THE UNIVERSITY *of* EDINBURGH
informatics

Lecture 8: Bernstein-Vazirani Algorithm

Raul Garcia-Patron Sanchez

THE UNIVERSITY of EDINBURGH
informatics

Phase kickback subroutine

Raul Garcia-Patron Sanchez

From classical to quantum oracles

Every classical oracle has a quantum analogue

Construction via reversible classical oracle

Classical oracle

$x \rightarrow \boxed{O_f} \rightarrow f(x)$

Reversible oracle

Address bits

Target bit

$x \rightarrow \boxed{O_f} \rightarrow x$

$y \rightarrow \boxed{O_f} \rightarrow y \oplus f(x)$

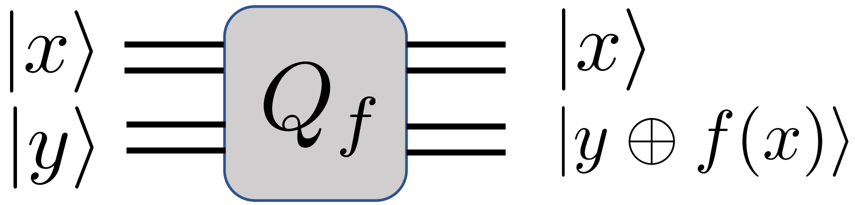
Quantum oracle

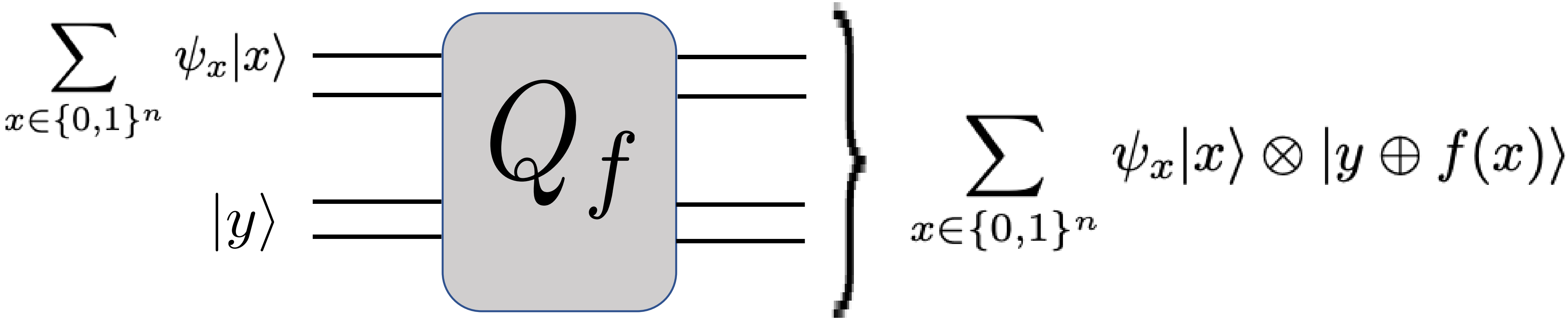
$|x\rangle \rightarrow \boxed{Q_f} \rightarrow |x\rangle$

