L’ordinateur quantique.

Richard Feynman

Charles Bennett

L'ordinateur quantique : pour quoi faire ?

La théorie classique de l'information a été décrite par ailleurs. Elle est basée sur l'existence de la notion de bit, une variable discrète pouvant prendre deux états contrastés, notés '0' et '1'. La notion d'information est aussi fondamentale, en physique, que l'énergie : nous avons vu, dans l'exposé consacré à la thermodynamique, qu'en la reliant intimement à la notion d'entropie, elle lui consacre un principe d'égale importance.

Cette théorie n'est pas seulement un modèle abstrait décrivant la meilleure manière de stocker, de traiter et d'échanger de l'information. Elle présente également de nombreuses applications pratiques qui gravitent toutes dans le domaine de l'informatique appliquée. L'ordinateur joue pour l'information un rôle comparable à celui que le moteur joue vis-à-vis de l'énergie : l'un comme l'autre permettent d'illustrer concrètement le principe de la physique auxquels ils sont étroitement associés.

D'une manière générale, la théorie de l'information ne se préoccupe pas de la propriété physique qui réalise l'encodage des bits au sein d'un système donné, l'ordinateur, par exemple. La physique classique offre, à cet égard, une infinité de possibilités parmi lesquelles les concepteurs de l'ordinateur de l'an 2000 ont dû faire un choix. Ils ont clairement adopté les systèmes à deux états de tension électrique. Aucun modèle alternatif n'est sinon à l'étude, du moins en passe de supplanter rapidement le système transistorisé.

Si l'ordinateur classique existe, avec des performances que nous jugeons acceptables, il a pourtant ses faiblesses :

- Il est terriblement entropogène par rapport à ce qu'exigent les lois de la physique et cela se manifeste par une dissipation excessive de chaleur dans l'environnement. Ce point a été abondamment discuté dans le chapitre réservé à la thermodynamique du calcul et nous y avons vu un obstacle sérieux à une miniaturisation poussée toujours plus loin.

- Une autre faiblesse est qu'il épouse le schéma de la machine de Turing classique et qu'à ce titre il effectue ses calculs en séquence. La conséquence est qu'il est impuissant à démêler, dans un temps raisonnable, un grand nombre d'instances des problèmes NP.

Feynman fut le premier à réfléchir aux avantages que présenterait la construction d'un ordinateur où l'encodage du bit serait miniaturisé à l'échelle atomique. Naturellement les lois auxquelles obéirait une telle machine seraient les lois quantiques mais précisément il y a vu la possibilité d'optimiser de façon définitive le traitement de l'information.

En encodant l'information au niveau atomique, il est clair qu'on atteint la miniaturisation maximale désirée et que, de plus, on évite les sources de dissipation habituellement liées aux frottements macroscopiques. Mais il y a mieux car nous verrons qu'au niveau du traitement de cette information, les performances de l'ordinateur quantique sont théoriquement très supérieures à celles de l'ordinateur classique : le calcul séquentiel est en effet remplacé par un calcul massivement parallèle qui ouvre, de ce fait, la voie à une résolution rapide des instances ardues des problèmes NP avec toutes les conséquences bouleversantes que cela aurait, en particulier dans le domaine de la cryptographie.

En cette matière, le conditionnel est tout à fait de rigueur car l'ordinateur quantique n'est actuellement guère plus qu'un rêve même si aucune loi connue de la physique n'interdit

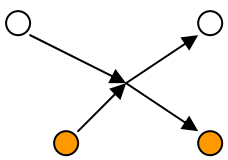
d'espérer le réaliser un jour. Les études théoriques ont bien avancé mais la technologie ne suit pas et il n'est pas du tout certain qu'elle rattrapera un jour son retard. Le problème majeur qui se pose est le revers de la médaille à l'absence de dissipation. Car si les frottements sont souvent ressentis comme une gêne, ils ont aussi leurs beaux côtés : ils sont souvent les garants d'une stabilité bien nécessaire du fait qu'ils offrent une protection naturelle contre les bruits. On peut, par exemple, encoder classiquement un bit en décidant de charger ou non un condensateur sous une tension de 5V. On sait que les charges et décharges successives de ce condensateur entraîneront une dissipation de chaleur dans la résistance de charge mais au moins on a la certitude qu'aucune fluctuation raisonnable de tension due à l'environnement ne viendra jamais fausser l'encodage. On voit bien qu'en passant de 5V à 0.5V, on diminuerait la dissipation mais on augmenterait simultanément, de façon préoccupante, le risque de perturbation externe.

Tout cela cesse d'être vrai à l'échelle quantique où l'absence de dissipation exige l'isolation parfaite du système vis-à-vis de l'environnement et ce problème majeur n'est pas résolu à ce jour. Actuellement, en 2005, on est en mesure de maintenir la cohérence de 6 ou 7 qubits (nom donné aux bits quantiques) maximum alors qu'il en faudrait quelques centaines pour entrer dans le domaine de l'application pointue.

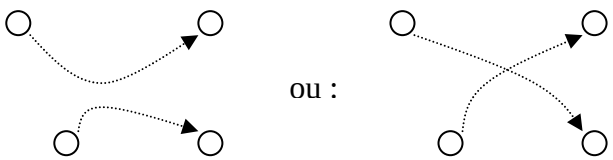
Pour comprendre ce qui différencie l'ordinateur quantique de son homologue classique, il est nécessaire de se remémorer le détail des principes de la mécanique quantique. On se souvient qu'une particularité du qubit isolé, par rapport au bit classique, est de pouvoir exister dans des états de superposition linéaire. Mais il y a plus : lorsqu'on considère simultanément plusieurs qubits confinés, ils sont indiscernables au point d'enchevêtrer (on dit aussi intriquer) leur vecteur d'état commun. C'est assurément la possibilité d'intriquer plusieurs qubits qui rend prometteur le traitement quantique de l'information. En revanche, la fragilité de cette intrication fait que des systèmes quelque peu complexes brisent aisément leur cohérence et rejoignent le monde classique. Précisons en quoi l'intrication est au cœur de la différence de performances entre les ordinateurs classique et quantique. Un détour s'impose par un postulat supplémentaire de la mécanique quantique : le principe d'indiscernabilité.

Le principe d'indiscernabilité.

Une conséquence inattendue du principe d'incertitude concerne l'indiscernabilité des particules identiques. Dans le monde macroscopique, les boules de billard peuvent se ressembler autant que l'on veut, il y a toujours moyen de les suivre à la trace sans perturber leur mouvement de manière appréciable en sorte que lors d'une collision, par exemple, il est parfaitement possible de dire quelle boule entrante sort sous un angle déterminé. Cela n'est plus vrai du tout avec des électrons puisque la notion même de trajectoire a perdu toute signification : le problème n'est pas tant qu'on serait incapable de les « voir » avec une sonde appropriée mais bien que cette sonde chamboulerait complètement leur état.



boules de billard



électrons

L'exemple suivant aide à comprendre la différence de comportements des objets classiques et quantiques.

Système planétaire à trois corps. Deux planètes qui gravitent autour d'une même étoile forment un système à trois corps qui possèdent leur individualité propre, que les équations de la mécanique respectent en les traitant séparément. Autrement dit, ce système peut être décomposé en n=3 sous-systèmes auxquelles les lois classiques s'appliquent individuellement. Par exemple on écrirait :

$$m_i \ddot{\vec{r}}_i = G m_i \sum_{j=1, j\neq i}^{n} \frac{m_j (\vec{r}_j - \vec{r}_i)}{\left|\vec{r}_j - \vec{r}_i\right|^{3/2}} \qquad (i = 1, \cdots, n).$$

La solution numérique de ce problème peut être calculée en un temps raisonnable par un ordinateur classique. Certes ce système a toutes les chances d'être chaotique mais à condition d'encoder les, 6x3=18, conditions initiales avec une précision suffisante, rien ne s'oppose à ce qu'on prédise l'évolution du système jusqu'à n'importe quel temps t, fixé d'avance. La solution du même problème, à n>3 corps cette fois, prendrait sans doute plus de temps car le nombre des variables passerait de 6x3 à 6xn mais le fait est que ce temps resterait raisonnable et en tous cas accessible à un ordinateur classique. Au fond, ce qui rend le problème classique à n corps abordable (pour n raisonnablement modéré), c'est le fait que la dimension de l'espace vectoriel nécessaire à sa résolution ne croît que comme une puissance (ici la première puissance) du nombre n. En effet, le produit cartésien des espaces de phases de chacun des n corps ne comporte que 6xn dimensions au total.

