LECTURE 4
INTRODUCTION TO QUANTUM COMPUTING, THE CIRCUIT MODEL

INF587 Quantum computer science and applications

Thomas Debris-Alazard

Inria, École Polytechnique

THE OBJECTIVE OF THE DAY

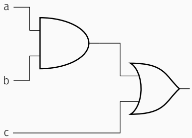
Computer science: art of computing...

What do we mean by quantum computing?

$\longrightarrow$ The quantum circuit model!

1. Notation and basic circuits
   - Quantum circuits: representation of unitaries and measurement
   - The quantum gate CNOT
   - Controlled unitaries
2. The Solovay-Kitaev theorem and the quantum gate model (universal quantum gates)
3. Simulating classical circuits with quantum circuits
4. Quantum parallelism and interference
5. A quantum algorithm: Simon's algorithm

Boolean circuit: finite directed acyclic (no loop) graph with **AND**, **OR** and **NOT** **classical** gates which has input and output nodes.



A circuit computes $f : \{0,1\}^n \longrightarrow \{0,1\}^m$ if given n input bits $\mathbf{x}$, it outputs m bits given by $f(\mathbf{x})$.

A circuit C_n **decides a language** $L \subseteq \{0,1\}^n$ if C_n given $\mathbf{x} \in \{0,1\}^n$ outputs one if and only if $\mathbf{x} \in L$.

Two questions:

- What are the **classical** gates that enable to compute any function $f : \{0,1\}^n \longrightarrow \{0,1\}^m$?
- What class of languages circuits recognize?

Universality

Logic gates **AND**, **OR** and **NOT** are enough to compute any function $f : \{0,1\}^n \longrightarrow \{0,1\}^m$.

$\longrightarrow$ Is it doable quantumly?

Problem: *any quantum operation is invertible (even unitary)* but **AND** is not invertible...

Universality

Logic gates **AND**, **OR** and **NOT** are enough to compute any function $f : \{0,1\}^n \longrightarrow \{0,1\}^m$.

$\longrightarrow$ Is it doable quantumly?

Problem: *any quantum operation is invertible (even unitary)* but **AND** is not invertible...

Toffoli (also CCNOT) Gate

The Toffoli gate takes 3 input bits and outputs 3 bits as follows:

$$\textsf{Toffoli}(x, y, z) = (x, y, z \ \textsf{XOR} \ (x \ \textsf{AND} \ y))$$

Proposition: Inversability and Universality

- The Toffoli gate is invertible,
- Any classical circuit computing a function f consisting of N gates in the set $\{\textsf{AND}, \textsf{OR}, \textsf{NOT}\}$ can be computed using $O(N)$ Toffoli gates.

$\longrightarrow$ In particular: the number of Toffoli gates is roughly the same

But is the classical circuit model meaningful?

Complexity Theory: uniformly polynomial circuits

Family of circuits $C \stackrel{\text{def}}{=} \{C_n\}_n$ with n input bits and one output bit *such that* there is polylog(n)-space Turing machine that outputs C_n given n.

$$L_C \stackrel{\text{def}}{=} \bigcup_n \{x \in \{0,1\}^n \ : \ C_n(x) = 1\}$$

$L \in \mathsf{P}$ if and only if there exits a uniform family of circuits C such that $L = L_C$.

$\longrightarrow$ Given a uniform family of circuits $C = \{C_n\}$: C_n **has at most** poly(n)**-gates!**

What about quantum computation?

Is the circuit model reasonable? If yes, what is doable quantumly and at which cost?

What about quantum computation?

Is the circuit model reasonable? If yes, what is doable quantumly and at which cost?

Two intuitions:

- "Quantum circuit" can simulate classical circuits because Toffoli gates are universal...

  $\longrightarrow$ Therefore: quantum circuits define a "reasonable" model of computation.

