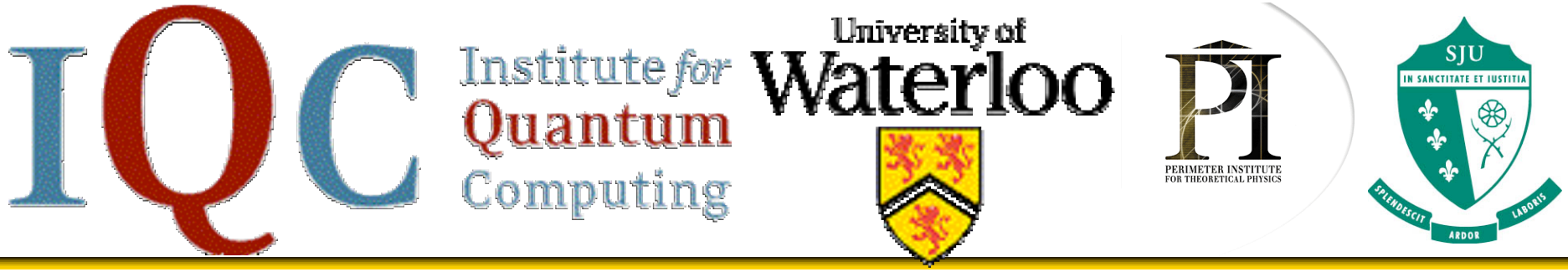


Basic Quantum Algorithms

Michele Mosca

Canada Research Chair in Quantum Computation

PIMS-MITACS Summer School on Quantum Information Science

June 2003

IQC Institute for Quantum Computing

Centre for Applied Cryptographic Research

The University of Waterloo

SJU
IN SANCTITATE ET IUSTITIA
SPLENDESCIT ARDOR LABORIS

www.iqc.ca

PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

Perimeter Institute is a community of theoretical physicists dedicated to investigating fundamental issues in theoretical physics.

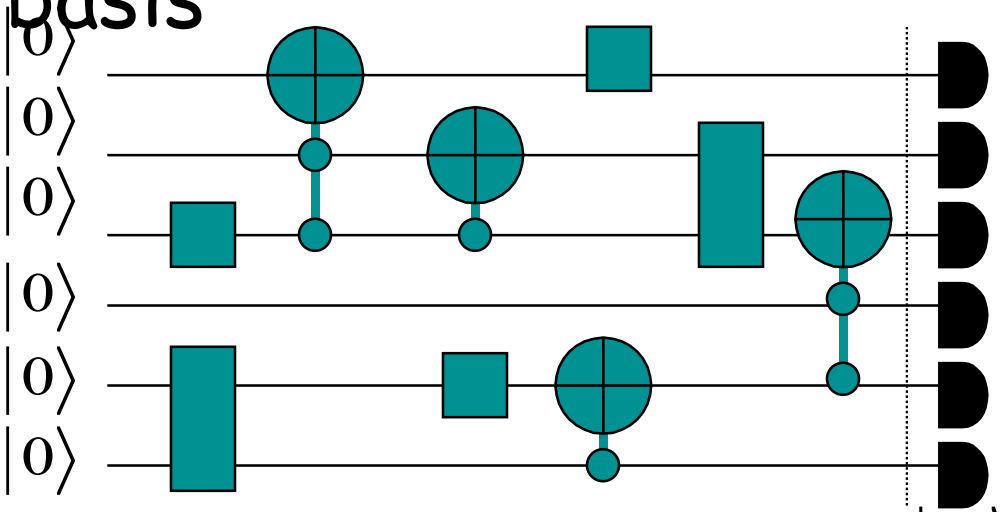
www.perimeterinstitute.ca

Overview

- Partial and implicit measurements
- Basis changes
- Eigenvalue kick-back
- Some simple algorithms

A Quantum Computing Model

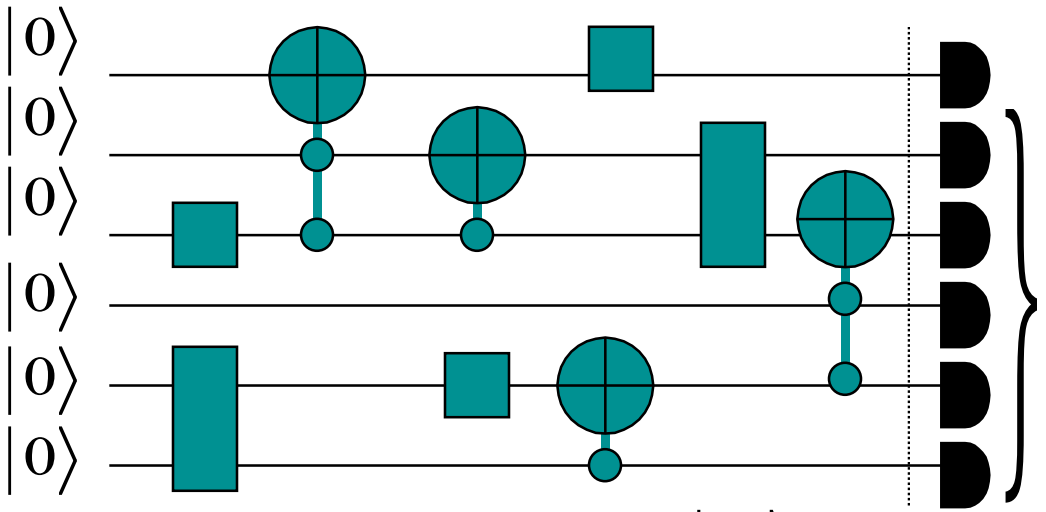
Acyclic circuits of *unitary* gates (from a finite "universal set") and von Neumann measurements in the "computational" basis



$$|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

Partial Measurement

Suppose we only look at the outcome of the bottom n-1 bits.

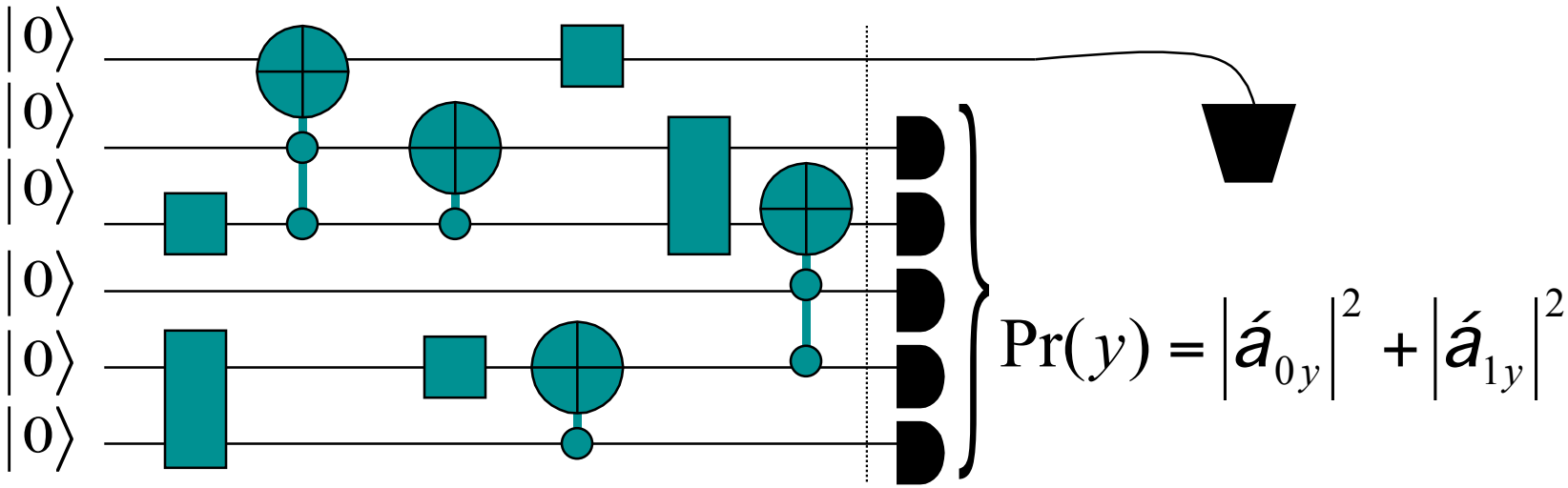


$$\Pr(y) = \left|\alpha_{0y}\right|^2 + \left|\alpha_{1y}\right|^2$$

$$|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

Implicit Measurement

The probability outcome is not affected by whether or not we measure the first qubit.



