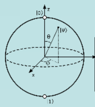
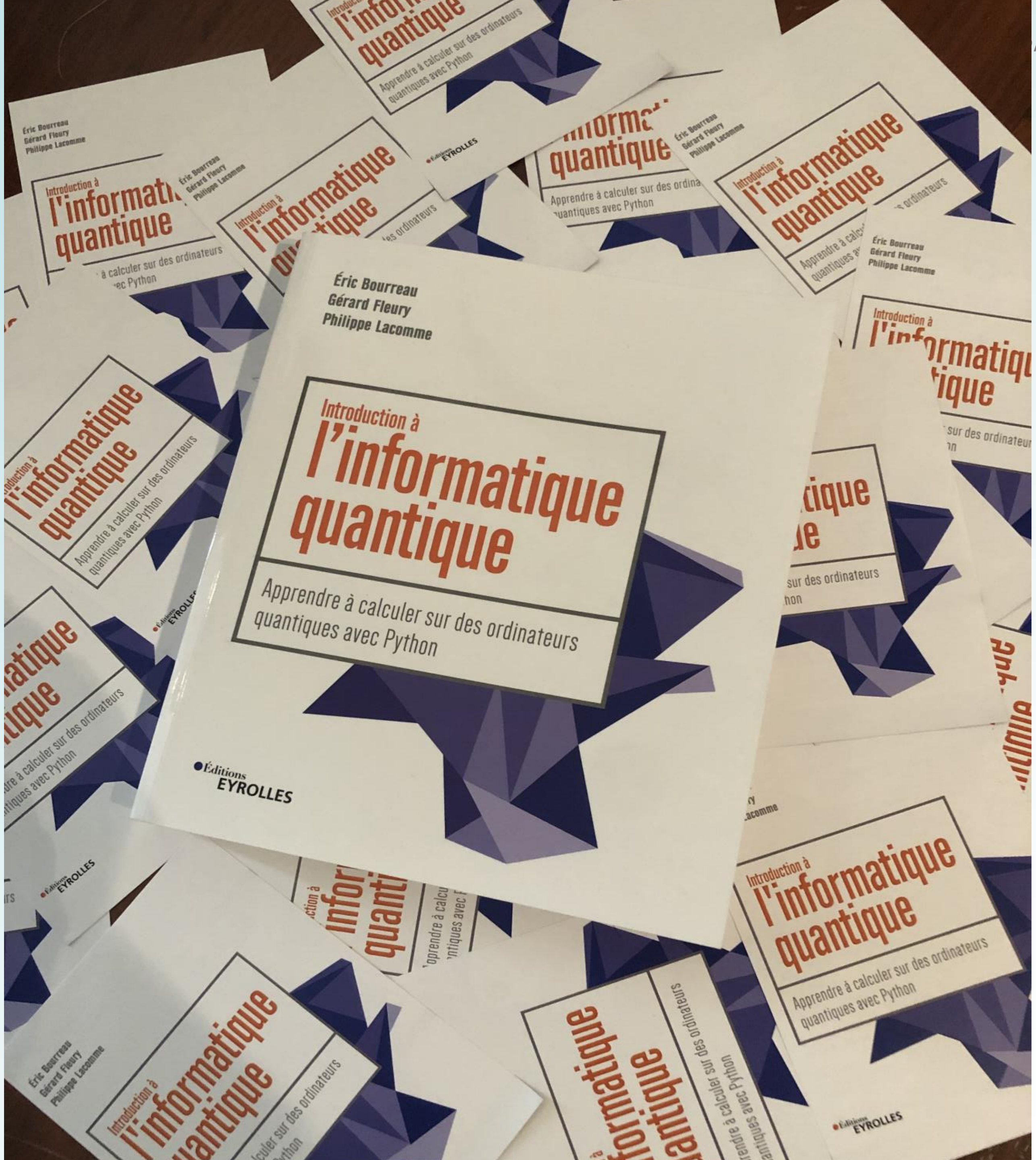
# rdinateurs quantiques : nouvelle révolution informatique ?

**Eric Bourreau, LIRMM (Laboratoire d'Informatique Robotique et Microélectronique de Montpellier)**

**Université de Montpellier**

eric.bourreau@umontpellier.fr



# Breaking News

17:24 54%

Menu SCIENCES AVENIR Connexion S'ABONNER DÈS 1€

QUANTIQUE

## Alain Aspect, prix Nobel de physique 2022 : "La deuxième révolution de la physique quantique ne fait que commencer"

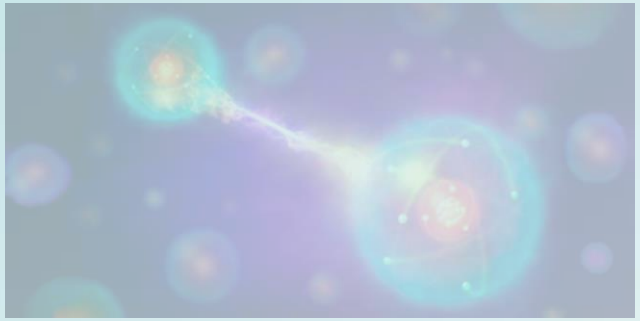
Par Jean-François Haït le 04.10.2022 à 12h22, mis à jour le 04.10.2022 à 17h10

ABONNÉS

Lecture 12 min.

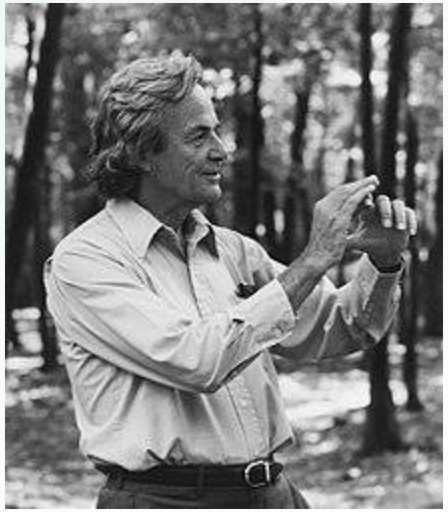
Le prix Nobel de physique 2022 a été attribué au Français Alain Aspect, à l’Américain John F. Clauser et à l’Autrichien Anton Zeillinger, pour leurs travaux en physique quantique. Il y a quelques jours seulement, *Sciences et Avenir* réalisait l'interview d'Alain Aspect pour son hors-série "Les indispensables" dédié à "La grande histoire de la physique" et en kiosque le 21 décembre 2022. Entretien à découvrir en exclusivité sur notre site.

