Introduction à l'informatique quantique

Philippe DENIEL (philippe.deniel@cea.fr)

CEA / ENSIEE

2024

Introduction

De quoi va-t-on parler pendant ces 42 heures de cours ?

Plan

Quelques citations

Niels Bohr - Si la mécanique quantique ne vous a pas encore profondément choqué, alors vous ne l'avez pas encore comprise. Tout ce que nous appelons réel est fait de choses qui ne peuvent pas être considérées comme étant réelles.

Niels Bohr - Si une idée ne semble pas bizarre, il n'y a rien à espérer d'elle.

Heinz Pagels - Dieu a utilisé de merveilleuses mathématiques pour créer le monde.

Richard Feynmann - Je pense pouvoir dire sans trop me tromper que personne ne comprend la mécanique quantique.

Richard Feynmann, 1982 - Nature isn't classical, dammit, and if you want to make a simulation of nature, you better make it quantum mechanical

Albert Einstein - If you can't explain it simply, you don't understand it well enough

L'informatique quantique n'est pas si récente

Le *Quentum Computing* est né dans les années 80

- Une première conférence sur le QC au MIT en 1981
- Beaucoup d'études théoriques sur le QC
  - Algorithme de Shor, 1994
  - Algorithme de Grover, 1996

L'informatique quantique a de solides bases théoriques

- dans le domaine de la physique (physique quantique, physique statistique)
- dans le domaine des mathématiques (algèbre linéaire, algèbre hermitienne)

En revanche les implémentations physiques "réelles" des QPUs sont très récents.

Les liens entre informatique quantique et physique quantique

Le *Quantum Computing* est un nouveau paradigme informatique basé sur les phénomènes à la physique quantique :

1. la superposition,
   - qui permet d'induire une forme de parallélisme (à relativiser...)
2. l'intrication,
   - qui permet de coupler des systèmes simples pour de bâtir des systèmes plus complexes
3. les interférences,
   - qui permettent de mesurer les états quantiques et d'obtenir des résultats de calcul.

La première révolution quantique

La physique quantique est déjà très présente dans notre monde

- imagerie médicale : IRM (imagerie par résonance magnétique,
- composants électroniques : transistors à effet tunnel, LED,
- lasers,
- écrans LCD,
- panneaux solaires photovoltaïques : interaction photon/matière.

Le QC et la deuxième révolution quantique

L'informatique quantique fait partie de la deuxième révolution quantique

Les **QPU** commencent à apparaître sur le marché.

On prévoit plusieurs phases dans le QC

- NISQ : **N**oisy **I**ntermediate **S**cale **Q**uantum
- FTQC : **F**ault **T**olerant **Q**uantum **Q**uantum
- LSQ : **L**arge **S**cale **Q**uantum

On est actuellement dans la période NISQ

Ce que l'informatique quantique n'est pas.

Le QC ne va pas remplacer le HPC

- Les QPUs appartiennent à un nouveau paradigme du HPC, comme les GPUs.
- le QC est une nouvelle arme dans l'arsenal du HPC

Attention à la "hype" autour du QC, entretenue par certains constructeurs (dont IBM et Google)

- Des annonces "publicitaires", parfois éloignées de la réalité scientifique
- Des notions "grand public" aux contours souvent très flous...
- le QC ce n'est pas "faire 2^n calculs en même temps, le parallélisme exponentiel existe mais il est loin d'être systématique
- le QC est efficace pour caractériser rapidement une propriété globale d'un problème
  - périodicité d'une fonction entière (Shor)
  - parcours de graphe (marches quantiques)
  - Recherches d'optima de forme quadratiques (QUBO)

Plan

Les espaces de Hilbert

Un espace de Hilbert est un espace vectoriel sur les corps $\mathbb{R}$ ou $\mathbb{C}$ qui dispose des propriétés suivantes :

- il est euclien ou hermitien, c'est à dire qu'il dispose d'un produit scalaire (euclidien si basé sur $\mathbb{R}$, hermitien si base sur $\mathbb{C}$), ce dernier permet de définir une distance, mais aussi des notions d'angles et d'orthogonalité ;
- il est *complet*.

Dans un espace vectoriel *complet*, les suites de Cauchy convergent.

Suites de Cauchy

Les suites de Cauchy désignent les suites $(u_n)_{n\in\mathbb{N}}$ qui vérifient la propriété suivante (La fonction $d()$ désigne ici la distance dans l'espace de Hilbert) :

$$\lim_{p,q\to+\infty} d(r_p, r_q) = 0$$

Intuitivement, une suite de Cauchy est une suite dont les termes se rapprochent de plus en plus quant l'indice de la suite augmente. On a un espace de Hilbert quand ces suites convergent vers une valeur qui est dans l'espace en question.
En bref, un espace de Hilbert, c'est un espace vectoriel qui contient tous les "outils" mathématiques dont on a besoin pour y faire de l'analyse.

