Quantum computation: lecture 3

- Deutsch's model of quantum circuits
- Deutsch's problem
- Classical method of resolution
- Quantum algorithm:

  Deutsch-Josza's algorithm

Deutsch's model of quantum circuits

As already mentioned, every circuit can be represented by a single unitary operation:

n input qubits $\quad |\psi_{in}\rangle \; - \boxed{\; U \;} - \; |\psi_{out}\rangle = U|\psi_{in}\rangle \quad$ n output qubits

$\in \mathbb{C}^{2^n} \qquad\qquad\qquad \in \mathbb{C}^{2^n}$

and the extraction of information happens via a measurement in $\{|x_1 .. x_n\rangle,\ x_1 .. x_n \in \{0,1\}\}$, with $\text{prob}(|x_1 .. x_n\rangle) = |\langle x_1 .. x_n | \psi_{out}\rangle|^2$

Why to use quantum circuits?

1) To simulate quantum physical systems (not our aim)

2) To solve efficiently classical problems involving a Boolean function $f: \{0,1\}^n \to \{0,1\}^m$

= our aim!

3 generic stages

1. Any input of $f: \{0,1\}^n \to \{0,1\}^m$ is a sequence of n bits $x_1 \dots x_n$, which can be encoded into a quantum state $|x_1 \dots x_n\rangle$. We will construct <u>superpositions</u> of states $|\psi\rangle = \sum_{x_1 \dots x_n \in \{0,1\}} \alpha_{x_1 \dots x_n} |x_1 \dots x_n\rangle$ (with $\sum_{x_1 \dots x_n \in \{0,1\}} |\alpha_{x_1 \dots x_n}|^2 = 1$).

2. Unitary operation $U^{(f)}$ performed on $|\psi\rangle$

$$U^{(f)}|\psi\rangle = \sum_{x_1 \dots x_n \in \{0,1\}} \alpha_{x_1 \dots x_n} U^{(f)} |\psi\rangle$$

by linearity.

3. Measurement: outcome $= |x_1 \dots x_n\rangle$ with probability $|\langle x_1 \dots x_n | U^{(f)} | \psi \rangle|^2$; should be high (or at least >0) for states $|x_1 \dots x_n\rangle$ corresponding to the solution of the pb.

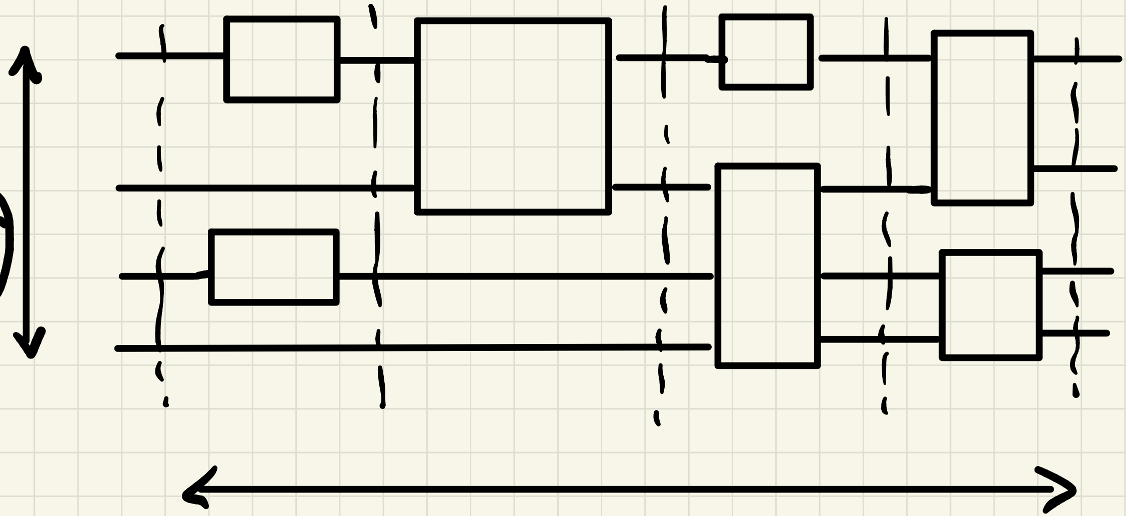
Here are two assumptions: (without loss of generality)

- initial state $= |0,0,\dots,0\rangle$
- final measurement performed in the computational basis $\{ |x_1 .. x_n\rangle, x_1 \dots x_n \in \{0,1\} \}$

These assumptions come sometimes with some additional cost on <u>circuit complexity</u>.

