Quantum programming and algorithms

Master of Computer Science, Minerve and ATHENA

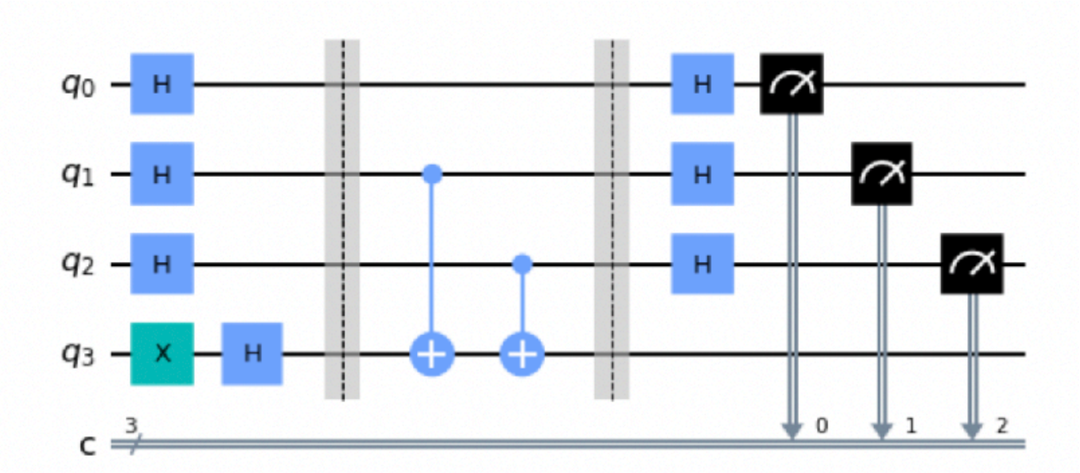
Nicolas Ollinger, Ioan Todinca

2025-2026

Discover quantum computing through the programming of quantum circuits

Différences between quantum/classical algorithms

- qubit, quantum gates, quantum circuits vs. bit, logic gates, Boolean circuits
- quantum specificities (peculiarities?): superposition, interference, entanglement, etc.
- programming elements in Qiskit (Python notebook)



Cultural aspects: promises and challenges of quantum computing

Practical work to be carried out on a computer, in Qiskit

Plan

1. Promises and challenges of quantum computing
2. Quantum computing: differences from the classical model
3. Qubit, quantum gates, quantum circuits. Mathematical basics.
4. Superposition. Entanglement. ‘Destructive’ interference
5. The Bernstein-Vazirani problem and its quantum algorithm
6. Grover's algorithm: Polynomial acceleration but... it would be one of the most useful algorithms in practice
7. Impact of quantum computing on today's and tomorrow's computing
8. Conclusion and recommended reading

1. Promises and challenges of quantum computing

- In the early 1980s, several scientists questioned the use of quantum processes for computing.
- Richard Feynman (Nobel Prize winner in physics, famous for his research but also for his teaching), 'Simulating physics with computers.' International Journal of Theoretical Physics, 1981:
  'Can you do it with a new kind of computer — a quantum computer? Now it turns out, as far as I can tell, that you can simulate this with a quantum system, with quantum computer elements. It's not a Turing machine, but a machine of a different kind.'
- David Deutsch. 'Quantum theory, the Church–Turing principle and the universal quantum computer", 1985.
  Formalises the concept of the quantum computer and raises the question of advantages in terms of computing speed (quantum versus classical complexity). First surprising algorithms.

1. Promises and challenges of quantum computing

Quantum computer: computes the same things as a classical computer, while potentially being more efficient (time complexity) for certain calculations.
1992-1997

- E. Bernstein et U. Vazirani. (Polynomial) speed-up for a specific problem... see next.
- L. Grover. Search for a value among N in time $O(\sqrt{N})$ — classical algorithms need $\Theta(N)$ time.
- D. Simons. **Exponential speed-up** for another problem: compute the period s of a function $f : \{0,1\}^n \to \{0,1\}^n$ such that $\forall x \neq y, f(x) = f(y) \Rightarrow x \oplus y = s$. The problem is artificial, but...
- P. Shor uses some ideas to décomposé a given N in prime factors, in poly time with respect to $\log N$. Computes the order r of a number a, i.e., the minimum r s.t. $a^r \equiv 1 \bmod N$.
  We do not know how to do this today with a conventional computer. If it were doable, many cryptographic protocols would become easy to break.

If we had quantum computers...

Some calculations would be done exponentially faster than on conventional machines (but no, we would not solve NP-hard problems in poly time). The cryptography of credit cards and other devices would have to be completely redesigned!

Quantum communication and cryptography: the most advanced field (but we won't talk about it much).

Is this doable ?

- S. Haroche, J.-M. Raimond. Quantum computing: dream or nightmare? Physics Today, 49(8):51–54, 1996. Decoherence, errors inherent in quantum phenomena. Quantum computer: “The computer scientist’s dream [but] the experimenter’s nightmare.”
- P. Shor (the same): quantum error-correcting codes. In theory, we can move forward.
- In practice? Shor's algorithm was implemented in 2021 to factor the number 21. Apparently, it gave 3×7. No imminent threat to cryptography...
- Announcements of ‘quantum supremacy’ for specific problems... Debatable.
- Let's stay calm, the future will tell. There are many obstacles to overcome. But it's worth looking into!

NISQ : Noisy Intermediate-Scale Quantum

The current state of quantum computing

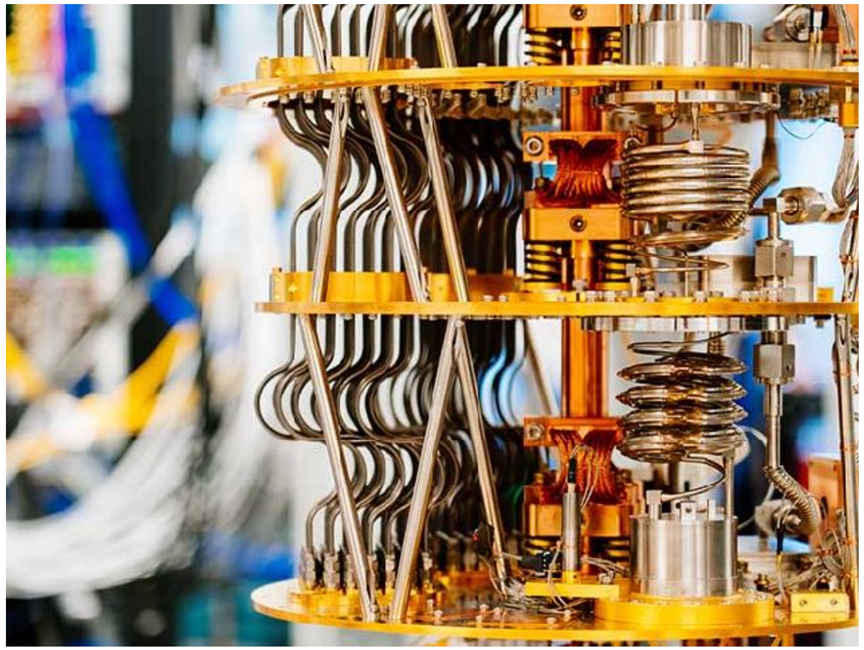


Image Google, Quantum AI Lab, Santa Barbara, USA

- Intermediate-scale: a few dozen qubits
- Noisy: no error correction
- Sycamore (Google), 53 qubits aligned along a 2D grid. The entanglement of a subit is possible with its neighbours in the grid. Circuits with dozens of gates, with measurement at the end.
- Heron (IBM), 156 qubits, 2D grid
- Pasqual: completely different quantum processor, based on ‘quantum annealing’

Some companies, in France and worldwide

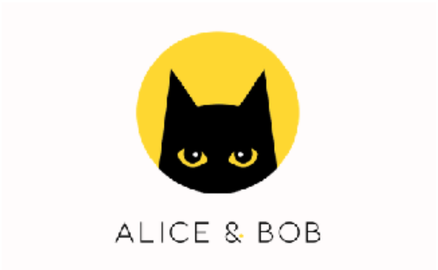
France : strong compétences in physics (S. Haroche, A Aspect and students)

PASQAL

IBM

QUANDELA

Google



D:wave
The Quantum Computing Company™

C12

QILIMANJARO
QUANTUM · TECH

IQuEra
COMPUTING INC.

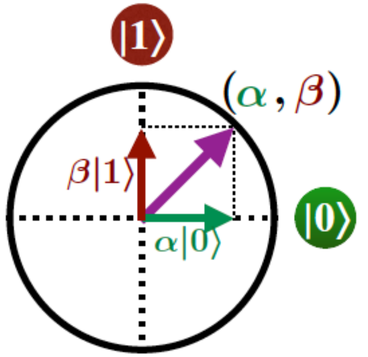
EVIDEN

emulation

parityqc

2. Quantum computing — qubit, superposition

Here: computation with quantum circuits. The model is universal. as It's not the only universal quantum comptine model, see e.g., the PhD thesis of Arthur Braida (U. Orléans-LIFO/Atos-Eviden) on **quantum annealing**.



[F. Magniez, exposé Collège de France]

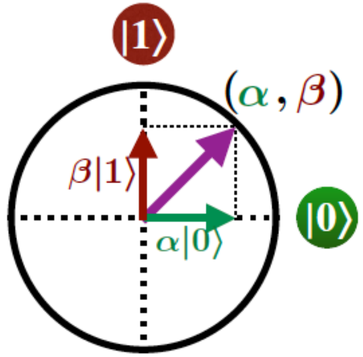
- qubit: **superposition** of $|0\rangle$ and $|1\rangle$. It's a 2-dimensional vector!
  $\alpha|0\rangle + \beta|1\rangle \quad$ with $\quad \alpha, \beta \in \mathbb{C} \quad$ such that $\quad |\alpha|^2 + |\beta|^2 = 1$
- **Superposition** is a quantum phenomenon systematically exploited in quantum algorithms, through quantum states such as

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ or } \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

2. Quantum computing — qubit, measurement

$$\alpha\,|\mathbf{0}\rangle + \beta\,|\mathbf{1}\rangle \xrightarrow{|\alpha|^2} |\mathbf{0}\rangle \ \textit{on mesure}\ \mathbf{0}$$

$$\alpha\,|\mathbf{0}\rangle + \beta\,|\mathbf{1}\rangle \xrightarrow{|\beta|^2} |\mathbf{1}\rangle \ \textit{on mesure}\ \mathbf{1}$$



The **measurement** of a qubit will output 0 or 1 with the above probabilités.

Exercise. Describe the possible outputs after measuring the following qubits, with their respective probabilités:

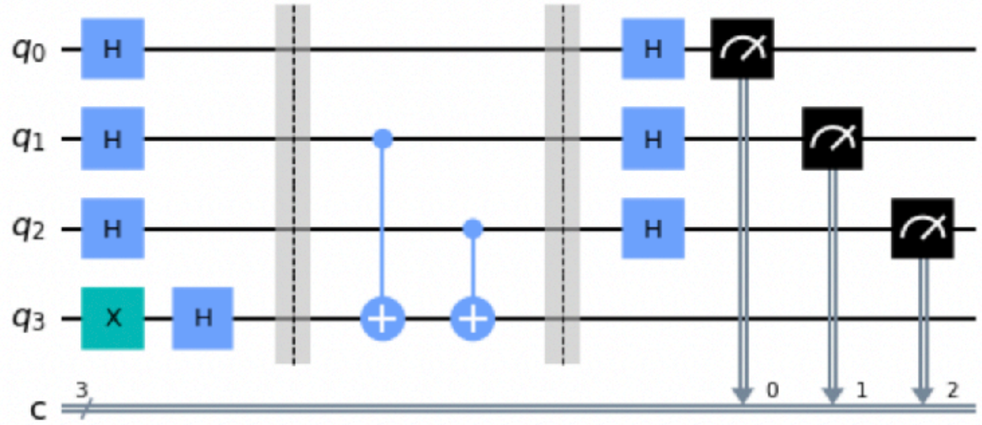
a. $|0\rangle$ b. $|1\rangle$ c. $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ d. $\dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

2. Quantum computing — circuits, gates

Register of n qubits, initially all set to $|0\rangle$. This gives $N = 2^n$ possibilities, after measurement.

Gates : transformations $U : \mathbb{C}^{\{0,1\}^n} \to \mathbb{C}^{\{0,1\}^n}$, unitaires, i.e. preservation of the norm + linearity: $U\left(\alpha|\varphi\rangle + \beta|\psi\rangle\right) = \alpha U|\varphi\rangle + \beta U|\psi\rangle$

- sequential composition: matrix product
- parallel composition: tensor product
  $|x\rangle \otimes |y\rangle = |xy\rangle$



N.B. Matrices of size 2^n with complex coefficients. By linearity, **it suffices to know the behaviour for each boolean bitstring $|x\rangle = |x_1 x_2 \ldots x_n\rangle$, with boolean x_i.**

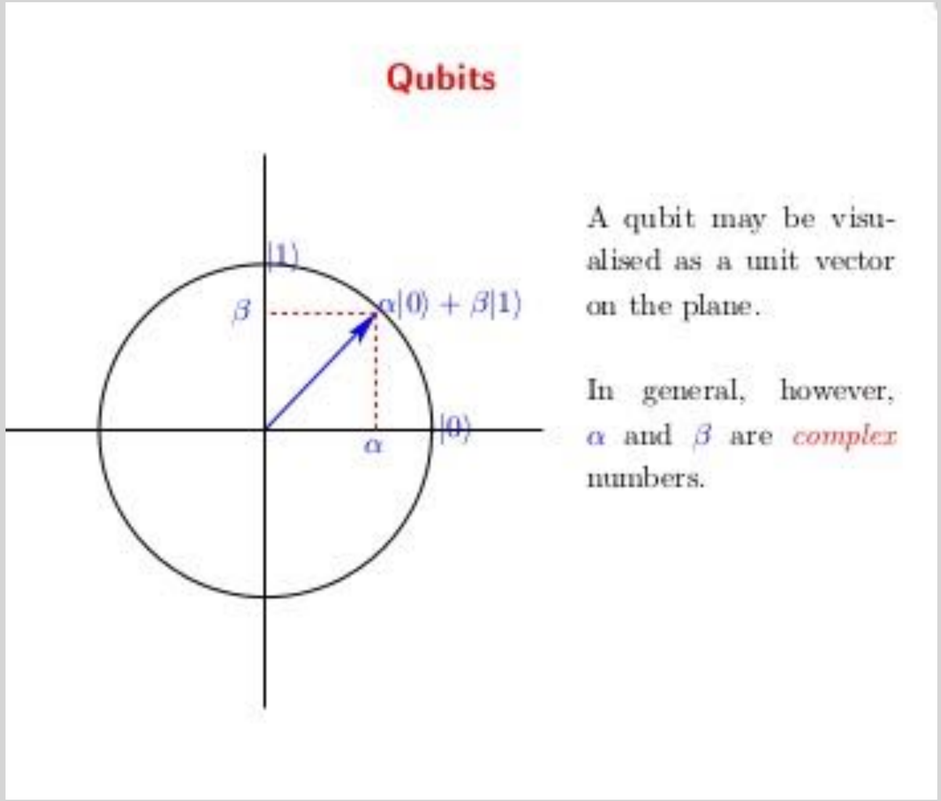
Mathematical background and Dirac's notation

"Complicated but not difficult"; not exactly intuitive…

An n-qubits register corresponds to a vector of dimension $N = 2^n$, with complex coefficients, of norm 1.

One qubit : $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$

Example: $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}} = \begin{bmatrix} \dfrac{1}{\sqrt{2}} \\ \dfrac{1}{\sqrt{2}} \end{bmatrix}$



quora.com

More qubits — Dirac's notation

(or bra-ket)

Parallel composition: tensor product.

