THE UNIVERSITY *of* EDINBURGH
informatics

Lecture 7: Phase-kickback and Deutsch-Jozsa Algorithm

Raul Garcia-Patron Sanchez

Balanced or equal function Game

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

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

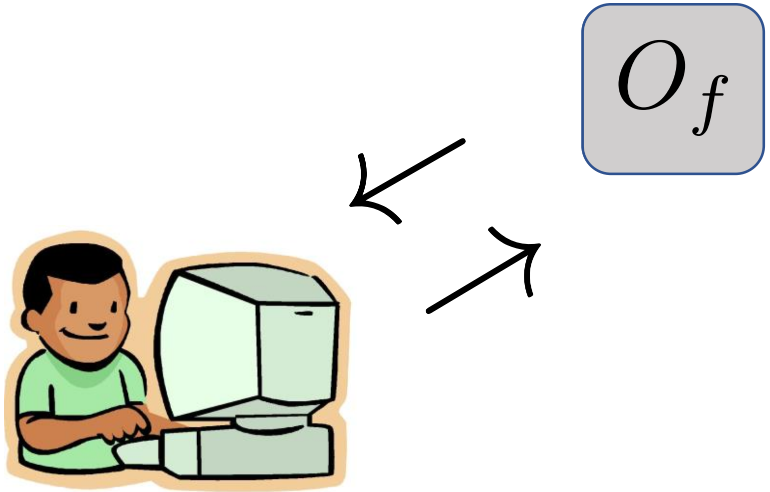
Balanced: $f(x) = 1$ on half of the bits

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:

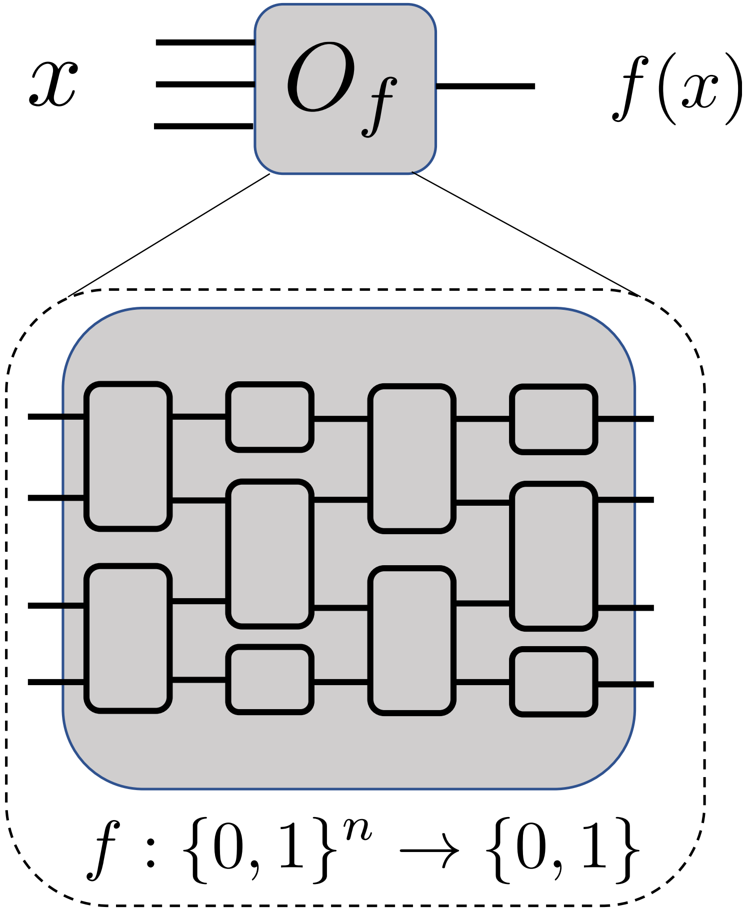
1 single query!



Oracles

"**An oracle** is a person or agency considered to provide wise and insightful counsel or **prophetic predictions** or precognition of the future, inspired by the gods. As such it is **a form of divination**." Wikipedia

Classical oracle



An oracle is a sort of subroutine

In the oracle model we do not care about the complexity of the circuit, only about the existence of a circuit.

In the oracle model the resource is the number of calls to the oracle: *queries*.

