

Introduction à la théorie quantique de l'information.



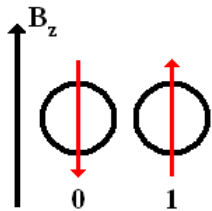
Richard Feynman



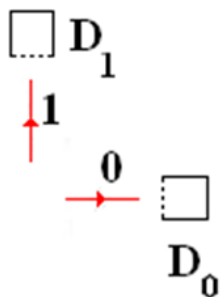
Charles Bennett

Bits & Qubits.

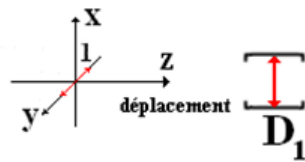
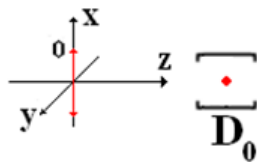
L'information est une grandeur quantifiée et le quantum d'information est le bit ou le qubit selon la nature, classique ou quantique, du support physique qui l'abrite. Voici quelques systèmes physiques élémentaires, capables d'encoder un qubit, ils nous serviront de fils conducteurs, notés, A, B et C.



A : Une particule porteuse d'un moment magnétique, μ , (électron, noyau, ...) adopte l'orientation parallèle ou anti parallèle lorsqu'elle est soumise à une induction magnétique extérieure : ce sont ses états de base. L'état '1' est plus probable que l'état '0' car son énergie, $E = -\vec{\mu} \cdot \vec{B} = -\mu_z B_z$ est moindre. Au zéro absolu, seul l'état '0' est possible.

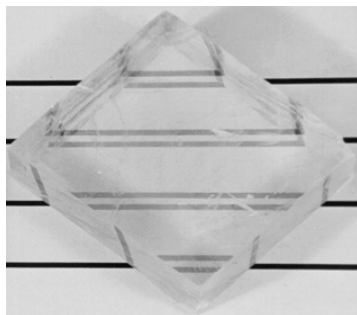


B : Un photon astreint à ne se déplacer que d'Ouest en Est ou de Sud en Nord, sur une table d'optique, encode également un qubit. Cet encodage repose sur les états spatiaux du photon, de loin les plus simples à comprendre. On évitera de les confondre avec les états de polarisation décrits ci-après et qui réclament davantage d'explications.

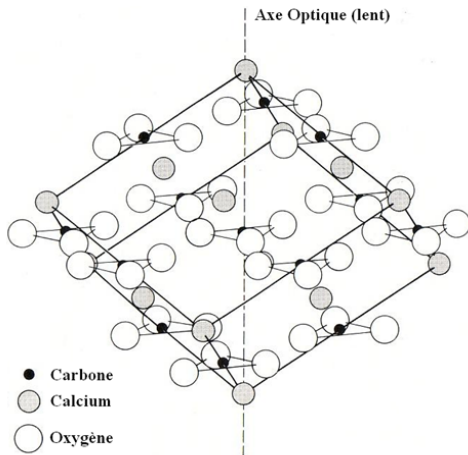


C : Le même photon autorise un autre encodage du qubit, selon son état de polarisation linéaire, parallèle à Ox ou à Oy. On différencie ces états en interposant un polariseur analyseur sur le trajet du photon.

Il laisse passer la lumière polarisée selon sa propre direction passante et absorbe la lumière polarisée perpendiculairement. Pour rappel, il n'existe pas de photons polarisés longitudinalement et cela est en rapport avec le fait que le photon ne possède que deux états internes de spin.

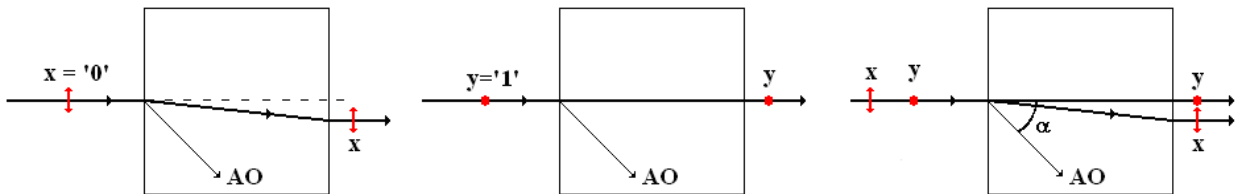


L'œil humain n'est pas équipé pour distinguer les deux états de polarisation de la lumière, il lui faut de l'aide. Une aide possible est fournie par un cristal biréfringent, de calcite (CaCO_3), par exemple. Celui-ci, taillé en forme de lame à faces parallèles, fournit généralement deux images de tout objet, posé en-dessous de lui. Une image, dite ordinaire, est simplement dans l'axe de l'objet tandis que l'autre, dite extraordinaire, est décalée par rapport à l'objet. Ce comportement résulte de l'anisotropie dans la disposition des atomes au sein du cristal.



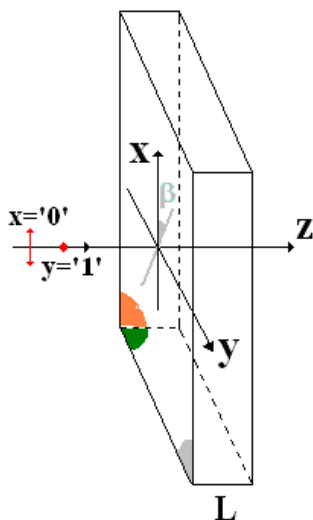
Une conséquence de cette anisotropie est que la lumière se déplace plus lentement dans la direction de l'axe optique que dans n'importe quelle direction orthogonale.

Autrement dit l'indice de réfraction, n , dépend de la direction de propagation de la lumière et dans le cas de la calcite, il est maximum dans la direction de l'axe optique. Une lame de calcite sépare donc les états de polarisation de la lumière en ses composantes parallèles ou perpendiculaires à l'axe optique. Les 2 figures suivantes (à gauche) distinguent clairement les deux cas puis elles envisagent (à droite) le cas où la lumière est un mélange des deux types de polarisation.