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ 0 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

States of the form $|x\rangle = |x_1 x_2 \ldots x_n\rangle$ with $x_i \in \{0,1\}$ provide a basis for the vector space. Any other states can be written as

$$|\varphi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle, \text{ with } \alpha_x \in \mathbb{C} \text{ and } \sqrt{\sum_{x \in \{0,1\}^n} |\alpha_x|^2} = 1$$

Produit tensoriel $A \otimes B$ de deux matrices de taille $m \times n$ et $p \times q$: une matrice de taille $mp \times nq$

$$A \otimes B = \begin{bmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{bmatrix}$$

Dirac's notation — continued

$$|\varphi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$$

Example (Bell state) :

$$\frac{|00\rangle - |11\rangle}{\sqrt{2}} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix}$$

$$|00\ldots00\rangle \iff \left.\begin{pmatrix}1\\0\\0\\\vdots\\0\\0\end{pmatrix}\right\} 2^n, \quad |00\ldots01\rangle \iff \begin{pmatrix}0\\1\\0\\\vdots\\0\\0\end{pmatrix}, \quad \cdots$$

$$\cdots \quad , \quad |11\ldots10\rangle \iff \begin{pmatrix}0\\0\\0\\\vdots\\1\\0\end{pmatrix}, \quad |11\ldots11\rangle \iff \begin{pmatrix}0\\0\\0\\\vdots\\0\\1\end{pmatrix}.$$

An Introduction to Quantum Computing, P. Kaye, R. Laflamme, M. Mosca

Gates. Sequence: matrix product

X

(NOT gate)

$|0\rangle \mapsto |1\rangle$

$|1\rangle \mapsto |0\rangle$

Matrix :

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

H

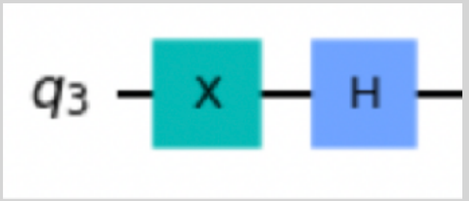
(Hadamard)

$$|0\rangle \mapsto \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

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

Matrix :

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

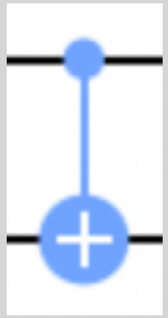


$$H(X|0\rangle) = H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

Gates — more qubits

sequential composition: matrix product



$|xy\rangle \mapsto |x\rangle|x \oplus y\rangle$

CX

(Controlled-NOT)

$|00\rangle \mapsto |00\rangle$

$|01\rangle \mapsto |01\rangle$

$|10\rangle \mapsto |11\rangle$

$|11\rangle \mapsto |10\rangle$

Matrix:

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

Heron

Quantum volume: 512

At 156 qubits, Heron is an Eagle-sized upgrade to Egret that pulls in substantial innovations in signal delivery that were previously deployed in Osprey. The signals required to enable the fast, high-fidelity two-qubit and single-qubit control are delivered with high-density flex cabling.

- View available Heron processors ↗
- Native gates and operations: `cz, id, delay, measure, reset, rz, sx, x, if_else, for_loop, switch_case`

Revisions

`r2` (July 2024) This is a revision of the original Heron processor. The chip has been redesigned to include 156 qubits in a heavy-hexagonal lattice. While continuing to make use of the innovations of the original Heron processors, it also introduces a new TLS mitigation feature that controls the TLS environment of the chip, thereby improving coherence and stability across the whole chip.

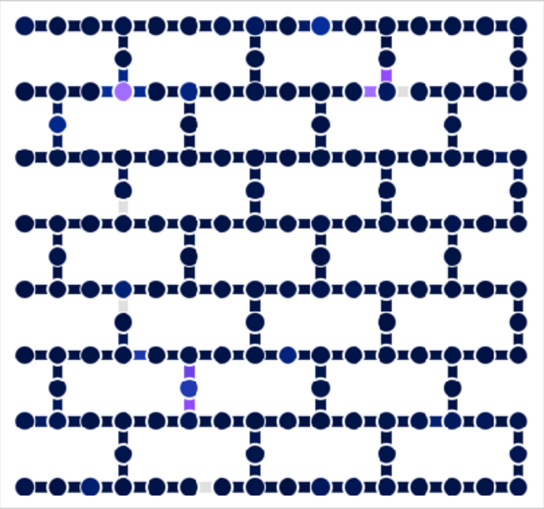
IBM (2024)

Supraconducting qubits, microwave-impulsions gates

Small set of quantum gates!

- 2 qubits : CZ ($|11\rangle \mapsto -|11\rangle$, the others stay identical autres inchangés)
- 1 qubit: X, SX, RZ

Connectivity:

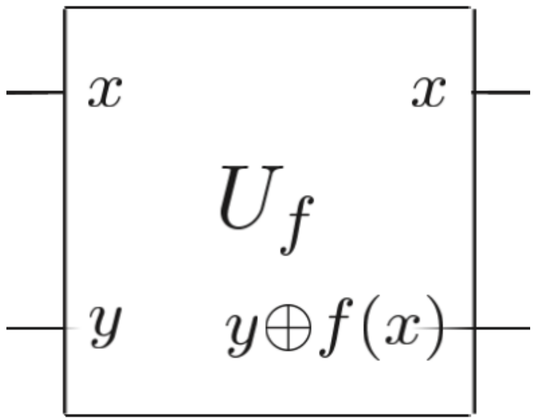


https://quantum.cloud.ibm.com/computers?processorType=Heron&system=ibm_pittsburgh

2. From classical to quantum computing (compatibilité)

Every classical computation of a boolean function $f : \{0,1\}^n \to \{0,1\}^m$ can be simulated by a quantum circuit U_f of similar size, on $n + m$ qubits, such that

$$|x, y\rangle \mapsto |x, y \oplus f(x)\rangle$$



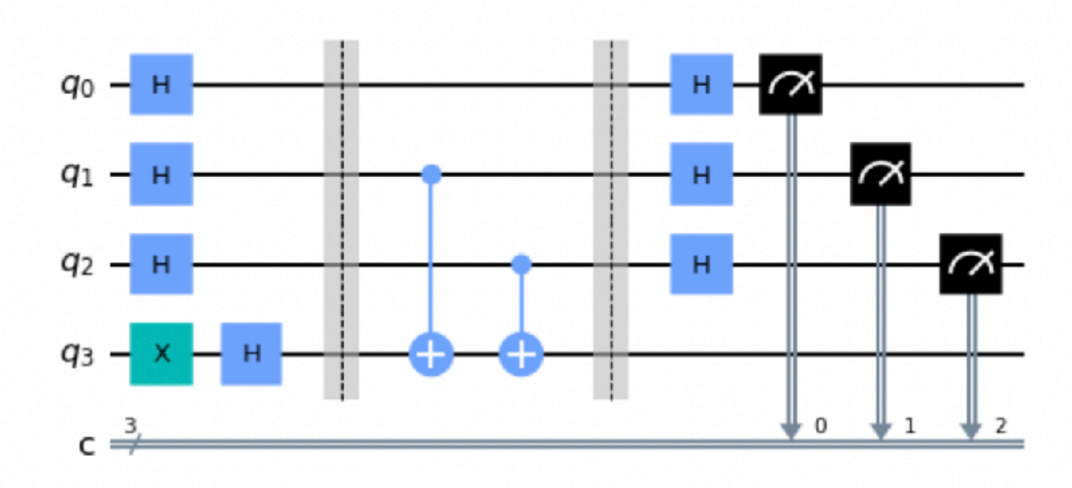
(A bit informal, some uniformity requirements hidden under the carpet.)

N.B. This boils down to programming with very basic tools, by explicitely constructing the circuit...

2. Quantum computing — "parallelism"

Most **quantum algorithms** work on the following principle:

- create a relevant superposition of qubits from $|00\ldots0\rangle$
- perform a classical calculation **in parallel** on the superposition of inputs;
- perform a relevant **quantum transformation**;
- observe the result using **measurements**.

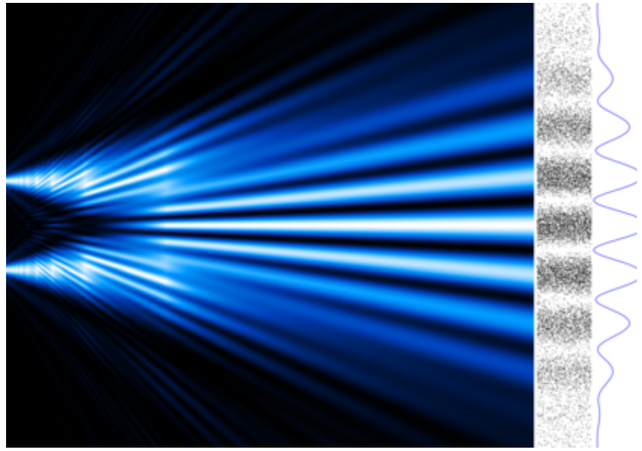


Exercise.

Recall the states $H|0\rangle$ and $H|1\rangle$. Prove that $H^{\otimes n}|00\cdots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$

2. Quantum computing — interference

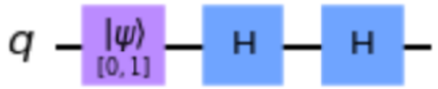
in particular, destructive interférences



Fentes de Young - Wikipedia

Interference: a combination of two waves.
See Young's double-slit experiment:
“constructive” and “destructive”
interference.

Exercise. Analyse the result of two consecutive H gates: compute $H(H|0\rangle)$ and $H(H|1\rangle)$.

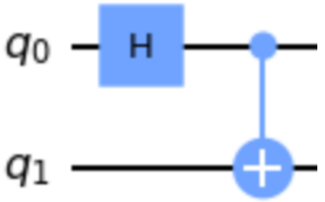


2. Quantum entanglement

in French: « intrication » or « enchevêtrement »

Bell state: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$

A circuit producing this state:



- Any of the two qubits has a probability $\frac{1}{2}$ to be measured 0, same for 1.
- Assume that we have measured the first qubit, obtaining 0. What happens if we measure the 2nd qubit? Conclude that the properties of the two qubits are correlated.

Disturbing, because we can separate the two qubits far apart, and they remain entangled... Einstein called this a “spooky action at a distance”.
Bohr - Einstein controversy; Nobel prize 2022 J. Clauser, **Alain Aspect**, and A. Zeiliger.

3. Bernstein-Vazirani problem/algorithm

Quite surprising (quantum advantage), yet (relatively) easy to understand

The problem

- Input: a function $f : \{0,1\}^n \to \{0,1\}$, as a circuit
- Promise: there exists $s \in \{0,1\}^n$ such that $f(x) = x \cdot s$
- Output: find s

Exercise.

Propose a classical algorithm to solve the problem. How many calls to f do you need?

Reminder: given $x = x_1 x_2 \cdots x_n$ and $s = s_1 s_2 \cdots s_n$ we denote by $x \cdot s$ their scalar product:

$$x \cdot s = x_1 \cdot s_1 \oplus x_2 \cdot s_2 \oplus \cdots \oplus x_n \cdot s_n$$

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \cdot \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} \to XOR \left(\begin{bmatrix} x_1 \cdot s_1 \\ x_2 \cdot s_2 \\ x_3 \cdot s_3 \\ x_4 \cdot s_4 \end{bmatrix} \right)$$

3. Bernstein-Vazirani problem/algorithm

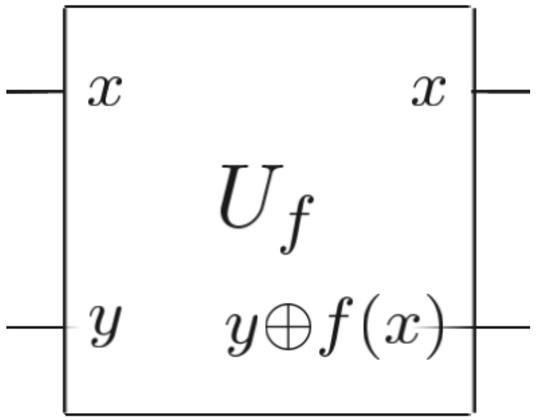
Quantum algorithm: a unique call to f

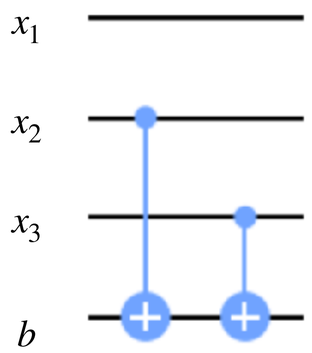
$f(x) = x \cdot s$ for some « hidden » $s \in \{0,1\}^n$

1. **Construct first** $U_f : |xb\rangle \rightarrow |x\rangle |b \oplus f(x)\rangle$
2. Replace b with $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$. We obtain:

$$U_f : |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \rightarrow (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

3. Apply H gates on the first n qubits, at the very beginning. What do we obtain, without measuring?
4. Apply H gates on the first n qubits, at the very end. Measure them and show that we obtain precisely s.





$s = 011$

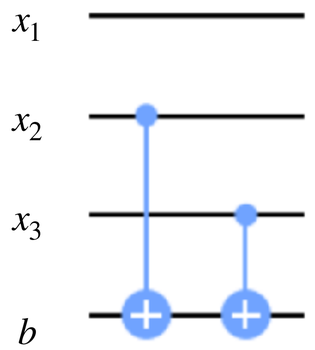
3. Bernstein-Vazirani problem/algorithm

$f(x) = x \cdot s$ for some « hidden » $s \in \{0,1\}^n$

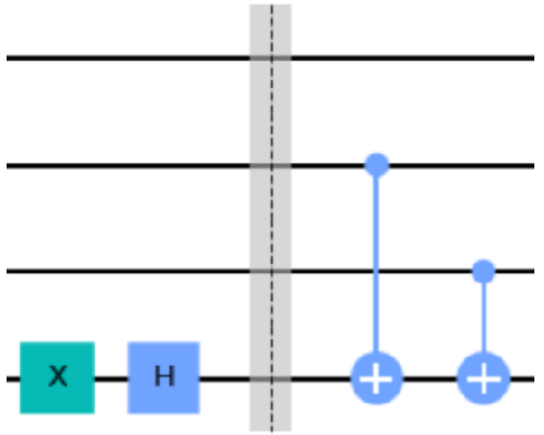
1. Construct first $U_f : |xb\rangle \rightarrow |x\rangle\,|b \oplus f(x)\rangle$
2. **Replace b with $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$.** We obtain:

$$U_f : |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \rightarrow (-1)^{f(x)}\,|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

3. Apply H gates on the first n qubits, at the very beginning. What do we obtain, without measuring?
4. Apply H gates on the first n qubits, at the very end. Measure them and show that we obtain precisely s.