Remark: circuit complexity = width × depth

width
(= number of qubits)



depth
(= number of layers)

Finally, before we proceed to the study of our first quantum algorithm, let us introduce the quantum "oracle" gate U_f associated to a Boolean function $f: \{0,1\}^n \longrightarrow \{0,1\}$

(we consider the case $m=1$ here, but this can be generalized)

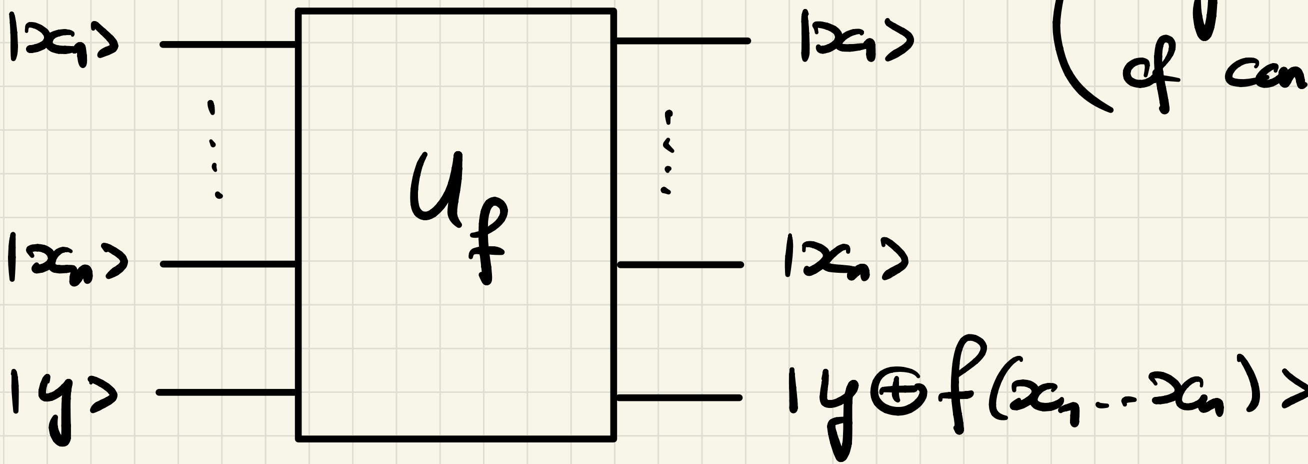
Observe first that unless $n=1$ & f is bijective, the evaluation of a Boolean function f is in general <u>irreversible</u>.

A reversible way of evaluating a function f is obtained by <u>augmenting the memory</u> with an "ancilla" bit:

$$\tilde{f}(x_1 \dots x_n, y) = (x_1 \dots x_n, y \oplus f(x_1 \dots x_n))$$

Corresponding quantum circuit:

(~ generalization of controlled-U)



$$U_f\left(|x_1 \ldots x_n\rangle \otimes |y\rangle\right) = |x_1 \ldots x_n\rangle \otimes |y \oplus f(x_1 \ldots x_n)\rangle$$

(Note: needs to be constructed for each f)

__U_f is unitary__. Indeed, for all basis elements:

$$\langle x_1' \ldots x_n' | \otimes \langle y' | \, U_f^\dagger U_f \, | x_1 \ldots x_n \rangle \otimes | y \rangle$$

$$= \Big(\langle x_1' \ldots x_n' | \otimes \langle y' \oplus f(x_1' \ldots x_n') | \Big) \cdot \Big(| x_1 \ldots x_n \rangle \otimes | y \oplus f(x_1 \ldots x_n) \rangle \Big)$$

$$= \underbrace{\langle x_1' | x_1 \rangle}_{= \delta_{x_1' x_1}} \cdot \ldots \underbrace{\langle x_n' | x_n \rangle}_{= \delta_{x_n' x_n}} \cdot \langle y' \oplus f(\underline{x_1' \ldots x_n'}) | y \oplus f(\underline{x_1 \ldots x_n}) \rangle$$

same!

