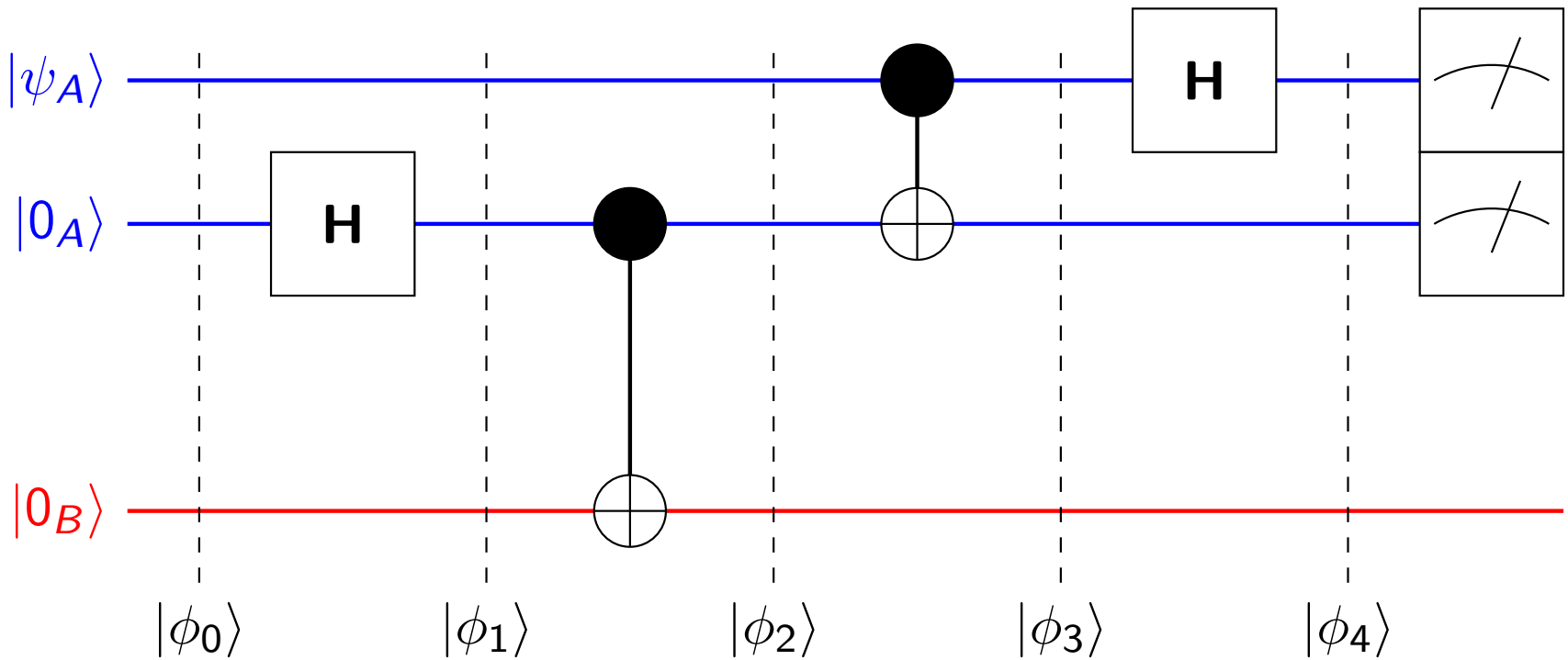
$$|\phi_2\rangle = \frac{1}{\sqrt{2}}(\alpha\,|0\rangle(|00\rangle + |11\rangle) + \beta\,|1\rangle(|00\rangle + |11\rangle))$$

$$|\phi_3\rangle = \frac{1}{\sqrt{2}}(\alpha\,|0\rangle(|00\rangle + |11\rangle) + \beta\,|1\rangle(|10\rangle + |01\rangle))$$

$$\begin{aligned}
|\phi_4\rangle &= \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)) \\
&= \frac{1}{2}(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) \\
&\quad +\beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)) \\
&= \frac{1}{2}(|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\beta\,|0\rangle + \alpha\,|1\rangle) \\
&\quad + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(-\beta\,|0\rangle + \alpha\,|1\rangle))
\end{aligned}$$

Step 3: Measurement

Alice measures her two qubits. As a result all **three** qubits of the system collapse to one of the four possible states.



