Information quantique–cours

Paul Baird

1. Les postulats de la mécanique quantique

Outils mathématiques : L'objet de base est un *espace séparable de Hilbert* H – il s'agit d'un espace vectoriel sur les complexes muni d'une base dénombrable et d'un produit scalaire hermitien $\langle v|w\rangle$: $\langle av|w\rangle = \overline{a}\,\langle v|w\rangle$. Dans ce cours $H = \mathbf{C}^n$ muni du produit hermitien $\langle v|w\rangle = \sum_j \overline{v_j} w_j$ $(v = (v_1, \ldots, v_n))$.

Un *opérateur hermitien* $A : H = \mathbf{C}^n \to \mathbf{C}^n$ est une transformation linéaire vérifiant $A = A^*$ où A^* est la transposée conjuguée de A. Les valeurs propres d'une telle transformation sont réelles et les espaces propres corréspondants aux valeurs propres distincts sont orthogonaux par rapport au produit hermitien.

Une *transformation unitaire* $U : \mathbf{C}^n \to \mathbf{C}^n$ est une transformation linéaire qui respecte le produit scalaire : $\langle v|w\rangle = \langle Uv|Uw\rangle$ ce qui revient au fait que $UU^* = I_n$ (la matrice identité de rang n).

Notation : En dimension 2:

$$|v\rangle = \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} = v_0\,|0\rangle + v_1\,|1\rangle \qquad \langle v| = |v\rangle^* = \begin{pmatrix} \overline{v_0} & \overline{v_1} \end{pmatrix}$$

où $\{|0\rangle, |1\rangle\}$ est une base orthonormée. En dimension n, une base o. n. s'écrit : $\{|1\rangle, |2\rangle, \ldots, |n\rangle\}$ et $v_j = \langle j|v\rangle$. Si $A : H \to H$ est un opérateur linéaire , alors le coefficient $A_{mn} = \langle m|A|n\rangle$. Un opérateur linéaire particulier est donné par $|v\rangle\langle w| : H \to H$, $|v\rangle\langle w| = \sum_{i,j} v_i \overline{w_j}\,|i\rangle\langle j|$. L'opérateur $|v\rangle\langle v|$ est le projecteur P_v sur le sous-espace engendré par le vecteur v. Si $L \subset H$ est un sous-espace muni de la base o. n. $j = 1, \ldots m$, alors

$$P_L = \sum_{j=1}^{m} |j\rangle\langle j|$$

est le projecteur sur L. On remarque que ${P_L}^2 = P_L$, ce qui caractérise de telles applications linéaires. La *relation de complétitude* est le fait que $\sum_{j=1}^{n} |j\rangle\langle j| = I_n$.

Les postulats : **1. Système** : À un système physique on associe un espace séparable complexe H. Les rayons dans H correspondent aux états du système. Habituellement on normalise un état afin de representer un état par $|\varphi\rangle \in H$ tel que $\langle\varphi|\varphi\rangle = ||\varphi||^2 = 1$. À noter qu'il reste toujours une liberté de phase : $\langle e^{i\theta}\varphi|e^{i\theta}\varphi\rangle = \langle\varphi|\varphi\rangle$.

L'espace de Hilbert d'un système composé est le produit tensoriel des espaces associés à chaque composante.

2. Observable : A toute propriété observable (un *observable*) correspond un opérateur hermitien A sur H. Pour un système dans l'état $|\varphi\rangle$, l'espérance de A est donné par $\langle\varphi|A|\varphi\rangle$.

3. Mesure : La mesure d'une grandeur physique représentée par l'observable A ne peut fournir que l'une des valeurs propres de A . Si la mesure de la grandeur physique A sur un système représenté par le vecteur $|\varphi\rangle$ donne comme résultat la valeur propre a_n , alors l'état du système immédiatement après la mesure est projeté sur le sous-espace propre associé à a_n .

Remarques complémentaires : Si $|\varphi\rangle$ et $|\psi\rangle$ sont deux états normalisés ; la amplitude de probabilité $a(\varphi \to \psi)$ de trouver φ en état ψ est donnée par $\langle\psi|\varphi\rangle$ et la probabilité que φ passe le test ψ est :

$$p(\varphi \to \psi) = |a(\varphi \to \psi)|^2 = \langle\psi|\varphi\rangle^2 = \langle\varphi|A|\varphi\rangle$$

lorsque $A = |\psi\rangle\langle\psi| = P_\psi$. Après le test, le système est dans l'état $|\psi\rangle$:

$$P_\psi|\varphi\rangle \mapsto \frac{P_\psi|\varphi\rangle}{\sqrt{\langle\varphi|P_\psi|\varphi\rangle}}$$

Un principe de la mécanique quantique est qu'on prend la somme des amplitudes de probabilités pour des chemins indiscernables.

Theorem 1.1. *M hermitien. Alors M s'écrit comme une combinaison de projecteurs:*

$$M = \sum_j a_j P_j, \quad P_j P_k = \delta_{jk} P_j, \quad \sum_j P_j = I$$

où les coefficients a_j sont les valeurs propres de M.

Il y a une autre façon de décrire un état comme un *opérateur densité*. On considère un système composé de deux sous-systèmes K et L munis des bases o.n. $|i\rangle$ et $|\mu\rangle$. Un état s'écrit comme $|\varphi\rangle = \sum_{i,\mu} \alpha_{i\mu}|i \otimes \mu\rangle$. On suppose M un observable du sous-système K: $|(M \otimes I_L)\varphi\rangle = \sum_{i,\mu} \alpha_{i\mu}|Mi \otimes \mu\rangle$ avec éspérance

$$\begin{aligned}
\langle\varphi|M \otimes I_L|\varphi\rangle &= \sum_{j,\nu}\sum_{i,\mu} \overline{\alpha_{j\nu}}\alpha_{i\mu}\langle j \otimes \nu|Mi \otimes \mu\rangle \\
&= \sum_{i,j}\sum_{\mu} \overline{\alpha_{j\mu}}\alpha_{i\mu}\langle j|Mi\rangle = \sum_{i,j}\rho_{ij}\langle j|Mi\rangle \\
&= \sum_{i,j}\rho_{ij}M_{ji} = \operatorname{tr}(\rho M)
\end{aligned}$$

où $\rho_{ij} = \sum_\mu \alpha_{i\mu}\overline{\alpha_{j\mu}}$. L'opérateur ρ est *l'opérateur densité* associé au sous-système K. L'opérateur ρ donne un moyen convenable pour décrire un systéme pour lequel l'état n'est pas complètement connu. L'opérateur ρ est hermitien, non-nég ($\rho \geq 0$) et $\operatorname{tr}\rho = 1$ ($\operatorname{tr}\rho = ||\varphi||^2$).

Puisque ρ est hermitien, on peut le diagonaliser par rapport à une base o.n. :

$$\rho = \sum_i p_i|i\rangle\langle i| \qquad p_i \geq 0\,,$$

de plus $\operatorname{tr}\rho = 1 \Rightarrow \sum_i p_i = 1$: ρ represente un *mélange statistique* d'états $|i\rangle$, chacun ayant probabilité p_i ; il n'est pas considéré comme une superposition d'états. Un état du type $\rho = |\psi\rangle\langle\psi|$ est appelé *pur*. En général ρ n'est pas pur.

L'entropie de Von Neumann : $S = -k\operatorname{tr}(\rho\log_2\rho) = -k\sum_i \lambda_i \log_2\lambda_i$ où λ_i sont les valeurs propres de ρ et k est la constante de Boltzman. Si l'état est pur ($\rho = |\psi\rangle\langle\psi|$) l'entropie est nul (il n'y a aucune incertitude sur l'état du système) car l'opérateur densité n'a qu'une seule valeur propre 1 associé au vecteur propre $|\psi\rangle$.

Theorem 1.2. (Gleason) *On suppose donné une mesure p définie sur l'ensemble de projecteurs agissant sur un espace séparable de Hilbert de dimension fini H vérifiant $0 \le p(P) \le 1$, $p(I) = 1$, $p(P_i + P_j) = p(P_i) + p(P_j)$ lorsque $P_iP_j = \delta_{ij}P_i$ (les projecteurs sont orthogonaux). Alors si $\dim H \ge 3$, il existe un opérateur non-négatif hermitien unique ρ de trace 1 tel que*

$$p(P) = \operatorname{tr}(\rho P)\,.$$

pour chaque projecteur P.

Conclusion : On peut representer un mélange statistique d'états par un opérateur densité ρ (non-négatif hermitien de trace 1). L'espérance d'un observable A pour le mélange ρ est $\operatorname{tr}(\rho A)$ (si $\rho = |\psi\rangle\langle\psi|$ est pur alors $\operatorname{tr}(\rho A) = \langle\psi|A|\psi\rangle$).

4. Changement d'état : Un changement d'état $|\varphi(0)\rangle \to |\varphi(t)\rangle$ s'effectue par une transformation linéaire qui préserve la norme, c'est à dire par une transformation unitaire $U(t,0)$: $|\varphi(t)\rangle = U(t,0)|\varphi(0)\rangle$. On impose la propriété de semigroupe : $U(t_2,t_1) = U(t_2,t')U(t',t_1)$ et $U(t,t) = I$. Le dévelopement limité montre que

$$U(t+\mathrm{d}t,t_0) = U(t+\mathrm{d}t,t)U(t,t_0) \sim \left(I - \frac{\mathrm{i}}{\hbar}\widehat{H}(t)\mathrm{d}t\right)U(t,t_0)$$

où

$$\widehat{H}(t) = \mathrm{i}\hbar\frac{\mathrm{d}U(t',t)}{\mathrm{d}t'}|_{t'=t}\,.$$

De plus,

$$\begin{aligned} I = U(t+\mathrm{d}t,t)^*U(t+\mathrm{d}t,t) &\sim \left(I + \frac{\mathrm{i}}{\hbar}\widehat{H}(t)^*\mathrm{d}t\right)\left(I - \frac{\mathrm{i}}{\hbar}\widehat{H}(t)\mathrm{d}t\right) \\ &\sim I + \frac{\mathrm{i}}{\hbar}(\widehat{H}^* - \widehat{H})\,, \end{aligned}$$

ce qui montre que $\widehat{H}$ est hermitien. On en déduit l'équation de Schrödinger :

$$\mathrm{i}\hbar\frac{\mathrm{d}U(t,t_0)}{\mathrm{d}t} = \widehat{H}(t)U(t,t_0)$$

ou, en écrivant $|\varphi(t)\rangle = U(t,0)|\varphi(0)\rangle$

$$\mathrm{i}\hbar\frac{\mathrm{d}|\varphi\rangle}{\mathrm{d}t} = \widehat{H}|\varphi\rangle\ .$$

L'opérateur $\widehat{H}$ étant hermitien represent un observable : l'énergie. Si $\widehat{H}$ est independant de t, on peut intégrer l'équation de Schrödinger explicitement pour donner $U(t,t_0) = \exp(-\mathrm{i}(t-t_0)\widehat{H}/\hbar)$.

2. **Qubit**

Un *qubit* (bit quantique) est l'état quantique qui représente une unité de stockage d'information quantique.

Rappel: Donné un espace de probabilités : $(S, \mathcal{T}, p)$, le contenu d'information d'un evenement $E \in \mathcal{T}$ est

$$I(E) := -\log_2(p(E))\,.$$

Si $X : S \to R$ est une variable aléatoire à valeurs dans un espace R, alors

$$p(X = a) := p(X^{-1}\{a\})\,,$$

d'où, si X est une variable aléatoire symétrique de Bernouilli (distribution uniforme) prenant les valeurs 0 et 1, alors

$$I(X = 0) = I(X = 1) = -\log_2(1/2) = 1\,.$$

On obtient un bit d'information quand on choisit entre deux alternatives equiprobables.

