



THE UNIVERSITY of EDINBURGH
informatics

Lecture 8: Bernstein-Vazirani Algorithm

Raul Garcia-Patron Sanchez





THE UNIVERSITY of EDINBURGH
informatics

Recap Deutsch-Jozsa

Raul Garcia-Patron Sanchez



Deutsch-Jozsa Algorithm

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

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

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

x	000	001	010	011	100	101	110	111
f(x)	0	0	0	0	0	0	0	0

x	000	001	010	011	100	101	110	111
f(x)	1	0	0	0	1	0	1	1

- How many queries to the function we need to answer with full certainty?
- Classical oracle $2^n/2$ queries.

• Quantum:

1 single query!



O_f

- Classical probabilistic strategy: Constant queries.

Balanced or equal function Game

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

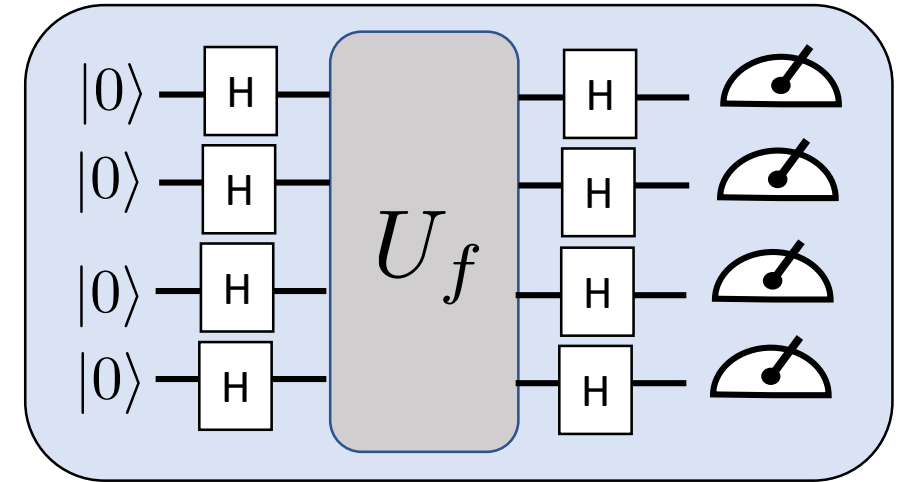
Constant: $f(x) = c \forall x$

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

Phase Kickback

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

U_f



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

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

Outcome zero decides

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

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

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

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

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

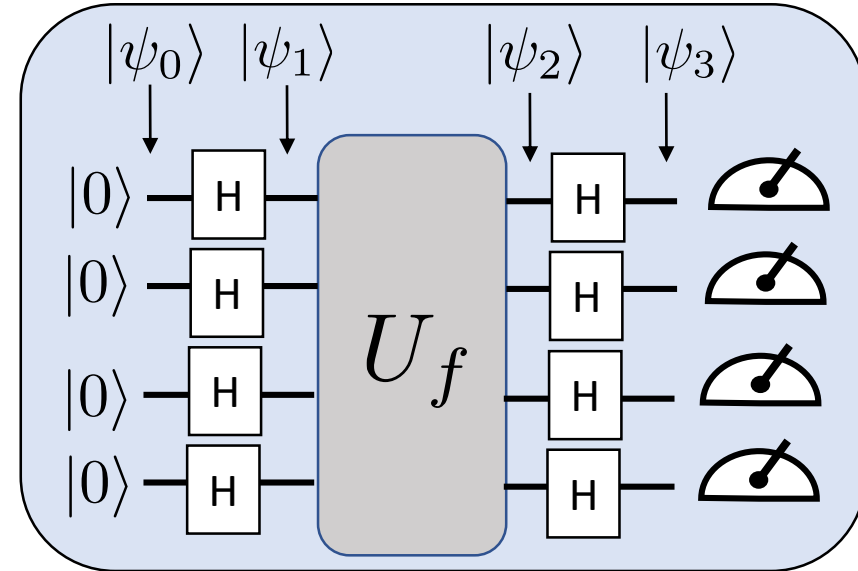
$$= \sum_{y \in \{0,1\}^n} \left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)+x \cdot y} \right) |y\rangle$$

