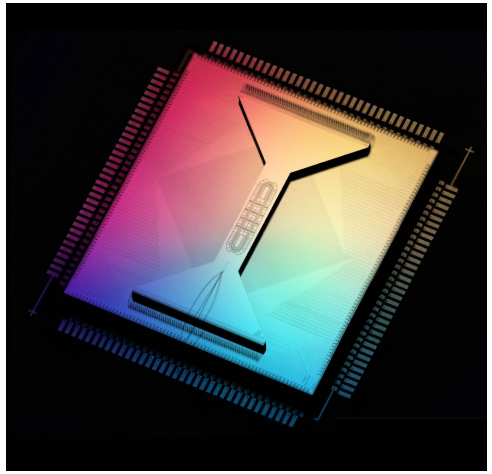
Cours 13

Introduction aux ordinateurs quantiques et au calcul quantique

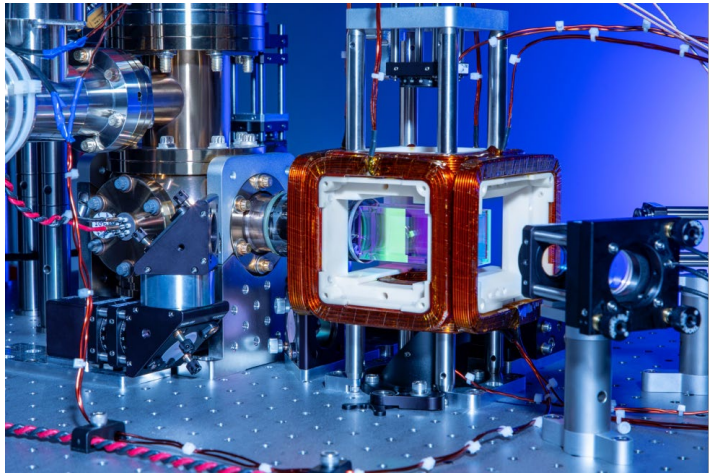
Les ordinateurs quantiques

Depuis les années 80, quand l'idée du calcul quantique a été proposée, les ordinateurs quantiques ont fait d'énormes progrès.



QPU à **ions piégés**
Quantinuum H2
32 quantum bits, mai 2023

QPU à **circuit supraconducteur**
IBM Heron
133 quantum bits, nov. 2023



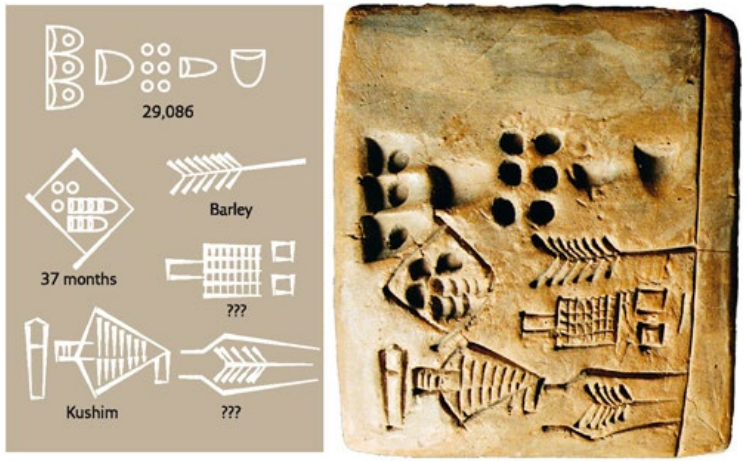
QPU à **atomes de Rydberg**
Quera Aquila
256 quantum bits, juin 2023

Qiskit

IBM Quantum Software Development Kit
https://www.ibm.com/quantum/qiskit

Nature physique de l’information

L’information est un phénomène physique. Tout mécanisme de **stockage**, **élaboration**, et **communication** de l’information se fait par le biais de systèmes qui sont régis par les lois de la physique.

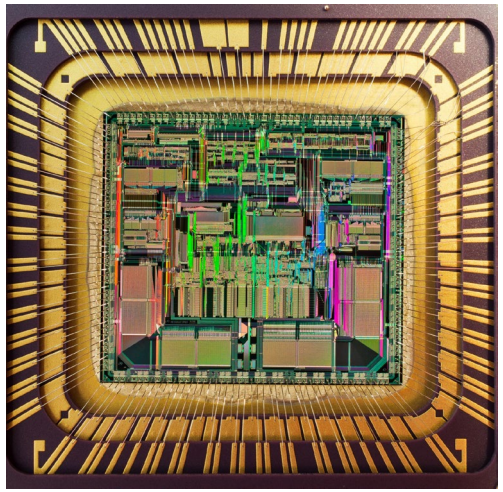


“Kushim” clay tablet (3400 – 3000 BC)

“Quipu” (3000 – 2000 BC)

Nature physique de l’information

L’information est un phénomène physique. Tout mécanisme de **stockage**, **élaboration**, et **communication** de l’information se fait par le biais de systèmes qui sont régis par les lois de la physique.



Actuellement, tout système de traitement de l’information se base sur les lois de la physique classique.

Les phénomènes de la nature sont régis par les lois de la physique quantique non relativiste.

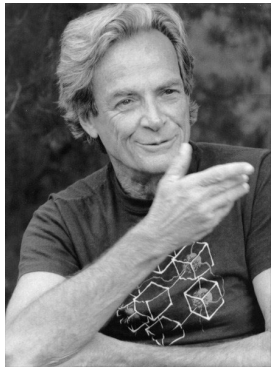
Les systèmes actuels n’utilisent pas la **superposition** et **l’intrication quantiques**.

Peut-on développer **un nouveau paradigme de calcul** en utilisant ces phénomènes?