$s = 011$



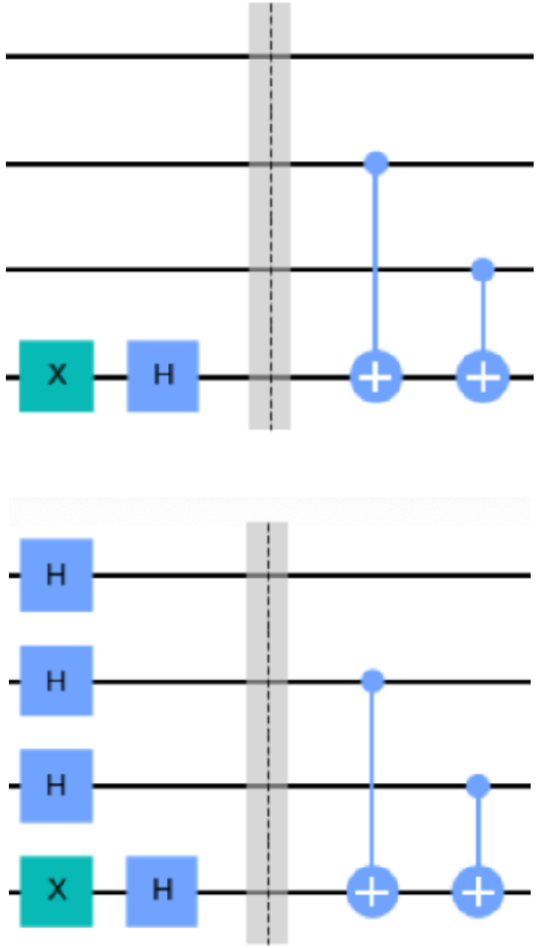
3. Bernstein-Vazirani problem/algorithm

$f(x) = x \cdot s$ for some « hidden » $s \in \{0,1\}^n$

1. Construct first $U_f : |xb\rangle \rightarrow |x\rangle\,|b \oplus f(x)\rangle$
2. Replace b with $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$. We obtain:

$$U_f : |x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \rightarrow (-1)^{f(x)}|x\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

3. **Apply H gates on the first n qubits, at the very beginning. What do we obtain, without measuring?**
4. Apply H gates on the first n qubits, at the very end. Measure them and show that we obtain precisely s.



3. Bernstein-Vazirani problem/algorithm

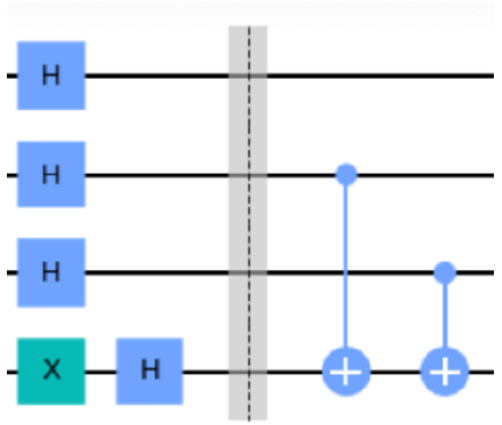
$f(x) = x \cdot s$ for some « hidden » $s \in \{0,1\}^n$

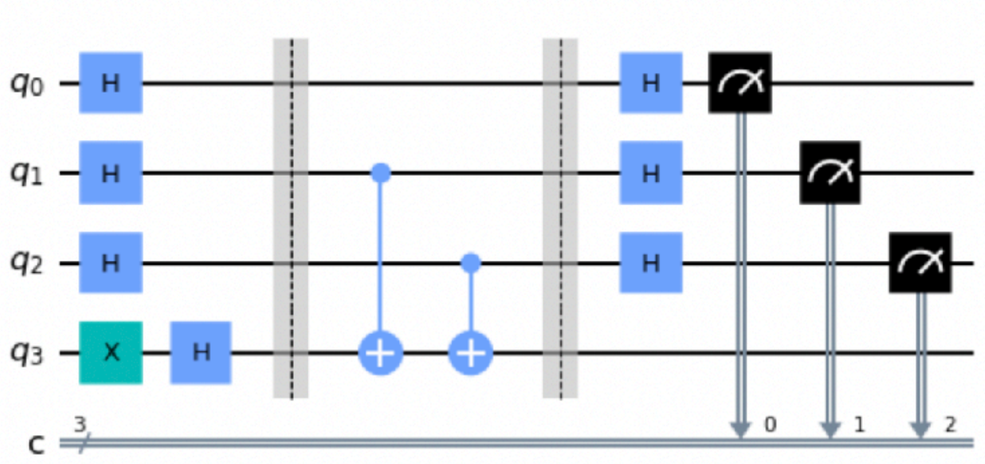
1. Construct first $U_f : |xb\rangle \rightarrow |x\rangle |b \oplus f(x)\rangle$
2. Replace b with $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$. We obtain:

$$U_f : |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \rightarrow (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

3. Apply H gates on the first n qubits, at the very beginning. What do we obtain, without measuring?
4. **Apply H gates on the first n qubits, at the very end. Measure them and show that we obtain precisely s.**

The output is s, with probability 1!





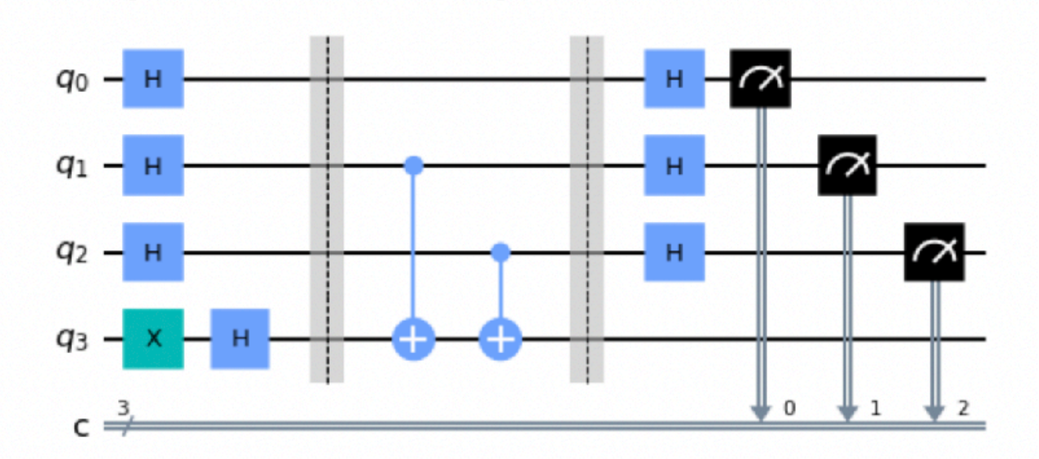
Mesure : 011

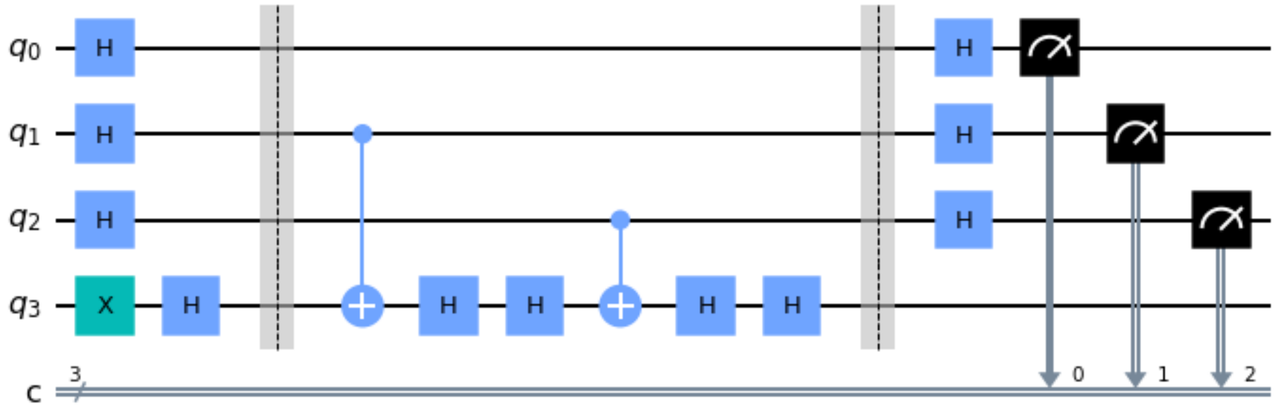
3. Proof of the Bernstein-Vazirani algorithm

An almost combinatorial proof, no heavy calculations

Lemma 1:

≡ Identité

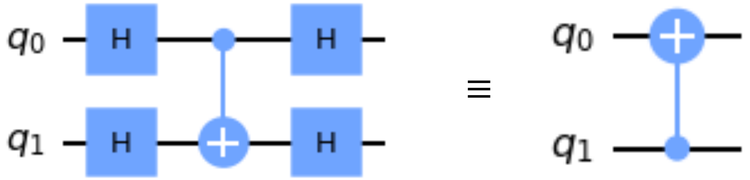


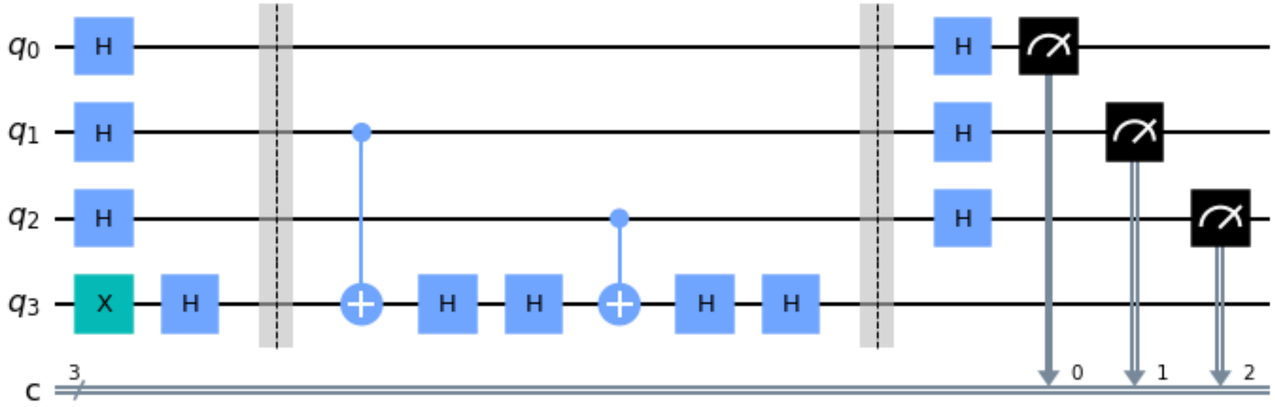


3. Proof of the Bernstein-Vazirani algorithm

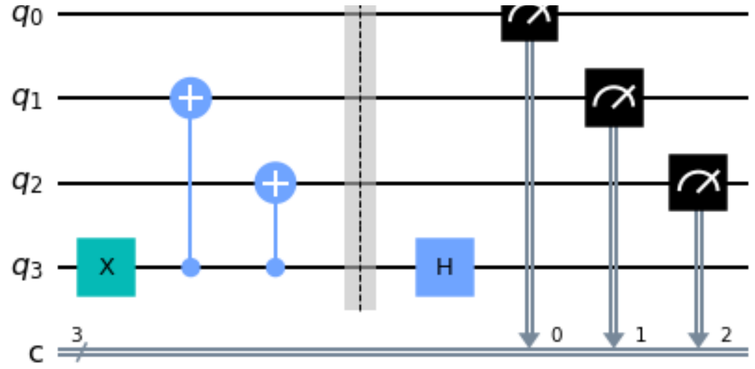
An almost combinatorial proof, no heavy calculations

Lemma 2:





At the end, the circuit acts as if we reversed all CNOT gates, knowing that the last qubit is set to $|1\rangle$



Sortie : 011

4. Grover's algorithm

The problem. We are given a function $f : \{0,1\}^n \to \{0,1\}$, as a black box (circuit). We aim to find, if it exists, a vector $x \in \{0,1\}^n$ such that $f(x) = 1$.

Grover's algorithm (1996) solves the problem in time $O(\sqrt{2^n})$ while any classical algorithm requires $\Omega(2^n)$ time.

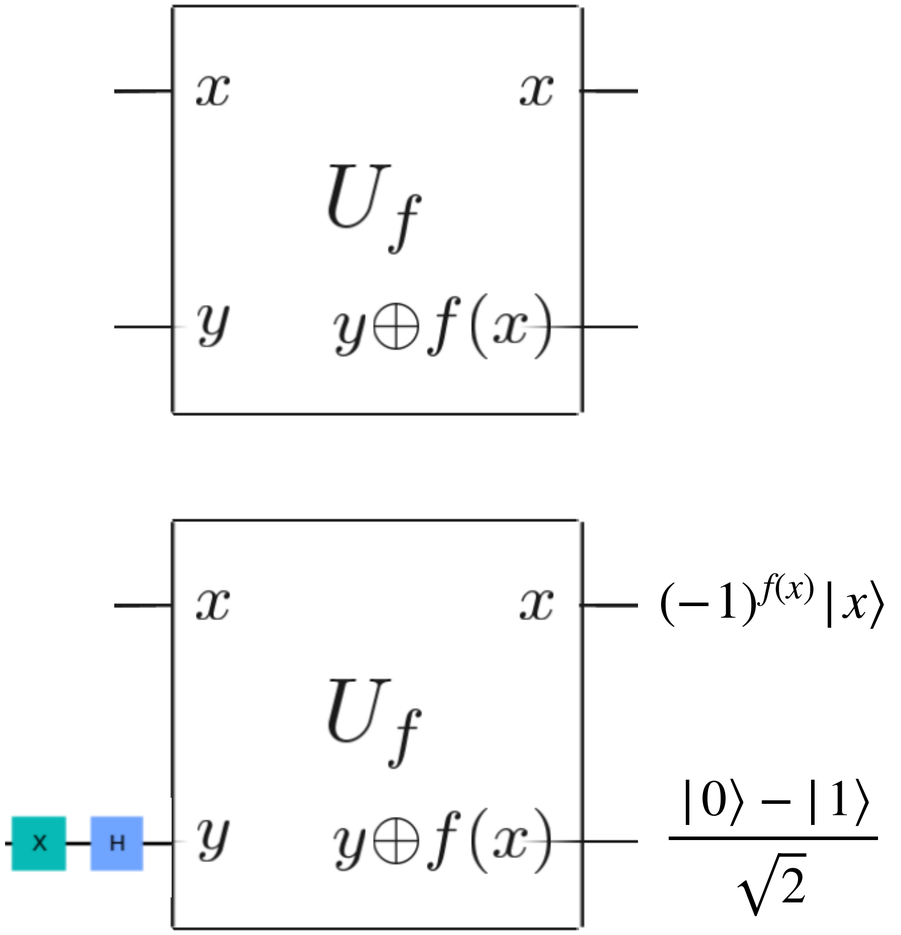
It is a probabilistic algorithm: it finds the solution with a probability of at least $2/3$.

Standard amplification techniques can bring it as close to 1 as desired.

SAT (satisfiability) problem, in classical terms: even if f is a known Boolean function, we cannot do better than, roughly, 2^n time, under some complexity assumptions.

Grover would be one of the most useful algorithms, providing a (polynomial) speed-up for many classical algorithms. More details during the last lecture.