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

$$|\psi_1\rangle$$

$$|\psi_2\rangle$$

$$|\psi_3\rangle$$



Phase Kickback

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

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

$$P(0) = |\langle 0^n | \psi_3 \rangle|^2$$



THE UNIVERSITY of EDINBURGH
informatics

Phase kickback subroutine

Raul Garcia-Patron Sanchez



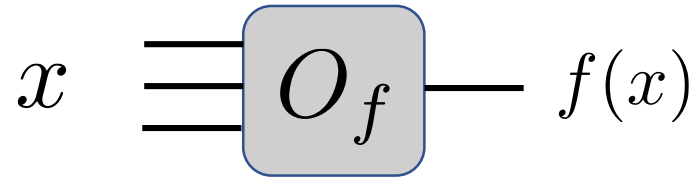
From classical to quantum oracles

Every classical oracle has a quantum analogue

Construction via reversible classical oracle



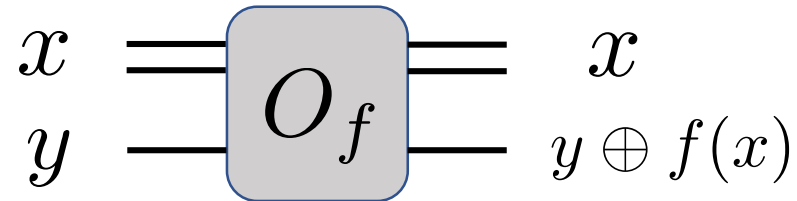
Classical oracle



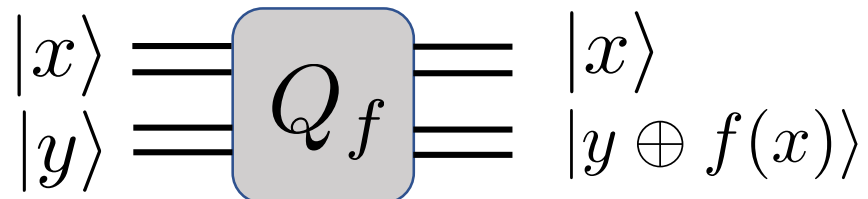
Reversible oracle

Address bits

Target bit

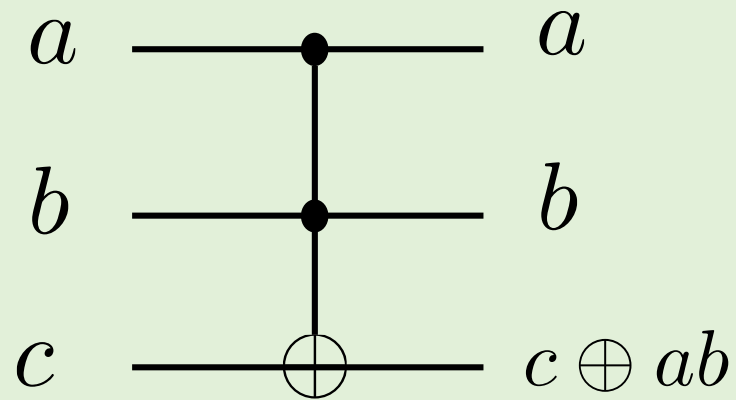


Quantum oracle

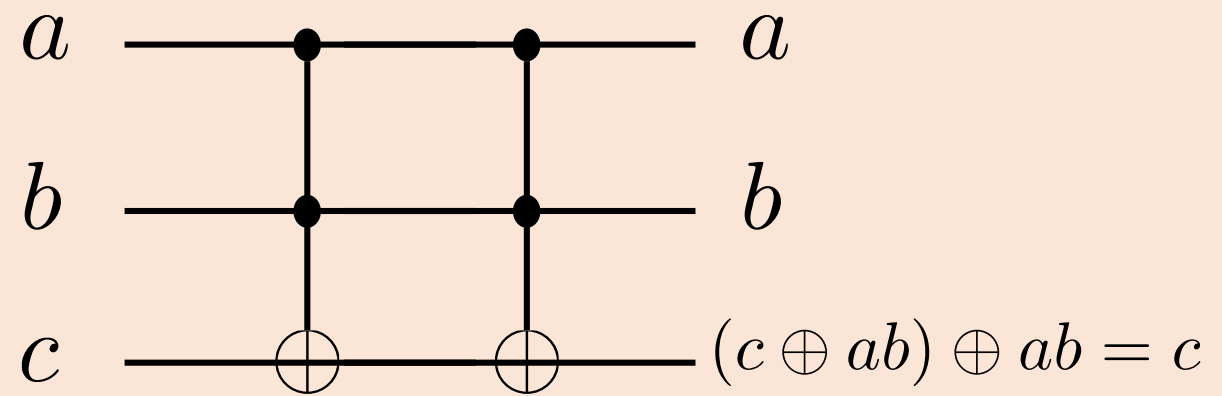


Reversible classical circuits: Toffoli gates

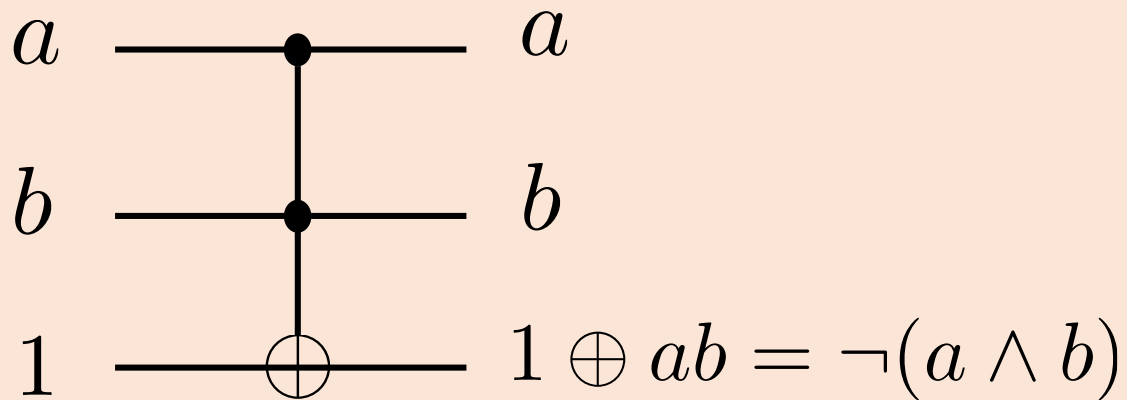
Toffoli gate