$|y\rangle \rightarrow \boxed{Q_f} \rightarrow |y \oplus f(x)\rangle$

Allow superposition of inputs

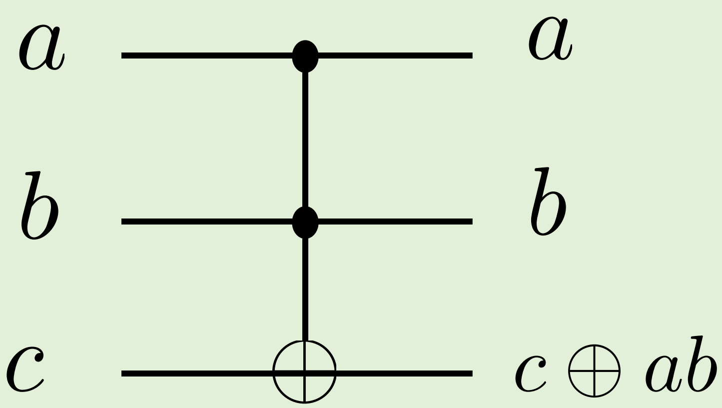
Quantum oracle



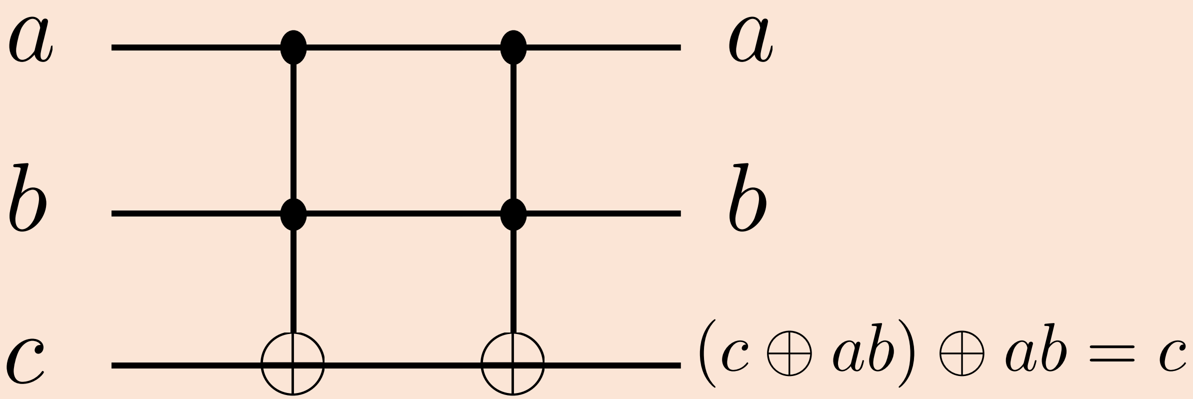


Reversible classical circuits: Toffoli gates

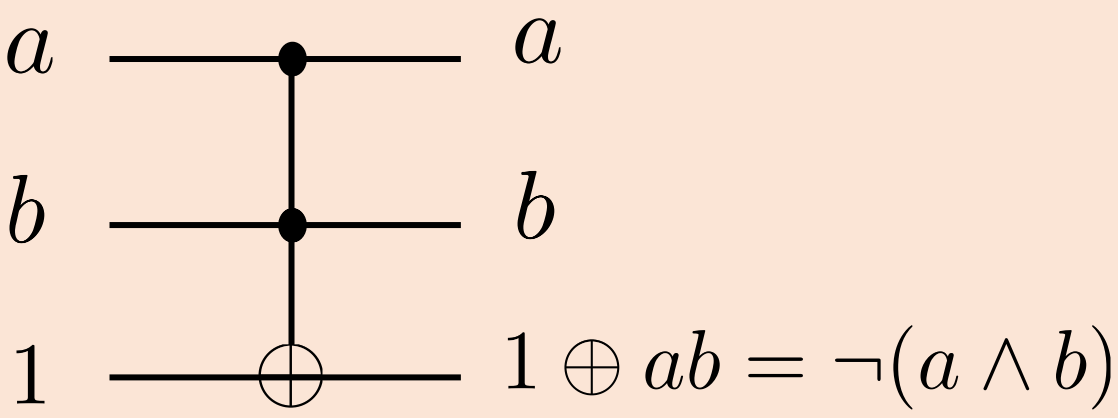
Toffoli gate



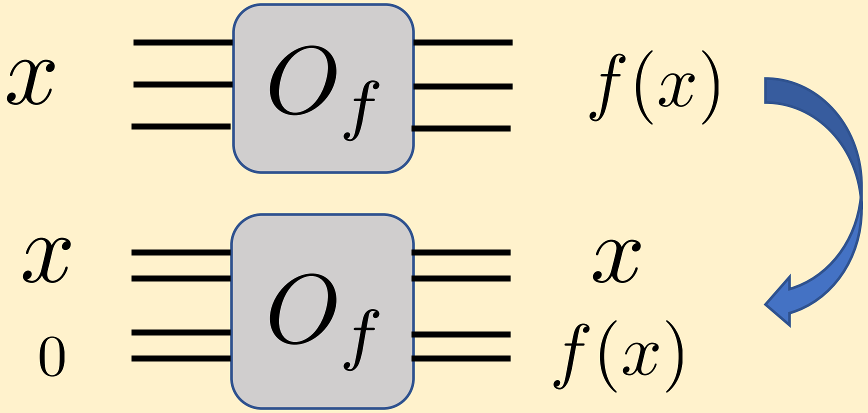
Reversible as self-inverse