Example

For example: If Alice measures $|10\rangle$ then Bob's qubit is with certainty $\alpha|0\rangle - \beta|1\rangle$.

The problems now are that:

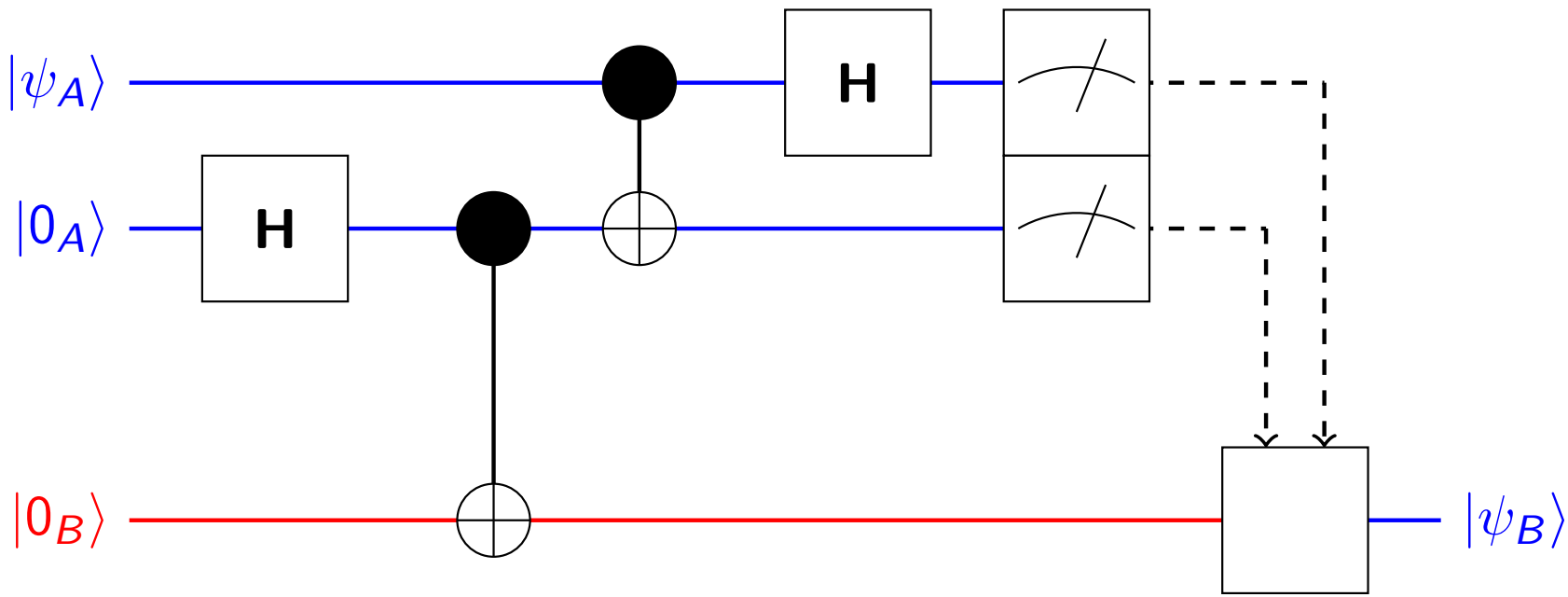
- Alice knows the measurement results, but not Bob.
- Bob's qubit is $\alpha|0\rangle - \beta|1\rangle$ not the initial $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

To overcome there are two remedies:

- Alice sends her measurement results to Bob by **classical** means over a classical channel.
- Bob's qubit has to **reconstructed** depending on the measurement outcome he receives.