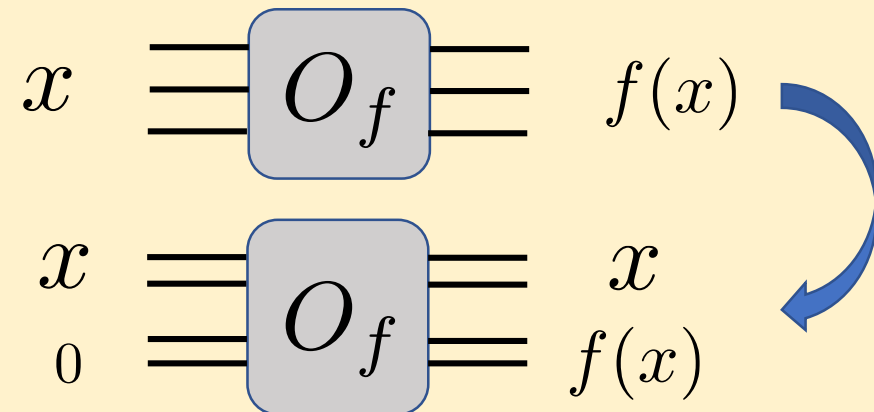
Reversible as self-inverse



Simulates NAND

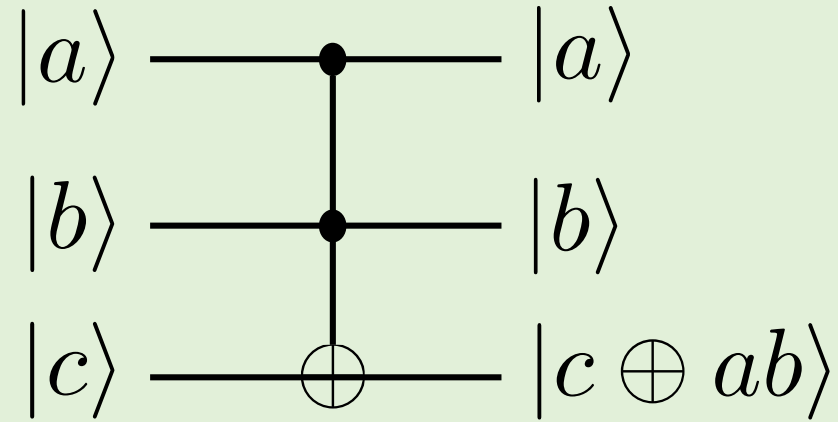


Replace every NAND by a TOFFOLI

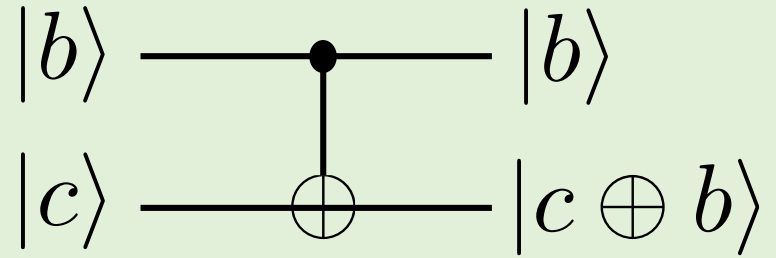


From classical reversible to quantum circuit

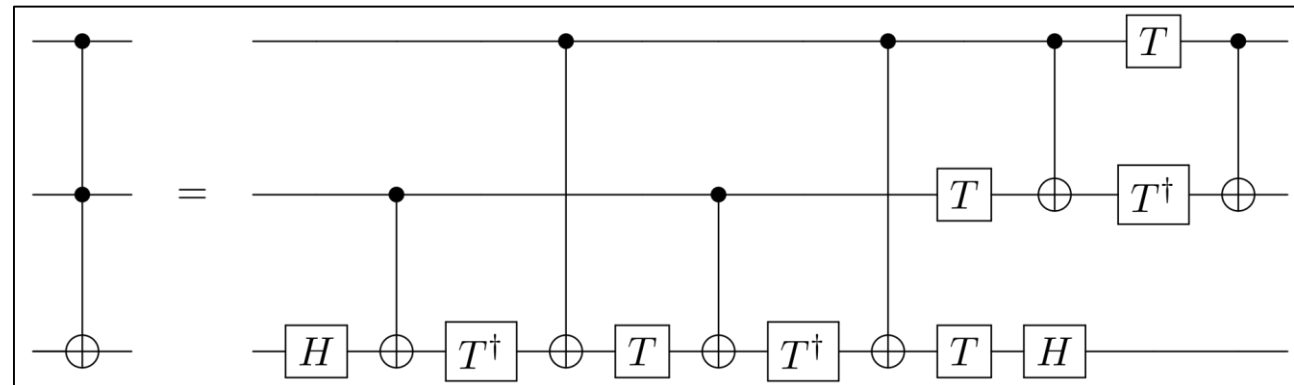
Toffoli gate



CNOT gate



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



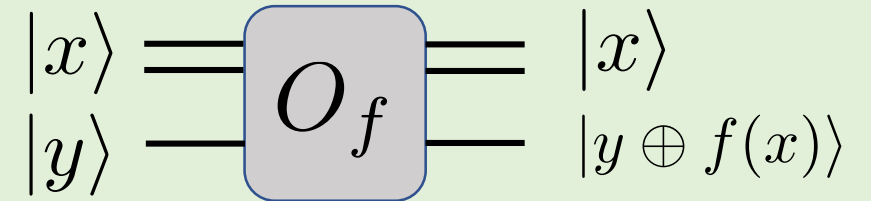
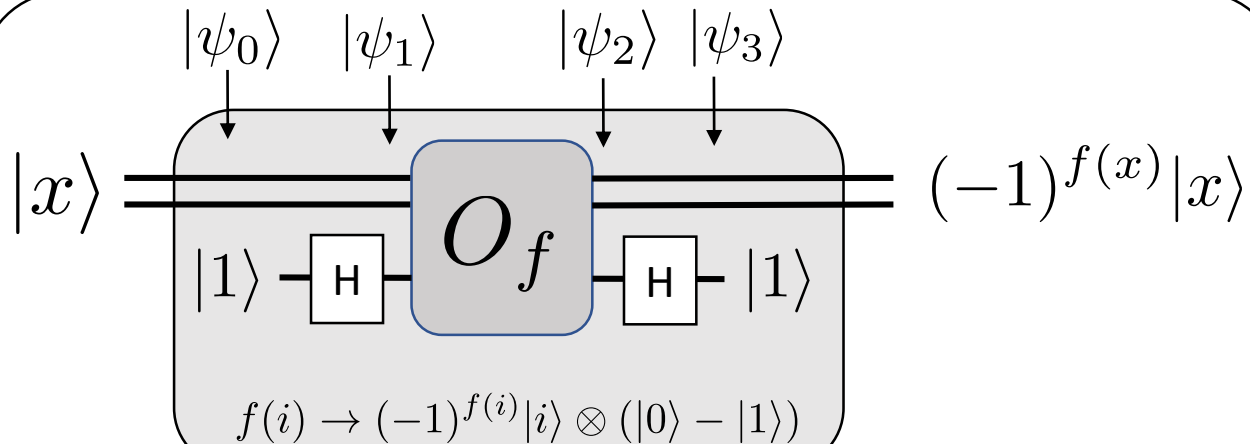
Phase Kickback