L’aube du calcul quantique

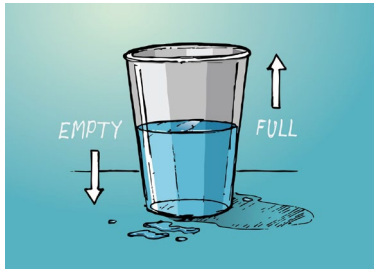
Le problème à N-corps en physique quantique est régi par **l’équation de Schrödinger dépendante du temps**.

Sa solution numérique est **un problème non tractable** par les ordinateurs classiques: le **temps** et la **mémoire** requis **augmentent exponentiellement** avec la taille N du problème.



“… nature isn’t classical, dammit, and if you want to make a simulation of nature, you’d better make it quantum mechanical, and by golly it’s a wonderful problem, because it doesn’t look so easy.”

Richard Feynman
Simulating physics with computers (1981)



Ce fait est **une ressource plutôt qu’une limitation**! La nature «résout» l’équation de Schrödinger indépendamment de la taille du problème! Si on pouvait «traduire» un problème computationnel en une équation de Schrödinger, et puis construire un système physique qui obéit à cette équation, alors le simple comportement de ce système au cours du temps nous donnerait la solution du problème computationnel!

Puisque l’équation de Schrödinger «sait faire» des tâches qu’on ne peut pas faire avec le calcul conventionnel, alors on peut s’attendre à un **avantage quantique** sur la solution de certains problèmes.

Notation

On indique l'état d'un système quantique par un symbole appelé **«ket»**: $|\psi\rangle$

Le symbole qu'on met dans le ket n'a pas nécessairement une signification mathématique. Il sert seulement à **évoquer de quel type d'état il s'agit**. Example:

$$|\psi\rangle = |\text{  }\rangle + |\text{  }\rangle$$

L'équation de Schrödinger dépendante du temps s'écrit, pour un opérateur Hamiltonien H, comme:

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle$$

Pour une condition initiale $|\psi(0)\rangle$ au temps t=0, on indique sa solution au temps t sous forme intégrale

$$|\psi(t)\rangle = U|\psi(0)\rangle$$

Où U est un opérateur (un opérateur différentiel si les états sont représentés par des fonctions d'onde). L'opérateur U est unitaire. Cela veut dire qu'il ne change pas la norme d'un état. On verra ce que cela implique dans le contexte des quantum bits plus tard.

Le paradigme classique de l'information

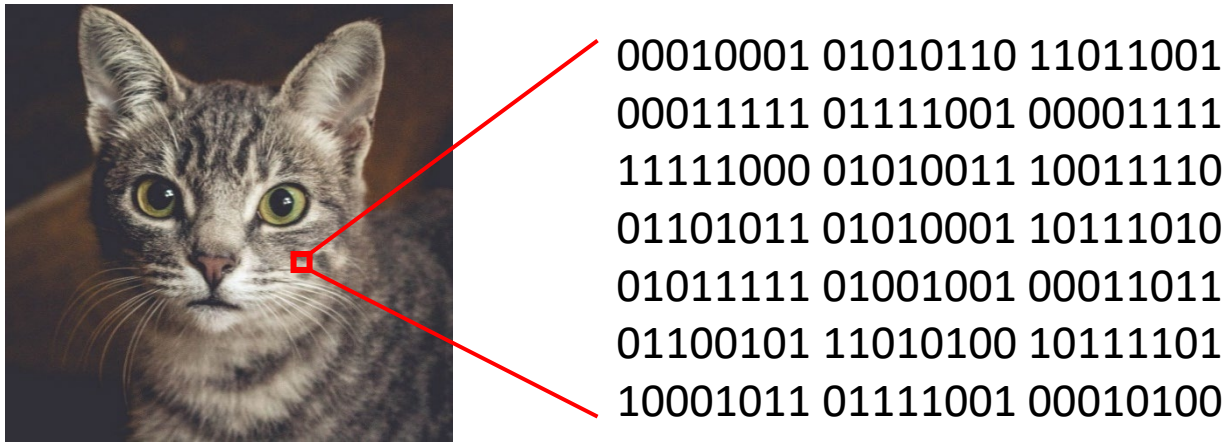
L'élément d'information classique est le « bit »: il peut prendre les valeurs **0** ou **1**

Un nombre peut être exprimé en code binaire: 42 = 101010

Tout type de données – par exemple une photo – peut être traduit en chiffres

Ensembles complets d'opérateurs: {NAND}, {NOR}, ou {AND, NOT}

Extended (physical) Church-Turing thesis: *Toute fonction physiquement calculable est calculable sur une machine de Turing à un coût polynomial*



00010001 01010110 11011001
00011111 01111001 00001111
11111000 01010011 10011110
01101011 01010001 10111010
01011111 01001001 00011011
01100101 11010100 10111101
10001011 01111001 00010100

Le quantum bit ou «qubit»

Un **qubit** est un système quantique qui ne peut prendre que deux états «classiques». Ces deux états sont indiqués par $|0\rangle$ et $|1\rangle$

Le **principe de superposition** en physique quantique dit que le qubit peut aussi se trouver dans un état de superposition du type

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \alpha,\,\beta \in \mathbb{C} \qquad |\alpha|^2 + |\beta|^2 = 1$$

Si on a **un système fait par n qubits**, alors les états «classiques» possibles sont simplement les combinaisons des états de chaque qubit:

$$|00\cdots0\rangle\,,\ |00\cdots1\rangle\,,\ \ldots,\ |11\cdots0\rangle\,,\ |11\cdots1\rangle$$