$$|\varphi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

Partial Measurement

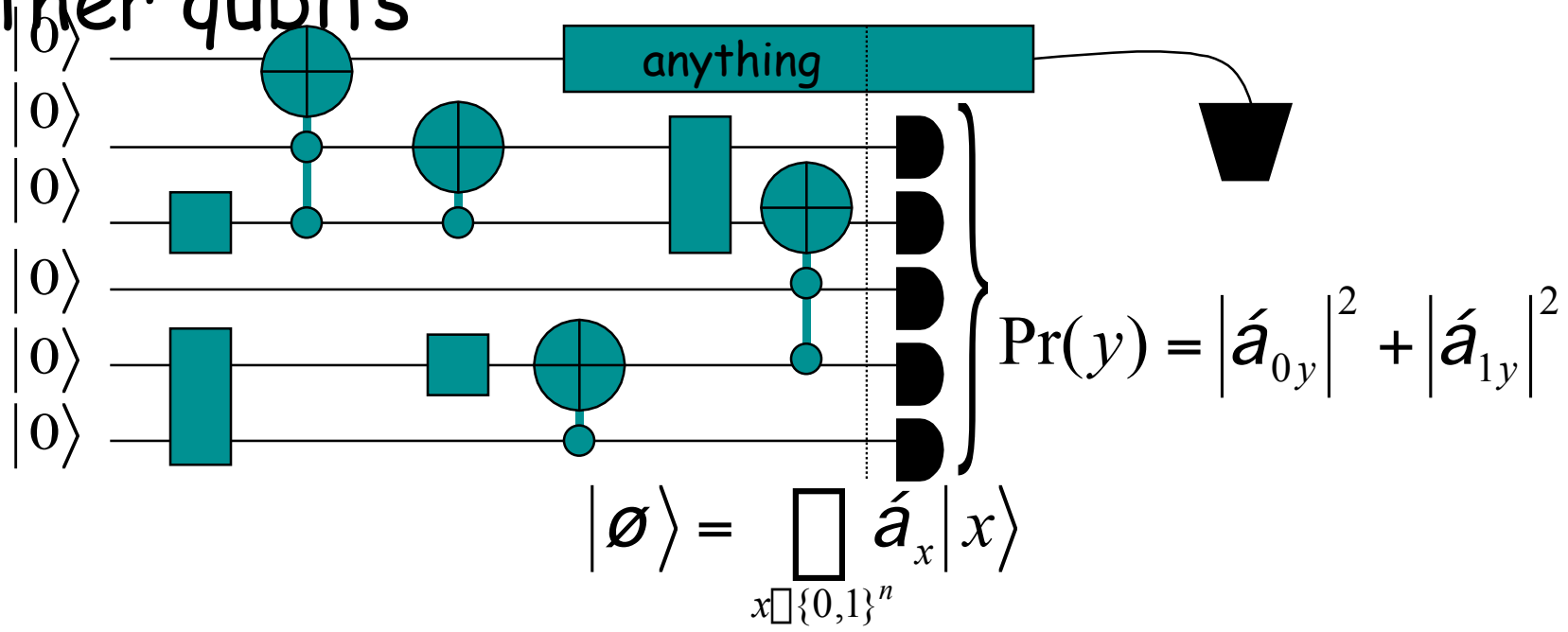
If we don't measure the first qubit, it will be found in the state $\frac{1}{\left|\alpha_{0y}\right|^2+\left|\alpha_{1y}\right|^2}\left(\alpha_{0y}\left|0\right\rangle+\alpha_{1y}\left|1\right\rangle\right)$

$$\left|\phi\right\rangle=\sum_{x\in\{0,1\}^n}\alpha_x\left|x\right\rangle=\sum_{y\in\{0,1\}^{n-1}}\alpha_{0y}\left|0y\right\rangle+\alpha_{1y}\left|1y\right\rangle$$

$$=\sum_{y\in\{0,1\}^{n-1}}\sqrt{\Pr(y)}\left(\frac{\alpha_{0y}}{\sqrt{\Pr(y)}}\left|0\right\rangle+\frac{\alpha_{1y}}{\sqrt{\Pr(y)}}\left|1\right\rangle\right)\left|y\right\rangle$$

Implicit Measurement

The probability outcome is not affected by any operations we do to the first qubit after it last interacts with the other qubits



BASIS CHANGES

Distinguishing orthogonal states

Given a state

$$|\phi\rangle \in B = \{|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_N\rangle\}$$

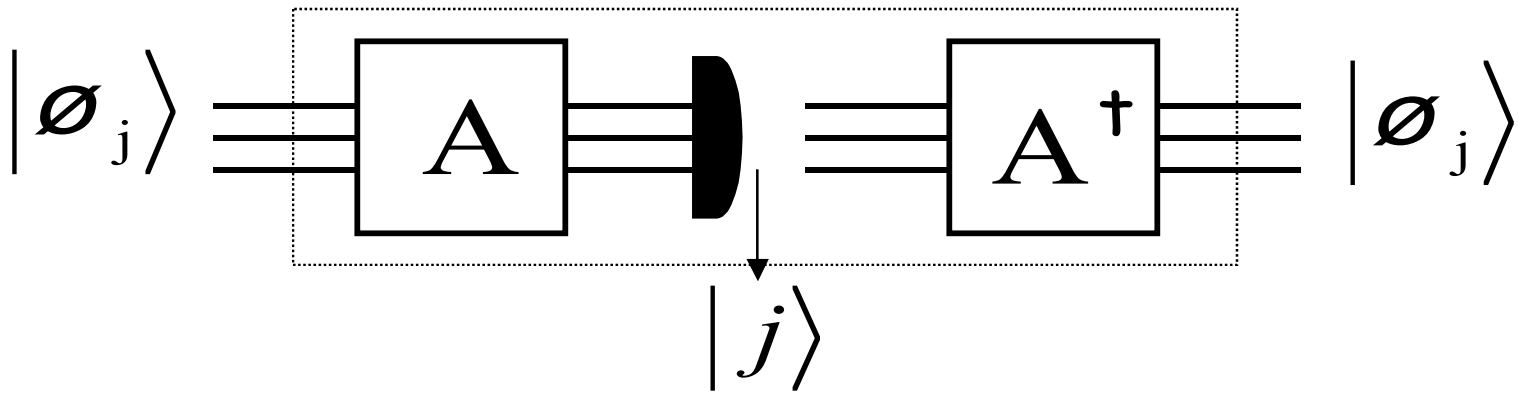
$$\langle \phi_i | \phi_j \rangle = \delta_{ij}$$

we can in principle determine which state we have by "performing a Von Neumann measurement with respect to the basis B"

Distinguishing orthogonal states

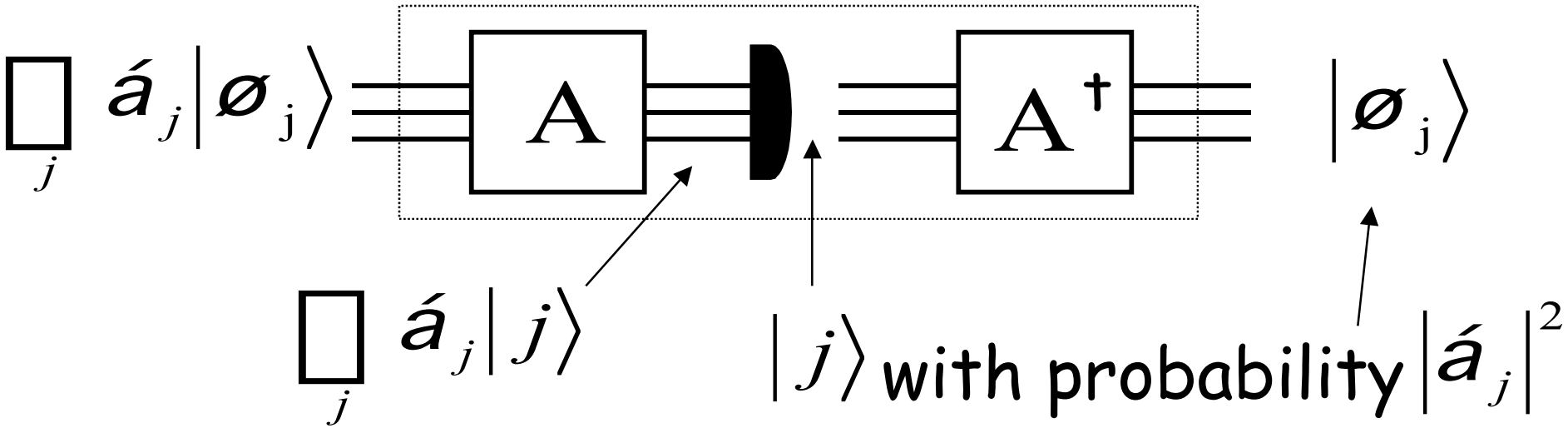
We can implement this measurement efficiently if we can efficiently implement the unitary transformation