Simulates NAND

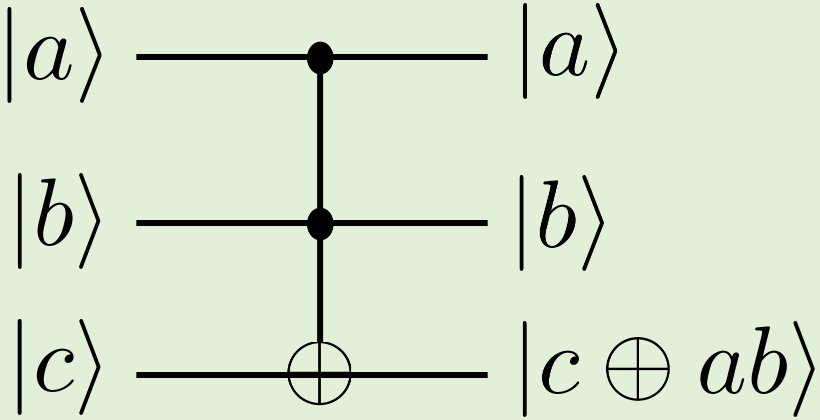


Replace every NAND by a TOFFOLI

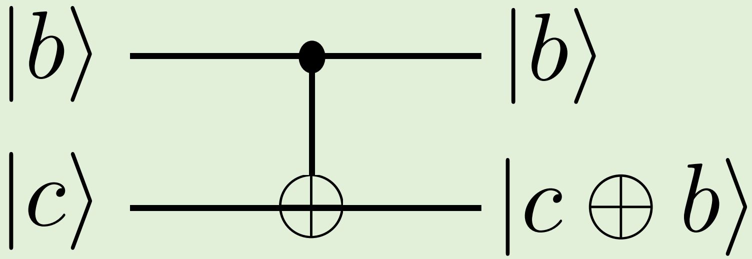


From classical reversible to quantum circuit

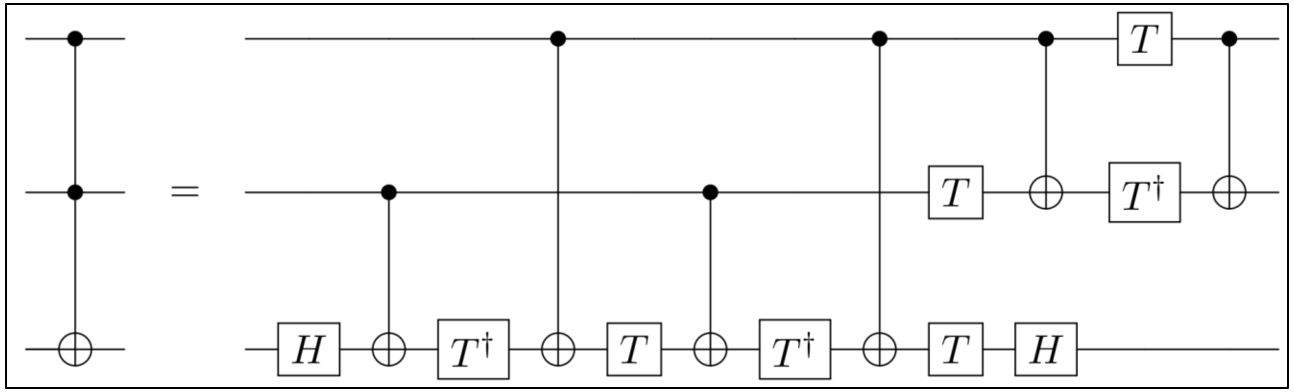
Toffoli gate



CNOT gate



- Now allow for superpositions!
- Toffoli gate $\equiv$ Control-control-NOT
- A 2-qubit gate circuit