Deutsch-Jozsa Algorithm

Parallelization

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

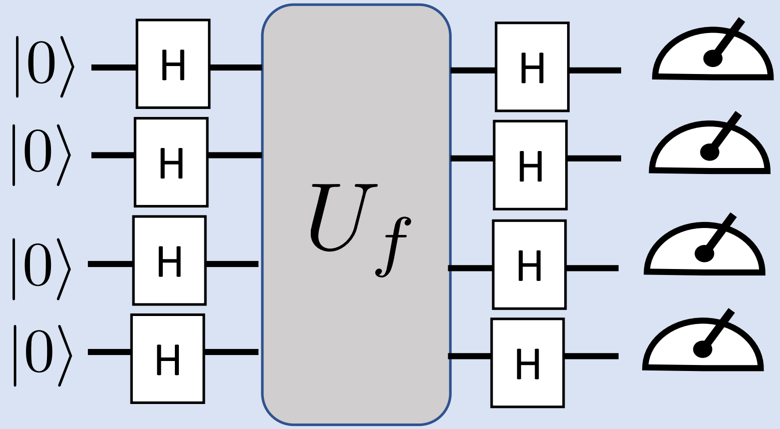
Phase Kickback

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

U_f

1. Unitary
2. Its own inverse
3. Diagonal in computational basis

Interference
with
Walsh–Hadamard transform

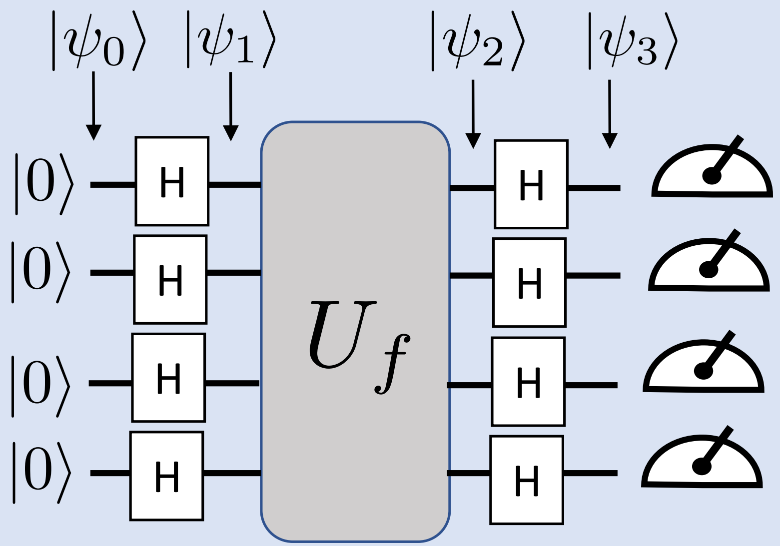


Parallelization

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

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

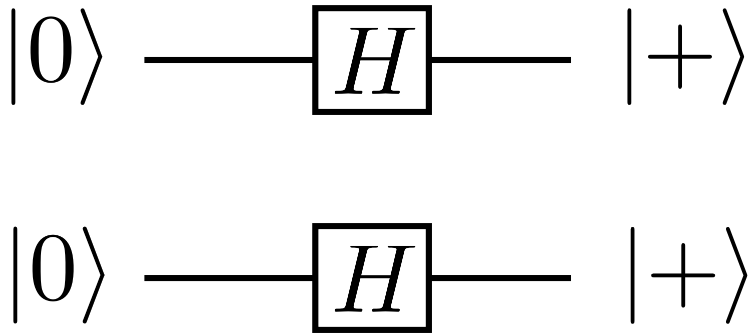
Balanced: $f(x) = 1$ on half of the bits



$$|0\rangle^{\otimes n} \xrightarrow{H^{\otimes n}} (H|0\rangle)^{\otimes n} = |+\rangle^{\otimes n} = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)^{\otimes n}$$