$$A\left|\varnothing_j\right\rangle = \left|j\right\rangle$$



In general

We can measure any state wrt the basis B in this way



The Hadamard basis change

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

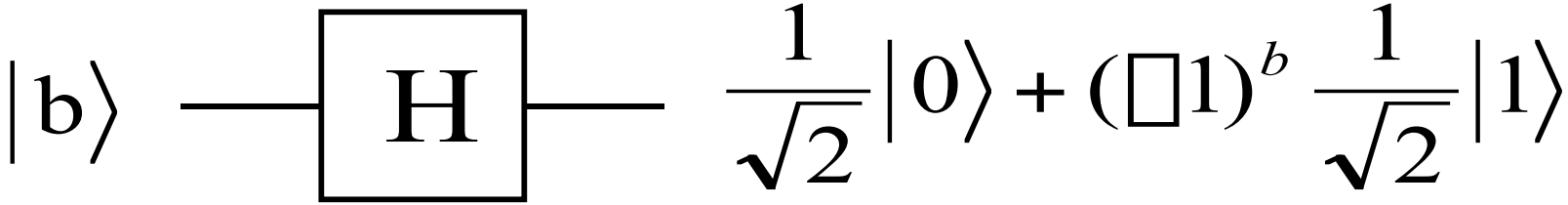
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{H} |0\rangle$$

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{H} |1\rangle$$

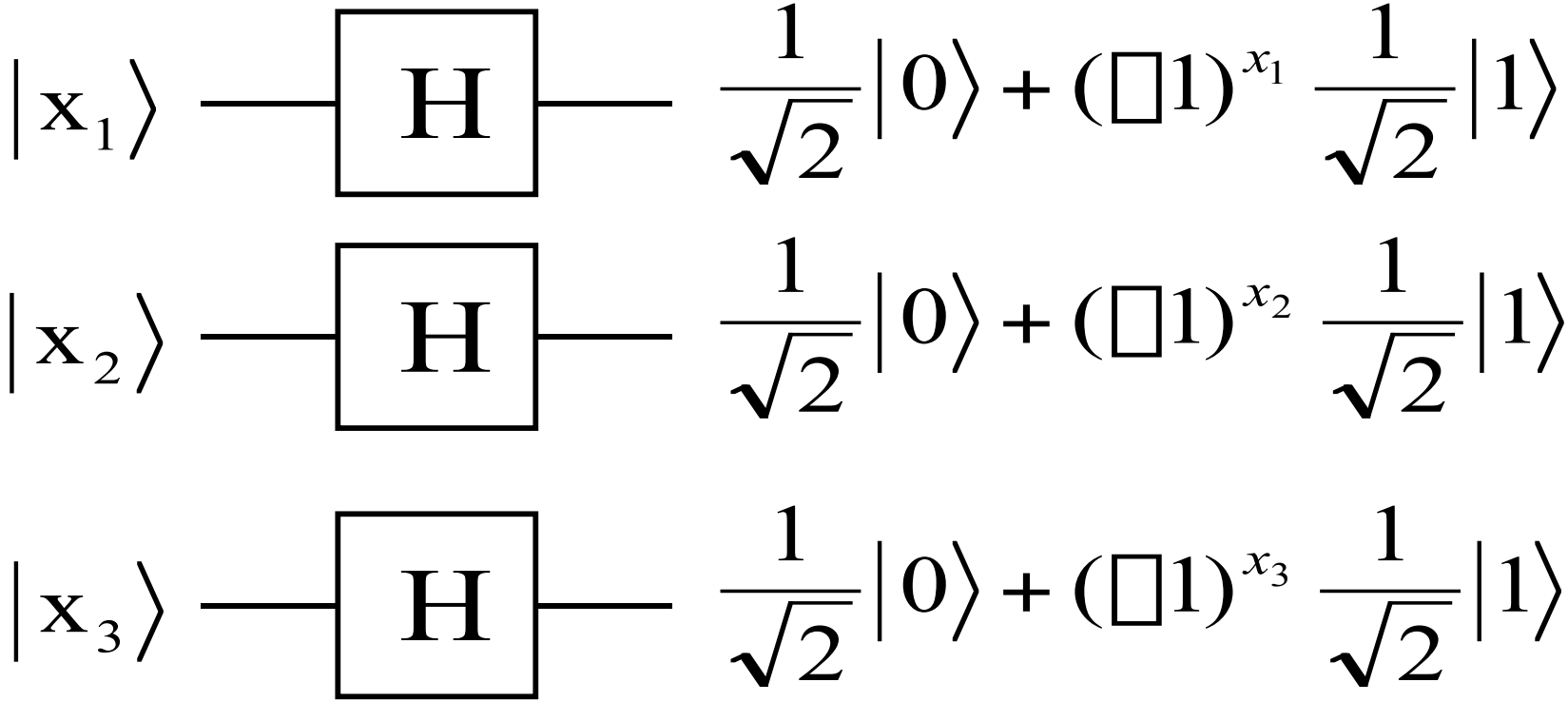
The Hadamard transformation: summary

$$|b\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle + (-1)^{b}\frac{1}{\sqrt{2}}|1\rangle$$

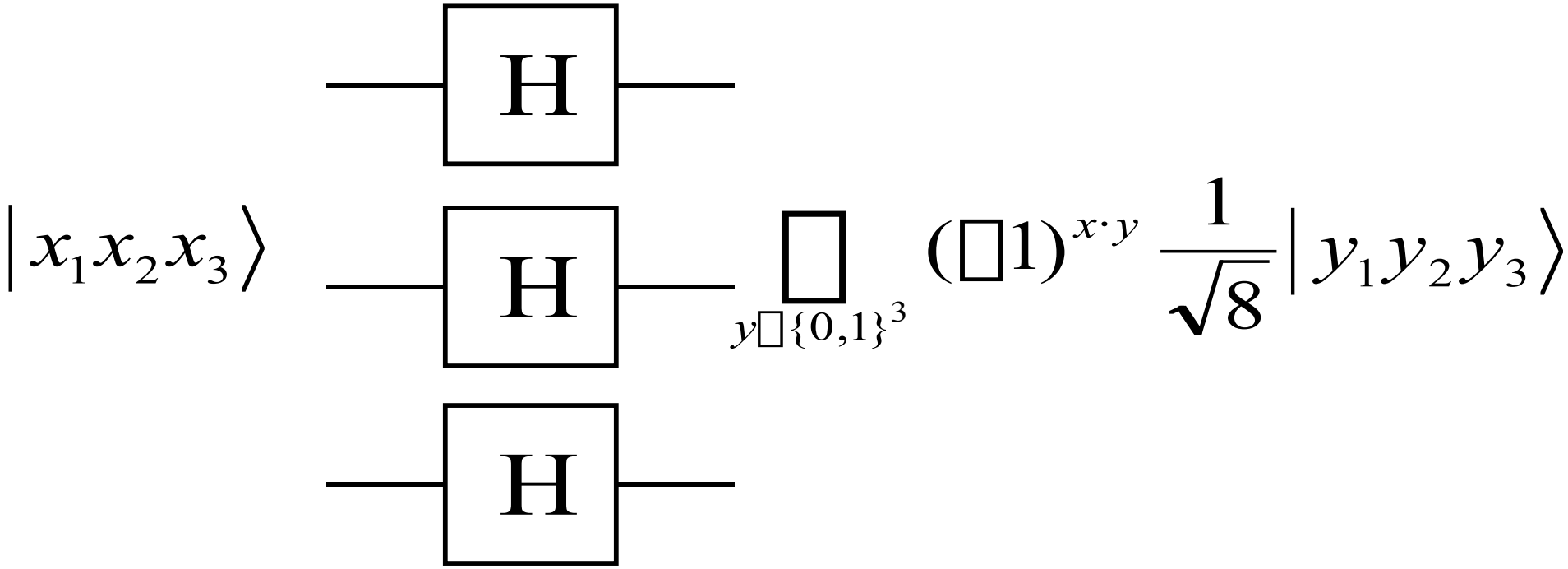
The Hadamard transformation: circuit notation