2 RÉACTIONS



# Informatique Quantique

- Un ordinateur quantique
  - Richard Feynmann
    ***Simulating Physics with Computers***, Int. J. Theor. Physics, vol 21, n°6/7, 1982, pp 471-493
    *« …a place where the relationship of physics and computation has turned itself the other way and told us something about the possibilities of computation … »*
    *« Can you do it with a new kind of computer--**a quantum computer**? »*



- Des phénomènes étranges
  - **Superposition**
  - **Intrication**
  - **Fragilité d’observation**

# Exemples de Superposition


# De la théorie à la pratique

1982 Feynmann

→ 1994 Shor → 1996 Grover

→ 2000 : ordinateur 5 Qubits → 2011 Dwave 1er ordinateur commercial

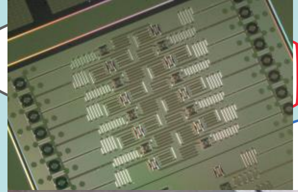
→ Rigetti, IBM, IonQ, …

→ 2019 Google : Suprématie Quantique

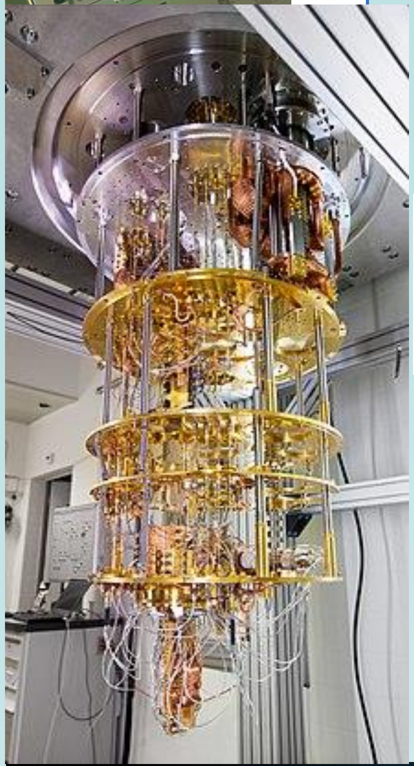
D::Wave IBM Google Qiskit rigetti

https://en.wikipedia.org/wiki/Timeline_of_quantum_computing_and_communication

# Les machines

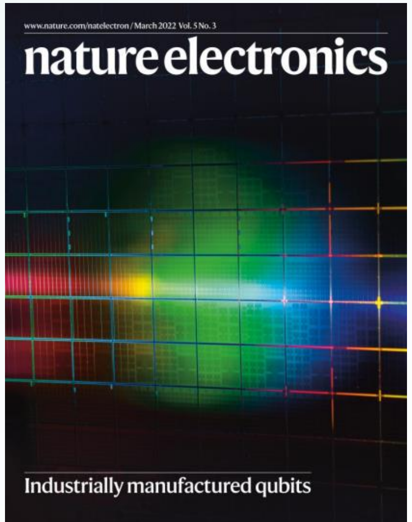


## Technologies utilisées



| | recuit quantique | boucles supra-conductrices | qubits topologiques | optique linéaire | quantum dots silicium | ions piégés | cavités diamants |
|---|---|---|---|---|---|---|---|
| **qubit** | supraconducteur effet Josephson | supraconducteur effet Josephson | quasi-particules faites de paires d'anyons | photons | spin d'électrons dans semi-conducteur | ions piégés magnétiquement | spin de noyau d'atomes |
| **# qubit** | **2048 qubits** (D-Wave) | **50 qubits** (IBM) **72 qubits** (Google) | **N/A** | **quelques-uns** | **49 qubits** (Intel) | **53 qubits** (IonQ) **51 qubits** (MIT) **20 qubits** (IQOQI) | **6 qubits** (QDTI) |
| **état** | sens du courant | phase de résonnance ou sens du courant | sens de l'anyon | phase de photon | spins d'électrons | niveau énergétique de l'ion piégé | niveau d'énergie de la cavité |
| **portes** | micro-ondes 5 GHz et effet Josephson | micro-ondes 5 GHz et effet Josephson | inversions 2D d'anyons | filtres polarisants et dichroïques | micro-ondes | laser | laser |
| **mesure** | magnétomètre | magnétomètre | fusion d'anyons | détecteurs de photons | conversion spins to charge | fluorescence | fluorescence |


祖冲之 *Zuchongzhi*




**+ Pasqal : atomes froids, 100+ qbits**

# Les start-ups

# Programmer un ordinateur quantique

Théorie : automates finis….

Ecrire un algorithme → Compiler → Exécuter →

Langage : C/C++
Primitives : for, while, loop….