$|\psi_1\rangle$

Recap

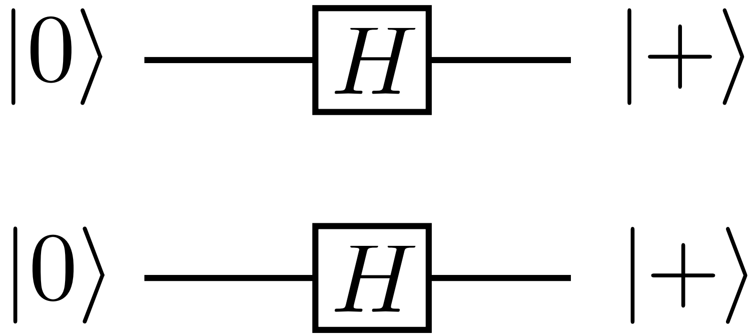


$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$$

$$\begin{aligned}(H \otimes H)(|0\rangle \otimes |0\rangle) &= (H|0\rangle) \otimes (H|0\rangle) = |+\rangle \otimes |+\rangle \\ &= \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \\ &= \frac{1}{2}\left(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right)\end{aligned}$$

Recap

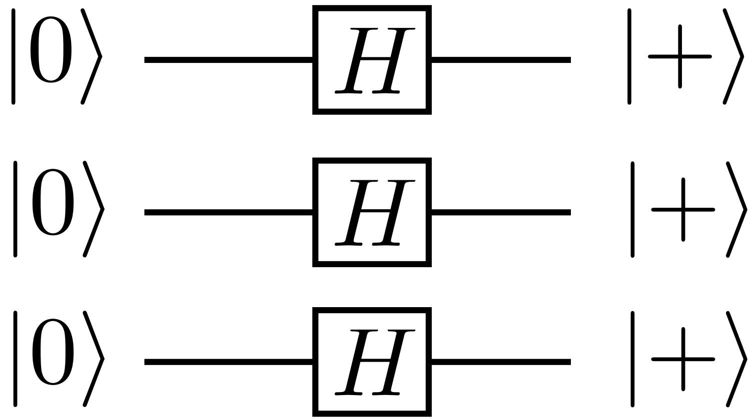


$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$$

$$\begin{aligned}(H \otimes H)(|0\rangle \otimes |0\rangle) = (H|0\rangle) \otimes (H|0\rangle) = |+\rangle \otimes |+\rangle \\ = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \\ = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)\end{aligned}$$

Recap



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

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle$$

$$H^{\otimes 3}|0\rangle \otimes |0\rangle \otimes |0\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H^{\otimes 3}|0\rangle \otimes |0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle$$

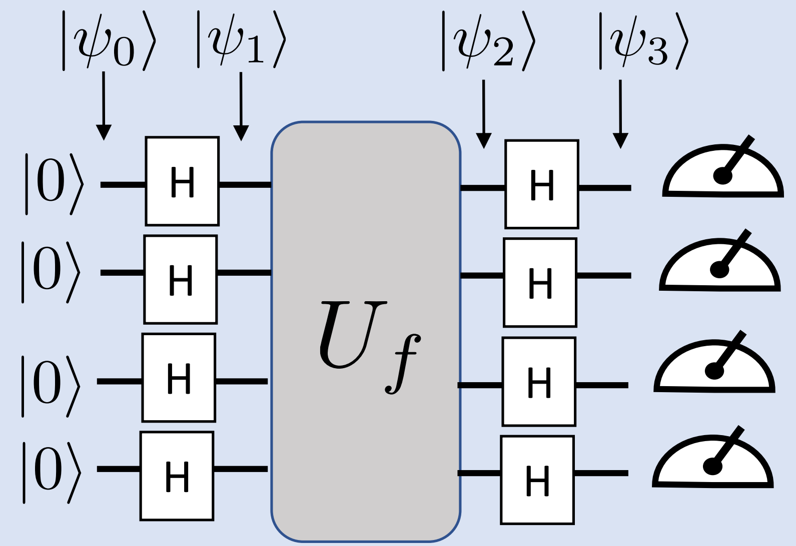
$$+|100\rangle + |101\rangle + |110\rangle + |111\rangle)$$

Parallelization

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

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

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



$$|0\rangle^{\otimes n} \xrightarrow{H^{\otimes n}} (H|0\rangle)^{\otimes n} = |+\rangle^{\otimes n} = \left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right)^{\otimes n}$$

$|\psi_1\rangle$

$$= \frac{1}{\sqrt{2^n}}(|0....00\rangle + |0....01\rangle + ... + |1....11\rangle)$$