Step 4: Teleportation

Alice's sends her measurement results as classical bits to Bob who then transforms his qubit in order to obtain the initial $|\psi\rangle$.



Step 4: Reconstruction

The correction operations which needs to be applied to Bob's qubit in order to obtain the initial $|\psi\rangle$ depending on Alice's bits.

$$\mathbf{C}_{00} \quad \mathbf{C}_{01} \quad \mathbf{C}_{10} \quad \mathbf{C}_{11}$$

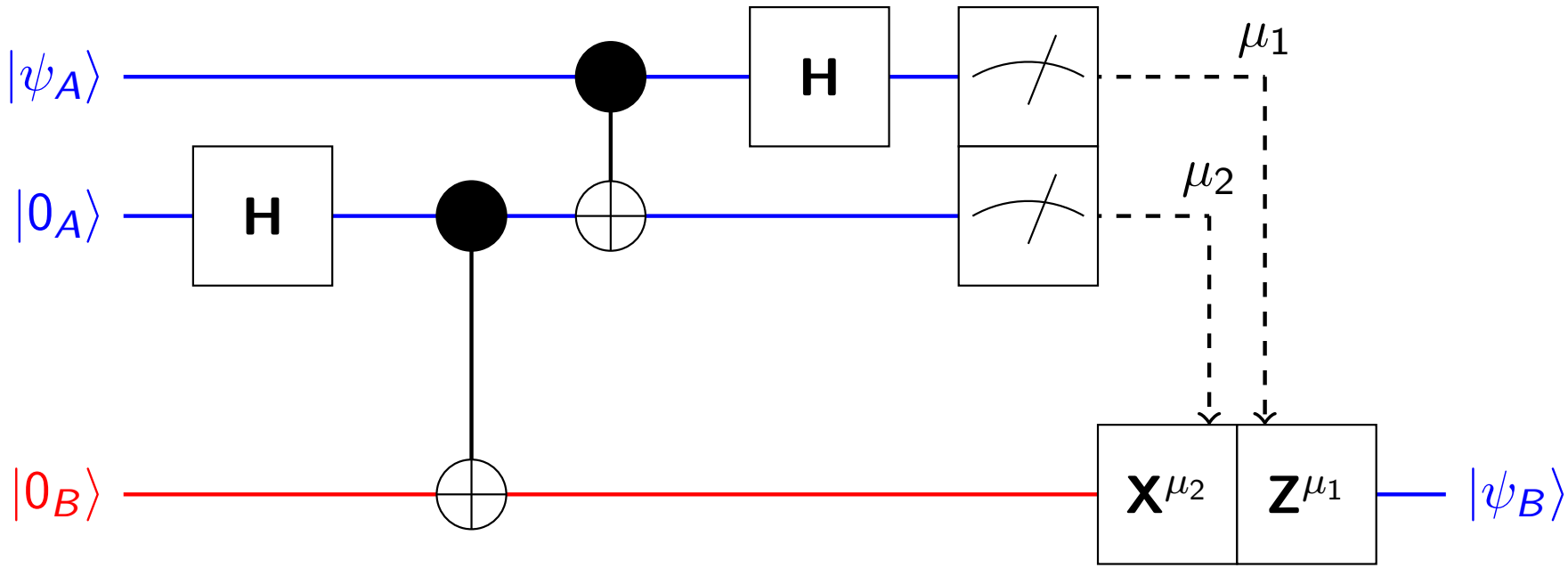
$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Example: If, as before, Alice measures $|10\rangle$ then Bob's qubit is $\alpha|0\rangle - \beta|1\rangle = (\alpha, -\beta)^T$. Applying the matrix for '10' gives:

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle$$

Correction Operation

We can express Bob's correction operations using **Pauli Gates**:



$$\mathbf{C}_{00} = \mathbf{I} \quad \mathbf{C}_{01} = \mathbf{X} \quad \mathbf{C}_{10} = \mathbf{Z} \quad \mathbf{C}_{11} = \mathbf{ZX}$$