L'atome d'hélium. Deux électrons prisonniers d'un noyau d'hélium forment également un système à trois corps, quantique cette fois. La grande différence est que ces électrons sont totalement indiscernables : ils forment un système intriqué. Leur vecteur d'état, $|\psi\rangle = |\psi(v_1, v_2, t)\rangle$, où les v_i abrègent la notation des variables externes de position et internes de spin, doit certainement traduire quelque part cette indifférence à toute tentative de numérotation des particules individuelles. Nous savons que ce vecteur d'état évolue conformément à la loi,

$$i\hbar \partial_t |\psi\rangle = H(v_1, v_2)|\psi\rangle.$$

Même en se contentant d'étudier les seuls états stationnaires, qui obéissent à l'équation volontairement simplifiée, où l'on ignore toute contribution de spin,

$$H(\vec{r}_1, \vec{r}_2)|\psi\rangle = -\frac{\hbar^2}{2m}(\Delta_1 + \Delta_2)|\psi\rangle + V(\vec{r}_1, \vec{r}_2)|\psi\rangle = E|\psi\rangle,$$

on peut montrer que cette équation aux 6 (!) dérivées partielles ne constitue généralement pas un problème bien posé : elle possède, en fait, une infinité de solutions appartenant toutes à L_2. Autrement dit, l'ensemble des principes de la mécanique quantique tels qu'ils ont été énoncés dans la première partie, ne suffit pas à définir une solution unique au problème posé par les systèmes de particules identiques.

On peut s'en convaincre plus aisément sur l'exemple simplifié d'un système de deux particules identiques soumises à une interaction additive du type, $V(\vec{r}_1, \vec{r}_2) = V_1(\vec{r}_1) + V_2(\vec{r}_2)$.

Dans ce cas, il est certainement possible de trouver une solution acceptable, $(\in L_2)$, s'écrivant sous la forme séparable, $|\psi(\vec{r}_1,\vec{r}_2)\rangle = |\psi_1(\vec{r}_1)\rangle \otimes |\psi_2(\vec{r}_2)\rangle$. Mais alors, il vient immédiatement que $|\psi(\vec{r}_1,\vec{r}_2)\rangle = |\psi_1(\vec{r}_2)\rangle \otimes |\psi_2(\vec{r}_1)\rangle$ est également solution, d'où n'importe quelle combinaison linéaire des deux l'est aussi :

$$|\psi(\vec{r}_1,\vec{r}_2)\rangle = \lambda_1 |\psi_1(\vec{r}_1)\rangle \otimes |\psi_2(\vec{r}_2)\rangle + \lambda_2 |\psi_1(\vec{r}_2)\rangle \otimes |\psi_2(\vec{r}_1)\rangle .$$

Or rien dans les principes généraux de la mécanique quantique ne permet de choisir la « bonne » solution parmi toutes celles que l'on vient d'écrire. Autrement dit, il manque un principe qui réduit les solutions acceptables à une seule.

L'observation suivante guide le choix de ce principe supplémentaire : le hamiltonien ne peut faire aucune différence entre deux particules indiscernables d'où il est nécessairement symétrique par rapport à l'échange des variables, v_1 et v_2 :

$$H(v_1,v_2) = H(v_2,v_1) .$$

On pose en principe, dit de symétrisation, que le vecteur d'état associé à un système de n particules indiscernables est obligatoirement soit totalement symétrique soit totalement antisymétrique par rapport à toute permutation dans la numérotation des particules. Cela donnerait deux possibilités, dans le cas particulier d'un potentiel additif, (n=2) :

1) $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\psi_1(v_1)\rangle \otimes |\psi_2(v_2)\rangle + |\psi_1(v_2)\rangle \otimes |\psi_2(v_1)\rangle\right)$, si les particules sont de spin demi-entier (fermions, ce sont les particules de matière, électron, nucléons, …) et plus généralement, si le potentiel est quelconque : $|\psi(v_1,v_2\rangle = |\psi(v_2,v_1\rangle$.

2) $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\psi_1(v_1)\rangle \otimes |\psi_2(v_2)\rangle - |\psi_1(v_2)\rangle \otimes |\psi_2(v_1)\rangle\right)$, si les particules sont de spin entier (bosons, ce sont les particules médiatrices d'interaction entre fermions, photons, pions, …) et plus généralement : $|\psi(v_1,v_2\rangle = -|\psi(v_2,v_1\rangle$.

Remarque : la notation, v_i, regroupe les variables d'espace et de spin. Une particule dénuée de spin se verrait attribuer un vecteur d'état scalaire et dans ce cas simple le principe de symétrie ne porterait que sur les variables d'espace. Dès que la particule est spinale, son vecteur d'état évolue dans l'espace de Hilbert résultant du produit extérieur des deux sous-espaces correspondants aux variables externes et internes. Dans une représentation matricielle, on écrirait :

$$|\psi(v_1,v_2)\rangle = c_1(\vec{r}_1,\vec{r}_2)|0\rangle + c_2(\vec{r}_1,\vec{r}_2)|1\rangle = \begin{pmatrix} c_1(\vec{r}_1,\vec{r}_2) \\ c_2(\vec{r}_1,\vec{r}_2) \end{pmatrix}.$$

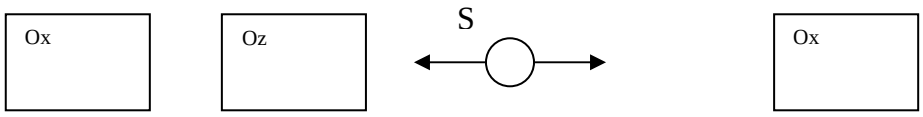
Dans ce cas, c'est le vecteur d'état global qui est soumis au principe de symétrie :

$$\begin{pmatrix} c_1(\vec{r}_1,\vec{r}_2) \\ c_2(\vec{r}_1,\vec{r}_2) \end{pmatrix} = + \begin{pmatrix} c_2(\vec{r}_2,\vec{r}_1) \\ c_1(\vec{r}_2,\vec{r}_1) \end{pmatrix} \text{ (bosons)}$$

ou

$$\begin{pmatrix} c_1(\vec{r}_1,\vec{r}_2) \\ c_2(\vec{r}_1,\vec{r}_2) \end{pmatrix} = + \begin{pmatrix} c_2(\vec{r}_2,\vec{r}_1) \\ c_1(\vec{r}_2,\vec{r}_1) \end{pmatrix} \text{ (fermions).}$$

Le principe de symétrie vient s'ajouter aux principes de base déjà énoncés. A ce titre, il ne se démontre pas mais on le crédibilise grâce à l'expérience suivante. Considérons une source, S, de spin nul, n'ayant fait l'objet d'aucune préparation particulière, qui émet en opposition deux particules de spins 1/2, nécessairement opposés afin de satisfaire la loi de conservation du moment angulaire.



En l'absence de toute mesure de spin, le système des deux particules, numérotées 1 et 2, est intriqué et il peut être décrit par le vecteur d'état :

$$|\psi\rangle = \alpha|z+\rangle_1|z-\rangle_2 + \beta|z-\rangle_1|z+\rangle_2 \qquad (|\alpha|^2 + |\beta|^2 = 1).$$

On cherche une procédure expérimentale capable de révéler les valeurs des coefficients α et β. Imaginons, à cet effet, que nous analysions la particule émise à gauche par un appareil de Stern-Gerlach orienté selon Oz : on trouve +1/2 et –1/2 en moyenne une fois sur deux. Ceci indique que, $|\alpha|^2 = |\beta|^2 = 1/2$, donc que le vecteur d'état devait s'écrire, à une phase globale inessentielle près :

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|z+\rangle_1|z-\rangle_2 + e^{i\varphi}|z-\rangle_1|z+\rangle_2\right).$$

A ce stade, la phase résiduelle, φ, demeure inconnue. Plaçons à présent, symétriquement, deux analyseurs orientés selon Ox de telle manières qu'ils soient traversés après le premier et voyons avec quelle probabilité, $P_{++,x}$, les mesures, effectuées selon Ox, donneraient le même résultat, +1/2, tant à gauche qu'à droite de la source. L'expérience indique qu'avec des électrons cette probabilité est nulle, $P_{++,x} = 0$. Or le calcul de $P_{++,x}$ donne :

$$P_{++,x} = \left|{}^1\langle x+|{}^2\langle x+|\psi\rangle\right|^2 = \left|{}^1\langle x+|{}^2\langle x+|\frac{1}{\sqrt{2}}\left(|z+\rangle_1|z-\rangle_2 + e^{i\varphi}|z-\rangle_1|z+\rangle_2\right)\right|^2$$

$$= \left|{}^1\langle x+|{}^2\langle x+|\frac{1}{2\sqrt{2}}\left((|x+\rangle_1 - |x-\rangle_1)(|x+\rangle_2 + |x-\rangle_2) + e^{i\varphi}(|x+\rangle_1 + |x-\rangle_1)(|x+\rangle_2 - |x-\rangle_2)\right)\right|^2$$

$$= \frac{1}{2}\cos^2\frac{\varphi}{2}$$

d'où on conclut que, $\varphi = \pi$, et que le vecteur d'état des électrons émis par la source est antisymétrique :

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|z+\rangle_1|z-\rangle_2 - |z-\rangle_1|z+\rangle_2\right).$$

Nous verrons sous peu qu'une expérience similaire conduite avec des photons et des polariseurs en lieu et place d'appareils de Stern-Gerlach donnerait un résultat différent : la probabilité, $P_{++,x}$, serait égale à 1/2 d'où la phase φ serait nulle et le vecteur d'état symétrique,

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|z+\rangle_1|z-\rangle_2 + |z-\rangle_1|z+\rangle_2\right).$$

L'intrication du vecteur d'état a une conséquence dramatique sur le calcul des états d'un atome possédant n électrons : il n'est plus possible de considérer séparément chaque électron comme on le fait classiquement avec des planètes. La mécanique quantique traite ses problèmes dans des espaces de Hilbert dont le nombre de degrés de libertés augmente exponentiellement en fonction du nombre n de corps présents. Techniquement parlant, cela résulte du fait que l'espace de Hilbert global est le produit tensoriel (et non plus cartésien) des espaces individuels.