Outils : compilateur

Outils : Machine
Machine : bits

Ecrire un algorithme → Transpiler → Compiler Envoyer → Exécuter →

Langage : Qiskit/Q-Asm/Q#
Primitives : portes quantiques

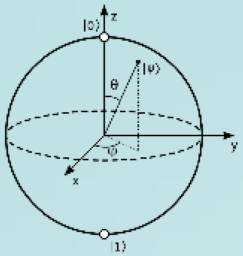
Outils : Transpilateur

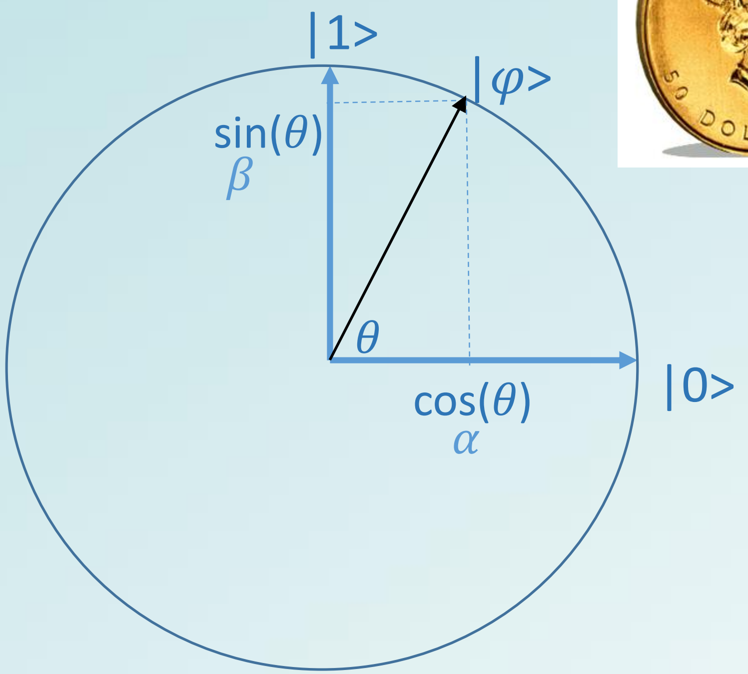
Outils : librairie Python

Outils : Machine Quantique
Machine : qubits

Théorie : espace Hilbert,  superposition d'états….

# Qubit





- Définition théorique :
  Un bit quantique (ou QuBit) est un vecteur de norme 1 dans l'espace canonique $\mathbb{C}^2$ de Hilbert
- Les bases sont :

$$|0\rangle = \begin{pmatrix} \mathbf{1} \\ \mathbf{0} \end{pmatrix} \text{ et } |1\rangle = \begin{pmatrix} \mathbf{0} \\ \mathbf{1} \end{pmatrix}$$

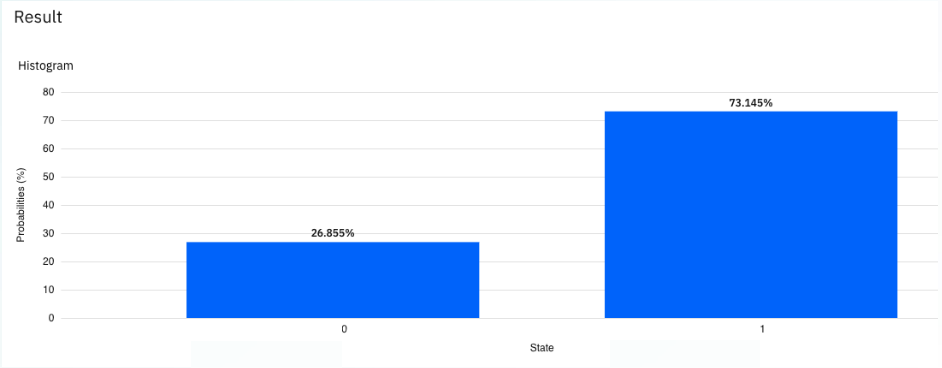
Il est dans un
une infinité d'
état superposé

- Son vecteur d'état est une combinaison linéaire entre les deux états |0> et |1>

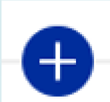
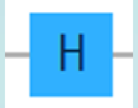
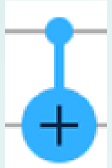
$$\boxed{|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ avec } |\alpha|^2+|\beta|^2=1,\ \alpha \text{ et } \beta \in \mathbb{C}}$$

(La représentation graphique ne considère ici que $\alpha$ et $\beta \in \mathbb{R}$ )

- Un qubit peut être observé uniquement dans
  un état aléatoirement choisi entre |0> ou |1> avec une probabilité proportionnelle à son amplitude au carré $\alpha^2$ et $\beta^2$
- Une fois mesuré un qubit est projeté définitivement dans un état (il s'écroule – *collapse*) et détruit toute son information



