Quantum Computer Algorithms: basics

Michele Mosca

MSRI Workshop on Quantum Computation

Overview

- Basis changes
- Eigenvalue kick-back
- Deutsch algorithm
- Deutsch-Jozsa algorithm
- Bernstein-Vazirani algorithm
- Simon's algorithm

Distinguishing orthogonal states

Given a state

$$|\psi\rangle \in B = \{|\psi_1\rangle, |\psi_2\rangle, \mathrm{K}\ , |\psi_N\rangle\}$$

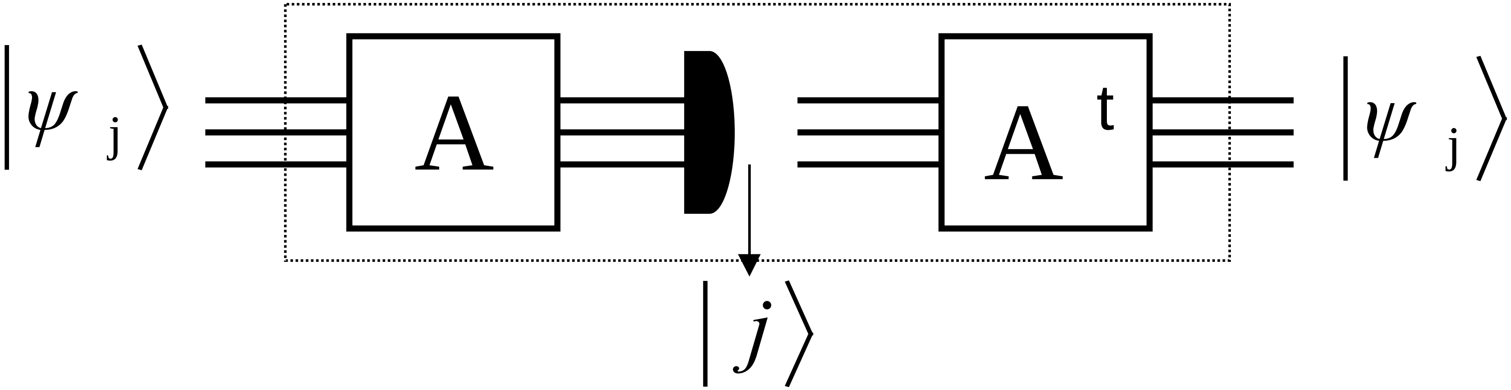
$$\langle\psi_i|\psi_j\rangle = \delta_{ij}$$

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

Distinguishing orthogonal states

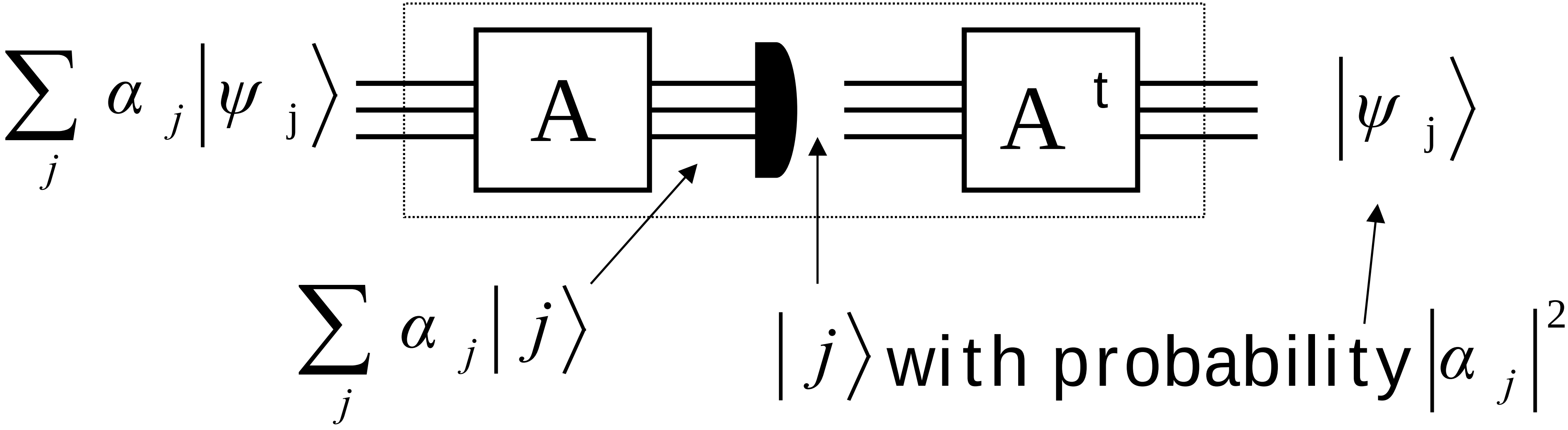
We can implement this measurement efficiently if we can efficiently implement the unitary transformation

$$A|\psi_j\rangle = |j\rangle$$



In general

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



$\sum_j \alpha_j |\psi_j\rangle$

$|\psi_j\rangle$

$\sum_j \alpha_j |j\rangle$

$|j\rangle$ with probability $|\alpha_j|^2$

The Hadamard basis change

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

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

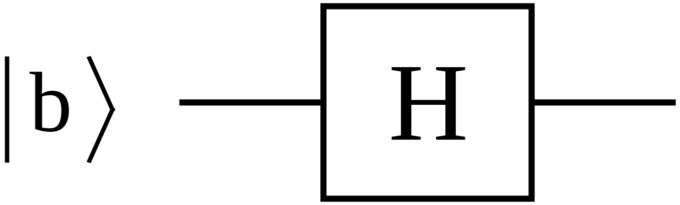
$$\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle \xrightarrow{\text{H}} \left|0\right\rangle$$