Les photons polarisés selon y (resp. x) subissent une réfraction (extra)ordinaire. L'angle, r_e , que font les rayons réfractés ordinaire et extraordinaire est donné par la relation suivante :

$$\text{tg}(r_e) = \frac{(n_e^2 - n_o^2) \sin \alpha \cos \alpha}{n_o^2 \sin^2 \alpha + n_e^2 \cos^2 \alpha}$$



Un cas particulier s'avère essentiel pour la suite, soit lorsque $\alpha=90^\circ$. La lame de calcite est alors taillée parallèlement à l'axe optique et les photons sortent de la lame selon une trajectoire unique quel que soit leur état de polarisation. Dans cette disposition, les deux paramètres essentiels de la lame sont d'une part l'angle, β , que l'axe optique fait avec l'axe Ox et le déphasage, δ , relié à l'épaisseur de la lame par la relation, $\delta = \frac{2\pi(\Delta n)L}{\lambda}$ (où, $\Delta n = n_e - n_o$). Cette lame est l'outil de choix permettant de modifier à loisir la polarisation des photons.

Plus généralement, tout système quantique possédant n états discrets peut encoder un alphabet à n symboles et le cas, $n=2$, correspond évidemment à l'encodage binaire. On trouve, en annexe, l'exemple de l'encodage d'un qutrit à l'aide d'une particule chargée de spin 1.

Vecteur d'état d'un qubit.

Dans le formalisme de la mécanique quantique, les états de base du qubit sont représentés par deux vecteurs, notés, $|0\rangle$ et $|1\rangle$. Ils évoluent dans un espace de Hilbert à 2 dimensions où ils acceptent la représentation matricielle, $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Ils sont orthonormés :

$$\langle 0|0\rangle = \langle 1|1\rangle = 1 \quad \text{et} \quad \langle 0|1\rangle = \langle 1|0\rangle = 0$$

Préparer un qubit dans son état de base $|0\rangle$ est chose plus ou moins aisée :

A : Il "suffit" d'abaisser progressivement la température du noyau : en pompant l'énergie du système, on l'amène à coup sûr dans son état d'énergie minimum.

B : Il suffit d'orienter le faisceau de lumière d'ouest en est.

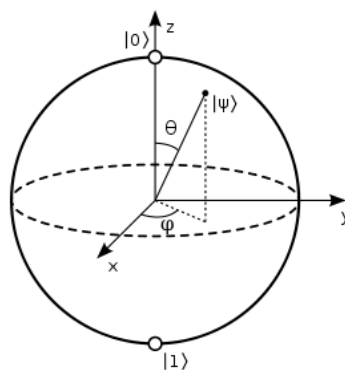
C : Il suffit d'absorber toute composante polarisée selon Oy au moyen d'un filtre polarisant orienté selon Ox.

Alors qu'un bit classique n'existe que dans l'un ou l'autre de ses états de base, 0 ou 1, un qubit peut exister dans un état quelconque de superposition quantique,

$$|\psi\rangle = c_1|0\rangle + c_2|1\rangle$$

Cependant le contenu informationnel n'excède pas 1 bit pour autant : il est inscrit dans les principes de la mécanique quantique que toute mesure ne peut révéler aléatoirement que l'un ou l'autre des états, $|0\rangle$ (avec la probabilité, $|c_1|^2$) ou $|1\rangle$ (avec la probabilité, $|c_2|^2$). Les coefficients c_1 et c_2 doivent donc respecter la relation de normalisation, $|c_1|^2 + |c_2|^2 = 1$.

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi} \sin(\theta/2)|1\rangle \quad (0 \leq \theta \leq \pi, \quad 0 \leq \varphi < 2\pi).$$



Cet état admet une représentation géométrique immédiate sous la forme d'un point de coordonnées sphériques, θ et φ , sur la sphère de Bloch. Les pôles N et S sont associés aux états de base, $|0\rangle$ et $|1\rangle$, tandis que l'équateur correspond aux états, $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle)$.

Evolution du qubit isolé.

Un qubit reste dans l'état où on l'a préparé tant qu'il n'est pas soumis à une intervention externe. Dans le formalisme de la mécanique quantique, un opérateur unitaire est associé à toute transformation affectant l'état d'un qubit. Il agit sur cet état et le modifie conformément à la règle,

$$|new\ state\rangle = O|old\ state\rangle$$

Les systèmes quantiques purs étant exempts de toutes formes de frottements, il en résulte qu'aucune énergie n'est jamais dissipée. Vu le principe de Landauer, il s'ensuit une absence de perte d'information. Tout opérateur agissant sur le qubit isolé doit donc être unitaire, afin de préserver la norme des vecteurs d'états auxquels il est appelé à s'appliquer, il donc être de la forme générale suivante ($n_x^2 + n_y^2 + n_z^2 = 1$) :

$$\begin{aligned} U &= e^{i\alpha} [(\cos \omega + i n_z \sin \omega) |0\rangle\langle 0| + (i n_x + n_y) \sin \omega |0\rangle\langle 1| + \\ &\quad (i n_x - n_y) \sin \omega |1\rangle\langle 0| + (\cos \omega - i n_z \sin \omega) |1\rangle\langle 1|] \\ &= e^{i\alpha} \begin{pmatrix} \cos \omega + i n_z \sin \omega & i(n_x - i n_y) \sin \omega \\ i(n_x + i n_y) \sin \omega & \cos \omega - i n_z \sin \omega \end{pmatrix} = e^{i\alpha} [\cos \omega \text{ Id} + i \sin \omega \vec{n} \cdot \vec{\sigma}] \end{aligned}$$

où les matrices 2x2, σ_x , σ_y et σ_z , sont les matrices de Pauli.