Exemple : Alice envoye à Bob un message

$$110101110\cdots$$

En pratique, on le transmet le long d'un fibre optique: un photon polarisé le long de $0x$ corréspond à 0 ; un photon polarisé le long de $0y$ correspond à 1. Alors un photon polarisé à 45^o aux axes est un exemple d'un qubit.

En général, un qubit est un état quantique $|\varphi\rangle$ d'un système pour lequel son espace de Hilbert corréspondant est isomorphe à $\mathbf{C}^2$:

$$|\varphi\rangle = \lambda\,|0\rangle + \mu\,|1\rangle\,, \qquad |\lambda|^2 + |\mu|^2 = 1\,.$$

Les coefficients λ et μ sont complexes mais dans l'exemple ci-dessus, un photon polarisé à un angle θ à l'axe des x est représenté par

$$|\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\ .$$

L'amplitude de probabilité qu'un photon orienté à un angle θ passe par un analyseur orienté à un angle α est

$$a(\theta \to \alpha) = \cos(\theta - \alpha) = \langle\alpha|\theta\rangle\ .$$

La probabilité de passer par l'analyseur est $\cos^2(\theta - \alpha)$.

D'autres réalisations d'un qubit: une particule de spin 1/2 ; une atome à deux niveaux.

Spin 1/2 : Un proton a un moment angulaire de spin qui prend deux et seulement deux valeurs le long d'un champ magnétique (cette propriété caracterise les particules de spin 1/2). Il y a alors deux états possibles $|0\rangle$ et $|1\rangle$ qui détermine une base d'un espace vectoriel complexe $V \simeq \mathbf{C}^2$.

Parametrisation : $\{(\lambda,\mu)\in\mathbf{C}^2,\ |\lambda|^2+|\mu|^2=1\}\leftrightarrow S^3$: On identifie (λ,μ) et $(e^{\mathrm{i}\theta}\lambda,e^{\mathrm{i}\theta}\mu)$ ce qui correspond aux fibres de la fibration de Hopf $S^3\to S^2$, d'où (λ,μ) sont paramétrés par les points de S^2. Expression générale :

$$|\varphi\rangle=e^{-\mathrm{i}\alpha/2}\cos\frac{\theta}{2}\,|0\rangle+e^{\mathrm{i}\alpha/2}\sin\frac{\theta}{2}\,|1\rangle \tag{2.1}$$

où $\alpha\in[0,2\pi]$ et $\theta\in[0,\pi]$. Cet état est séléctionné avec certitude par un champ magnétique parallèle à $\widehat{n}$ où

$$\widehat{n}=(n_1,n_2,n_3)=(\sin\theta\cos\alpha,\sin\theta\sin\alpha,\cos\theta)\,.$$

Une base pour les opérateurs hermitiens définis sur $\mathbf{C}^2$ est donnée par

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \sigma_1=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \sigma_2=\begin{pmatrix}0&-\mathrm{i}\\\mathrm{i}&0\end{pmatrix},\quad \sigma_3=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

où $\sigma_1,\sigma_2,\sigma_3$ sont les matrices de Pauli. Ces matrices sont toutes hermitiennes et unitaires. Par exemple les vecteurs propres de σ_3 sont $|0\rangle$ et $|1\rangle$ avec valeurs propres ±1. La matrice $n_1\sigma_1+n_2\sigma_2+n_3\sigma_3$ a $|\varphi\rangle$ dans (2.1) comme vecteur propre avec valeur propre $+1$. Il s'ensuit qu'on peut considérer σ_3 comme la mesure de spin le long de l'axe des z.

En général, donné une particule dans l'état $|\varphi\rangle=\lambda\,|0\rangle+\mu\,|1\rangle$, la probabilité de la trouver dans l'etat $|0\rangle$ est $|\,\langle0|\varphi\rangle\,|^2=|\lambda|^2$, et dans l'état $|1\rangle$ elle est $|\mu|^2$. On peut tester cette affirmation en préparant la particule dans l'état $|\varphi\rangle$ (par exemple avec un appareil de Stern-Geralach) et puis on fait le $|0\rangle$–test, disons. C'est à dire on pose $\theta=0$ dans (2.1), ce qui correspond à un alignement du champs magnétique le long de l'axe des z. On voit combien de particules donne le resultat $+1$ quand on mesure leur spin le long de cet axe.

Etat à deux qubits : Du point de vue classique il y a quatre états possibles : $\begin{pmatrix}u_0\\u_1\end{pmatrix}\otimes\begin{pmatrix}v_0\\v_1\end{pmatrix}$ où $u_0,u_1,v_0,v_1\in\{0,1\}$. On les écrit :

$$|00\rangle=\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\quad |01\rangle=\begin{pmatrix}0\\1\\0\\0\end{pmatrix},\quad |10\rangle=\begin{pmatrix}0\\0\\1\\0\end{pmatrix},\quad |11\rangle=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Ils déterminent une base d'un espace vectoriel d'états de dimension 4 : $V\simeq\mathbf{C}^4$. Un élément de V représente un état à deux qubits :

$$|\varphi\rangle=\lambda_{00}\,|00\rangle+\lambda_{01}\,|01\rangle+\lambda_{10}\,|10\rangle+\lambda_{11}\,|11\rangle\quad(|\lambda_{00}|^2+|\lambda_{01}|^2+|\lambda_{10}|^2+|\lambda_{11}|^2=1)\,.$$

Si on mesure la premier qubit x_1 disons, alors $p(x_1 = 1) = |\lambda_{10}|^2 + |\lambda_{11}|^2 = \langle\varphi|P|\varphi\rangle$ où

$$P = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = |10\rangle\langle 10| + |11\rangle\langle 11| \ .$$

Après l'expérience, l'état s'effondre dans l'état :

$$|\varphi'\rangle = \frac{P|\varphi\rangle}{\sqrt{\langle\varphi|P|\varphi\rangle}} \, .$$

Etat intriqué à deux qubits : Il s'agit d'un état du type ci-dessus qui n'est pas le produit tensoriel de deux états à un qubit : $|\varphi\rangle \neq |\alpha\rangle \otimes |\beta\rangle$. Par exemple

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

est un état intriqué.

On peut bien évidemment généraliser aux états à n qubits.

3. Circuits quantiques et portes quantiques

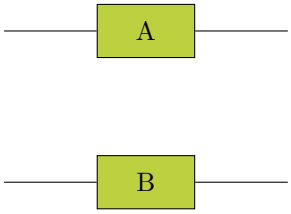
Un circuit classique est construit des chemins et des portes logiques. Pour un seul bit classique, la seule porte logique non-triviale est la porte NOT : $\begin{cases} 0 & \to & 1 \\ 1 & \to & 0 \end{cases}$

Une porte quantique pour un seul qubit prend la forme :

où U est un (2×2)–opérateur unitaire agissant sur $\mathbf{C}^2$: $|\varphi\rangle \to U|\varphi\rangle$. C'est la seule contrainte sur une porte quantique. Par exemple, la porte quantique NOT est donnée par $U = X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$: $|\varphi\rangle = \lambda|0\rangle + \mu|1\rangle \mapsto \mu|0\rangle + \lambda|1\rangle$. On définit la porte $Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et la porte Hadamard $H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Composée de deux portes :

Porte à deux qubits : deux opérations en parallèle :



correspond à $A \otimes B$. Explicitement :

$$A \otimes B = \left(\begin{array}{c|c} A_{11}B & A_{12}B \\ \hline A_{21}B & A_{22}B \end{array}\right) = \left(\begin{array}{cc|cc} A_{11}B_{11} & A_{11}B_{12} & \cdots & \cdots \\ A_{11}B_{21} & A_{11}B_{22} & \cdots & \cdots \\ \hline \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{array}\right)$$

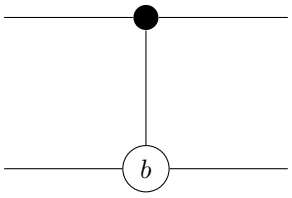
Exemple "Controlled–NOT gate" : Donné deux qubits $|a\rangle$ et $|b\rangle$ comme entrées, la porte interchange la valeur de vérité de $|b\rangle$ si $|a\rangle$ est vrai (0 = faux, 1 = vrai) :

$$|a, b\rangle \mapsto |a, b \oplus a\rangle$$

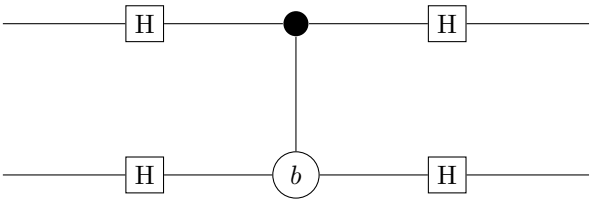
où $b \oplus a$ est addition modulo 2. Dans ce cas

$$U = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right) = \left(\begin{array}{c|c} I & 0 \\ \hline 0 & X \end{array}\right)$$

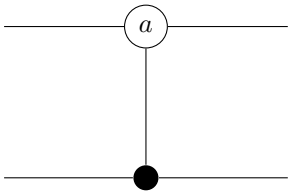
par rapport à la base $|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ etc.. Représentation :



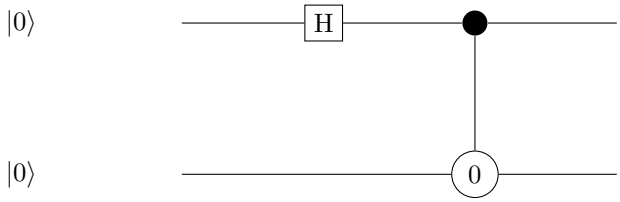
Exercice :



est équivalent à



Exemple important :



La sortie de cette porte est l'état intriqué $|\varphi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Si on mesure la valeur de vérité d'un qubit on apprend la valeur de vérité de l'autre – non-localité.

4. **"No-cloning", téléportation quantique**

No-cloning : On veut effectuer une transformation du type $|\psi\rangle \otimes |s\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle$ où $|\psi\rangle$ est la donnée et $|s\rangle$ est la cible. C'est à dire on veut créer un clone de l'état $|\psi\rangle$. On suppose U fixé. Ce n'est pas possible car la partie droite est quadratique en $|\psi\rangle$ et une tranformation linéaire ne peut pas transformer linéaire en quadratique.

Preuve : Donnée deux états : $|\psi\rangle$ et $|\varphi\rangle$, il nous faut

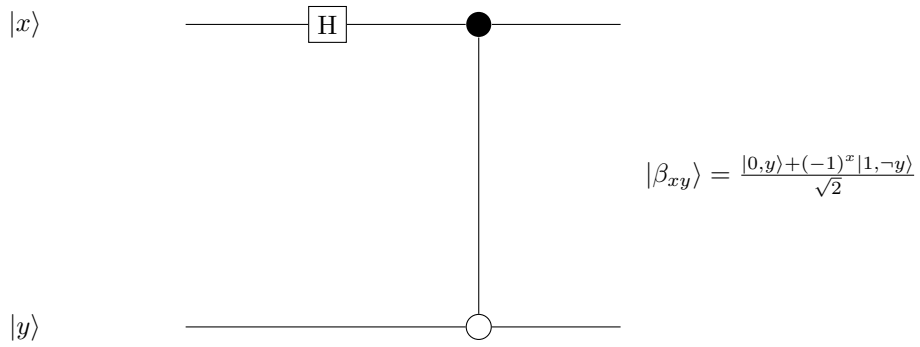
$$\begin{aligned} U(|\psi\rangle \otimes |s\rangle) &= |\psi\rangle \otimes |\psi\rangle \\ U(|\varphi\rangle \otimes |s\rangle) &= |\varphi\rangle \otimes |\varphi\rangle \end{aligned}$$

On prend le produit scalaire des parties gauche et droite de ces équations (U unitaire) :

$$\langle\psi|\varphi\rangle = \langle\psi|\varphi\rangle^2$$

Mais il n'existe que deux solutions à cette équation : $x = \langle\psi|\varphi\rangle = 0$ ou 1, d'où soit $|\psi\rangle = |\varphi\rangle$ soit $|\psi\rangle$ et $|\varphi\rangle$ sont orthogonaux. □

Téléportation quantique :



$$\begin{aligned} |00\rangle &\rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\beta_{00}\rangle \\ |01\rangle &\rightarrow \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\beta_{01}\rangle \\ |10\rangle &\rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\beta_{10}\rangle \\ |11\rangle &\rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\beta_{11}\rangle \end{aligned}$$

On les appelle des *états de Bell* ou des *paires EPR*.