Envisageons plus concrètement un atome à n électrons. Il est décrit par une fonction d'onde obéissant à l'équation de Schrödinger, dont l'amplitude dépend de toutes les variables de position (on néglige les corrections de spin qui ne feraient qu'aggraver la situation) :

$$\psi = \psi(\vec{r}_1, \vec{r}_2, \cdots, \vec{r}_n).$$

En réalité, les n électrons sont indiscernables en sorte que la fonction d'onde doit, en fait, être antisymétrique pour toutes permutations des particules. Or la fonction d'onde d'un système de n particules identiques s'écrit comme une somme de n ! fonctions du type :

$$\psi_{antisym} = \frac{1}{\sqrt{n!}}\sum_{\forall perm}(-1)^{sign}\psi(\vec{r}_{i1}, \vec{r}_{i2}, \vec{r}_{i3}, \cdots, \vec{r}_{in}).$$

Lorsque n augmente cette fonction devient rapidement ingérable pour un ordinateur classique. Rien que l'écriture d'un bout de programme calculant l'atome de fer (26 électrons) exigerait d'y inscrire une fonction d'onde combinant la bagatelle de 26 ! = 4.10^{26} fonctions individuelles. Ce n'est pas irréalisable en théorie mais c'est totalement irréaliste. Insistons, il ne s'agit nullement d'une incapacité fondamentale à régler le problème : rien n'empêcherait

l'ordinateur classique de calculer l'atome de fer, si on le voulait, car son principe repose sur celui d'une machine de Turing universelle et le propre d'une MTU est d'être capable de calculer tout ce qui est calculable. L'incapacité se situe au niveau du temps de calcul qui dépasserait largement l'âge de l'univers, sans parler de l'encombrement de la mémoire.

Au fond, cette croissance dramatique en fonction de n est typique des problèmes NP : nous avons vu, dans le chapitre réservé à la calculabilité, que lorsqu'on tente une résolution du problème du voyageur de commerce par la méthode exhaustive on se heurte également à un nombre d'éventualités à prendre en considération de l'ordre de n !

Pourtant la nature calcule l'évolution, en temps réel, de tous ses atomes même les plus compliqués ! Si l'on pose, comme on le fait en physique classique, qu'un système quantique, tel un atome de béryllium, est équivalent à une MT (quantique) particulière dédicacée précisément au calcul de sa propre évolution en temps réel, la supériorité de la machine quantique saute aux yeux. Evidemment un atome de béryllium n'est pas équivalent à une MTU mais on verra que le concept de MTU reste valable dans le monde quantique et qu'en s'y prenant adroitement on peut, au moins en théorie, espérer l'implémenter un jour physiquement sous la forme d'un véritable ordinateur quantique.

Opérations logiques élémentaires sur le qubit isolé.

Nous avons appris comment préparer un qubit isolé dans un état de superposition arbitrairement donné : seules sont nécessaires les portes de Hadamard et de déphasage. Une fois le qubit préparé quel genre de traitement arithmético-logique peut-on imaginer lui faire subir ? Dans le cas du bit classique la réponse est simple, il n'y en a que deux : l'identité (Id) et la négation (Not). Les transformations unitaires qui effectuent les mêmes opérations sur le qubit isolé possèdent les représentations matricielles suivantes :

$$\boldsymbol{Id} = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \textit{et} \qquad \boldsymbol{Not} = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

On vérifie qu'elles conservent le nombre de '0' et de '1' :

Exemple : $\boldsymbol{Not}(c_1|0\rangle + c_2|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} c_2 \\ c_1 \end{pmatrix} = (c_2|0\rangle + c_1|1\rangle)$.

Le qubit isolé autorise d'autres transformations unitaires dont certaines effectuent des opérations fort peu intuitives. Ainsi la transformation, SqNot, notée comme suit :

$$\boldsymbol{SqNot} = \frac{e^{-i\pi/4}}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

On vérifie que : $\boldsymbol{SqNot}^2 = \boldsymbol{Not}$. En d'autres termes, la même opération effectuée deux fois de suite équivaut à la négation. C'est un exemple d'une performance impossible à réaliser en théorie classique de l'information.

Les portes de déphasage, Φ, et de Hadamard, H, formant un couple universel pour les transformations unitaires du qubit isolé, il doit donc être possible de réduire SqNot à un assemblage de ces deux portes. De fait, on vérifie que trois portes suffisent :

$$SqNot = e^{-i\pi/4}\Phi(\pi/2)H\Phi(\pi/2).$$

Registres de n qubits.

Le qubit isolé ne mène pas très loin en théorie de l'information. Un ensemble de n (qu)bits, s'appelle un registre. Un registre classique de n bits peut stocker 2^n messages différents, par exemple tous les entiers binaires de 0 à 2^n-1, mais il ne peut en stocker qu'un seul à la fois. Un registre quantique peut faire beaucoup mieux car la superposition quantique lui permet de les stocker tous en même temps. Naturellement, lorsqu'on cherche à prendre connaissance du contenu du registre, l'acte de mesure ne peut révéler qu'un seul message sélectionné au hasard. Ce sera tout l'art de la programmation quantique de tirer parti du bénéfice sans pâtir de la limitation.

L'écriture des contenus possibles d'un registre soulève un problème de notations. Par exemple, si n=2, 4 messages distincts sont autorisés. Une première manière de les noter consiste à les prendre dans l'ordre arithmétique, $(|0\rangle,|1\rangle,|2\rangle,|3\rangle)$. Dans cette optique, l'encodage se fait sur base d'un produit tensoriel en respectant l'ordre binaire et on écrit indifféremment :

$$\begin{aligned}
|0\rangle &\equiv |00\rangle_{AB} \equiv |0\rangle_A \otimes |0\rangle_B \equiv |0\rangle_A|0\rangle_B \\
|1\rangle &\equiv |01\rangle_{AB} \equiv |0\rangle_A \otimes |1\rangle_B \equiv |0\rangle_A|1\rangle_B \\
|2\rangle &\equiv |10\rangle_{AB} \equiv |1\rangle_A \otimes |0\rangle_B \equiv |1\rangle_A|0\rangle_B \\
|3\rangle &\equiv |11\rangle_{AB} \equiv |1\rangle_A \otimes |1\rangle_B \equiv |1\rangle_A|1\rangle_B
\end{aligned}.$$

Les indices A et B ne sont pas indispensables mais ils aident à se remémorer que les vecteurs indicés différemment évoluent dans des espaces distincts. En particulier, les relations d'orthonormation ne concernent que les vecteurs de mêmes indices :

$${}^A\langle 0|0\rangle_A = {}^A\langle 1|1\rangle_A = {}^B\langle 0|0\rangle_B = {}^B\langle 1|1\rangle_B = 1 \qquad {}^A\langle 0|1\rangle_A = {}^A\langle 1|0\rangle_A = {}^B\langle 0|1\rangle_B = {}^B\langle 0|1\rangle_B = 0.$$

On peut généraliser la représentation matricielle au cas des registres mais l'agrément qu'elle procure est tempéré par le fait qu'en général, le produit tensoriel de deux vecteurs de dimensions m_1 et m_2 est de dimension m1xm2. Même pour des dimensions modérées, la notation matricielle devient rapidement encombrante. Par exemple dans le cas n=2, les quatre vecteurs de base de l'espace de Hilbert où le registre évolue se notent :

$$|0\rangle_A \otimes |0\rangle_B = \begin{pmatrix}1\\0\end{pmatrix}_A \otimes \begin{pmatrix}1\\0\end{pmatrix}_B = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \qquad |0\rangle_A \otimes |1\rangle_B = \begin{pmatrix}1\\0\end{pmatrix}_A \otimes \begin{pmatrix}0\\1\end{pmatrix}_B = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|1\rangle_A \otimes |0\rangle_B = \begin{pmatrix} 0 \\ 1 \end{pmatrix}_A \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix}_B = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |1\rangle_A \otimes |1\rangle_B = \begin{pmatrix} 0 \\ 1 \end{pmatrix}_A \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}_B = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Les indices A et B sont utiles lorsqu'on passe aux opérateurs. Il est, en effet, ambigu de déclarer soumettre un registre comprenant deux qubits à l'opération Not tant qu'on ne précise pas si cet opérateur s'applique à A, à B ou aux deux simultanément. Les représentations matricielles sont évidemment différentes dans chaque cas :

$$Not_A \otimes Id_B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_A \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_B = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$Id_A \otimes Not_B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}_A \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$Not_A \otimes Not_B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_A \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}_B = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

On voit que l'encombrement de la notation matricielle augmente quand on passe aux opérateurs. Cela est bien naturel puisque le produit tensoriel entre opérateurs de dimensions (m_1, n_1) et (m_2, n_2) est lui-même de dimension $m_1m_2xn_1n_2$.