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

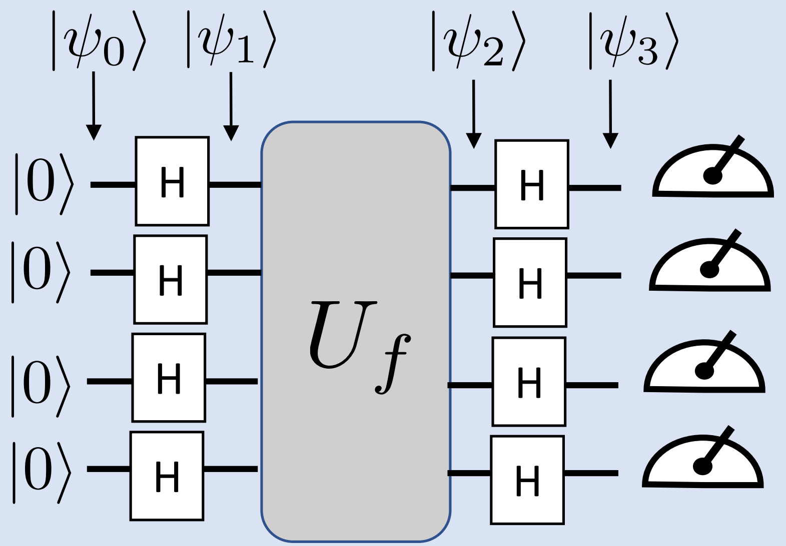
$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Phase Kickback

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

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

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



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

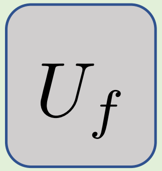
$$\xrightarrow{U_f} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$$

Phase Kickback

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

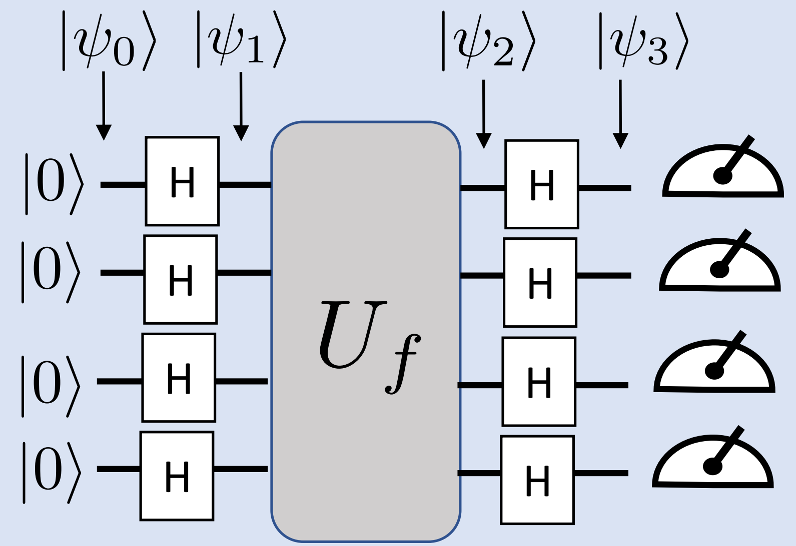


If constant function

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

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

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



$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle$$

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

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

$$= (-1)^c \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle, \text{ if } f(x) = c$$

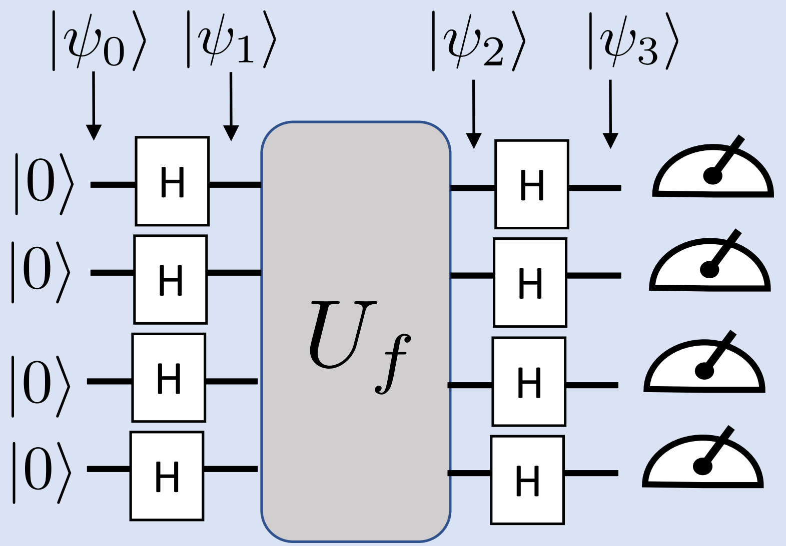
$$\xrightarrow{H^{\otimes n}} (-1)^c (H|+\rangle)^{\otimes n} = (-1)^c |0\rangle^{\otimes n}$$

