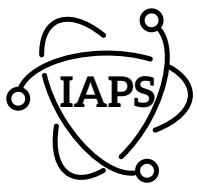
Lecture 16

QUANTUM CRYPTOGRAPHY. PART 1 - Deutsch-Jozsa Algorithm

of the course "Fundamentals of Quantum Computing"
(by IAPS and QUANTERALL)

Stoyan Mishev



INSTITUTE *for* ADVANCED
PHYSICAL STUDIES

NEW
BULGARIAN
UNIVERSITY

September 16, 2022

D. Deutsch, R. Jozsa, Proc. R. Soc. Lond. Ser. A 439(1907), 553 (1992)
https://qiskit.org/textbook/ch-algorithms/deutsch-jozsa.html

Hadamard gate and state preparation (refresher)

Hadamard gate and state preparation (refresher)

$$H^{\otimes n}|0\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle$$

see see

lecture 12. Elementary quantum circuits and programs. Part 2.

Hadamard gate and state preparation (refresher)

$$H^{\otimes n}|0\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle$$

see see

lecture 12. Elementary quantum circuits and programs. Part 2.

$$H^{\otimes n}|x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x \overset{2}{\odot} y} |y\rangle$$

$$x \overset{2}{\odot} y = x_{n-1}y_{n-1} \overset{2}{\oplus} \ldots \overset{2}{\oplus} x_0 y_0$$

(remember $a \overset{2}{\oplus} b := (a+b) \bmod 2$)

Definition 6.1 (*Deutsch's Problem*) Let $n \in \mathbb{N}$ and $f : \{0,1\}^n \to \{0,1\}$ be a function of which we know that it is

either constant, that is,

$$f(x) = c \in \{0,1\} \qquad \text{for all } x \in \{0,1\}^n$$

or balanced, that is,

$$f(x) = \begin{cases} 0 & \text{for one half of the } x \in \{0,1\}^n \\ 1 & \text{for the other half of the } x \in \{0,1\}^n \end{cases}$$

DEUTSCH'S Problem is to find the most efficient way to decide with certainty whether f is constant or balanced.

Definition 6.1 (*Deutsch's Problem*) Let $n \in \mathbb{N}$ and $f : \{0,1\}^n \to \{0,1\}$ be a function of which we know that it is

either constant, that is,

$$f(x) = c \in \{0,1\} \qquad \text{for all } x \in \{0,1\}^n$$

or balanced, that is,

$$f(x) = \begin{cases} 0 & \text{for one half of the } x \in \{0,1\}^n \\ 1 & \text{for the other half of the } x \in \{0,1\}^n \end{cases}$$

DEUTSCH'S Problem is to find the most efficient way to decide with certainty whether f is constant or balanced.

Any classical method will require at least $2^{n-1} + 1$ queries

Proposition 6.2 *Let f be as in Definition 6.1 and*

$$\begin{aligned} U_f : \P\mathbb{H}^{\otimes n} \otimes \P\mathbb{H} &\longrightarrow \P\mathbb{H}^{\otimes n} \otimes \P\mathbb{H} \\ |x\rangle \otimes |y\rangle &\longmapsto |x\rangle \otimes |y \overset{2}{\oplus} f(x)\rangle \,. \end{aligned} \tag{6.1}$$

Then there is a quantum algorithm which uses only one application of U_f and solves DEUTSCH*'s problem.*

Proposition 6.2 *Let f be as in Definition 6.1 and*

$$\begin{aligned} U_f : \P\mathbb{H}^{\otimes n} \otimes \P\mathbb{H} &\longrightarrow \P\mathbb{H}^{\otimes n} \otimes \P\mathbb{H} \\ |x\rangle \otimes |y\rangle &\longmapsto |x\rangle \otimes |y \overset{2}{\oplus} f(x)\rangle \,. \end{aligned} \tag{6.1}$$

Then there is a quantum algorithm which uses only one application of U_f and solves DEUTSCH*'s problem.*

Let $|x\rangle \otimes |y\rangle = |0\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \equiv \Psi_0$ and act on it with $(H^{\otimes n} \otimes 1) U_f (H^{\otimes n} \otimes 1)$:

Proposition 6.2 *Let f be as in Definition 6.1 and*

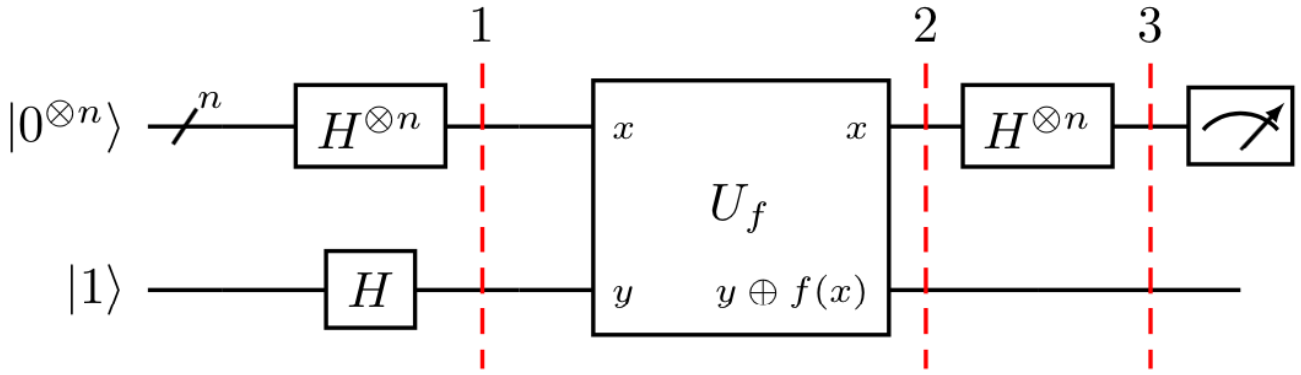
$$U_f : \P\mathbb{H}^{\otimes n} \otimes \P\mathbb{H} \longrightarrow \P\mathbb{H}^{\otimes n} \otimes \P\mathbb{H}$$
$$|x\rangle \otimes |y\rangle \longmapsto |x\rangle \otimes |y \overset{2}{\oplus} f(x)\rangle . \tag{6.1}$$

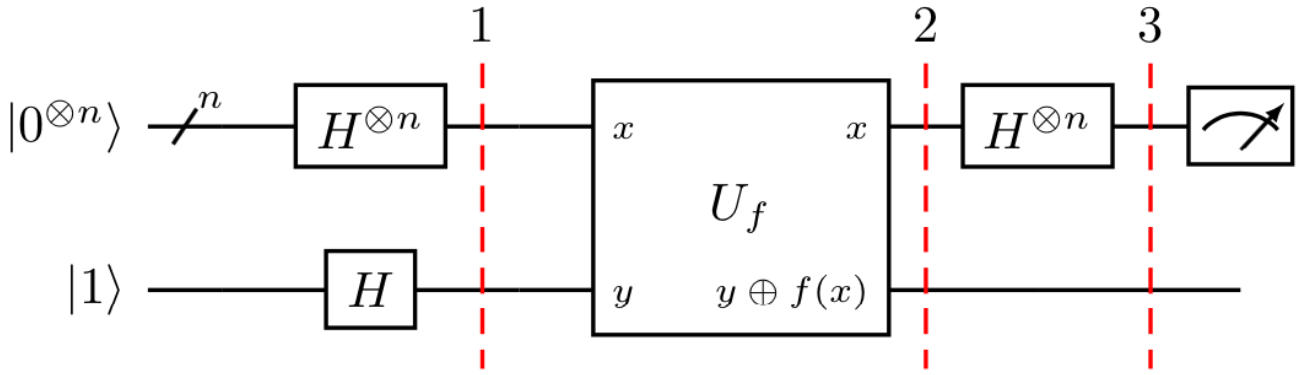
Then there is a quantum algorithm which uses only one application of U_f and solves DEUTSCH*'s problem.*

Let $|x\rangle \otimes |y\rangle = |0\rangle^n \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \equiv \Psi_0$ and act on it with $(H^{\otimes n} \otimes 1) U_f (H^{\otimes n} \otimes 1)$:

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

$$= \frac{1}{2^n} \sum_{x,y=0}^{2^n-1} (-1)^{f(x) + x \overset{2}{\oplus} y} |y\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$


1
2
3
$|0^{\otimes n}\rangle$
n
$H^{\otimes n}$
x
x
U_f
$|1\rangle$
H
y
$y \oplus f(x)$
$H^{\otimes n}$



Reminder...