L'opérateur général, U, transforme l'état $|0\rangle$ en l'état de superposition le plus général dans lequel le qubit peut exister :

$$U|0\rangle = e^{i\alpha} [(\cos \omega + i n_z \sin \omega) |0\rangle + (i n_x - n_y) \sin \omega |1\rangle]$$

qu'on réécrit généralement, à une phase inessentielle près, sous la forme canonique,

$$|\psi\rangle = \cos(\theta/2) |0\rangle + e^{i\varphi} \sin(\theta/2) |1\rangle \quad (0 \leq \theta \leq \pi, \quad 0 \leq \varphi < 2\pi)$$

En pratique, on n'a pas besoin de considérer la transformation unitaire générale, U. On se contente de trois cas particuliers, Not, H (Hadamard) et Φ (déphasage), plus faciles à appréhender, et qui, par assemblage convenable, sont de toutes façons capables de reproduire le cas général. Ces trois cas se notent :

- Porte Not ($n_x=1, n_y=n_z=0, \omega=\pi/2$) :

$$Not = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

On vérifie que l'on a bien :

$$\begin{aligned} NOT|0\rangle &= |1\rangle \\ NOT|1\rangle &= |0\rangle \end{aligned}$$

- Porte H, de Hadamard ($n_y=0$, $n_x=n_z=1/\sqrt{2}$, $\omega=\pi/2$) :

$$H = \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

La porte de Hadamard transforme les états de base en états de superpositions équilibrées :

$$H|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{et} \quad H|1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

- Porte Φ , de déphasage ($n_z=1$, $n_x=n_y=0$) :

$$\Phi(\varphi) = |0\rangle\langle 0| + e^{i\varphi}|1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

$$\Phi|0\rangle = |0\rangle \quad \text{et} \quad \Phi|1\rangle = e^{i\varphi}|1\rangle$$

Voyons à présent comment on peut implémenter la transformation unitaire, U, dans les trois cas qui nous servent d'exemples.

A : Bien que la méthode soit inapplicable à un noyau isolé (sans contaminer les voisins), une induction magnétique constante, $\vec{B} = (B_x, B_y, B_z)$, appliquée pendant un temps, t, à une particule de moment magnétique, μ , agit comme une porte logique,

$$P(\vec{B}, t) = (\cos[\frac{\mu_B B}{2\hbar} t] + i \frac{B_z}{B} \sin[\frac{\mu_B B}{2\hbar} t]) |0\rangle\langle 0| + \frac{iB_x + B_y}{B} \sin[\frac{\mu_B B}{2\hbar} t] |0\rangle\langle 1| + \frac{iB_x - B_y}{B} \sin[\frac{\mu_B B}{2\hbar} t] |1\rangle\langle 0| + (\cos[\frac{\mu_B B}{2\hbar} t] - i \frac{B_z}{B} \sin[\frac{\mu_B B}{2\hbar} t]) |1\rangle\langle 1|$$

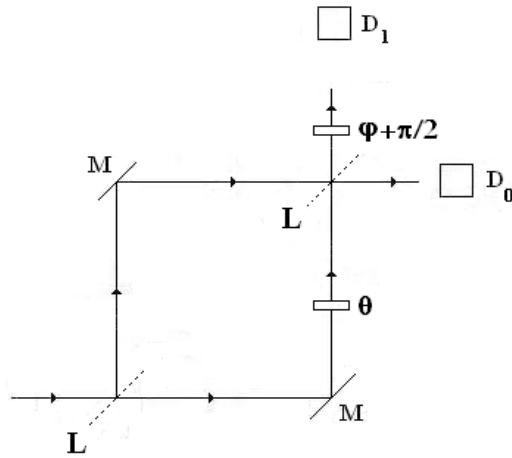
$$= \begin{pmatrix} \cos[\frac{\mu_B B}{2\hbar} t] + i \frac{B_z}{B} \sin[\frac{\mu_B B}{2\hbar} t] & \frac{iB_x + B_y}{B} \sin[\frac{\mu_B B}{2\hbar} t] \\ \frac{iB_x - B_y}{B} \sin[\frac{\mu_B B}{2\hbar} t] & \cos[\frac{\mu_B B}{2\hbar} t] - i \frac{B_z}{B} \sin[\frac{\mu_B B}{2\hbar} t] \end{pmatrix}$$

- Une induction magnétique constante, B_x , orientée selon Ox et agissant sur le noyau pendant un temps, $t = \frac{\hbar}{2\mu B_x}$, équivaut donc à une porte **NOT**, à une phase inessentielle près.

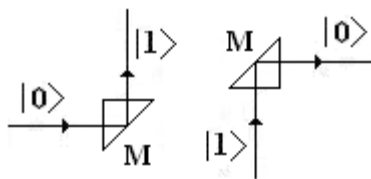
- Une induction magnétique constante, $\vec{B} = \frac{1}{\sqrt{2}}(B, 0, B)$, agissant pendant un temps, $t = \frac{\hbar}{2\mu B_x}$, équivaut à une porte de Hadamard, à une phase globale près.

- Une induction magnétique constante, B_z , orientée selon Oz pendant un temps, $t = \frac{\varphi\hbar}{\mu B_z}$, équivaut à une porte de déphasage, à une phase globale près.

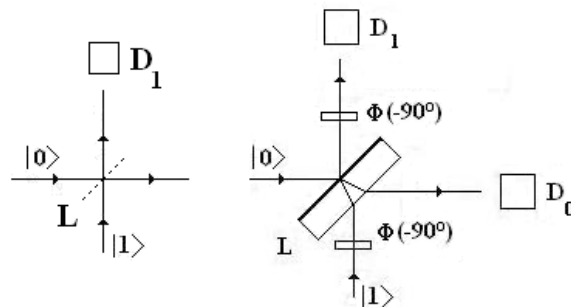
B : Un interféromètre de Mach-Zehnder, muni de lames retardatrices simulant les déphasages adéquats, transforme l'état de base, $|0\rangle$, en $\cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle$ (à une phase près).



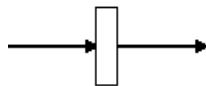
- Le miroir (mieux, un prisme à réflexion totale afin d'éviter un déphasage parasite de π dans le cas du miroir) équivaut à une porte NOT.