The Hadamard transformation on several bits



The Hadamard transformation: global view



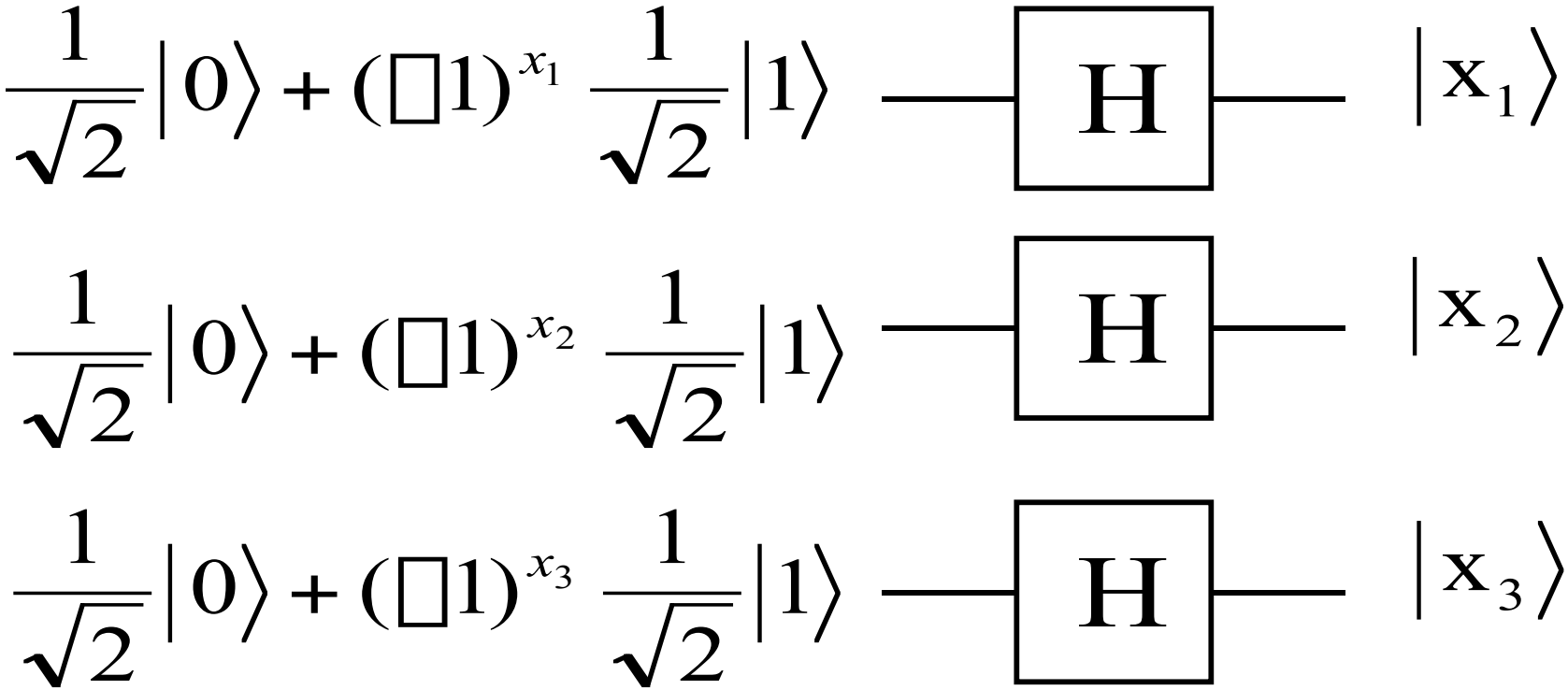
The Hadamard transformation: global view

$$\left|x_1 x_2 x_3\right\rangle \rightarrow H \otimes H \otimes H \rightarrow \sum_{y \in \{0,1\}^3} (-1)^{x \cdot y} \frac{1}{\sqrt{8}} \left|y_1 y_2 y_3\right\rangle$$

The Hadamard transformation: global view

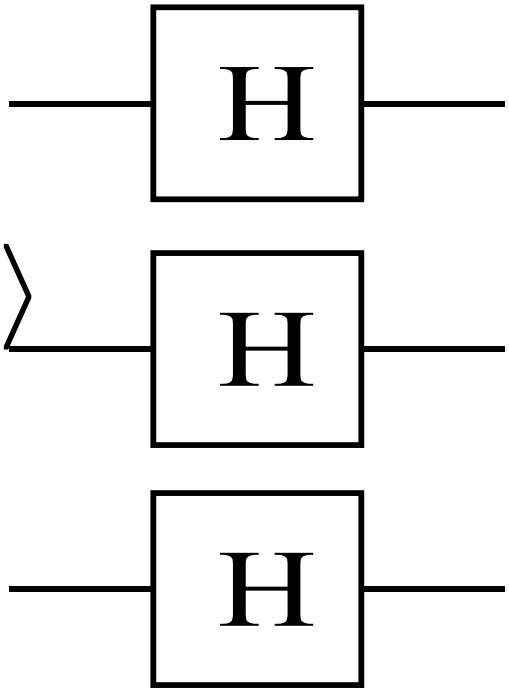
$$H \quad H \quad H\left|x_1x_2x_3\right\rangle = \sum_{y\in\{0,1\}^3} (-1)^{x\cdot y}\frac{1}{\sqrt{8}}\left|y_1y_2y_3\right\rangle$$

The Hadamard transformation on several bits



The Hadamard transformation: global view

$$\sum_{y \in \{0,1\}^3} (-1)^{x \cdot y} \frac{1}{\sqrt{8}} |y_1 y_2 y_3\rangle$$



$$|x_1 x_2 x_3\rangle$$

The Hadamard transformation: global view

$$\sum_{y \in \{0,1\}^3} (-1)^{x \cdot y} \frac{1}{\sqrt{2}} |y_1 y_2 y_3\rangle \; \square \; H \; H \; H \; \square \; |x_1 x_2 x_3\rangle$$

Looking at NOT and CNOT in Hadamard bases

Consider applying a NOT (or "X") gate to the following states

$$|0\rangle + |1\rangle \xrightarrow{X} |0\rangle + |1\rangle$$

$$|0\rangle - |1\rangle \xrightarrow{X} -(|0\rangle - |1\rangle)$$

In other words:

$$X = HZH \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

e.g.

Now consider applying a controlled-NOT gate to the following states

$$|0\rangle(|0\rangle + |1\rangle) \xrightarrow{\text{CNOT}} |0\rangle(|0\rangle + |1\rangle)$$

$$|1\rangle(|0\rangle + |1\rangle) \xrightarrow{\text{CNOT}} |1\rangle(|0\rangle + |1\rangle)$$

$$|0\rangle(|0\rangle - |1\rangle) \xrightarrow{\text{CNOT}} |0\rangle(|0\rangle - |1\rangle)$$

$$|1\rangle(|0\rangle - |1\rangle) \xrightarrow{\text{CNOT}} -|1\rangle(|0\rangle - |1\rangle)$$

e.g.