Lemma 2.39 *In the basis* $\{|0\rangle, |1\rangle\}$ *the* HADAMARD *transformation has the matrix*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.159}$$

and satisfies

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2.160}$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{2.161}$$

$$H|x_j\rangle = \frac{|0\rangle + \mathrm{e}^{\pi \mathrm{i} x_j}|1\rangle}{\sqrt{2}} \tag{2.162}$$

$$H^2 = \mathbf{1}, \tag{2.163}$$

$$
\begin{aligned}
|\Psi_1\rangle &= \big(H^{\otimes n}\otimes \mathbf{1}\big)U_f\big(H^{\otimes n}\otimes \mathbf{1}\big)|\Psi_0\rangle \\
&= \big(H^{\otimes n}\otimes \mathbf{1}\big)U_f\left(H^{\otimes n}|0\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\
&\underbrace{=}_{(6.2)} \big(H^{\otimes n}\otimes \mathbf{1}\big)U_f\left(\frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1}|x\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\
&= \big(H^{\otimes n}\otimes \mathbf{1}\big)\frac{1}{2^{\frac{n+1}{2}}}\sum_{x=0}^{2^n-1}\Big(U_f\big(|x\rangle\otimes|0\rangle-|x\rangle\otimes|1\rangle\big)\Big) \\
&\underbrace{=}_{(6.1)} \big(H^{\otimes n}\otimes \mathbf{1}\big)\frac{1}{2^{\frac{n+1}{2}}}\sum_{x=0}^{2^n-1}|x\rangle\otimes\big(|f(x)\rangle-|1\overset{2}{\oplus}f(x)\rangle\big) \\
&= \big(H^{\otimes n}\otimes \mathbf{1}\big)\frac{1}{2^{\frac{n+1}{2}}}\sum_{x=0}^{2^n-1}|x\rangle\otimes(-1)^{f(x)}\big(|0\rangle-|1\rangle\big) \\
&= \frac{1}{2^{\frac{n}{2}}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}H^{\otimes n}|x\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}} \\
&\underbrace{=}_{(6.3)} \frac{1}{2^n}\sum_{y,x=0}^{2^n-1}(-1)^{f(x)+x\overset{2}{\odot}y}|y\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}\,.
\end{aligned}
$$

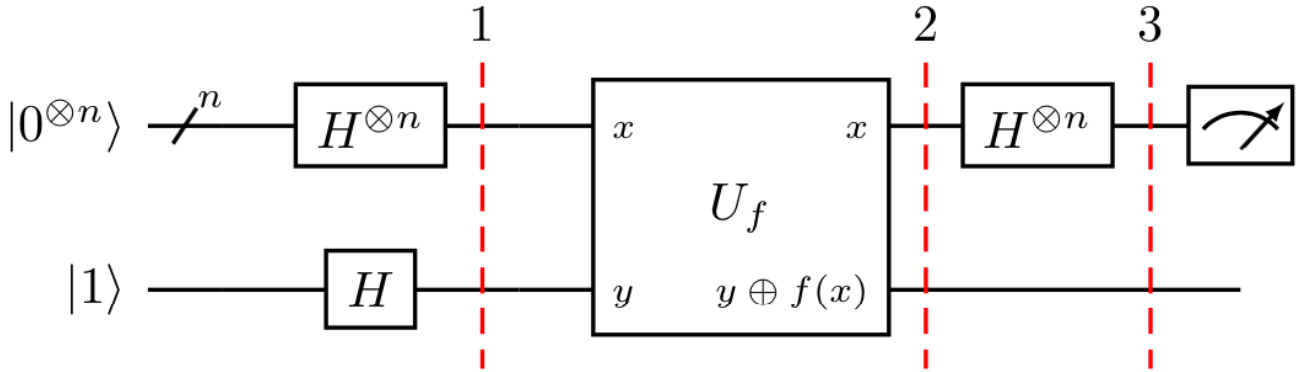
$$... = \frac{1}{2^n} \sum_{x,y=0}^{2^n-1} (-1)^{f(x)+x \overset{2}{\oplus} y} |y\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} =$$