Le principe de superposition dit alors que **l'état le plus général d'un registre de n qubits** est

$$|\psi\rangle = \alpha_0\,|00\cdots0\rangle + \alpha_1\,|00\cdots1\rangle + \cdots + \alpha_{2^n-2}\,|11\cdots0\rangle + \alpha_{2^n-1}\,|11\cdots1\rangle$$

$$\alpha_j \in \mathbb{C} \qquad \sum_{j=0}^{2^n-1} |\alpha_j|^2 = 1$$

Etats séparables

Si deux qubits se trouvent chacun dans un état de superposition,

$$|\psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad\qquad |\psi_2\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$$

L'état du système fait par les deux qubits est

Produit tensoriel. Pas de panique!

$$\begin{aligned}|\psi\rangle &= |\psi_1\rangle \otimes |\psi_2\rangle \\ &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle) \\ &= \alpha\gamma\,|00\rangle + \beta\gamma\,|10\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|11\rangle\end{aligned}$$

Ici il faut juste retenir le fait que le produit tensoriel est distributif par rapport à la somme, tout comme la multiplication arithmétique.

Notation: $|x\rangle \otimes |y\rangle = |xy\rangle$

Etats non-séparables ou intriqués

L'état suivant de deux qubits:

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|11\rangle$$

Ne peut pas s'écrire comme un seul produit tensoriel du type vu avant

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

On dit qu'il n'est **pas séparable**, ou que **les deux qubits se trouvent dans un état intriqué**.

Ce fait a des implications physiques très importantes. En particulier, **il est impossible de répondre à la question: «quel est l'état du 1er qubit? (ou du 2ème ?)»**. **Seul l'état global des deux qubits est bien défini**.

Parmi tous les états possibles d'un registre fait de n qubits,

$$|\psi\rangle = \alpha_0\,|00\cdots0\rangle + \alpha_1\,|00\cdots1\rangle + \cdots + \alpha_{2^n-2}\,|11\cdots0\rangle + \alpha_{2^n-1}\,|11\cdots1\rangle$$

la **quasi-totalité de ces états sont non-séparables, donc intriqués**. Ce fait est à l'origine:

(1) de la difficulté de calculer la solution de l'équation de Schrödinger à n-corps,

(2) de **l'avantage quantique** que les ordinateurs quantiques offrent pour la solution de certains problèmes computationnels.

Comment réaliser un qubit?

Il y a plusieurs plateformes technologiques très prometteuses pour la réalisation des qubits. C'est un vaste domaine de recherche. Voici une liste (loin d'être complète)

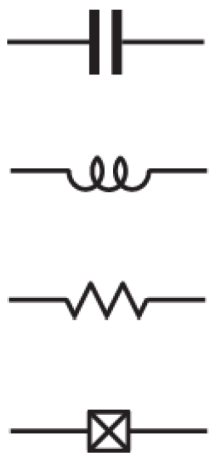
- Circuits supraconducteurs
- Ions piégés
- Atomes de Rydberg
- Spin des électrons dans les semiconducteurs
- Systèmes photoniques
- Qubits topologiques
- Spin des noyaux des atomes dans une molécule (NMR quantum computing)
- …

A présent ces trois technologies sont les seules qui permettent de réaliser des ordinateurs quantiques à plusieurs dizaines de qubits

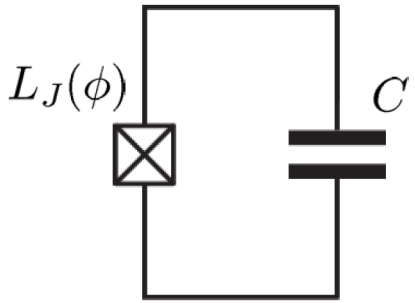
Circuits supraconducteurs

On peut réaliser un qubit avec un circuit supraconducteur, où **la résistance est zéro**. On réalise un simple **circuit LC**, où on peut produire un courant oscillant. Pour un oscillateur, la physique quantique prévoit des niveaux d'énergie quantifiés. On utilise une **inductance non-linéaire**, c.-à-d. où le courant n'est pas proportionnel au flux magnétique. Le résultat est que **les niveaux d'énergie ne sont pas espacés de manière uniforme**, et on peut utiliser les deux niveaux les plus bas comme états pour le qubit.

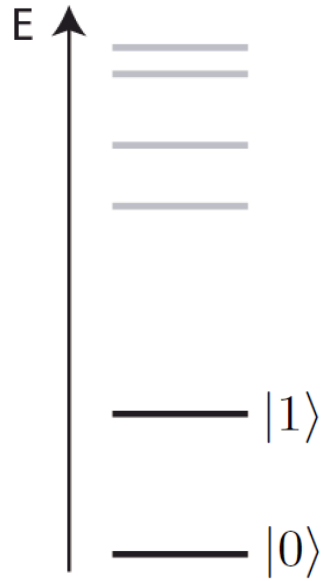
circuit elements:



anharmonic oscillator:



non-linear energy level spectrum:



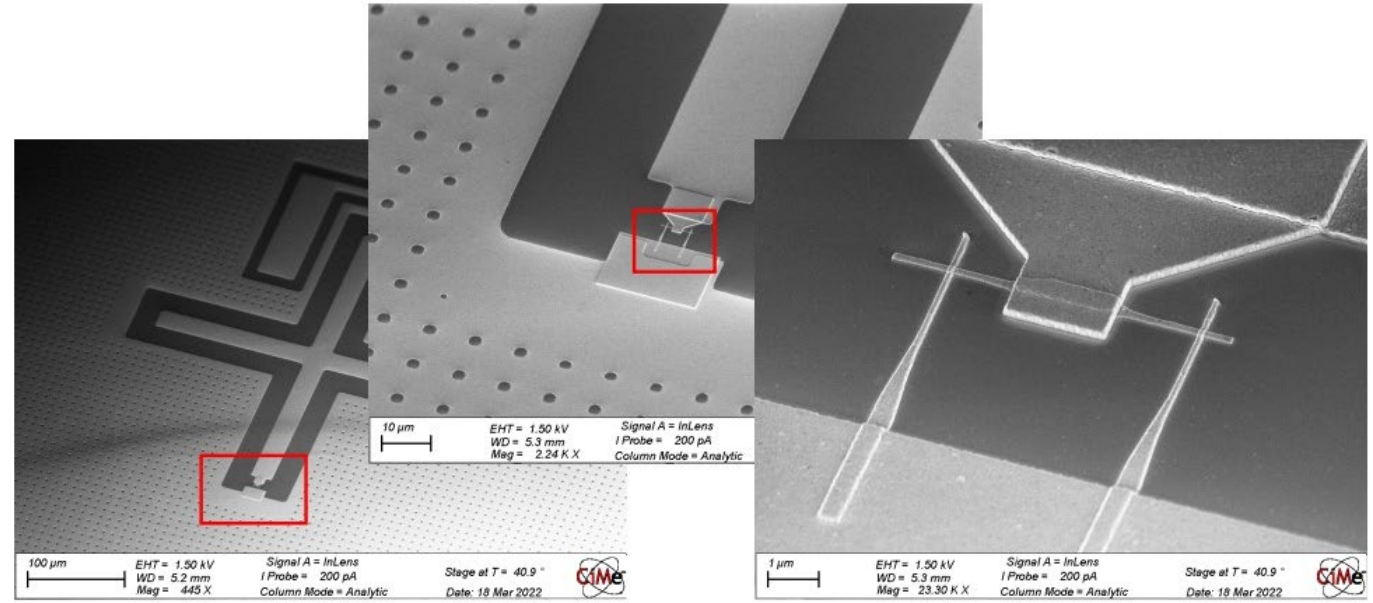
Josesphson junction:
a non-dissipative nonlinear element (inductor)

$$L_J(\phi) = \left(\frac{\partial I}{\partial \phi}\right)^{-1} = \frac{\phi_0}{2\pi I_c}\frac{1}{\cos(2\pi\phi/\phi_0)}$$

Circuits supraconducteurs

Le fait que le circuit est supraconducteur rend la superposition quantique plus robuste et donc utilisable. C'est ainsi qu'on peut fabriquer des ensembles de qubits. IBM Quantum a produit le plus grand processeur quantique, la puce Condor avec 1121 qubits en décembre 2023. Les ordinateurs quantiques de IBM Quantum sont disponibles en ligne (en accès limité). On les programme avec la librairie Qiskit basée sur python

QPU Condor de IBM (2023)



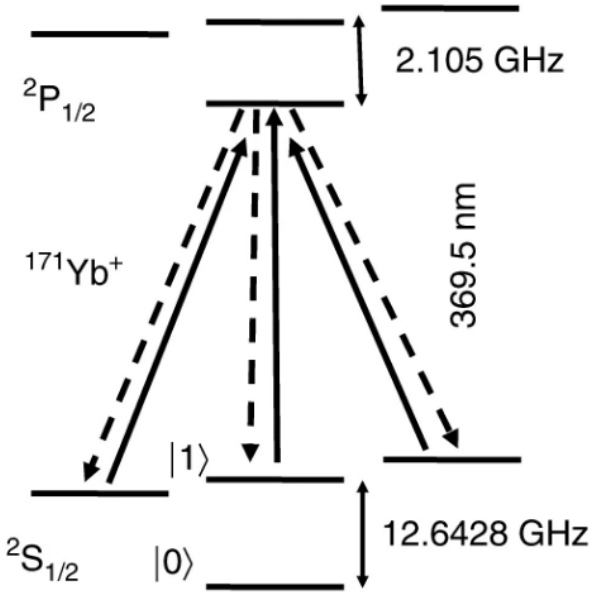
S. Frasca, *High-kinetic inductance superconducting technology for quantum applications*, PhD Thesis, EPFL, 2023

Un qubit supraconducteur réalisé à l'EPFL par P. Scarlino (2022)

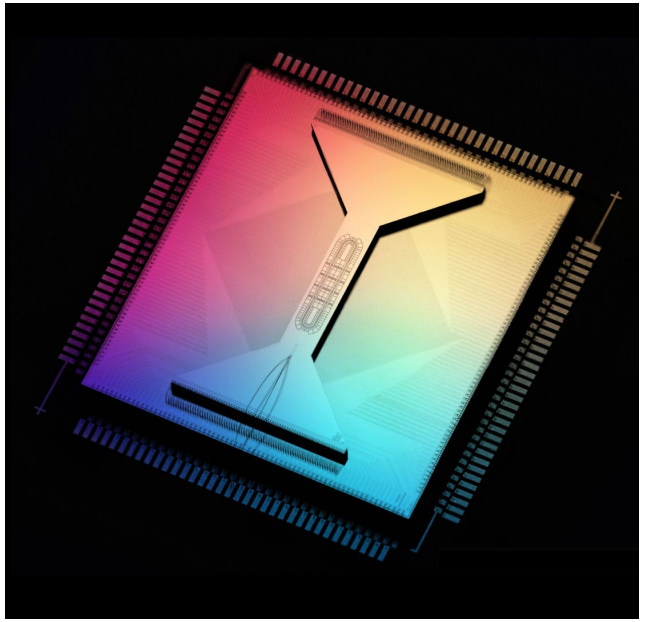
Ions piégés

Dans un ordinateur quantique à **ions piégés**, un qubit est fait par les deux niveaux d'énergie les plus bas d'un ion. On utilise des ions $^{171}Yb^{+}$ et les deux états avec m=0 de la **structure hyperfine** de l'ion.