$$= \delta_{x_1' x_1} \ldots \delta_{x_n' x_n} \underbrace{\langle y' \oplus f(x_1 \ldots x_n) | y \oplus f(x_1 \ldots x_n) \rangle}_{= \delta_{y' y} \text{ for every } f\,!} \quad \#$$

Deutsch's problem

- We are given a Boolean function $f:\{0,1\}^n \to \{0,1\}$ and an oracle capable of evaluating $f(x)$ for a given x at no cost.
- On top of that, we are informed that

$$\begin{cases} \text{either } f \text{ is constant, i.e. } f(x)=f(y) \ \forall x,y \in \{0,1\}^n \\ \text{or } f \text{ is balanced, i.e. } \begin{cases} f(x)=1 & \text{for half of the } x\text{'s} \\ f(x)=0 & \text{for the other half} \end{cases} \end{cases}$$

The aim of the problem is to decide between these two alternatives with the least possible number of calls to the oracle.

<u>Note</u>: We do not know anything a priori about the structure of f; just the above information.

Classical method of resolution

Call the oracle in k different points $x^{(1)} \dots x^{(k)} \in \{0,1\}^n$:

- if $f(x^{(1)}) = \dots = f(x^{(k)})$, declare "$f$ is constant"
- otherwise, declare "f is balanced"

In the worst case, $k = 2^{n-1} + 1$ calls to the oracle are needed ($>$ half the total # of points) in order to obtain a 100% correct answer.

Probabilistic algorithm (still classical)

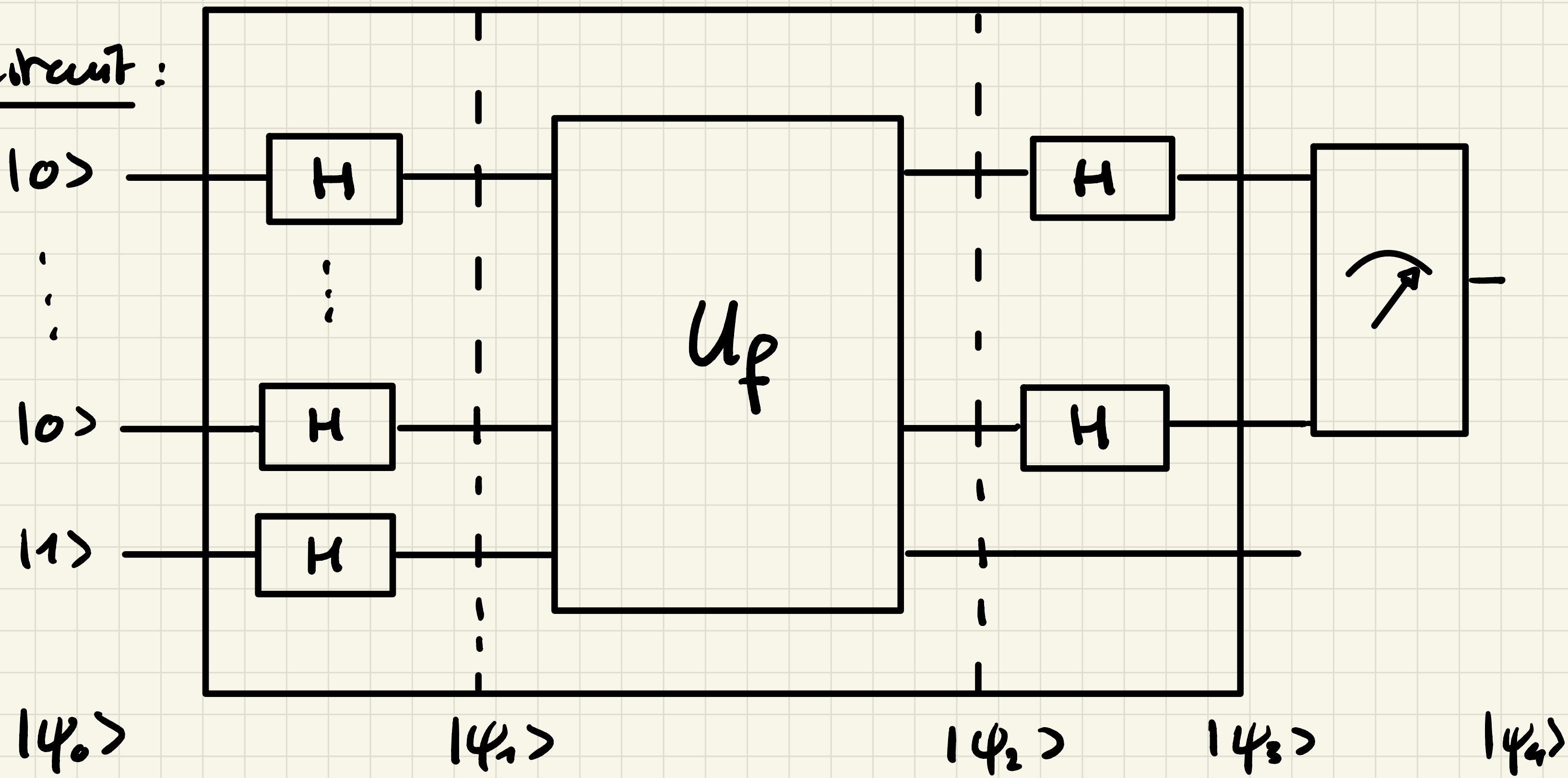
Fix $k \geq 1$ & draw k iid points $x^{(1)} .. x^{(k)} \in \{0,1\}^n$ (with possible replacement). Again:

- if $f(x^{(1)}) = \ldots = f(x^{(k)})$, declare "$f$ is constant"
- otherwise, declare "f is balanced"

The probability of making an error (which can only happen in the first case) is $\dfrac{1}{2^{k-1}}$, so can be made as small as wanted in $O(1)$ calls.

Deutsch-Josza's quantum algorithm

Circuit:



Stage 0

Initial state: $|\varphi_0\rangle = \underbrace{|0\rangle \otimes \ldots \otimes |0\rangle}_{n \text{ qubits}} \otimes \underset{\substack{\uparrow \\ \text{"ancilla"} \\ \text{qubit}}}{|1\rangle}$

$$= |0,0,\ldots,0\rangle \otimes |1\rangle$$

An extra "ancilla" qubit is added to the input to allow for computations later.

Stage 1: superposition of states

$$|\psi_1\rangle = H^{\otimes(n+1)} |\psi_0\rangle$$

$$= H|0\rangle \otimes \dots \otimes H|0\rangle \otimes H|1\rangle$$

Note: $H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \sum_{x_1 \in \{0,1\}} |x_1\rangle$, $H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

$$\Rightarrow |\psi_1\rangle = \frac{1}{\sqrt{2}} \sum_{x_1 \in \{0,1\}} |x_1\rangle \otimes \dots \otimes \frac{1}{\sqrt{2}} \sum_{x_n \in \{0,1\}} |x_n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$= \frac{1}{2^{n/2}} \sum_{x_1 \dots x_n \in \{0,1\}} |x_1, \dots, x_n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Stage 2 : passage through the quantum oracle

Recall $U_f(|x_1 \dots x_n\rangle \otimes |y\rangle) = |x_1 \dots x_n\rangle \otimes |y \oplus f(x_1 \dots x_n)\rangle$

$$|\psi_2\rangle = U_f |\psi_1\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{x_1 \dots x_n \in \{0,1\}} U_f\left(|x_1 \dots x_n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{2^{n/2}} \sum_{x_1 \dots x_n \in \{0,1\}} |x_1 \dots x_n\rangle \otimes \frac{|f(x_1 \dots x_n)\rangle - |\overline{f(x_1 \dots x_n)}\rangle}{\sqrt{2}}$$