- Complexity of computation will be taken into account from the number of "quantum gates"

  $\longrightarrow$ Therefore: we expect quantum circuits to measure the complexity as in the classical case

NOTATION AND BASIC CIRCUITS

During this course we consider the state space $\mathbb{C}^{2^n} = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}}$ of n-qubits register

State space, computational basis and measurement

We will always write n-qubits registers as

$$\sum_{\mathsf{x} \in \{0,1\}^n} \alpha_{\mathsf{x}} |\mathsf{x}\rangle \quad \text{where } |\mathsf{x}\rangle = |x_1, \ldots, x_n\rangle \ (= |x_1\rangle \otimes \cdots \otimes |x_n\rangle) \text{ and } \sum_{\mathsf{x} \in \{0,1\}^n} |\alpha_{\mathsf{x}}|^2 = 1.$$

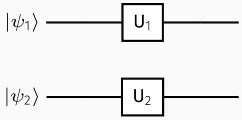
The family $(|\mathsf{x}\rangle)_{\mathsf{x} \in \{0,1\}^n}$ is known as the computational basis

$\longrightarrow$ All the considered measurements (in this course) will be in the computational basis.

Given two quantum states $|\psi_1\rangle$, $|\psi_2\rangle$ and two unitaries U_1, U_2, the circuit representation of

$$(U_1 \otimes U_2)\,(|\psi_1\rangle \otimes |\psi_2\rangle)$$

is given by



Exercise

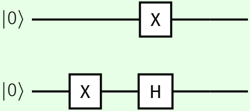
1. What becomes $\frac{|00\rangle+|01\rangle}{\sqrt{2}}$ when feeding to the above circuit?
2. Describe a quantum circuit that transforms $|00\rangle$ into $\frac{|10\rangle-|11\rangle}{\sqrt{2}}$.

Solution

1. What becomes $\frac{|00\rangle + |01\rangle}{\sqrt{2}}$ when feeding to the above circuit?

   It becomes: $\mathbf{U}_1 |0\rangle \otimes \mathbf{U}_2 \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}} \mathbf{U}_1 |0\rangle \otimes \mathbf{U}_2 |0\rangle + \frac{1}{\sqrt{2}} \mathbf{U}_1 |0\rangle \otimes \mathbf{U}_2 |1\rangle$.

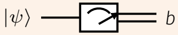
2. Describe a quantum circuit that transforms $|00\rangle$ into $\frac{|10\rangle - |11\rangle}{\sqrt{2}}$.



A measurement converts $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ into a probabilistic classical bit $b \in \{0, 1\}$ where

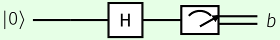
$$\mathbb{P}(b = 0) = |\alpha|^2 \quad \text{and} \quad \mathbb{P}(b = 1) = |\beta|^2.$$

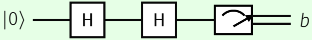
The circuit representation of a measurement is



Exercise

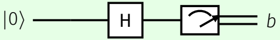
Give the distribution of the following probabilistic bits b:

1. 

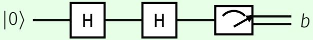
2. 

Exercise

Give the distribution of the following probabilistic bits b:

1. 

   The output bit b is uniform, namely: $\mathbb{P}(b = 0) = \mathbb{P}(b = 1) = \frac{1}{2}$.

2. 

   As $\mathsf{H}^2 = \mathsf{I}_2$, the output bit b is always zero.

THE QUANTUM CNOT GATE

Let us introduce the Controlled-NOT gate (unitary) over 2-qubits:

$$|a, b\rangle \mapsto |a, a \oplus b\rangle$$

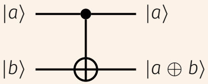
It is a unitary (it maps the computational basis to the computation basis).

Quantum CNOT-gate $|a, b\rangle \mapsto |a, a \oplus b\rangle$

- **Matrix representation:**

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

- **Circuit representation:**



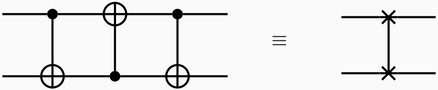
$$|a, b\rangle \mapsto |a, a \oplus b\rangle$$

is the quantum generalization of the **XOR** operation!

Be careful

The **XOR** operation $(a, b) \mapsto a \oplus b$ cannot be a quantum operation because is not invertible.

Given two wires, is it possible to swap two qubits?



$$
\begin{aligned}
|a, b\rangle &\longrightarrow |a, a \oplus b\rangle \\
&\longrightarrow |a \oplus (a \oplus b), a \oplus b\rangle \\
&\longrightarrow |b, (a \oplus b) \oplus b\rangle \\
&= |b, a\rangle \, .
\end{aligned}
$$

Given a qubit $|\psi\rangle$, is it possible to build a quantum circuit that copies it?