La QPU Quantinuum H2, présentée en mai 2023, a 32 qubits, et les ions peuvent être déplacés sur un parcours, pour pouvoir approcher une paire arbitraire de ions. La proximité est nécessaire pour effectuer des **opérations à deux qubits**.



Niveaux d'énergie du ion $^{171}Yb^{+}$



QPU Quantinuum H2

Simple modèle de mesure

Qu'arrive-t-il si je lis le contenu d'un qubit? **« Lecture » = « Mesure »**

Supposons $|\psi\rangle = a|0\rangle + b|1\rangle$

Mesure: on suppose de se limiter à interroger la machine sur l'état du qubit **parmi ceux de la base computationnelle, soit 0 ou 1**

La mesure donne 0 ou 1 de façon aléatoire

Les probabilités sont $P(0) = |a|^2$ $P(1) = |b|^2$

Après la mesure l'état change (collapse). Le nouvel état est $|0\rangle$ si on mesure 0 et $|1\rangle$ si on mesure 1.

Pour plusieurs qubits: $|\psi\rangle = \sum_j a_j|j\rangle$

On obtient de façon aléatoire j avec probabilité $|a_j|^2$ et l'état après la mesure sera l'état $|j\rangle$

Simple modèle de mesure

Attention à la signification de « aléatoire »!

Après la mesure, et le collapse, la définition même de mesure vue avant nous dit qu'**une deuxième mesure (et toutes les mesures suivantes) donneront le même résultat**

« Aléatoire » signifie que, si nous préparons **plusieurs qubits** (ou plusieurs fois le même qubit), **dans le même état** $|\psi\rangle = a|0\rangle + b|1\rangle$, **la même mesure effectuée sur le même état donnera en général des valeurs différentes**

$$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow \text{mesure} \longrightarrow |0\rangle$$
$$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow \text{mesure} \longrightarrow |1\rangle$$
$$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow \text{mesure} \longrightarrow |1\rangle$$
$$|\psi\rangle = a|0\rangle + b|1\rangle \longrightarrow \text{mesure} \longrightarrow |0\rangle$$
$$\vdots$$

En général, le résultat d'un calcul quantique n'est pas déterminé. Les algorithmes quantiques doivent **exploiter cette caractéristique de manière utile**

Opérations quantiques sur un qubit

L'opération la plus générale qu'on peut effectuer sur l'état d'un qubit – qui **conserve sa norme, et compatible avec le principe de recouvrement** – est **un opérateur U unitaire**, c.-à-d. ayant la propriété $U^\dagger = U^{-1}$

Si $|\psi\rangle = a|0\rangle + b|1\rangle$ et $|\psi'\rangle = c|0\rangle + d|1\rangle$, alors en **notation matricielle**

$$\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = U \begin{pmatrix} a \\ b \end{pmatrix}$$

L'équation de Schrödinger, qui en physique quantique décrit **l'évolution d'un état d'un système dans le temps**, peut s'écrire sous la forme

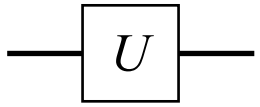
$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle \qquad U = e^{-iHt} \qquad (\hbar = 1)$$

Ici H est **l'opérateur hamiltonien** (l'énergie associée aux interactions et aux sollicitations externes) et est un opérateur unitaire

Donc une opération quantique est l'équivalent de l'évolution naturelle du système dans le temps, pour un hamiltonien donné

Notation des circuits quantiques

un qubit



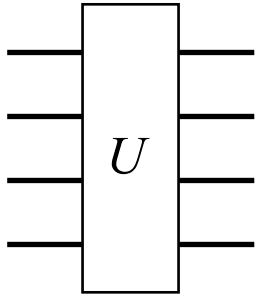
une porte logique quantique

Grâce au **principe de recouvrement**, il suffit de définir l'action de la porte logique sur **les états de la base computationnelle**

in	out
$\|0\rangle$	$\|\psi_0\rangle$
$\|1\rangle$	$\|\psi_1\rangle$

si en input $\quad |\psi\rangle = a|0\rangle + b|1\rangle$

en output $\quad |\psi'\rangle = a|\psi_0\rangle + b|\psi_1\rangle$



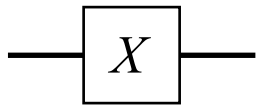
une porte logique à plusieurs qubits

il suffit de définir son action sur les états

$|00\ldots0\rangle,\ |00\ldots1\rangle,\ \ldots,\ |11\ldots1\rangle$

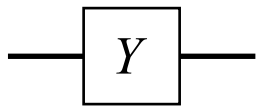
le principe de recouvrement fait le reste

Certaines opérations à un qubit



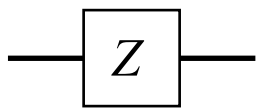
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

NOT

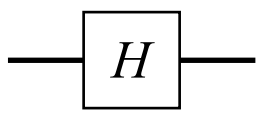


$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Pauli gates



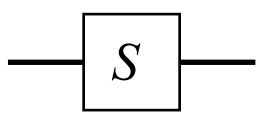
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

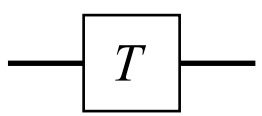
Hadamard gate

$$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$$
$$H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$$