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

Phase Kickback

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

U_f

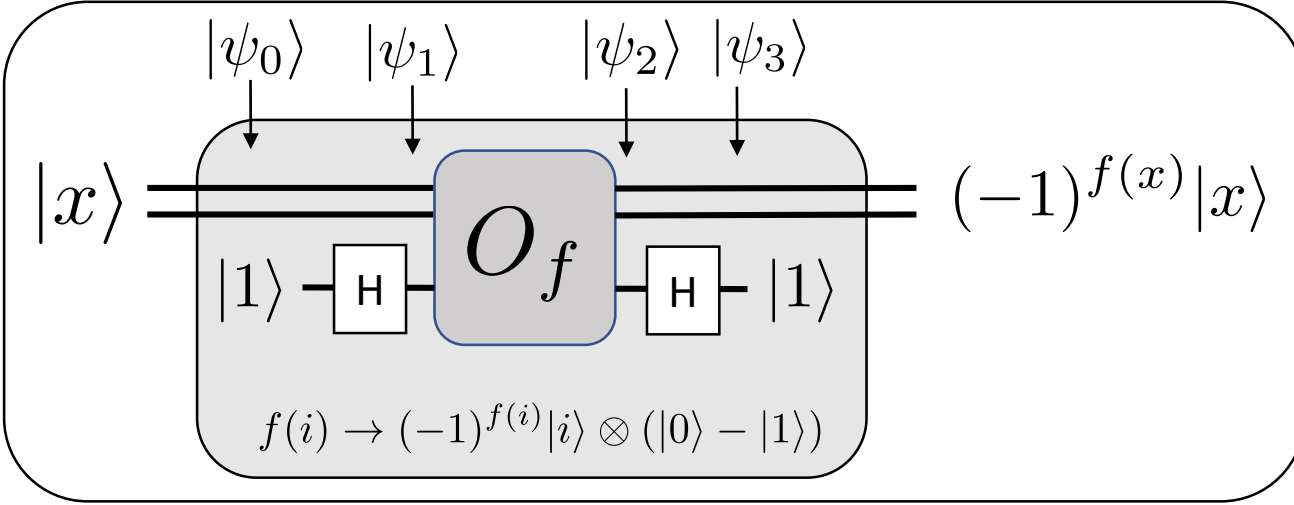
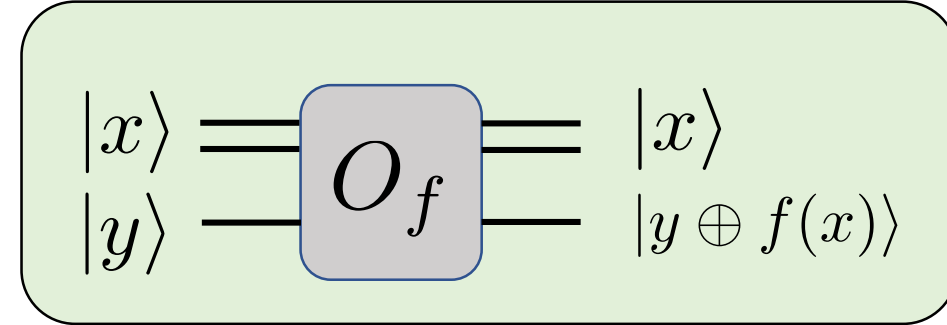
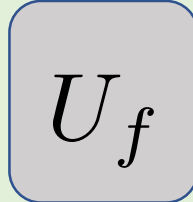