$\longrightarrow$ **No!** Because the no-cloning theorem (see Exercise session 1)

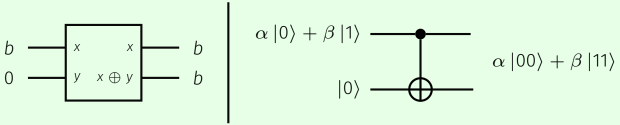
But it is doable for classical bit $(b, 0) \mapsto (b, 0 \oplus b) = (b, b)$...

Given a qubit $|\psi\rangle$, is it possible to build a quantum circuit that copies it?

$\longrightarrow$ **No!** Because the no-cloning theorem (see Exercise session 1)

But it is doable for classical bit $(b, 0) \mapsto (b, 0 \oplus b) = (b, b)$...

Take a look at the quantum case

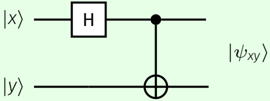


We have built an **entangled** state!

Bell States

$$|\psi_{xy}\rangle \stackrel{\text{def}}{=} \frac{|0, y\rangle + (-1)^x |1, (1 \oplus y)\rangle}{\sqrt{2}}$$

The quantum circuit building Bell states



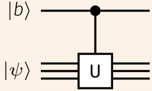
$$|x, y\rangle \xrightarrow{H \otimes I_2} \frac{|0\rangle + (-1)^x |1\rangle}{\sqrt{2}} \otimes |y\rangle = \frac{|0, y\rangle + (-1)^x |1, y\rangle}{\sqrt{2}} \xrightarrow{\text{C-NOT}} \frac{|0, y\rangle + (-1)^x |1, (1 \oplus y)\rangle}{\sqrt{2}}$$

Controlled U-gate

Let $\mathbf{U}$ be any unitary over n-qubits. The controlled $\mathbf{U}$-gate has one control qubit $|b\rangle$ and n target qubits $|\psi\rangle$. It is defined as

- If $b = 0$, it outputs $|b\rangle \otimes |\psi\rangle$.
- If $b = 1$, it outputs $|b\rangle \otimes \mathbf{U}\,|\psi\rangle$.

Circuit representation:



$\longrightarrow$ Controlled-$\mathbf{U}$ $\equiv$ If condition then instruction $\mathbf{U}$

Exercise

Show that the CNOT gate is the controlled $\mathbf{X}$-gate.

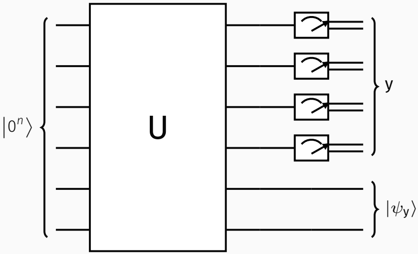
Quantum circuits: starting from n qubits initialized at $|0^n\rangle$ and then successively apply the two admissible operations (unitary and measurements).

Applying $\mathbf{U}_1$ and then $\mathbf{U}_2$ is equivalent to applying $(\mathbf{U}_2\mathbf{U}_1)$

$\longrightarrow$ we can assume the algorithm performs a unitary, then a measurement, then a unitary, then measurement and so on...

We will consider only algorithms where **we first perform all the unitary operations and then perform measurements in the computational basis**.

$\longrightarrow$ As powerful as general algorithms (admitted)



AUXILIARY QUBITS

$$\mathsf{U} : |\psi\rangle \longrightarrow \mathsf{U}\,|\psi\rangle$$

$\longrightarrow$ It is often easier to build $\mathsf{U}' : |\psi\rangle\,|0\rangle_{\text{aux}} \longrightarrow \mathsf{U}(|\psi\rangle)\,|0\rangle_{\text{aux}}$

Extra qubits are called auxiliary qubits, ancilliary qubits or workspace.

$\longrightarrow$ it is important that they start at $|0\rangle$ and end at $|0\rangle$ (see Exercise session)

SOLOVAY-KITAEV THEOREM AND GATE MODEL

Any classical function can be computed with gates {**AND**, **OR**, **NOT**} (universal gates)

What are the quantum universal gates?