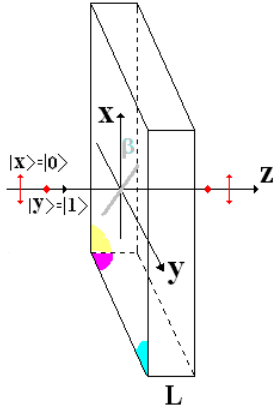
- La lame semi-transparente équivaut à une porte de Hadamard. Pour être tout-à-fait exact, il faut mentionner que la lame semi-transparente possède une épaisseur non nulle et qu'un déphasage valant π est induit à chaque réflexion s'opérant de l'air dans le verre. On ne prend généralement pas la peine de dessiner le montage complet et il suffit de savoir que la lame pointillée doit en fait être dessinée comme suit :



- Une simple lame retardatrice à faces parallèles, de verre d'indice, n , et d'épaisseur, d , induit un déphasage valant, $2\pi n x / \lambda$. Elle implémente la porte Φ .



C :



On montre, en optique (ne précisez pas quantique, ce serait un pléonasme, car les équations de Maxwell sont les équations de Dirac du photon : elles sont automatiquement relativistes et quantiques), qu'une lame biréfringente, taillée parallèlement à l'axe optique de telle façon que cet axe fasse un angle de β avec Ox, équivaut à une porte logique dont l'opérateur se note :

$$Lame(\beta, \delta) = (e^{i\delta/2} \cos^2 \beta + \sin^2 \beta) |0\rangle\langle 0| + i \sin(2\beta) \sin(\delta/2) |0\rangle\langle 1| + i \sin(2\beta) \sin(\delta/2) |1\rangle\langle 0| + (e^{-i\delta/2} \cos^2 \beta + e^{i\delta/2} \sin^2 \beta) |1\rangle\langle 1|$$

où δ est relié à l'épaisseur de la lame via la relation : $\delta = \frac{2\pi(\Delta n)L}{\lambda}$ (où Δn représente la différence entre les indices ordinaire et extraordinaire).

- Une lame biréfringente demi-onde ($\delta=\pi$), orientée à $\beta=45^\circ$, est une porte NOT à un facteur i inessentiel près :

$$Lame(\pi/4, \pi) = i(|0\rangle\langle 1| + |1\rangle\langle 0|)$$

- Une lame biréfringente demi-onde ($\delta=\pi$), orientée à $\beta=22.5^\circ$, est une porte de Hadamard à un facteur, i , inessentiel près :

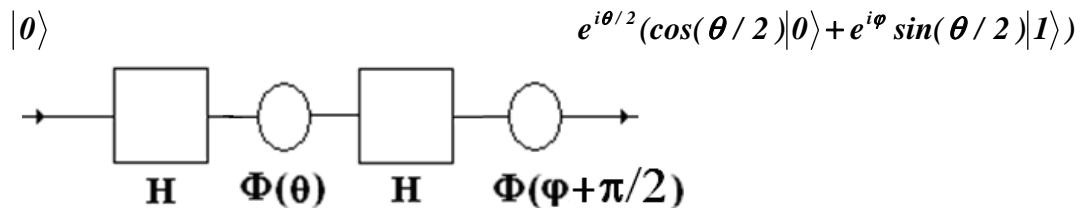
$$Lame(\pi/8, \pi) = \frac{i}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)$$

- Une lame biréfringente, orientée à 0° , est une porte de déphasage :

$$Lame(0, \delta) = e^{i\delta/2}(|0\rangle\langle 0| + e^{-i\delta}|1\rangle\langle 1|)$$

Universalité du couple, H et Φ , pour la préparation du qubit isolé.

Pour préparer un qubit dans un état de superposition arbitraire, on part d'un qubit préparé dans l'état $|0\rangle$, que l'on fait basculer dans l'état souhaité par application de 4 portes logiques, deux portes de Hadamard, H, et deux portes de déphasage, Φ .



On n'accorde aucune importance à la phase excédentaire $e^{i\theta/2}$: elle affecte globalement le vecteur d'état final et n'entraîne de ce fait aucune conséquence observable. La représentation matricielle de cet ensemble s'obtient tout naturellement en multipliant les matrices dans l'ordre inverse, ce qui donne :

$$U(\theta, \varphi) = \Phi(\theta + \pi/2) \cdot H \cdot \Phi(\varphi) \cdot H = e^{i\theta/2} \begin{pmatrix} \cos(\theta/2) & -i \sin(\theta/2) \\ e^{i\varphi} \sin(\theta/2) & ie^{i\varphi} \cos(\theta/2) \end{pmatrix}$$

et on vérifie que l'on a bien :

$$\begin{aligned} U(\theta, \varphi)|0\rangle &= e^{i\theta/2} \begin{pmatrix} \cos(\theta/2) & -i \sin(\theta/2) \\ e^{i\varphi} \sin(\theta/2) & ie^{i\varphi} \cos(\theta/2) \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = e^{i\theta/2} \begin{pmatrix} \cos(\theta/2) \\ e^{i\varphi} \sin(\theta/2) \end{pmatrix} \\ &= e^{i\theta/2} (\cos(\theta/2)|0\rangle + e^{i\varphi} \sin(\theta/2)|1\rangle) \end{aligned}$$

En résumé, les portes H et Φ suffisent à construire l'état de superposition le plus général du qubit isolé; on dit qu'elles forment un couple universel pour la préparation du qubit isolé.

Non clonage d'un qubit inconnu.

Un observateur qui reçoit un qubit en état de superposition est incapable de prendre connaissance de ses coefficients exacts, c_1 et c_2 . Toute mesure de sa part ne peut, en effet, révéler que l'un ou l'autre résultat, $|0\rangle$ (avec la probabilité, $|c_1|^2$) ou $|1\rangle$ (avec la probabilité, $|c_2|^2$). Autrement dit, cet observateur est dans l'incapacité de cloner ce qubit inconnu puisque toute mesure est, par essence, destructrice de l'état à copier. Insistons sur le fait qu'il est, par contre, parfaitement possible de cloner un qubit dont l'état est connu : il suffit de le fabriquer en respectant la procédure qui précède.