Alice et Bob engendrent la paire EPR $|\beta_{00}\rangle$. Chacun prend un qubit de la paire, appelons les $|a\rangle$ et $|b\rangle$ resp., et se séparent à une grande distance. La mission pour Alice est de livrer un qubit $|\psi\rangle$ à Bob sans savoir son état. Elle ne peut qu'envoyer de l'information classique à Bob. A noter qu'elle ne peut pas déterminer l'état $|\psi\rangle$ car si elle essaye, l'état va s'effondrer sur un vecteur propre. En plus, puisqu' il est impossible d'engendrer un clone, elle ne peut mesurer le qubit qu'une seule fois. On suppose $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.

Elle peut transmettre l'information comme suite : elle forme $|a\rangle \otimes |\psi\rangle$; elle passe cet état par des portes quantiques ; elle mesure le résultat : il y en a quatre possibilités : 00, 01, 10, 11 ; elle transmet l'information à Bob. Bob peut alors récuperer l'état $|\psi\rangle$!

Les donnée sont

$$|\Psi_0\rangle := |\psi\rangle \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}} \{\alpha |0\rangle \otimes (|00\rangle + |11\rangle) + \beta |1\rangle \otimes (|00\rangle + |11\rangle)\}$$

Dans cette expression, les deux premiers qubits dans chaque terme appartiennent à Alice et le dernier qubit à Bob. Alice transmet ses deux qubits par une porte CNOT :

$$|\Psi_1\rangle := \frac{1}{\sqrt{2}} \{\alpha |0\rangle \otimes (|00\rangle + |11\rangle) + \beta |1\rangle \otimes (|10\rangle + |01\rangle)\}$$

Alice transmet son premier qubit par une porte Hadamard :

$$\begin{aligned} |\Psi_2\rangle &:= \frac{1}{2} \{\alpha(|0\rangle + |1\rangle) \otimes (|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle) \otimes (|10\rangle + |01\rangle)\} \\ &= \frac{1}{2} \left\{ |00\rangle \underbrace{(\alpha |0\rangle + \beta |1\rangle)}_{\text{Bob}} + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle) \right\} \end{aligned}$$

Alice prend une mesure et elle l'envoye à Bob:

Alice	Bob
$\|00\rangle$	$\alpha \|0\rangle + \beta \|1\rangle$
$\|01\rangle$	$\alpha \|1\rangle + \beta \|1\rangle$
$\|10\rangle$	$\alpha \|0\rangle - \beta \|1\rangle$
$\|11\rangle$	$\alpha \|1\rangle - \beta \|0\rangle$

Dès que Bob apprend la mesure d'Alice, il peut recuperer l'état $|\psi\rangle$ en transmettrant son état par la bonne porte quantique :

Alice transmet	Bob applique la porte
$\|00\rangle$	aucune
$\|01\rangle$	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\|10\rangle$	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
$\|11\rangle$	ZX

Alice a alors transmis l'état $|\psi\rangle$ à Bob sans le connaître elle-même.

Tentative de communiquer à une vitesse plus grande que la lumière : On suppose Alice et Bob partage la paire intriquée $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. On considère la base $\{|0\rangle, |1\rangle\}$ de vecteurs propres pour Z et la base $\{|+\rangle, |-\rangle\}$ de vecteurs propres pour X : $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Si Bob mesure son qubit dans la Z–base et il observe $|0\rangle$ ou $|1\rangle$ alors le qubit d'Alice sera dans le

même état. Puisqu'on a aussi $|\psi\rangle = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$, si Bob mesure son qubit dans la X–base et il observe $|+\rangle$ ou $|-\rangle$, le qubit d'Alice sera encore dans le même état.

Bob ne peut pas controller le resultat de son mesure mais il peut controller la base par rapport à laquelle il prend sa mesure. Il peut alors tenter de communiquer un bit d'information comme suite. S'il veut communiquer 0 il mesure son qubit dans la Z–base, s'il veut communiquer 1 il le mesure dans la X–base. Dans le premier cas, l'état du qubit d'Alice est $|v\rangle =$ soit $|0\rangle$ soit $|1\rangle$ chacun avec probabilité $1/2$. Dans le deuxième cas, l'état est $|v\rangle =$ soit $|+\rangle$ soit $|-\rangle$ encore avec probabilité $1/2$. Y a-t-il un moyen pour Alice de distinguer entre ces deux scenarios ?

On voit l'intervention d'un *melange statistique*. Dans le premier cas, l'état du qubit d'Alice n'est pas une superposition des deux états $|0\rangle$ et $|1\rangle$, mais plutôt un melange statistique $\rho = \sum_j p(j)\,|j\rangle\,\langle j|$ de ces deux états, chacun ayant la probabilité $1/2$ (au lieu d'une amplitude complexe). On se rappelle que pour une mesure associée à un projecteur P, sa probabilité est donnée par

$$p = \mathrm{tr}\,(\rho P)\,.$$

Mais

$$\rho = \frac{1}{2}(|0\rangle\,\langle 0| + |1\rangle\,\langle 1|) = \frac{1}{2}(|+\rangle\,\langle +| + |-\rangle\,\langle -|) = \frac{1}{2}I_2\,.$$

Puisque la matrice identité est la même quelque soit la base, l'opérateur densité ρ est une distribution des probabilités uniforme quelque soit la base par rapport à laquelle on prend la mesure. Le choix de Bob n'a aucun effet sur la mesure d'Alice. Du point de vu empirique, un effet n'est pas réel si on ne peut pas le mesurer, donc il n'y a aucun sens pour lequel la mesure de Bob peut influencer le qubit d'Alice. Pourtant..... l'inégalité de Bell !

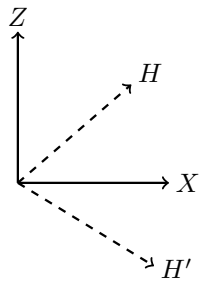
5. **L'inégalité de Bell-CHSH (Clauser, Horne, Shimony et Holt)**

Rappel : à un observable il correspond un opérateur hermitien : $M^* = M$. On prend une base de vecteurs propres : si on mesure $|v\rangle$ dans cette base (c'est à dire, si on applique M), on observe l'une des valeurs propres λ de M avec probabilité $p(\lambda) = \langle v|P_\lambda|v\rangle$, où P_λ est le projecteur de l'éspace des états sur l'espace propre associé à λ. Puisque $M = \sum_\lambda \lambda P_\lambda$, l'espérance est donnée par $\mathbb{E}[\lambda] = \sum_\lambda \lambda P(\lambda) = \langle v|M|v\rangle$.

Par exemple, l'opérateur Z mesure le spin autour de l'axe des z. Ses valeurs propres sont ± 1 : *spin up* ou *spin down*. L'opérateur X mesure le spin autour de l'axe des x. Deux opérateurs ont les mêmes vecteurs propres si et seulement si ils commutent. Par exemple, $XZ = -ZX$: X et Z n'ont aucun vecteur propre en commun. On ne peut pas mesurer simultanément deux observables qui ne commutent pas (principle d'incertitude de Heisenberg). La Z–base est donnée par $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ et la X–base par $\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}$.

Alice et Bob créent un état intriqué, par exemple $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice prend l'un des qubits et Bob l'autre. Les deux se separent. Si Bob mesure son qubit il connait l'état de celui d'Alice !

Soit H la matrice de Hadamard : $H = \dfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ et soit $H' = XHX = \dfrac{1}{\sqrt{2}}\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$.



Si Alice mesure son qubit par rapport à une base et Bob mesure le sien par rapport à une autre base, les deux opértateurs corréspondants commutent. Par exemple, si Alice fait sa mesure dans la Z–base ou le X–base, elle applique $Z_A = Z \otimes I_2$ ou $X_A = X \otimes I_2$. Si Bob fait sa mesure dans la H–base ou le H'–base, il applique $H_B = I_2 \otimes H$ ou $H'_B = I_2 \otimes H'$. On ne peut pas mesurer Z_A et X_A simultanément, mais on peut mesurer Z_A et H_B simultanément : $Z_A H_B = H_B Z_A = Z \otimes H$.

Si X, Y sont deux variables aléatoires indépendantes, alors $\mathbb{E}[XY] = \mathbb{E}[X]\mathbb{E}[Y]$. On va considérer $\mathbb{E}[XY]$ comme une façon de mesurer la *corrélation* entre X et Y (pas tout à fait la même chose que la correlation dans le sens de la théorie des probabilités : $\rho(X,Y) = \mathrm{cov}\,(X,Y)/\sigma_X\sigma_Y$ où σ_X est la déviation). On l'appelle la *corrélation quantique*.

Lemma 5.1. *Soit $A_1 = A \otimes I_2$ et $B_2 = I_2 \otimes B$ (A et B hermitiennes). Alors $\mathbb{E}[A_1 B_2] = \frac{1}{2}\mathrm{tr}\,(AB^t)$.*

Preuve : $\mathbb{E}[A_1 B_2] = \langle\psi|A_1 B_2|\psi\rangle$ (on se rappelle qu'on mesure l'espérance par rapport à l'état $\psi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$). On la calcule explicitement pour obtenir $\frac{1}{2}(A_{00}B_{00} + A_{01}B_{01} + A_{10}B_{10} + A_{11}B_{11})$ qui est exactement $\frac{1}{2}\mathrm{tr}\,(AB^t)$. □

Soit S^θ l'opérateur hermitien

$$S^\theta = (\cos\theta)Z + (\sin\theta)X = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix},$$

qui correspond à la mesure de spin autour d'un axe dans le xz–plan à un angle θ à l'axe des z. Ses vecteurs propres sont $|v_+\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$ et $|v_-\rangle = \sin\frac{\theta}{2}|0\rangle - \cos\frac{\theta}{2}|1\rangle$. Alice et Bob partage l'état intriqué $|\psi\rangle$. On suppose que ils mesurent leurs qubits dans des bases qui diffèrent par un angle θ, par exemple, on suppose que Alice applique la Z_A–Base et Bob la S^θ–Base. La correlation entre les mesures est $\mathbb{E}[Z_A S^\theta_B] = \frac{1}{2}(Z(S^\theta)^t) = \cos\theta$. On remarque que $\mathbb{E}[Z_A] = \mathbb{E}[Z \otimes I_2] = \frac{1}{2}(\langle 00|Z \otimes I|00\rangle + \cdots) = \frac{1}{2}(\langle 0|Z|0\rangle\langle 0|I|0\rangle + \cdots) = \frac{1}{2}(1 + 0 + 0 - 1) = 0$, donc