Magic!

$$|x_1 \dots x_n\rangle \otimes \frac{|f(x_1 \dots x_n)\rangle - |\overline{f(x_1 \dots x_n)}\rangle}{\sqrt{2}}$$

$$= \begin{cases} |x_1 \dots x_n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \text{if } f(x_1 \dots x_n) = 0 \\ |x_1 \dots x_n\rangle \otimes \frac{|1\rangle - |0\rangle}{\sqrt{2}} & \text{if } f(x_1 \dots x_n) = 1 \end{cases}$$

$$= |x_1 \dots x_n\rangle \otimes (-1)^{f(x_1 \dots x_n)} \cdot \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$= (-1)^{f(x_1 \dots x_n)} \cdot |x_1 \dots x_n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

So $|\psi_2\rangle = \frac{1}{2^{n/2}} \sum_{x_1 \ldots x_n \in \{0,1\}} (-1)^{f(x_1 \ldots x_n)} |x_1 \ldots x_n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

The action of U_f on the ancilla qubit, which is in a superposition state, has now been transferred to the first n qubits!

<u>Note</u>: From now on, we could forget the ancilla qubit...

Stage 3: "analysis"

$$|\psi_3\rangle = \left(H^{\otimes n} \otimes I\right) |\psi_2\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{x_1 .. x_n \in \{0,1\}} (-1)^{f(x_1 .. x_n)} \underbrace{H^{\otimes n} |x_1 .. x_n\rangle}_{*} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$* = H|x_1\rangle \otimes \dots \otimes H|x_n\rangle$$

Note: $H|x_1\rangle = \frac{|0\rangle + (-1)^{x_1}|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \sum_{z_1 \in \{0,1\}} (-1)^{z_1 \cdot x_1} |z_1\rangle$

$$\text{So } * = \frac{1}{2^{n/2}} \sum_{z_1 \dots z_n \in \{0,1\}} (-1)^{z_1 x_1 + \dots + z_n x_n} |z_1 \dots z_n\rangle$$

Gathering everything together, we obtain:

$$|\psi_3\rangle = \frac{1}{2^{n/2}} \sum_{x_1 \dots x_n \in \{0,1\}} (-1)^{f(x_1 \dots x_n)}$$

$$\cdot \frac{1}{2^{n/2}} \sum_{z_1 \dots z_n \in \{0,1\}} (-1)^{z_1 \cdot x_1 + \dots + z_n \cdot x_n} |z_1 \dots z_n\rangle$$

$$\otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Reordering the terms:

$$|\psi_3\rangle = \sum_{z_1 \ldots z_n \in \{0,1\}} \underbrace{\left(\frac{1}{2^n} \sum_{x_1 \ldots x_n \in \{0,1\}} (-1)^{f(x_1 \ldots x_n) + z_1 x_1 + \ldots + z_n x_n} \right)}_{:= \alpha_{z_1 \ldots z_n}} |z_1 \ldots z_n\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

<u>Stage 4</u>: measurement of the first n qubits

state $|z_1 \ldots z_n\rangle$ is observed with prob. $|\alpha_{z_1 \ldots z_n}|^2$

Let us consider the particular state $|00\ldots0\rangle$:

$$|\alpha_{00\ldots0}|^2 = \left| \frac{1}{2^n} \sum_{x_1\ldots x_n \in \{0,1\}} (-1)^{f(x_1\ldots x_n)} \right|^2$$

$$= \begin{cases} 1 & \text{if } f \text{ is constant} \\ 0 & \text{if } f \text{ is balanced} \end{cases}$$

<u>So</u>: if the output state is $|00\ldots0\rangle$, f is constant; otherwise, f is balanced.

(and this with a single call to the quantum oracle)

Final remarks:

- In an actual quantum computer, there is noise, so the probability of a correct answer is not 100%.
- The problem is a toy problem, as the full knowledge of f is required to build the gate U_f...