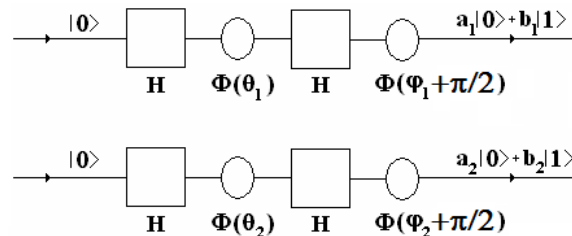
L'impossibilité liée au clonage de qubits inconnus est à la base de la distribution (quantique) totalement sécurisée des clés cryptographiques. Ce point sera évoqué dans la section consacrée aux applications des algorithmes quantiques.

Remarque 1 : la situation change quelque peu si l'observateur reçoit en continu des copies exactes d'un même qubit inconnu. Une étude statistique permet de remonter des probabilités observées vers les modules des coefficients. Pour remonter aux phases, une mesure après déphasage contrôlé est nécessaire. L'opération de recouvrement s'apparente à une stratégie tomographique.

Remarque 2 : l'existence des superpositions d'états quantiques ne signifie nullement que le contenu informationnel observable du qubit excède la valeur classique de 1 bit car toute lecture de son contenu passe par une mesure quantique qui a pour effet de projeter cet état sur un des états propres associés à l'appareil de mesure.

Notion de registre.

On ne va pas très loin avec un qubit isolé ! Plusieurs qubits constituent un registre. Les portes H et Φ suffisent pour préparer les qubits individuels de ce registre dans un état de superposition quelconque mais elles ne suffisent pas pour préparer le registre dans son état de superposition le plus général. Voyons le cas de 2 qubits.



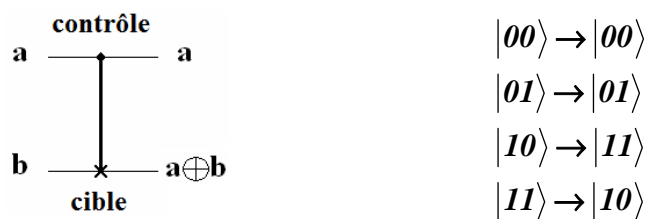
Même si l'on prépare chaque qubit dans son état le plus général, le registre ne peut se trouver que dans un état séparable,

$$(a_1|0\rangle + b_1|1\rangle)(a_2|0\rangle + b_2|1\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

Jamais on ne parviendra à le préparer, de cette manière, dans un état non séparable - on dit intriqué - par exemple, dans l'état $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Cette limitation est intolérable dès que l'on a en vue de construire un ordinateur calculant tout ce qui est calculable. On verra un exemple lors du développement d'un algorithme quantique de factorisation par transformée de Fourier.

La porte CNot.

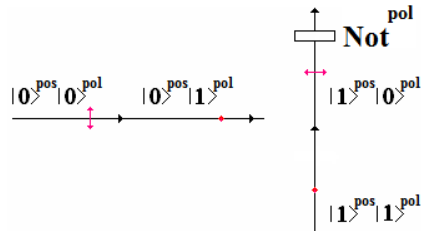
Il manque une porte pour préparer un registre dans n'importe quel état intriqué, c'est la porte CNot. Cette porte agit sur deux qubits solidaires, le contrôle et la cible, $|contrôle\rangle|cible\rangle$. Elle se contente d'inverser la cible si et seulement si le contrôle vaut 1 :



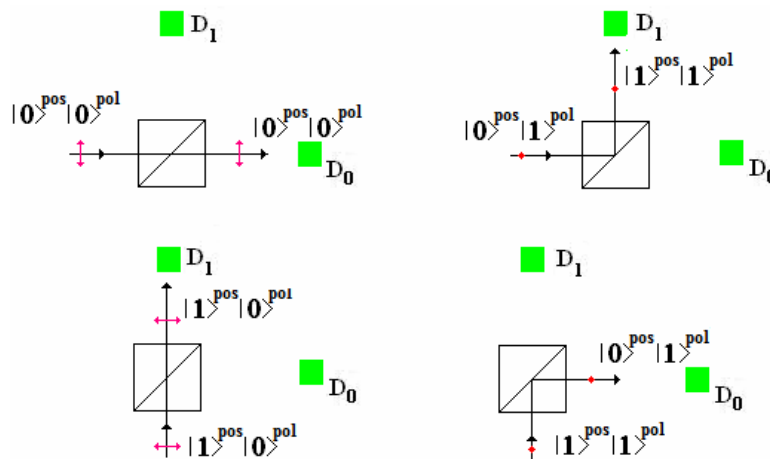
Une implémentation sur base d'un qubit magnétique est possible mais elle n'est pas assez simple pour figurer dans un exposé élémentaire. On peut en dire autant d'une implémentation photonique recourant à deux photons distincts : les photons n'interagissant pas, on est contraint d'utiliser le 2^{ème} photon pour modifier l'indice de réfraction du milieu emprunté par le premier photon. Cette manœuvre recourt à un effet (Kerr) d'optique non linéaire. La technique prometteuse n'est pas opérationnelle actuellement par manque de milieux suffisamment actifs.

On se contente ici de rester dans le domaine de l'optique linéaire, axant deux implémentations distinctes mais équivalentes, sur base des qubits de position et de polarisation d'un même photon.