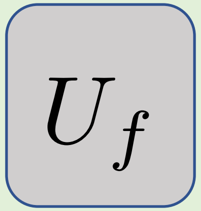


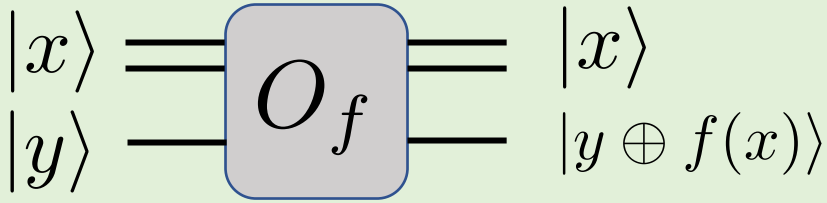
Phase Kickback

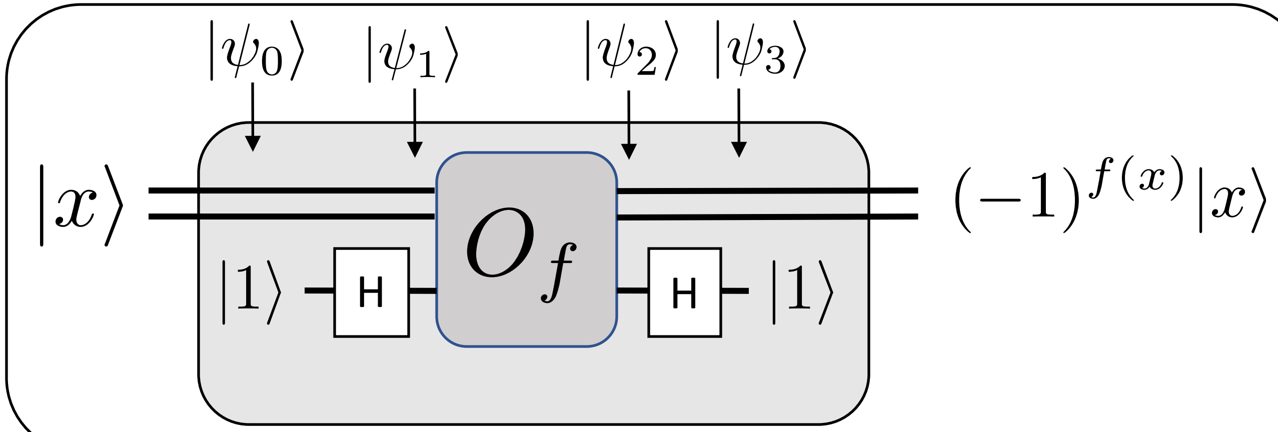
$f : \{0,1\}^n \to \{0,1\}$

Phase Kickback

$$U_f : |x\rangle \to (-1)^{f(x)}|x\rangle$$





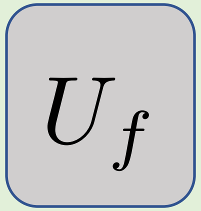


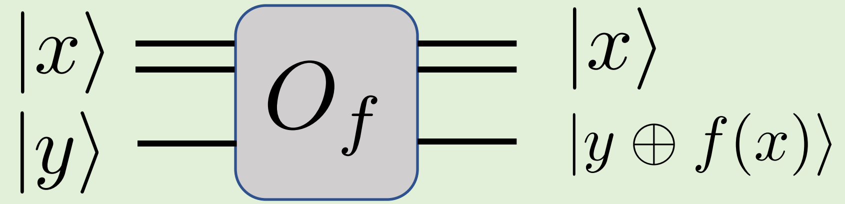
Phase Kickback

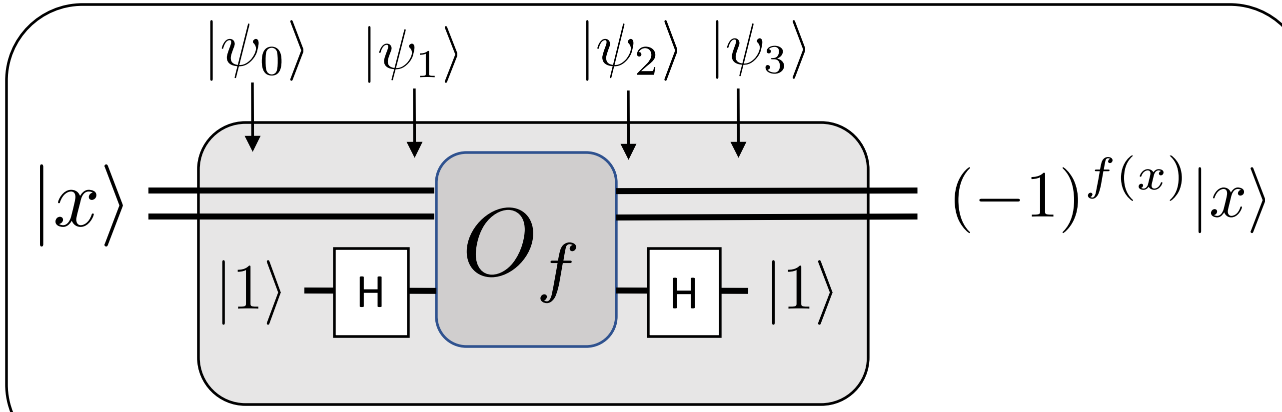
$f : \{0,1\}^n \to \{0,1\}$

Phase Kickback

$$U_f : |x\rangle \to (-1)^{f(x)}|x\rangle$$







$$|\psi_0\rangle = |x\rangle \otimes |1\rangle$$

$$|\psi_1\rangle = |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\psi_2\rangle = |x\rangle \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |f(x) \oplus 1\rangle)$$

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

$$|\psi_3\rangle = (-1)^{f(x)}|x\rangle \otimes |1\rangle$$

$$|f(x)\rangle - |f(x) \oplus 1\rangle$$

$$f(x) = 0 : |0\rangle - |1\rangle$$

$$f(x) = 1 : -1(|0\rangle - |1\rangle)$$

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

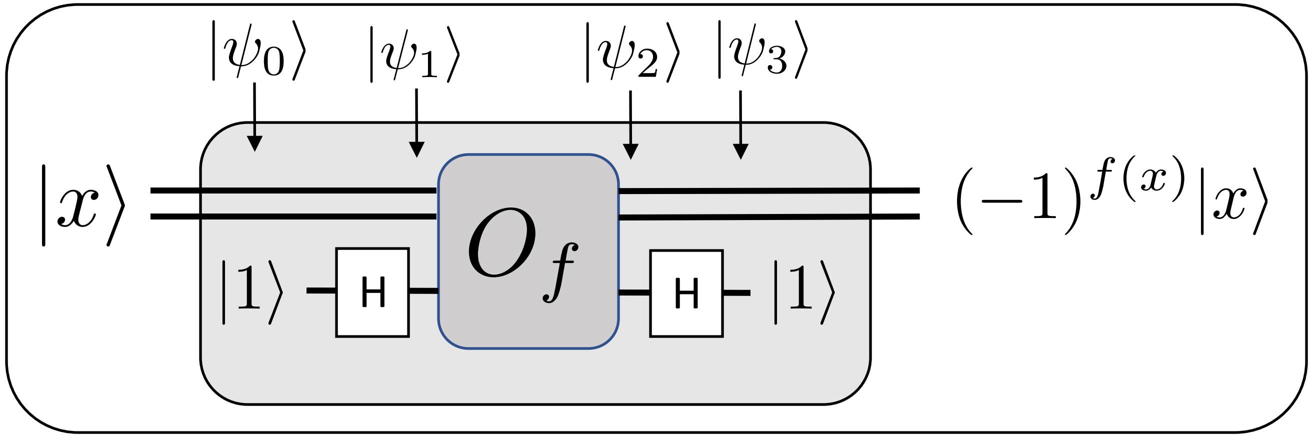
We can forget the ancillary qubit output

Phase Kickback

$$U_f : |x\rangle \to (-1)^{f(x)}|x\rangle$$

U_f

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



$|\psi_0\rangle$

$$|\phi\rangle \otimes |1\rangle = \left(\sum_{x\in\{0,1\}^n} \phi_x |x\rangle\right) \otimes |1\rangle = \sum_{x\in\{0,1\}^n} \phi_x |x\rangle \otimes |1\rangle$$