Now consider applying a controlled-NOT gate to the following states

$$(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \xrightarrow{\text{CNOT}} (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$$

$$(|0\rangle - |1\rangle)(|0\rangle + |1\rangle) \xrightarrow{\text{CNOT}} (|0\rangle - |1\rangle)(|0\rangle + |1\rangle)$$

$$(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \xrightarrow{\text{CNOT}} (|0\rangle - |1\rangle)(|0\rangle - |1\rangle)$$

$$(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) \xrightarrow{\text{CNOT}} (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$$

Eigenvalue kick-back

Computing functions into the phase

Suppose we know how to compute a function

$$f : \{0,1\} \to \{0,1\}$$

$$|x\rangle|c\rangle \xrightarrow{U_f} |x\rangle|c \oplus f(x)\rangle$$

$$|x\rangle\left(|0\rangle - |1\rangle\right) \to (-1)^{f(x)}|x\rangle\left(|0\rangle - |1\rangle\right)$$

Computing functions into the phase

Suppose we know how to compute a function

$$|x\rangle|c\rangle \xrightarrow{U_f} |x\rangle|c \oplus f(x)\rangle$$

$$|x\rangle\left(|0\rangle - |1\rangle\right) = |x\rangle|0\rangle - |x\rangle|1\rangle$$

$$\xrightarrow{a} |x\rangle|f(x)\rangle - |x\rangle|\overline{f(x)}\rangle$$

$$= |x\rangle\left(|f(x)\rangle - |\overline{f(x)}\rangle\right)$$

$$= (-1)^{f(x)}|x\rangle\left(|0\rangle - |1\rangle\right)$$

Generalization: Eigenvalue "kick-back"

Suppose we know how to compute an operator $U|\varnothing\rangle = e^{i\ddot{O}}|\varnothing\rangle$

Then the "controlled-U" gives us

$$c\square U|0\rangle|\varnothing\rangle = |0\rangle|\varnothing\rangle$$

$$c\square U|1\rangle|\varnothing\rangle = e^{i\ddot{O}}|1\rangle|\varnothing\rangle$$

$$c\square U\left(|0\rangle + |1\rangle\right)|\varnothing\rangle = \left(|0\rangle + e^{i\ddot{O}}|1\rangle\right)|\varnothing\rangle$$

Must make the "global" phase a "relative" phase

A global phase has no physical significance.

In other words, states that differ only by a global phase are equivalent

$$U\left(\sum_x \alpha_x |x\rangle\right) = \sum_x \beta_x |x\rangle$$

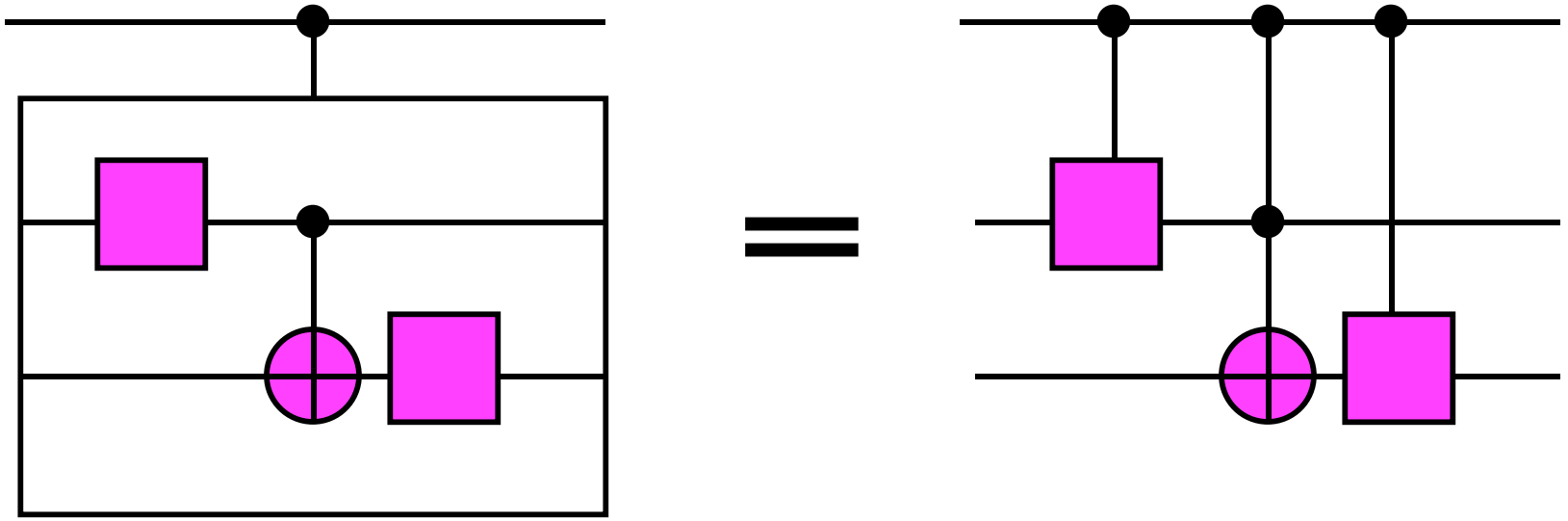
$$U\left(e^{i\theta}\sum_x \alpha_x |x\rangle\right) = e^{i\theta}\sum_x \beta_x |x\rangle$$

so $e^{i\theta}|\psi\rangle \equiv |\psi\rangle$

How do we implement c-U?

Replace every gate G in the circuit for with a c-G.

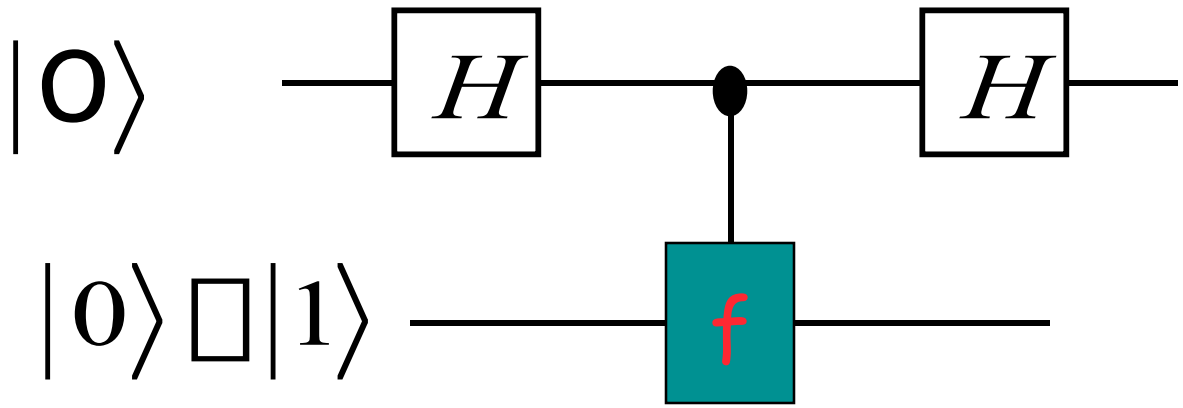
For example,



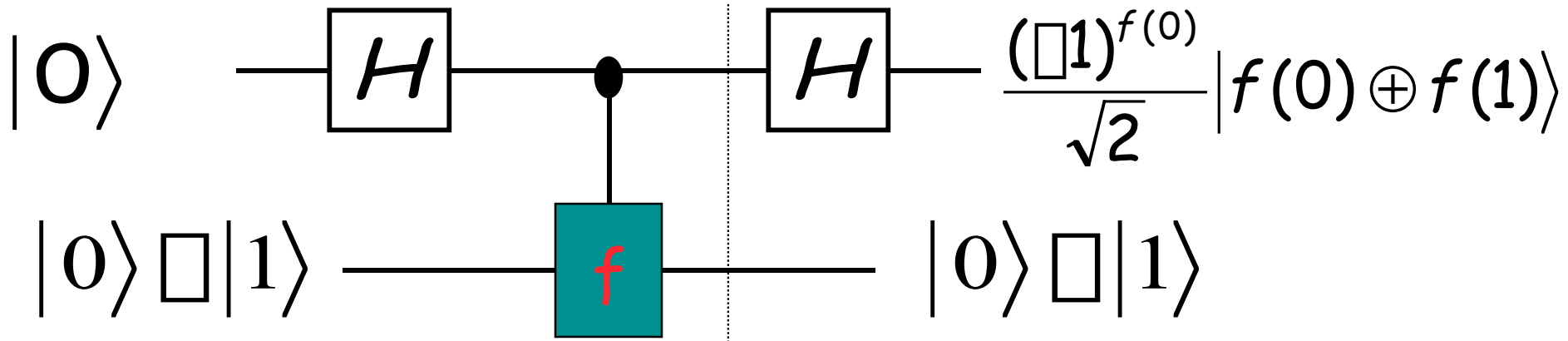
SOME SIMPLE ALGORITHMS

Deutsch's problem

Compute $f(0) \oplus f(1)$ using U_f only once



Deutsch algorithm



$$\frac{(\square 1)^{f(0)}}{\sqrt{2}}\left|f(0)\oplus f(1)\right\rangle$$

$$\frac{1}{\sqrt{2}}\left((\square 1)^{f(0)}\left|0\right\rangle+(\square 1)^{f(1)}\left|1\right\rangle\right)\left(\left|0\right\rangle\square\left|1\right\rangle\right)$$