B : 1^{ère} version : contrôle = position et cible = polarisation (Une *Lame*($\pi/4, \pi$) fait l'affaire) :

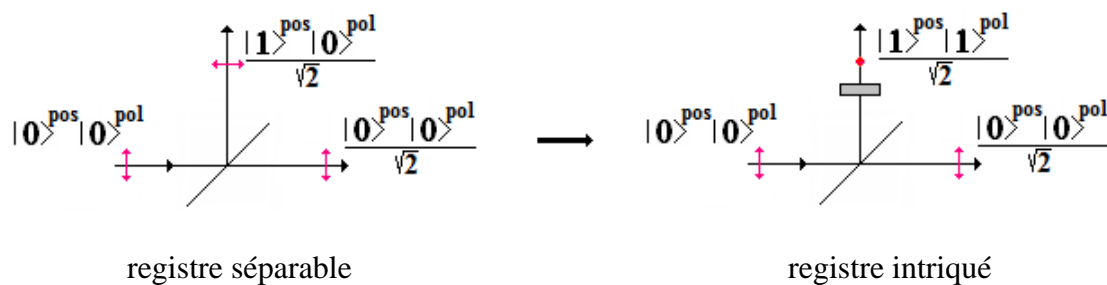


C : 2^{ème} version : contrôle = polarisation et cible = position (Un prisme séparateur polarisant fait l'affaire, qui transmet la polarisation selon x et réfléchit la polarisation selon y) :

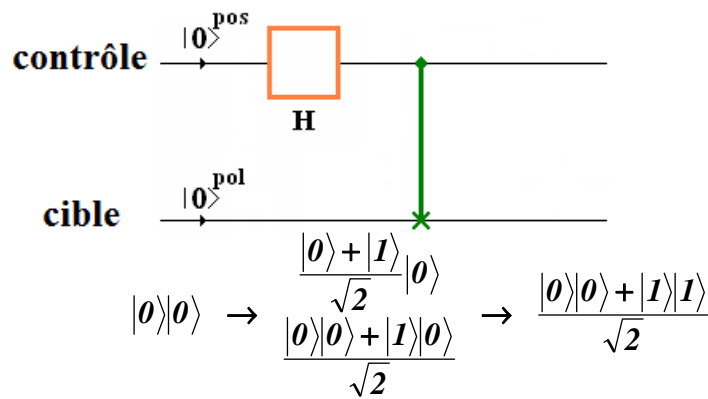


Universalité du triplet, H , Φ et CNot pour la préparation de registres intriqués.

L'adjonction de la porte CNot permet d'envisager la construction d'un registre quelconque; Montrons, à titre d'exemple, que H et CNot suffisent pour fabriquer l'état intriqué, dit de Bell, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

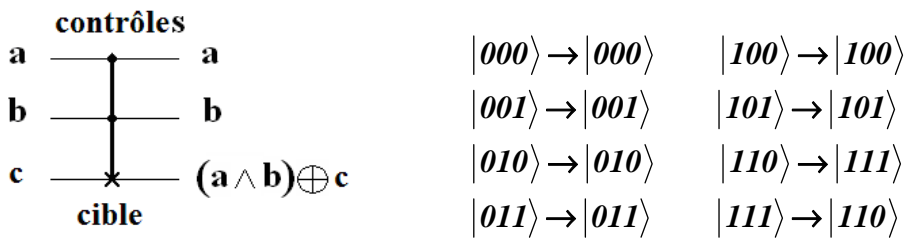


ou sous forme de diagramme générique :

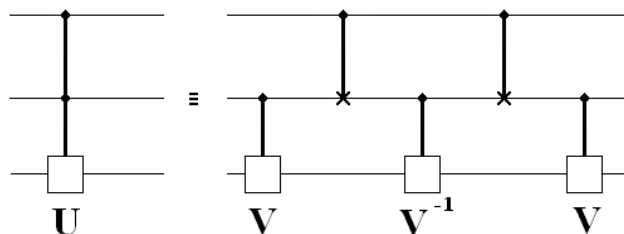


La porte CCNot.

Une porte agissant sur trois qubits est d'un emploi fréquent, c'est la porte CCNot, encore appelée porte de Toffoli. Elle utilise deux qubits de contrôle et un qubit cible, n'inversant la cible que si les deux contrôles valent 1.



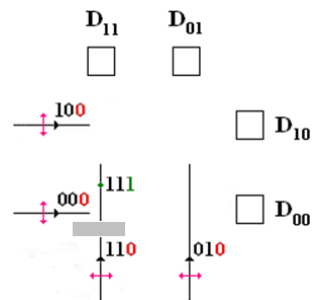
Cette porte est déductible des portes H et Φ mais le montage est tellement compliqué qu'on préfère la définir une fois pour toute en lui donnant un nom. De façon générale, toute porte CCU (qui n'exerce une transformation unitaire donnée U que si les deux contrôles valent 1) peut être construite sur base de la racine carrée, V, de U ($V^2=U$) :



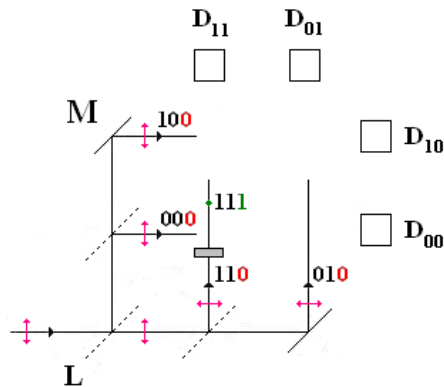
Dans l'exemple de la porte de Toffoli, on a que U=Not, d'où on a :

$$V = e^{i\pi/4} \Phi(-\pi/2) \cdot H \cdot \Phi(-\pi/2) = e^{i\pi/4} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}$$

Trois qubits étant concernés, il semblerait que deux photons soient nécessaires dans une implémentation photonique de la porte CCNot, comme dans le montage suivant où on considère les états spatiaux de deux photons et l'état de polarisation de l'un d'entre eux :