$\mathbb{E}[Z_A S_B^\theta] \neq \mathbb{E}[Z_A]\mathbb{E}[S_B^\theta]$ en général et les mesures sont corrélées. Alors

$$\mathbb{E}[Z_A H_B] = \mathbb{E}[X_A H_B] = \mathbb{E}[X_a H'_B] = -\mathbb{E}[Z_A H'_B] = \cos\frac{\pi}{4} = \frac{1}{\sqrt{2}}\,.$$

Soit W l'opérateur hermitien :

$$W = Z_A H_B + X_A H_B + X_A H'_B - Z_A H'_B\,.$$

En général $\mathbb{E}[X+Y] = \mathbb{E}[X] + \mathbb{E}[Y]$, d'où

$$\mathbb{E}[W] = 2\sqrt{2} \tag{5.1}$$

On va écrire W autrement :

$$W = Z_A(H_B - H'_B) + X_A(H_B + H'_B) \tag{5.2}$$

Alors chacun des quatre opérateurs $Z_A H_B$, $X_A H_B$, $Z_A H'_B$ et $X_A H'_B$ ne peut que donner ± 1 comme valeur propre. Si les mesures de $Z_A H_B$ et $Z_A H'_B$ coincident, c'est à dire Bob a obtenu la même valeur pour les expériences H_B et H'_B, alors $W = 2X_A H_B$ et les resultats en appliquant W appartiennent à $\{\pm 2\}$. De même si Bob a obtenu deux valeurs différentes pour ces expériences. Dans tous les case $|\mathbb{E}[W]| \leq 2$ – il s'agit de l'inégalité de Bell–CHSH. En effet l'une des deux expressions $H_B - H'_B$ et $H_B + H'_B$ s'annulle et l'autre vaut ± 2. Bien evidemment, Bob ne peut pas prendre les mesures H_B et H'_B simultanément puisque les opérateurs ne commutent pas. Dans la pratique, on obtient les resultats statistiques de plusieurs expériences (voir ci-dessous). Cette inégalité est valable quelque soit l'ensemble de quatre variables aléatoires Z_A, X_A, H_B, H'_B à valeurs dans $\{\pm 1\}$ choisit par rapport à n'importe quelle distribution de probabilité avec des corrélations quelconques entre eux. Pourtant l'inégalité contredit (5.1). Pourquoi ?

Dans la factorisation (5.2) on a supposé que le Z_A dans l'expression $Z_A H_B$ est le même que le Z_A dans $Z_A H'_B$, c'est à dire que la mesure de la grandeur physique associée à Z_A n'est pas influencée par le choix de base de Bob à une distance de plusieurs années–lumiére.

Réalisme local : On suppose que Alice et Bob partage l'état intriqué $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice, en considérant son qubit, peut savoir avec certitude si elle va trouver $+1$ ou -1 si elle déciderait de prendre une mesure autour d'un axe $\vec{u}$: elle demande à Bob de prendre une mesure autour du même axe et de lui téléphoner le resultat. Elle sait avec certitude qu'elle aurait trouver le même resultat si elle avait fait l'expérience elle-même. Il est alors raisonable de supposer que son qubit a une valeur bien définie (mais aléatoire) *avant* d'avoir pris la mesure puisque que Alice n'a eu aucune intéraction avec la particule mais pourtant elle a un moyen de connaitre la valeur de son observable. Ce point de vue, qui attribue une réalité à une grandeur physique sans l'avoir mesuré, est connu sous le nom : *réalisme local*.

Localité : Il s'agit de la supposition que Alice, en prennant une mesure n'a aucune influence sur le resultat de la mesure de Bob.

L'inégalité de Bell est violée dans des expériences d'où on est ramené à abandonner l'une ou l'autre de ces suppositions.

Remarques complémentaires : Bob ne peut pas mesurer H_B et H'_B simultanément. Dans la pratique de l'expérience, Alice et Bob partagent un grand nombre d'états intriqués identiques. Pour chaque expérience, Alice et Bob prennent une mesure : Alice par rapport à soit Z_A soit X_A ; Bob par rapport à soit H_B soit H'_B. Après chaque expérience, Alice et Bob peuvent changer les polarizations de leur appareil. En répétant l'expérience plusieurs fois on peut accumuler des moyens statistiques des quatres configurations. D'après la principe d'incertitude de Heisenberg, on ne peut pas avoir des resultats simultanés de $Z_A H_B$ et $Z_A H'_B$, mais d'après le réalisme local ces mesures sont bien définies pour chaque réalisation de l'expérience même si on ne peut que réaliser l'une de ces deux, ce qui devrait donner $|E[W]| \leq 2$. Les expériences de A. Aspect et d'autres (http://arxiv.org/ftp/quant-ph/papers/0402/0402001.pdf) montrent que cette inégalité est violée [voir aussi : S. Haroche et J-M. Raimond, Exploring the Quantum. Oxford Univ. Press 2006].

6. **Algorithmes**

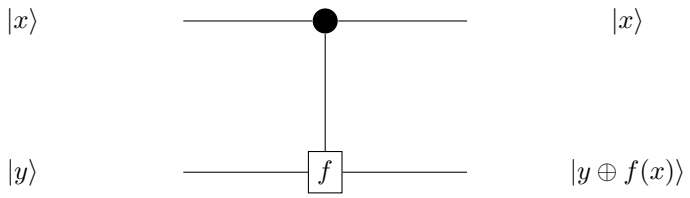
Certains problèmes sont bien adaptés aux algorithmes quantique, notamment les problèmes de la recherche des symétries. Un algorithme va s'exprîmer comme un circuit quantique. Il y a une entrée et une sortie et entre les deux, une transformation unitaire que dépend du problème.

6.1. **Algorithme de Deutsch (1985)**

On suppose donnée une fonction f d'un seul bit qui retourne un seul bit comme sortie ($f : \{0,1\} \to \{0,1\}$). On pose la question: Est-ce-que les deux valeurs de f sont les mêmes ou différentes? Du point de vue classique, on doit retourner $f(0)$ et $f(1)$ separamment. Dans la mécanique quantique une seule interrogation suffit.

Il s'agit de quoi une interrogation en mécanique quantique? Donné un qubit y, on ne peut pas simplement poser $y = f(x)$, car l'état s'effondrait et on perdrait l'information contenue en y.

Première tentative : On interroge f en interchangeant les valeurs de vérité de y si $f(x)$ est vraie ($0 =$ fausse, $1 =$ vraie): précisément, on définit l'opérateur unitaire $U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle$ où $\oplus$ est l'addition modulo 2.



Par exemple, si $f(x) = x$, alors U_f est une porte CNOT (*controlled NOT gate*). Si $f(0) = 1$ et $f(1) = 0$, alors U_f interchange la valeur y si et seulement si $|x\rangle$ est fausse.

Si on prépare $|x\rangle$ comme une superposition uniforme : $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et on prépare $|y\rangle$ dans létat $|0\rangle$, on a :

$$U_f(|+\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle) \tag{6.1}$$

Avec une seule interrogation, on a obtenu une sortie qui contient des informations conçernant $f(0)$ et $f(1)$. Malheureusement, l'état donné par la sortie n'est pas très utile: si on mesure x, on voit soit $|0\rangle \otimes |f(0)\rangle$ soit $|1\rangle \otimes |f(1)\rangle$ chacun avec probabilité 1/2 - donc on apprend soit $f(0)$ soit $f(1)$ mais on ne peut pas controller lequel. En effet il s'agit plutôt d'un calcul classique aléatoire. On peut faire mieux en notant que U_f s'écrit comme :

$$U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes X^{f(x)} |y\rangle \ ,$$

où $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. On prépare $|y\rangle$ dans l'état $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (il s'agit d'un vecteur propre de X avec valeur propre -1). Alors

$$U_f(|x\rangle \otimes |-\rangle) = (-1)^{f(x)} |x\rangle \otimes |-\rangle \ .$$

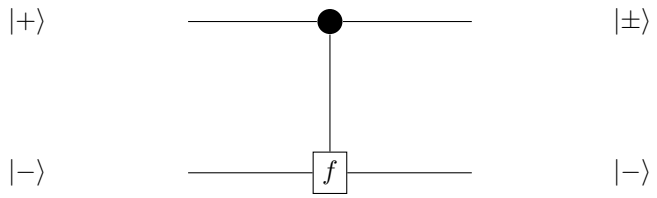
Ensuite, on prépare $|x\rangle$ dans l'état $|+\rangle$:

$$U_f(|+\rangle \otimes |-\rangle) = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}\,|0\rangle \otimes |-\rangle + (-1)^{f(1)}\,|1\rangle \otimes |-\rangle\right) .$$

On peut ignorer le facteur de phase $(-1)^{f(0)}$, d'où $U_f(|+\rangle \otimes |-\rangle) = |\psi\rangle \otimes |-\rangle$, avec

$$|\psi\rangle = \frac{1}{\sqrt{2}}((-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{f(0)\oplus f(1)}\,|1\rangle)\,. \tag{6.2}$$

Il s'ensuit que si $f(0) = f(1)$ alors $|\psi\rangle = |+\rangle$ et que si $f(0) \neq f(1)$ alors $|\psi\rangle = |-\rangle$. Donc, si on mesure $|\psi\rangle$ dans la X–base, on apprend la parité $f(0) \oplus f(1)$ en une seule interrogation U_f (*l'opérateur d'interrogation*) :



(On peut revenir à la base du départ avec des portes de Hadamard.

Remarques complémentaires : 1. Souvent, dans un algortihme quantique on considère une fonction f comme une "boite noire" et on essaye de découvrir une propriété de f en l'interrogeant. On va considérer la complexité d'un tel problème comme le nombre de questions qu'on doit poser, autrement dit, comme le nombre de fois U_f apparaît dans le circuit.

2. L'algorithme de Deutsch est un exemple de ce qu'on appelle *phase kickback* (en anglais !) On prépare la "sortie" comme un vecteur propre et sa valeur propre influence la phase de l'entrée. Au lieu de mesurer la sortie, on la jette et on apprend des informations conçernant la fonction en mesurant l'entrée.

6.2. **Généralisation à n bits et la transformée de Fourier quantique**

On suppose que f applique une liste de n bits en 1 bit. Par exemple, si $n = 3$, l'entrée $|\underline{x}\rangle$ fait partie de la liste:

$$|\underline{x}\rangle = |000\rangle\,,\ |001\rangle\,,\ |010\rangle\,,\ |011\rangle\,,\ |100\rangle\,,\ |101\rangle\,,\ |110\rangle\,,\ |111\rangle\ ,$$

où $|000\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle$ etc. On prend n arbitraire et on définit

$$U_f\,|\underline{x}, y\rangle = |\underline{x}, y \oplus f(\underline{x})\rangle\ .$$

On prépare $\underline{x}$ dans l'état

$$\underline{x} = |+\rangle \otimes \cdots \otimes |+\rangle = \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} |\underline{x}\rangle\ .$$

On prépare y dans l'état $|-\rangle$. Alors

$$U_f \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} |\underline{x}, -\rangle = \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} U_f\,|\underline{x}, -\rangle = \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} (-1)^{f(\underline{x})}\,|\underline{x}, -\rangle = |\psi\rangle \otimes |-\rangle\ , \tag{6.3}$$

où

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} (-1)^{f(\underline{x})} |\underline{x}\rangle \ .$$

On remarque que cette expression contient les valeurs $f(\underline{x})$ dans les phases des amplitudes de $\underline{x}$ dans la partie droite.

Plus généralement, on pose

$$|\psi\rangle = \sum_{\underline{x}} a_{\underline{x}} |\underline{x}\rangle \ ,$$

où les 2^n amplitudes $a_{\underline{x}} \in \mathbf{C}$. On va définir la transformée de Fourier: il s'agit d'un changement de base où on écrit $|\psi\rangle$ comme une combinaison linéaire dans un autre base.