If constant function

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

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

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



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

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

$$= (-1)^c \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle, \text{ if } f(x) = c$$

$$\xrightarrow{H^{\otimes n}} (-1)^c |0\rangle^{\otimes n}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle$$

$$P(0) = |\langle 0^n | \psi_3 \rangle|^2 = 1$$

Balanced case

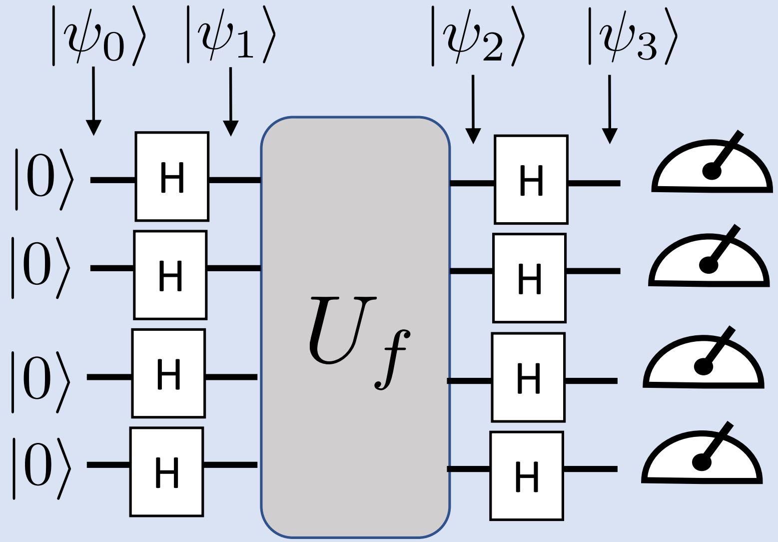
$f : \{0,1\}^n \to \{0,1\}$

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

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

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

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



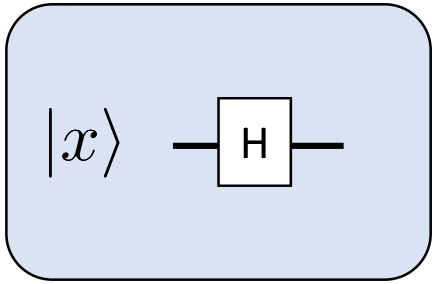
$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$$