La représentation matricielle des opérateurs devient progressivement ingérable dès que le nombre des qubits du registre excède 2 : il faudrait travailler dans un espace de dimension 2^n. Dans ce cas, seule la notation tensorielle est concevable mais elle requiert du soin dans la gestion des indices, A, B, C, … . On aurait par exemple :

$$Not_A = |0\rangle_A {}^A\langle 1| + |1\rangle_A {}^A\langle 0| \qquad et \qquad Not_B = |0\rangle_B {}^B\langle 1| + |1\rangle_B {}^B\langle 0|,$$

d'où on écrit :

$$Not_A \otimes Not_B = \left(|0\rangle_A {}^A\langle 1| + |1\rangle_A {}^A\langle 0|\right)\left(|0\rangle_B {}^B\langle 1| + |1\rangle_B {}^B\langle 0|\right).$$

Quelle que soit la notation retenue, on vérifie que l'on a bien, par exemple :

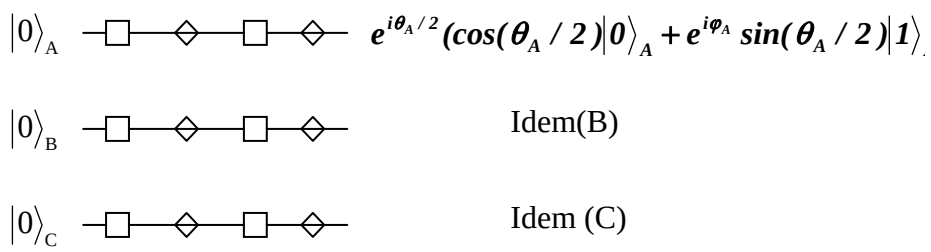
$$\left(Not_A \otimes Not_B\right)\left(|0\rangle_A \otimes |1\rangle_B\right) = |1\rangle_A \otimes |0\rangle_B.$$

Préparation d'un registre de n qubits.

Préparer un registre dans un état donné est plus compliqué que pour le qubit isolé. L'opération n'est simple que si l'état est séparable : on veut dire par là que le vecteur d'état est complètement factorisable par rapport aux n qubits qui le composent, ce que traduit la notation,

$$\left|\psi_{sep}\right\rangle = \bigotimes_{i=1}^{n}\left(\alpha_i\left|0_i\right\rangle + \beta_i\left|1_i\right\rangle\right).$$

Pour préparer un tel état séparable, on procède en deux temps comme dans le cas du qubit isolé. On commence par le préparer dans un état de base, disons $\left|000\cdots0\right\rangle$, en filtrant chaque qubit du registre dans l'état correspondant, $\left|0\right\rangle$. Ensuite, on applique, en parallèle, la transformation, U(θ,φ), à chaque qubit :



L'état de superposition d'un registre peut être plus ou moins complet, ainsi :

- l'état, $\left|000\right\rangle$, n'est pas superposé, c'est un état de base élargie à l'espace du registre,
- l'état, $\frac{1}{\sqrt{2}}\left(\left|0\right\rangle+\left|1\right\rangle\right)\otimes\left|1\right\rangle\otimes\left|1\right\rangle = \frac{1}{\sqrt{2}}\left(\left|011\right\rangle+\left|111\right\rangle\right) = \frac{1}{\sqrt{2}}\left(\left|3\right\rangle+\left|7\right\rangle\right)$, est partiellement superposé,
- enfin l'état,

$$\frac{1}{\sqrt{2}}\left(\left|0\right\rangle+\left|1\right\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(\left|0\right\rangle+\left|1\right\rangle\right)\otimes\frac{1}{\sqrt{2}}\left(\left|0\right\rangle+\left|1\right\rangle\right) =$$
$$\frac{1}{\sqrt{8}}\left(\left|000\right\rangle+\left|001\right\rangle+\left|010\right\rangle+\left|011\right\rangle+\left|100\right\rangle+\left|101\right\rangle+\left|110\right\rangle+\left|111\right\rangle\right) =$$
$$\frac{1}{\sqrt{8}}\left(\left|0\right\rangle+\left|1\right\rangle+\left|2\right\rangle+\left|3\right\rangle+\left|4\right\rangle+\left|5\right\rangle+\left|6\right\rangle+\left|7\right\rangle\right)$$

est maximalement superposé.

La plupart des états de registres ne sont pas séparables. Dans l'exemple, n=3, l'état noté,

$$\left|\psi_{\text{int}}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|000\right\rangle+\left|111\right\rangle\right),$$

n'est manifestement pas séparable car il est impossible de l'écrire sous la forme d'un produit tensoriel de trois facteurs, un par qubit. Un tel état est dit intriqué (ou enchevêtré). Plus généralement, l'état,

$$\psi = c_1|000\rangle + c_2|001\rangle + c_3|010\rangle + c_4|011\rangle + c_5|100\rangle + c_6|101\rangle + c_7|110\rangle + c_8|111\rangle \qquad \left(\sum_{i=1}^{8}|c_i|^2 = 1\right)$$

est intriqué s'il est impossible de le factoriser sous la forme,

$$|\psi_{int}\rangle = \bigotimes_{i=1}^{3}\left(\alpha_i|0\rangle + \beta_i|1\rangle\right).$$

Cela se produit toutes les fois que le polynôme,

$$c_1 + c_2u + c_3u^2 + c_4u^3 + c_5u^4 + c_6u^5 + c_7u^6 + c_8u^7 ,$$

n'est pas complètement factorisable en trois facteurs de degrés, 2^0=1, 2^1=2 et 2^2=4. Par exemple, $1 + 2u + u^2 + 2u^3 + u^4 + 2u^5 + u^6 + 2u^7 = (1 + 2u)(1 + u^2)(1 + u^4)$ donc :

$$\psi = \frac{1}{\sqrt{20}}\left(|000\rangle + 2|001\rangle + |010\rangle + 2|011\rangle + |100\rangle + 2|101\rangle + |110\rangle + 2|111\rangle\right)$$

est factorisable. L'idée qui se trouve derrière ce critère tient dans la correspondance suivante :

$$\left(\alpha_1|0\rangle + \beta_1|1\rangle\right)\otimes\left(\alpha_2|0\rangle + \beta_2|1\rangle\right)\otimes\left(\alpha_3|0\rangle + \beta_3|1\rangle\right) \leftrightarrow \left(\alpha_1 + \beta_1u^4\right)\left(\alpha_1 + \beta_1u^2\right)\left(\alpha_1 + \beta_1u\right)$$

Le critère de Schmidt permet de décider si un état est séparable sans passer par la factorisation d'un polynôme. Montrons, sans justification, comment il fonctionne. On considère l'état normalisé d'un registre à deux qubits :

$$|\psi\rangle_{AB} = \alpha|0\rangle_A|0\rangle_B + \beta|0\rangle_A|1\rangle_B + \gamma|1\rangle_A|0\rangle_B + \delta|0\rangle_A|0\rangle_B \qquad (|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1),$$

pour quelles valeurs des coefficients est-il séparable ? La réponse s'obtient en calculant la représentation matricielle, dans l'espace B (ou dans l'espace A, au choix) de la trace, ρ, dans l'espace A (dans l'espace B), du projecteur, $|\psi\rangle_{AB}{}^{AB}\langle\psi|$. On trouve dans l'exemple retenu :

$$\rho = Tr_A[(\alpha|0\rangle_A|0\rangle_B + \beta|0\rangle_A|1\rangle_B + \gamma|1\rangle_A|0\rangle_B + \delta|0\rangle_A|0\rangle_B)(\alpha^*{}^A\langle 0|^B\langle 0| + \beta^*{}^A\langle 0|^B\langle 1| + \gamma^*{}^A1^B\langle 0| + \delta^*{}^A\langle 1|^B\langle 1|)]$$

On calcule cette quantité dans le sous-espace, A, en tenant compte de ce que :

La trace de : $|0\rangle_A{}^A\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$ vaut 1,

celle de : $|0\rangle_A{}^A\langle 1| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}$ vaut 0,

celle de : $|1\rangle_A {}^A\langle 0| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ vaut 0,

enfin celle de : $|1\rangle_A {}^A\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ vaut 1.

On trouve sans difficultés :

$$\rho = \begin{pmatrix} |\alpha|^2 + |\gamma|^2 & \alpha\beta^* + \gamma\delta^* \\ \alpha^*\beta + \gamma^*\delta & |\beta|^2 + |\delta|^2 \end{pmatrix}.$$

Le nombre de valeurs propres non nulles de ρ s'appelle le nombre de Schmidt de l'état, $|\psi\rangle_{AB}$. Quelle que soit la valeur de n, on a que l'état est intriqué dès que deux valeurs propres, au moins, sont différentes de zéro, sinon il est séparable. Dans l'exemple, l'équation aux valeurs propres se simplifie en :

$$\lambda^2 - \lambda + |\alpha\delta - \beta\gamma|^2 = 0,$$

et la séparabilité exige : $\alpha\delta - \beta\gamma = 0$. La plupart du temps, cette condition ne sera pas satisfaite d'où il résulte que les états intriqués sont beaucoup plus nombreux que les états séparables.