$|\psi_1\rangle$

$$\xrightarrow{I_{2^n}\otimes H} \sum_{x\in\{0,1\}^n} \phi_x |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

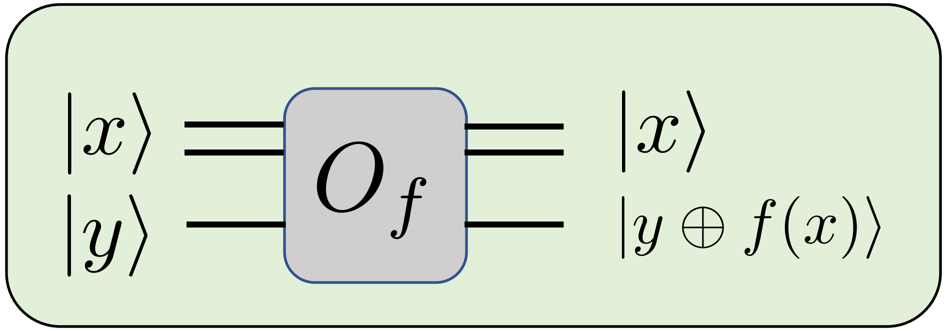
$|\psi_2\rangle$

$$\xrightarrow{O_f} \sum_{x\in\{0,1\}^n} \psi_x (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

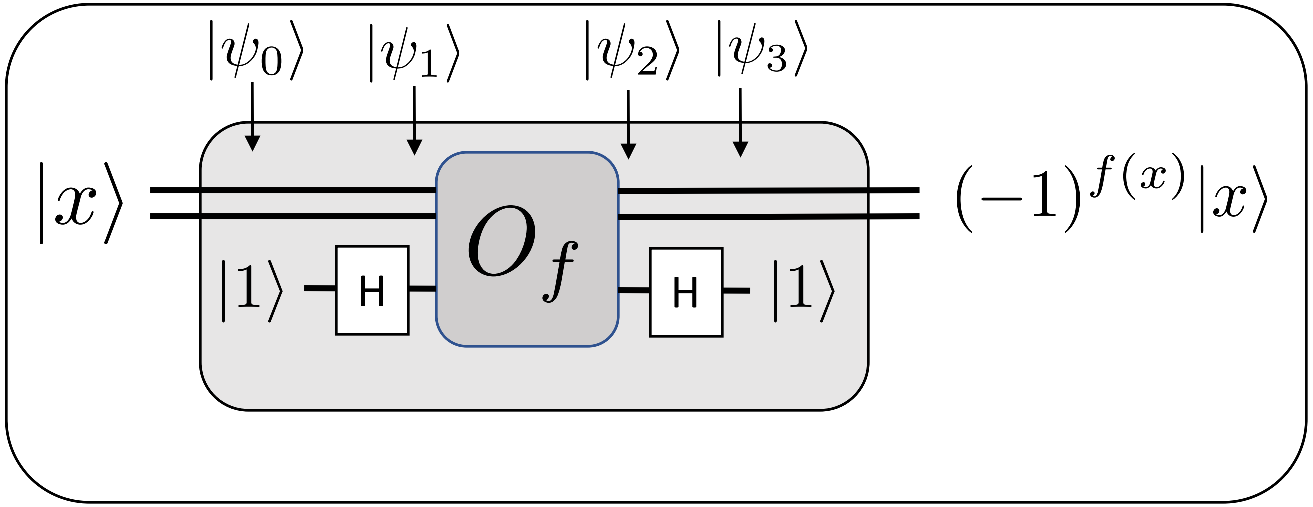
$|\psi_3\rangle$

$$\xrightarrow{I_{2^n}\otimes H} \sum_{x\in\{0,1\}^n} \psi_x (-1)^{f(x)} |x\rangle \otimes |1\rangle = \left(\sum_{x\in\{0,1\}^n} \psi_x (-1)^{f(x)} |x\rangle\right) \otimes |1\rangle$$