Phase Kickback

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

Walsh–Hadamard transform

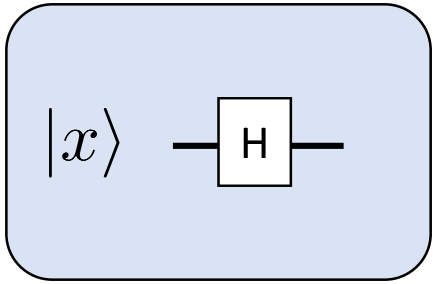


$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

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

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

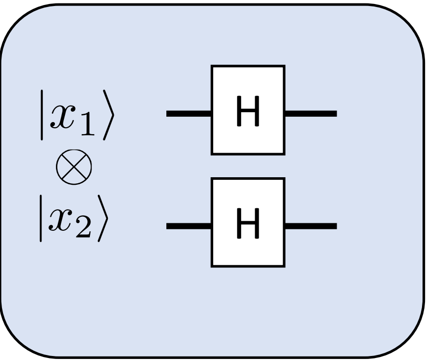
Walsh–Hadamard transform



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

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

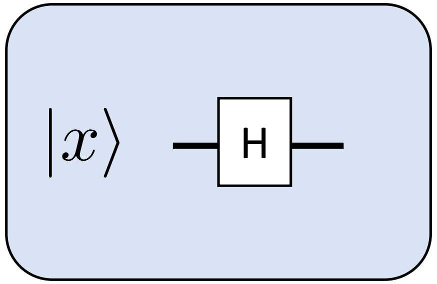
$$H|x_1\rangle = \frac{1}{\sqrt{2}}[|0\rangle + (-1)^{x_1}|1\rangle] = \frac{1}{\sqrt{2}}\sum_{y_1\in\{0,1\}}(-1)^{x_1 y_1}|y_1\rangle$$



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

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

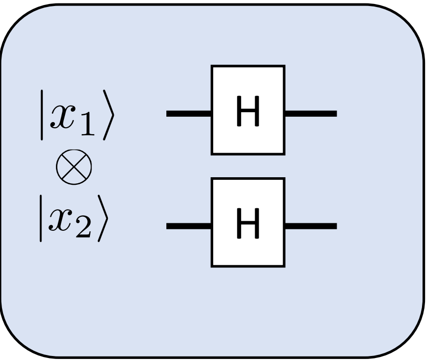
Walsh–Hadamard transform



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

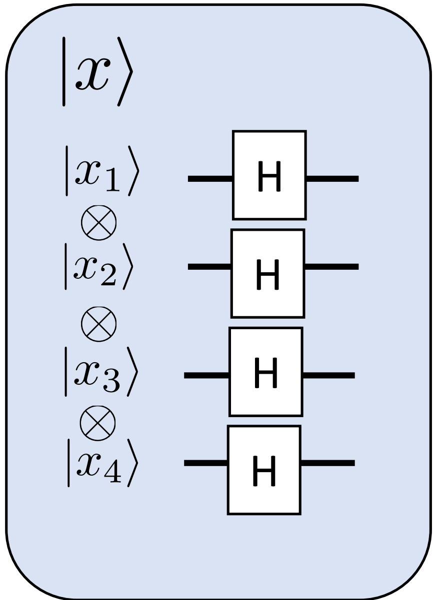
$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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



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

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



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

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

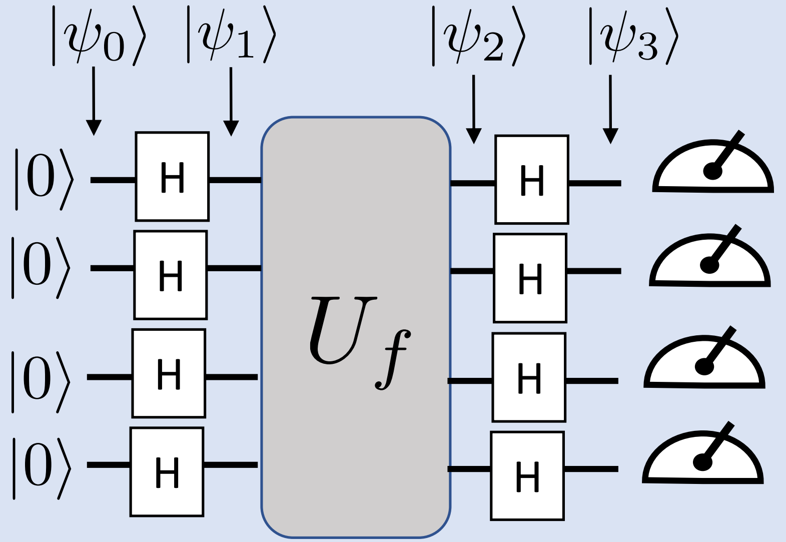
$$|x\rangle \xrightarrow{H^{\otimes n}} \bigotimes_{i}^{n} H|x_i\rangle = \frac{1}{\sqrt{2^n}} \bigotimes_{i}^{n} \left[\sum_{y_i \in \{0,1\}} (-1)^{x_i y_i}|y_i\rangle\right] = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y}|y\rangle$$