$$\ldots = \frac{1}{2^n} \sum_{x,y=0}^{2^n-1} (-1)^{f(x)+x \overset{2}{\oplus} y} |y\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} =$$

$$= \frac{1}{2^n} \left(\sum_{x=0}^{2^n-1} (-1)^{f(x)} |0\rangle + \sum_{x,y=1}^{2^n-1} (-1)^{f(x)+x \overset{2}{\oplus} y} |y\rangle \right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \Psi_1^A \otimes \frac{|0\rangle -}{\sqrt{}}$$

$$|\langle 0|\Psi_1^A\rangle|^2 = \left(\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right)^2 =$$

$$= \begin{cases} \left(\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^c \right)^2 & = 1 \quad \text{if } f \text{ is constant} \\ \left(\frac{1}{2^n} \left(2^{n-1} - 2^{n-1} \right) \right)^2 & = 0 \quad \text{if } f \text{ is balanced} \end{cases}$$



1. Prepare two quantum registers. The first is an n-qubit register initialized to $|0\rangle$, and the second is a one-qubit register initialized to $|1\rangle$:

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$$

2. Apply a Hadamard gate to each qubit:

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle \left(|0\rangle - |1\rangle\right)$$

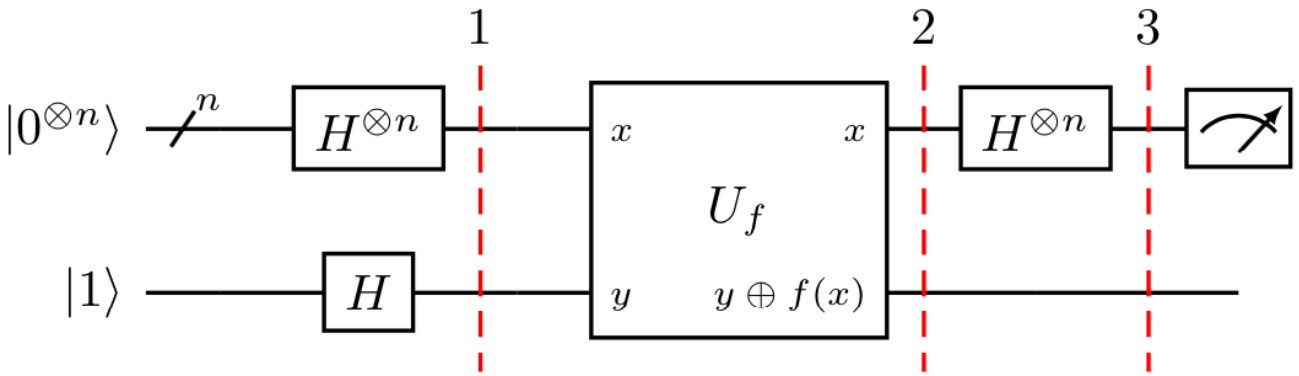
3. Apply the quantum oracle $|x\rangle|y\rangle$ to $|x\rangle|y \oplus f(x)\rangle$:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \end{aligned}$$

since for each x, $f(x)$ is either 0 or 1.

[1] q. oracle

https://docs.microsoft.com/en-us/azure/quantum/concepts-oracles



4. At this point the second single qubit register may be ignored. Apply a Hadamard gate to each qubit in the first register:

$$
\begin{aligned}
|\psi_3\rangle &= \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \left[\sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle \right] \\
&= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[\sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} \right] |y\rangle
\end{aligned}
$$

where $x \cdot y = x_0 y_0 \oplus x_1 y_1 \oplus \ldots \oplus x_{n-1} y_{n-1}$ is the sum of the bitwise product.

5. Measure the first register. Notice that the probability of measuring $|0\rangle^{\otimes n} = |\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|^2$, which evaluates to 1 if $f(x)$ is constant and 0 if $f(x)$ is balanced.

THANK YOU FOR YOUR ATTENTION!

БЛАГОДАРЯ ЗА ВНИМАНИЕТО!