Plan

Rappels : les matrices

Une matrice à m lignes et n colonnes dont chaque case prend sa valeur dans un corps $\mathbb{K}$.
Dans le périmètre de ce cours, le corps en question sera toujours le corps des nombres complexes $\mathbb{C}$
On notera les éléments $a_{i,j}$ d'une matrice $A = (a_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}$ soit encore

$$A_{m,n} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} \end{pmatrix}$$

Rappels : matrices transposées et adjointes

La transposée d'une matrice A de taille m.n est notée A^t, c'est une matrice de taille n.m telle que

$$A' = (a'_{i,j})_{1\leq i\leq n, 1\leq j\leq m} = A^t, \forall i, 1 \leq i \leq m, \forall j, 1 \leq j \leq n, a'_{j,i} = a_{i,j}$$

La matrice adjoite d'une matrice A de taille m.n est notée A^*, c'est une matrice de taille n.m telle que

$$A' = (a'_{i,j})_{1\leq i\leq n, 1\leq j\leq m} = A^*, \forall i, 1 \leq i \leq m, \forall j, 1 \leq j \leq n, a'_{j,i} = \overline{a_{i,j}}$$

Matrice Adjointe = transposée + conjugaison

Rappels : trace d'une matrice

La trace d'une matrice carrée est une fonction qui associe à une matrice la somme des éléments sur sa diagonale. En termes mathématiques, on écrira

$$A = (a_{ij})_{1 \leq i,j \leq n}, Tr(A) = \sum_{i=1}^{n} a_{ii}$$

La trace possède différentes propriétés remarquables :

$$\begin{aligned} Tr(A+B) &= Tr(A) + Tr(B) \\ Tr(\alpha A) &= \alpha Tr(A) \\ Tr(A^t) &= Tr(A) \\ Tr(AB) &= Tr(BA) \end{aligned}$$

La trace est un *invariant de similitude*

$$Tr(PAP^{-1}) = Tr(APP^{-1}) = Tr(A)$$

Produit matriciel (usuel)

Le produit matriciel est plus complexe. Le produit est non-commutatif et il impose que le nombre de colonnes de l'élément de gauche est égale au nombre de lignes de l'élément de droite, on ne pourra donc former le produit $A \times B$ que si A est une matrice de taille $m \times n$ et B une matrice de taille $n \times p$. Le résultat est une matrice de taille $m \times p$.
Si $a_{i,j}, b_{i,j}$ et $c_{i,j}$, sont les coefficients des matrices A, B et C, le produit sera défini par

$$\forall i, 1 \leq i \leq m, \forall j, 1 \leq j \leq p, c_{i,j} = \sum_{k=1}^{n} a_{i,k}.b_{k,j}$$

Le produit matriciel standard n'est pas commutatif, il est associatif et distributif à droite et à gauche par rapport à la somme.

Produit de Kronecker 1/2

Le produit de Kronecker, ou produit tensoriel est très intuitif. Il n'est pas commutatif et peut agir sur tout couple de matrices, quelque soit leurs taillse.
Si A est une matrice $m \times n$ et N une matrice $p \times q$, le produit $C = A \otimes B$ sera une matrice de taille $mp \times nq$

$$A_{m,n} \otimes B_{p,q} = C_{mp,nq} = \begin{pmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,n}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1}B & a_{m,2}B & \cdots & a_{m,n}B \end{pmatrix}$$

Produit de Kronecker 2/2

Ce qui revient à écrire :

$$A_{m,n} \otimes B_{p,q} = \begin{pmatrix} a_{1,1}b_{1,1} & a_{1,1}b_{1,2} & \cdots & a_{1,1}b_{1,q} & \cdots & \cdots & a_{1,n}b_{1,1} & a_{1,n}b_{1,2} & \cdots & a_{1,n}b_{1,q} \\ a_{1,1}b_{2,1} & a_{1,1}b_{2,2} & \cdots & a_{1,1}b_{2,q} & \cdots & \cdots & a_{1,n}b_{2,1} & a_{1,n}b_{2,2} & \cdots & a_{1,n}b_{2,q} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{1,1}b_{p,1} & a_{1,1}b_{p,2} & \cdots & a_{1,1}b_{p,q} & \cdots & \cdots & a_{1,n}b_{p,1} & a_{1,n}b_{p,2} & \cdots & a_{1,n}b_{p,q} \\ \vdots & \vdots & \ddots & \vdots & & \vdots & & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{m,1}b_{1,1} & a_{m,1}b_{1,2} & \cdots & a_{m,1}b_{1,q} & \cdots & \cdots & a_{m,n}b_{1,1} & a_{m,n}b_{1,2} & \cdots & a_{m,n}b_{1,q} \\ a_{m,1}b_{2,1} & a_{m,1}b_{2,2} & \cdots & a_{m,1}b_{2,q} & \cdots & \cdots & a_{m,n}b_{2,1} & a_{m,n}b_{2,2} & \cdots & a_{m,n}b_{2,q} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{m,1}b_{p,1} & a_{m,1}b_{p,2} & \cdots & a_{m,1}b_{p,q} & \cdots & \cdots & a_{m,n}b_{p,1} & a_{m,n}b_{p,2} & \cdots & a_{m,n}b_{p,q} \end{pmatrix}$$

Exemple de produit tensoriel

Par exemple :

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} & 2 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} \\ 3 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} & 1 \times \begin{pmatrix} 0 & 3 \\ 2 & 1 \end{pmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} 1 \times 0 & 1 \times 3 & 2 \times 0 & 2 \times 3 \\ 1 \times 2 & 1 \times 1 & 2 \times 2 & 2 \times 1 \\ 3 \times 0 & 3 \times 3 & 1 \times 0 & 1 \times 3 \\ 3 \times 2 & 3 \times 1 & 1 \times 2 & 1 \times 1 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 3 & 0 & 6 \\ 2 & 1 & 4 & 2 \\ 0 & 9 & 0 & 3 \\ 6 & 3 & 2 & 1 \end{pmatrix}$$

Propriétés importantes du produit tensoriel

Le produit tensoriel a des propriétés notables vis-à-vis du produit matriciel classique et de la transposition :

$$(A \otimes B) \times (C \otimes D) = (A \times C) \otimes (B \times D)$$

$$(A \otimes B)^t = A^t \otimes B^t$$

Produit tensoriel d'espaces vectoriel - définition

Le produit tensoriel de matrice est intimement lié à une autre notion, celle de produit tensoriel d'espaces vectoriels. D'une manière très intuitive, un groupe ou un espace vectoriel sont des ensembles qui possèdent certaines structures qui leur donnent des propriétés intéressantes.