La série de Fourier d'une fonction $f(t)$ est donnée par

$$f(t) = \sum_{\alpha} \widetilde{f}(\alpha) e^{\mathrm{i}\alpha t}$$

où la somme est prise sur un ensembles de fréquences α. La fonction $\widetilde{f}$ qui donne le coefficient pour chaque α s'appelle la transformée de Fourier de f.

Dans la version discrète, on suppose que $t \in \{0, 1, \ldots, n-1\}$ et on considère des fréquences qui sont des multiples de $2\pi/n$. Soit $\omega_n = e^{2\mathrm{i}\pi/n}$, alors on obtient la transformée de Fourier discrète:

$$f(t) = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \widetilde{f}(k) (\omega_n)^{kt} \ .$$

On peut inverser cette formule. Elle s'écrit comme

$$\begin{pmatrix} f(0) \\ f(1) \\ f(2) \\ \vdots \end{pmatrix} = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & \\ 1 & \omega_n & \omega_n^2 & \cdots \\ 1 & \omega_n^2 & \omega_n^4 & \\ & \vdots & & \ddots \end{pmatrix} \begin{pmatrix} \widetilde{f}(0) \\ \widetilde{f}(1) \\ \widetilde{f}(2) \\ \vdots \end{pmatrix}$$

Plus convenablement: $f = Q\widetilde{f}$ où $Q_{tk} = \omega_n^{ky}/\sqrt{n}$. On remarque que $QQ^* = I_n$ d'où $\widetilde{f} = Q^* f$.

Revenons à l'état $|\psi\rangle$. On définit la transformée de Fourier des coefficients $a_{\underline{x}}$ qui dépendent de $\underline{x}$. On va écrire $a_{\underline{x}}$ comme une combinaison linéaire en une base de fonctions qui font des oscillations à une fréquence particulière. Par *fréquence*, on comprend un vecteur $\underline{k}$ comme $\underline{x}$ avec coefficients entières modulo 2: le coefficient avec fréquence $\underline{k}$ est

$$(-1)^{\underline{k}\cdot\underline{x}} := (-1)^{k_1 x_1 + \cdots + k_n x_n} \ ,$$

et l'état de base corréspondant

$$|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} (-1)^{\underline{k}\cdot\underline{x}} |\underline{x}\rangle \ .$$

(on l'a normalisé afin que $\langle \underline{k} | \underline{k} \rangle = 1$.

La transformée de Fourier est un changement de base unitaire obtenu en écrivant $|\psi\rangle$ comme une combinaison linéaire des $|\underline{k}\rangle$ au lieu des $|\underline{x}\rangle$:

$$|\psi\rangle = \sum_{\underline{k}} b_{\underline{k}} \, |\underline{k}\rangle \ .$$

Les amplitudes $b_{\underline{k}}$ sont les transformées de Fourier des $a_{\underline{x}}$:

$$b_{\underline{k}} = \langle \underline{k}|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} (-1)^{\underline{k}\cdot\underline{x}} a_{\underline{x}} \, . \tag{6.4}$$

Soit Q la matrice unitaire qui transforme la $|x\rangle$–base dans la $|k\rangle$–base. Alors ses coefficients sont données par

$$Q_{\underline{k},\underline{x}} = \langle \underline{k}|\underline{x}\rangle = \frac{1}{\sqrt{2^n}} (-1)^{\underline{k}\cdot\underline{x}} = \prod_{j=1}^{n} \frac{1}{\sqrt{2}} (-1)^{k_j x_j} \ .$$

Il s'ensuit que $Q = H \otimes \cdots \otimes H$ (on applique Q en appliquant H à chaque qubit). La transformation Q s'appelle la *transformée de Fourier quantique* (TFQ – QFT en anglais) définie sur le groupe $(\mathbf{Z}_2)^n$ (on peut la définir sur d'autres groupes).

Si on prend $|y\rangle = |1\rangle$, après avoir appliqué l'algorithme, la sortie est $(Q\,|\psi\rangle) \otimes |1\rangle$. Si on mesure les n premiers qubits, on obtient $|\underline{k}\rangle$ avec probabilité

$$p(\underline{k}) = |\, \langle \underline{k}|\psi\rangle \,|^2 = |b_{\underline{k}}|^2$$

où

$$a_{\underline{x}} = \frac{1}{\sqrt{2^n}} (-1)^{f(\underline{x})} \qquad \text{et} \qquad b_{\underline{k}} = \frac{1}{2^n} \sum_{\underline{x}} (-1)^{\underline{k}\cdot\underline{x} + f(\underline{x})} \, .$$

Par exemple, si $n = 1$ (l'algorithme de Deutsch), il existe deux fréquences possibles : $k = 0$ et $k = 1$.

Si $f(0) = f(1)$ alors $|b_0|^2 = 1$ et $|b_1|^2 = 0$.

Si $f(0) \neq f(1)$ alors $|b_0|^2 = 0$ et $|b_1|^2 = 1$.

Le problème de Deutsch-Jozsa (1992) : On prend n quelconque et on suppose que soit (a) f est constante ; soit (b) f est équilibrée : c'est à dire que $f(\underline{x}) = 0$ pour la moitié des $\underline{x}$ et $f(\underline{x}) = 1$ pour l'autre moitié. On voudrait savoir lequel de ces cas est vrai. On considére la probabilité $p(\underline{0})$ d'observer la fréquence $\underline{0} = (0, \ldots, 0)$. Alors le coefficient de Fourier correspondant:

$$b_{\underline{0}} = \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} a_{\underline{x}} = \frac{1}{2^n} \sum_{\underline{x}} (-1)^{f(\underline{x})} \, .$$

Il s'agit de la moyenne de $(-1)^{f(\underline{x})}$ sur tous les $\underline{x}$ qui est ± 1 si f est constante et 0 si f est équilibrée. D'où

$$p(\underline{0}) = |b_{\underline{0}}|^2 = \begin{cases} 1 & \text{si } f \text{ est constante} \\ 0 & \text{si } f \text{ est équilibrée} \end{cases}$$

Une observation de $\underline{k}$ suffit : retourne *constante* si $k_i = 0$ pour tout i ; sinon retourne *équilibrée*.

6.3. **Symétries cachées et le problème de Simon**

On suppose maintenant que f est définie comme une fonction des n–vecteurs $|\underline{x}\rangle$ avec coefficients dans $\mathbf{Z}_2$ et qu'elle prend ses valeurs dans l'espace des m-vecteurs $|\underline{y}\rangle$ avec coeffients dans $\mathbf{Z}_2$. Comme avant, on définit

$$U_f\,|\underline{x}\otimes\underline{y}\rangle = |\underline{x}\otimes(\underline{y}\oplus f(\underline{x}))\rangle\ .$$

En particulier:

$$U_f\left(\frac{1}{\sqrt{2^n}}\sum_{\underline{x}}|\underline{x}\otimes\underline{0}\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{\underline{x}}|\underline{x}\otimes f(\underline{x})\rangle\ . \tag{6.5}$$

Si on prend une mesure de l'état donné par la partie droite on observe une des 2^n valeurs possibles de f avec une probabilité uniforme. Pourtant il est possible d'obtenir des informations utiles conçernant des relations entre les valeurs de f pour un ensemble de différentes valeurs de $\underline{x}$.

Supposons que pour chaque entrée $\underline{x}$ il existe exactement un partenaire $\underline{x}'$ tel que $f(\underline{x}) = f(\underline{x}')$. En plus, on suppose qu'il existe un vecteur fixé $\underline{z}$ tel que

$$f(\underline{x}) = f(\underline{x}') \text{ si et seulement si } \underline{x}' = \underline{x}\oplus\underline{z}$$

Par example, si $n = 3$ et $\underline{z} = 101$ alors

$$f(000) = f(101),\ f(001 = f(100),\ f(010) = f(111),\ f(011) = f(110)\,,$$

et en plus ces quatre valeurs sont distinctes. Alors combien de fois faut-il interroger f afin d'apprendre $\underline{z}$? Si on mesure l'état donné par la partie droite de (6.5) on va observer l'une des 2^{n-1} valeurs possibles, $f = c$ disons, avec probabilité uniforme. Après la mesure, l'état s'effondra sur une superposition des $\underline{x}$ tel que $f(\underline{x}) = c$. Spécifiquement, d'après les hypothèses, l'état qui en resulte est

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\underline{x}_0\rangle + |\underline{x}_0\oplus\underline{z}\rangle\ .$$

pour un $\underline{x}_0$. Cet état est une superposition des deux états $\underline{x}_0$ et $\underline{x}_0' = \underline{x}_0\oplus\underline{z}$. On veut maintenant prendre une mesure de $|\psi\rangle$ afin d'apprendre quelque chose sur $\underline{z}$. De prendre une mesure dans la $\underline{x}$–base n'est pas utile ; on change de base en appliquant la transformée de Fourier. D'après (6.4), la transformée de Fourier donne les amplitudes :

$$b_{\underline{k}} = \frac{1}{\sqrt{2^n}}\frac{1}{\sqrt{2}}\left((-1)^{\underline{k}\cdot\underline{x}_0} + (-1)^{\underline{k}\cdot(\underline{x}_0\oplus\underline{z})}\right) = \frac{(-1)^{\underline{k}\cdot\underline{x}_0}}{\sqrt{2^{n-1}}}\left(\frac{1+(-1)^{\underline{k}\cdot\underline{z}}}{2}\right)\ .$$

On remarque que $\underline{x}_0$, et par suite la valeur c qu'on a observé, n'a qu'une influence sur la phase, ce qui n'intervient pas dans le calcul de la probabilité $p(\underline{k})$ pour observer une fréquence $\underline{k}$:

$$p(\underline{k}) = |b_{\underline{k}}|^2 = \frac{1}{2^{n-1}}\left(\frac{1+(-1)^{\underline{k}\cdot\underline{z}}}{2}\right)^2\ .$$

Cette probabilité dépend sur la valeur $\underline{k} \cdot \underline{z}$ qui est 0 ou 1, où géométriquement, sur la propriété que $\underline{k}$ soit perpendiculier à $\underline{z}$ ou non. On peut l'écrire comme

$$p(\underline{k}) = \begin{cases} 1/2^{n-1} & \text{si } \underline{k} \perp \underline{z} \\ 0 & \text{autrement} \end{cases}$$

Donc on observe un vecteur de fréquence $\underline{k}$ choisit au hazard parmi les 2^{n-1} vecteurs perpendiculiers à $\underline{z}$. L'ensemble de tels vecteurs détermine un sous-espace de dimension $n-1$ et on peut déterminer $\underline{z}$ dès qu'on a observé un ensemble de vecteurs $\underline{k}$ qui engendre ce sous-espace.

Une exercice assez difficile montre qu'on peut trouver $\underline{z}$ après $\mathcal{O}(n)$ interrogations. D'autre part, du point de vue classique, on peut montrer qu'il prend à peu près $\sqrt{2^n} = 2^{n/2}$ interrogations afin de trouver une paire $\underline{x}$, $\underline{x}'$ telle que $f(\underline{x}) = f(\underline{x}')$; avant de trouver une telle paire on n'a aucune information sur $\underline{z}$.

Il s'agit d'un exemple du problème de trouver un sous-groupe caché : une fonction f est définie sur un groupe G et le défi est de trouver un sous-groupe de symétries de f. Dans ce cas $G = (\mathbf{Z}_2)^n$ et $H = \{\underline{0}, \underline{z}\}$. L'algorithme quantique résout le problème exponentiellement plus vite que l'algorithme classique.