Quantum Algorithms

- Goal is to find algorithms in the quantum circuit model that solve problems faster than the best know classical algorithms
- Previous example of Deutsch algorithm to decide if f on $\{0, 1\}$ is balanced or constant: two classical queries versus one quantum query
- Computational complexity theory: classifying computational problems according to their difficulty
- Decision problem is a problem with a yes/no answer
  $\Rightarrow$ basis for definition of computational complexity classes

Complexity classes (informally)

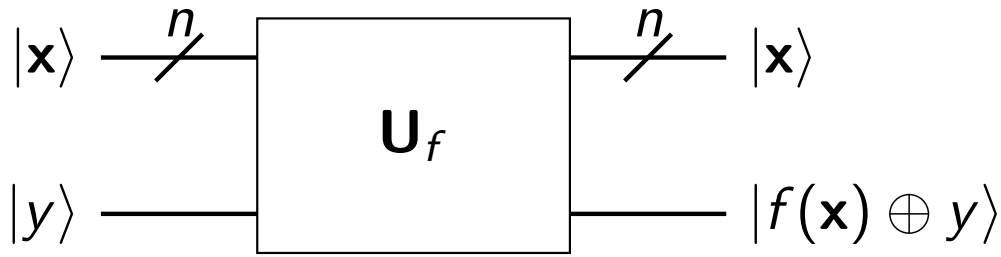
- **P** = polynomial size (in the length of the input n) classical circuit that obtains the right answer
- **BPP** = unbounded randomness + polynomial size classical circuit that obtains the right answer with probability $p > \frac{1}{2}$
  $\Rightarrow$ efficient on classical computers (e.g., n, n^2, n^3)
- **EQP** = polynomial size quantum circuit that obtains the right answer
- **BQP** = polynomial size quantum circuit that obtains the right answer with probability $p > \frac{1}{2}$
  $\Rightarrow$ efficient on quantum computers
- Ultimate question about super-polynomial speed-up:
  Are there problems in **BQP** that are not in **P**/**BPP**?

Deutsch-Jozsa Problem

Consider Deutsch's problem for functions $f : \{0,1\}^n \to \{0,1\}$.

A function $f : \{0,1\}^n \to \{0,1\}$ is said to be:

- balanced: $f(\mathbf{x}) = 0$ or $f(\mathbf{x}) = 1$ for exactly half the inputs
- constant: $f(\mathbf{x}) = 0$ or $f(\mathbf{x}) = 1$ for all inputs



Here $|\mathbf{x}\rangle$ represents an n-qubit register, i.e. $|\mathbf{x}\rangle = |x_0 x_1 x_2 \ldots x_{n-1}\rangle$.

Function Representation

It is straight forward to construct the matrix representation $\mathbf{U}_f$.
For example, for a function $f : \{0,1\}^2 \to \{0,1\}$ we write:

$$f = \begin{cases} 00 & \mapsto & 1 \\ 01 & \mapsto & 1 \\ 10 & \mapsto & 0 \\ 11 & \mapsto & 0 \end{cases} \qquad \mathbf{U}_f = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Some Notation: Binary "Inner Product"

Consider two n bit-stings ($x_i, y_i \in \{0,1\}$):

$$\mathbf{x} = x_0 x_1 \ldots x_{n-1} \qquad \mathbf{y} = y_0 y_1 \ldots y_{n-1}$$

We have the bitwise exclusive-or:

$$\mathbf{x} \oplus \mathbf{y} = (x_0 \oplus y_0)(x_1 \oplus y_1) \ldots (x_{n-1} \oplus y_{n-1})$$

Define a "binary" inner product (in fact $(\mathbb{Z}_2)^n \to \mathbb{Z}_2$):

$$[\mathbf{x}, \mathbf{y}] = (x_0 \wedge y_0) \oplus (x_1 \wedge y_1) \oplus \ldots \oplus (x_{n-1} \wedge y_{n-1})$$