The following gate is important (first time in this course)

The $\pi/8$-gate

It maps $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto e^{i\pi/4}|1\rangle$:

$$\mathbf{T} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Origin of the terminology

Up to an unimportant global phase $\mathbf{T}$ is equal to $\mathbf{T} = e^{i\pi/8}\begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$

Solovay-Kitaev Theorem (admitted)

Let $\mathcal{G} = \{\mathbf{CNOT}, \mathbf{H}, \mathbf{T}\}$. Any unitary $\mathbf{U}$ over n-qubits can be approximated by applying

$$O\left(2^{2n} \log^4\left(\frac{1}{\varepsilon}\right)\right)$$

gates from $\mathcal{G}$ with accuracy ε.

In other words, from the description of $\mathbf{U}$, one can construct a sequence $\mathbf{G}_1, \ldots, \mathbf{G}_N \in \mathcal{G}$ with $N = O(2^{2n} \log^4(\frac{1}{\varepsilon}))$ and

$$||\mathbf{G}_N \ldots \mathbf{G}_1 - \mathbf{U}|| \leq \varepsilon,$$

where $||\mathbf{G}_N \ldots \mathbf{G}_1 - \mathbf{U}|| \overset{\text{def}}{=} \max_{|\psi\rangle} ||\mathbf{G}_N \ldots \mathbf{G}_1 |\psi\rangle - \mathbf{U} |\psi\rangle||$ is the *operator norm*.

$\longrightarrow$ The **log** term is important: exponential accuracy with a polynomial number of gates

Other universal gates?

Yes! The **CNOT** and qubits gates are also universal

Quantum circuits $\iff$ Unitary evolutions

$O\left(2^{2n} \log^4\left(\frac{1}{\varepsilon}\right)\right)$ gates $\{\text{CNOT}, \text{H}, \text{T}\}$ to approximate **any** unitary **U**

$\longrightarrow$ exponential cost 2^{2n}

Does any unitary need an exponential number of gates to be built?

$O\left(2^{2n}\log^4\left(\frac{1}{\varepsilon}\right)\right)$ gates $\{\mathbf{CNOT}, \mathbf{H}, \mathbf{T}\}$ to approximate **any** unitary $\mathbf{U}$

$\longrightarrow$ exponential cost 2^{2n}

Does any unitary need an exponential number of gates to be built?

No! As for classical computations there are unitaries easy to compute, other not...

The Quantum Gate Model

The quantum running time of a unitary U is the amount of 1 and 2-qubit gates needed to apply U.

The running time of a single-qubit measurement is 1.

One may say that estimating the running time as the number of 1-2 qubits unitaries is an overkill

$\longrightarrow$ It can be hard to implement some 1 or 2 qubits unitary...

A more reasonable model

Running time: number **H**, **T** and **CNOT** gates that are used

$\longrightarrow$ The "difficulty" to implement quantum circuits reduces to compute this small set of gates!

By the Solovay-Kitaev theorem

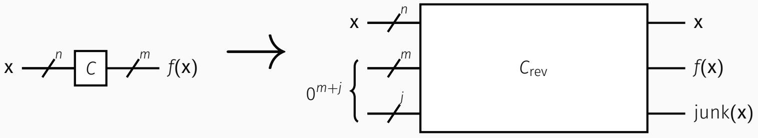
The running time of the above model is the same than in the quantum gate model, but up to polynomial factor (in the input length n) if one targets an exponentially close accuracy...

In conclusion: lot of debates to define the running time of quantum circuits...

For us: no debates, we don't care of polynomial factors (even if it is a hard problem to handle in "practice"...) and we will use the quantum gate model

CLASSICAL CIRCUITS WITH QUANTUM CIRCUITS

C computing a function f with T gates can be transformed into a reversible circuit C_{rev} that consists only of $O(T)$ Toffoli gates, possibly with some junk state $\text{junk}(\mathbf{x})$.