L'algorithme de Shur (1994) résout le problème de factorisation d'un nombre N en cherchant la symétrie–en particulier la periodicité–d'une fonction définie sur les entiers modulo N. En effet, on cherche des racines carrées de 1 $\mod N$. Pour chaque N il y en a au moins deux: 1 et $N-1$. Mais si N est divisible par deux nombres premiers impaires distincts il y en a au moins deux autres racines carrées de 1, qu'on appelle non-triviales. Si on peut en trouver une on peut trouver un diviseur non-trivial de N, car $y^2 - 1 = (y+1)(y-1) = kN$ $(n \neq \pm 1)$ entraîne que $\text{pgcd}(y+1, N)$ et $\text{pgcd}(y-1, N)$ sont diviseurs propres de N. Quel est le lien avec la periodicité ?

Donné $c \in \mathbf{Z}_N^*$, son ordre est le plus petit entier $r > 0$ tel que $c^r \equiv 1 \mod N$. Autrement dit r est la périodicité de la fonction $f(x) = c^x \mod N$. Supposons qu'on peut trouver l'ordre r pour un c donné. Si on a de la chance r est paire et $c^{r/2}$ est une racine carrée de 1. Si on a encore de la chance, $c^{r/2} \neq -1 \mod N$ est il s'agit d'une racine non-triviale. La TFQ permet de trouver la periodicité d'une fonction en temps polynomial (plutôt qu'en temps exponentiel).

6.4. **La transformée de Fourier quantique**

La transformée de Fourier discrète (TFD) transforme N nombres complexes f_k en N nombres complexes $\widetilde{f_j}$:

$$\widetilde{f_j} = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{-jk} f_k$$

où $\omega_N = \exp(2\mathrm{i}\pi/N)$. Son inverse est donné par

$$f_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^{jk} \widetilde{f_k} \, .$$

Pour $N = 2$, la transformée de Fourier quantique (TFQ) est la transformée de Hadamard:

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

Donné un qubit $a_0 |0\rangle + a_1 |1\rangle$, la transformée de Hadamard nous donne un nouveau état:

$$a_0 |0\rangle + a_1 |1\rangle \mapsto \frac{1}{\sqrt{2}}(a_0 + a_1) |0\rangle + \frac{1}{\sqrt{2}}(a_0 - a_1) |1\rangle = \widetilde{a}_0 |0\rangle + \widetilde{a}_1 |1\rangle \ .$$

Pour $N = 2$, la porte Hadamard est le TFD *sur les amplitudes de l'état* dans la base de calcul. Plus généralement, la TFQ effectue une transformation des amplitudes d'un état en N dimensions:

$$\sum_{x=0}^{N-1} a_x |x\rangle \mapsto \sum_{x=0}^{N-1} \widetilde{a}_x |x\rangle = \sum_{x=0}^{N-1} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{-xy} a_y |x\rangle \ .$$

C'est à dire :

$$a_x \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{-xy} a_y \, .$$

Bien evidemment, la TFQ transforme les états de base :

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{-xy} |y\rangle \ .$$

Il s'ensuit que la matrice de la TFQ est donnée par

$$U = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \omega_N^{-xy} |y\rangle \langle x| \ .$$

Il s'agit d'une matrice unitaire.

On suppose que $N = 2^n$ et que les états de base sont de la forme : $|x\rangle = |x_1 x_2 \cdots x_n\rangle$ où $x_j \in \{0, 1\}$. On applique la TFQ :

$$\begin{aligned}
|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \omega_N^{-xy} |y\rangle &= \frac{1}{\sqrt{2^n}} \sum_{y_1,\ldots,y_n \in \{0,1\}} \omega_N^{-x \sum_{k=1}^n 2^{n-k} y_k} |y_1 y_2 \cdots y_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{y_1,\ldots,y_n \in \{0,1\}} \bigotimes_{k=1}^n \omega_N^{-x 2^{n-k} y_k} |y_k\rangle \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{k=1}^n \left\{ \sum_{y_k \in \{0,1\}} \omega_N^{-x 2^{n-k} y_k} |y_k\rangle \right\} \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{k=1}^n \left\{ |0\rangle + \omega_N^{-x 2^{n-k}} |1\rangle \right\} .
\end{aligned}$$

Si on adopte la notation décimale binaire :

$$0.x_j x_{j+1} \cdots x_n = \frac{x_j}{2} + \frac{x_{j+1}}{4} + \cdots + \frac{x_n}{2^{n-j+1}}$$

alors

$$|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \left\{ |0\rangle + e^{-2i\pi 0.x_n} |1\rangle \right\} \otimes \left\{ |0\rangle + e^{-2i\pi 0.x_{n-1} x_n} |1\rangle \right\} \otimes \cdots \otimes \left\{ |0\rangle + e^{-2i\pi 0.x_1 x_2 \cdots x_n} |1\rangle \right\}$$

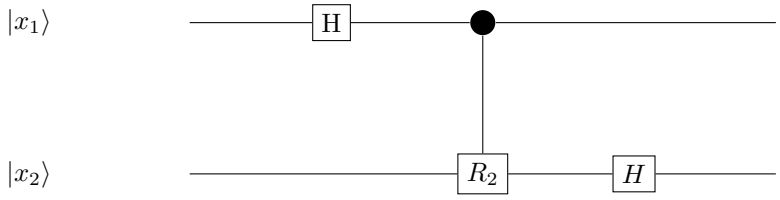
On remarque que $e^{-2i\pi 0.a} = \pm 1$, d'où si on applique la transformée de Hadamard au premier quibit de $|x_1 x_2 \cdots x_n\rangle$, on obtient

$$|x\rangle \mapsto \frac{1}{\sqrt{2}} \left\{ |0\rangle + e^{-2i\pi 0.x_1} |1\rangle \right\} \otimes |x_2 \cdots x_n\rangle .$$

On introduit la porte de rotation :

$$R_k := \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(-\frac{2\pi i}{2^k}\right) \end{pmatrix} .$$

On peut ainsi controller cette porte avec d'autres qubits afin d'obtenir le circuit quantique qui représente la TFQ, e.g. $n = 2$:



La transformation $Q = H \otimes H \otimes \cdots \otimes H$ de §6.2 et définie de manière similaire mais il ne s'agit pas du TFQ :

$$a_{\underline{x}} \mapsto b_{\underline{k}} = \frac{1}{\sqrt{2^n}} \sum_{\underline{x}} (-1)^{\underline{k} \cdot \underline{x}} a_{\underline{x}} .$$

6.5. **L'algorithme de recherche de Grover (1996)**

Cet algorithme effectue une recherche dans une base de données non-structurée, par exemple, la recherche d'un nom dans une annuaire téléphonique lorsqu'on ne connait que le numéro.

Soit N le nombre d'entrées. Alors un algorithme classique prend en moyenne $N/2$ tentatives. L'algorithme de Grover prend approximativement $\sqrt{N}$ tentatives.

Le problème est de trouver une aiguille dans une botte de foin. On suppose que l'espace des états est muni d'une base de N éléments $|j\rangle$, $1 \leq j \leq N$. L'aiguille se trouve à la place i. On veut la trouver. On peut interroger la botte de foin: on regarde l'endroit j afin de voir si l'aiguille est là. On peut représenter cette opération par un opérateur unitaire :

$$|j\rangle \otimes |y\rangle \mapsto \begin{cases} |j\rangle \otimes X\,|y\rangle & \text{si} \quad j = i \\ |j\rangle \otimes |y\rangle & \text{si} \quad j \neq i\,. \end{cases}$$

Autrement dit, on définit une fonction $f(j)$ telle que $f(j) = 0$ pour $j \neq i$ et $f(i) = 1$. Alors on a l'opération :

$$|j\rangle \otimes |y\rangle \mapsto |j\rangle \otimes |y \oplus f(x)\rangle\ .$$

On peut vérifier si on a une solution :

$$|j\rangle \otimes |0\rangle \mapsto \begin{cases} |j\rangle \otimes |0\rangle & j \text{ n'est pas bonne} \\ |j\rangle \otimes |1\rangle & j \text{ est bonne} \end{cases}$$

Si on pose $|y\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, on obtient

$$|j\rangle \otimes |-\rangle \mapsto \begin{cases} |j\rangle \otimes |-\rangle & j \text{ n'est pas bonne} \\ |j\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) & j \text{ est bonne} \end{cases}$$

On peut reporter la signe de $-$ sur le premier qubit et représenter cette opération par

$$U : |j\rangle \mapsto (-1)^{f(j)}\,|j\rangle\ .$$

Le circuit va distinguer le qubit $|j\rangle$ si $j = i$.

Grover: après chaque interrogation (chaque application de U) on adapte la superposition des endroits j où on va faire l'interrogation en appliquant un *opérateur de diffusion* :

$$D = \frac{2}{N}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Alors D est unitaire et $D^2 = I$.

On demarre l'algorithme avec un état uniforme sur tous les N états:

$$|u\rangle = \frac{1}{N}\sum_{j=1}^{N} |j\rangle\ .$$

Ensuite, on applique U et D de manière alternée. Après t itérations on obtient l'etat:

$$|\psi\rangle = \underbrace{DUDU\cdots DU}_{t}|u\rangle = (DU)^t\,|u\rangle\ .$$

Lorsque $t = \mathcal{O}(\sqrt{N})$, si on mesure $|\psi\rangle$ on observe $|i\rangle$ avec une grande probabilité (c'est à dire, lorsqu'on mesure $|\psi\rangle$, l'état s'effondra dans l'état propre $|i\rangle$ avec grande probabilité). Pourquoi ?

Pour un vecteur unitaire $|u\rangle$, réflexion dans l'axe engendré par $|u\rangle$ est donnée par

$$R_u = 2\,|u\rangle\,\langle u| - I.$$

En plus R_u est unitaire. Alors D est l'opérateur de réflexion dans l'axe de la distribution uniforme $|u\rangle$:

$$D = 2\,|u\rangle\,\langle u| - I = R_u\,.$$

De même, à une signe près, l'opérateur U est une réflexion dans l'axe $|i\rangle$:

$$U = I - 2\,|i\rangle\,\langle i| = -R_i\,.$$

L'algorithme a lieu dans un espace de dimension N, pourtant l'état $|\psi\rangle$ est toujours dans un sous-espace de dimension 2 : $W := \mathrm{vec}\,\{|i\rangle\,,|u\rangle\}$, ce qui équivaut à l'espace $W = \mathrm{vec}\,\{|i\rangle\,,|v\rangle\}$ où

$$|v\rangle = \frac{1}{\sqrt{N-1}}\sum_{j\neq i}|j\rangle = \frac{1}{\sqrt{N-1}}(\sqrt{N}\,|u\rangle - |i\rangle)\,.$$

Puisque $|i\rangle$ et $|v\rangle$ sont perpendiculiers, l'opérateur de projection est donné par

$$P_W = |i\rangle\,\langle i| + |v\rangle\,\langle v|$$

et restreint à W on a $I_W = P_V$, d'où

$$U|_W = |v\rangle\,\langle v| - |i\rangle\,\langle i| = 2\,|v\rangle\,\langle v| - I_W = R_v$$

Deux réflexions valent une rotation. Chaque itération DU est une rotation par 2θ dans W où θ est l'angle entre $|u\rangle$ et $|v\rangle$. Notre objectif est de pivoter $|\psi\rangle$ afin qu'il s'approche de $|i\rangle$. Au départ, $|\psi\rangle = |u\rangle$ qui est proche de $|v\rangle$ lorsque N est grand. L'angle entre $|v\rangle$ et $|i\rangle$ est $\pi/2$, donc il nous faut $t = \frac{\pi}{2}/2\theta$ itérations afin que $|\psi\rangle$ soit proche de $|i\rangle$ (en fait $|\psi\rangle$ commence à $|u\rangle$ plutôt que $|v\rangle$, donc l'angle initial est $\frac{\pi}{2} - \theta$ ce qui ajoute un demi-étape).