Si je dispose de deux ensemble A et B, je peux construire leur produit cartésien $A \times B$ dont les éléments seront des couples de la forme (x, y) avec $x \in A$ et $y \in B$. Le produit tensoriel, en approche simplifiée, permet de conserver les structures intéressantes des groupes ou des espaces vectoriels dans le produit cartésien.

Dans le cas des espaces vectoriels relatifs à un corps commutatif $\mathbb{K}$, on définira le produit tensoriel de deux espaces vectoriels E et F par l'existence d'une application bilinéaire Φ telle que :

$$\Phi : E \times F \longrightarrow E \otimes F$$

Les éléments de $E \otimes F$ sont définis par Φ en posant

$$\forall x \in E, \forall y \in F, x \otimes y = \Phi(x, y)$$

Produit tensoriel d'espace vectoriel - comment s'en servir ?

Le produit tensoriel peut être vue comme une astuce de notation car il permet de gérer des applications multilinéaires comme s'il s'agissait d'une application linéaire appliquée sur le produit tensoriel des espaces vectoriels source.

Considérons par exemple l'application bilinéaire g opérant sur $E \times F$, on peut lui adjoindre une unique forme linéaire$\hat{g}$ telle que $g = \hat{g} \circ \Phi$, où Φ représente l'isomorphisme entre $E \times F$ et $E \otimes F$. On a donc

$$\forall x \in E, \forall y \in F, g(x, y) = \hat{g}(x \otimes y)$$

On peut substituer à g, qui est bilinéaire, $\hat{g}$ qui est simplement linéaire. Grâce au produit tensoriel d'espaces vectoriels, traiter des formes multilinéaires revient à traiter de simples formes linéaires.

La dimension de l'espace produit tensoriel $E \otimes F$ est égal au produit des dimensions de E et F :

$$dim(E \otimes F) = dim(E).dim(F)$$

Retour sur le produit de Kronecker

Le lien entre le produit tensoriel d'espaces vectoriels et le produit tensoriel de matrices est canonique. En effet, connaissant une application linéaire sur E décrite par la matrice A, et une application linéaire décrite par la matrice B, je peux construire une application linéaire $A \otimes B$ sur $E \otimes F$ avec le produit de Kronecker.

La notation de produit tensoriel est très utilisée en informatique quantique. Elle servira beaucoup quand il s'agira de gérer de multiples qubits.

Attention : la notation $\otimes$ qui représente le produit tensoriel ne doit pas être confondue avec la notation $\oplus$ qui représente le XOR booléen.

Plan

Rappels - Série de Taylor 1/2

On rappelle que la fonction exponentielle peut s'écrire comme la série suivante (série de Taylor de la fonction exponentielle) :

$$\forall x \in \mathbb{R}, e^x = \sum_{n=0}^{+\infty} \frac{x^n}{n!}$$

Application à la trigonométrie
Si on y applique la série précédente à la forme $e^{i\theta}$:

$$\begin{aligned} e^{i\theta} = \sum_{n=0}^{+\infty} \frac{(i\theta)^n}{n!} &= \sum_{p=0}^{+\infty} \frac{(i\theta)^{2p}}{2p!} + \sum_{p=0}^{+\infty} \frac{(i\theta)^{2p+1}}{2p+1!} \\ &= \sum_{p=0}^{+\infty} \frac{(-1)^p.\theta^{2n}}{2p!} + i.\sum_{p=0}^{+\infty} \frac{(-1)^n\theta^{2p+1}}{2p+1!} \\ &= cos((\theta) + i.sin(\theta) \end{aligned}$$

Rappels - Série de Taylor 2/2

Par conséquent on peut en déduire les développements en série de Taylor des fonctions sinus et cosinus :

$$cos(x) = \sum_{n=0}^{+\infty} (-1)^n \frac{x^2 n}{(2n)!}$$

$$sin(x) = \sum_{n=0}^{+\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$$

Exponentielle de matrices

Comme on sait multiplier des matrices carrées et les ajouter, il est possible d'utiliser la série de Taylor de l'exponentielle sur les matrices carrées. On aura donc la définition suivante :

$$\forall A \text{ matrice carrée}, e^A = \sum_{n=0}^{+\infty} \frac{A^n}{n!}$$

Exponentielles de matrice et valeurs propres

Les valeurs propres d'une exponentielle de matrice sont les exponentielles des valeurs propres. Ce résultat est simple à voir. En effet, si D désigne la matrice diagonale dont les coefficients sont les valeurs propres, on a trivialement

$$\exists P, A = PDP^{-1}, \forall n \in \mathbb{N}, A^n = PD^nP^{-1}$$

Par conséquent,

$$e^A = \sum_{n=0}^{+\infty} \frac{A^n}{n!} = \sum_{n=0}^{+\infty} \frac{PD^nP^{-1}}{n!} = P(\sum_{n=0}^{+\infty} \frac{D^n}{n!})P^{-1} = P.e^D.P-1$$

On en déduit qu'une matrice et son exponentielle ont les mêmes vecteurs propres (et par ailleurs les mêmes vecteurs propres que toutes ses puissances).

ATTENTION A LA COMMUTATIVITÉ !!!!!!!

