

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:

$$\begin{array}{ccccc} n \text{ input} & |\psi_{\text{in}}\rangle & \text{---} \boxed{U} \text{---} & |\psi_{\text{out}}\rangle = U |\psi_{\text{in}}\rangle & n \text{ output} \\ \text{qubits} & \in \mathbb{C}^{2^n} & & \in \mathbb{C}^{2^n} & \text{qubits} \end{array}$$

and the extraction of information happens

Via a measurement in $\{|x_1 \dots x_n\rangle, x_1 \dots x_n \in \{0,1\}\}$,

with $\text{prob}(|x_1 \dots x_n\rangle) = |\langle x_1 \dots x_n | \psi_{\text{out}} \rangle|^2$

Why to use quantum circuits?

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

2) To solve efficiently classical problems involving a Boolean function $f: \{0,1\}^n \rightarrow \{0,1\}^m$
= our aim!

3 generic stages

1. Any input of $f: \{0,1\}^n \rightarrow \{0,1\}^m$ 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 superpositions of states $|\psi\rangle = \sum_{x_1 \dots x_n \in \{0,1\}^n} \alpha_{x_1 \dots x_n} |x_1 \dots x_n\rangle$ (with $\sum_{x_1 \dots x_n \in \{0,1\}^n} |\alpha_{x_1 \dots x_n}|^2 = 1$).

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

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

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

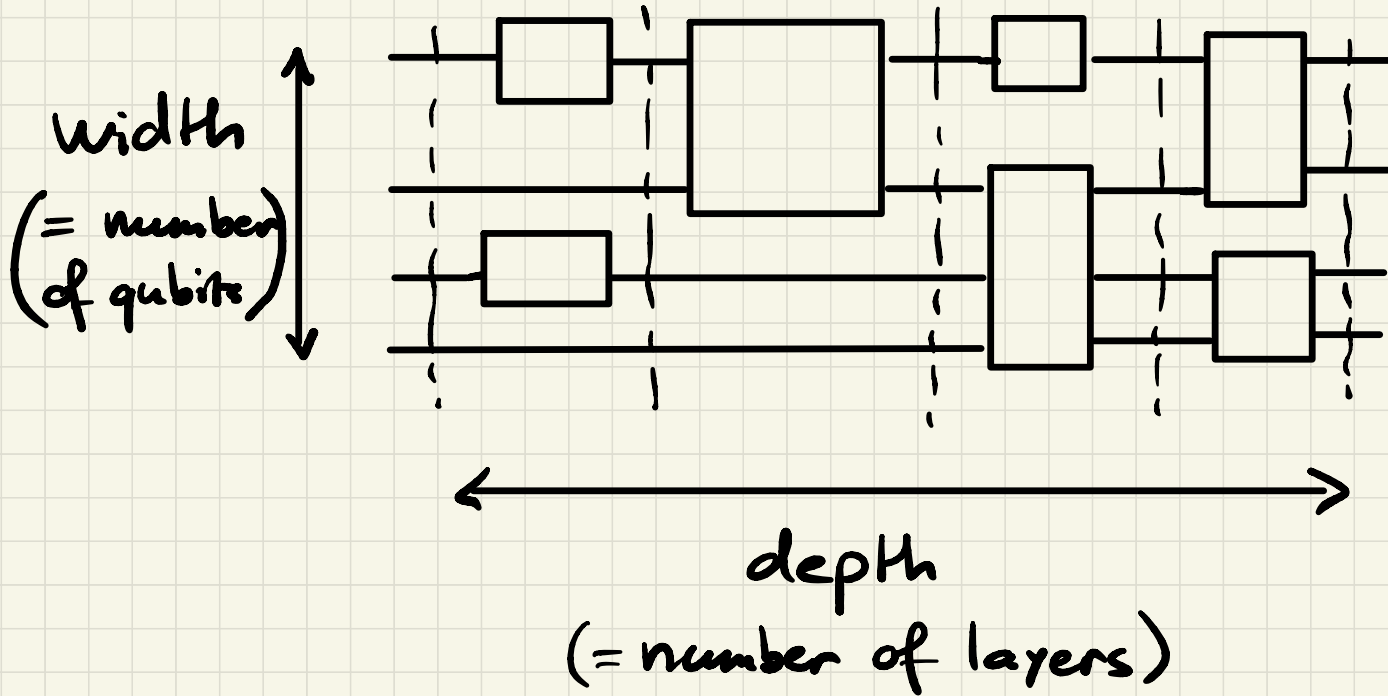
$|x_1 \dots x_n\rangle$ corresponding to the solution of the pb.