$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

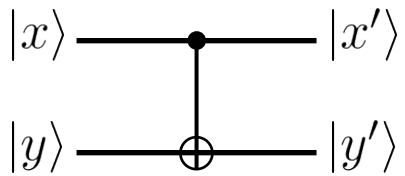
Phase gate



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

π/8 gate

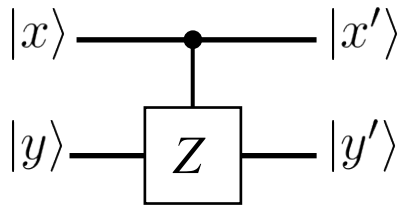
Certaines opérations à deux qubits



$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

x y	$x'y'$
0 0	0 0
0 1	0 1
1 0	1 1
1 1	1 0

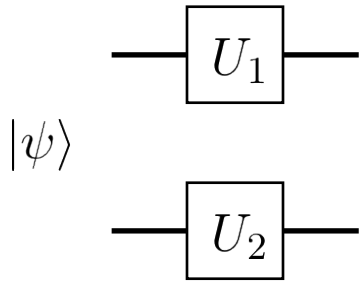
Le CNOT effectue un **NOT sur le 2ème qubit, à condition que le 1er qubit soit dans l'état 1**. Autrement, il ne fait rien. Le 1er qubit n'est pas modifié. Il agit sur les états superposition toujours selon le **principe de recouvrement**



$$\text{C-Z} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Le C-Z effectue un **Z sur le 2ème qubit, à condition que le 1er qubit soit 1**

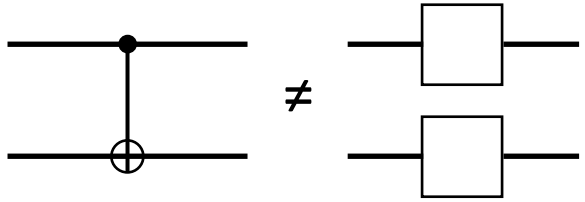
Séparabilité

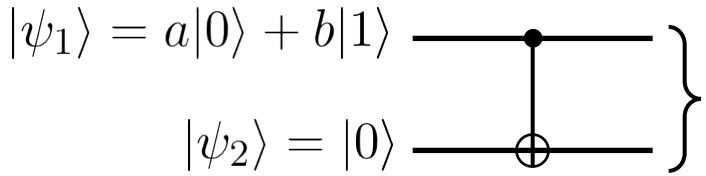


Si $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ alors $|\psi'\rangle = |\psi'_1\rangle \otimes |\psi'_2\rangle$

Une opération sur deux qubits $U = U_1 \otimes U_2$ qui est séparable, c.-à-d. composée de deux opérations distinctes à un qubit, **ne peut pas générer de l'intrication quantique**. Si l'input n'est pas intriqué, l'output ne le sera pas non plus

Le CNOT, par exemple, n'est pas séparable





Ensemble universel de portes logiques quantiques

En appliquant une séquence appropriée de portes logiques H et T, on peut **approximer avec précision arbitraire l'action d'une opération unitaire arbitraire U sur un qubit**

En appliquant une séquence appropriée de portes logiques H, T, et $CNOT$ (sur une paire arbitraire de qubits), on peut **approximer avec précision arbitraire l'action d'une opération unitaire arbitraire U sur plusieurs qubit**

En ajoutant la porte logique S, **l'ensemble {H, T, S, $CNOT$ }, est un ensemble universel de portes logiques quantiques** « fault tolerant »

Malheureusement, même si l'ensemble est universel, il n'est pas efficace: en général on a besoin d'un nombre de portes logiques élémentaires qui croit exponentiellement avec le nombre de qubits

Il faut chercher des « **algorithmes quantiques** », c.-à-d. des séquences limitées de portes logiques élémentaires qui effectuent des tâches utiles

A quoi sert un ordinateur quantique?

Une notion très populaire est le « **parallélisme quantique** »

$$|\psi\rangle = |\text{  }\rangle + |\text{  }\rangle + \ldots + |\text{  }\rangle$$

Un registre quantique peut en principe contenir une quantité d'information exponentiellement plus élevée qu'un registre classique.

Grâce à la superposition quantique, une opération serait alors effectuée « en parallèle » sur toute l'information contenue dans le registre. Hélas ce n'est pas si simple. La lecture de l'information produirait un collapse et effacerait la plupart de l'information à jamais.

readout

$$|\psi\rangle = |\text{  }\rangle + |\text{  }\rangle + \ldots + |\text{  }\rangle \quad \Rightarrow \quad |\psi\rangle = |\text{  }\rangle$$

L'argument du parallélisme quantique est faux! La conséquence est qu'une machine quantique universelle, capable d'effectuer toute tâche de manière plus efficace qu'un algorithme classique, n'est pas possible.

L'algorithmique quantique cherche des algorithmes quantiques qui permettent de tirer un avantage du parallélisme quantique en contournant le problème de la mesure.

Certains algorithmes avec avantage quantique

Algorithme de Shor.
Trouve les facteurs premiers d'un nombre entier à n-bits. Le nombre de portes logiques requises (donc le temps de calcul) est $O(n^2 \log(n) \log(\log(n)))$. Le meilleur algorithme classique demande un temps $\exp(O(n^{1/3} \log(n)^{2/3}))$. On a donc un **avantage exponentiel**! C'est l'algorithme vitrine de l'information quantique. **L'algorithme de partage de clés cryptographiques couramment utilisé sur internet – le RSA – dépend de cette complexité**

Algorithmes de Grover.
Recherche dans une base de données non ordonnée de taille N. Complexité $O(N^{1/2})$!!! Meilleur algorithme classique: O(N) L'impact sur tous les **problèmes d'optimisation, de recherche, d'intelligence artificielle**, etc., serait colossal!