Phase Kickback $f : \{0,1\}^n \to \{0,1\}$



N+1 qubits



N+1 qubits

N qubits

Phase Kickback

$$U_f : |x\rangle \to (-1)^{f(x)}|x\rangle$$

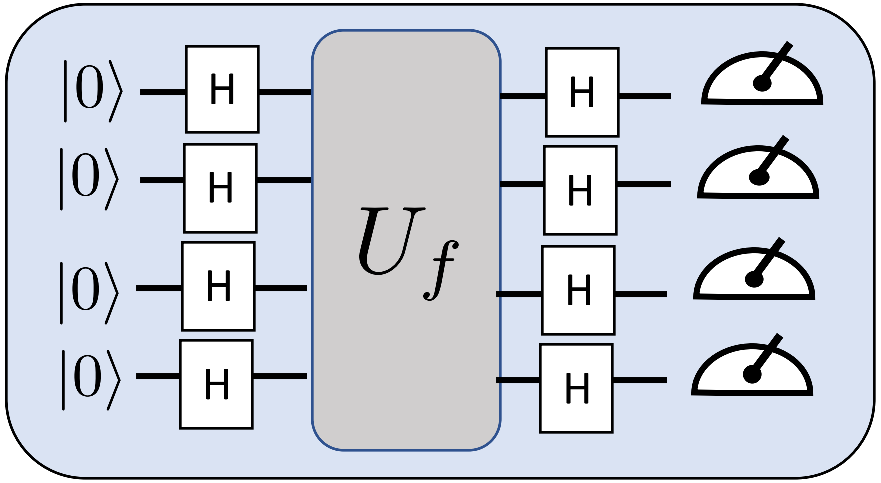
U_f

Balanced or equal function Game

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

Constant: $f(x) = c \ \forall x$

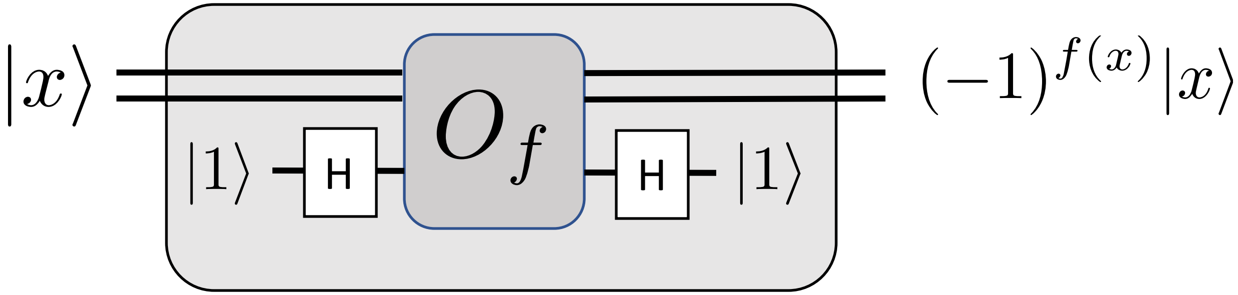
Balanced: $f(x) = 1$ on half of the bits



Phase Kickback

$$U_f : |x\rangle \to (-1)^{f(x)}|x\rangle$$

U_f



Constant: $P(0^n) = 1$

Balanced: $P(0^n) = 0$

THE UNIVERSITY *of* EDINBURGH
informatics

Bernstein-Vazirani Algorithm

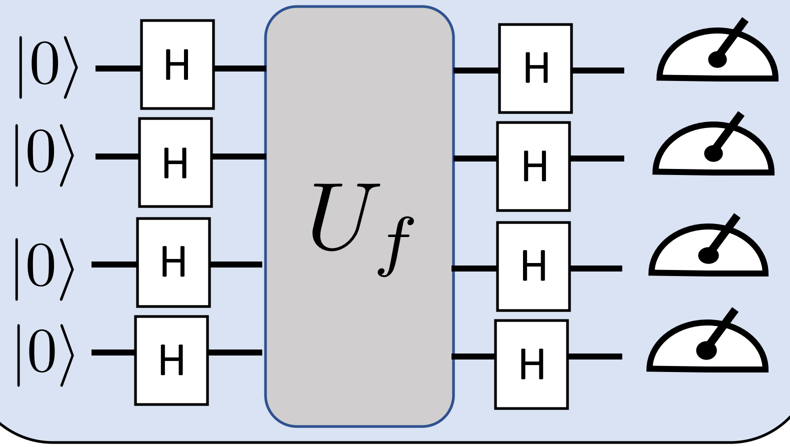
Raul Garcia-Patron Sanchez

Detecting linear functions

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

$$\text{Promise: } f(x) = a \cdot x = \sum_i a_i x_i \bmod 2$$

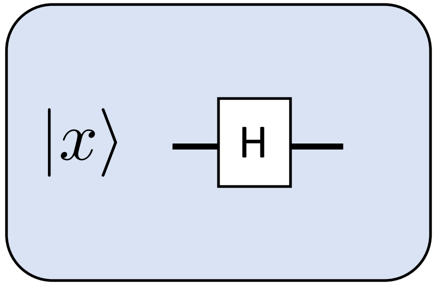
$$\text{Problem: Find } a$$



The same circuit as for Deutsch-Jozsa allow to guess "a" with a single query to the quantum oracle where classically we need at least n queries.

1 single query!