Here are two assumptions: (without loss of generality)

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

These assumptions come sometimes with some additional cost on circuit complexity.

Remark: circuit complexity = width $\times$ depth



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

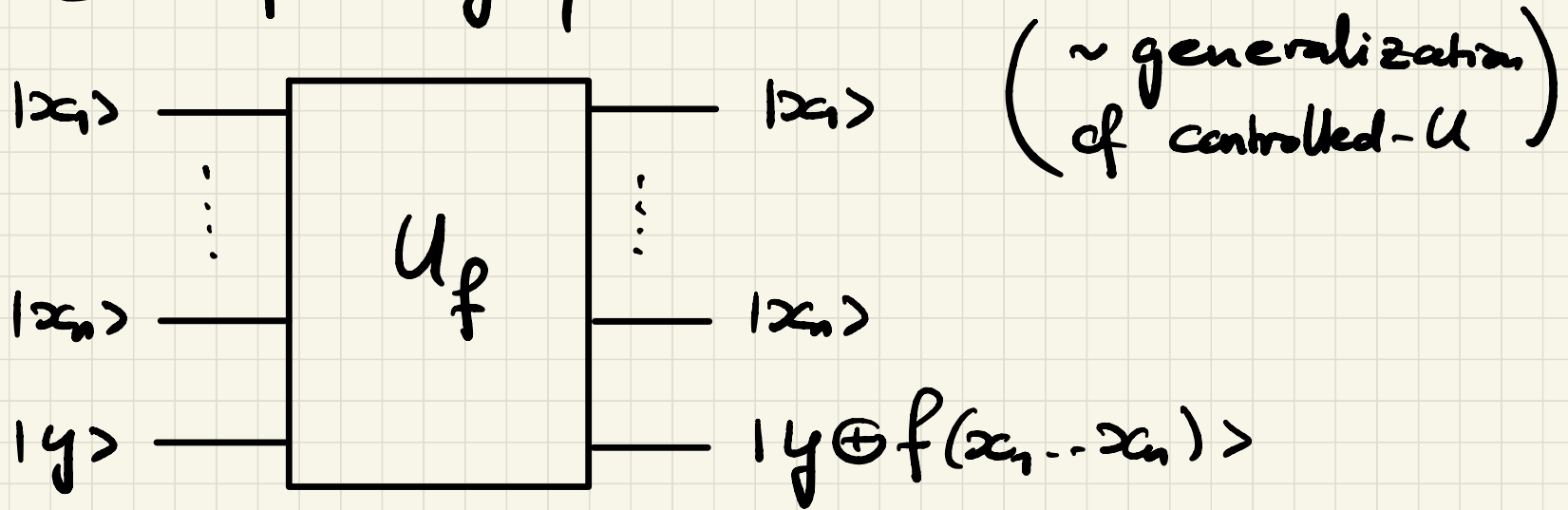
(we consider the case $m=1$ here, but)
this can be generalized

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

A reversible way of evaluating a function f is obtained by augmenting the memory 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:



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

(Note: needs to be constructed for each f)