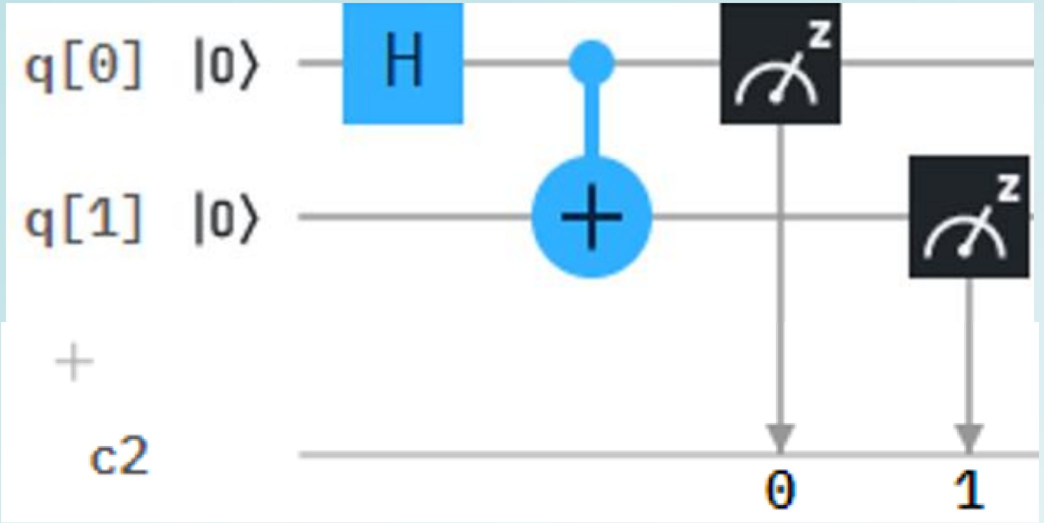
# Les portes quantiques

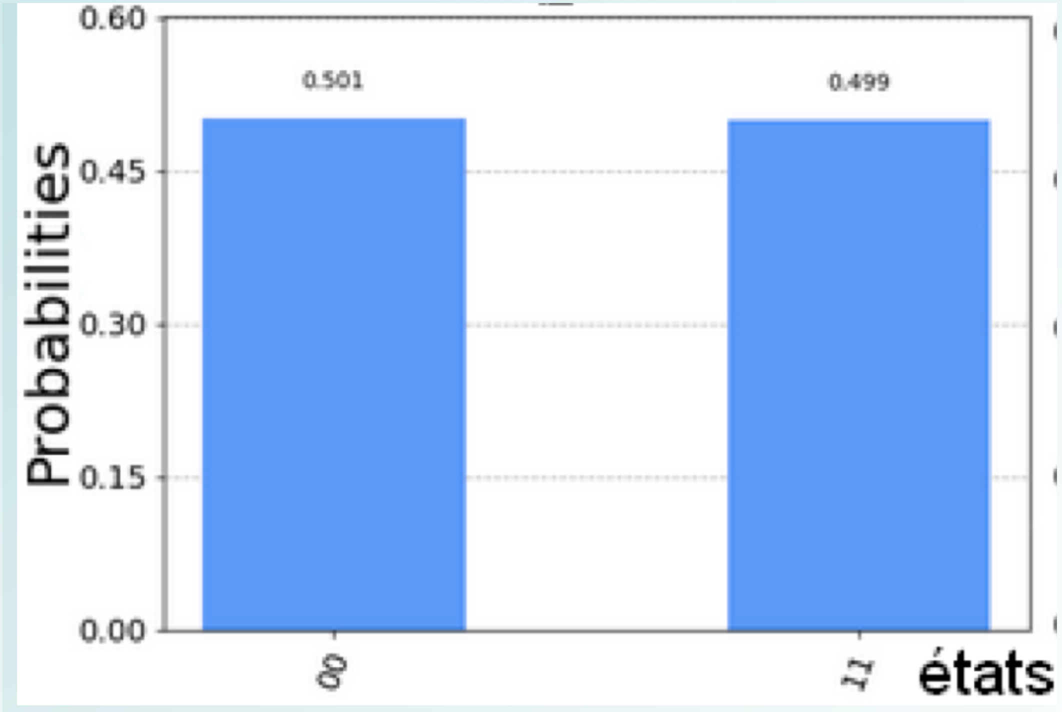
- Il est possible de faire des opérations sur les qubits sans détruire les états quantiques
- Ces opérateurs peuvent être représentés par des portes ou des matrices 2 x 2 unitaires (préservant la norme)
- Nous allons nous intéresser à 4 portes
  - **X** : bitFlip (équivalent au NOT) 
  - 
    
    **H** : permettant de ***superposer*** deux états
  - **CNOT** : porte binaire ***intriquant*** des états 
  - 
    
    **M** : permettant de ***mesurer*** un qubit

- H, S, T et CNOT forment un ensemble de portes universelles

| Operator | Gate(s) | | Matrix |
|---|---|---|---|
| Pauli-X (X) | X | $\oplus$ | $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ |
| Pauli-Y (Y) | Y | | $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ |
| Pauli-Z (Z) | Z | | $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ |
| Hadamard (H) | H | | $\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ |
| Phase (S, P) | S | | $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ |
| $\pi/8$ (T) | T | | $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ |
| Controlled Not (CNOT, CX) | $\oplus$ | | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ |
| Controlled Z (CZ) | Z | | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$ |
| SWAP | | | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ |
| Toffoli (CCNOT, CCX, TOFF) | $\oplus$ | | $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$ |

# Hello World (superposé et intriqué)

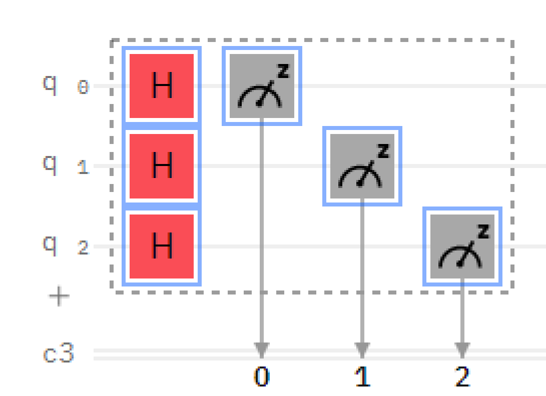




*« Etat de Bell »*

$$\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|00> + \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}|11>$$

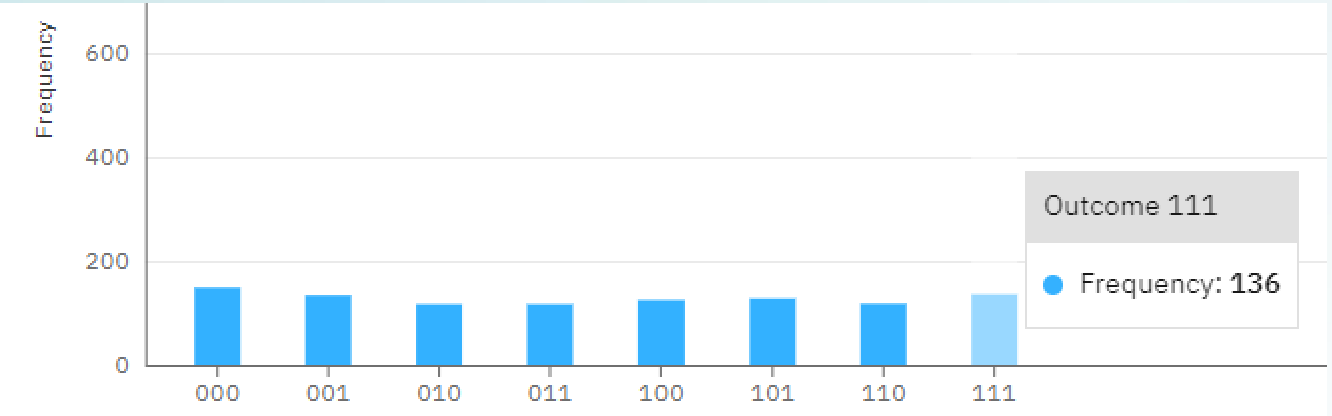
$$\cancel{|\varphi_1>\otimes|\varphi_2> = \alpha_1\alpha_2|00> + \alpha_1\beta_2|01> + \beta_1\alpha_2|10> + \beta_1\beta_2|11>}$$

# Représenter des entiers (simultanément)




- Un registre de 3 QuBits s'écrit $|q_2q_1q_0>$ (représentation binaire d'un entier)
- Chaque Qubit superpose l'état |0> et |1> équitablement (porte H)
- La lecture des 3 QuBits (portes grises) fournit aléatoirement un chiffre entre 0 et 7
- L'exécution 1000 fois de ce circuit fournit une distribution de probabilités

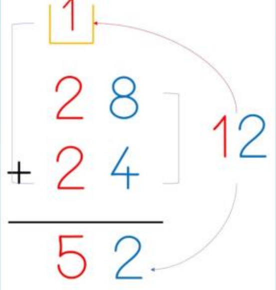
Exemple : 3 qubits, 8 états




*"The rule of simulation that I would like to have is that the number of computer elements required to simulate a large physical system is only to be* ***proportional*** *to the space-time volume of the physical system.* ***I don't want to have an explosion****. That is, if you say I want to explain this much physics, I can do it exactly and I need a certain-sized computer.* ***If doubling the volume*** *of space and time means I'll* ***need an exponentially larger computer****, I consider that* ***against*** *the rules" Feynmann 1982*

Remarque : 40 QuBits peuvent « stocker » un Tera d'états.