Certes, dans cet exemple, n ne vaut que 2 et on aurait pu déduire ce résultat plus simplement en identifiant les coefficients de l'état donné à ceux de la forme séparable la plus générale, $|\psi_{sep}\rangle = \bigotimes_{i=1}^{n}(\alpha_i|0\rangle + \beta_i|1\rangle)$, mais la procédure exposée présente l'avantage de rester effective pour les valeurs de n supérieures à 2.

Intrication logique d'un registre à deux qubits.

Les arguments développés montrent que l'encodage de tous les messages possibles sur n qubits, tous coefficients confondus, passent par l'intrication du registre. La question reste posée de savoir s'il existe des portes logiques quantiques capables de préparer des états intriqués à partir des états de base, et, dans l'affirmative, s'il est possible de les implémenter physiquement. Les deux réponses sont positives mais dans un premier temps nous ne considérons que la première.

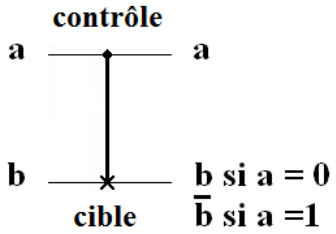
Rappelons que les portes, H et Φ(φ), suffisent pour préparer n'importe quel registre sous forme séparable. Une seule porte supplémentaire est nécessaire pour passer de la superposition à l'intrication, la porte Controlled-Not (CNot). Celle-ci agit sur deux qubits d'entrée qu'elle soumet à la transformation logique :

$$CNot|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle.$$

Dans cette relation, le premier ket apparaît comme un qubit de contrôle et le deuxième est la cible. Le qubit de contrôle n'est pas altéré par la porte logique et la cible ne l'est que si le contrôle vaut '1'. Voici une manière équivalente mais plus explicite d'exprimer les choses :

$$CNot|0\rangle|y\rangle = |0\rangle|y\rangle$$
$$CNot|1\rangle|y\rangle = |1\rangle|\neg y\rangle$$

Les représentations matricielle, graphique et tensorielle de la porte CNot s'écrivent respectivement (dans la représentation graphique, le point noir signifie que le bit situé à sa gauche est un bit de contrôle et la croix désigne la porte Not) :



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

$$cNot_{AB} = |0\rangle_A {}^A\langle 0| \otimes Id_B + |1\rangle_A {}^A\langle 1| \otimes Not_B .$$

Quelle que soit la notation retenue, on vérifie que CNot appliquée à $|1\rangle_A|0\rangle_B$, par exemple, fournit à la sortie, $|1\rangle_A|1\rangle_B$, comme il se doit.

En préparant la cible, B, dans l'état logique '0', on voit que la porte CNot réalise la copie exacte d'un état de base encodé au niveau du qubit de contrôle. On a, en effet :

$$CNot_{AB}|x\rangle_A|0\rangle_B = |0\rangle_A {}^A\langle 0|x\rangle_A|0\rangle_B + |1\rangle_A {}^A\langle 1|x\rangle_A|1\rangle_B = |x\rangle_A|x\rangle_B \qquad (x = 0,1) .$$

Bref retour au théorème de non-clonage.

On pourrait penser avoir trouvé avec la porte CNot le moyen de cloner un état donné mais il est facile de voir que cette copie ne fonctionne que sur les états de base, $|0\rangle$ et $|1\rangle$, et pas du tout sur leur superposition, en effet :

$$CNot_{AB}(\alpha|0\rangle_A + \beta|1\rangle_A)|0\rangle_B = \alpha|0\rangle_A|0\rangle_B + \beta|1\rangle_A|1\rangle_B ,$$

qui est très différent de la copie espérée :

$$CNot_{AB}(\alpha|0\rangle_A + \beta|1\rangle_A)|0\rangle_B \neq (\alpha|0\rangle_A + \beta|1\rangle_A)(\alpha|0\rangle_A + \beta|1\rangle_A) .$$

C'est un fait général qu'il n'existe aucune porte capable de dupliquer un état quelconque et d'effectuer l'opération,

$$U|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle .$$

De fait, si U existait, on pourrait écrire :

$$U(|a\rangle + |b\rangle)|0\rangle = |aa\rangle + |bb\rangle \neq (|a\rangle + |b\rangle)(|a\rangle + |b\rangle) .$$

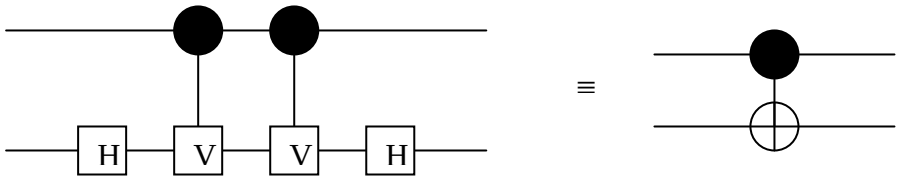
Portes controlled-U.

La porte CNot est un cas particulier de toute une famille de portes appelées portes controlled-U (CU), qui fonctionnent sur le même principe : elles conservent toujours le qubit de contrôle et elles n'altèrent la cible, par la transformation unitaire, U, que si le qubit de contrôle vaut '1' :

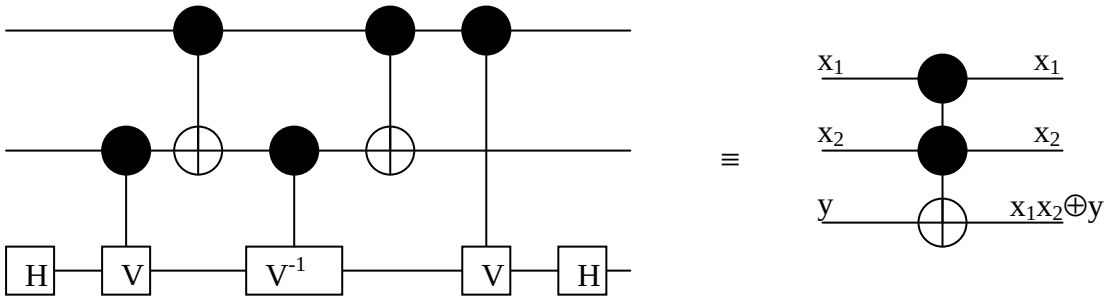
$$CU_{AB}|0\rangle_A|y\rangle_B = |0\rangle_A|y\rangle_B$$
$$CU_{AB}|1\rangle_A|y\rangle_B = |1\rangle_A|Uy\rangle_B .$$

La plupart des portes CU provoquent l'intrication des qubits d'entrée : jointes aux portes H et Φ, elles suffisent dès lors généralement à construire un système universel au sens de Turing. On utilise fréquemment la porte CV = $C\Phi(\pi/2)$.

Par exemple, on pourrait construire la porte CNot comme suit :



Poursuivant dans la même veine, on observe que quatre portes CV successives équivalent à l'identité. On en déduit que trois portes CV successives représentent ensemble l'opération inverse de CV, que l'on note $(CV)^{-1}$. Grâce à $(CV)^{-1}$, on construit la très utile porte controlled-controlled-NOT (CCNot), encore appelée porte de Toffoli (T) :



Par définition, une porte du type, CCU, ne modifie la cible que si les deux qubits de contrôle valent '1'.

Il n'est pas question de proposer une représentation matricielle de la porte de Toffoli, nécessairement 8x8, par contre son écriture tensorielle reste abordable :

$$\boldsymbol{CCNot_{ABC} = |0\rangle_A{}^A\langle 0| \otimes Id_B \otimes Id_C + |1\rangle_A{}^A\langle 1| \otimes |0\rangle_B{}^B\langle 0| \otimes Id_C + |1\rangle_A{}^A\langle 1| \otimes |1\rangle_B{}^B\langle 1| \otimes Not_C}.$$

Il existe également une porte « controlled swap », encore appelée porte de Fredkin, F :

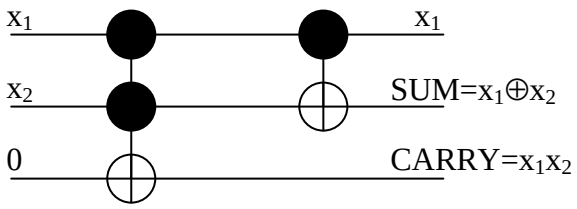
$$\boldsymbol{F = |0\rangle_A{}^A\langle 0| \otimes Id_B \otimes Id_C + |1\rangle_A{}^A\langle 1| \otimes (|00\rangle_{BC}{}^{BC}\langle 00| + |01\rangle_{BC}{}^{BC}\langle 10| + |10\rangle_{BC}{}^{BC}\langle 01| + |11\rangle_{BC}{}^{BC}\langle 11|)}$$

.

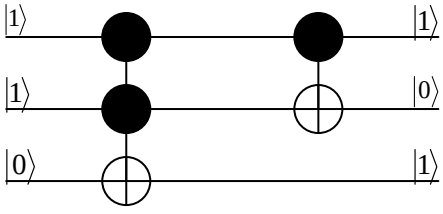
Les portes de déphasage, de Hadamard et CV (ou CNot) forment un ensemble complet pour la manipulation d'un nombre arbitraire de qubits. En garantissant l'universalité au sens de Turing, elles autorisent, en théorie du moins, la construction et l'assemblage des circuits logiques qui composent un ordinateur quantique. L'unitarité de ces portes, qui est inscrite dans les principes mêmes de la mécanique quantique, garantit la réversibilité du calcul.