4. Grover's algorithm - basic tools

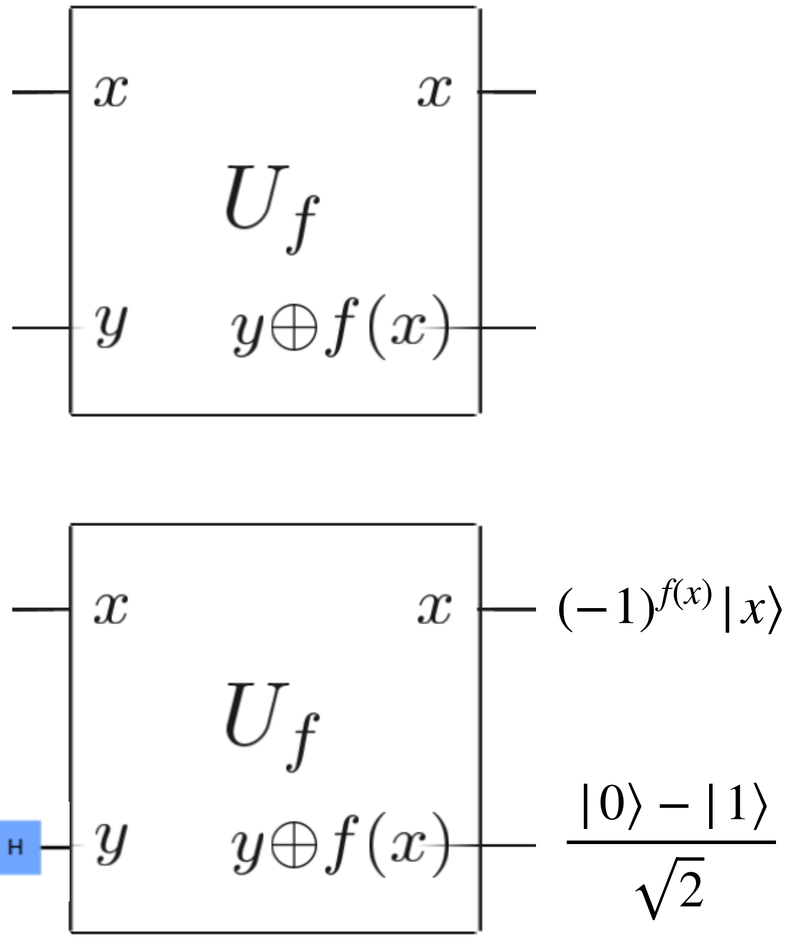


Oracle Z_f

Reminder from previous lectures

- For any boolean function f, we can build $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$
- We denote $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- **By setting $y = |-\rangle$, we obtain as output $(-1)^{f(x)}|x\rangle|-\rangle$**
- **This new circuit is denoted Z_f.**

4. Grover's algorithm - basic tools



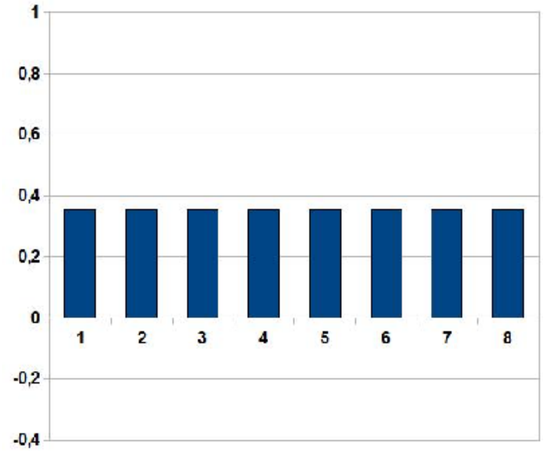
Oracle Z_f

Simplifying hypothesis. Assume that our function $f : \{0,1\}^n \to \{0,1\}$ is such that there exists a unique x_1 satisfying $f(x_1) = 1$.

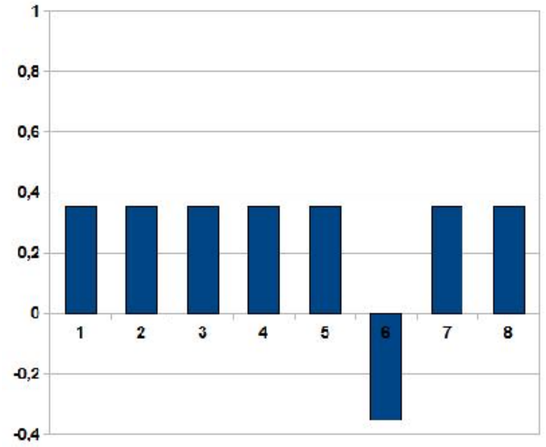
(We'll eventually solve the general case, don't worry.)

Exercise. What is the state of Z_f if we add an H gate on each of the first n input qubits?

4. Algorithme de Grover — première observation



Initial state after the H gates



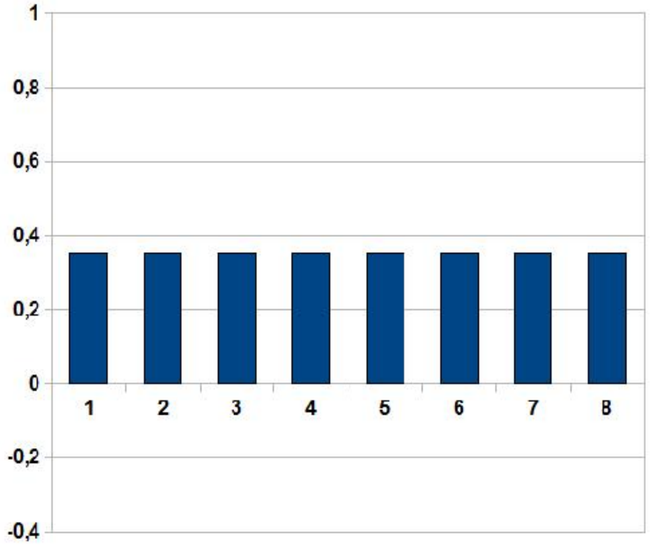
Output

Images : https://fr.wikipedia.org/wiki/Algorithme_de_Grover

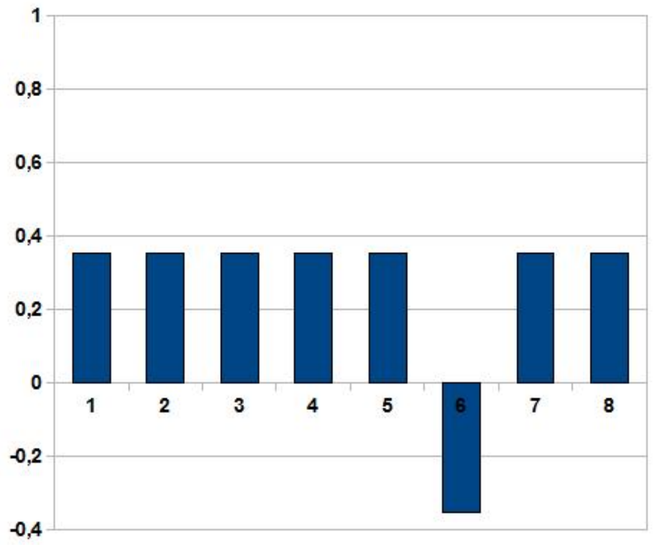
Symplifying hypothesis (reminder). For our function $f : \{0,1\}^n \to \{0,1\}$ there exists a unique x_1 such that $f(x_1) = 1$.

Exercise. What is the state of Z_f if we add an H gate on each of the first n input qubits?

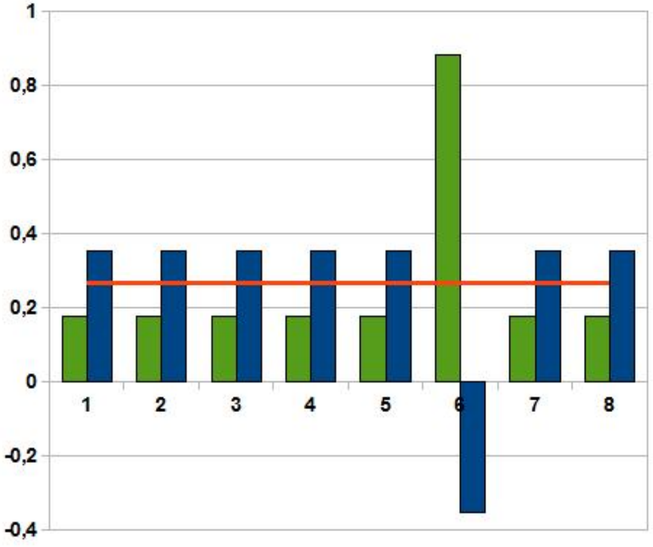
- Up: the state right after the H gates (amplitudes)
- Down: output state, the amplitude of x_1 has changed its sign



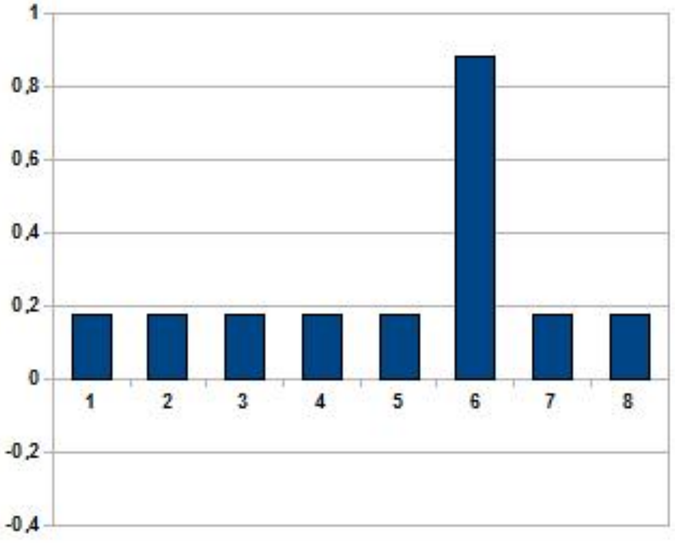
Initial state after the H gates



State after the Z_f circuit



Symmetry around the average

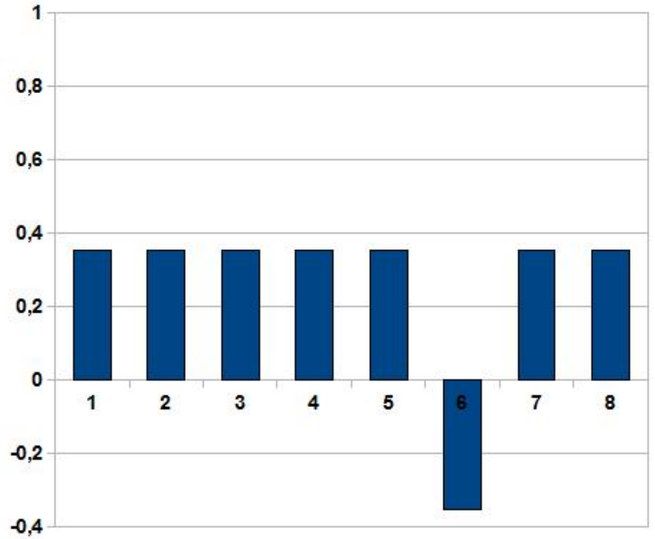


New state after all these steps

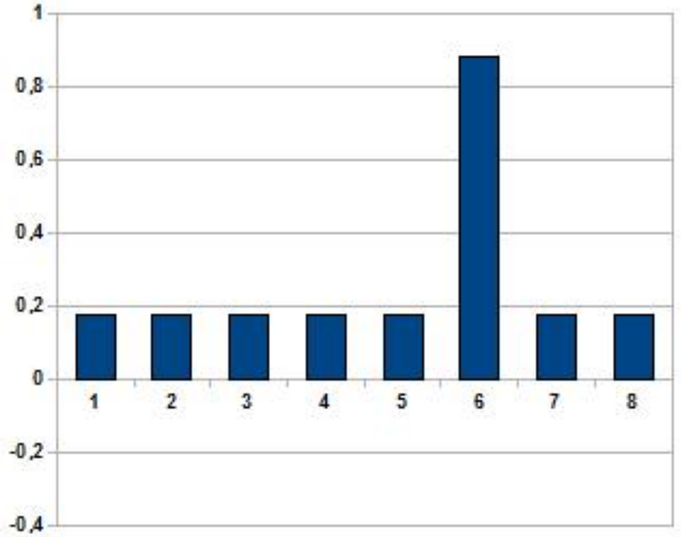
4. Grover's algorithm — symmetry w.r.t this average

Grover's operator

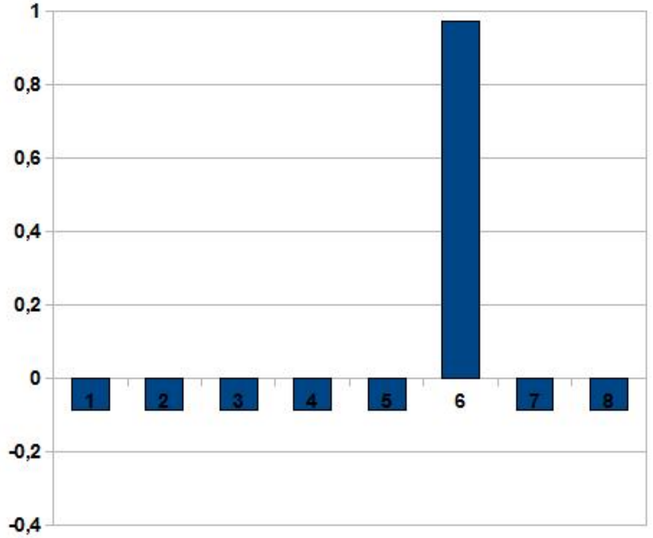
- Intuition: as if we compute the average of the amplitudes, and we apply a symmetry w.r.t this average
- We'll detail the implementation and the proofs



State after H gates and one Z_f



State after one Grover operator



State after two Grover operator

4. Grover's algorithm — repeate

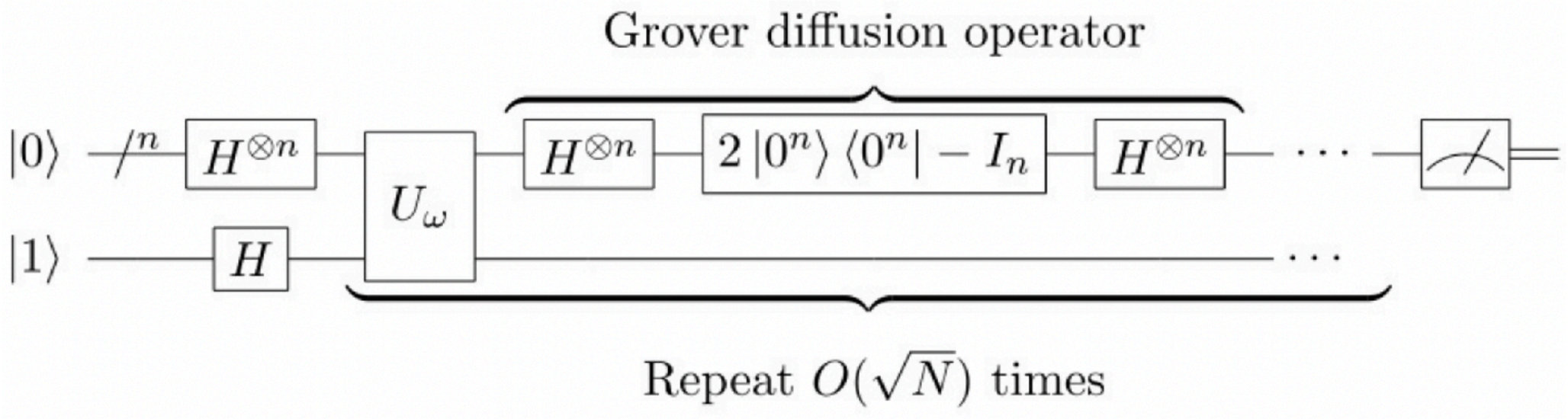
... a well-chose number of times

- In the example we measure x_1 with probability larger than 90 %

We still need to:

- Detail the implementation
- Transform this small example into an actual proof

4. Grover's algorithm



https://fr.wikipedia.org/wiki/Algorithme_de_Grover

General scheme. Here U_ω is just another notation for U_f.

Grover's diffusion operator performs this "mirror around the average". Its implementation is fairly easy:

$$H^{\oplus n} Z_{OR} H^{\oplus n}$$

Would you take some more maths?

"bra" notation and projections

Recall that a state $|\psi\rangle = |a_1 a_2 \ldots a_n\rangle$ represents a vector (1-column matrix).

We denote by $\langle\psi| = \langle a_1 a_2 \ldots a_n|$ its conjugate transpose: the column is turned into a row. For each coordinate a_i we should take its complex conjugate... but since we deal with real numbers only, its conjugate is still a_i.

$\langle 0^n|$ represents $\langle 00\ldots0|$, with n zeros, i.e. the matrix $[10\ldots0]$, with one row and 2^n columns.