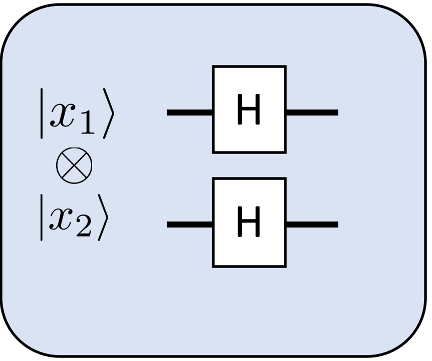
Walsh–Hadamard transform



$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

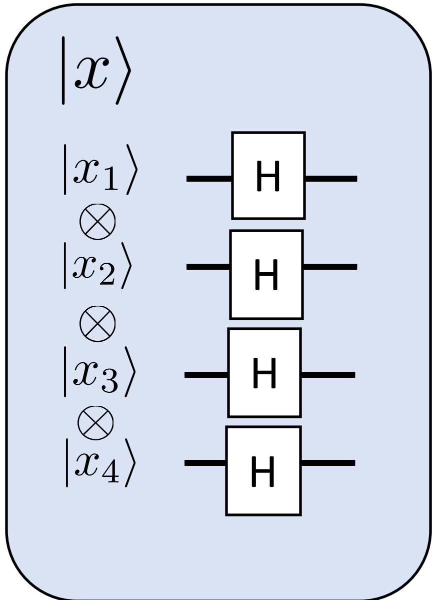
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\boxed{H|x_1\rangle = \frac{1}{\sqrt{2}}[|0\rangle + (-1)^{x_1}|1\rangle] = \frac{1}{\sqrt{2}}\sum_{y_1\in\{0,1\}}(-1)^{x_1 y_1}|y_1\rangle}$$



$$(H\otimes H)|x_1\rangle\otimes|x_2\rangle = \frac{1}{2}\Big(\sum_{y_1\in\{0,1\}}(-1)^{x_1 y_1}|y_1\rangle\Big)\otimes\Big(\sum_{y_2\in\{0,1\}}(-1)^{x_2 y_2}|y_2\rangle\Big)$$

$$(H\otimes H)|x_1\rangle\otimes|x_2\rangle = \frac{1}{2}\sum_{y_1,y_2\in\{0,1\}}(-1)^{x_1 y_1 + x_2 y_2}|y_1\rangle\otimes|y_2\rangle$$



$$|x\rangle = |x_1, x_2, \dots, x_n\rangle = |x_1\rangle\otimes|x_2\rangle\otimes\dots\otimes|x_n\rangle$$

$$\boxed{\text{where } x\cdot y = \sum_{i=0}^{n} x_i y_i}$$

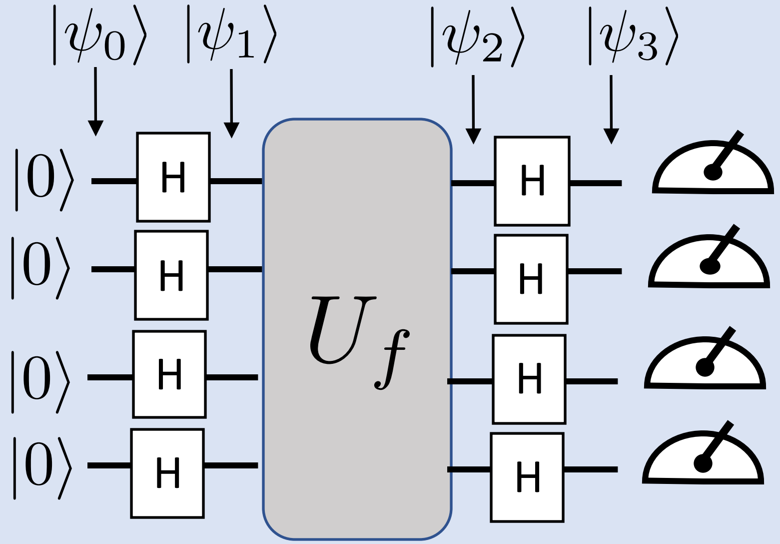
$$|x\rangle \xrightarrow{H^{\otimes n}} \bigotimes_i^n H|x_i\rangle = \frac{1}{\sqrt{2^n}}\bigotimes_i^n\left[\sum_{y_i\in\{0,1\}}(-1)^{x_i y_i}|y_i\rangle\right] = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle$$

Balanced case

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

Promise: $f(x) = a\cdot x = \sum_i a_i x_i \bmod 2$

Problem: Find a



$$|0\rangle^{\otimes n} \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

$$\xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle$$

$$\xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \left(\frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle \right)$$

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

Walsh-Hadamard transform

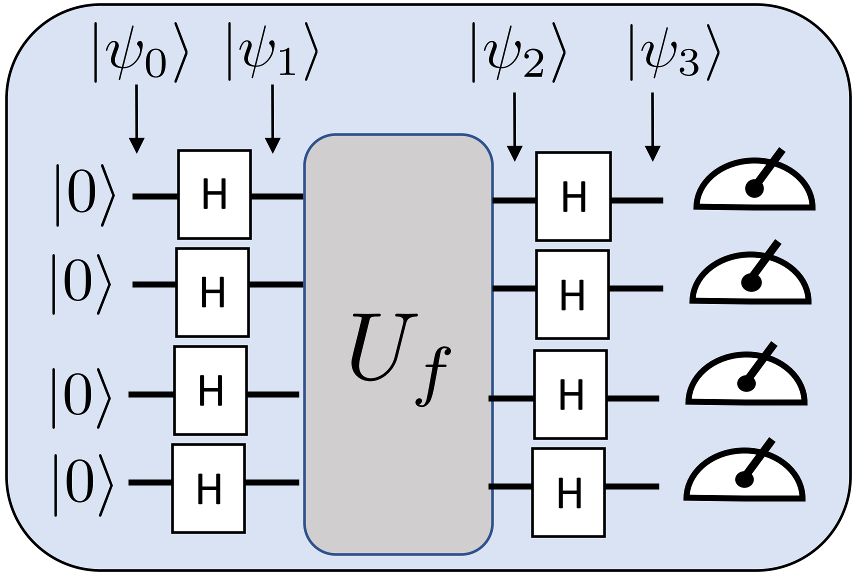
$$|x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}|y\rangle$$