Helpful properties of $[\mathbf{x}, \mathbf{y}]$ and $\mathbf{x} \oplus \mathbf{y}$ for example:

$$[\mathbf{x} \oplus \mathbf{x}', \mathbf{y}] = [\mathbf{x}, \mathbf{y}] \oplus [\mathbf{x}', \mathbf{y}] \qquad [\mathbf{x}, \mathbf{y} \oplus \mathbf{y}'] = [\mathbf{x}, \mathbf{y}] \oplus [\mathbf{x}, \mathbf{y}']$$

$$[0^n, \mathbf{y}] = 0 = [\mathbf{x}, 0^n]$$

Multi-Hadamard Gates

To deal with n qubit registers we need to consider the nth tensor product of Hadamard gates $\mathbf{H}^{\otimes n}$.

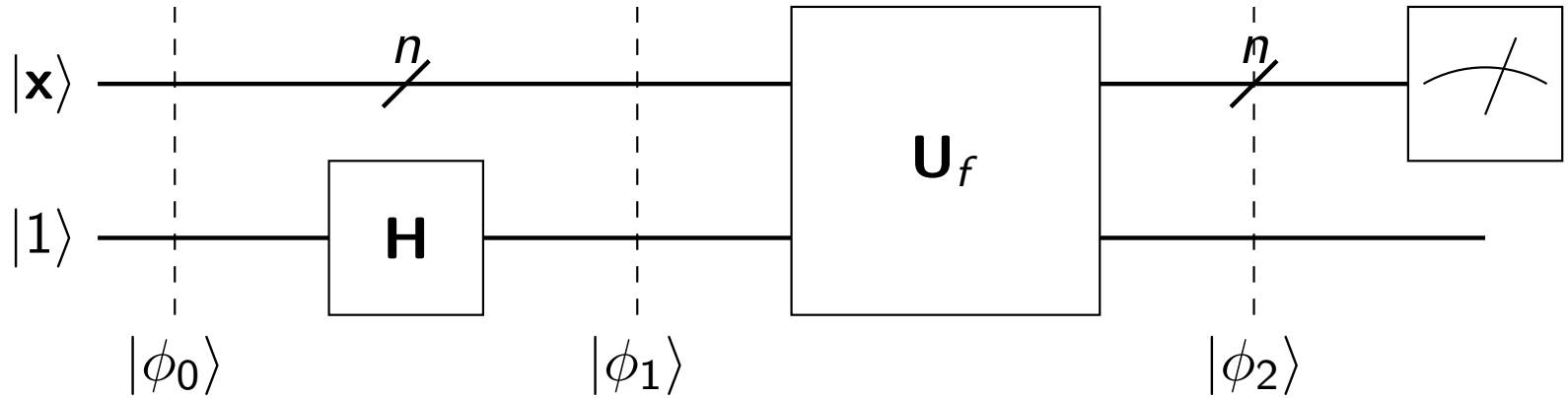
One can show (by induction) that

$$(\mathbf{H}^{\otimes n})_{\mathbf{ij}} = \frac{1}{\sqrt{2^n}}(-1)^{[\mathbf{i},\mathbf{j}]}$$

and that for an arbitrary base state $|\mathbf{y}\rangle$ in $(\mathbb{C}^2)^{\otimes n}$

$$\mathbf{H}^{\otimes n}\,|\mathbf{y}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{[\mathbf{x},\mathbf{y}]}\,|\mathbf{x}\rangle$$