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

The Hadamard transformation: summary

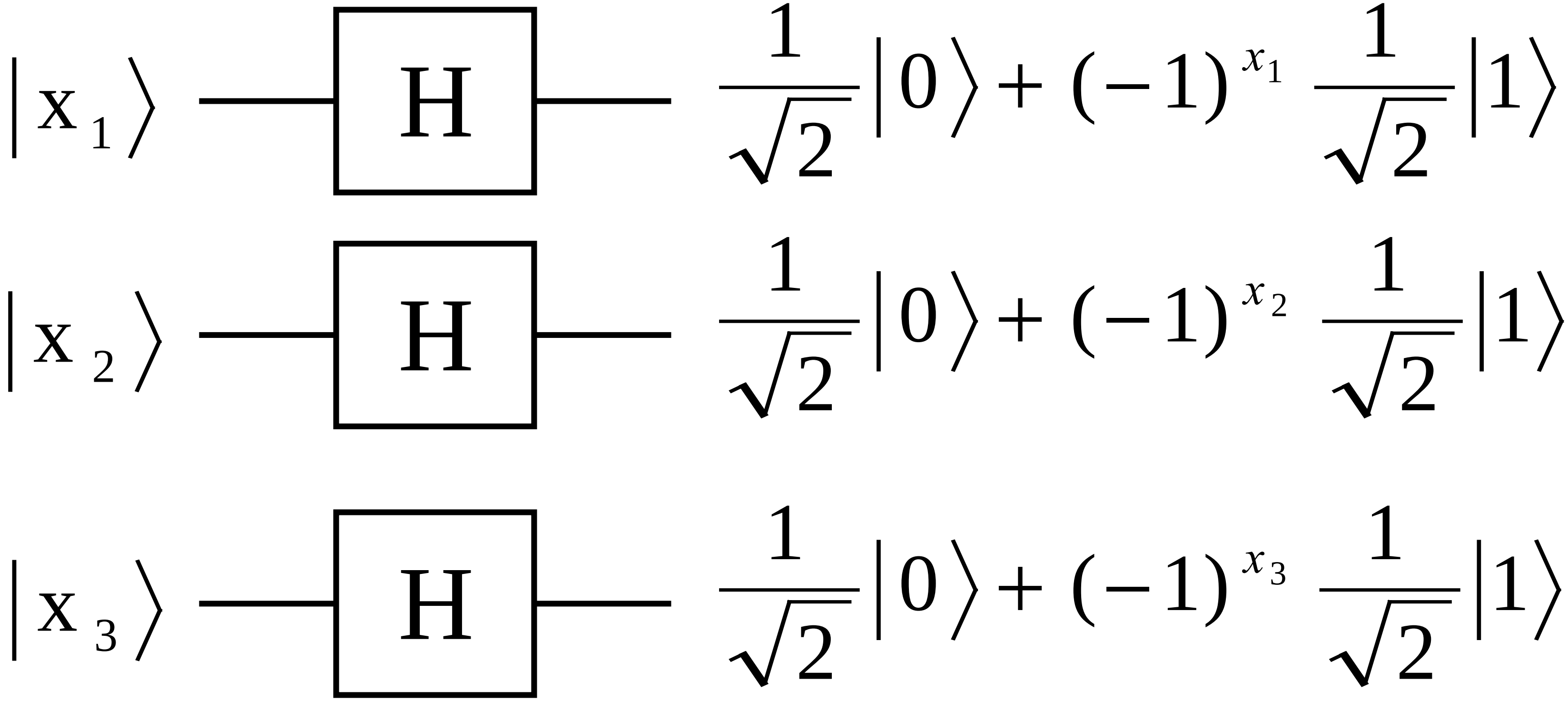
$$\left|\mathrm{b}\right\rangle \xleftrightarrow{H} \frac{1}{\sqrt{2}}\left|0\right\rangle + (-1)^{b}\,\frac{1}{\sqrt{2}}\left|1\right\rangle$$

The Hadamard transformation: circuit notation



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

The Hadamard transformation on several bits



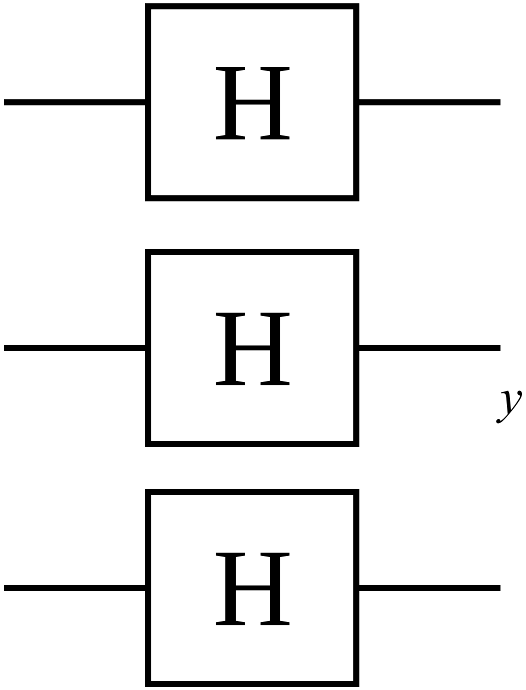
$$|x_1\rangle \quad \frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_1}\frac{1}{\sqrt{2}}|1\rangle$$

$$|x_2\rangle \quad \frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_2}\frac{1}{\sqrt{2}}|1\rangle$$

$$|x_3\rangle \quad \frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_3}\frac{1}{\sqrt{2}}|1\rangle$$

The Hadamard transformation: global view

$$\left|x_1 x_2 x_3\right\rangle$$



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

The Hadamard transformation: global view

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

The Hadamard transformation: global view

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

The Hadamard transformation on several bits

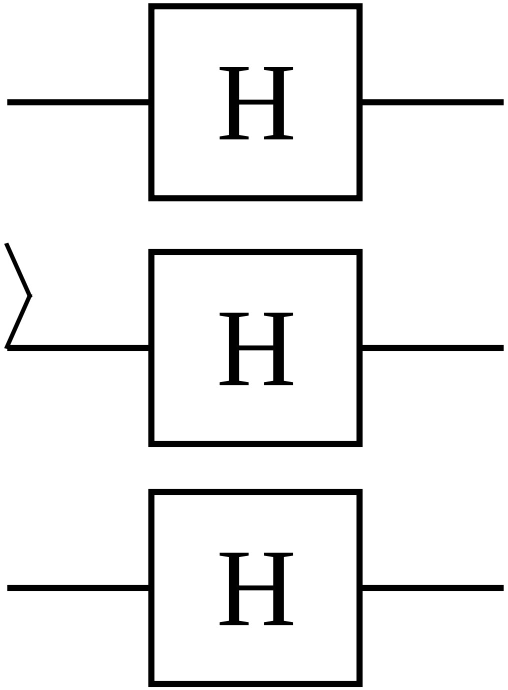
$$\frac{1}{\sqrt{2}}\left|0\right\rangle + (-1)^{x_1}\frac{1}{\sqrt{2}}\left|1\right\rangle \quad \text{---}\boxed{\mathrm{H}}\text{---} \quad \left|\mathrm{x}_1\right\rangle$$

$$\frac{1}{\sqrt{2}}\left|0\right\rangle + (-1)^{x_2}\frac{1}{\sqrt{2}}\left|1\right\rangle \quad \text{---}\boxed{\mathrm{H}}\text{---} \quad \left|\mathrm{x}_2\right\rangle$$

$$\frac{1}{\sqrt{2}}\left|0\right\rangle + (-1)^{x_3}\frac{1}{\sqrt{2}}\left|1\right\rangle \quad \text{---}\boxed{\mathrm{H}}\text{---} \quad \left|\mathrm{x}_3\right\rangle$$