L'exponentielle de la somme de deux matrices n'est le produit des exponentielles des matrices que si celles-ci commutent.

$$\text{En général } e^{A+B} \neq e^{A}.e^{B} \text{ ce n'est vrai que si } AB = BA$$

Plus généralement, on dispose de la formule de *Glauber*

$$e^{X}e^{Y} = e^{X+Y+\frac{1}{2}[X,Y]}$$

Où $[X, Y]$ est le commutateur $[X, Y] = XY - YX$

Propriétés des exponentielles de matrices

L'exponentielle de la matrice nulle est la matrice identité : $e^0 = I$

Le déterminant de l'exponentielle d'une matrice est égal à l'exponentielle de sa trace :

$$det(e^X) = e^{Tr(X)}$$

Si Y est une matrice inversible alors

$$e^{YXY^{-1}} = Ye^X Y^{-1}$$

Plan

Produit scalaire euclidien et produit scalaire hermitien

Dans $\mathbb{R}^n$, on peut définir le produit scalaire (à valeurs dans $\mathbb{R}$) des vecteurs $x = (x_1, x_2, \cdots, x_n)$ et $y = (y_1, y_2, \cdots, y_n)$ par $x.y = x_1.y_1 + x_2.y_2 + \cdots + x_n.y_n = \sum_{k=1}^{n} x_k.y_k$

Dans $\mathbb{C}^n$, on définira le produit scalaire hermitien (à valeurs dans $\mathbb{C}$) des vecteurs $x = (x_1, x_2, \cdots, x_n)$ et $y = (y_1, y_2, \cdots, y_n)$ par $x.y = \overline{x_1}.y_1 + \overline{x_2}.y_2 + \cdots + \overline{x_n}.y_n = \sum_{k=1}^{n} \overline{x_k}.y_k$

On rappelle que si $x = a + i.b$ alors $\overline{x} = a - i.b$ est son conjugué.

Matrice adjointe

Étant donné une matrice $(a_{ij})_{1\leq i,j\leq n}$, sa matrice *adjointe* est la matrice conjuguée et transposée

$$A^{\dagger} = (a'_{ij})_{1\leq i,j\leq n},\ \text{adjointe de A}\ , \forall i,j, a'_{ij} = \overline{a_{ji}}$$

Un vecteur dans $\mathbb{C}^n$ peut être vu comme une "matrice colonne" avec n lignes et une seule colonne. Son adjoint est donc une "matrice ligne" avec une seule ligne et n colonnes. Le produit scalaire hermitien entre les deux vecteurs peut s'écrire comme le produit matriciel suivant :

$$\forall x \in \mathbb{C}^n, \forall y \in \mathbb{C}^n, x.y = x^{\dagger} \times y$$

Matrices hermitiennes et matrices unitaires

définition : matrice hermitienne Une matrice hermitienne est une matrice auto-adjointe, elle est également à sa matrice adjointe

$$A \text{ est une matrice hermitienne} \iff A = A^*$$

définition : matrice unitaire Une matrice unitaire U est telle que son inverse est sa matrice adjointe.

$$U^\dagger = U^{-1} \text{ soit } U \times U^\dagger = U^\dagger \times U = I$$

Une matrice peut être à la fois hermitienne et unitaire, c'est le cas des portes de la porte H et des portes de Pauli en particulier.

Propriétés des matrices hermitiennes

Une matrice hermitienne

- est diagonalisable et la matrice de passage est une matrice unitaire ;
- a des valeurs propres réelles (à valeurs dans $\mathbb{R}$) ;

Propriétés des matrices unitaires

Une matrice unitaire

- est inversible (et son inverse est sa matrice adjointe) ;
- est diagonalisable et la matrice de passage est une matrice unitaire ;
- possède une matrice adjointe qui est également unitaire (puisque étant son inverse) ;
- possède des colonnes qui forment une base orthonormale de $\mathbb{C}^n$ vis-à-vis du produit scalaire hermitien ;
- est normale (elle commute avec son adjointe, c'est évident puisque ce produit vaut l'identité) ;
- a des valeurs propres qui sont complexes (pas forcément réelles) mais dont la norme est égale à 1, elles sont donc toutes de la forme $e^{i\theta}$;
- possède un déterminant dont la valeur est 1 ;
- peut s'écrire sous la forme d'une exponentielle de matrice e^{iH} où H est une matrice hermitienne (et donc iH est anti-hermitienne).

Une matrice unitaire transforme une base orthonormale en une autre base orthonormale.

Matrices unitaires et produit scalaire

$$Ux.Uy = (Ux)^\dagger \times Uy = x\dagger \times U^\dagger \times U \times y$$
$$\text{mais U est unitaire donc } U^\dagger \times U = \mathbb{I} \text{ et par conséquent}$$
$$Ux.Uy = x^\dagger \times y = x.y$$

On a donc $Uy.Uy = x.y$

Les opérateurs unitaires conservent le produit scalaire, ce qui signifie qu'ils ne changent ni les normes ni les angles entre vecteurs.

Eléments de physique quantique ! !

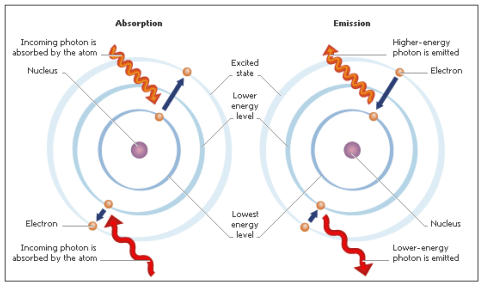
Disclaimer : ceci n'est pas un cours de physique quantique ! ! ! !

Plan

Quantas

Les objets quantiques n'évoluent pas de manière coninue. Ils possèdent différents états *discrets*, correspondant à des états énergétiques identifiés, séparés par des *quanta*.