Informally, the junk part keeps a place to perform intermediary computations

Simulating classical circuits with quantum circuits

Classical Toffoli gates can be interpreted as a quantum unitary acting on three qubits:

$$\textbf{Toffoli}\,|x, y, z\rangle \stackrel{\text{def}}{=} |x, y, z \oplus xy\rangle$$

Therefore: C_{rev} can be interpreted as a unitary $\mathbf{U}$:

$$\mathbf{U}\left|\mathbf{x}, 0^{m+j}\right\rangle \stackrel{\text{def}}{=} |\mathbf{x}\rangle\,|f(\mathbf{x})\rangle\,|\text{junk}(\mathbf{x})\rangle$$

$\longrightarrow$ Quantum computers are at least as powerful as classical computers!

The unitary U_f

For any function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ that can be computed classically with a circuit that runs in time T, there exists a quantum circuit on $n+m$ qubits that runs in time $O(T)$ that can perform the unitary

$$U_f : |x\rangle |y\rangle \rightarrow |x\rangle |y \oplus f(x)\rangle \,.$$

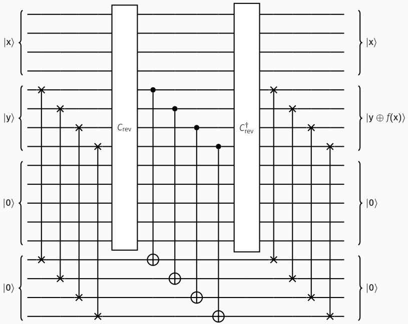
Be careful:

$|x\rangle \mapsto |f(x)\rangle$ may not be a quantum operation (for instance f be the zero function).

$\longrightarrow$ The auxiliary qubit $|y\rangle$ ensures that **U_f is a unitary!**

Proof

1. On input $|x\rangle\,|y\rangle\,|0\rangle\,|0\rangle$, first swap the second and fourth registers to get $|x\rangle\,|0\rangle\,|0\rangle\,|y\rangle$.
2. Apply C_{rev} on the 3 first registers to get the state $|x\rangle\,|f(x)\rangle\,|\text{junk}(x)\rangle\,|y\rangle$.
3. For i from 1 to m, apply a **CNOT** gate between the i^{th} wire of the second register and the i^{th} wire of the forth register. We then have the state $|x\rangle\,|f(x)\rangle\,|\text{junk}(x)\rangle\,|y \oplus f(x)\rangle$.
4. Apply $C_{\text{rev}}^{\dagger}$ on the three first registers to get the state $|x\rangle\,|0\rangle\,|0\rangle\,|y \oplus f(x)\rangle$.
5. Swap the second and forth register to get the state $|x\rangle\,|y \oplus f(x)\rangle\,|0\rangle\,|0\rangle$.

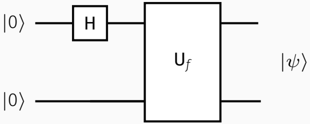


QUANTUM PARALLELISM AND INTERFERENCE

$$\text{Let } f : \{0,1\} \to \{0,1\}$$

$$\mathsf{U}_f : |x\rangle\,|y\rangle \to |x\rangle\,|y \oplus f(x)\rangle$$

Consider the following quantum circuit:

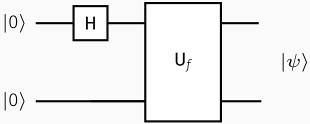


What quantum state is $|\psi\rangle$?

Let $f : \{0, 1\} \to \{0, 1\}$

$$\mathbf{U}_f : |x\rangle\,|y\rangle \to |x\rangle\,|y \oplus f(x)\rangle$$

Consider the following quantum circuit:



What quantum state is $|\psi\rangle$?

1. After the first gate we have: $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle = \frac{|00\rangle+|10\rangle}{\sqrt{2}}$,
2. Applying $\mathbf{U}_f$ leads to (use the linearity):

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

$\longrightarrow$ We have a superposition of the values of f

QUANTUM PARALLELISM: GENERAL CASE

Tensorization of the Hadamard Gate

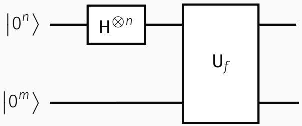
Consider,

$$\mathsf{H}^{\otimes n} \stackrel{\text{def}}{=} \underbrace{\mathsf{H} \otimes \cdots \otimes \mathsf{H}}_{n \text{ times}}$$

Then (see Exercise session 1),

$$\mathsf{H}^{\otimes n} \left|0^n\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \, .$$

The following circuit performs the quantum parallelism (here $f : \{0,1\}^n \to \{0,1\}^m$)



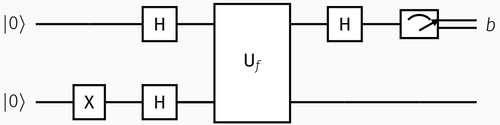
$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x, f(x)\rangle$

Measurement of $\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}} |\mathbf{x}, f(\mathbf{x})\rangle$ gives $f(\mathbf{x})$ for only one value of $\mathbf{x}$...