# L'addition (adder)



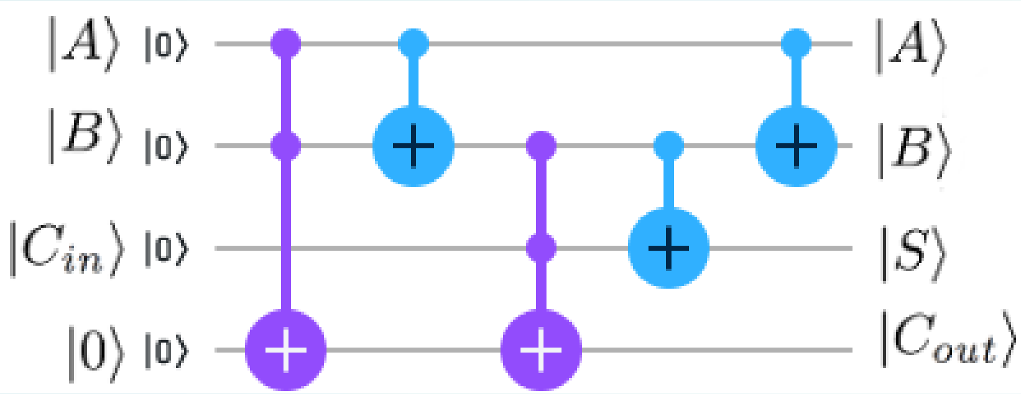

$^{1\,1}$1 1 1 0 0
1 1 0 0 0
-------------
1 1 0 1 0 0

- Des entier A,B représentés sur des registres de taille $\lceil \log_2(A) \rceil$ et $\lceil \log_2(B) \rceil$

  $A = a_n 2^n + a_{n-1} 2^{n-1} + \ldots + a_2 2^2 + a_1 2^1 + a_0 2^0$

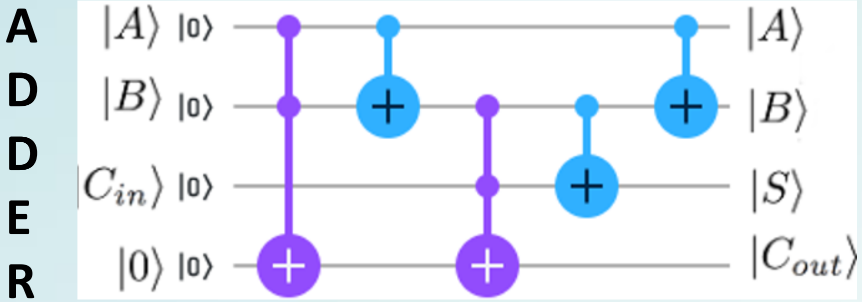
- Somme entre deux entiers comme à l'école : A+B=S

$$
\begin{array}{cccccccc}
c_{n-1} & c_n & c_{n-1} & \ldots & c_2 & c_1 & c_0 \\
 & b_n & b_{n-1} & \ldots & b_2 & b_1 & b_0 \\
+ & a_n & a_{n-1} & \ldots & a_2 & a_1 & a_0 \\
 & \multicolumn{6}{c}{====================} \\
s_{n+1} & s_n & s_{n-1} & \ldots & s_2 & s_1 & s_0
\end{array}
$$




| $\|A\rangle$ | $\|B\rangle$ | $\|C_{in}\rangle$ | $\|A\rangle$ | $\|B\rangle$ | $\|S\rangle$ | $\|C_{out}\rangle$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 |

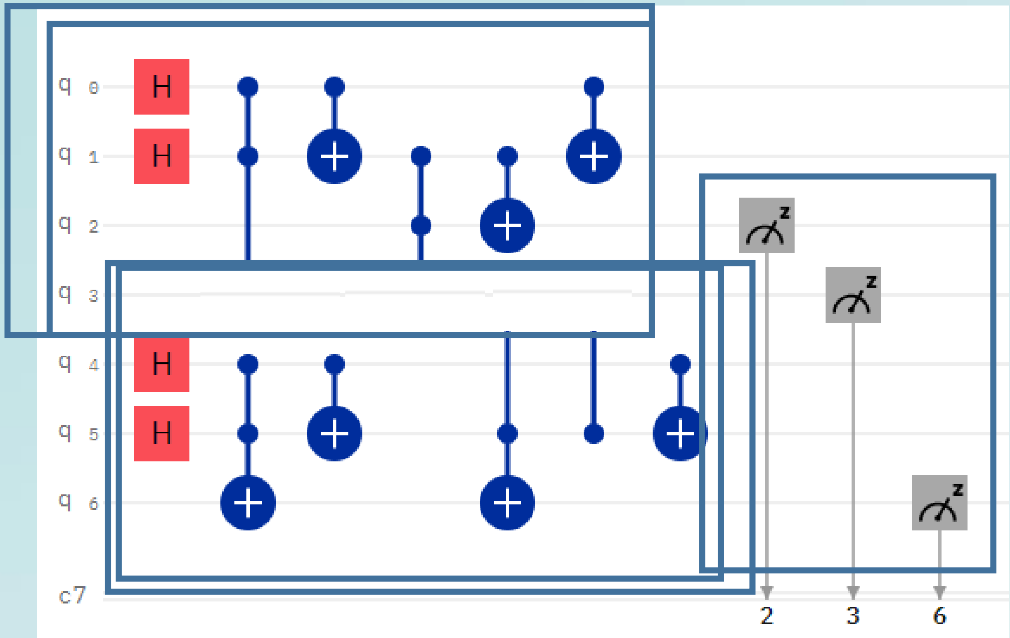
# Full Adder : Somme (superposée)