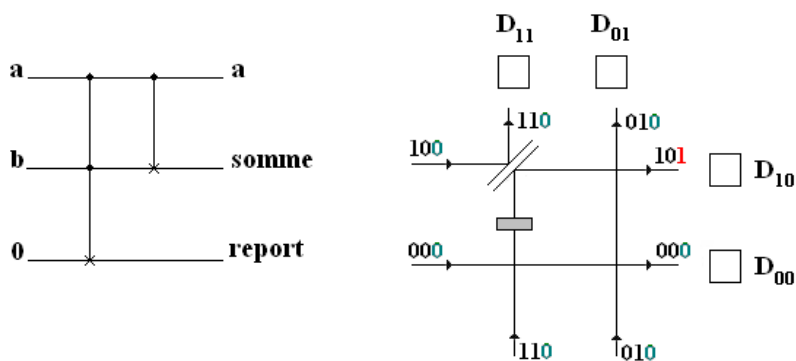


Cependant un photon unique peut faire l'affaire à condition de démultiplier le nombre des lames semi transparentes, comme dans le montage suivant :



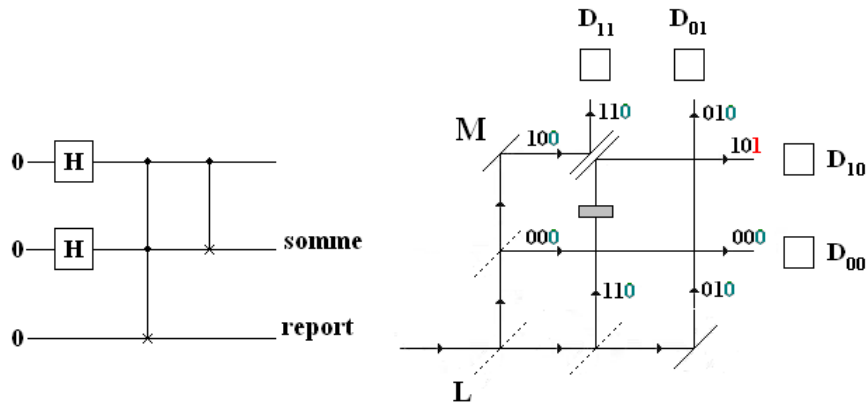
Semi-additionneur binaire.

Une porte CCNot plus une porte CNot suffisent pour construire un semi additionneur binaire, qui calcule la somme de deux entiers, 0 ou 1, modulo 2, ainsi que le report correspondant. Voici le diagramme et l'implémentation sur base de deux photons :



On voit que pour obtenir le résultat de l'addition modulo 2, il suffit de lancer un photon sur la bonne trajectoire. Toutefois ce calcul d'une instance particulière ne présente aucun intérêt par rapport à ce qu'un ordinateur classique apporterait.

L'intérêt de la procédure quantique réside dans la possibilité de mettre les 4 instances de l'addition modulo2 en parallèle, les calculant toutes en un seul passage :



Dans ce montage, la première lame semi transparente incarne la porte H du premier qubit, les deux autres lames incarnent conjointement la deuxième porte H, la lame biréfringente incarne la porte CCNot et le miroir double face incarne la porte CNot.

Si on alimente ce circuit par un photon unique, dans l'état $|0\rangle$, et que l'on mesure l'état du registre de sortie, on s'attend à trouver un des 8 états possibles,

$$|000\rangle |001\rangle |010\rangle |011\rangle |100\rangle |101\rangle |110\rangle |111\rangle$$

En fait, le calcul détaillé de l'évolution du registre montre qu'on n'observe que 4 cas :

$$\begin{aligned} |0\rangle|0\rangle|0\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle = \frac{1}{2}(|0\rangle|0\rangle|0\rangle+|0\rangle|1\rangle|0\rangle+|1\rangle|0\rangle|0\rangle+|1\rangle|1\rangle|0\rangle) \\ &\rightarrow \frac{1}{2}(|0\rangle|0\rangle|0\rangle+|0\rangle|1\rangle|0\rangle+|1\rangle|0\rangle|0\rangle+|1\rangle|1\rangle|1\rangle) \\ &\rightarrow \frac{1}{2}(|0\rangle|0\rangle|0\rangle+|0\rangle|1\rangle|0\rangle+|1\rangle|1\rangle|0\rangle+|1\rangle|0\rangle|1\rangle) \end{aligned}$$

On a effectivement calculé les 4 instances de l'addition mod 2 en parallèle, mais la mesure ne révèle qu'un seul résultat avec une probabilité définie et encore on ne sait généralement même pas quelle instance a été calculée ! Tout se passe comme si on avait trouvé une réponse sans savoir à quel énoncé elle correspond !

A ce stade on est en droit de se demander quel peut bien être l'intérêt de la procédure quantique. En tous cas, la programmation d'un ordinateur quantique promet d'être très différente de celle d'un ordinateur classique. Une issue possible repose sur le fait qu'on puisse construire des circuits quantiques qui privilégient l'occurrence des résultats intéressants au détriment des résultats inintéressants. Le circuit qui calcule la transformée de Fourier discrète d'une suite est de ce type. Il reparaitra lors de l'étude de l'algorithme de Schor.

Circuit quantique calculant la transformée de Fourier discrète d'une suite.

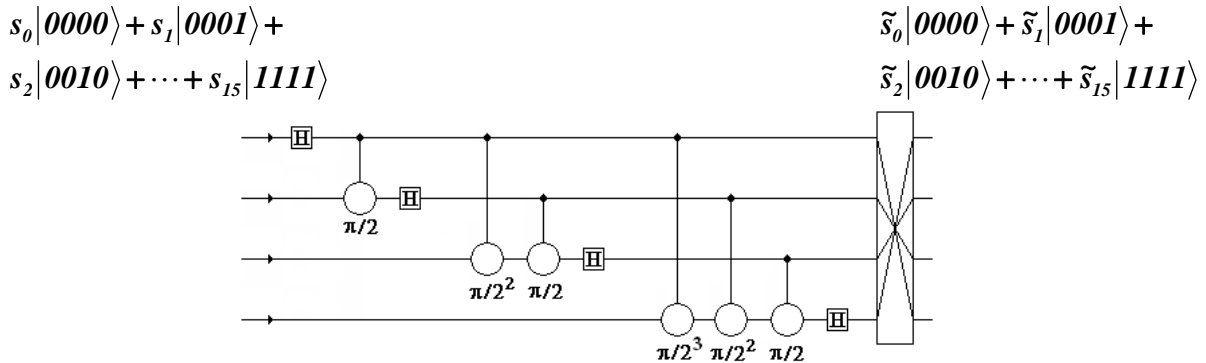
La transformée de Fourier discrète (TFD) d'une suite, s_k ($k=0, 1, \dots, N-1$), est définie comme suit :

$$s_j \rightarrow \tilde{s}_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \text{Exp}[2i\pi \frac{jk}{N}] s_k$$