A Too Weak Attempt



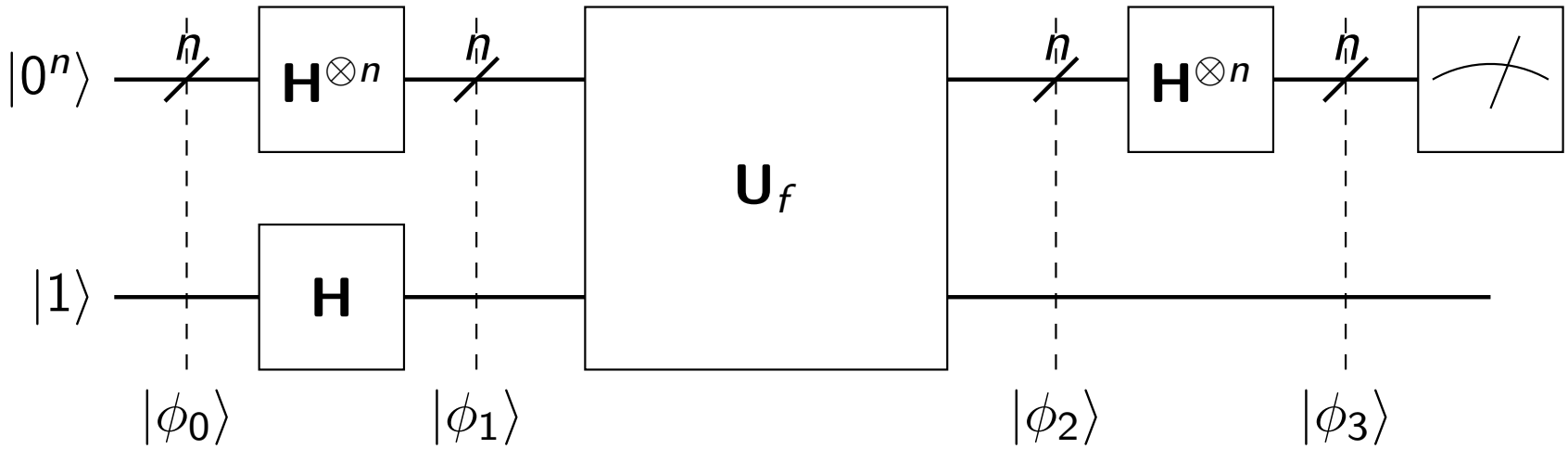
$$|\phi_0\rangle = |\mathbf{x}1\rangle$$

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}(|\mathbf{x}0\rangle - |\mathbf{x}1\rangle)$$

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}|\mathbf{x}\rangle\left(|f(\mathbf{x}) \oplus 0\rangle - |f(\mathbf{x}) \oplus 1\rangle\right) = \frac{1}{\sqrt{2}}|\mathbf{x}\rangle\left(|f(\mathbf{x})\rangle - |\overline{f(\mathbf{x})}\rangle\right)$$

$$|\phi_2\rangle = (-1)^{f(\mathbf{x})}\frac{1}{\sqrt{2}}|\mathbf{x}\rangle\left(|0\rangle - |1\rangle\right)$$

Deutsch-Jozsa Circuit



$$|\phi_0\rangle = |0^n 1\rangle = |0^n\rangle \otimes |1\rangle$$

$$|\phi_1\rangle = \frac{1}{\sqrt{2^n}}\Big(\sum_{\mathbf{x}\in\{1,0\}^n} |\mathbf{x}\rangle\Big) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\phi_2\rangle = \frac{1}{\sqrt{2^n}}\Big(\sum_{\mathbf{x}\in\{1,0\}^n} (-1)^{f(\mathbf{x})}\,|\mathbf{x}\rangle\Big) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Deutsch-Jozsa States

$$
\begin{aligned}
|\phi_3\rangle &= \frac{1}{2^n}\left(\sum_{\mathbf{x}\in\{1,0\}^n}(-1)^{f(\mathbf{x})}\sum_{\mathbf{y}\in\{1,0\}^n}(-1)^{[\mathbf{y},\mathbf{x}]}\,|\mathbf{y}\rangle\right)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\\
&= \frac{1}{2^n}\left(\sum_{\mathbf{x}\in\{1,0\}^n}\sum_{\mathbf{y}\in\{1,0\}^n}(-1)^{f(\mathbf{x})}(-1)^{[\mathbf{y},\mathbf{x}]}\,|\mathbf{y}\rangle\right)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\\
&= \frac{1}{2^n}\left(\sum_{\mathbf{x}\in\{1,0\}^n}\sum_{\mathbf{y}\in\{1,0\}^n}(-1)^{f(\mathbf{x})\oplus[\mathbf{y},\mathbf{x}]}\,|\mathbf{y}\rangle\right)\otimes\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)
\end{aligned}
$$

Question: What is the probability that $|\phi_3\rangle$ collapses $|0^n\rangle$?