Dans le cas des différents états d'excitation d'un électron, on aura la chose suivante :



L'électron ne "passe" pas d'une orbite à une autre, il est dans toutes les orbites à la fois, avec différentes probabilités de l'y trouver à cet endroit

Etats superposés

Un objet quantique est **simultanément** dans plusieurs états à la fois, c'est le phénomène de **superposition d'états**.

ATTENTION : ce concept est très contre-intuitif

- Les électrons sont sur plusieurs orbites d'un atome en même temps
- les particules ont des *spin* de valeurs inverses.. en même temps
- les photons peuvent avoir différentes sortes de polarisation ... en même temps
- un même photon peut être simultanément dans deux fibres optiques
- dans une boucle supraconductrice, le courant circulent à la fois dans le sens direct et dans le sens rétrograde

On identifie les états de base par des numéros. Un état $|\Psi\rangle$ sera une composition de ces états de la forme

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle + \delta\,|3\rangle$$

Effondrement quantique

En physique quantique, observer, c'est consommer de l'information. En observant un état superposé, on va effondrer celui-ci sur l'un des états de bases qui le composent. Ensuite, il ne bougera plus et restera à jamais ainsi, comme s'il avait "choisi sont camp".

Si on considère l'état du slide précédent

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle + \delta\,|3\rangle$$

L'observer donnera soit $|1\rangle$, $|2\rangle$, $|3\rangle$ ou $|4\rangle$.

Si on observe, par exemple $|3\rangle$, les mesure suivantes donneront **toujours** $|\Psi\rangle = |3\rangle$

Densités de probabilités

Dans la forrmulation

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle + \gamma\,|2\rangle + \delta\,|3\rangle$$

Les termes α à δ sont des nombres à valeurs dans $\mathbb{C}$, ou **densités de probabilités**.
Elles expriment les probabilités que $|\rangle\,\Psi$ est à la fois dans les états $|1\rangle$, à $|4\rangle$. Ce ne sont pas des probabilités "classiques", au sens de Kolmogorov.

Si on mesure $|\Psi\rangle$, il y a une probabilité $|\alpha|^2$ de mesurer $|0\rangle$, $|\beta|^2$ de mesurer $|1\rangle$, $|\gamma|^2$ de mesurer $|2\rangle$ et $|\delta|^2$ de mesurer $|3\rangle$

On a en revanche, il y a 100% de chances de mesure l'un des états, d'où la **condition de normalisation**

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

Si on sait reproduire $|\Psi\rangle$ à volonté, on peut, de manière probabiliste, connaître les valeurs des carrés des modules, en faisant suffisament de mesures.

Plan

Le paradoxe EPR

L'intrication est une notion fondamentale en physique quantique. Elle aa été sujette à de nombreuses controverses, dont le célèbre paradoxe EPR, dû à Einstein, Podolsky et Rosen.

Il faudra attendre 1982 et l'expérience de Alain Aspect pour clore le débat. Alain Aspect obtiendra par la suite le Prix Noble de Physique en 2022.

Qu'est-ce que l'intrication ?

Lorsque des objets quantiques interagissent, elles forment un système, ou **état intriqués**.

Les objets intriqués ne peuvent plus être considérés de manière autonome, il faut considérer l'ensemble du système intriqué, en particulier **agir sur une particule** c'est **agir sur l'état intriqué tout entier**.

En particulier, observer l'un quelconque des composants d'un état intriqué provoque son effondrement et l'effondrement de l'ensemble de l'état intriqué.

Plan

La programmation quantique, c'est quoi ?

La programmation quantique consiste à :

- utiliser la superposition pour accélérer le calcul sur n qubits
- utiliser l'intrication pour construire des interactions complexes
- **mais** on ne peut mesurer qu'un seul des 2^n état possible

La programmation quantique, c'est construire un opérateur unitaire, sur les qubits, tel que l'état mesuré, ou le plus probablement mesuré, représentera la solution cherchée pour le problème concerné.

La notation de Dirac

En informatique quantique, on utilisera la notation de Dirac. Les vecteurs de $\mathbb{C}^n$ ne seront pas notés x mais $|x\rangle$
Cette notation se nomme "ket", $|x\rangle$ se lira "ket x". Elle correspond à un vecteur écrit "en colonne" soit $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$.
L'adjoint d'un vecteur $x \in \mathbb{C}^n$ écrit en colonne est écrit "en ligne" , soit $x^\dagger = (\overline{x_1}, \overline{x_2}, \cdots, \overline{x_n})$
Avec la notation de Dirac, l'adjoint de $|x\rangle$ sera noté $\langle x|$, cette forme se nomme "bra" et lire "bra x".

Produit scalaire hermitien et notation de Dirac

Le produit scalaire hermitien peut être écrit comme le produit d'une matrice "ligne" et d'une matrice "colonne" :

$$\begin{aligned} x.y = \overline{x_1}.y_1 + \overline{x_2}.y_2 + \cdots + \overline{x_n}.y_n &= \sum_{k=1}^{n} \overline{x_k}.y_k \\ &= (\overline{x_1}, \overline{x_2}, \cdots, \overline{x_n}) \times \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \\ &= \langle x|y\rangle \end{aligned}$$

La norme d'un vecteur est quant à elle donnée par

$$\|x\| = \sqrt{\langle x|x\rangle}$$

Matrices et notation de Dirac

Si A est une matrice de $\mathbb{C}^{n\times n}$ représentant une application linéaire, le produit simplement noté $A|x\rangle$.