The scalar product of vectors $|\phi\rangle$ and $|\psi\rangle$ is also denoted $\langle\varphi|\psi\rangle$; matrix product of $\langle\varphi|$ and $|\psi\rangle$.

Projector operator: $|\psi\rangle\langle\psi|$. It's the sensor product of the two matrices $\langle\psi|$ and $|\psi\rangle$.

The **scalar product** of real vectors $|\phi\rangle$ and $|\psi\rangle$ equals $\langle\varphi| \times |\psi\rangle$, denoted $\langle\varphi|\psi\rangle$.

Projection operator: $|\psi\rangle\langle\psi|$. The tensor product of the two matrices $|\psi\rangle \otimes \langle\psi|$.

Properties of the sensor product :

- $(|\psi\rangle\langle\psi|)|\varphi\rangle = |\psi\rangle(\langle\psi|\varphi\rangle)$ is the projection of vector $|\varphi\rangle$ on $|\psi\rangle$
- Given two matrices A, B of size $N \times N$,

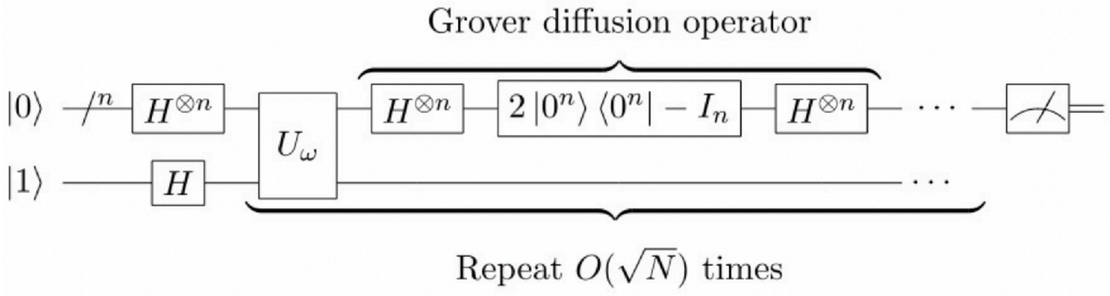
$$A(|\psi\rangle\langle\psi|)B = (A|\psi\rangle) \otimes (\langle\psi|B)$$

Exercise 1. Write the matrix of $|0^n\rangle\langle 0^n|$, then the one of $2|0^n\rangle\langle 0^n| - I_n$.

Exercise 2. Show that $2|0^n\rangle\langle 0^n| - I_n$ corresponds to the circuit Z_{OR} of function OR_n.

Exercise 3. Show that $H^{\oplus n}(2|0^n\rangle\langle 0^n| - I_n)H^{\oplus n} = 2|u\rangle\langle u| - I_n$, where $u = H^{\oplus n}|0^n\rangle$.

4. Grover's algorithm : the proof

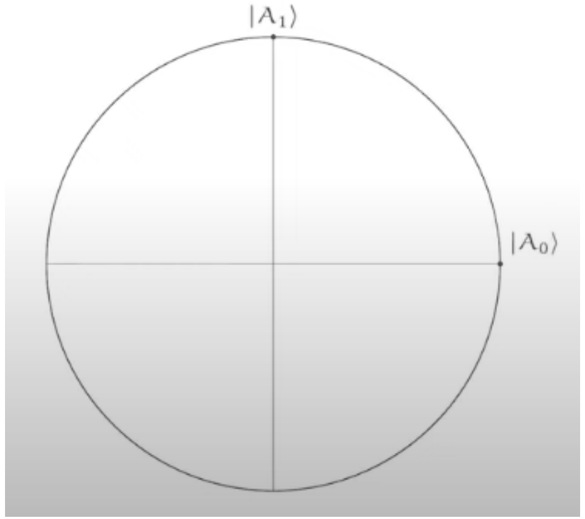


https://fr.wikipedia.org/wiki/Algorithme_de_Grover

We denote $A_1 = \{x_1\}$ and
$A_0 = \{x \in \{0,1\}^n : f(x) = 0\}$

For any set of boolean vectors A of size n let

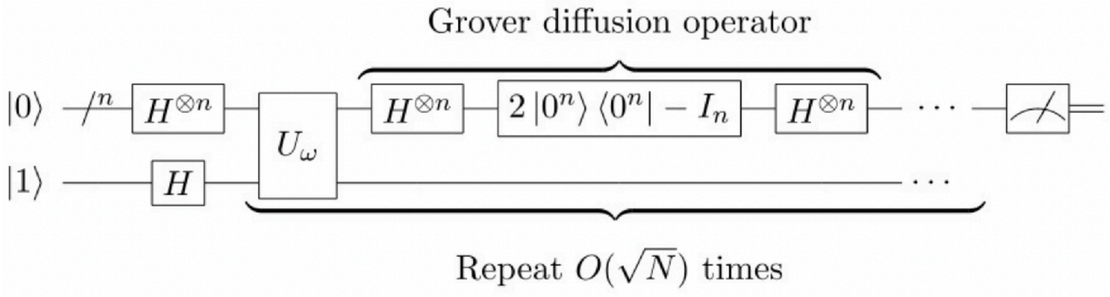
$$|A\rangle = \frac{1}{\sqrt{|A|}} \sum_{x \in A} |x\rangle.$$



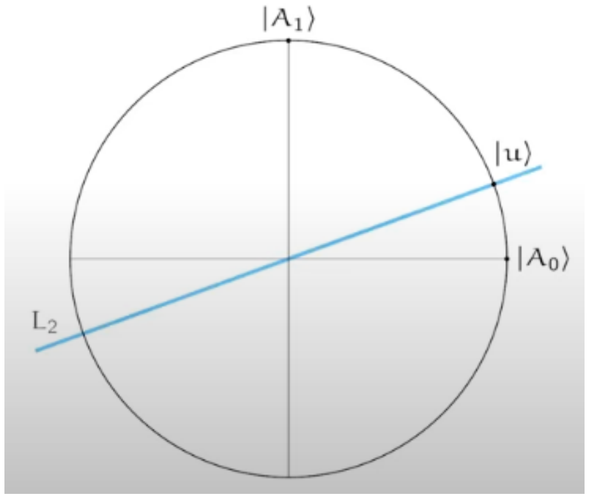
John Watrous, IBM, YouTube video

Observe that vectors $|A_0\rangle$ and $|A_1\rangle$ are orthogonals.

4. Grover's algorithm : the proof



https://fr.wikipedia.org/wiki/Algorithme_de_Grover



John Watrous, IBM

Let $|u\rangle = H^{\otimes n}|0^n\rangle$, the "uniform superposition" vector

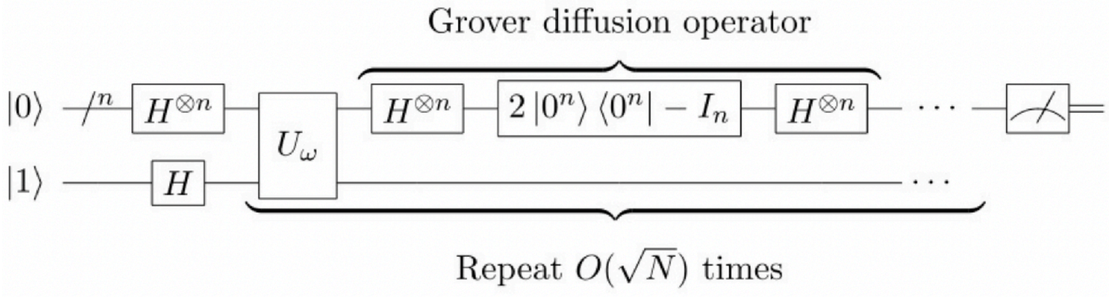
$$|u\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle$$

$$|u\rangle = \frac{1}{\sqrt{N}} \left(\sum_{x_0\in A_0} |x_0\rangle + \sum_{x_1\in A_1} |x_1\rangle \right)$$

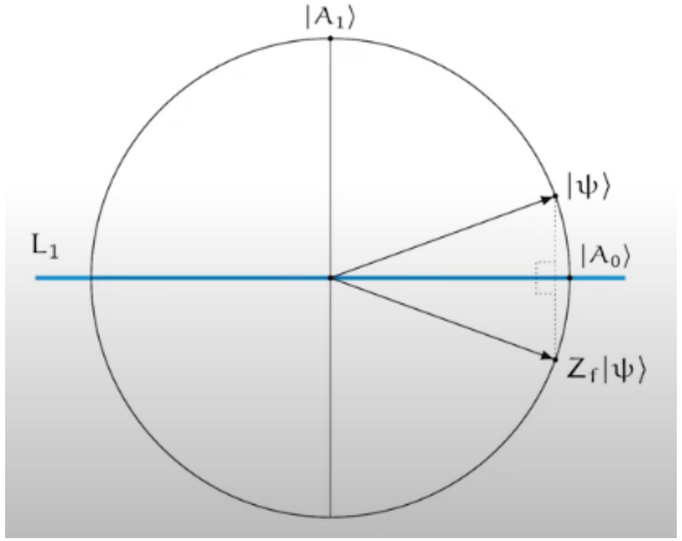
$$|u\rangle = \frac{\sqrt{|A_0|}}{\sqrt{N}} |A_0\rangle + \frac{\sqrt{|A_1|}}{\sqrt{N}} |A_1\rangle$$

$|u\rangle$ is a lainera combination of $|A_0\rangle$ and $|A_1\rangle$

4. Grover's algorithm : the proof



https://fr.wikipedia.org/wiki/Algorithme_de_Grover



John Watrous, IBM

Understanding $Z_f|\psi\rangle$: symmetry around $|A_0\rangle$.

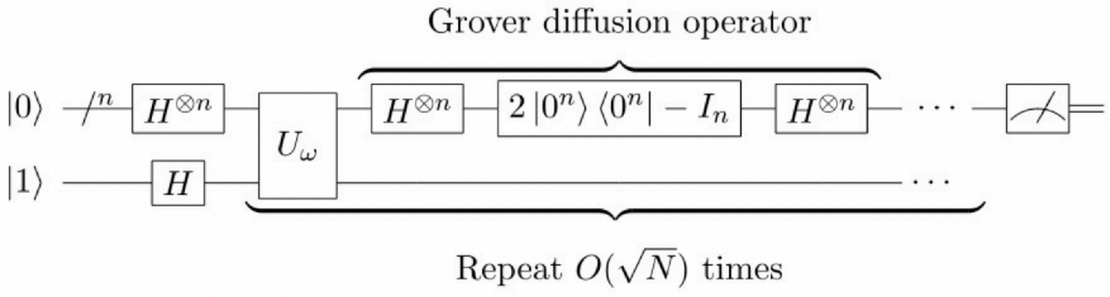
$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$$

$$|\psi\rangle = \sum_{x_0\in A_0} \alpha_{x_0} |x_0\rangle + \sum_{x_1\in A_1} \alpha_{x_1} |x_1\rangle$$

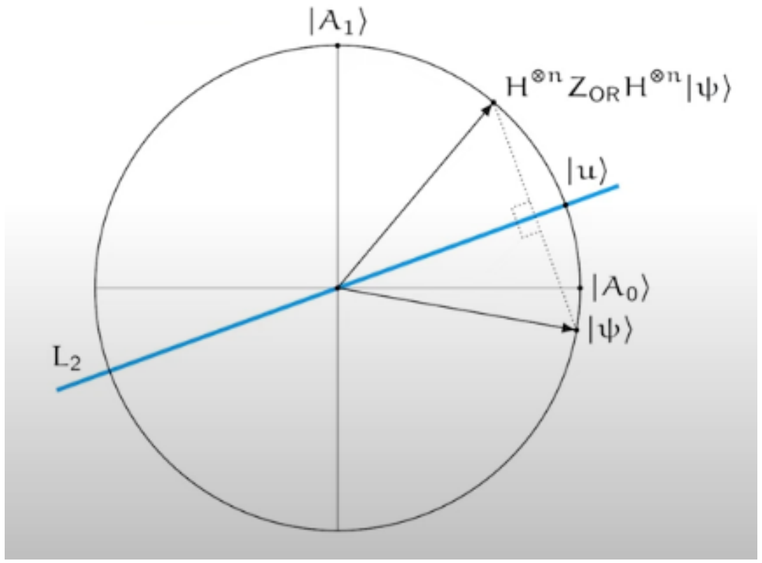
$$Z_f|\psi\rangle = \sum_{x_0\in A_0} \alpha_{x_0}(-1)^{f(x_0)} |x_0\rangle + \sum_{x_1\in A_1} \alpha_{x_1}(-1)^{f(x_1)} |x_1\rangle$$

$$Z_f|\psi\rangle = \sum_{x_0\in A_0} \alpha_{x_0} |x_0\rangle - \sum_{x_1\in A_1} \alpha_{x_1} |x_1\rangle$$

4. Grover's algorithm : the proof



https://fr.wikipedia.org/wiki/Algorithme_de_Grover



John Watrous, IBM

Understanding $H^{\oplus n} Z_{OR} H^{\oplus n} |\psi\rangle$: symmetry around $|u\rangle$.

$$Z_{OR} = 2\,|0^n\rangle\langle 0^n| - I$$

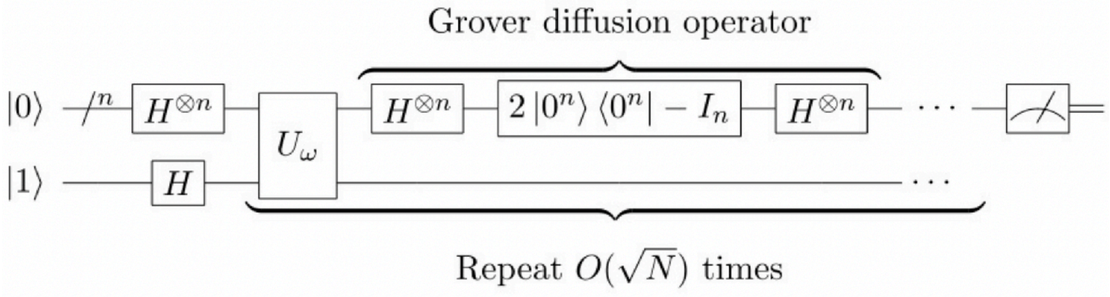
$$H^{\oplus n} Z_{OR} H^{\oplus n} |\psi\rangle = H^{\oplus n}(2\,|0^n\rangle\langle 0^n| - I)H^{\oplus n}$$

$$= 2H^{\oplus n}(|0^n\rangle\langle 0^n|)H^{\oplus n} - H^{\oplus n} I H^{\oplus n}$$

$$= 2\,|u\rangle\langle u| - I$$

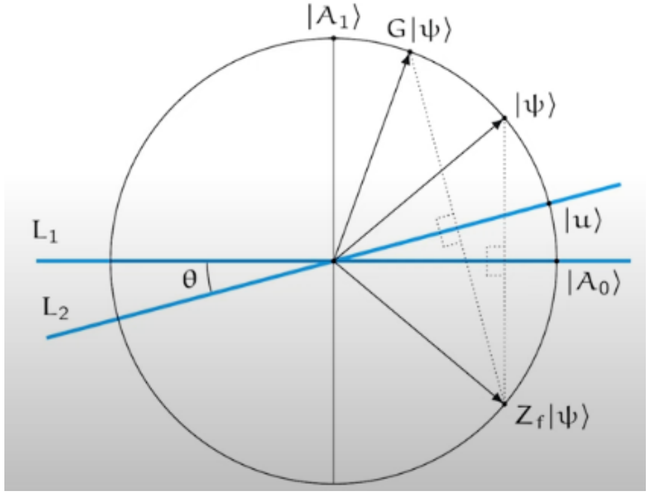
We used the fact that $H^{\oplus n}|0^n\rangle = |u\rangle$