Measurement

Consider $\mathbf{y} = 0^n$. This implies $[\mathbf{y}, \mathbf{x}] = [0^n, \mathbf{x}] = 0$ for all $\mathbf{x}$. We get

$$|\phi_3\rangle = \frac{1}{2^n} \left(\sum_{\mathbf{x} \in \{1,0\}^n} (-1)^{f(\mathbf{x})} |0^n\rangle \right) \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

- For f constant 1:

$$|\phi_3\rangle' = \frac{1}{2^n} \sum_{\mathbf{x} \in \{1,0\}^n} (-1) |0^n\rangle = \frac{-(2^n)}{2^n} |0^n\rangle = -1 |0^n\rangle$$

- For f constant 0:

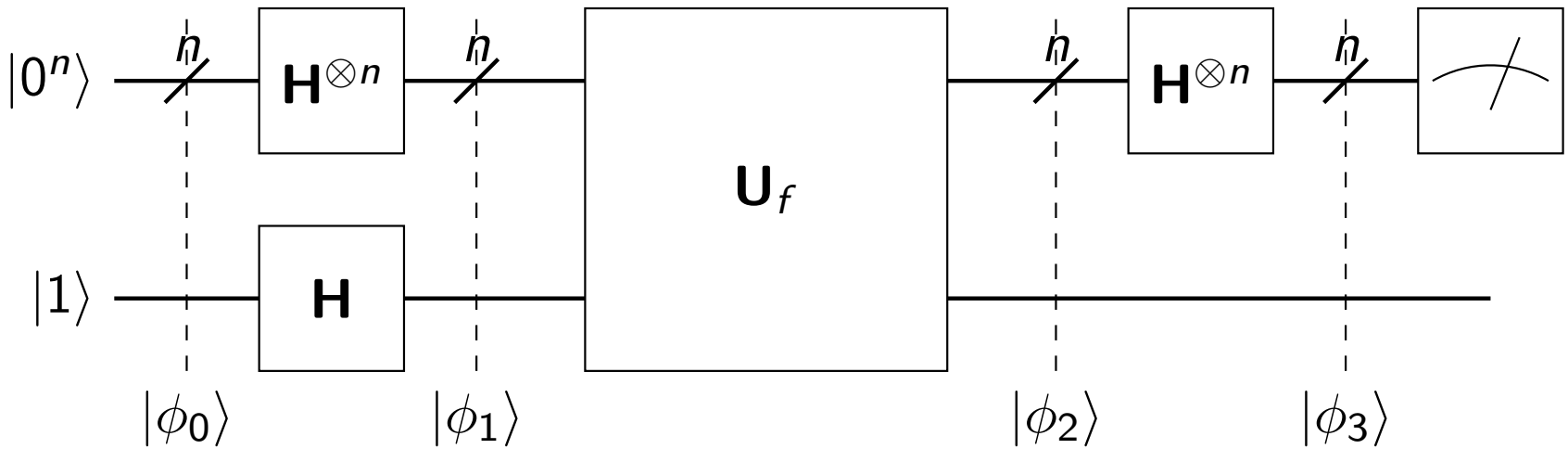
$$|\phi_3\rangle' = \frac{1}{2^n} \sum_{\mathbf{x} \in \{1,0\}^n} (+1) |0^n\rangle = \frac{+(2^n)}{2^n} |0^n\rangle = +1 |0^n\rangle$$

- For f balanced:

$$|\phi_3\rangle' = \frac{1}{2^n} \sum_{\mathbf{x} \in \{1,0\}^n} (-1)^{f(\mathbf{x})} |0^n\rangle = \frac{0}{2^n} |0^n\rangle = 0 |0^n\rangle$$

Summary Deutsch-Jozsa

Assuming that we have a function $f : \{0,1\}^n \to \{0,1\}$ which is either **constant** or **balanced**.