The Hadamard transformation: global view

$$\sum_{y\in\{0,1\}^3}(-1)^{x\cdot y}\frac{1}{\sqrt{2}}\left|y_1 y_2 y_3\right\rangle$$



$$\left|x_1 x_2 x_3\right\rangle$$

The Hadamard transformation: global view

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

Looking at NOT and CNOT in Hadamard bases

Consider applying a NOT gate to the following states

$$|0\rangle + |1\rangle \xrightarrow{\text{NOT}} |0\rangle + |1\rangle$$

$$|0\rangle - |1\rangle \xrightarrow{\text{NOT}} -\left(|0\rangle - |1\rangle\right)$$

e.g.

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

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

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

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

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

e.g.

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

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

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

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

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

Searching example

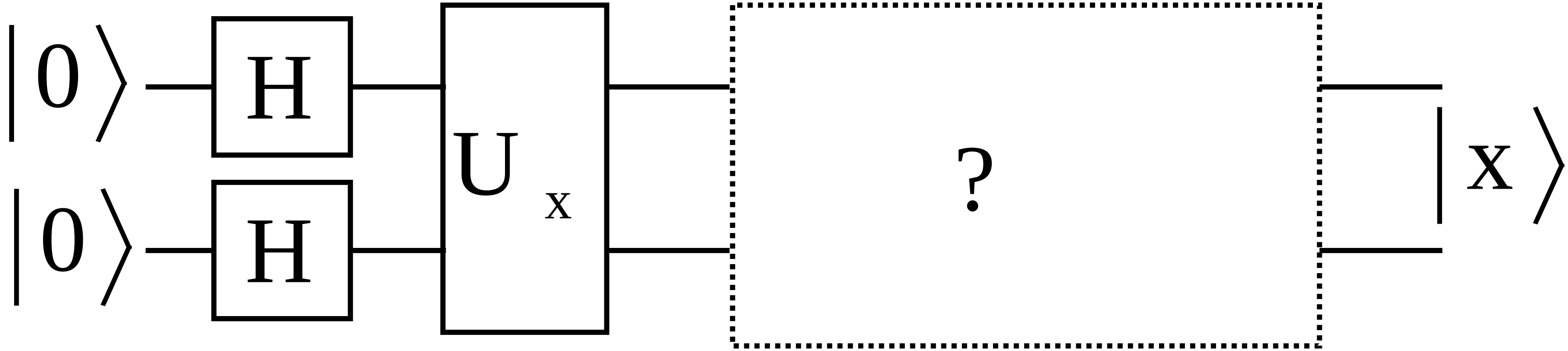
Suppose that for some $x \in \{00, 01, 10, 11\}$ we have U_x

$$U_x |x\rangle = -|x\rangle$$

$$U_x |y\rangle = |y\rangle \qquad y \neq x$$

Can we find x using U_x only once?

Guessing an algorithm



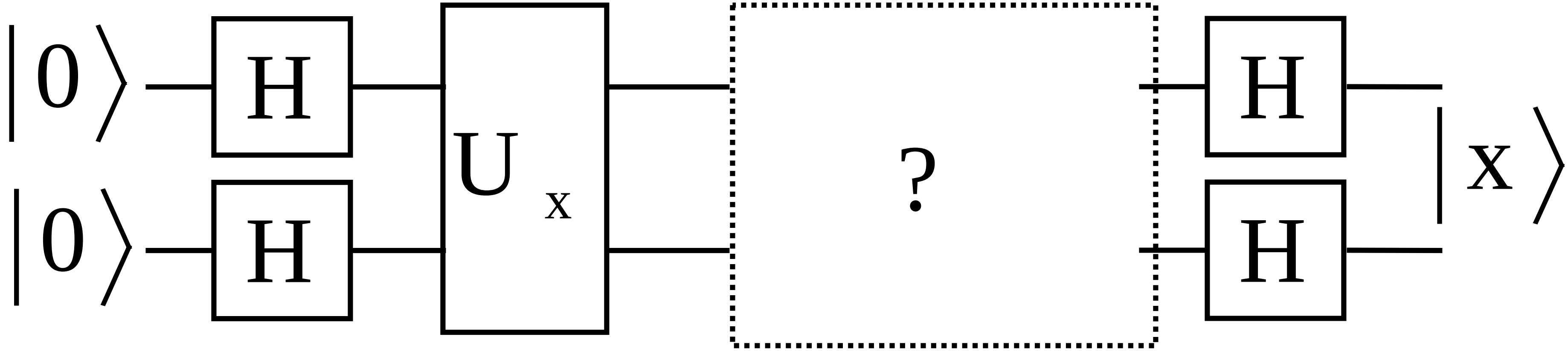
$$-|00\rangle+|01\rangle+|10\rangle+|11\rangle \xrightarrow{?} |00\rangle$$