4. Grover's algorithm : the proof



https://fr.wikipedia.org/wiki/Algorithme_de_Grover

Understanding the Grover diffusion operator:
$(H^{\oplus n} Z_{OR} H^{\oplus n}) Z_f |\psi\rangle$

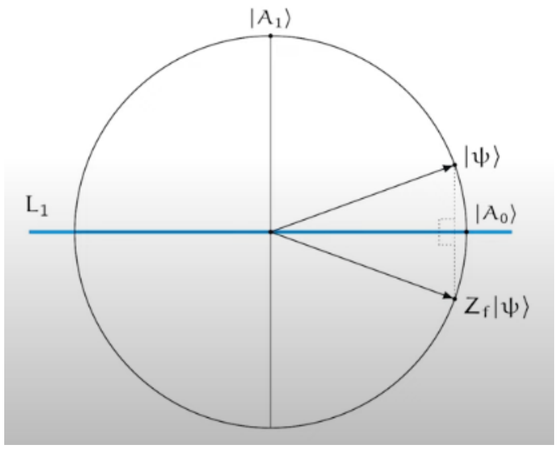


John Watrous, IBM

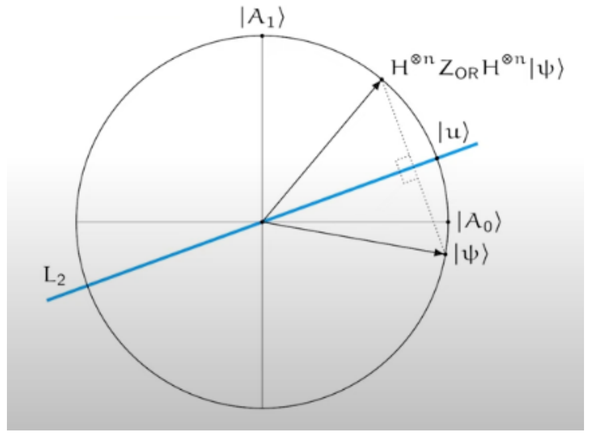
1. Symmetry around $|A_0\rangle$
2. Symmetry around $|u\rangle$

Equivalent to a rotation of vector $|\psi\rangle$ of angle 2θ, where θ is the angle between vectors $|u\rangle$ and $|A_0\rangle$

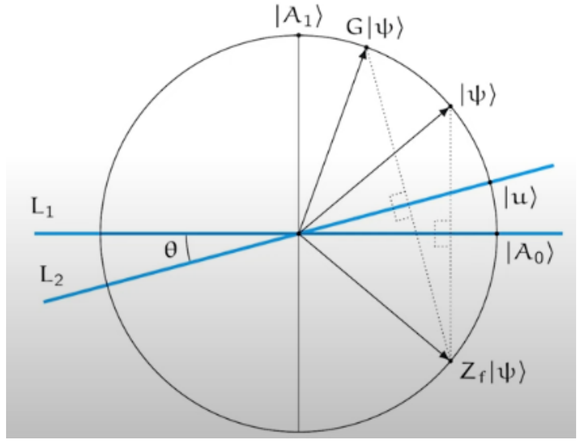
4. Grover's algorithm : the proof



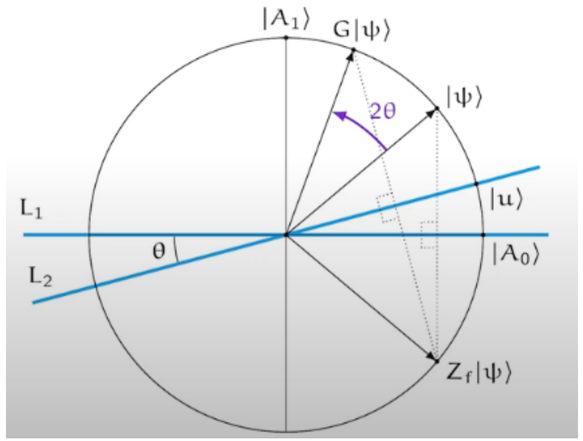
1. On applique Z_f



2. Puis $H^{\oplus n} Z_{OR} H^{\oplus n}$



3. La combinaison des deux produit...



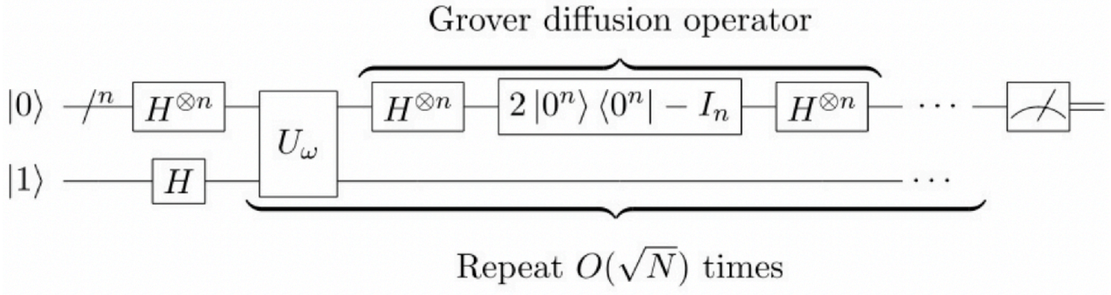
Une rotation d'angle 2θ

Understanding the Grover diffusion operator:
$(H^{\oplus n} Z_{OR} H^{\oplus n}) Z_f |\psi\rangle$

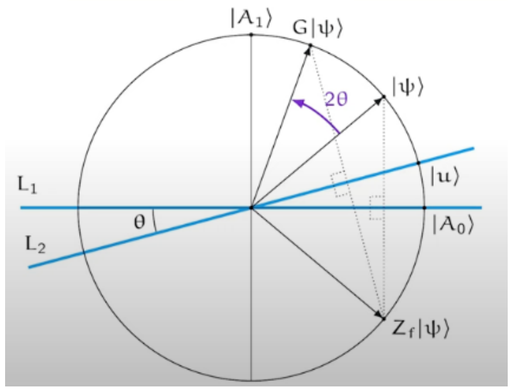
1. Symmetry around $|A_0\rangle$
2. Symmetry around $|u\rangle$

Equivalent to a rotation of vector $|\psi\rangle$ of angle 2θ, where θ is the angle between vectors $|u\rangle$ and $|A_0\rangle$

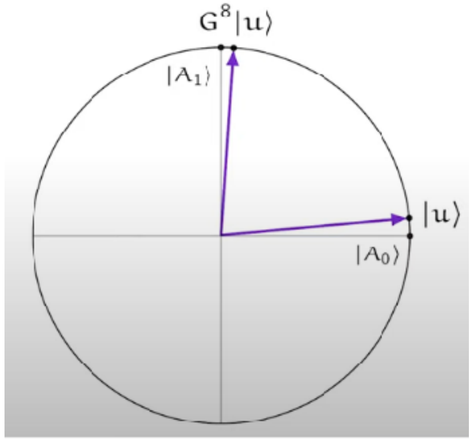
4. Grover's algorithm : choose the number of itérations



https://fr.wikipedia.org/wiki/Algorithme_de_Grover



Une rotation d'angle 2θ



$N = 128, t = 8$

1. We start from $\psi_0 = |u\rangle$, of angle θ with $|A_0\rangle$
2. After t itérations, the angle becomes $(2t+1)\theta$ $|A_0\rangle$
3. We aim to measure A_1, thus we want the angle to become roughly 90°, or $\pi/2$

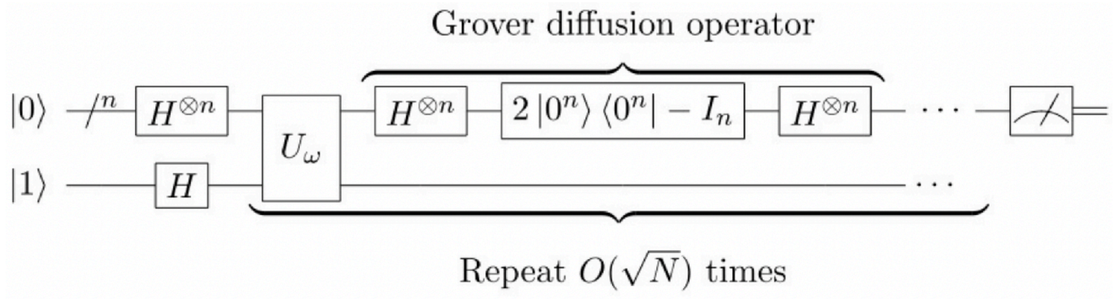
$$|u\rangle = \frac{1}{\sqrt{N}}|A_1| + \frac{\sqrt{N-1}}{\sqrt{N}}|A_0\rangle$$

$$|u\rangle = \sin(\theta)|A_1| + \cos(\theta)|A_0\rangle$$

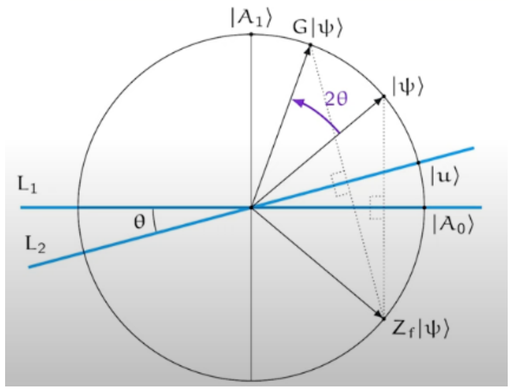
Thus $\sin(\theta) = \frac{1}{\sqrt{N}}$, and for large N, $\theta \sim \frac{1}{\sqrt{N}}$.

Therefore, we choose $t = \lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ itérations

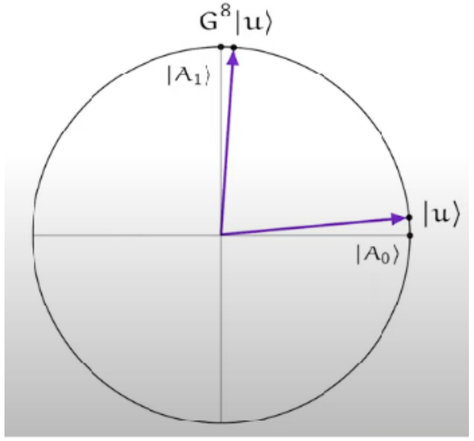
4. Grover's algorithm — the circuit



https://fr.wikipedia.org/wiki/Algorithme_de_Grover



Une rotation d'angle 2θ



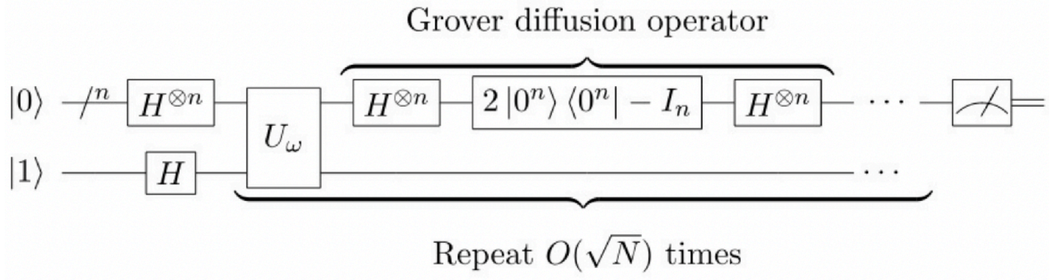
$N = 128, t = 8$

Grover's circuit, $n+1$ qubits

1. Apply $H^{\oplus n}$: H gates on the first n qubits
2. Apply X and H on qubit $n+1$
3. repeat $t = \lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ times the Grover operator:
4. add Z_f
5. add $H^{\oplus n}$
6. add Z_{OR}
7. add $H^{\oplus n}$
8. measure the n first

For the implementation of Z_f and Z_{OR} we use circuits U_f and U_{OR}, with the last qubit set to $|-\rangle$.

4. Grover's algorithm — the circuit



https://fr.wikipedia.org/wiki/Algorithme_de_Grover

Theorem. Grover's algorithm measures x_1 with probability at least $1 - \frac{1}{N}$, where $N = 2^n$.

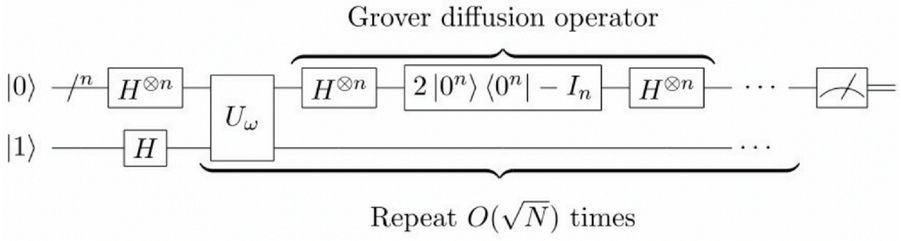
Grover's circuit

1. Apply $H^{\oplus n}$ on the first n qubits, set the last one to $|-\rangle$
2. repeat $t = \lfloor \frac{\pi}{4}\sqrt{N} \rfloor$ times the Grover operator:
3. add Z_f then $H^{\oplus n}$ then Z_{OR} then $H^{\oplus n}$
4. Measure the first n qubits

Extensions

- If f has an arbitrary number of solutions, choose the number t of iterations uniformely at random in $\{1,\ldots,\pi\sqrt{N}/4\}$. Success probability $\geq 40\,\%$.
- One can do better, cf. [John Watrous, YouTube].
- Optimisation : $f : \{0,1\}^n \to \mathbb{N}$, compute x s.t. $f(x)$ is maximum: même complexité, [Dürr, Høyer '97].
- Many applications but $2^{n/2}$ gates! Why is this an issue?

4. Grover's algorithm



https://fr.wikipedia.org/wiki/Algorithme_de_Grover

Theorem. Grover's algorithm measures x_1 with probability at least $1 - \frac{1}{N}$, where $N = 2^n$.

Exercise 1.

1. Describe completely Grover's algorithm, in the "simplified" case (unique solution).
2. Apply it to a function with 2 bits as input. Analyze the change in amplitudes after each step. What is the probability of finding the solution?
3. Same question for a 1-bit function.

Exercise 2. Now let us consider that the input function has no particular restrictions.

1. Recall the mixed classical/quantum algorithm, which finds a solution x_1 such that $f(x_1) = 1$ with probability $\geq 40\%$, if such a solution exists.
2. Modify the algorithm to obtain a solution with probability at least $1 - 1/N$. Specify its time complexity.

5. The impact of quantum computing

in the short and medium term

Objective: explore the impact of quantum programming tools on modern computing and delve deeper into the details of a “mixed” algorithm that would sometimes use quantum code.

A. Shor's algorithm: factorisation and discrete logarithm. Consequences for cryptography, ‘post-quantum’ cryptography.

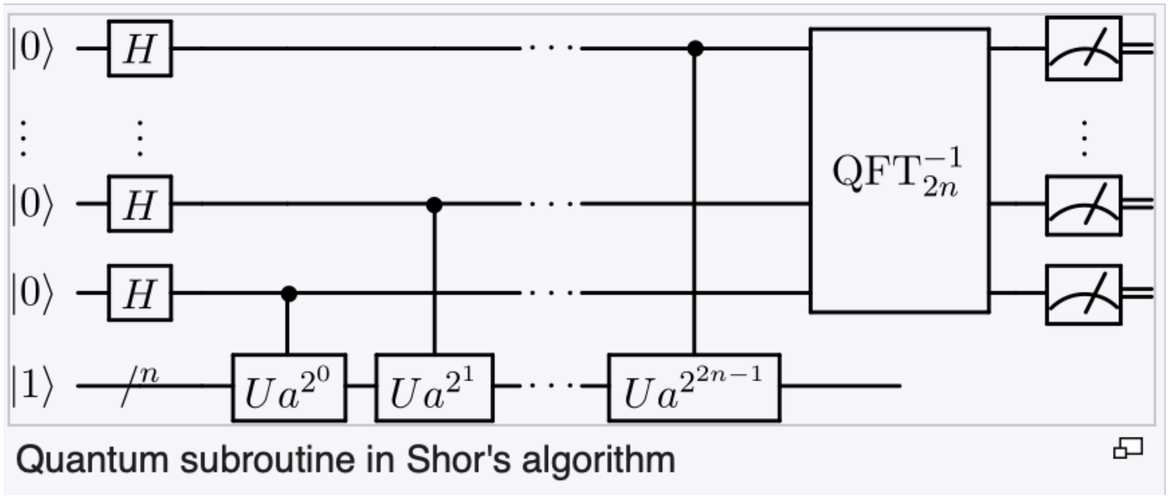
B. Quantum key exchange: BB84 algorithm.