U_f is unitary. Indeed, for all basis elements:

$$\begin{aligned}
 & \langle x'_1 \dots x'_n | \otimes \langle y' | U_f^\dagger U_f | x_1 \dots x_n \rangle \otimes | y \rangle \\
 &= (\langle x'_1 \dots x'_n | \otimes \langle y' \oplus f(x'_1 \dots x'_n) |) \cdot (| x_1 \dots x_n \rangle \otimes | y \oplus f(x_1 \dots x_n) \rangle) \\
 &= \underbrace{\langle x'_1 | x_1 \rangle}_{= \delta_{x'_1 x_1}} \cdots \underbrace{\langle x'_n | x_n \rangle}_{= \delta_{x'_n x_n}} \cdot \underbrace{\langle y' \oplus f(x'_1 \dots x'_n) | y \oplus f(x_1 \dots x_n) \rangle}_{\substack{\uparrow \text{ same! } \uparrow}} \\
 &= \delta_{x'_1 x_1} \cdots \delta_{x'_n x_n} \underbrace{\langle y' \oplus f(x_1 \dots x_n) | y \oplus f(x_1 \dots x_n) \rangle}_{= \delta_{y' y} \text{ for every } f!} \neq
 \end{aligned}$$

Deutsch's problem

- We are given a Boolean function $f: \{0,1\}^n \rightarrow \{0,1\}$ and an oracle capable of evaluating $f(x)$ for a given x at no cost.
- On top of that, we are informed that
 - { either f is constant, i.e. $f(x) = f(y) \quad \forall x, y \in \{0,1\}^n$
 - { or f is balanced, i.e. $\begin{cases} f(x) = 1 & \text{for half of the } x\text{'s} \\ f(x) = 0 & \text{for the other half} \end{cases}$

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

Note: 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 $x^{(1)} \dots x^{(k)} \in \{0,1\}^n$
(with possible replacement). Again:

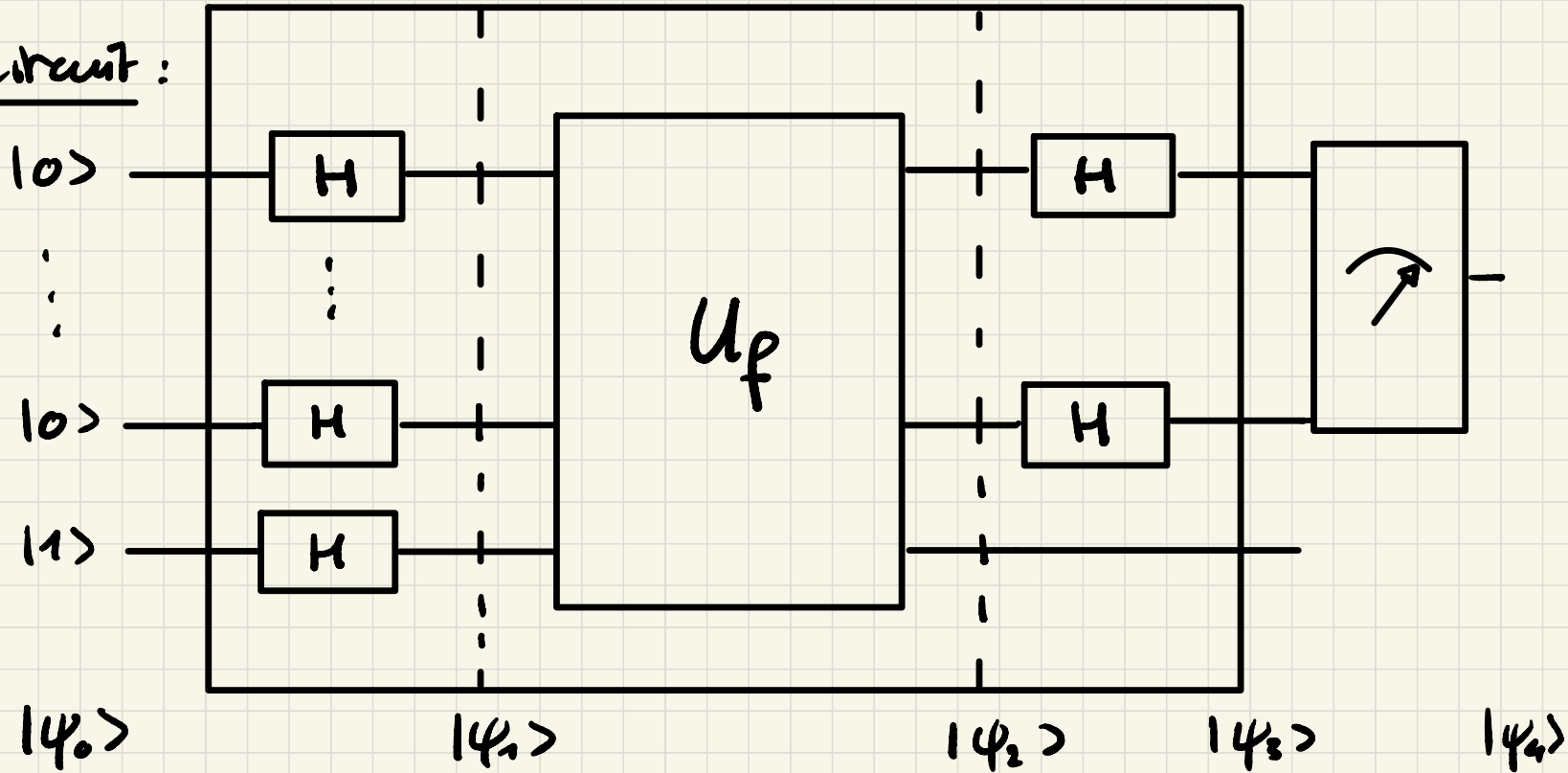
- if $f(x^{(1)}) = \dots = f(x^{(k)})$, declare "f is constant"
- otherwise, declare "f is balanced"