$$|00\rangle-|01\rangle+|10\rangle+|11\rangle \xrightarrow{?} |01\rangle$$

$$|00\rangle+|01\rangle-|10\rangle+|11\rangle \xrightarrow{?} |10\rangle$$

$$|00\rangle+|01\rangle+|10\rangle-|11\rangle \xrightarrow{?} |11\rangle$$

Guessing an algorithm



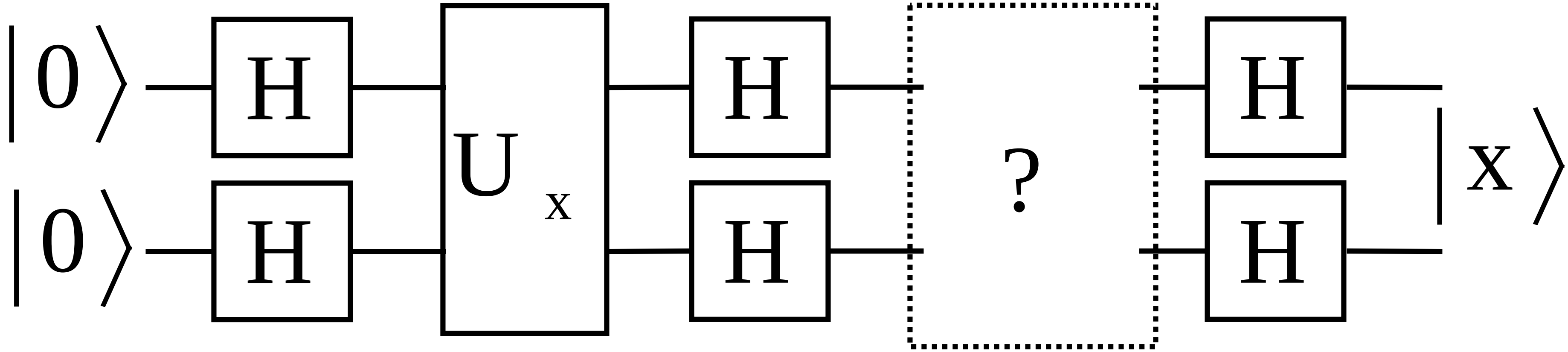
$$-|00\rangle+|01\rangle+|10\rangle+|11\rangle \xrightarrow{?} |00\rangle+|01\rangle+|10\rangle+|11\rangle$$

$$|00\rangle-|01\rangle+|10\rangle+|11\rangle \xrightarrow{?} |00\rangle-|01\rangle+|10\rangle-|11\rangle$$

$$|00\rangle+|01\rangle-|10\rangle+|11\rangle \xrightarrow{?} |00\rangle+|01\rangle-|10\rangle-|11\rangle$$

$$|00\rangle+|01\rangle+|10\rangle-|11\rangle \xrightarrow{?} |00\rangle-|01\rangle-|10\rangle+|11\rangle$$

Guessing an algorithm



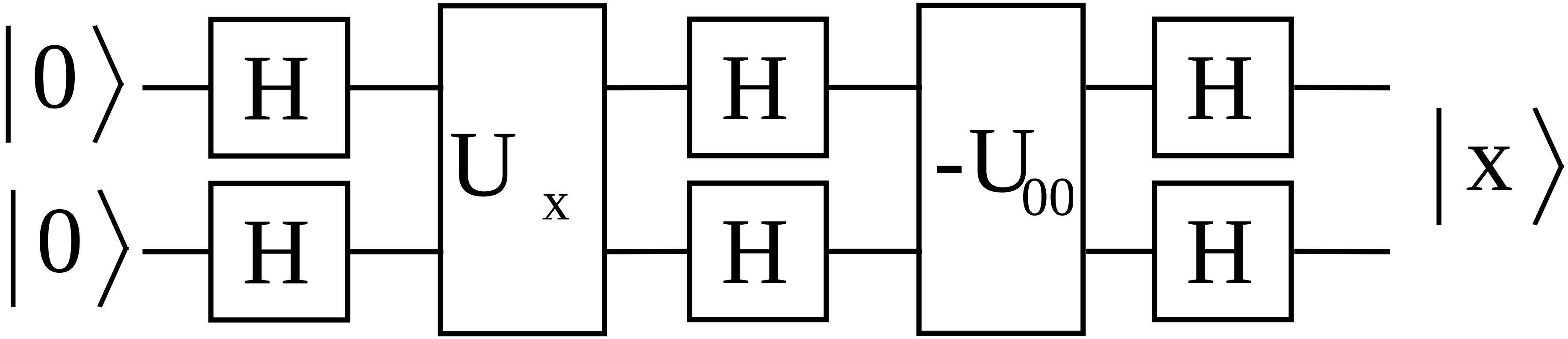
$$|00\rangle - |01\rangle - |10\rangle - |11\rangle \xrightarrow{?} |00\rangle + |01\rangle + |10\rangle + |11\rangle$$

$$|00\rangle + |01\rangle - |10\rangle + |11\rangle \xrightarrow{?} |00\rangle - |01\rangle + |10\rangle - |11\rangle$$

$$|00\rangle - |01\rangle + |10\rangle + |11\rangle \xrightarrow{?} |00\rangle + |01\rangle - |10\rangle - |11\rangle$$

$$|00\rangle + |01\rangle + |10\rangle - |11\rangle \xrightarrow{?} |00\rangle - |01\rangle - |10\rangle + |11\rangle$$

Guessing an algorithm



Computing functions into the phase

Suppose we know how to compute a function

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

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

$$|x\rangle\big(|0\rangle - |1\rangle\big) \alpha \; (-1)^{f(x)}|x\rangle\big(|0\rangle - |1\rangle\big)$$

Generalization: Eigenvalue “kick-back”

Suppose we know how to compute an operator

$$U\left|\psi\right\rangle = e^{i\varphi}\left|\psi\right\rangle$$

Then the “controlled-U” gives us

$$c-U\left|0\right\rangle\left|\psi\right\rangle = \left|0\right\rangle\left|\psi\right\rangle$$

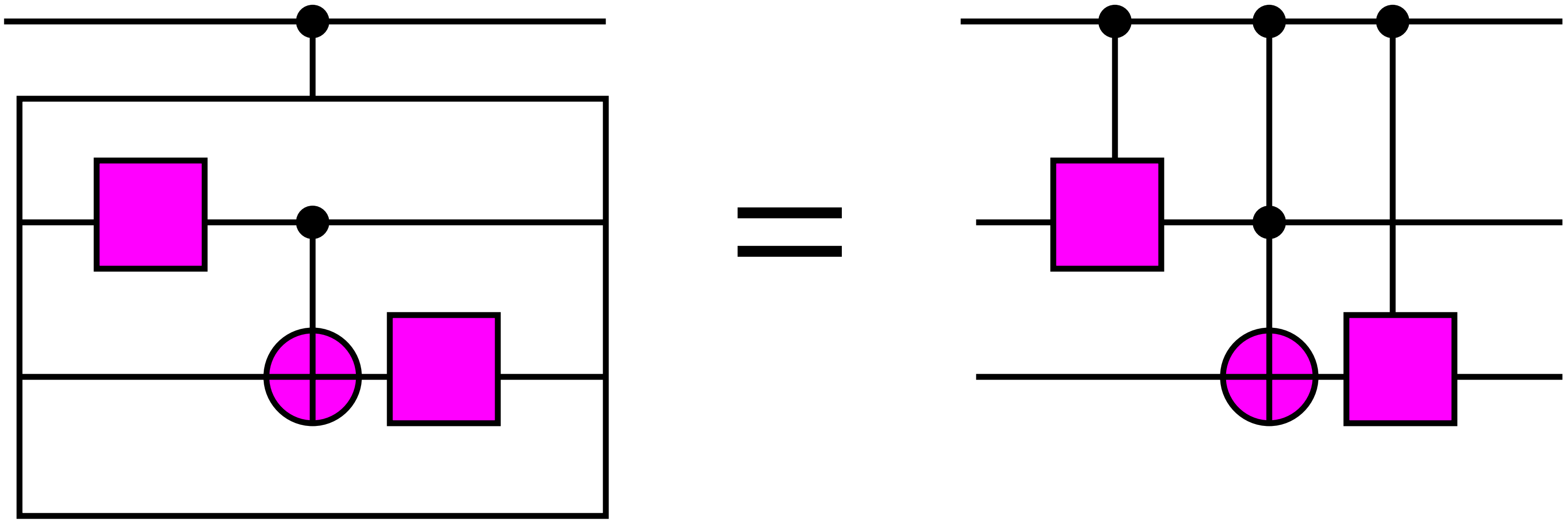
$$c-U\left|1\right\rangle\left|\psi\right\rangle = e^{i\varphi}\left|1\right\rangle\left|\psi\right\rangle$$