Balanced case

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

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

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



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

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

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

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

Walsh-Hadamard transform

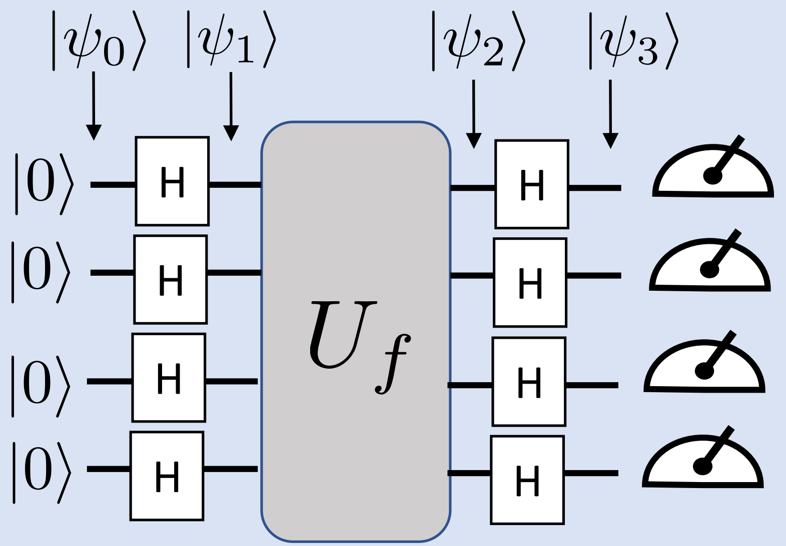
$$|x\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle$$

Balanced case

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

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

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



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

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

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

Walsh-Hadamard transform

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

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

Measurement postulate

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

Balanced or equal function Game

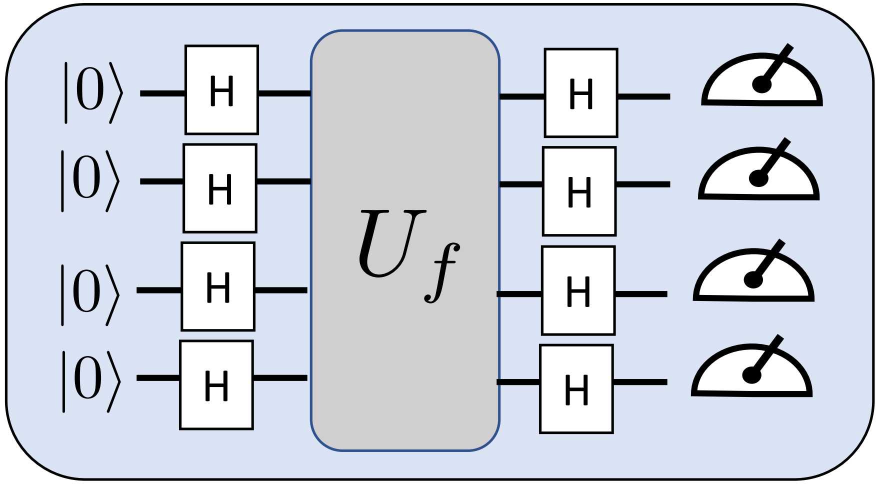
$$f : \{0,1\}^n \rightarrow \{0,1\}$$

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

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

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



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

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

THE UNIVERSITY of EDINBURGH
informatics

Discussion

Raul Garcia-Patron Sanchez

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

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

- Classical oracle $2^n/2$ queries.

- Quantum:

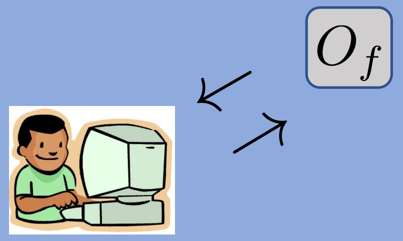
1 single query!

Classical strategies

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

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

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



- Deterministic solution

  We need $> 2^n/2$ queries: if balance we could just always obtain the same value

- Probabilistic solution

  We need only 2 queries to solve it with probability $2/3$

Protocol

1 – Query two values x and x'

2 – If $f(x) \neq f(x')$ output balanced

3 – If $f(x) = f(x')$ say constant with probability $2/3$ and balanced with probability $1/3$

References

Reading references

1. Deutsch-Jozsa NC 1.4.3 and 1.4.4
2. Phase kick-back RdW 2.4.1 and G 7.1-7.4

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