C. Tools for mixed classical/quantum programming: focus on Grover's algorithm, if it needed to be adapted to applications.

A. Shor's algorithm [P. Shor '94]

Allows to solve, in polynomial time w.r.t. the number of bits of the input:

- Problem Factorisation(N): find a divisor of N, different from 1 and N, if any;
- The discrète logarithme modulo N: find $\log_b(a) = x$ such that $b^x = a \mod N$.



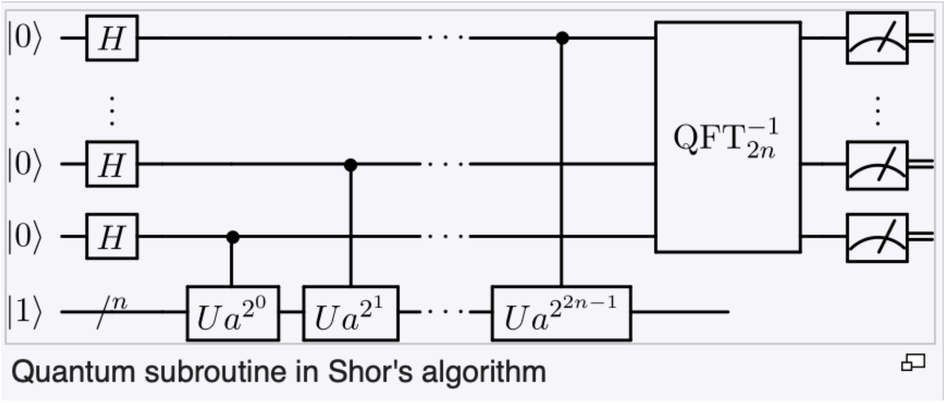
Wikipedia, Shor's algorithm

The "quantum" part computes, given numbers a and N, the smallest integer r such that $a^r = 1 \mod N$. The rest is classical. Complexity $O(n^2) = O((\log N)^2)$.

A. Consequence: post-quantum cryptographie

If we could efficient implement Shor's algorithm, it would break:

- **RSA encryption protocol** [Rivest, Shamir, Adelman '77], whose security relies on the difficulty of factoring a (large) number into prime factors..
- **Diffie-Hellman key exchange protocol** [Diffie, Hellman '76], whose security relies on the difficulty of calculating the discrete logarithm.



Wikipedia, Algorithme de Shor

Most protocols currently in use are based on these two problems...

The emergence of **post-quantum cryptography**, which has nothing to do with quantum physics and offers other protocols that are resistant to this type of attack.

Examples: CRYSTALS-Kyber (keys), CRYSTALS-Dilithium (signature), based on 'structured Euclidean networks'.

B. Secure key exchange [Bennett-Brassard 84]

For secure key exchange, a quantum solution already exists.

Recommended reading and videos: Frédéric Magniez's lectures at the Collège de France, https://www.college-de-france.fr/chaire/frederic-magniez-informatique-et-sciences-numeriques-chaire-annuelle/events

Objective of key exchange: A and B must agree on a key (random sequence of bits).

- Assumption that A and B are properly identified (no identity theft).
- At the end of the protocol, A and B must have the shared key and must be the only ones to possess it. If someone has listened into the conversation between A and B, they must realise it.

Why BB84 ?

4

1. It can be presented in 20 minutes
   - by simplifying it a lot…
   - but without butchering it, I hope
2. It uses several properties of qubits:
   - vectorial aspect (superposition, measurement)
   - non-cloning theorem
3. **It has already been implemented!**
   - qubits: photons
   - optical fibre

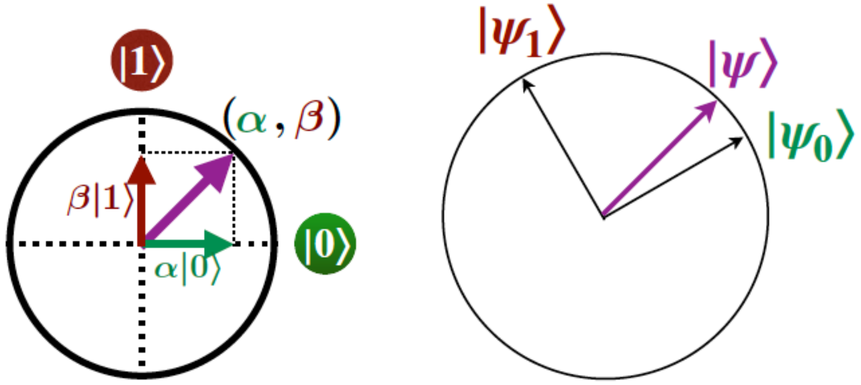
C. Bennet

G. Brassard

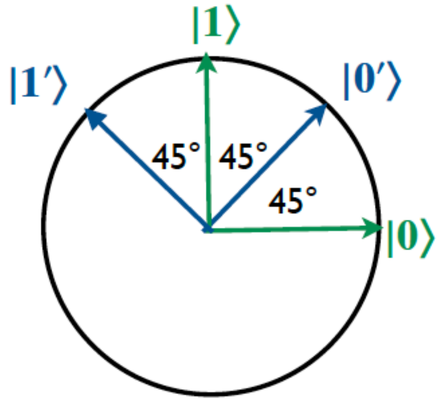
1st tool : measures in different bases

[Images from the talks of F. Magniez at Collège de France]

Measure and basis: a qubit can be measured in any orthogonal basis



We will choose two bases $|0\rangle, |1\rangle$ and $|0'\rangle, |1'\rangle$ with a rotation of 45°.

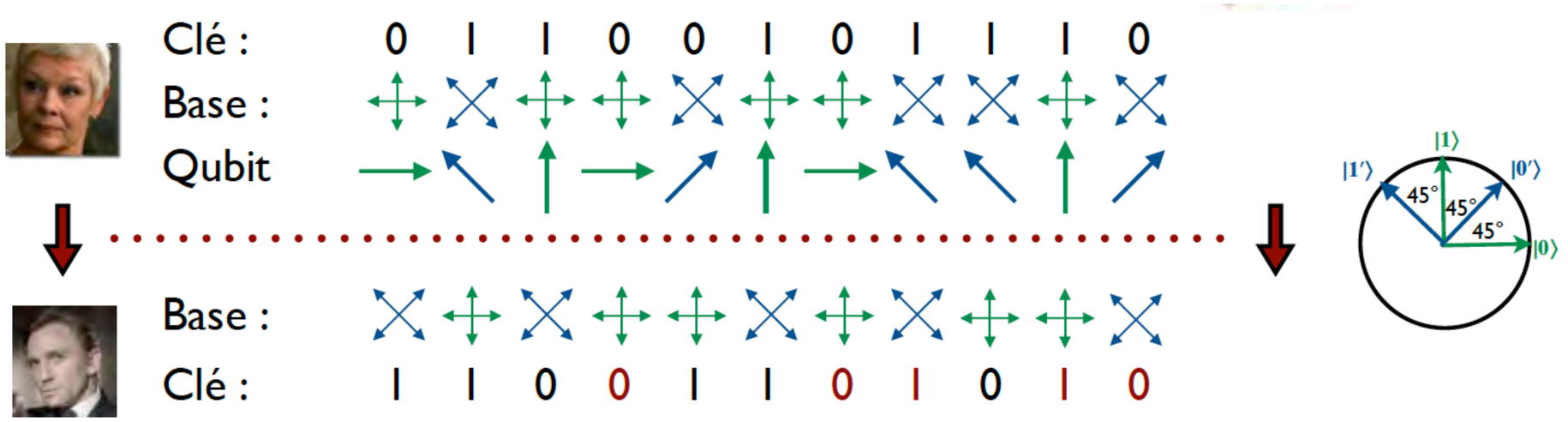


Observation: the $|0'\rangle$ measured into the base $|0\rangle, |1\rangle$ gives 0 with probability 1/2 and 1 with probability 1/2. Same for any other 'mismatched' measure

BB84 putting the details under the carpet (1)

Quantum communication from **Alice to Bob.**

Alice chooses a bitstring (uniformly at random), and a séquence of bases. This yields a sequence of qubits, by interpreting each bit in the corresponding base. These qubits are communicated to Bob.

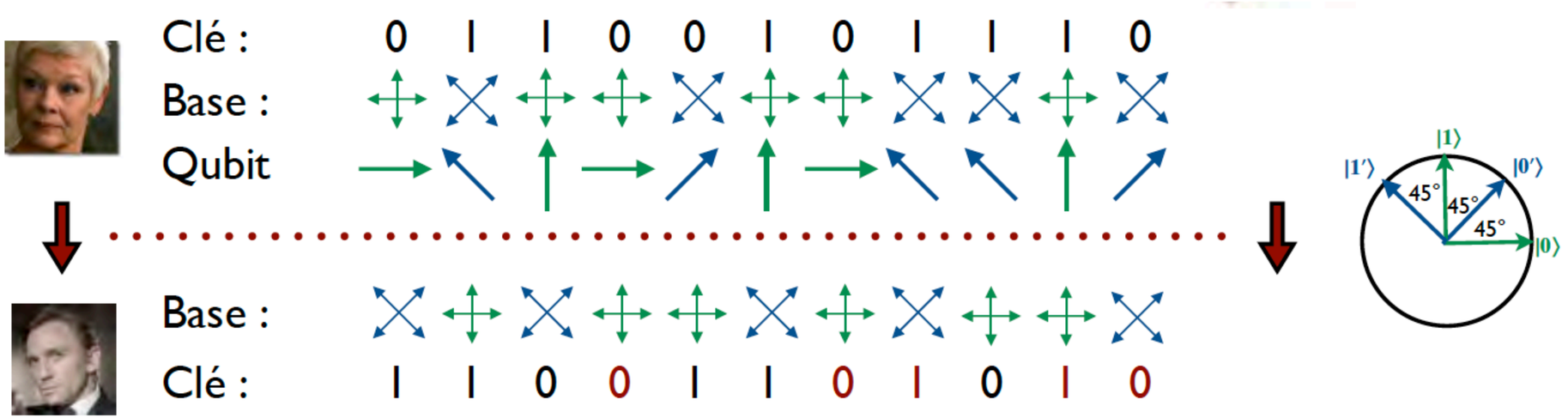


Talk of F. Magniez

BB84 putting the details under the carpet (2)

Bob chooses a sequence of bases and measures the received qubits in those bases.

Alice and Bob communicate the bases choosen by each of them.

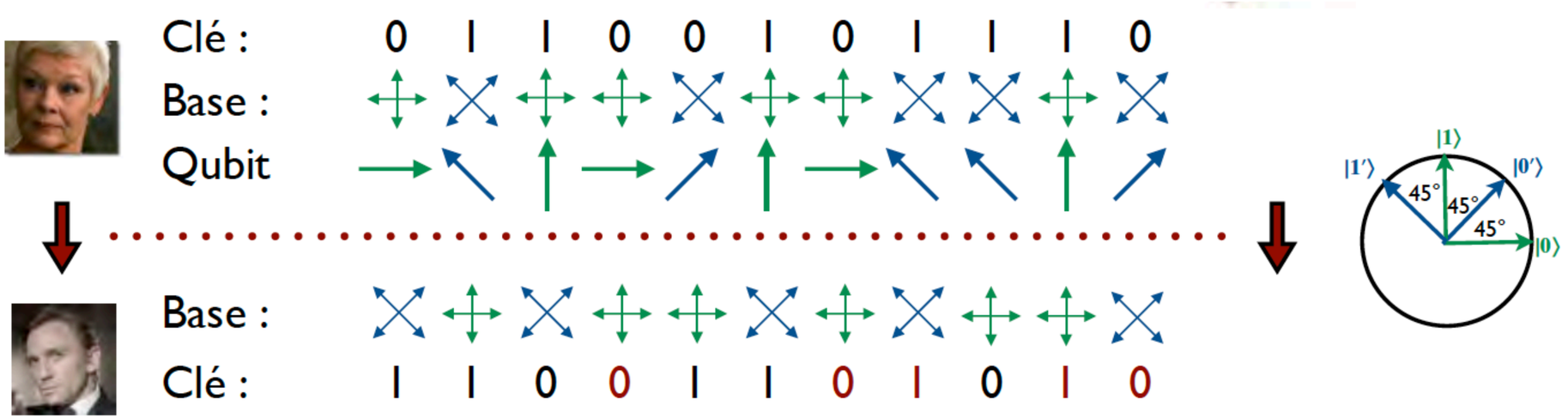


Talk of F. Magniez

BB84 putting the details under the carpet (3)

On average, half of the bases chosen by Alice and Bob coincide. Only these bits are kept as keys. Conclusion: Alice and Bob agreed on half of the bits! (Well, modulo errors, but that's **not the subject of today's discussion**).

What about intruders and eardropping ???



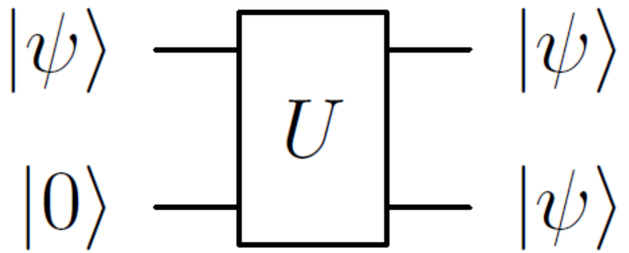
Talk of F. Magniez

2nd tool: no cloning theorem

Theorem. It is impossible to duplicate an unknown qubit.

- Informally: if we measure it, we distroy its superposition (vectoriel behaviour)
- Formally: prove it using the linearity of quantum transformations. See 1st session of exercises.

Counterintuitive but not difficult to demonstrate, by linearity.

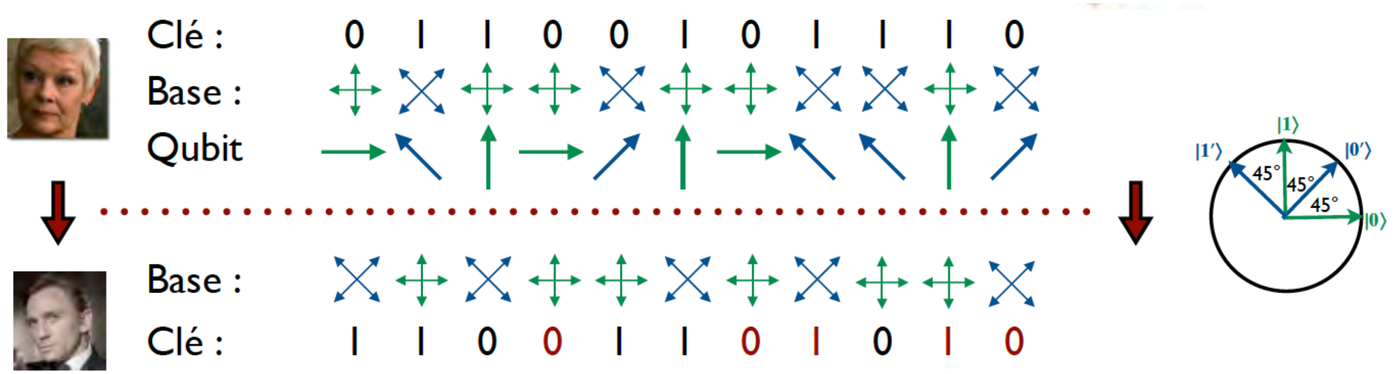


Consequences of no cloning on BB84

Admit that some intruder listened to Alice's messages to Bob.