$$c-U\left(\left|0\right\rangle + \left|1\right\rangle\right)\left|\psi\right\rangle = \left(\left|0\right\rangle + e^{i\varphi}\left|1\right\rangle\right)\left|\psi\right\rangle$$

How do we implement c-U?

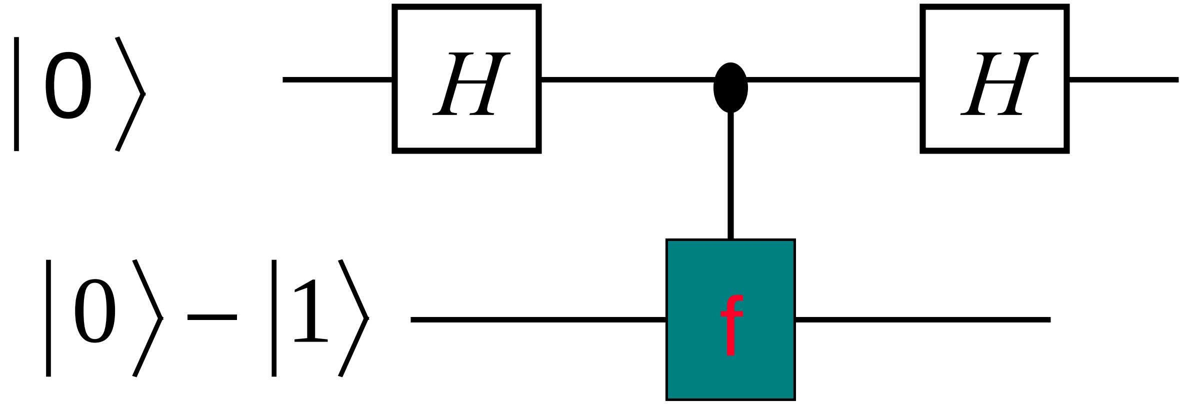
Replace every gate G in the circuit for with a c-G.

For example,

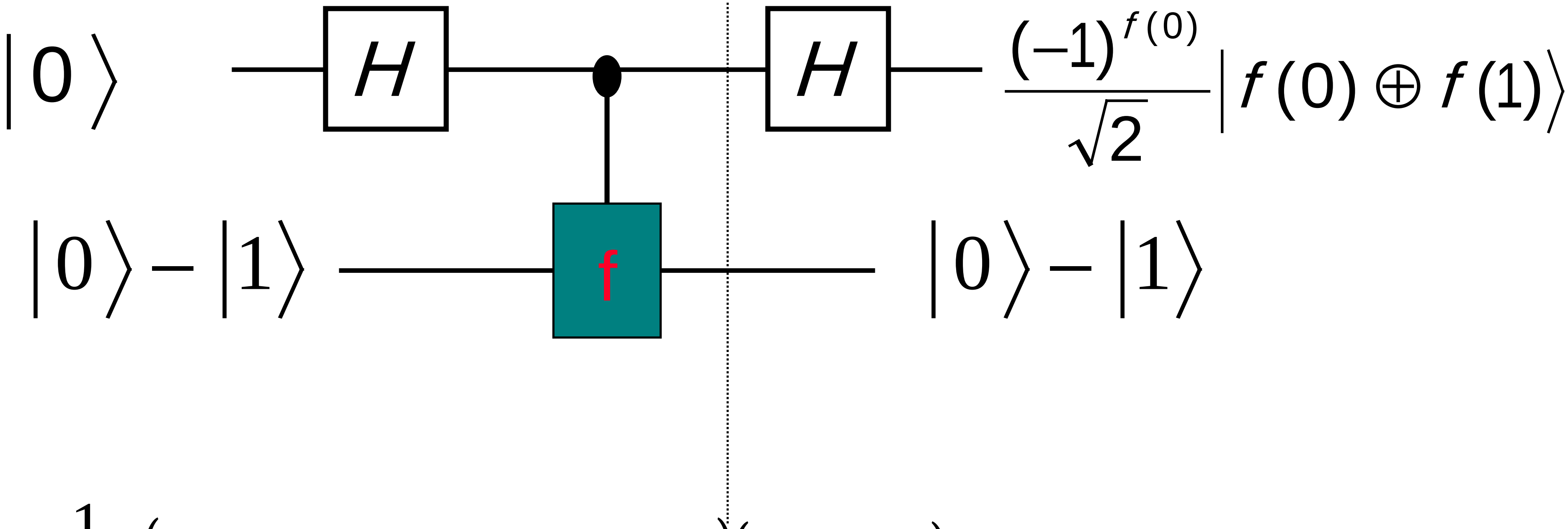


Deutsch's problem

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



Deutsch algorithm



$|0\rangle$

$|0\rangle - |1\rangle$

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

$|0\rangle - |1\rangle$

$$\frac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)\Big(|0\rangle - |1\rangle\Big)$$

$$= \frac{(-1)^{f(0)}}{\sqrt{2}}\Big(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\Big)\Big(|0\rangle - |1\rangle\Big)$$