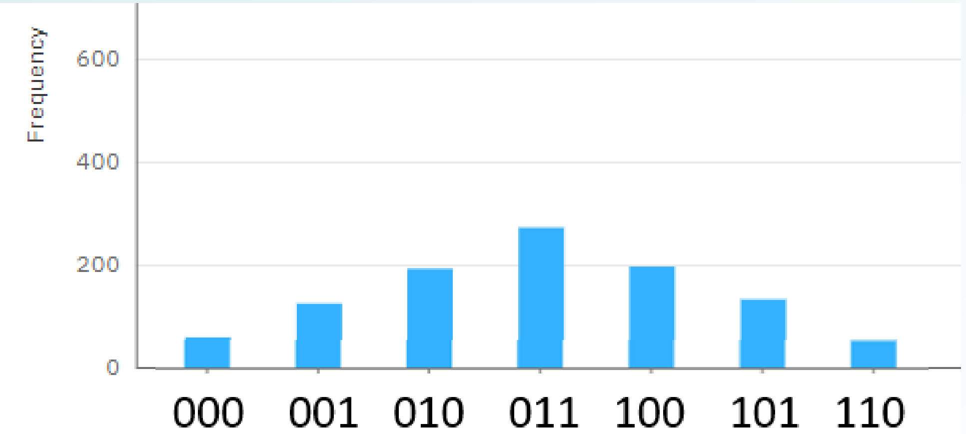

Additionnons 2 registres A et B (stockés sur 2 QuBits) dans S (3 QuBits)

A = |q4q0>   B = |q5q1>   S=|q6q3q2>

$c_2$ $c_1$
$b_1b_0$
$+ a_1a_0$
=========
$c_2s_1s_0$



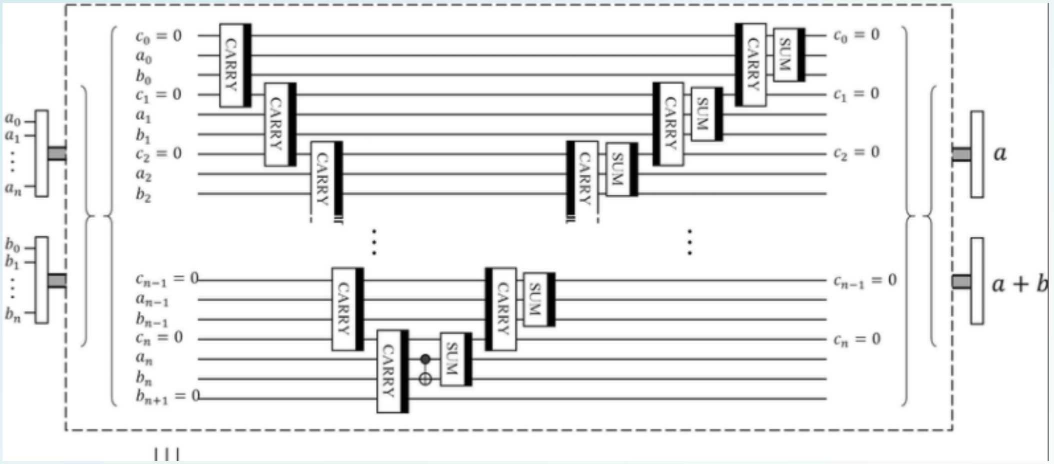

$a_0$
$b_0$
0 $..s_0$ ←
$..c_1..s_1$ ←
$a_1$
$b_1$
$..c_2$ ←




- Il « manque » l'état 111
- Les probabilités correspondent à la convolution des deux lois de probabilité uniforme … en 0(10)

# Dérivés de la somme

- Circuit itéré de la somme (et bien plus)
  - *« Quantum Networks for Elementary Arithmetic Operations », Vedral et al, Physical Review 95*
- Circuit optimisé de la somme
  - *Steven Cuccaro, Thomas Draper, Samuel Kutin, and David Moulton. A new quantum ripple-carry addition circuit. 11 2004. 15*
  - (a,b) => (a,a+b)+1 carry



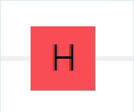

- Circuit de la soustraction
  - *Circuit de la somme de droite à gauche*
  - (a,b) => (a,b-a)
- Circuit de la comparaison
  - À partir de la soustraction, on test le résultat du carry : 0 si b≥a et 1 sinon, on inverse le carry (car on cherche le booleen a<b) puis on refait l'addition
  - (a,b) => (a,b-a)+carry=>(a,b)+carry « a < b »