Si la matrice représente une forme hermitienne, elle est associée à une forme hermitienne F telle que

$$\forall x \in \mathbb{C}^n, \forall y \in \mathbb{C}^n, F(x,y) = x^\dagger A y$$

En utilisant la notation de Dirac, l'équation précédente s'écrira

$$\forall x \in \mathbb{C}^n, \forall y \in \mathbb{C}^n, F(x,y) = \langle x|A|y\rangle$$

Base canonique et notation de Dirac

L'espace vectoriel $\mathbb{C}^2$ dispose d'une base canonique : $\begin{pmatrix}1\\0\end{pmatrix}$ et $\begin{pmatrix}0\\1\end{pmatrix}$.

Dans la notation de Dirac, on écrira

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

Les vecteurs $|0\rangle$ et $|1\rangle$ forment la **base canonique** de $\mathbb{C}^2$.

ATTENTION ! ! ! !, le vecteur $|0\rangle$ n'est pas le vecteur nul : $\overrightarrow{0} = \begin{pmatrix}0\\0\end{pmatrix}$

Produit tensoriel et notation de Dirac

Quand on manipule plusieurs qubits, on va rapidement devoir manipuler des produits tensoriels de ces qubits.

$$\text{On notera } |0\rangle \otimes |0\rangle = |00\rangle \text{ et plus généralement si } (x, y) \in \{0, 1\}^2, |x\rangle \otimes |y\rangle = |xy\rangle$$

Le plus souvent, on n'utilise pas le symbole $\otimes$ qui devient implicite et on pourra écrire

$$|01\rangle\,|0\rangle = |010\rangle$$

Base canonique sur plusieurs qubits

Si l'on dispose de n qubits, on est dans $\mathbb{C}^{2^n}$, qui est isomorphe à $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$
On construit les bases canoniques en construisant les produits tensoriels avec les bases canoniques de $\mathbb{C}^2$. Ainsi $\mathbb{C}^4$ a comme base canonique $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1. \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0. \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1. \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0. \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Plan

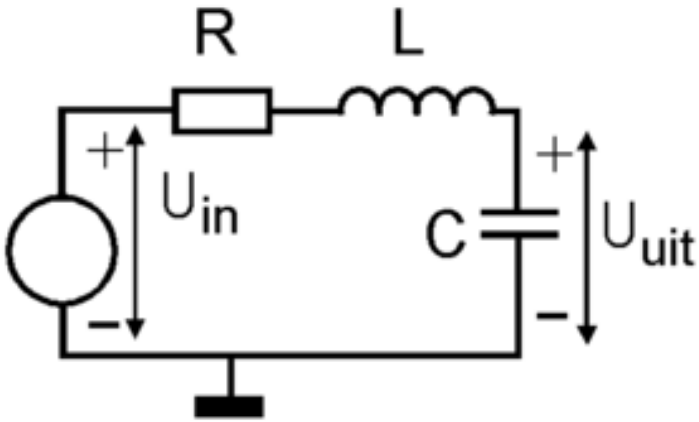
Programmation quantique à portes

Dans la programmation quantique à portes, on programme l'opérateur unitaire sous la forme d'un "circuit"

- le circuit est composé de différentes étapes,
- le circuit est un assemblage de composants génériques, plus simples.

ATTENTION : Un circuit quantique est une manière "graphique" de décrire une matrice $2^n \times 2^n$ potentiellement très complexe.

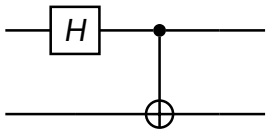
Ceci est un circuit (électrique)



Ceci n'est pas une pipe

Ceci n'est pas un circuit, ceci est une matrice

le circuit suivant construit une *paire EPR*



On verra que ce circuit correspond à la matrice

$$\frac{1}{2}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

Les qubits

Un qubit est un vecteur de $\mathbb{C}^2$, contrairement à un bit, il ne prend pas que les valeurs 0 et 1. Un qubit est un état quantique écrit ainsi

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

Les valeurs α et β sont des *densités de probabilité*, en mesurant $|\phi\rangle$ on aura

- la valeur $|0\rangle$ avec une probabilité de $|\alpha|^2$
- la valeur $|1\rangle$ avec une probabilité de $|\beta|^2$

Mesure d'un qubit et effondrement

On mesure un qubit $|\phi\rangle$ par rapport à une base orthonormée $(|v_1\rangle, |v_2\rangle)$ ou il s'écrit $|\phi\rangle = \alpha |v_1\rangle + \beta |v_2\rangle$ avec $|\alpha|^2 + |\beta|^2 = 1$

La mesure est effectuée grâce à un opérateur dont on peut mesurer les vecteurs propres. Mesurer un état provoque son *effondrement*. Après une mesure, le qubit s'effondre sur l'une de ses deux composantes, et il reste, il devient donc toujours soit $|v_1\rangle$ soit $|v_2\rangle$

Mesurer c'est **perdre de l'information**, mais on est obligé de faire des mesures pour avoir des résultats.