Simulation quantique.
L'idée originale de Richard Feynman. Calculer $U = e^{-iHt}$ pour n qubits a une complexité $O(n^3 \log(n))$. Meilleur algorithme classique $O(2^n)$. Impact énorme sur la **recherche en matériaux, pharmacologie, environnement**, etc.

https://quantumalgorithmzoo.org/

L’ère NISQ

Le taux d’erreur actuel d’un qubit (supraconducteur) est d’environ **une erreur sur 1000 opérations** (1 erreur sur 10^{17} opération pour un transistor classique). La cause des erreurs est **l’influence aléatoire de l’environnement sur le système**. La superposition quantique, soumise à cette influence, est très fragile, ce qui explique le taux élevé d’erreurs dans les ordinateurs quantiques.

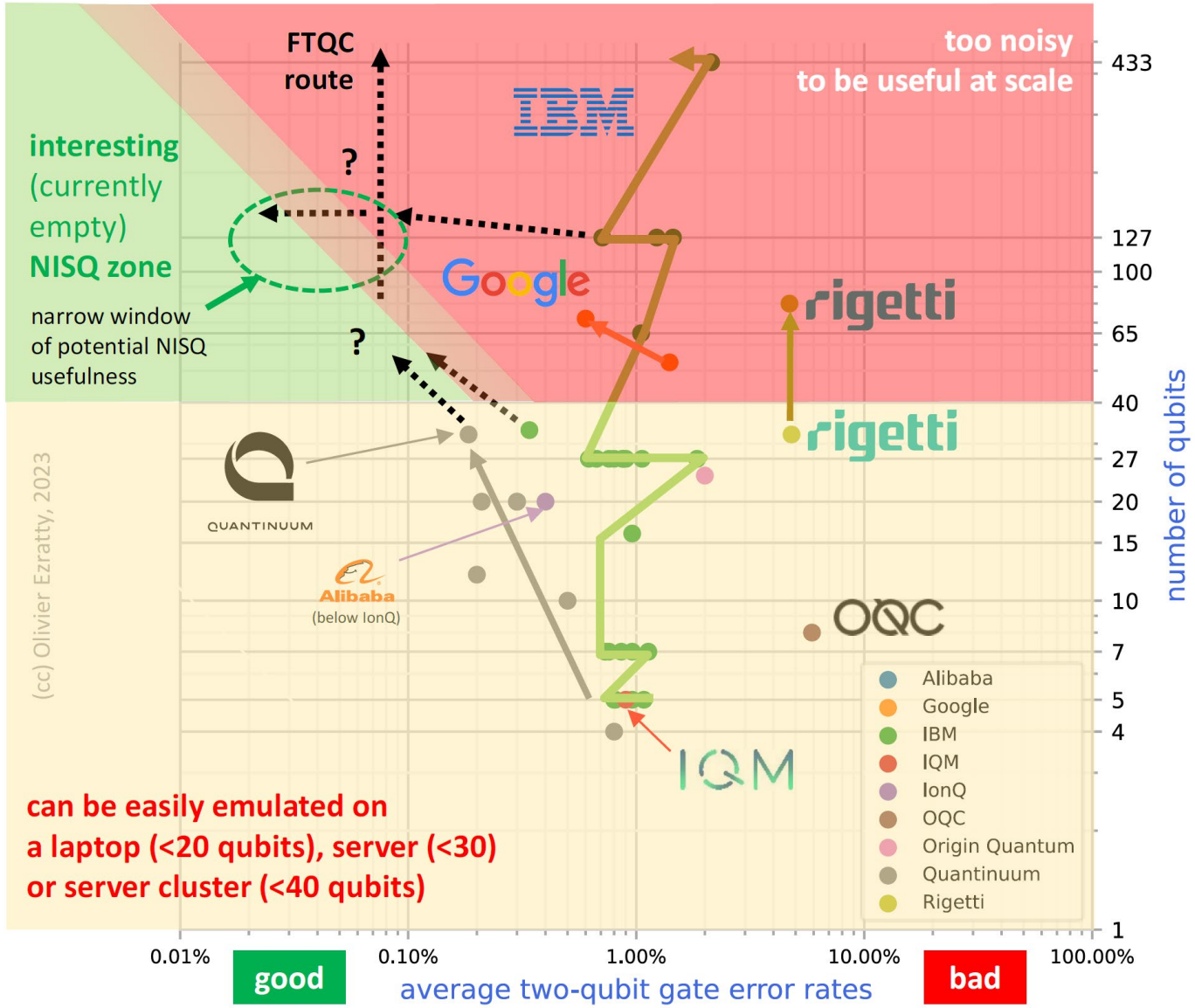
Le sujet de la **correction d’erreur quantique** est un vaste domaine de recherche. Un **ordinateur quantique qui peut corriger ses erreurs est dit «fault tolerant»**. A aujourd’hui nous ne sommes pas encore capables de construire des grands ordinateurs quantiques fault tolerant.

On peut par contre accepter les erreurs et espérer qu’ils ne vont pas trop compromettre le résultat des calculs. On le fait aussi pour les ordinateurs classiques. On parle alors de **Noisy Intermediate Scale Quantum technology (NISQ)**. Voir arXiv:1801.00862 , arXiv:2305.09518 .

Pour ce faire, on est limités à des algorithmes quantiques «petits», c.-à-d. peux de qubits et peux d’opérations, car le taux d’erreurs est par qubit et par opération.

On peut utiliser librement des ordinateurs quantiques NISQ en ligne. Mis à disposition par **IBM, Rigetti, Microsoft, Alibaba, etc**. On peut se servir d’un grand nombre de **kits de développement quantique**, comme **QisKit (IBM), Q# (MS)**, etc. Voir https://quantumcomputingreport.com/resources/tools/

L’ère NISQ



Extrait de arXiv:2305.09518

Certains algorithmes NISQ

Les algorithmes vus avant ont besoin pour fonctionner d'un ordinateur quantique fault tolerant.