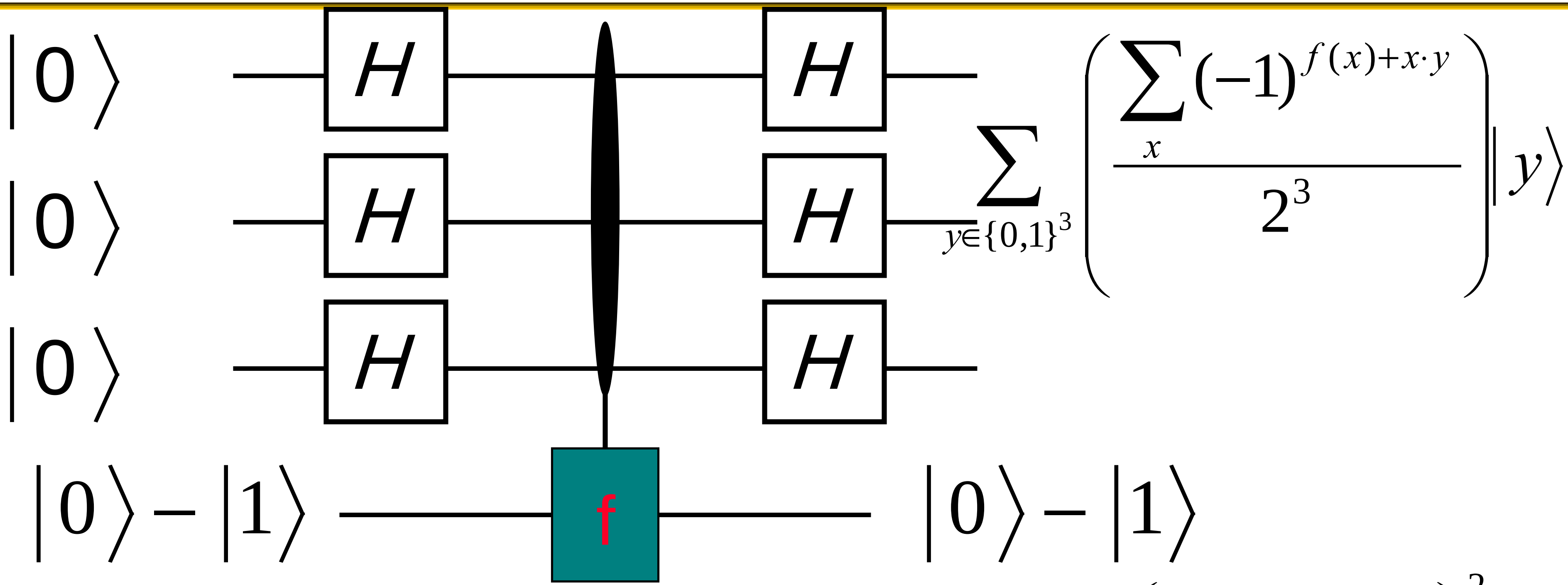
Deutsch-Jozsa problem

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

Decide if f is constant or balanced.

Equivalently, determine $$\left(\frac{\sum_x (-1)^{f(x)}}{2^n} \right)^2$$

Deutsch-Jozsa problem



$$\sum_{y\in\{0,1\}^3}\left(\frac{\sum_x (-1)^{f(x)+x\cdot y}}{2^3}\right)|y\rangle$$

Probability of measuring $|000\rangle$ is $\left(\frac{\sum_x (-1)^{f(x)}}{2^3}\right)^2$

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

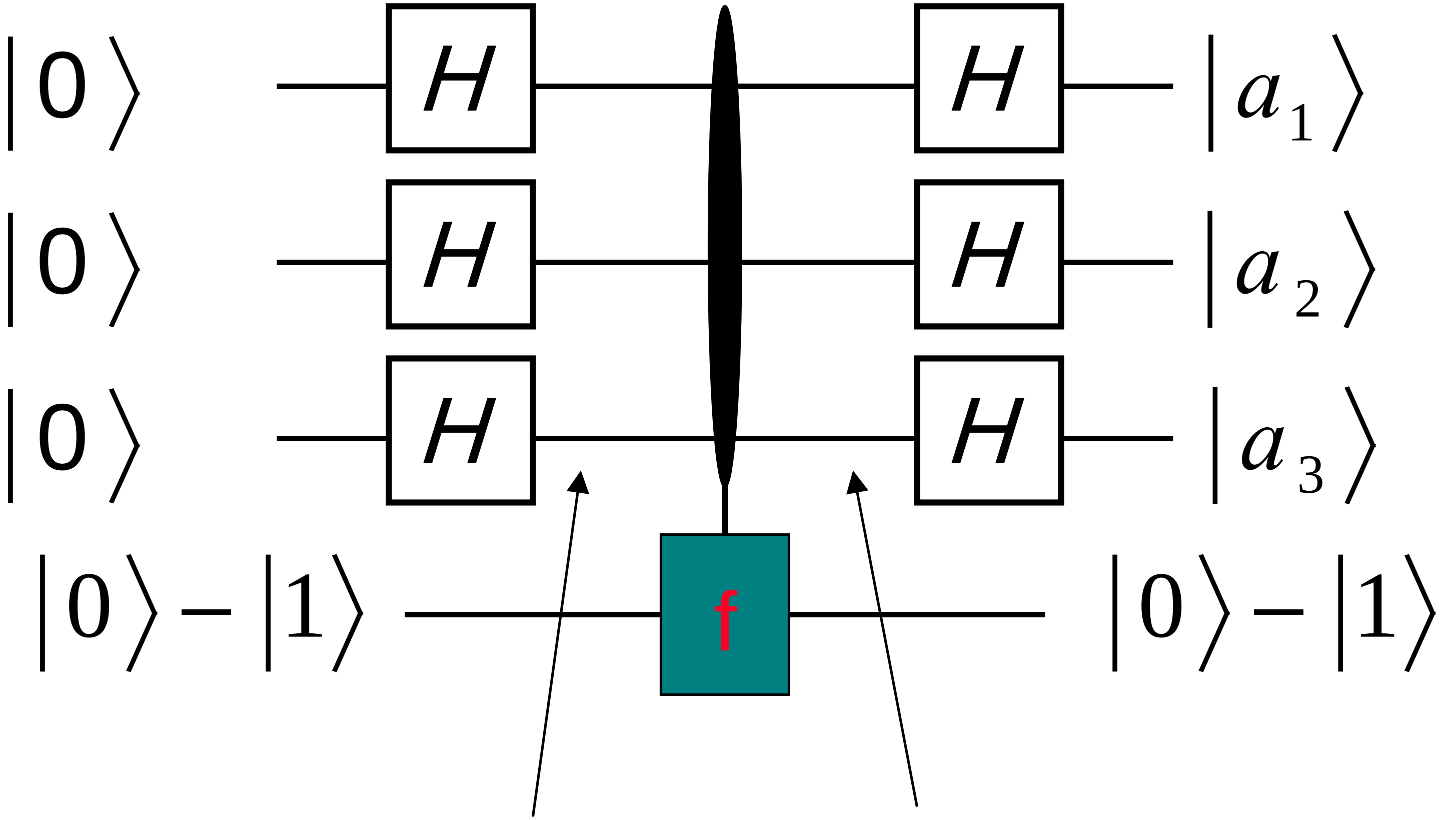
Bernstein-Vazirani problem

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

Given $|x\rangle|c\rangle \overset{U_f}{\alpha} |x\rangle|c \oplus f(x)\rangle$
determine