Plan

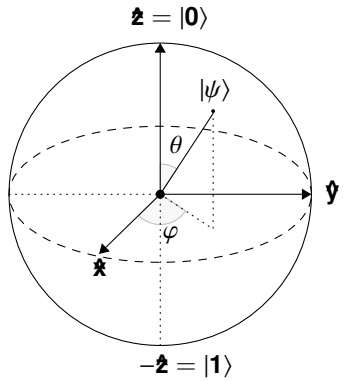
Zoologie des opérateurs sur 1 qubit

Les opérateurs sur 1 qubit sont des matrices unitaires dans $\mathbb{C}^{2\times 2}$
On va détailler

- la porte de Hadamard
- les portes de Pauli
- les portes de Clifford
- les portes paramétrées

La sphère de Bloch

La sphère de Bloch est un moyen classique de représenter un qubit. C'est la vue en perspective d'une projection d'un hyperplan à trois dimensions de $\mathbb{C}^2$



Construire la sphère de Bloch 1/2

Un état quantique est un vecteur $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ avec α et β des nombres complexes tels que $||\alpha||^2 + ||\beta||^2 = 1$. On peut noter α et β sous formes polaires

$$\exists! r_1 \in [0;1], \exists! \psi_1 \in [0;2\pi[, \alpha = r_1.e^{i\phi_1}$$
$$\exists! r_2 \in [0;1], \exists! \psi_2 \in [0;2\pi[, \beta = r_2.e^{i\phi_2}$$

et donc

$$\begin{aligned}|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle &= r_1.e^{i\phi_1}|0\rangle + r_2.e^{i\phi_2}|1\rangle \\ &= e^{i\phi_1}(r_1|0\rangle + r_2 e^{i(\phi_2-\phi_1)}|1\rangle) \\ &= e^{i\phi_1}(r_1|0\rangle + r_2 e^{i\phi}|1\rangle) \text{ avec } \phi = \phi_2 - \phi_1\end{aligned}$$

On ne peut pas mesurer la phase $e^{i\phi_1}$ dont la norme est 1, donc $|\Psi\rangle \equiv e^{-i\phi_1}|\Psi\rangle$, il est ond légitime d'ignorer le facteur $e^{i\phi_1}$ dans l'équation précédente et donc

$$|\Psi\rangle \equiv r_1|0\rangle + r_2 e^{i\phi}|1\rangle, r1, r2 \in [0;1], \phi \in [0;2\pi[$$

Construire la sphère de Bloch 2/2

Les carrés des modules composants en $|0\rangle$ et $|1\rangle$ vaut 1, par conséquent ${r_1}^2 + {r_2}^2 = 1$, ce qui est analogue à l'équation $cos^2(\theta) + sin^2(\theta) = 1$

Il est donc possible de trouver un angle θ tel que $r_1 = cos(\frac{\theta}{2})$ et $r_2 = sin(\frac{\theta}{2})$,

comme r_1 et r_2 sont dans $[0; 1]$ alors $\frac{\theta}{2}$ varie dans $[0, \pi]$. On peut donc écrire $|\Psi\rangle$ sous la forme $|\Psi\rangle = cos(\frac{\theta}{2})|0\rangle + sin(\frac{\theta}{2})e^{i\phi}|1\rangle$,

un état quantique est donc totalement défini par deux angles $\theta \in [0, \pi]$ et $\phi \in [0; 2\pi]$

Note : Une construction plus algébrique de la sphère de Bloch est possible, en exploitant le corps des quaternions.

La porte X, ou porte NOT

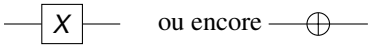
La porte X a les effets suivants sur la base canonique (bit flip)

- le qubit $|0\rangle$ devient $|1\rangle$, soit $X|0\rangle = |1\rangle$
- le qubit $|1\rangle$ devient $|0\rangle$, soit $X|1\rangle = |0\rangle$

La porte X est représentée par la matrice unitaire suivante

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

La porte X est représentée ainsi



La porte X réalise une **rotation** d'un angle π autour de l'axe X de la sphère de Bloch.

La porte Z

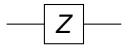
La porte Z a les effets suivants sur la base canonique (phase flip)

- le qubit $|0\rangle$ devient $0\rangle$, qui est invariant, soit $Z|0\rangle = |0\rangle$
- le qubit $|1\rangle$ devient $-|1\rangle$, soit $Z|1\rangle = -|1\rangle$

La porte Z est aussi appelée "porte d'inversion de phase" ou *phase flip*.
Elle est représentée par la matrice unitaire suivante

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

La porte Z est représentée ainsi



La porte Z réalise une **rotation** d'un angle π autour de l'axe Z de la sphère de Bloch.

La porte Y

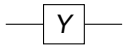
La porte Y a les effets suivants sur la base canonique

- le qubit $|0\rangle$ devient $i|1\rangle$, soit $Y|0\rangle = i|1\rangle$
- le qubit $|1\rangle$ devient $-i|0\rangle$, soit $Y|1\rangle = -i|0\rangle$

La porte Y réalise une **rotation** d'un angle π autour de l'axe Y de la sphère de Bloch.
Elle est représentée par la matrice unitaire suivante

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

La porte Y est représentée ainsi



$Y = iXZ$: Y est un bit filp (X), plus un phase flip (Z), plus une modification de phase.

Superposition

La base canonique n'est pas la seule base orthonormée de $\mathbb{C}^2$. Il est classique d'utiliser la base $|+\rangle, |-\rangle$ définie par

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

Ces deux états sont très importants car ils sont uniformément superposés, quand on mesure $|+\rangle$ ou $|-\rangle$ on a toujours

- $(\frac{1}{\sqrt{2}})^2 = 50\%$ de chance de mesurer $|0\rangle$
- 50% de chance de mesurer $|1\rangle$

On observera aussi que $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ et $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$

La porte H, ou porte de Hadamard

La porte de Hadamard est de loin la plus célèbre de toutes les portes quantiques et de loin l'une des plus utilisées. Elle doit son nom au mathématicien français Jacques Hadamard.