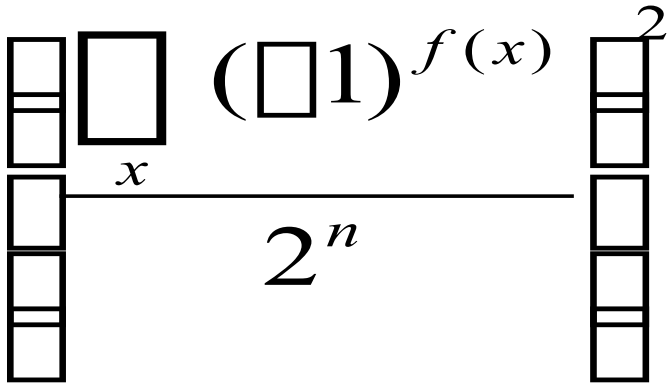
$$=\frac{(\square 1)^{f(0)}}{\sqrt{2}}\left(\left|0\right\rangle+(\square 1)^{f(0)\oplus f(1)}\left|1\right\rangle\right)\left(\left|0\right\rangle\square\left|1\right\rangle\right)$$

Deutsch-Jozsa problem

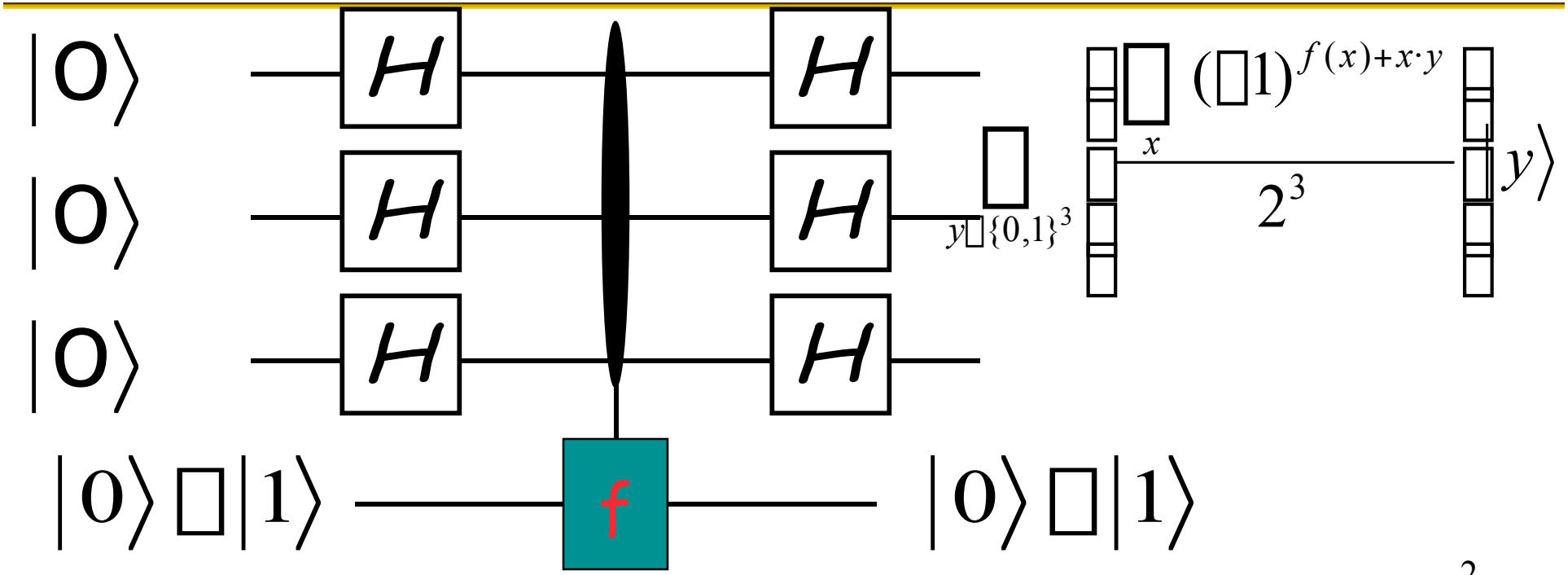
Suppose $f : \{0,1\}^n \to \{0,1\}$ with the promise that f is either constant or "balanced".

Decide if f is constant or balanced.

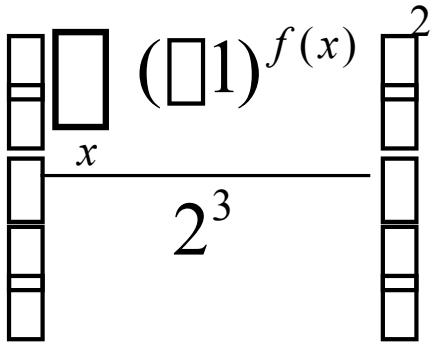
Equivalently, determine



Deutsch-Jozsa problem



Probability of measuring $|000\rangle$ is



i.e. we measure $|000\rangle$ iff f is constant

Bernstein-Vazirani problem

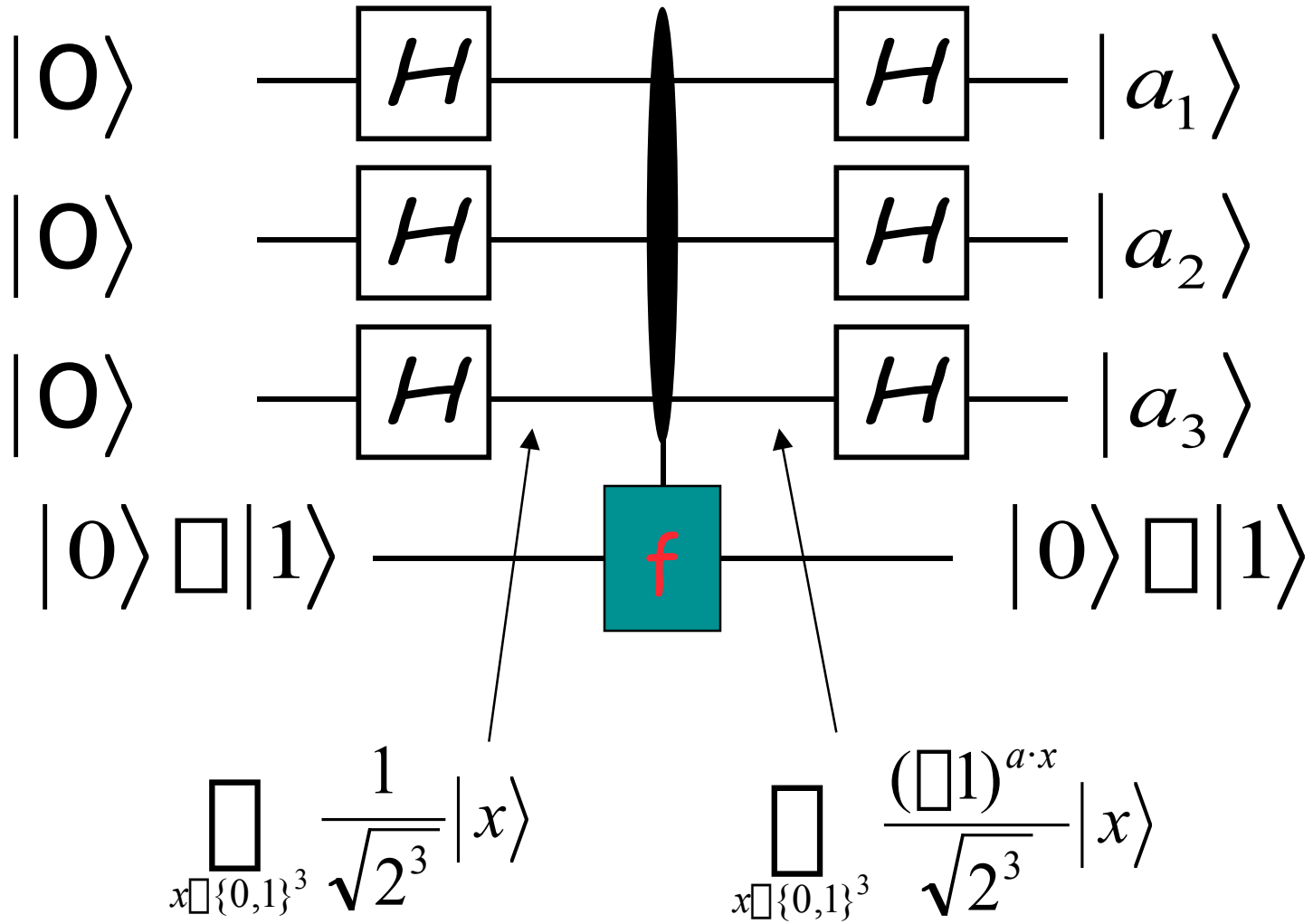
Suppose $f : \{0,1\}^n \to \{0,1\}$ is of the form $f(x) = a \cdot x$ for some $a \in \{0,1\}^n$