If the measurement of the first/upper n qubits of $|\phi_3\rangle$ returns ($|\phi_3\rangle$ collapse to):

$|0^n\rangle$ then f is **constant**,

anything else then f is **balanced** $\Rightarrow$ separates **P** vs. **EQP**

Simon's Problem

- Given a function $f : \{0,1\}^n \to \{0,1\}^n$ and the promise that for some unknown $\mathbf{c} \in \{0,1\}^n$ we have for all $\mathbf{x}, \mathbf{y} \in \{0,1\}^n$

$$f(\mathbf{x}) = f(\mathbf{y}) \quad \Leftrightarrow \quad \mathbf{x} = \mathbf{y} \oplus \mathbf{c},$$

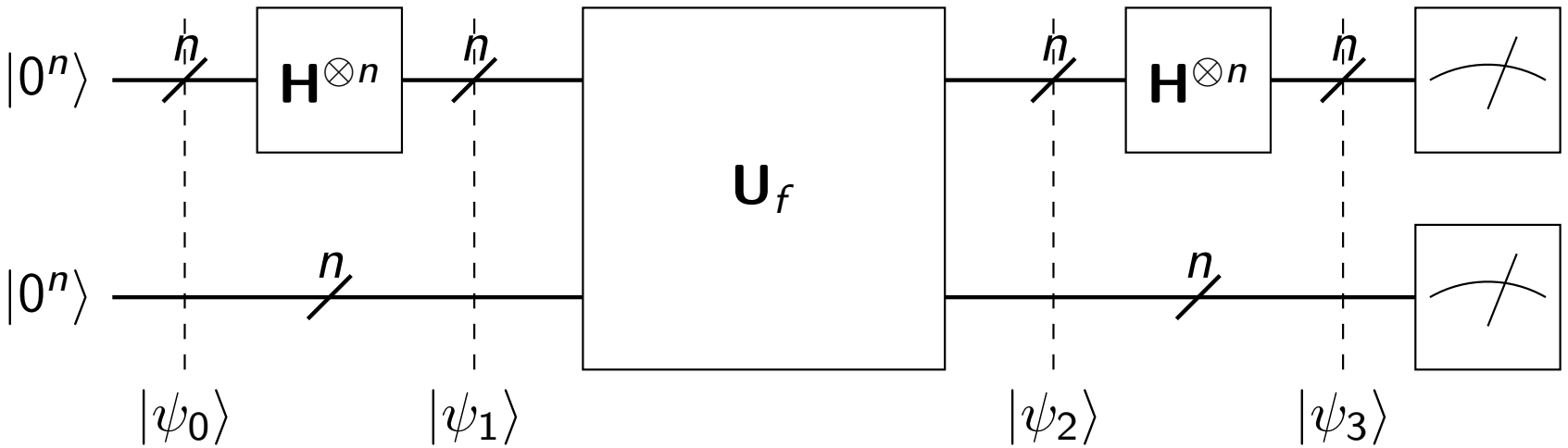
  the task is to determine $\mathbf{c}$ (the period of f).
- Classically, we will just evaluate up to half of the inputs before we get a repeat (if we still cannot find a match then $\mathbf{c} = 0^n$)

$$\mathbf{x}_1 = \mathbf{x}_2 \oplus \mathbf{c} \quad \Rightarrow \quad \mathbf{x}_1 \oplus \mathbf{x}_2 = \mathbf{x}_1 \oplus \mathbf{c} \oplus \mathbf{x}_2 = \mathbf{c}.$$

  That is, worst case we need $2^{n-1} + 1$ queries on f.
- Lower bound still holds under randomized algorithms (**BPP**).

Simon's Problem (continued)

- Quantum algorithm with n queries on f as follows



- Simon's algorithms succeeds with constant probability (at least $\frac{1}{4}$) in determining $\mathbf{c}$, which is improved via repetition
  $\Rightarrow$ separates **BPP** vs. **BQP**