$$a = a_1 a_2 \mathrm{K}\ a_n$$

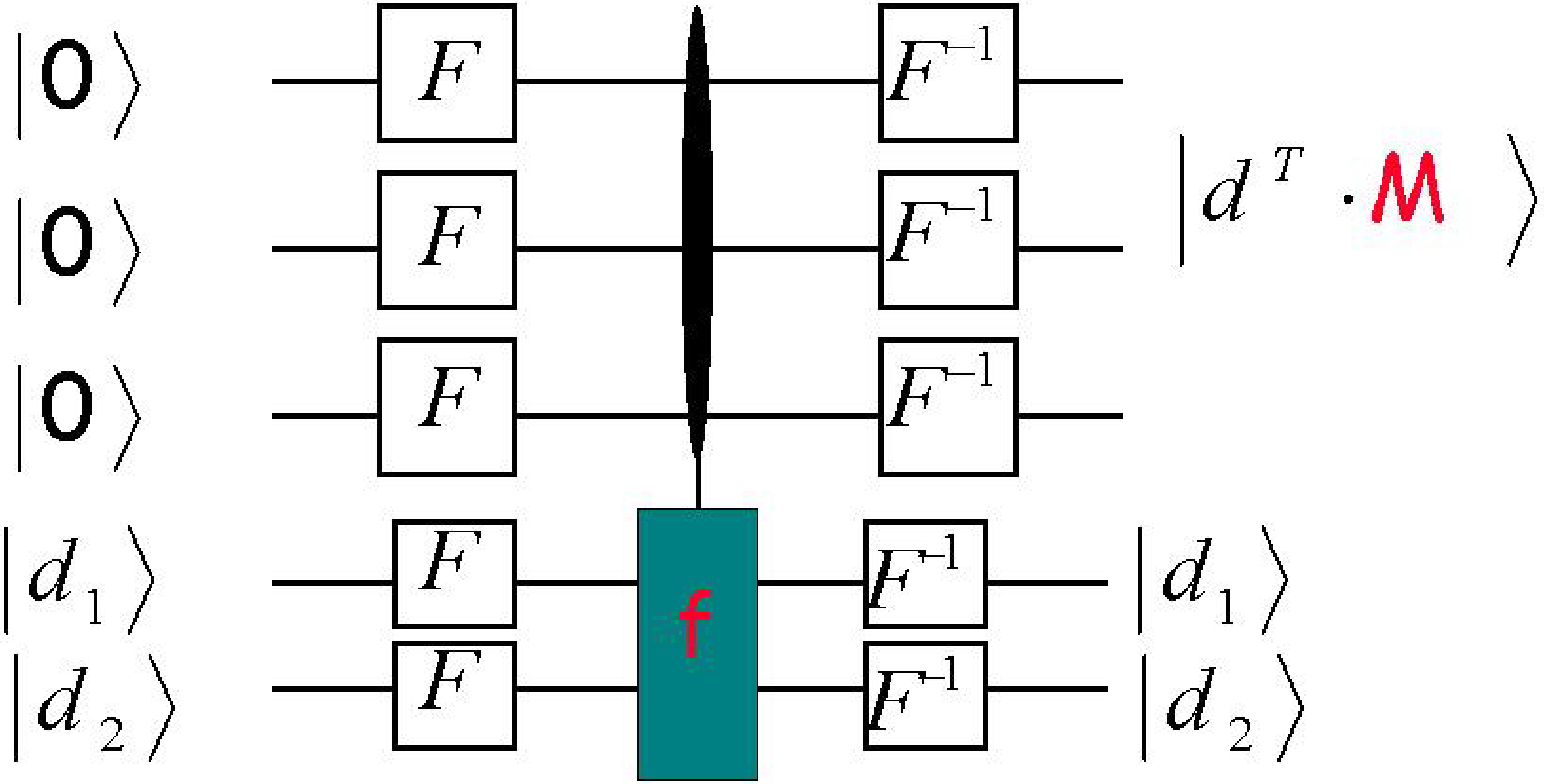
Bernstein-Vazirani problem



$$\sum_{x\in\{0,1\}^3} \frac{1}{\sqrt{2^3}}|x\rangle \qquad \sum_{x\in\{0,1\}^3} \frac{(-1)^{a\cdot x}}{\sqrt{2^3}}|x\rangle$$