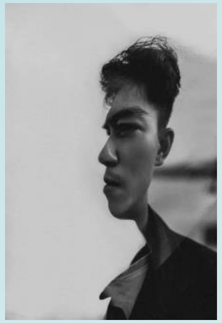
# Dualité Onde - Corpuscule

# L'informatique quantique

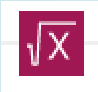

Bit d'info de profil

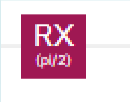
0 1

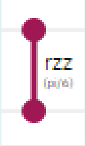


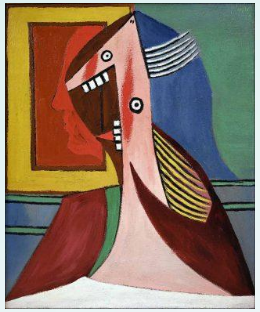



Superposition

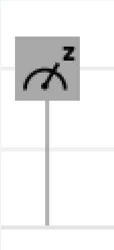


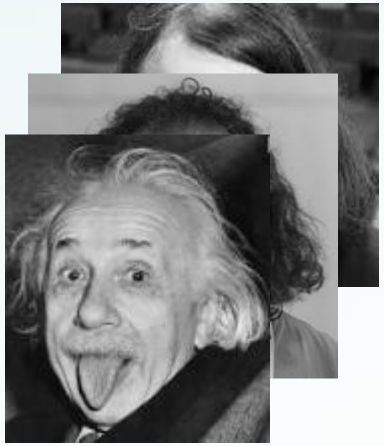



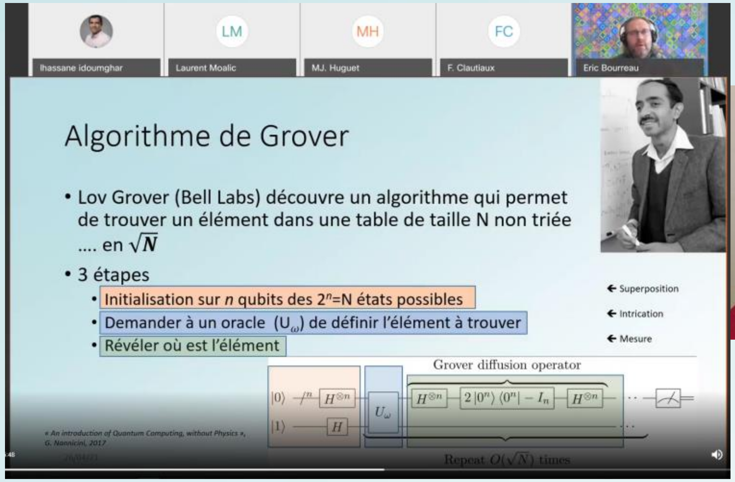



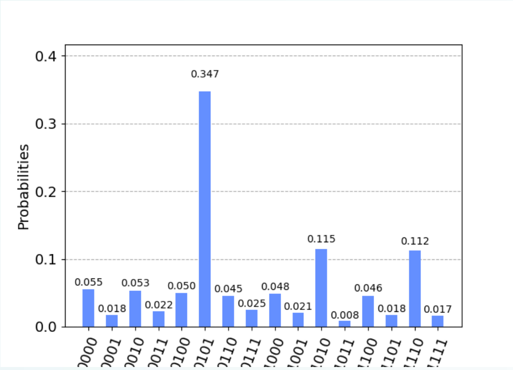
Déformation de la fonction d'onde




Mesure






https://roadef2021.sciencesconf.org/resource/page/id/11

Définition d'une Recherche Opérationelle Quantique (26/04/2021)

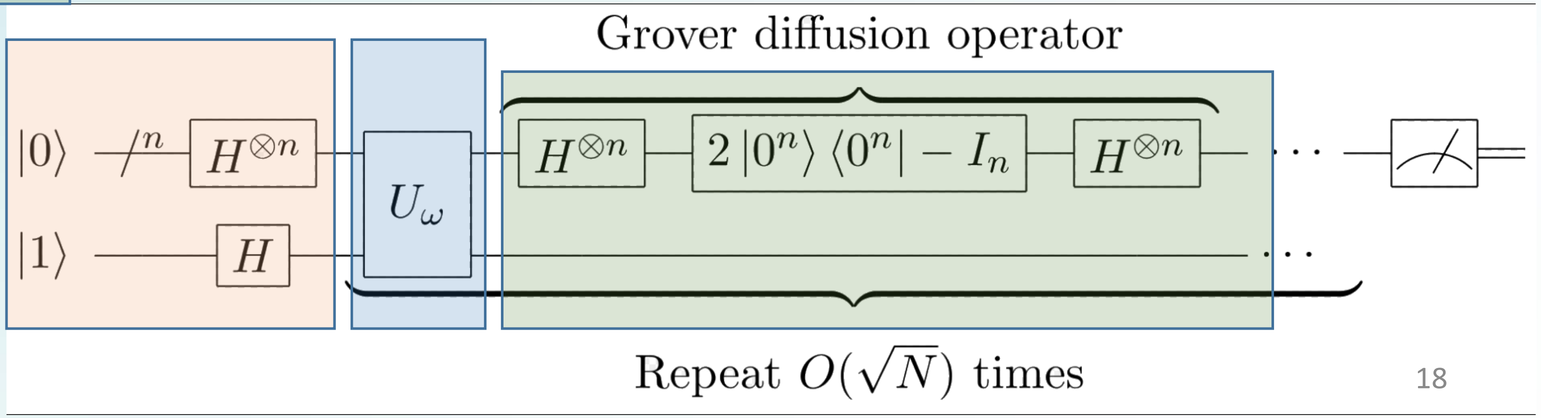
# Algorithme de Grover

- Lov Grover (Bell Labs) découvre un algorithme qui permet de trouver un élément dans une table de taille N non triée …. en $\sqrt{\boldsymbol{N}}$
- 3 étapes
  - Initialisation sur *n* qubits des $2^n$=N états possibles
  - Demander à un oracle ($U_\omega$) de définir l'élément à trouver
  - Révéler où est l'élément

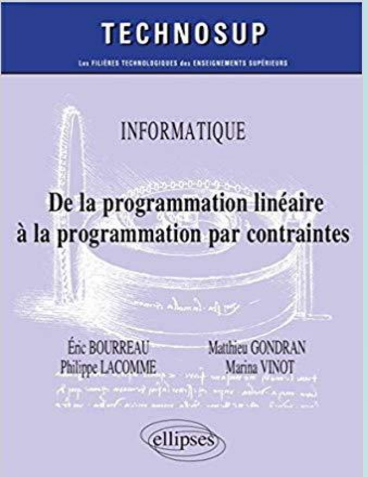
← Superposition

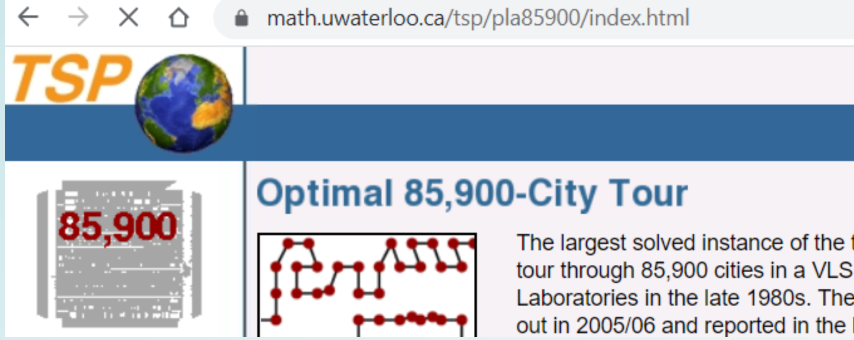
← Intrication

← Mesure




*« An introduction of Quantum Computing, without Physics », G. Nannicini, 2017*




# Voyageur de commerce

## 5.9 Modélisation PPC du TSP

### 5.9.1 Principe général

Une solution du TSP peut s'écrire sous la forme d'un vecteur $r$ : par exemple, $r = [2; 4; 5; 3,1]$ représente la tournée : 2-4-5-3-1 comme le montre la Figure 5-28.