Given $|x\rangle|c\rangle \xrightarrow{U_f} |x\rangle|c \oplus f(x)\rangle$

determine

$$a = a_1 a_2 \ldots a_n$$

Bernstein-Vazirani problem



Another property of Hadamard transformation

Consider $S \subseteq Z_2^n$

$$S^{\perp} = \{t : t \in Z_2^n, s \cdot t = 0 \ \forall s \in S\}$$

Let $|y + S\rangle = \sum_{s \in S} \frac{1}{\sqrt{|S|}} |y + s\rangle$

Then

$$H^{\otimes n} |y + S\rangle = \sum_{t \in S^{\perp}} \frac{(-1)^{y \cdot t}}{\sqrt{|S^{\perp}|}} |t\rangle$$

e.g.

Consider $S = \{0, s\}$

Then $|y + S\rangle = \frac{1}{\sqrt{2}}|y\rangle + \frac{1}{\sqrt{2}}|y \oplus s\rangle$

$$H^{\otimes n}|y + S\rangle = \sum_{t} \frac{(-1)^{y \cdot t}}{\sqrt{2^{n-1}}}|t\rangle$$

e.g.

$$H^{\otimes n}|y+S\rangle = \frac{1}{\sqrt{2}} H^{\otimes n}|y\rangle + \frac{1}{\sqrt{2}} H^{\otimes n}|y \oplus s\rangle$$

$$= \frac{1}{\sqrt{2}} \left[\sum_t \frac{(-1)^{y \cdot t}}{\sqrt{2^n}} |t\rangle \right] + \frac{1}{\sqrt{2}} \left[\sum_t \frac{(-1)^{(y \oplus s) \cdot t}}{\sqrt{2^n}} |t\rangle \right]$$

$$= \sum_t \left[\frac{(-1)^{y \cdot t} + (-1)^{(y \oplus s) \cdot t}}{\sqrt{2^{n+1}}} \right] |t\rangle$$

$$= \left[\sum_{t \cdot s = 0} \frac{(-1)^{y \cdot t}}{\sqrt{2^{n-1}}} |t\rangle \right]$$

SIMON's PROBLEM

Simon's problem (special case)

Suppose $f : \{0,1\}^n \to X$ has the property that

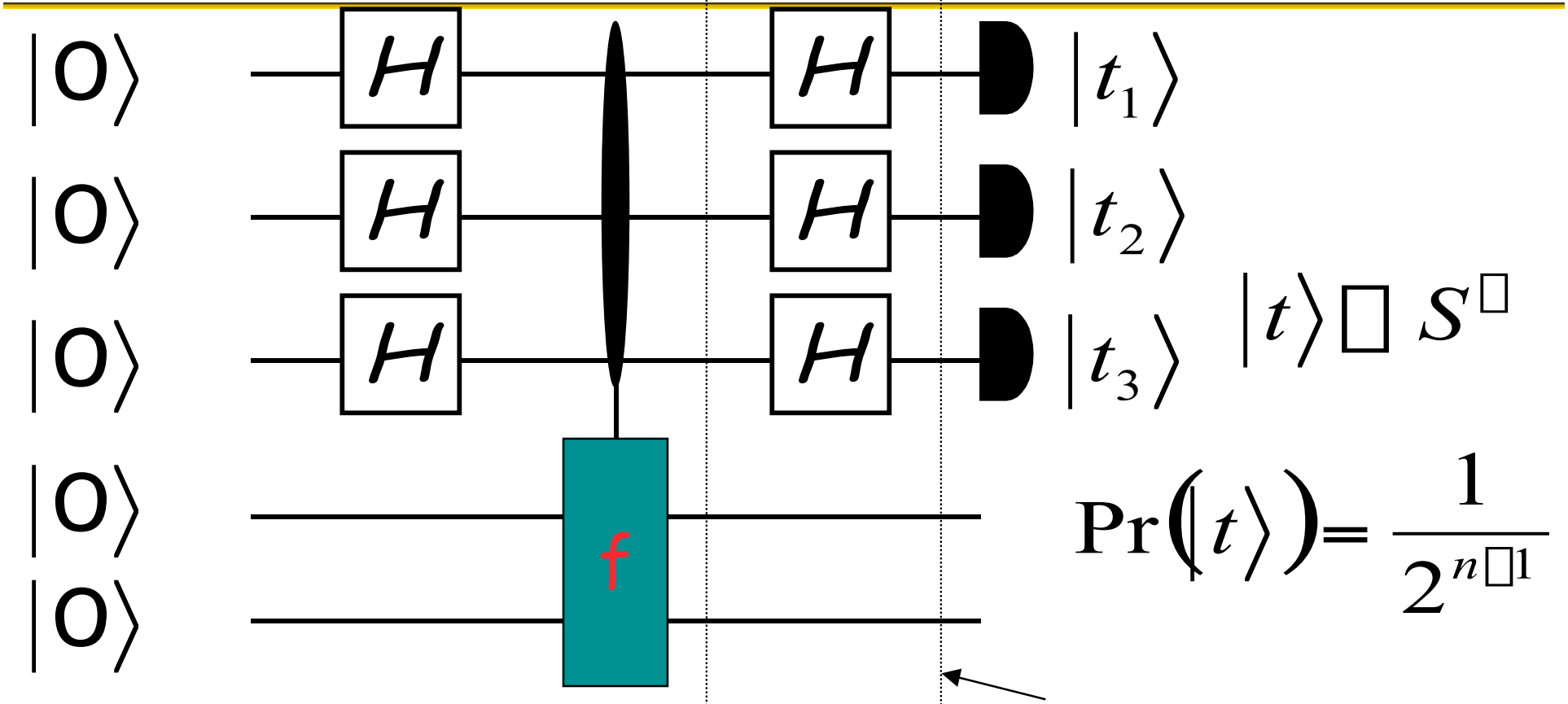
$$f(x) = f(y) \quad \text{iff} \quad x \oplus y \in \{0, s\}$$

$$\text{iff} \quad x + S = y + S$$

For some "hidden subgroup" $S \subseteq Z_2^{\,n}$

Given $|x\rangle|0\rangle \xrightarrow{U_f} |x\rangle|f(x)\rangle$ find S

Simon's algorithm (special case)