Phase Kickback

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

Phase Kickback

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



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

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

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

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

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

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

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

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

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

Balanced or equal function Game

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

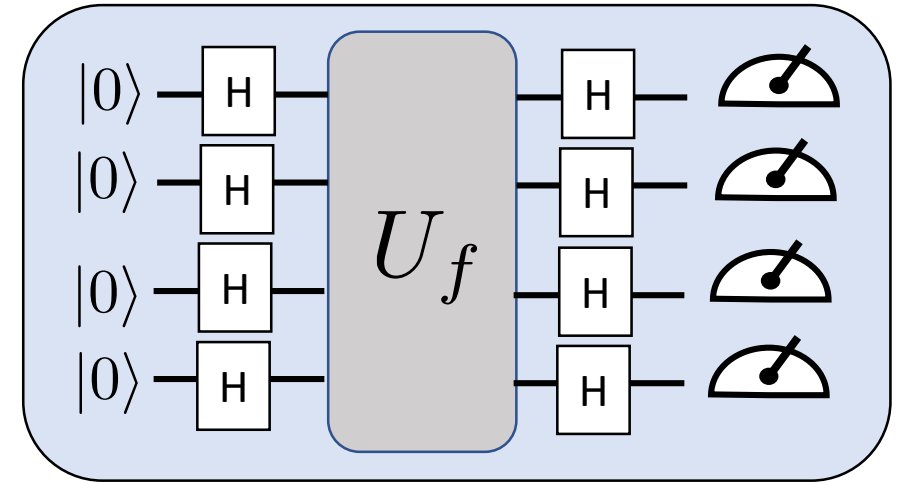
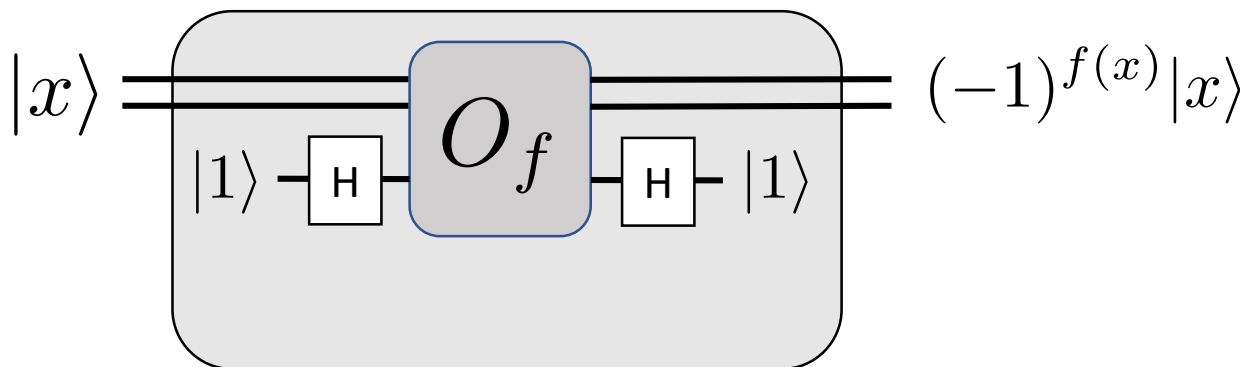
Constant: $f(x) = c \forall x$

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

Phase Kickback

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

U_f



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

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



THE UNIVERSITY of EDINBURGH
informatics

Bernstein-Vazirani Algorithm

Raul Garcia-Patron Sanchez

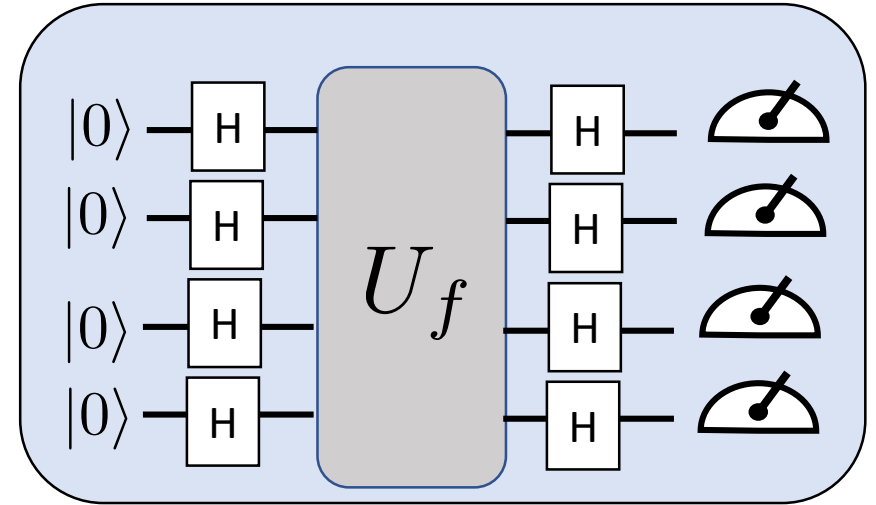


Detecting linear functions

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

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

Problem: Find a

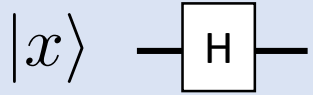


The same circuit as for Deutsch-Jozsa allow to guess “a” with a single query to the quantum oracle where classically we need at least n queries.