Generally

$f: Z_p^n \to Z_p^m \quad \times \; \alpha \quad M \times$



Another property of Hadamard transformation

Consider $S \leq Z_2^{\ n}$

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

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

Then

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

Simon's problem

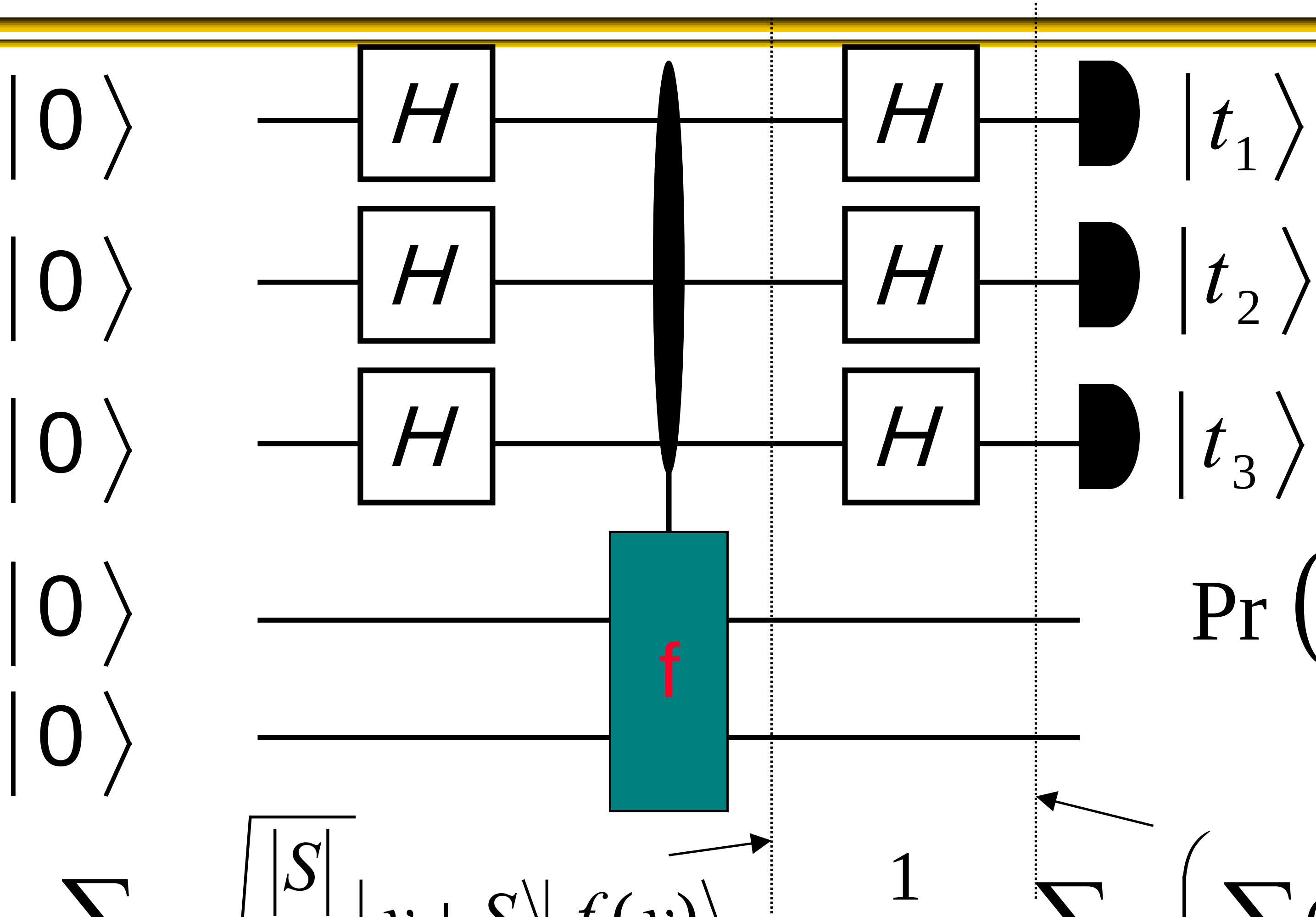
Suppose $f:\{0,1\}^n \to X$ has the property that

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

For some "hidden subgroup" $S \le Z_2^n$

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

Simon’s algorithm



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

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

$$\sum_{y+S\in {Z_2}^3/S} \sqrt{\frac{|S|}{|2^n|}}\,|y+S\rangle|f(y)\rangle$$

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

Abelian Hidden subgroup problem

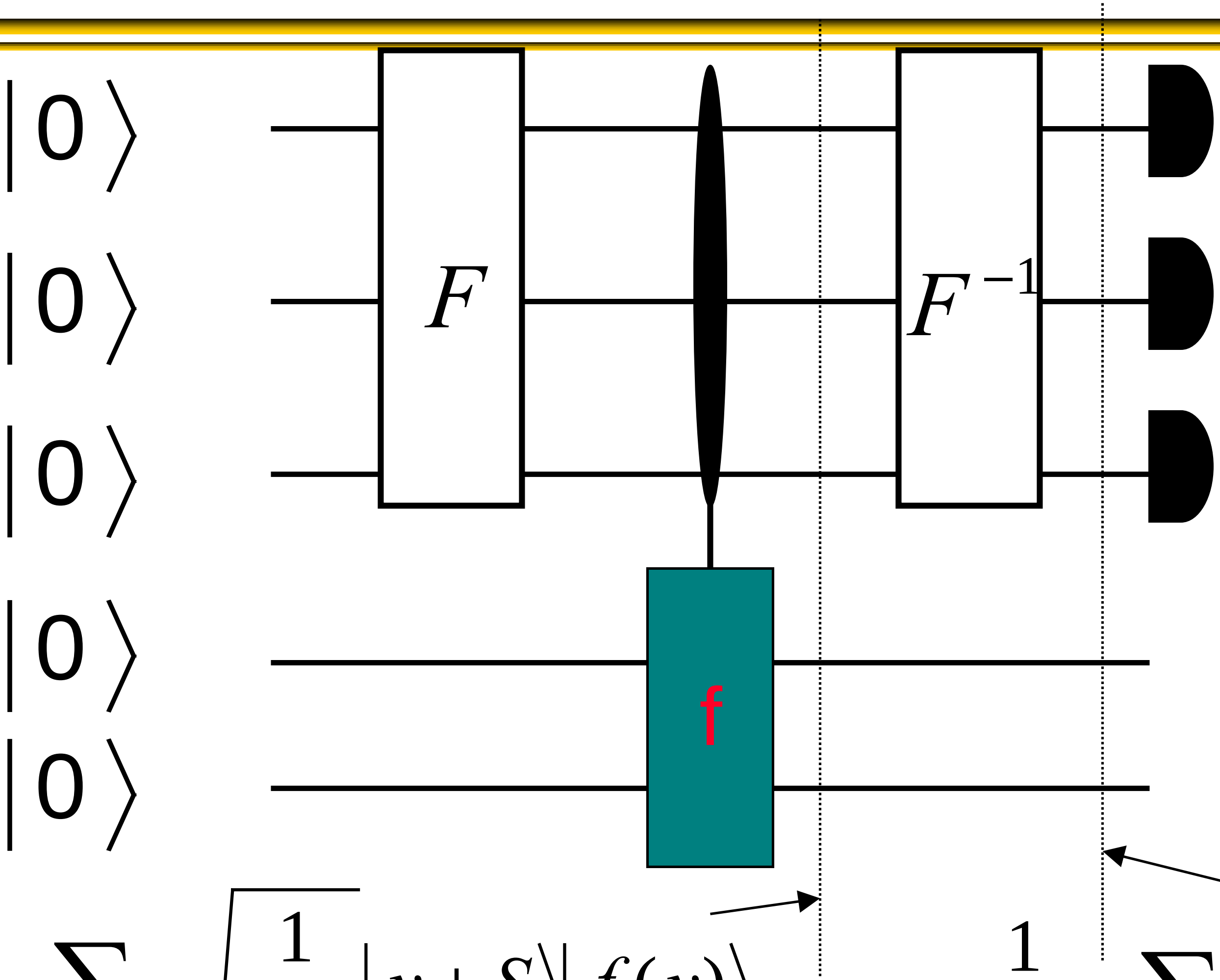
Suppose $f : G \to X$ has the property that

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

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

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

Hidden subgroup problem



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

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

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

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