Implémentation logique de quelques opérations arithmétiques élémentaires.

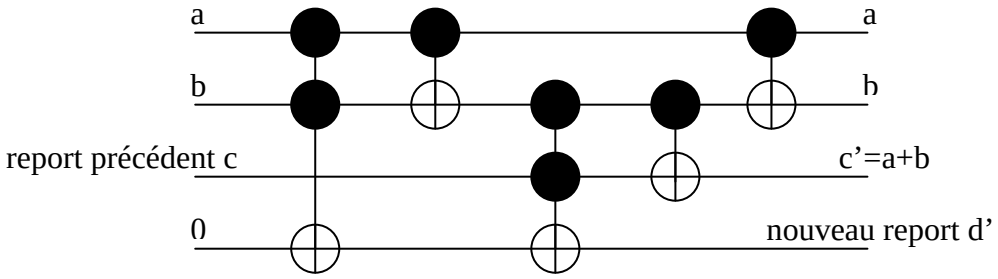
Les portes CNot et CCNot, correctement agencée, permettent de construire un semi-additionneur (half adder) binaire :



Ce réseau, alimenté par les données, x_1 et x_2, initialisées dans l'un ou l'autre de leurs états logiques, faciles à préparer, $|\boldsymbol{0}\rangle$ ou $|\boldsymbol{1}\rangle$, fournit la réponse au calcul élémentaire posé. Par exemple, l'activation du réseau transforme le registre d'entrée, $|\boldsymbol{in}\rangle = |\boldsymbol{110}\rangle$, en le registre de sortie, $|\boldsymbol{out}\rangle = |\boldsymbol{101}\rangle$. Les mesures des qubits 2 et 3 fournissent la somme et le report correspondants à une instance particulière du problème de l'addition de deux chiffres binaires.



On construit un additionneur complet (full adder) sur le même principe. On le nomme ainsi parce qu'il est capable de tenir compte d'un report consécutif à une opération antérieure :



Cahier des charges de l'ordinateur quantique.

La théorie qui précède assemble sur le papier les composantes de l'ordinateur quantique idéal. Elle donne l'illusion trompeuse que sa construction est à portée de main. Cependant l'inventaire des exigences du cahier des charges indique clairement qu'on est encore très loin du compte et les plus pessimistes estiment même qu'un ordinateur quantique digne de ce nom ne verra jamais le jour. Même en mettant les choses au mieux, les premiers ordinateurs quantiques seront à coup sûr dédicacés à quelques tâches particulières et certainement incapables de simuler une machine de Turing universelle. Dans ce sens restrictif, des specimens d'ordinateur quantique existent déjà : un appareil de Stern-Gerlach est un générateur de nombre aléatoire au sens de Kolmogorov, un gaz d'hélium simule son évolution en temps réel et des mesures spectrométriques renseignent immédiatement sur le schéma de ses niveaux énergétiques.

On ne peut plus schématiquement, l'ordinateur quantique part d'une configuration initiale où sont encodées les données du problème posé. Le cas échéant une provision de qubits excédentaires initialisés à '0' sont prévus afin de garantir la réversibilité du calcul. Le système est alors soumis à un hamiltonien variable au cours du temps qui affecte le contenu des registres en simulant le calcul en vue. Cette manœuvre est tellement précise et délicate qu'elle doit être pilotée par un ordinateur classique qui intervient comme auxiliaire de travail. Au terme de l'évolution des registres, la mesure quantique des qubits dédicacés à la sortie du programme renseigne sur la réponse cherchée. L'ordinateur quantique doit rencontrer les exigences suivantes :

- Emprunter une configuration physique à échelle variable (scalable quantum computer). On entend par là que le système physique doit permettre l'encodage d'un nombre arbitrairement grand de qubits. Cette exigence est analogue à l'exigence classique qui concerne toute machine de Turing universelle : la bande de lecture-écriture doit être de longueur potentiellement infinie. Rappelons que l'on veut dire par là qu'il ne doit pas exister de limitation théorique à l'étendue de la mémoire. Evidemment aucun ordinateur, pas même classique, ne respecte cette exigence au pied de la lettre. Le prix que l'on accepte de payer est l'éventuel plantage de la machine sous l'effet d'un dépassement de capacité mémoire. Cela dit, l'exigence paraît d'autant plus forte à propos de l'ordinateur quantique qu'en 2005 on peine déjà à rassembler un registre de quelques qubits.

- Autoriser la préparation d'un registre dans un état prédéfini. Cette exigence est fondamentale puisque tout calcul quantique passe par l'initialisation du registre dans

un état de base, par exemple $|000\cdots0\rangle$. Elle est anodine dans le cas d'un encodage des qubits par des particules en mouvement : un appareil de Stern-Gerlach ou un cristal de calcite sépare physiquement les faisceaux de polarisations différentes en sorte qu'un écran absorbeur suffit à réaliser le filtrage cherché. Mais la même exigence prend des proportions inquiétantes lorsqu'on utilise un encodage par des particules piégées dans une cavité. Sauf à travailler au zéro absolu, l'immersion d'une population de noyaux dans une induction magnétique répartit au hasard les individus en deux classes distinctes dont la population dépend de la température. Il en ressort toutes sortes de complications toutefois surmontables au prix de techniques qui dépassent un exposé élémentaire.

- Réagir à l'influence sélective d'un hamiltonien piloté de l'extérieur du système. Le hamiltonien doit pouvoir garantir un fonctionnement universel au sens de Turing donc au minimum simuler les portes de déphasage, de Hadamard et CNot. Nous avons vu que tous les modes d'encodage du qubit (électron, états internes ou spatiaux du photon) autorisent sans grand problème les deux premières portes. Si nous n'avons encore rien dit de la porte CNot, c'est que le problème qu'elle pose est infiniment plus délicat. La raison en est que la porte CNot exige le concours interactif de deux qubits avec l'environnement. Un peu de réflexion convaincra, en effet, qu'il n'y a rien d'évident à commander un photon d'inverser ou non son état de polarisation selon qu'un autre photon se trouve lui-même dans un état défini : c'est d'autant plus problématique que les photons n'interagissent pas. Le même problème posé avec des électrons ou des noyaux laisse toutefois entrevoir un début de solution : si une induction magnétique extérieure ne peut que piloter un changement d'orientation du moment magnétique, l'interaction spin-spin entre deux particules correctement choisies pourrait peut-être être domestiquée.

- Autoriser un adressage permettant l'interconnection des portes quantiques et la commande sélective du hamiltonien extérieur sur les qubits visés. En informatique classique, cela se fait sans ambiguïté par un assemblage de « fils » dissipatifs mais ce genre d'intermédiaire est précisément absent du monde quantique. De plus, l'indiscernabilité des particules identiques complique singulièrement cet adressage de même qu'il compliquera la lecture des résultats : comment être certain qu'on a manipulé ou lu le « bon » qubit ? En particulier rappelons que la porte CNot exige la manipulation conjointe et synchronisée de deux qubits imposés.

- Autoriser un mode de lecture des résultats. Il ne suffit pas d'effectuer un calcul, il faut encore pouvoir prendre connaissance de la réponse. Or cela ne peut se faire que via une mesure qui détruit inévitablement, en tout ou en partie, l'intrication des registres en projetant le système, au hasard, sur un seul état propre. Rappelons, sur un exemple simple, ce que cela signifie. Soit un registre à deux qubits qui a évolué vers l'état généralement intriqué,

$$|\psi\rangle_{AB} = \alpha|0\rangle_A|0\rangle_B + \beta|0\rangle_A|1\rangle_B + \gamma|1\rangle_A|0\rangle_B + \delta|1\rangle_A|1\rangle_B \qquad (|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1)$$

,

et supposons qu'une analyse théorique préalable ait révélé que la connaissance du premier qubit, noté, A, suffise à répondre à la question posée. La théorie de la mesure enseigne deux choses :

- que l'on trouvera la valeur 'i' (0 ou 1) avec la probabilité, $p_{A=i}$, valant :

$$p_{A=i} = {}^{AB}\langle\psi|P_{A,i}|\psi\rangle_{AB} = {}^{AB}\langle\psi|\left(|i\rangle_A\,{}^A\langle i|\right)|\psi\rangle_{AB}$$

- que la mesure projettera le registre dans le nouvel état renormalisé,

$$|\psi'\rangle_{AB} = \frac{P_{A,i}|\psi\rangle_{AB}}{\left|P_{A,i}|\psi\rangle_{AB}\right|} = \frac{\left(|i\rangle_A\,{}^A\langle i|\right)|\psi\rangle_{AB}}{\left|\left(|i\rangle_A\,{}^A\langle i|\right)|\psi\rangle_{AB}\right|} = \frac{|i\rangle_A\,{}^A\langle i|\psi\rangle_{AB}}{\sqrt{p_{A=i}}}\,.$$