La porte H transforme la base $(|0\rangle, |1\rangle)$ en la base $(|+\rangle, |-\rangle)$ et inversement. Elle introduit la superposition d'états

- $H|0\rangle = |+\rangle$ et $H|1\rangle = |-\rangle$
- $H|+\rangle = |0\rangle$ et $H|-\rangle = |1\rangle$

La porte H est représentée par la matrice unitaire suivante

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

On remarquera que

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}) = \frac{1}{\sqrt{2}} (X + Z)$$

Racines carrées de portes

Toutes les portes à 1 qubits sont des rotations dans $\mathbb{C}^2$, elles ont des racines carrées.

La matrice $\sqrt{X} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$ est telle que son carré est la matrice X

Il est possible de trouver des racines n-ièmes de toutes les portes.

On verra comment ces portes sont utiles pour construire une boite à outils universelle permettant de construire toutes les portes à n qubits.

Plan

Représenter les états intriqués algébriquement

Certains états à n qubits peuvent se factoriser, par exemple

$$\frac{1}{2}(|00\rangle + |10\rangle - |01\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |+\rangle \otimes |-\rangle$$

En revanche, certains ne peuvent pas se factoriser, comme celui-ci (appelé **paire EPR**)

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Les états non factorisables ne permettent pas de manipuler les qubits un par un, il faut considérer les n qubits ensemble, ils correspondent aux **états intriqués**

L'espace vectoriel des états factorisables a pour dimension $2n$, à comparer à la dimension 2^n de l'espace des qubits

Il y a **beaucoup plus** d'états intriqués que d'états non-intriqués.

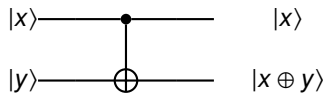
L'intrication et la porte CNOT

La porte CNOT, ou porte CX, est une porte NOT (ou porte X) qui agit sur le second qubit mais qui est contrôlée par le premier qubit.

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

L'effet d'une porte CNOT sur 2 qubit représenté par $|xy\rangle$ (x et 0 sont des bits) :

- si x = 0, ne pas toucher à $|y\rangle$, on obtient $|0y\rangle$ inchangé à la fin
- si x = 1, inverser y, on obtient donc $|1\neg y\rangle$



D'une manière synthétique, la porte CNOT ne touche pas le premier qubit $|x\rangle$ mais transforme le second qubit $|y\rangle$ en $|x \oplus y\rangle$.

Portes contrôlées (1/3)

La porte CNOT est la principale porte contrôlée. Les portes contrôlées

- permettent un traitement du type *if-then-else*
- s'appuient sur le phénomène d'intrication quantique

Si U est un opérateur unitaire de $\mathbb{C}^2$, il est algébriquement simple de définir une porte contrôlée CU qui est un opérateur unitaire de $\mathbb{C}^4$.
Considérons les *projecteurs* sur $|0\rangle$ et $|1\rangle$ (qui ne sont pas des opérateurs unitaires)

$$|0\rangle \times \langle 0| = \begin{pmatrix}1\\0\end{pmatrix} \times \begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix} \text{ et } |1\rangle \times \langle 1| = \begin{pmatrix}0\\1\end{pmatrix} \times \begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}$$

Alors la porte CU définie par

$$CU = (|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U$$

est une porte contrôlée unitaire : elle applique U sur le second qubit si le premier vaut $|1\rangle$

Portes contrôlées (2/3)

Il est simple de voir que CU est unitaire

$$CU = (|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U$$
$$= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes I + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes U = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

et

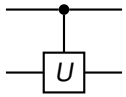
$$\begin{aligned} CU \times (CU)^\dagger &= (|0\rangle\langle 0| \otimes I + (|1\rangle\langle 1|) \otimes U) \times (|0\rangle\langle 0| \otimes I + (|1\rangle\langle 1|) \otimes U)^\dagger \\ &= (|0\rangle\langle 0|0\rangle\langle 0|) \otimes (I \times I) + (|1\rangle\langle 1|1\rangle\langle 1|) \otimes (U \times U^\dagger) + \\ &(|0\rangle\langle 0|1\rangle\langle 0|) \otimes (I \times U^\dagger) + (|1\rangle\langle 1|0\rangle\langle 0|) \otimes (U \times I) \\ &= (|0\rangle\langle 0|0\rangle\langle 0|) \otimes (I \times I) + (|1\rangle\langle 1|1\rangle\langle 1|) \otimes (U \times U^\dagger) \\ &= (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes I = I \otimes I = I \end{aligned}$$

Portes contrôlées (3/3)

$$\begin{aligned} CU|0x\rangle &= ((|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U) \times (|0\rangle \otimes |x\rangle) \\ &= (|0\rangle\langle 0|0\rangle \otimes I|x\rangle) + (|1\rangle\langle 1|0\rangle \otimes U|x\rangle) \\ &= |0\rangle \otimes I|x\rangle = |0\rangle \otimes |x\rangle = |0x\rangle \end{aligned}$$

$$\begin{aligned} CU|1x\rangle &= ((|0\rangle \times \langle 0|) \otimes I + (|1\rangle \times \langle 1|) \otimes U) \times (|1\rangle \otimes |x\rangle) \\ &= (|0\rangle\langle 0|1\rangle \otimes I|x\rangle) + (|1\rangle\langle 1|1\rangle \otimes U|x\rangle) \\ &= |1\rangle \otimes U|x\rangle = |1\rangle \otimes U|x\rangle \end{aligned}$$

Un porte U contrôlée sera dessinée comme ceci dans les circuits quantiques :



Il est légitime de faire des portes doublement contrôlées

Porte de Toffoli

La porte de Toffoli est une porte opérant sur 3 qubits, c'est une porte CCNOT (NOT à double contrôle)

$$CCX = \begin{pmatrix} I & 0 \\ 0 & CX \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Son effet est le suivant :