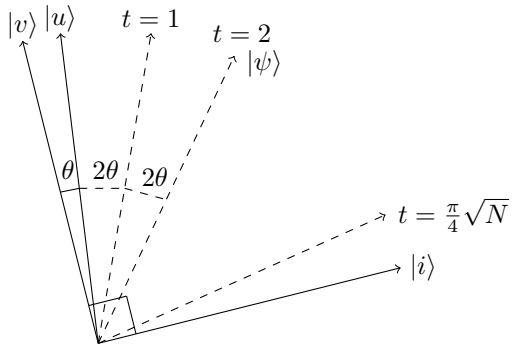
Il faut alors calculer l'angle θ entre $|u\rangle$ et $|v\rangle$.

$$\langle u|v\rangle = \cos\theta = \sqrt{1 - \frac{1}{N}} = 1 - \frac{1}{2N} - \mathbb{O}(N^{-2})$$

$$\begin{aligned}\cos\theta &= 1 - \frac{\theta^2}{2} + \mathcal{O}(\theta^4)\\ \Rightarrow\quad \theta &= \frac{1}{\sqrt{N}} + \mathcal{O}(N^{-3/2})\\ \Rightarrow\quad t &= \frac{\pi}{4\theta} = \frac{\pi}{4}\sqrt{N} - \mathcal{O}(N^{-1/2})\end{aligned}$$

En arrondisant t à l'entier le plus proche, après $t = \frac{\pi}{4}\sqrt{N}$ itérations de DU, l'angle entre $|\psi\rangle$ et $|i\rangle$ sera inférieur à θ et la probabilité d'observer i est

$$P(i) = |\langle\psi|i\rangle|^2 \geq \cos^2\theta = 1 - \mathcal{O}(\theta^2) = 1 - \mathcal{O}(1/N)\,.$$



Remarques : 1. S'il existe x aiguilles, l'angle θ est donnée par $\cos\theta = \sqrt{1 - \frac{x}{N}}$ et la probabilité de trouver une solution avec aiguilles identiques est grande après $\mathcal{O}(\sqrt{N/x})$ itérations.

2. Si $N = 4$ et la solution est unique, ou plus généralement si $x/N = 1/4$, l'algorithme de Grover trouve une solution avec probabilité 1 après un seul étape.

6.6. **L'algorithme de Shor – idée seulement**

On veut factoriser un grand nombre N. Pour illustrer la méthode on va factoriser 15 !

Choissisons un nombre < 15, par exemple 7. Calculer $f(k) = 7^k \mod 15$:

k	7^n	$7^n \mod 15$
1	7	7
2	49	4
3	343	13
4	2401	1
5	16807	7
⋮	⋮	⋮

On voit que la période de f est $R = 4$ (qui heureusement est paire). On calcule le pgcd$\{7^{R/2} \pm 1, 15\}$, par exemple

$$7^2 - 1 = 48 \quad \Rightarrow \quad \text{pgcd}\{48, 15\} = 3$$

$$7^2 + 1 = 50 \quad \Rightarrow \quad \text{pgcd}\{50, 15\} = 5$$

En général, pour $y < N$ on calcule $f(k) = y^k \mod N$ et on cherche la période R. Supposons $R = 2s$ paire. On remarque que $y^s \not\equiv 1 \mod N$ (la période est le plus petit R). Si $y^s \equiv -1 \mod N$ l'algorithme echoue et on doit reecommencer avec un different choix de y. Sinon

$$y^{2s} = 1 \mod N \quad \Rightarrow \quad (y^s - 1)(y^s + 1) = kN$$

ce qui entraîne que $\text{pgcd}\{y^s+1, N\}$ et $\text{pgcd}\{y^s-1, N\}$ sont des facteurs propres de N. Donc le problème de factoriser N se réduit en un problème de trouver les périodes paires $R = 2s$ de f pour lesquelles $y^s \neq -1 \mod N$.

L'idée derrière l'algorithme de Shor est

• Calculer simultanément toutes les valeurs d'une fonction périodique $y^k \mod N$;

• Adjuster les amplitudes de probabilité afin d'obtenir la période avec une grande probabilité (comment : en appliquant la transformée de Fourier quantique).

Illustration avec $N = 15$. On cherche la période de la fonction $f(k) = y^k \mod N$.

1. On choisit n afin que $2^n \geq N$; dans ce cas $n = 4$ suffit. On choisit $y < N$ tel que $\text{pgcd}\{y, N\} = 1$, par exemple $y = 13$.

2. On initialise deux états : $|\psi\rangle = |0000\rangle \otimes |0000\rangle$.

3. Au premier registre (les quatre premiers qubits) on applique une porte Hadamard à chaque qubit afin de créer un état intriqué uniforme :

$$|0000\rangle \mapsto \frac{1}{\sqrt{16}} \{|0000\rangle + |0001\rangle + |0010\rangle + \cdots + |1111\rangle\} = \sum_{k=0}^{15} \frac{1}{\sqrt{16}} |k\rangle$$

où k correspond à la version décimale de $|a_1a_2a_3a_4\rangle$: $k = a_1 2^3 + a_2 2^2 + a_3 2 + a_4$. On obtient alors l'état :

$$|\psi_1\rangle = \frac{1}{\sqrt{16}} \sum_{k=0}^{15} |k\rangle \otimes |\underline{0}\rangle \ .$$

4. On calcule la fonction $f(k) = 13^k \mod 15$ sur le 2ème quibit afin d'obtenir :

$$|\psi_2\rangle = \frac{1}{\sqrt{16}} \sum_{k=0}^{15} |k\rangle \otimes |f(k)\rangle = \frac{1}{\sqrt{16}} (|0\rangle \otimes |f(0)\rangle + |1\rangle \otimes |f(1)\rangle + \cdots)$$

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(k)$	1	13	4	7	1	13	4	7	1	13	4	7	1	13	4	7

Ceci est fait en une seule opération : *en appliquant le parallelisme quantique on peut calculer tous les $f(k)$ simultanément.*

5. On applique le TRQ au premier registre :

$$|k\rangle \mapsto \frac{1}{\sqrt{16}} \sum_{k=0}^{15} e^{2\pi i u k/16} |u\rangle$$

et on mesure l'état du premier registre.

Principe de la mesure implicite : Sans perdre la généralité, dans un circuit quantique, à la fin du circuit tout fil non-mesuré on peut supposer mesurer !

- Donc on peut supposer de plus que le 2ème registre est mesuré.

Pour le 2ème registre on obtient l'un de $|1\rangle, |13\rangle, |4\rangle, |7\rangle$ avec probabilité 1/4. Supposons qu'on obtient $|4\rangle$. On aura alors l'effondrement sur l'état :

$$\underbrace{\frac{1}{\sqrt{4}}(|2\rangle + |6\rangle + |10\rangle + |14\rangle)}_{|\psi_3\rangle} \otimes |4\rangle$$

6. On applique le TFQ à $|\psi_3\rangle$:

$$\begin{aligned}
|2\rangle &\mapsto \frac{1}{\sqrt{16}} \sum_{u=0}^{15} e^{2\pi i u \cdot 2/16} |u\rangle \\
|6\rangle &\mapsto \frac{1}{\sqrt{16}} \sum_{u=0}^{15} e^{2\pi i u \cdot 6/16} |u\rangle \\
|10\rangle &\mapsto \frac{1}{\sqrt{16}} \sum_{u=0}^{15} e^{2\pi i u \cdot 10/16} |u\rangle \\
|14\rangle &\mapsto \frac{1}{\sqrt{16}} \sum_{u=0}^{15} e^{2\pi i u \cdot 14/16} |u\rangle
\end{aligned}$$

On obtient dans le premier registre

$$\begin{aligned}
|\psi_4\rangle &= \frac{1}{\sqrt{4}} \frac{1}{\sqrt{16}} \sum_{u=0}^{15} \left\{ e^{2\pi i u \cdot 2/16} + e^{2\pi i u \cdot 4/16} + e^{2\pi i u \cdot 10/16} + e^{2\pi i u \cdot 14/16} \right\} |u\rangle \\
&= \frac{1}{8} \sum_{u=0}^{15} A_u |u\rangle \ .
\end{aligned}$$

La probabilité d'obtenir $|u\rangle$ en mesurant le 1er registre est

$$p_u = |\frac{1}{8} A_u|^2 .$$

On vérifie que $p_0 = p_4 = p_8 = p_{12} = 1/4$ avec toute autre probabilitié zéro. On peut également vérifier que si on choisit d'autres resultats pour le 2ème registre, par exemple $|1\rangle, |13\rangle$ ou $|7\rangle$ on obtient les mêmes probabilités : $p_0 = p_4 = p_8 = p_{12} = 1/4$. On peut démontrer dans cet exemple que la probabilité est non-nulle que si $2^n = 16$ divise uR où R est la période : $uR = 16\ell$.

Resumé : En appliquant l'algorithme de Shor, on obtient l'un parmi $|u\rangle = |0\rangle, |4\rangle, |8\rangle, |12\rangle$ chacun avec probabilité 1/4 et la période uR vérifie 16ℓ. Dans notre cas

$|u\rangle = |0\rangle$ ne donne aucune information – on refait l'algorithme ;

$|u\rangle = |4\rangle$ nous donne $4R = 16\ell : \ell = 1$ nous donne la période $R = 4$;

$|u\rangle = |8\rangle$ nous donne $8R = 16\ell : \ell = 1$ est incorrect et on refait l'algorithme ;

$|u\rangle = |12\rangle$ nous donne $12R = 16\ell : \ell = 3$ nous donne $R = 4$.

• L'algorithme a une probabilité de success de 1/2 après la première tentative.

7. **Processus quantiques**

En général un processus quantique est influencé par du bruit (*noise*) ou par une mesure. Tout système interagit avec le monde extérieur. On parle de système *ouvert* pour un système qui interagit avec son environment. Le formalisme mathématique pour incorporer le bruit est la notion de *processus quantique* (*quantum process*, ou *quantum operation*).

D'abord on considére un système classique. Soit p_0 et p_1 les probabilités initiales qu'un bit est dans les états 0 et 1 resp. et soit q_0 et q_1 les probabilités correspondantes après l'effet du bruit. Soit X l'état initial du bit et Y son état final. Alors

$$p(Y = y) = \sum_x p(Y = y|X = x)p(X = x)\,.$$

Par exemple, si p est la probabilité qu'un bit va changer son état et $1 - p$ la probabilité qu'il reste dans le même état, on aurait

$$\begin{pmatrix} q_0 \\ q_1 \end{pmatrix} = \begin{pmatrix} 1-p & p \\ p & 1-p \end{pmatrix} \begin{pmatrix} p_0 \\ p_1 \end{pmatrix}.$$

On suppose que les diverses bruits sont indépendants, d'où on obtient un processus stocastique de Markov $X \to Y \to Z$. Pour un seulétape, les probabilités de sortie $\vec{q}$ sont liées aux probabilités d'entrée $\vec{p}$ par une équation

$$\vec{q} = E\vec{p},$$

où E est une matrice de probabilités de transition - la matrice d'évolution. Donc l'état final est lié à l'état initial par une transformation linéaire.

Quelles sont les propriétés qu'une matrice d'évolution doit satisfaire ? Toutes les coefficients sont nécessairement ≥ 0 ; la somme de toutes les coefficients de chaque colonne est 1 (*complètitude*).