It will be impossible for him/her to "put" the intercepted qubits back into the channel without altering a large proportion of them. And that will be noticeable.

Extrait exposé F. Magniez



Talk of F. Magniez

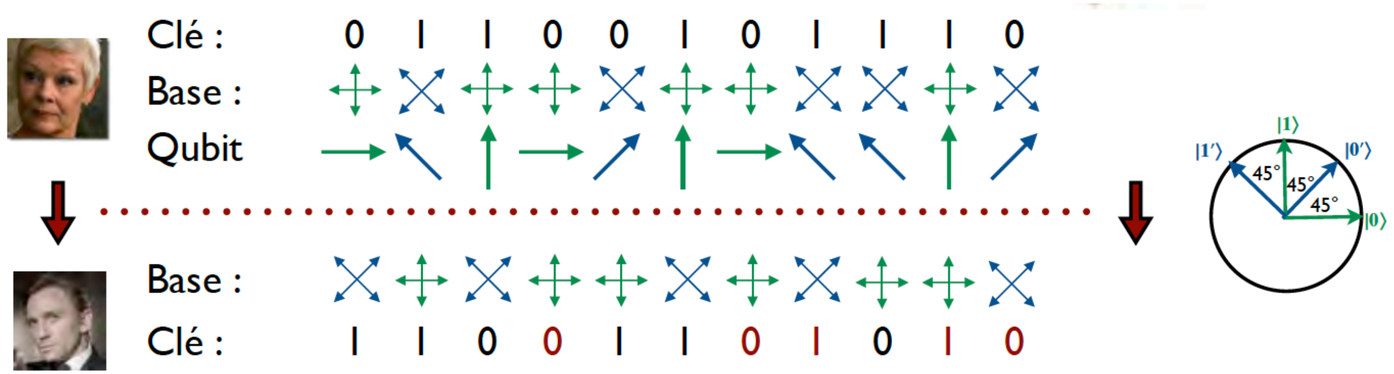
Informal, but it can be turned into proof, even if the intruder has clever strategies.

Consequences of no cloning on BB84

Admit that Eve (Evil) listened to the secret exchanges between Alice and Bob.

Option 1. Eve mesured each qubit sent by Alice to Bob in one of the two bases, at random, and “puts it back” in the same base.

Extrait exposé F. Magniez



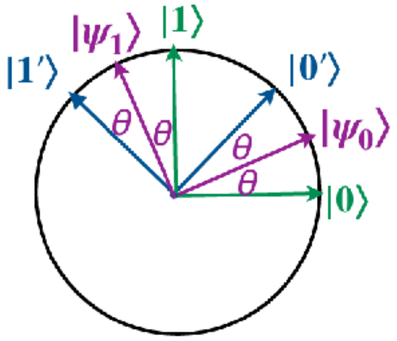
Exercise. Compute the probability that the qubit returned by Eve is identical to the qubit sent by Alice. Compute the probability that the bit read by Eve is equal to the one sent by Alice.

How would Bob detect the intrusion if Eve read k qubits?

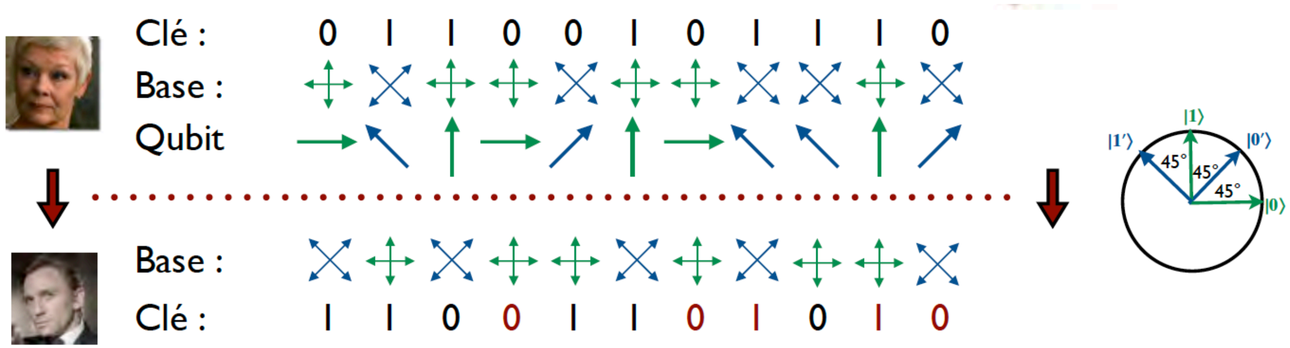
Consequences of no cloning on BB84

Assume that Eve adopts a more sophisticated strategy.

Option 2. Eve chooses some other base ($|\psi_0\rangle, |\psi_1\rangle$), in which she measures the qubit sent by Alice, and puts it back in this same base. Let θ be the angle of this base with the canonial one.



Talk by F. Magniez



Talk by F. Magniez

Exercise. What is the probability that the bit read by Bob is the one sent by Alice, despite the intrusion? What is the probability that the bit read by Eve is the one sent by Alice? How can the intruder be detected?

C. Grover's algorithm in mixed algorithms

1. Introduction Consider the following problem from a crossword puzzle:

_ _ r _ n h _ (Solution - piranha)

You have an online dictionary with 1, 000, 000 words in which the words are arranged alphabetically. You could program it to look for the solution to the puzzle so that it typically solves it after looking through 500, 000 words. It is very difficult to do much better than this. But that is: only if you limit yourself to a classical computer. A quantum computer can be in multiple states at the same time and, by proper design, can carry out multiple computations simultaneously. In case the above dictionary were available on a quantum computer, it would be possible to carry out the search in only about 1, 000 steps by using the quantum search algorithm.

Lov Grover, From Schrödinger's Equation to the Quantum Search Algorithm, ArXiV 2001.

Theorem. Grover's algorithm measures x_1 with probability at least $1 - \frac{1}{N}$, where $N = 2^n$.

Exercise. Let's imagine that we had to implement Grover's puzzle for real. We have discussed Grover's quantum circuit implementation at length.

1. What work would a computer scientist have to do if they only had Qiskit and a quantum computer at their disposal?
2. How could they encode a table of integers, or even Booleans? Even if it were inefficient?

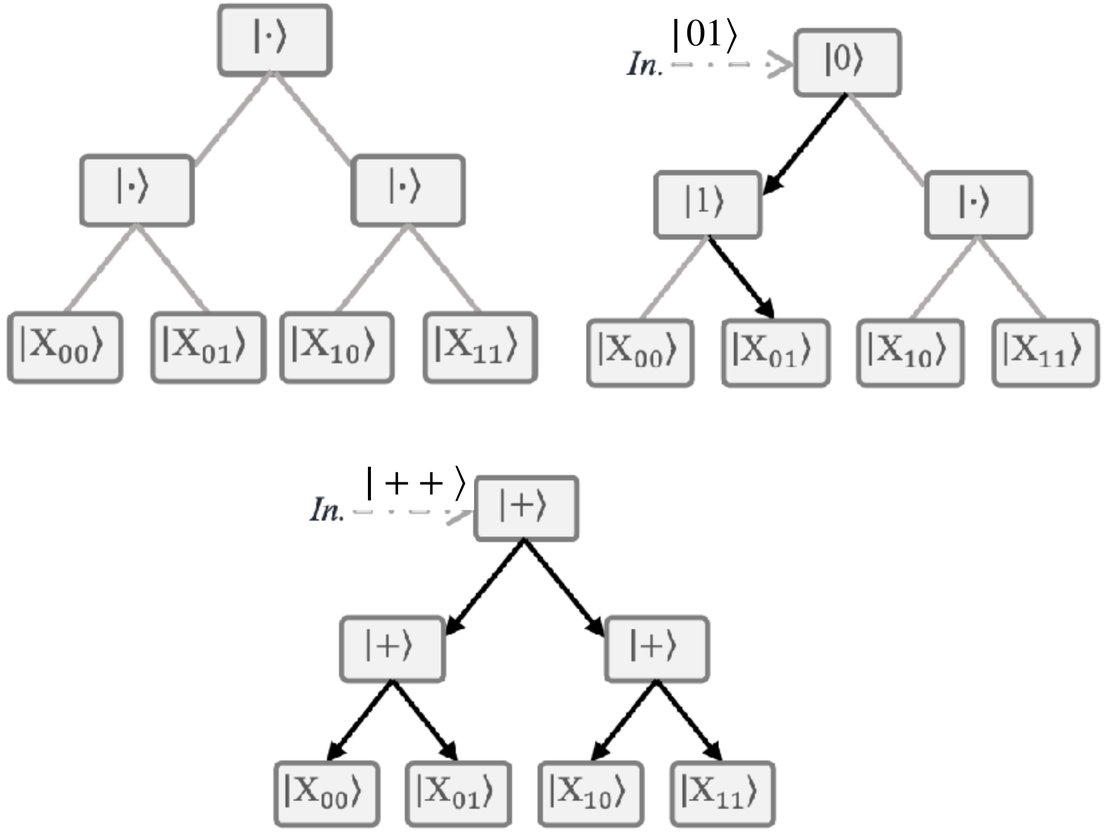
C. Quantum RAM : principe

To implement Grover's algorithm with an array, we would need a "QRAM" to store boolean (or integer) arrays X of size $N = 2^n$ and access $X[i]$ in time poly(n).

$$|i\rangle \mapsto |i\rangle\,|X[i]\rangle$$

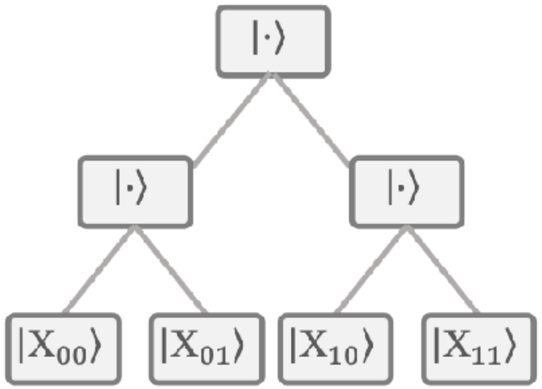
Moreover, we need superposed access::

$$\sum_{i=0}^{N-1} \alpha_i\,|i\rangle \mapsto \sum_{i=0}^{N-1} \alpha_i\,|i\rangle\,|X[i]\rangle$$



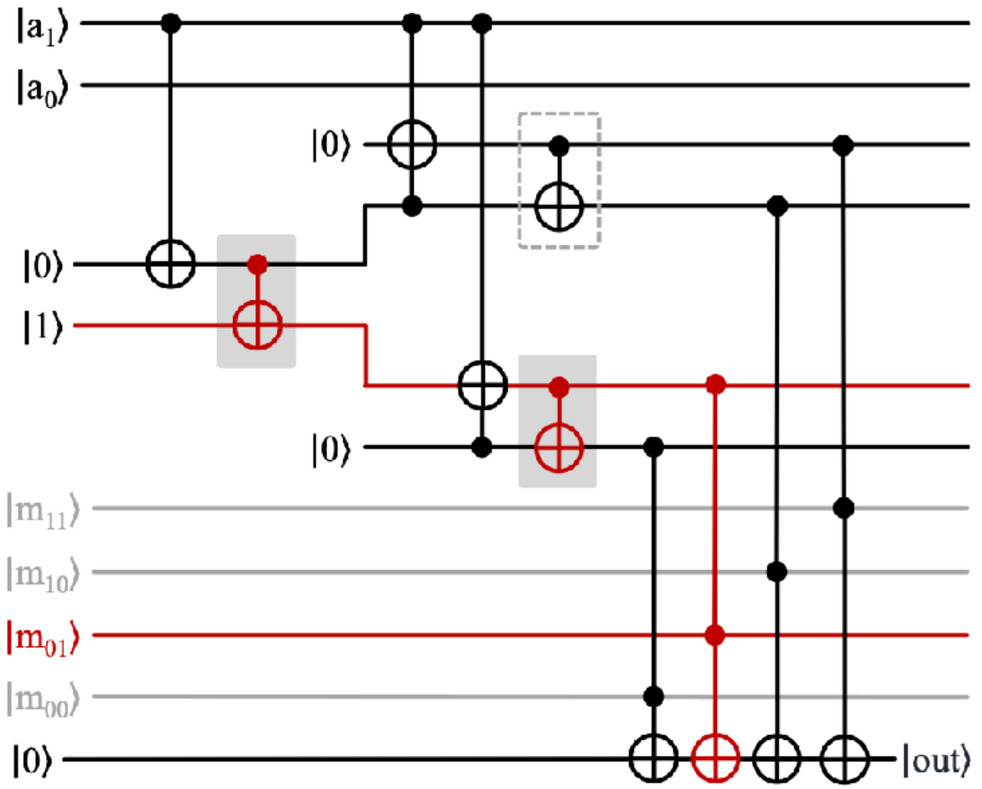
Phalak, Chatterjee, Ghosh, Quantum Random Access Memory For Dummies, ArXiV 2023

C. Quantum RAM : implémentation



From Phalak, Chatterjee, Ghosh, Quantum Random Access Memory For Dummies, ArXiV 2023.

See also Arunachalam *et al*., On the robustness of bucket brigade quantum RAM, ArXiV 2015.



Implementation of a QRAM for an array of size 4. In red, the gates activated when reading the address $|01\rangle$.
There is a bug in the circuit, can you find it?

6. Conclusion

and further reading

1. Quantum algorithms: circuits, qubits, quantum gates.
2. Unusual way of thinking; not that complicated mathematically, after all.
3. Not too complicated: Simons's algorithm. Finds the period of an n-to-n bits function, with a polynomial number of calls. Exponential speed-up w.r.t. classical randomized algorithms.
4. More subtle: Shor's algorithm for factorisation. Period estimation, (quantum) fast Fourrier transformé.
5. Quantum cryptography, "teleportation" of an unknown qubit. Entanglement, no cloning, measurement in different bases.

Présentations by Frédéric Magniez, Collège de France. Books, par ex. [Kaye, Laflamme, Mosca, *An Introduction to Quantum Computing*, 2007; Nielsen, Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2010].

Thesis of Arthur Braida (Eviden/LIFO - Univ Orléans) for adiabatic quantum computing

Lectures and lecture notes by John Watrous (IBM) on YouTube.

7. Entanglement

Cf. Nobel prize for Alan Aspect *et al.*

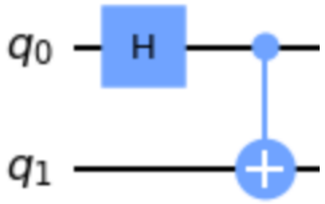
Bell states(2 entangled qubits): what happens if we separate them by a large distance?

Well... after measuring the first one, the second one will give the same measure — even if the delay between measurements is shorter than the time to communicate at light speed among them.

(Serious) doubts of Einstein [Einstein, Podolsky, Rosen '35] w.r.t. Bohr's interprétation; the former think it contradicts the locality principle. They propose the hidden variable theory, as if the qubits agreed on something before they were separated.

A. Aspect conducted an experiment in Orsay (with Grangier, Roger, and Dalibard) proving that the hidden variable theory does not hold (using Bell's inequalities).

Applications to cryptography. So-called 'teleportation', in the sense that an unknown qubit can be 'sent' to someone else, at a distance, without duplication.



Etat de Bell :

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$