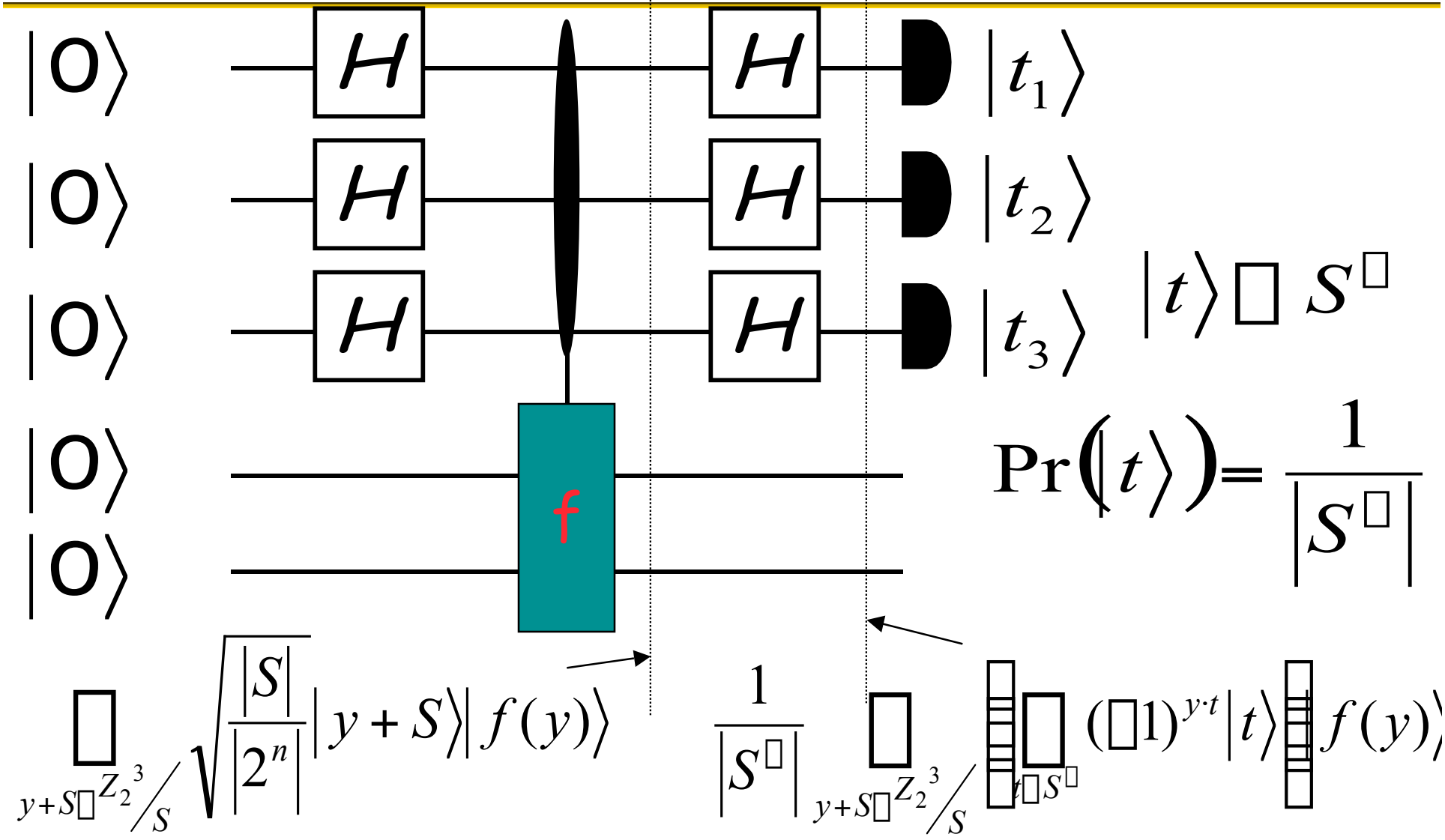
$$|t\rangle \in S^{\perp}$$

$$\Pr(|t\rangle) = \frac{1}{2^{n-1}}$$

$$\sum_{y \in Z_2^3 / S} \sqrt{\frac{1}{2^{n-1}}} \left| \frac{1}{\sqrt{2}} |y\rangle + \frac{1}{\sqrt{2}} |y \oplus s\rangle \right| f(y)\rangle$$

$$\frac{1}{2^{n-1}} \sum_{y \in Z_2^3 / S} \left| \sum_{t \in S^{\perp}} (-1)^{y \cdot t} |t\rangle \right| f(y)\rangle$$

Simon's algorithm (general case)



Abelian Hidden subgroup problem

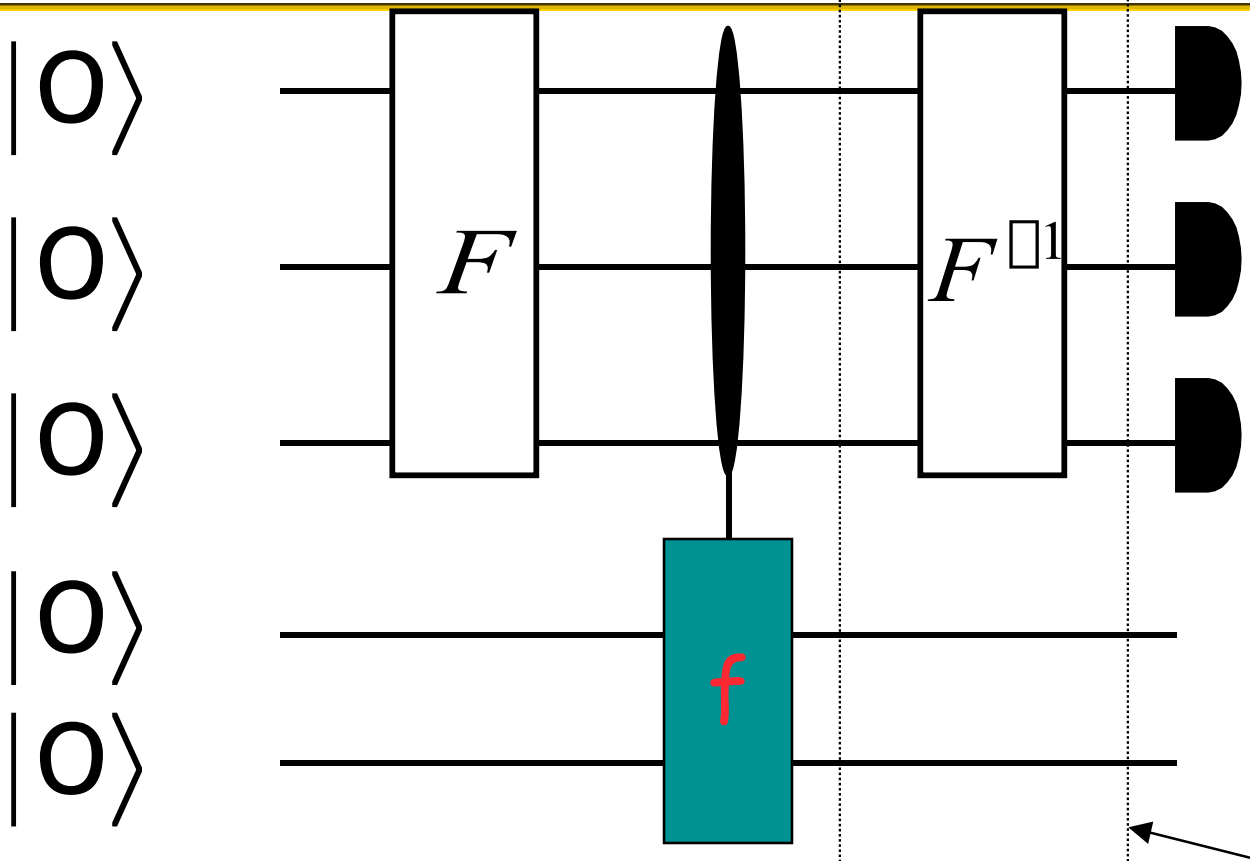
Suppose $f : G \to X$ has the property that

$f(x) = f(y)$ iff $x + S = y + S$

For some "hidden subgroup" $S \subseteq G$

Given $|x\rangle|0\rangle \xrightarrow{U_f} |x\rangle|f(x)\rangle$ find S

Hidden subgroup problem



$$|t\rangle \quad S^{\perp}$$

$$\Pr(|t\rangle) = \frac{1}{|S^{\perp}|}$$

$$\sum_{y+S \in G/S} \sqrt{\frac{1}{|S^{\perp}|}} |y+S\rangle |f(y)\rangle$$

$$\frac{1}{|S^{\perp}|} \sum_{y+S \in G/S} \left(\sum_{t \in S^{\perp}} \alpha_{y,t} |t\rangle \right) |f(y)\rangle$$