Outcome zero decides

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

Promise: $f(x) = a \cdot x = \sum_i a_i x_i \bmod 2$

Problem: Find a



$$|0\rangle^{\otimes n} \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

$|\psi_1\rangle$

$$\xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$$

$|\psi_2\rangle$

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

$|\psi_3\rangle$

$$P(y) = |\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{(a \oplus y) \cdot x}|^2$$

Phase Kickback

$$U_f : |x\rangle \to (-1)^{f(x)} |x\rangle$$

Walsh-Hadamard transform

$$|x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

Measurement postulate

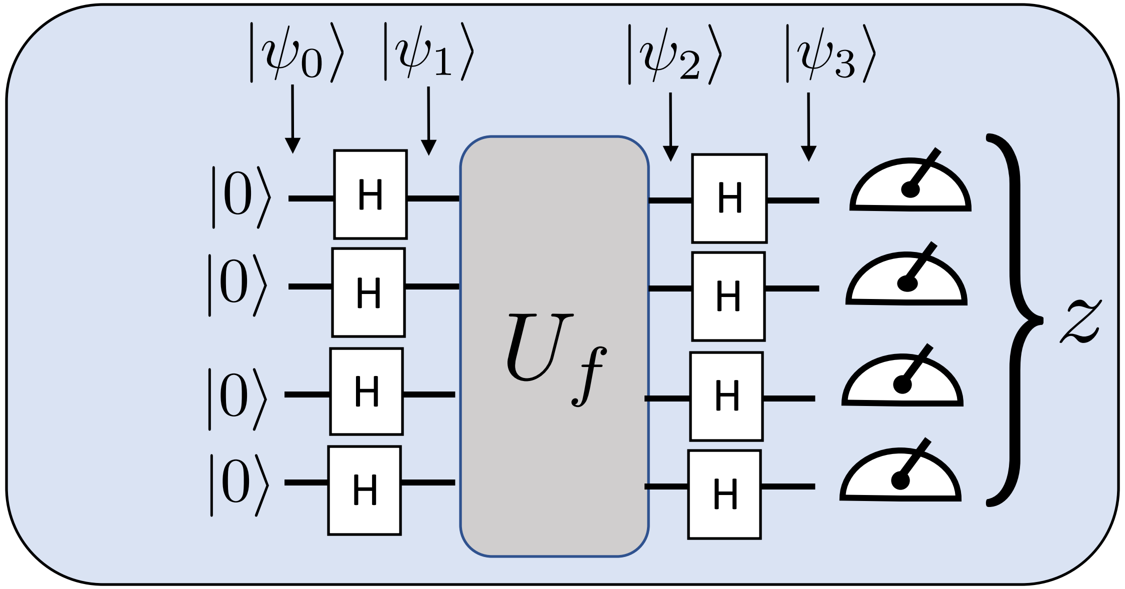
$$P(y) = |\langle y | \psi_3 \rangle|^2$$

Bernstein-Vazirani Algorithm[BV93]

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

Promise: $f(x) = a \cdot x = \sum_i a_i x_i \bmod 2$

Problem: Find a



$$P(y) = |\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{(a \oplus y) \cdot x}|^2$$

- If $y = a$ we have $(-1)^{(a \oplus y) \cdot x} = 1$ ➡ $P(a) = 1$
- As $\sum_i P(i) = 1$ we have that $\forall y \neq a : P(y) = 0$

Classical strategies

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

Promise: $f(x) = a \cdot x = \sum_i a_i x_i \bmod 2$

Problem: Find a

$\swarrow$ O_f $\nearrow$

- Each query reveals at most 1 bit of information about a

  a contains n bits, therefore we need $\Omega(n)$ queries to learn it

- Linear separation between the quantum and classical complexities.

- Recursive version of problem needs $\text{poly}(n)$ quantum queries.

  Classical randomized algorithms need $n^{\Omega(\log n)}$ queries.

Phase Kickback is a fundamental subroutine

General Phase Kickback

$$U_f : |x\rangle \rightarrow e^{i\theta_x}|x\rangle \quad \boxed{U_f}$$

Phase: $e^{i\phi}$ - Complex number of norm 1(scalar)

If $\phi = z\pi$ where $z = \{0,1\}$ we have $e^{i\phi} = (-1)^z$

This lecture $\theta_x = f(x)\pi$

$$U_f : |x\rangle \rightarrow (-1)^{f(x)}|x\rangle \quad \boxed{U_f}$$

References

Reading references

1. Bernstein-Vazirani NC 1.4.3 RdW 2.4.2 and G 7.5

NC ≣ Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information
Cambridge University Press (2010)
RdW ≣ Quantum Computing Lecture Notes, Ronald de Wolf, https://arxiv.org/abs/1907.09415
G ≣ Introduction to Quantum Computation, Sevag Gharibian, Lectures notes