$\longrightarrow$ Interference is a nice example of how using quantum parallelism!

Remember, the "-1" of the Hadamard gate gives you a huge power...

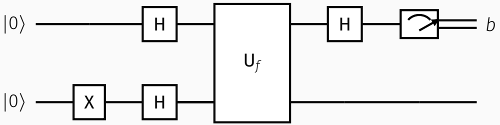
Consider the following circuit (here $f : \{0,1\} \to \{0,1\}$)



What is the value of b?

INTERFERENCE (DEUTSCH'S ALGORITHM)

Consider the following circuit (here $f : \{0,1\} \to \{0,1\}$)



What is the value of b?

1. After applying the **X** and **H** gates: $\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{|00\rangle-|01\rangle+|10\rangle-|11\rangle}{2}$,
2. Applying $\mathbf{U}_f$ leads to (use the linearity):
$$\frac{|0,f(0)\rangle - |0,1\oplus f(0)\rangle + |1,f(1)\rangle - |1,1\oplus f(1)\rangle}{2} = \begin{cases} \pm\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0)=f(1) \\ \pm\frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}} & \text{if } f(0)\neq f(1) \end{cases}$$
3. Applying the last Hadamard gate leads to (use that $\mathbf{H}^2 = \mathrm{I}_2$):
$$\begin{cases} \pm|0\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f(0)=f(1) \\ \pm|1\rangle \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}} & \text{if } f(0)\neq f(1) \end{cases}$$
4. Measuring the first qubit always leads to $f(0)\oplus f(1)$!

$\longrightarrow$ We obtained a global property of f $\left(i.e., f(0)\oplus f(1)\right)$ with **only one evaluation of $f(x)$!**

SIMON’S ALGORITHM

The problem

- **Input:** A function $f : \{0,1\}^n \longrightarrow \{0,1\}^n$.
- **Promise:** $\exists \mathsf{s} \in \{0,1\}^n$: $\Big(f(\mathsf{x}) = f(\mathsf{y}) \iff (\mathsf{x} = \mathsf{y})$ or $(\mathsf{x} = \mathsf{y} \oplus \mathsf{s})\Big)$.
- **Goal:** Find s.

1. Start from the $2n$ qubit state, with 2 registers of n qubits.

$$|\psi_0\rangle = \left|0^n\right\rangle \left|0^n\right\rangle .$$

2. Apply $\mathbf{H}^{\otimes n}$ on the first n qubits to get

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

3. Apply $\mathbf{U}_f$ on the state to get

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathsf{x} \in \{0,1\}^n} |\mathsf{x}\rangle |f(\mathsf{x})\rangle = \frac{1}{\sqrt{\sharp \mathrm{Im}(f)}} \sum_{\mathsf{y} \in \mathrm{Im}(f)} \frac{1}{\sqrt{2}} \left(|\mathsf{x_y}\rangle + |\mathsf{x_y} \oplus \mathsf{s}\rangle\right) |\mathsf{y}\rangle .$$

4. Measure the second register and obtain some value $\mathsf{y} \in \mathrm{Im}(f)$. The resulting state on the first register is

$$|\psi_4(\mathsf{y})\rangle = \frac{1}{\sqrt{2}} \left(|\mathsf{x_y}\rangle + |\mathsf{x_y} \oplus \mathsf{s}\rangle\right) .$$

5. Apply $\mathbf{H}^{\otimes n}$ on the first register to get

$$|\psi_5(\mathsf{y})\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathsf{z} \in \{0,1\}^n} \left(\frac{1}{\sqrt{2}} (-1)^{\mathsf{x_y} \cdot \mathsf{z}} + \frac{1}{\sqrt{2}} (-1)^{(\mathsf{x_y} \oplus \mathsf{s}) \cdot \mathsf{z}} \right) |\mathsf{z}\rangle .$$