Par exemple, on trouverait :

$$p_{A=0} = {}^{AB}\langle\psi|P_{A,0}|\psi\rangle_{AB} = {}^{AB}\langle\psi|\left(|0\rangle_A\,{}^A\langle 0|\right)|\psi\rangle_{AB} =$$
$$\left(\alpha^{*\,A}\langle 0|{}^B\langle 0| + \beta^{*\,A}\langle 0|{}^B\langle 1| + \gamma^{*\,A}\langle 1|{}^B\langle 0| + \delta^{*\,A}\langle 1|{}^B\langle 1|\right)\left(|0\rangle_A\,{}^A\langle 0|\right)\left(\alpha|0\rangle_A|0\rangle_B + \beta|0\rangle_A|1\rangle_B + \gamma|1\rangle_A|0\rangle_B + \delta|1\rangle_A|1\rangle_B\right)$$
$$= \left(\alpha^{*\,B}\langle 0| + \beta^{*\,B}\langle 1|\right)\left(\alpha|0\rangle_B + \beta|1\rangle_B\right) = |\alpha|^2 + |\beta|^2$$

De même on trouverait,

$$p_{A=1} = |\gamma|^2 + |\delta|^2\,,$$

d'où une probabilité totale valant naturellement 1. La généralisation à n qubits est immédiate. La plupart du temps (bien qu'il y ait des exceptions), une mesure unique du contenu d'un registre sera incapable de révéler la réponse au problème posé. C'est précisément tout l'art de la programmation quantique que de trouver des algorithmes capables d'extraire le résultat escompté de cette mesure destructrice. Cela implique incontestablement une refonte sérieuse des méthodes de programmation. Plusieurs stratégies sont envisageables : soit on découvre des invariants qui ne dépendent pas de l'état final projeté et qui suffisent à répondre à la question posée soit on trouve des algorithmes qui privilégient les réponses plausibles et faciles à vérifier (éventuellement à l'aide d'un ordinateur classique).

- Garantir la cohérence du système. Au vu de ce qui précède on voit bien l'ensemble des défis à relever aux niveaux software et hardware. L'informatique quantique théorique ne se préoccupe que de trouver des stratégies capables d'extraire la réponse à un problème posé à partir d'un acte de mesure essentiellement destructeur. C'est déjà un problème redoutable en soi mais il semble que tous les espoirs soient permis : le fait qu'on ait déjà trouvé un algorithme viable pour un problème de la classe NP, à savoir la factorisation des entiers longs, suggère que d'autres progrès sérieux devraient suivre. L'ingénierie, elle, s'occupe des possibilités d'implémentation et de préservation des registres. Il est clair que sans hardware, l'ordinateur quantique n'est qu'une fiction. Il existe cependant des cas où le software peut voler au secours d'un hardware déficient : c'est le cas toutes les fois que le système corrompt une partie de l'information pour quelques raisons que ce soit et elles ne manquent pas ! On envisage sérieusement de ne pas trop s'en inquiéter et de tolérer un certain pourcentage d'erreurs quitte à démultiplier, par 10 ou par 100 (!), le nombre de qubits au travers d'un système pensé de correction d'erreurs.

Voyons à présent un exemple d'implémentation effectivement à l'étude. En 2005, le seul modèle modestement effectif était basé sur la technologie NMR (nuclear magnetic resonance). Le record, peut-être provisoire, date de 2001 et a vu Isaac Chuang et une équipe d'IBM réussir à coordonner le fonctionnement d'un registre de 7 qubits. Depuis, la technique photonique a évolué et rejoint la NMR. Le principe suivant n'est donné qu'à titre indicatif car rien ne permet de penser que le modèle puisse s'étendre aux grands registres.

Considérons le proton d'un atome d'hydrogène ou plus généralement un noyau pourvu d'un moment magnétique, μ, de l'ordre du magnéton nucléaire ($1\mu_N = 5.05\ 10^{-27}$ J/T). Bien que mille fois plus faible que celui de l'électron ce moment est parfaitement mesurable avec une précision qui dépasse 10^{-6}. Si on enferme ce noyau dans une cavité où règne une induction magnétique uniforme, orientée selon Oz pour simplifier, il oriente son spin au hasard selon l'une des deux directions, $|z-\rangle$ ou $|z+\rangle$. Chaque direction correspond à un état énergétique particulier :

- le noyau décrit par le vecteur d'état, $|z-\rangle$, se trouve dans l'état fondamental d'énergie, $E_0 = -\mu B_z$,
- le noyau décrit par le vecteur d'état, $|z+\rangle$, se trouve dans l'état excité d'énergie, $E_1 = +\mu B_z$.

On peut utiliser cette dichotomie pour encoder un qubit : il suffit d'utiliser les deux états (nécessairement orthogonaux puisque états propres d'un hamiltonien hermitien) comme état de base de l'espace de Hilbert correspondant :

$$|z-\rangle = |0\rangle \qquad et \qquad |z+\rangle = |1\rangle .$$

Dans ce modèle, on peut imaginer préparer un qubit dans l'état, $|z-\rangle = |0\rangle$, en soumettant le noyau à une induction statique suffisamment intense orientée selon Oz et en abaissant la température au voisinage du zéro absolu. On peut ensuite diminuer le champ jusqu'à zéro sans perturber l'état préparé. Si l'on impose ultérieurement une induction faisant un angle quelconque avec la précédente, on réalise une mesure quantique qui a pour effet de projeter l'ancien état sur la nouvelle direction, Oz'. Nous avons appris comment calculer les probabilités de transition, $p[|z-\rangle \rightarrow |z'+\rangle]$ et $p[|z-\rangle \rightarrow |z'-\rangle]$.

A part l'inconfort de la manœuvre requise par l'abaissement de température, rien n'est nouveau par rapport aux modes d'encodages déjà étudiés. Par contre, le problème traditionnellement posé par l'indiscernabilité des qubits trouve ici une solution naturelle : il suffit de considérer n noyaux magnétiques situés en autant de sites inéquivalents d'une molécule. Vu que l'environnement physique donc les états énergétiques de chacune diffèrent, il devient possible de piloter le changement d'état d'un qubit particulier. Voici comment on pourrait simuler les portes de Hadamard et de déphasage.

Considérons un noyau dans l'état initial (t = 0),

$$|\psi(0)\rangle = c_0(0)|0\rangle + c_1(0)|1\rangle = \begin{pmatrix} c_0(0) \\ c_1(0) \end{pmatrix}.$$

En l'absence d'induction magnétique extérieure, les deux états de base, $|0\rangle$ et $|1\rangle$, sont caractérisés par des énergies égales à zéro et le vecteur d'état n'évolue pas.

Si on soumet le noyau à une induction magnétique constante d'orientation quelconque, la situation change radicalement : la dégénérescence des niveaux énergétiques est levée et le vecteur d'état évolue en conformité avec l'équation de Schrödinger :

$$i\hbar\partial_t\begin{pmatrix}c_0(t)\\c_1(t)\end{pmatrix}=-\mu_p\begin{pmatrix}B_z & B_x-iB_y\\B_x+iB_y & -B_z\end{pmatrix}\begin{pmatrix}c_0(t)\\c_1(t)\end{pmatrix}.$$

Sa solution est immédiate :

$$|\psi(t)\rangle=\begin{pmatrix}c_0(t)\\c_1(t)\end{pmatrix}=exp[\,i\frac{\mu_p t}{\hbar}\begin{pmatrix}B_z & B_x-iB_y\\B_x+iB_y & -B_z\end{pmatrix}\,]|\psi(0)\rangle$$

$$=\begin{pmatrix}\cos\frac{\mu Bt}{\hbar}+i\frac{B_z}{B}\sin\frac{\mu Bt}{\hbar} & \frac{iB_x+B_y}{B}\sin\frac{\mu Bt}{\hbar}\\ \frac{iB_x-B_y}{B}\sin\frac{\mu Bt}{\hbar} & \cos\frac{\mu Bt}{\hbar}-i\frac{B_z}{B}\sin\frac{\mu Bt}{\hbar}\end{pmatrix}|\psi(0)\rangle\quad.$$

Si on s'arrange pour que $B_x=B_y=0$ (d'où $B_z=B$), on trouve que l'action de cette induction constante pendant un temps t est équivalente à une porte logique de déphasage, $\Delta\varphi=\frac{2\mu Bt}{\hbar}$:

$$\Phi(\Delta\varphi)=\begin{pmatrix}exp[\,i\frac{\mu Bt}{\hbar}\,] & 0\\ 0 & exp[-i\frac{\mu Bt}{\hbar}\,]\end{pmatrix}.$$

Si on s'arrange pour que $B_x=B_z$ et $B_y=0$ (d'où $B_x=B_z=B/\sqrt{2}$), agissent pendant un temps t tel que $\cos(\mu Bt/\hbar)=0$, elle est équivalente à une porte logique de Hadamard. Toutefois cette procédure n'est jamais utilisée : d'une part imposer une induction constante agissant discontinument est impossible à réaliser et d'autre part elle affecterait tous les noyaux sans distinction alors qu'on souhaite une action sélective sur un noyau particulier.