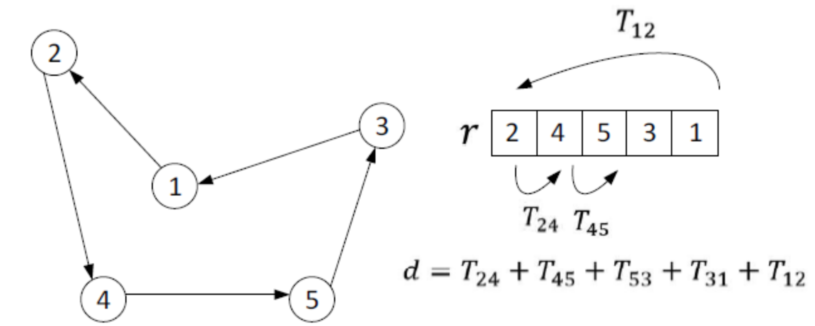


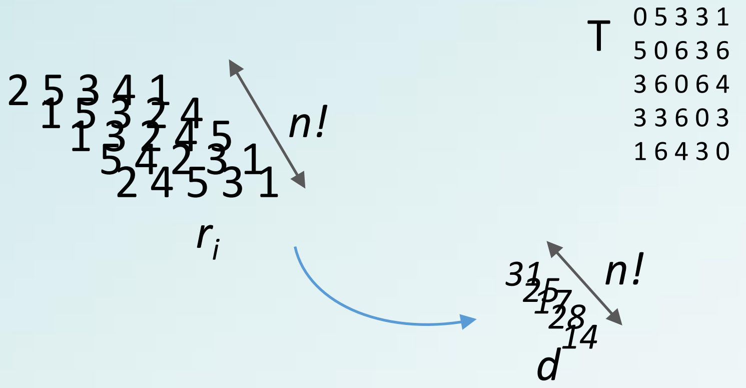

*Figure 5-28. Une solution modélisée avec le vecteur r*

Le coût d'une solution (distance totale) est la somme des distances à parcourir entre deux villes successives. Pour la tournée précédente, la distance est $d = T_{2,4} + T_{4,5} + T_{5,3} + T_{3,1} + T_{1,2}$.

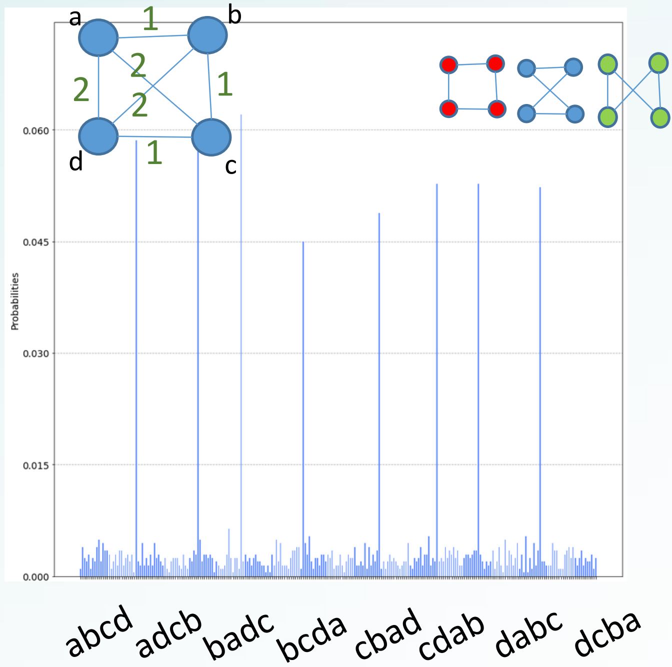
*Modélisation PPC du problème*

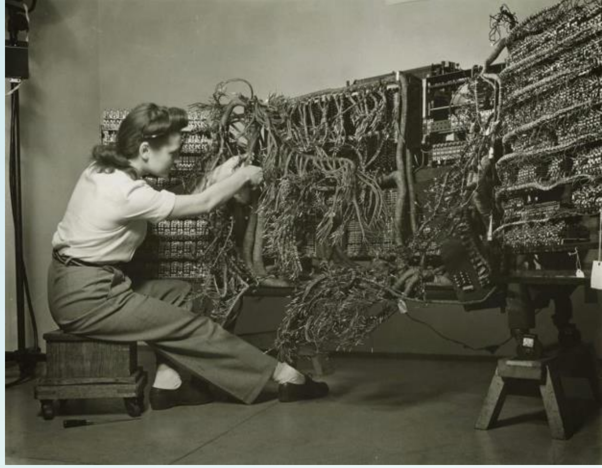
| | |
|---|---|
| $\forall i = 1..N$ | $r_i \in [1; n]$ |
| $\forall i = 1..N, \forall j = 1..N$ | $r_i \neq r_j$ |
| | $d = \sum_{i=1}^{N-1} T_{r_i r_{i+1}} + T_{r_N r_1}$ |
| | $Min\ d$ |

- Le problème consiste à visiter une et une seule fois chaque ville en minimisant la distance totale parcourue.
- Modélisation Quantique




- Minimiser somme sur i des $D_{P_i P_{i+1}}$
  ➔ accesseur d'une table
  (i,$P_i$,$P_{i+1}$, $D_{P_i P_{i+1}}$)
- Utiliser Grover pour exhiber le minimum de *d*



# Conclusion

- « En Informatique, la moitié des langages et des outils que vous utilisez actuellement auront disparus dans 5 ans. »

*Stephano Cerri, UM*

- L'informatique quantique est une réalité
- Cette présentation simplifie énormément (Clifford)