5. Apply $\mathsf{H}^{\otimes n}$ on the first register to get

$$|\psi_5(\mathsf{y})\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathsf{z}\in\{0,1\}^n} \left(\frac{1}{\sqrt{2}}(-1)^{\mathsf{x_y}\cdot\mathsf{z}} + \frac{1}{\sqrt{2}}(-1)^{(\mathsf{x_y}\oplus\mathsf{s})\cdot\mathsf{z}} \right) |\mathsf{z}\rangle \, .$$

Now, if $\mathsf{s}\cdot\mathsf{z} = 0$, we have $\left(\frac{1}{\sqrt{2}}(-1)^{\mathsf{x_y}\cdot\mathsf{z}} + \frac{1}{\sqrt{2}}(-1)^{(\mathsf{x_y}\oplus\mathsf{s})\cdot\mathsf{z}} \right) = \sqrt{2}(-1)^{\mathsf{x_y}\cdot\mathsf{z}}$ and if $\mathsf{s}\cdot\mathsf{z} = 1$, we have $\left(\frac{1}{\sqrt{2}}(-1)^{\mathsf{x_y}\cdot\mathsf{z}} + \frac{1}{\sqrt{2}}(-1)^{(\mathsf{x_y}\oplus\mathsf{s})\cdot\mathsf{z}} \right) = 0$. Therefore, we can write

$$|\psi_5(\mathsf{y})\rangle = \sqrt{\frac{2}{2^n}} \sum_{\substack{\mathsf{z}\in\{0,1\}^n \\ \mathsf{s}\cdot\mathsf{z}=0}} (-1)^{\mathsf{x_y}\cdot\mathsf{z}} |\mathsf{z}\rangle \, .$$

6. Measure this state in the computational basis. You get a random z satisfying $\mathsf{z}\cdot\mathsf{s} = 0$.

This algorithm gives $(z_1, \ldots, z_n)$ s.t $\sum_{i=1}^{n} z_i s_i = 0$.

We repeat the algorithm m times to get m random values $\mathbf{z}^1, \ldots, \mathbf{z}^m$ satisfying $\mathbf{z}^k \cdot \mathbf{s} = 0$

We obtain the following system ($\mathbf{s}$ is the unknown): $\mathbf{Z}\mathbf{s} = \mathbf{0}$ where $\mathbf{Z} \stackrel{\text{def}}{=} \left(z_i^j\right)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$.

$\longrightarrow$ If $\mathbf{Z}$ has rank n, we perform a Gaussian elimination to recover $\mathbf{s}$!

It will be verified with high probability if m large enough, $m = Cn$ for some constant $C > 0$.

- We have solved Simon's problem in polynomial time with high probability with **only $O(n)$ queries to f** (*i.e.*, $O(n)$ calls to $\mathbf{U}_f$, step 3)

$\longrightarrow$ Is it doable classically?

- Simon has proved that any classical randomized algorithm that finds $\mathbf{s}$ with high probability needs **to make $\geq C\sqrt{2^n}$ queries to f** where C constant

$\longrightarrow$ **Quantum computing provides an exponential advantage!**

There are many results about the query complexity of quantum algorithm

- *Ronald de Wolf's lecture notes, Chapters* 11-12.

`https://arxiv.org/pdf/1907.09415.pdf`

CONCLUSION

- We have solved Simon's problem in polynomial time with high probability with **only $O(n)$ queries to f** (*i.e.*, $O(n)$ calls to $\mathbf{U}_f$, step 3)

$\longrightarrow$ Is it doable classically?

- Simon has proved that any classical randomized algorithm that finds **s** with high probability needs **to make $\geq C\sqrt{2^n}$ queries to f** where C constant

$\longrightarrow$ **Quantum computing provides an exponential advantage!**

There are many results about the query complexity of quantum algorithm

- *Ronald de Wolf's lecture notes, Chapters* 11-12.

https://arxiv.org/pdf/1907.09415.pdf

But one may say that solving Simon's problem is useless...

Simon's algorithm has been "the starting point" of Shor's algorithm that quantumly breaks all current deployed public key cryptography

$\longrightarrow$ Come at Lecture 6!

EXERCISE SESSION