1 single query!



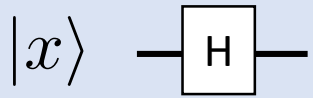
Walsh–Hadamard transform



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

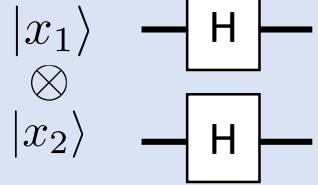
$$H|x_1\rangle = \frac{1}{\sqrt{2}}[|0\rangle + (-1)^{x_1}|1\rangle] = \frac{1}{\sqrt{2}} \sum_{y_1 \in \{0,1\}} (-1)^{x_1 y_1} |y_1\rangle$$

Walsh–Hadamard transform



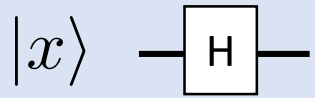
$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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



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

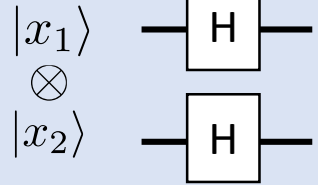
Walsh–Hadamard transform



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

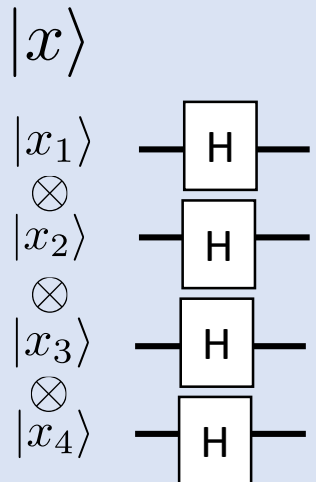
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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