The probability of making an error (which can only happen in the first case) is $\frac{1}{2^{k-1}}$,

so can be made as small as wanted in $O(1)$ calls.

Deutsch-Jozsa's quantum algorithm

Circuit:



Stage 0

$$\text{Initial state: } |\psi_0\rangle = \underbrace{|0\rangle \otimes \dots \otimes |0\rangle}_n \otimes |1\rangle$$

n qubits ↑
"ancilla" qubit

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

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!

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

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

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

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

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

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

Note: From now on, we could forget the ancilla qubit...

Stage 3: "analysis"

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

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

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

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

$$S_0 * = \frac{1}{2^{n/2}} \sum_{z_1 \dots z_n \in \{0,1\}} (-1)^{z_1 x_1 + \dots + z_n x_n} |z_1 \dots z_n\rangle$$

Gathering everything together, we obtain:

$$|\psi_3\rangle = \frac{1}{2^{n/2}} \sum_{z_1 \dots z_n \in \{0,1\}} (-1)^{f(z_1 \dots z_n)}$$

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

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

Reordering the terms:

$$|\psi_3\rangle = \sum_{z_1 \dots z_n \in \{0,1\}} \underbrace{\left(\frac{1}{2^n} \sum_{z_1 \dots z_n \in \{0,1\}} (-1)^{f(z_1 \dots z_n) + z_1 z_1 + \dots + z_n z_n} \right)}_{\textcircled{\times} \frac{|0\rangle - |1\rangle}{\sqrt{2}}} |z_1 \dots z_n\rangle$$

$$:= \alpha_{z_1 \dots z_n}$$

Stage 4: measurement of the first n qubits

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

Let us consider the particular state $|00\dots 0\rangle$:

$$\begin{aligned} |\alpha_{00\dots 0}|^2 &= \left| \frac{1}{2^n} \sum_{x_1 \dots x_n \in \{0,1\}} (-1)^{f(x_1 \dots x_n)} \right|^2 \\ &= \begin{cases} 1 & \text{if } f \text{ is constant} \\ 0 & \text{if } f \text{ is balanced} \end{cases} \end{aligned}$$

So: if the output state is $|00\dots 0\rangle$, 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 ...