Les algorithmes quantiques NISQ sont conçus pour donner un **résultat approximé même en présence d'erreurs**. Parmi les principaux algorithmes quantiques NISQ on a

Variational Quantum Eigensolver (VQE)

L'algorithme permet de **résoudre l'équation de Schrödinger stationnaire**, c.-à-d. **estimer les valeurs propres de l'énergie et les états stationnaires** correspondants, pour des systèmes quantiques à plusieurs corps en interaction

Quantum Approximate Optimization Algorithm (QAOA)

L'algorithme permet de trouver des **solutions approximées des problèmes d'optimisation combinatoire**, c.-à-d. où on cherche un minimum ou maximum d'une fonction de plusieurs variables discrète. Par exemple le **problème du voyageur de commerce**, ou le **protein folding**.

https://quantumalgorithmzoo.org/

A retenir

Le **paradigme de l'information quantique** est fortement basé sur le **principe de superposition** et sur **l'intrication quantique**

Il est possible de le traduire en un langage basé sur un **ensemble universel de portes quantiques élémentaires** à un et deux qubits

Avec ce paradigme on peut concevoir des **algorithmes quantiques** qui ont un **avantage quantique sur des tâches de calcul spécifiques** (pas de machine quantique universelle)

L'avantage consiste en une croissance du temps de calcul en fonction de la taille du problème qui est plus lente (parfois exponentiellement) qu'avec le meilleur algorithme classique. Les algorithmes quantiques connus sont très utiles

Les technologies quantiques actuelles sont basées sur les **circuits supraconducteurs** et sur les **ions piégés**. Ce sont des **technologies NISQ**

L'avantage quantique a été démontré plusieurs fois depuis 2019, mais dans des contextes très spécifiques. Tout le monde peut utiliser gratuitement des (petits) ordinateurs quantiques en ligne

Algorithme de Deutsch (1985)

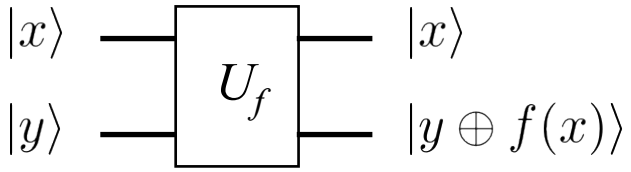
Supposons $y = f(x)$ avec $x, y \in \{0, 1\}$

On veut savoir si $f(x)$ est ou non dégénérée: $f(0) = f(1)$?

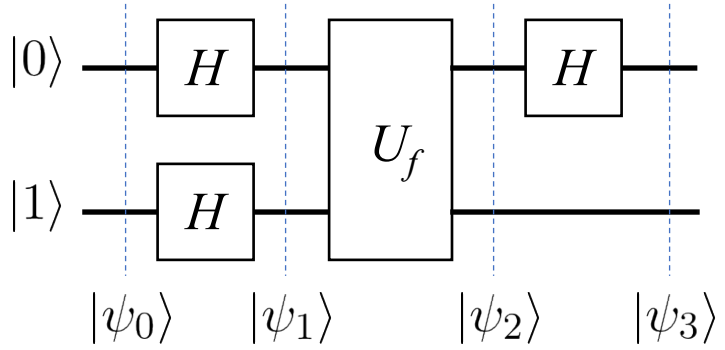
Evidemment, la seule approche classique possible demande que $f(x)$ soit calculée deux fois

L'algorithme de Deutsch le fait en calculant $f(x)$ une seule fois (sur un état de superposition, **grâce au principe de recouvrement**)

L'algorithme de Deutsch a besoin d'un « **oracle** ». Il s'agit d'une boîte noire qui effectue un CNOT conditionné à la valeur de $f(x)$



Algorithme de Deutsch (1985)



$$|\psi_0\rangle = |01\rangle$$

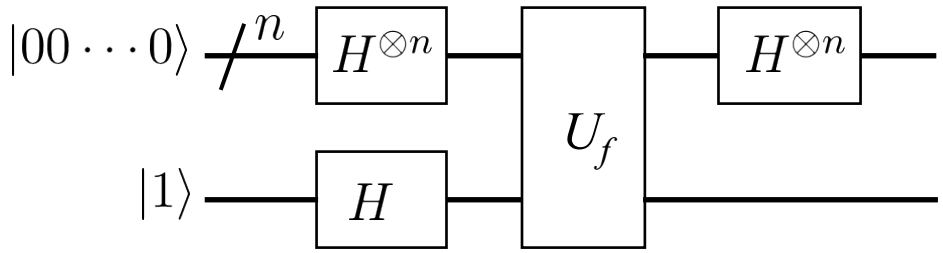
$$|\psi_1\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)$$

$$|\psi_2\rangle = \frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle)$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(-1)^{f(0)}|f(0) \oplus f(1)\rangle \otimes (|0\rangle - |1\rangle)$$

La mesure du 1er qubit donne, avec certitude, le résultat $f(0) \oplus f(1)$ qui correspond à l'information cherchée

Algorithme de Deutsch-Jozsa (1992)



Supposons $y = f(x)$ avec $y \in \{0, 1\}$ et $x \in \{0, 1, \ldots, 2^n - 1\}$

On sait que $f(x)$ est ou bien constante (même valeur pour tout x) ou équilibrée (vaut 0 pour la moitié des valeurs possibles de x et 1 pour l'autre moitié, mais on ne sait pas pour quelles valeurs)

Pire cas de l'approche classique: $2^{n-1}+1$ évaluations de $f(x)$

L'algorithme de Deutsch-Jozsa le fait toujours en une seule évaluation de $f(x)$

C'est un cas où le parallélisme quantique fonctionne. Ensemble avec l'algorithme de Deutsch, c'était la première preuve que **des algorithmes quantiques efficaces sont possibles. Met en doute la thèse de Church-Turing!**