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

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



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

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

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

Balanced case

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

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

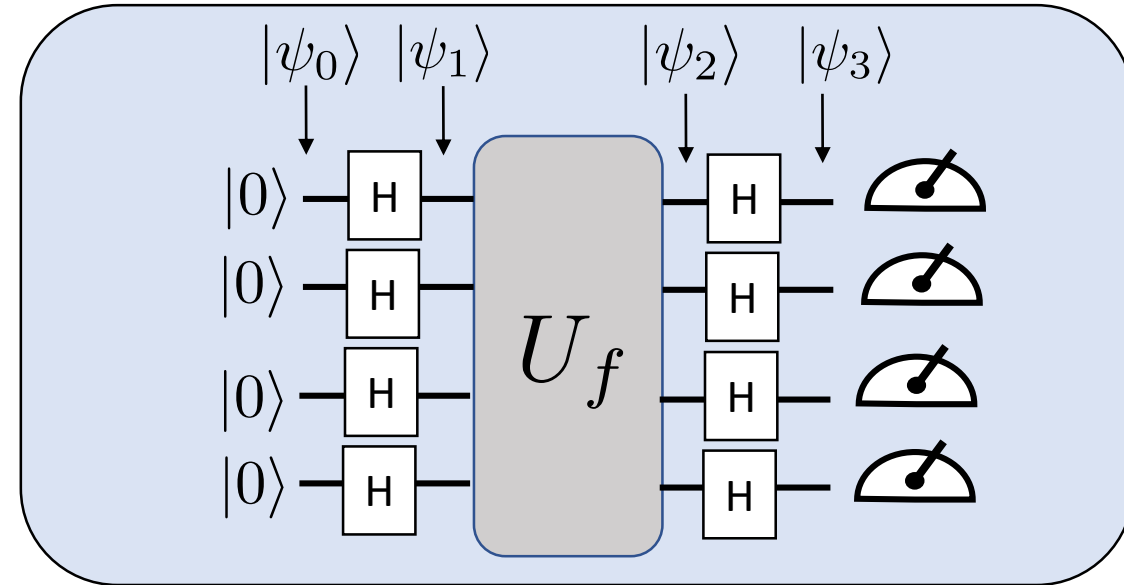
Problem: Find a

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

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

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

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



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

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

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

Problem: Find a

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

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

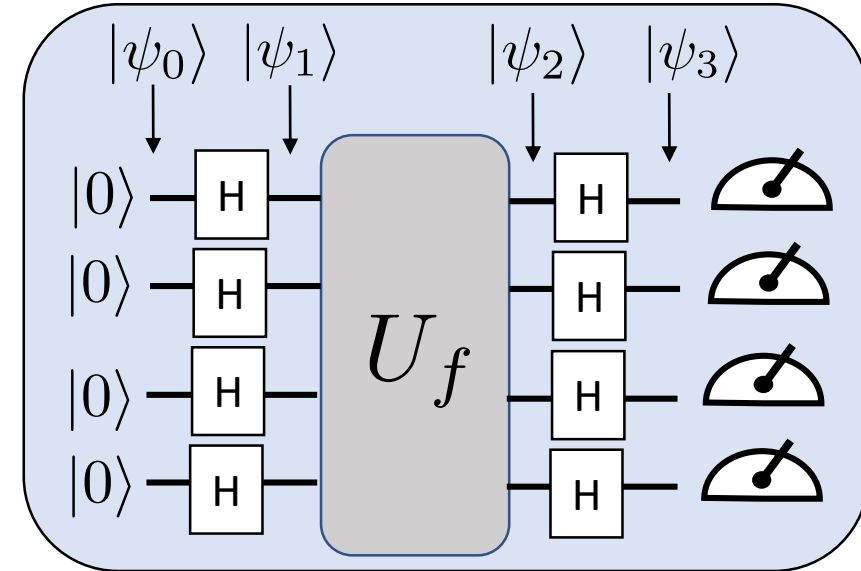
$$= \sum_{y \in \{0,1\}^n} \left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)+x \cdot y} \right) |y\rangle$$

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

$$|\psi_1\rangle$$

$$|\psi_2\rangle$$

$$|\psi_3\rangle$$



Phase Kickback

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

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

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

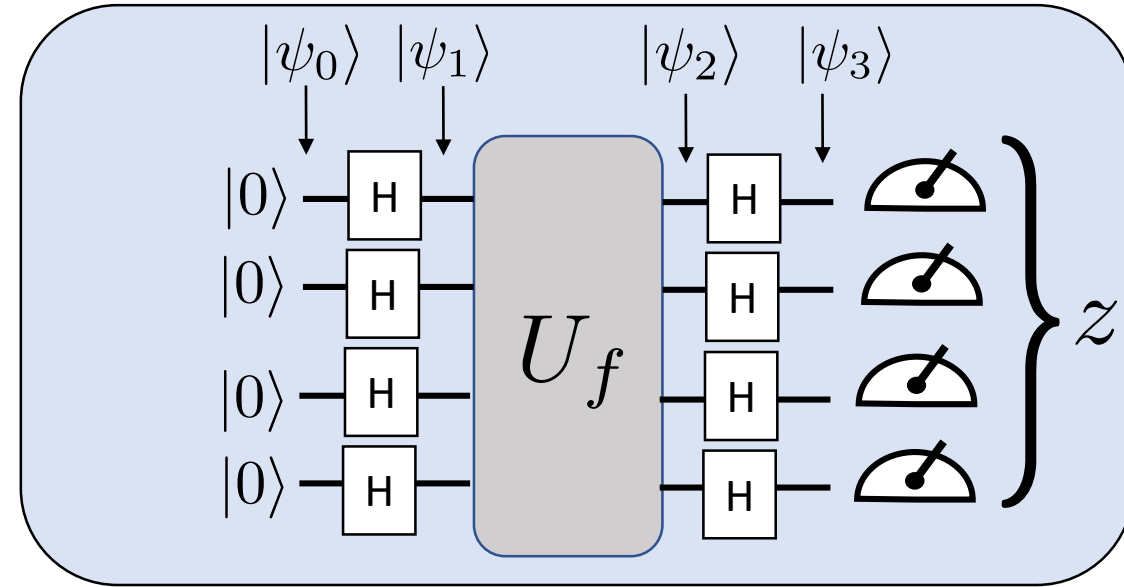
Bernstein-Vazirani Algorithm[BV93]

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

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

Problem: Find a

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



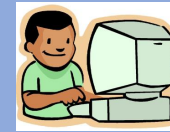
- If $y = a$ we have $(-1)^{(a \oplus y) \cdot x} = 1 \quad \rightarrow \quad P(a) = 1$
- As $\sum_i P(i) = 1$ we have that $\forall y \neq a : P(y) = 0$

Classical strategies

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

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

Problem: Find a



O_f



- 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.

References

Reading references

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

NC \equiv Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information
Cambridge University Press (2010)

RdW \equiv Quantum Computing Lecture Notes, Ronald de Wolf, <https://arxiv.org/abs/1907.09415>

G \equiv Introduction to Quantum Computation, Sevag Gharibian, [Lectures notes](#)