On résout le problème en superposant un champ constant, B_0, selon Oz et un champ, d'intensité B_1, tournant uniformément dans le plan Oxy. Nous connaissons le rôle joué par B_0 qui est de créer la différence énergétique entre les états de base. Celui joué par B_1 est de stimuler sélectivement les transitions, $|0\rangle\rightarrow|1\rangle$ et $|1\rangle\rightarrow|0\rangle$. Pour le voir, écrivons l'équation d'évolution,

$$i\hbar\partial_t\begin{pmatrix}c_0(t)\\c_1(t)\end{pmatrix}=-\mu\begin{pmatrix}B_0 & B_1e^{-i\omega t}\\B_1e^{i\omega t} & -B_0\end{pmatrix}\begin{pmatrix}c_0(t)\\c_1(t)\end{pmatrix}.$$

Elle est également soluble exactement sous la forme :

$$|\psi(t)\rangle = \begin{pmatrix} c_0(t) \\ c_1(t) \end{pmatrix} = exp[-i\frac{\omega}{2}\sigma_z t]\, exp\left[i\left((\frac{\omega}{2} + \frac{\mu B_0}{\hbar})\sigma_z + \frac{\mu B_1}{\hbar}\sigma_x \right) t \right] |\psi(0)\rangle$$

$$= \begin{pmatrix} \left(cos\frac{\Omega t}{2} - i\frac{2\mu B_0 + \hbar\omega}{\hbar\Omega} sin\frac{\Omega t}{2} \right) e^{-i\omega t/2} & \frac{2i\mu B_1}{\hbar\Omega} sin\frac{\Omega t}{2\hbar} e^{-i\omega t/2} \\ \frac{2i\mu B_1}{\hbar\Omega} sin\frac{\Omega t}{2} e^{i\omega t/2} & \left(cos\frac{\Omega t}{2} - i\frac{2\mu B_0 + \hbar\omega}{\hbar\Omega} sin\frac{\Omega t}{2} \right) e^{i\omega t/2} \end{pmatrix} |\psi(0)\rangle$$

où : $\Omega = \sqrt{4\mu^2(B_0^2 + B_1^2) + 4\mu\hbar\omega B_0 + (\hbar\omega)^2} = \sqrt{(2\mu B_0 + \hbar\omega)^2 + (2\mu B_1)^2}\ /\ \hbar$.

Avec la technique du champ tournant, on contrôle sélectivement l'évolution en se plaçant à la résonance du noyau visé, résonance caractérisée par la relation,

$$\omega_{res} = -\frac{2\mu B_0}{\hbar} \qquad \Rightarrow \qquad |\psi(t)\rangle = \begin{pmatrix} c_0(t) \\ c_1(t) \end{pmatrix} = \begin{pmatrix} cos\frac{\mu B_1 t}{\hbar} e^{i\mu B_0 t/\hbar} & i\, sin\frac{\mu B_1 t}{\hbar} e^{i\mu B_0 t/\hbar} \\ i\, sin\frac{\mu B_1 t}{\hbar} e^{-i\mu B_0 t/\hbar} & cos\frac{\mu B_1 t}{\hbar} e^{-i\mu B_0 t/\hbar} \end{pmatrix} |\psi(0)\rangle$$

.

On constate qu'à la résonance, on simule la porte de déphasage en un temps très court, $(\pi\hbar)/(\mu B_1)$, de l'ordre de la microseconde, la porte Not en un temps, $(\pi\hbar)/(2\mu B_1)$, et la porte de Hadamard (à deux portes de déphasages près, en fait, $\Phi_1 H \Phi_2$), en un temps $(\pi\hbar)/(4\mu B_1)$.

Hors résonance, le rapport $(\mu B_1)/(\hbar\Omega) \sim B_1/B_0$ peut être choisi suffisamment petit pour que la porte ne s'écarte pas de l'identité en un temps raisonnable, en tous cas nettement plus court que le temps de calcul visé.

Evidemment puisque les portes de déphasages et de Hadamard sont universelles pour le qubit isolé, la même technique permet d'implémenter toutes les portes du type, $e^{\pm i\alpha\sigma_{x,y,z}}$, où $\sigma_{x,y,z}$ représente n'importe quelle matrice de Pauli.

La sélectivité qu'offre la résonance permet alors de construire une porte CNot sur base des interactions spin-spin. On commence par observer que la transformation suivante inverse effectivement sélectivement un qubit « cible », t, en fonction de l'état d'un qubit de contrôle voisin, c :

$$cNot_c^t = e^{-i\pi/4}\, exp[-i(\pi/4)\sigma_y^{(c)}]\, exp[i(\pi/4)\sigma_x^{(c)}]\, exp[i(\pi/4)\sigma_y^{(c)}]\, exp[-i(\pi/4)\sigma_x^{(t)}]\, exp[i(\pi/4)\sigma_y^{(t)}]$$
$$exp[-i(\pi/4)\sigma_z^{(c)} \otimes \sigma_z^{(t)}]\, exp[-i(\pi/4)\sigma_y^{(t)}]$$

Tous les opérateurs qui figurent dans cette expression ont une implémentation connue sauf un, $exp[-i(\pi/4)\sigma_z^{(c)} \otimes \sigma_z^{(t)}]$, qui comme on pouvait s'y attendre, fait intervenir deux qubits simultanément. On peut espérer l'implémenter comme suit.

Les spins interagissent deux par deux de telle manière que chaque couple, (i, j), est caractérisé par une pulsation, ω_{ij}, parfaitement mesurable dont la valeur dépend évidemment de l'environnement. Ecrivons le hamiltonien et l'équation d'évolution correspondante dans le cas où n noyaux seraient présents :

$$\boldsymbol{H} = \sum_j \hbar\omega_j \boldsymbol{Id}^{(1)} \otimes \cdots \otimes \boldsymbol{\sigma}_z^{(j)} \otimes \cdots \otimes \boldsymbol{Id}^{(n)} + 2\sum_{j<k} \hbar\omega_{jk} \boldsymbol{Id}^{(1)} \otimes \cdots \otimes \boldsymbol{\sigma}_z^{(j)} \otimes \cdots \otimes \boldsymbol{\sigma}_z^{(k)} \otimes \cdots \otimes \boldsymbol{Id}^{(n)}$$

$$\Rightarrow \qquad i\hbar\partial_t |\psi\rangle = \boldsymbol{H}|\psi\rangle$$

.

Dans cette équation les pulsations, ω, sont connues expérimentalement avec une grande précision. La solution s'écrit :

$$|\psi(t)\rangle =$$
$$\prod_j exp[-i\omega_j \boldsymbol{Id}^{(1)} \otimes \cdots \otimes \boldsymbol{\sigma}_z^{(j)} \otimes \cdots \otimes \boldsymbol{Id}^{(n)} t] \prod_{j<k} exp[-2i\omega_{jk} \boldsymbol{Id}^{(1)} \otimes \cdots \otimes \boldsymbol{\sigma}_z^{(j)} \otimes \cdots \otimes \boldsymbol{\sigma}_z^{(k)} \otimes \cdots \otimes \boldsymbol{Id}^{(n)} t] |\psi(0)\rangle$$

dont la forme matricielle est trop barbare pour figurer ici. Il suffit de retenir qu'on peut solliciter le système par un champ tournant à la pulsation, ω_{jk}, voulue ce qui introduit le terme $\boldsymbol{exp[-i(\pi/4)\sigma_z^{(c)} \otimes \sigma_z^{(t)}]}$ requis par la porte CNot.

Un lecteur attentif aura toutefois remarqué que la technique du champ résonant exige la présence d'un champ directeur constant orienté selon Oz qui a pour seule fonction de différencier les niveaux énergétiques et d'autoriser la résonance. Or ce champ sollicite tous les noyaux indistinctement y compris ceux que l'on ne veut pas voir évoluer à cet instant. Il convient de neutraliser cette évolution parasite et on y parvient en utilisant une astuce dont le principe repose sur la remarque suivante. Les évolutions quantiques étant unitaires, il doit toujours être possible de les invertir. Effectivement l'exemple suivant le montre : si un qubit évolue sous l'action de l'opérateur, $\boldsymbol{e}^{+i\alpha\sigma_z}$, il suffit de le soumettre à deux transformations supplémentaires de type, σ_x, à savoir dans cet ordre, $\boldsymbol{\sigma_x e^{+i\alpha\sigma_z} \sigma_x = e^{-i\alpha\sigma_z}}$, pour qu'il réintègre son état antérieur. On voit qu'à condition de tenir à jour sa comptabilité, il devient possible de programmer à la carte l'évolution des registres.

L'implémentation NMR remplit toutes les prescriptions du cahier des charges de l'ordinateur quantique sauf une : il ne semble pas possible d'étendre la dimension, n, du registre de travail au-delà de quelques dizaines de noyaux. Le nombre des fréquences de résonance augmente au moins quadratiquement (rien qu'en s'en tenant aux interactions spin-spin) en sorte que leur résolution devient problématique. On ne s'étonnera donc pas que si l'implémentation NMR a été la première à enregistrer un modeste succès, celui-ci tarde à être amélioré. L'ordinateur photonique présente quelques avantages du côté de la stabilité des qubits, peu influençables, mais il se heurte au même problème d'extensibilité des registres, du moins dans l'approche linéaire. L'optique non linéaire améliorerait la situation en pilotant des modifications d'indices de réfraction à partir de photons de contrôles (effet Kerr) mais les milieux non-linéaires connus ne sont pas suffisamment actifs. Les cristaux photoniques pourraient s'avérer utiles mais ils sont encore en plein développements.