Le principe de l'encodage binaire de la suite au niveau d'un seul registre fait que l'on considère uniquement les cas où N est une puissance de 2, $N=2^n$:

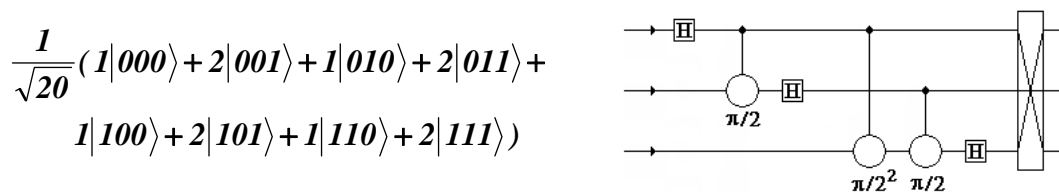
$$s_j \rightarrow \tilde{s}_j = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \text{Exp}[2i\pi \frac{jk}{2^n}] s_k$$

La suite, s_k , est encodée au niveau du registre d'entrée en temps que coefficients d'une superposition (normalisée) des états de base. La plupart du temps l'état du registre est intriqué car les états complètement séparables sont l'exception. Le circuit est composé de n portes de Hadamard et de $n(n-1)/2$ portes de déphasages disposées comme sur la figure suivante correspondant au cas, $n=4$. Le registre de sortie affiche un état de superposition dont les coefficients sont les composantes de la TFD cherchée. A noter la présence d'un inverseur qui a pour but de permettre la lecture du registre de sortie dans l'ordre naturel.

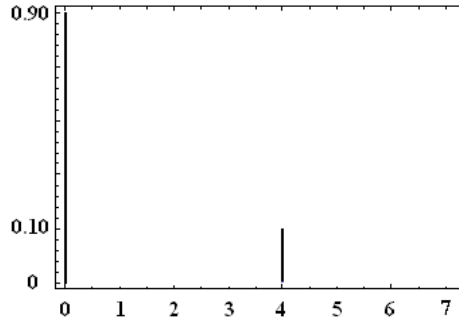


Bien que le circuit calcule la TFD complète en un seul passage, on n'y a pas vraiment accès : toute mesure du registre de sortie ne peut révéler que 0 ou 1 sur chaque qubit, constituant un binaire, B , apparaissant avec la probabilité, $|\tilde{s}_B|^2$. Pour remonter aux coefficients, il faudrait recommencer l'opération un grand nombre de fois et procéder par tomographie.

Voici l'exemple simpliste de la suite, de longueur 8, $\{1, 2, 1, 2, 1, 2, 1, 2\}$ analysée par une TFD de dimension, $n=3$:



Dans ce cas, la lecture du registre de sortie livre 000 (=0₂) dans 90% des cas et 100 (=4₂) dans 10% des cas; les 6 autres cas n'apparaissent jamais. Le graphe de cette distribution correspond au carré du module de la TFD cherchée, $|\tilde{s}_B|^2$. Il suffit pour constater que la suite d'entrée est périodique et pour déterminer sa période, 2 (=2ⁿ/B=8/4).

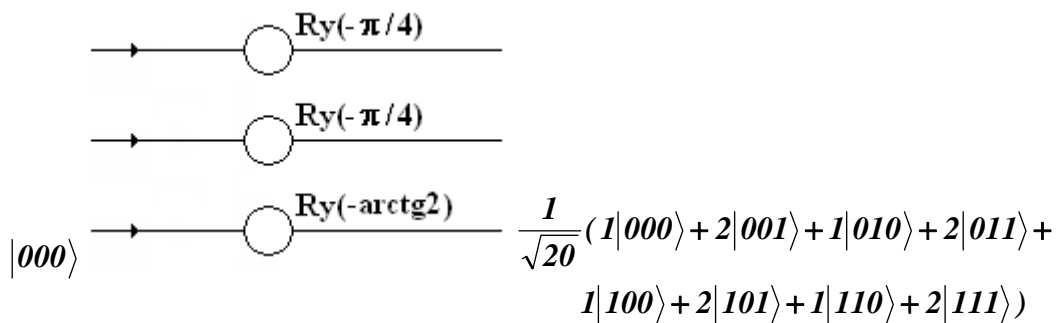


Il importe d'être conscient que l'encodage de l'état du registre d'entrée,

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

exige un circuit préparatoire qui transforme l'état initial, disons, $|000\rangle$, en cet état d'entrée. En principe, un assemblage correct de portes, H, Φ et CNot, est toujours possible puisqu'il est universel pour tout registre. En fait, dans cet exemple, tout est relativement simple car le registre est séparable. On le voit directement en observant que le polynôme suivant est entièrement factorisable en facteurs successifs de, $(1 + \lambda u^{2^k}) (k=0, 1, \dots, n=2)$,

$$1 + 2u + u^2 + 2u^3 + u^4 + 2u^5 + u^6 + 2u^7 = (1 + 2u)(1 + u^2)(1 + u^4)$$



La porte, Ry, associée à la matrice de Pauli de même indice, est évidemment déductible des portes de base pour le qubit isolé, H et Φ :

$$R_y(-2\theta) = e^{i\theta\sigma_y} = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix} = e^{i\theta} \Phi(\pi/2) \cdot H \cdot \Phi(-2\theta) \cdot H \cdot \Phi(-\pi/2)$$

Il suffit à présent de concaténer les deux circuits quantiques pour obtenir, en un seul passage, l'analyse de Fourier de la suite donnée, $\{1, 2, 1, 2, 1, 2, 1, 2\}$.