Système quantique: Rappelle sur l'opérateur densité ρ. Si on ne connait pas l'etat exact d'un système quantique mais on sait qu'il est dans l'état $|i\rangle$ avec probabilité p_i, on décrit le système avec un opérateur densité

$$\rho := \sum_i p_i \,|i\rangle \,\langle i|\ .$$

Pour un tel mélange statistique, l'espérance d'un observable A est $\mathrm{tr}\,(\rho A)$.

Si l'évolution du système est déterminée par un opérateur unitaire U (par exemple), après l'evolution le système est dans l'état $U\,|i\rangle$ avec probabilité p_i, d'où

$$\rho = \sum_i p_i \,|i\rangle \,\langle i| \xrightarrow{U} \sum_i p_i U \,|i\rangle \,\langle i|\, U^* = U\rho U^*$$

En général, un opérateur densité est un opérateur non-négatif hermitien de trace 1.

On se rappelle qu'une mesure est représentée par un opérateur Hermitien M qui s'écrit comme une combinaison de projecteurs

$$M = \sum_j a_j P_j, \quad P_j P_k = \delta_{jk} P_j, \quad \sum_j P_j = I\,,$$

où a_j sont les valeurs propres de M. Dans ce cas, la probabilité de mesurer m si l'état initial est i est

$$p(m|i) = \langle i|P_m^* P_m|i\rangle = \sum_j \langle j|P_m^* P_m|i\rangle \langle i|j\rangle = \mathrm{tr}\left(P_m^* P_m \left|i\right\rangle \langle i|\right). \tag{7.1}$$

On en déduit alors que

$$p(m) = \sum_i p(m|i)p_i = \sum_i p_i \mathrm{tr}\left(P_m^* P_m \left|i\right\rangle \langle i|\right) = \mathrm{tr}\left(P_m^* P_m \rho\right). \tag{7.2}$$

Après la mesure, si on obtient m comme résultat, alors le système est dans l'état

$$\psi_i^m := \frac{P_m \left|i\right\rangle}{\sqrt{\langle i|P_m^* P_m|i\rangle}}\,.$$

Donc on obtient un ensemble d'états $|\psi_i^m\rangle$ avec probabilité $p(i|m) = p(m|i)p_i/p(m)$ (loi de Bayes). Par suite, l'opérateur de densité correspondant est donné par (en appliquant (7.1) et (7.2))

$$\begin{aligned}\rho_m &= \sum_i p(i|m) \left|\psi_i^m\right\rangle \langle \psi_i^m| = \sum_i p(i|m) \frac{P_m \left|i\right\rangle \langle i| P_m^*}{\langle i|P_m^* P_m|i\rangle} \\ &= \sum_i p_i \frac{P_m \left|i\right\rangle \langle i| P_m^*}{\mathrm{tr}\left(P_m^* P_m \rho\right)} = \frac{P_m \rho P_m^*}{\mathrm{tr}\left(P_m^* P_m \rho\right)}\,.\end{aligned}$$

Supposons qu'on a perdu l'enregistrement du resultat m, mais on savait que on avait le système quantique ρ_m avec probabilité $p(m)$, alors on peut décrire l'état du système avec l'opérateur de densité

$$\rho = \sum_m p(m)\rho_m = \sum_m \mathrm{tr}\left(P_m^* P_m \rho\right) \frac{P_m \rho P_m^*}{\mathrm{tr}\left(P_m^* P_m \rho\right)} = \sum_m P_m \rho P_m^*\,.$$

Un processus quantique est une transformation du type

$$\rho' = \mathcal{E}(\rho)\,,$$

sur l'opérateur densité. L'application $\mathcal{E}$ est une *opération quantique*. Des exemples sont une transformation unitaire : $\mathcal{E}(\rho) = U\rho U^*$, ou le resultat d'une mesure : $\mathcal{E}_m(\rho) = P_m \rho P_m^*$.

Canal quantique: Soit H_1 et H_2 deux espaces de Hilbert de dimensions finies et soit $L(H_i) = \{$opérateurs linéaires aggisant sur $H_i\}$. On suppose ces deux espaces représentent deux systèmes quantiques dont les états sont déterminés par des opérateurs densité dans $L(H_i)$. Un *canal quantique* est un canal de communication qui transmet de l'information quantique ainsi que de l'information classique, par exemple l'état d'un qubit. Plus précisamment : un processus (ou opérateur) quantique $\mathcal{E}$ est une application sur l'ensemble des opérateurs densité des espaces respectifs tel que

(i) $0 \leq \mathrm{tr}\left(\mathcal{E}(\rho)\right) \leq 1$ pour tout état ρ.

(ii) $\mathcal{E}$ est convex linéaire sur l'ensemble des matrices densité :

$$\mathcal{E}\left(\sum_i p_i\rho_i\right) = \sum_i p_i\mathcal{E}(\rho_i)\,.$$

(iii) $\mathcal{E} : L(H_1) \to L(H_2)$ est *complètement positive* (CP) : $\mathcal{E}$ applique les opérateurs densité de H_1 aux opérateurs densité de H_2 de tel sorte que $\mathcal{E}(A)$ est positif pour tout A positif ; en plus, si on introduit un système R de dimension finie quelconque, il faut que $(\mathcal{I}\otimes\mathcal{E})(A)$ est positif sur le système $R\otimes H_1$ pour tout opérateur positif A, où $\mathcal{I}$ est l'opérateur identité sur R.

Remarques :
Opérateur positif : Un opérateur A est positive si $\langle v|A|v\rangle$ est réel et ≥ 0 pour tout vecteur $|v\rangle$. Tout opérateur positif est nécessairement hermitien : en effet, $A = \frac{1}{2}(A+A^*) + \frac{\mathrm{i}}{2}(\mathrm{i}(-A+A^*))$ s'écrit comme $B+\mathrm{i}C$ avec B et C hermitiens; en plus $\langle v|(A-A^*)v\rangle = 0$ pour tout v (par positivité) ce qui entraîne $A = A^*$.

Théorème de Choi : On identifie $L(H_1)$ avec $\mathbf{C}^{n\times n}$. Alors $\mathcal{E} : \mathbf{C}^{n\times n} \to \mathbf{C}^{m\times m}$ induit une autre application $I_k\otimes\mathcal{E} : \mathbf{C}^{k\times k}\otimes\mathbf{C}^{n\times n} \to \mathbf{C}^{k\times k}\otimes\mathbf{C}^{m\times m}$ donnée par $M\otimes A \mapsto M\otimes\mathcal{E}(A)$. Un élément de $\mathbf{C}^{k\times k}\otimes\mathbf{C}^{n\times n}$ s'exprîme comme

$$\begin{pmatrix} A_{11} & \cdots & A_{ik} \\ \vdots & \ddots & \vdots \\ A_{k1} & \cdots & A_{kk} \end{pmatrix},$$

où les A_{ij} sont des opérateurs sur $\mathbf{C}^n$ (ce qui identifie $\mathbf{C}^{k\times k}\otimes\mathbf{C}^{n\times n}$ avec $\mathbf{C}^{kn\times kn}$), d'où

$$(I_k\otimes\mathcal{E})\begin{pmatrix} A_{11} & \cdots & A_{ik} \\ \vdots & \ddots & \vdots \\ A_{k1} & \cdots & A_{kk} \end{pmatrix} = \begin{pmatrix} \mathcal{E}(A_{11}) & \cdots & \mathcal{E}(A_{ik}) \\ \vdots & \ddots & \vdots \\ \mathcal{E}(A_{k1}) & \cdots & \mathcal{E}(A_{kk}) \end{pmatrix}.$$

On dit que l'opérateur $\mathcal{E}$ est k positif si $I_k\otimes\mathcal{E}$ est positif (vu comme un élément de $\mathbf{C}^{kn\times kn}$), donc $\mathcal{E}$ est CP s'il est positif pour tout k.

Théorème de Choi : Soit $\mathcal{E} : \mathbf{C}^{n\times n} \to \mathbf{C}^{m\times m}$ positif, alors les affirmations suivantes sont équivalentes :

(i) $\mathcal{E}$ est n positif ;

(ii) $C_{\mathcal{E}} := (I_n\otimes\mathcal{E})\left(\sum_{i,j} E_{ij}\otimes E_{ij}\right) = \sum_{i,j} E_{ij}\otimes\mathcal{E}(E_{ij}) \in \mathbf{C}^{nm\times nm}$ est positif (la matrice de Choi) où E_{ij} est la matrice avec 1 dans la place ij et 0 ailleurs.

(iii) $\mathcal{E}$ est complètement positif.

Un non-exemple : L'opérateur de transposition $T : \mathbf{C}^{2\times 2} \to \mathbf{C}^{2\times 2}$ est positif mais pas 2-positif. Par exemple:

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

est positif dans $\mathbf{C}^4 \otimes \mathbf{C}^4$ mais son image sous $I_2 \otimes T$ est donné par

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

qui est une matrice de determinant -1 qui n'est pas alors positive.

Theorem 7.1. *L'application $\mathcal{E} : L(H_1) \to L(H_2)$ vérifie la caractérisation (i), (ii) et (iii) d'un opérateur quantique si et seulement si*

$$\mathcal{E}(\rho) = \sum_i E_i \rho E_i^* \tag{7.3}$$

où $E_i \in L(H_1, H_2)$ vérifient $\sum_i E_i^* E_i \leq I$.

Proof. Juste la partie qui en déduit les E_i (sinon c'est l'algèbre linéaire–voir Nielsen and Cheung Theorem 8.1).

On choisit un espace de Hilbert R tel que $\dim R = \dim H_1$. Soit $|i_r\rangle$ et $|i_{H_1}\rangle$ des bases orthonormée pour R et H_1 (on utilise le même indice i). Soit

$$|\alpha\rangle = \sum_i |i_r\rangle \otimes |i_{H_1}\rangle \in R \otimes H_1 \,.$$

Alors $|\alpha\rangle\langle\alpha| : R \otimes H_1 \to R \otimes H_1$. Soit

$$\sigma := (I_R \otimes \mathcal{E})(|\alpha\rangle\langle\alpha|) \in L(R \otimes H_1, R \otimes H_2) \,.$$

On peut décomposer σ comme $\sigma = \sum_i |s_i\rangle\langle s_i|$ où les vecteurs $|s_i\rangle$ ne sont pas nécessairement orthonormaux.

Soit $|\psi\rangle = \sum_j \psi_j |j_{H_1}\rangle \in H_1$ quelconque et soit $|\widetilde{\psi}\rangle := \sum_j \psi_j^* |j_R\rangle \in R$. On définit $E_i \in L(H_1, H_2)$ par $E_i(|\psi\rangle) = \langle\widetilde{\psi}|s_i\rangle$. Un calcul montre (7.3). □

Remarques : 1. La représentation (7.3) n'est pas unique.

2. Afin de connaître l'action de $\mathcal{E}$ sur un état quelconque de H_1 il suffit de connaître son action sur le seul état $|\alpha\rangle$ intriqué avec le système R.

Exemple 1. Les opérations de trace et trace partielle sont des opérations quantiques. On considère $H' = \text{vec}\{|0\rangle\}$ ($\dim H' = 1$). Soit $\{|i\rangle\}$ une base orthonormée pour H et soit

$$\mathcal{E}(\rho) = \sum_{i=1}^{n} |0\rangle \langle i|\rho|i\rangle \langle 0| = \text{tr}\,(\rho)\,|0\rangle \langle 0|\ ,$$

ce qui est de la forme (7.3) avec $E_i = |0\rangle \langle i|$.

Pour la trace partielle, on considère un système combiné $H \otimes R$ et on prend la trace sur R. Soit $\{|j\rangle\}$ une base orthonormée pour R et soit $E_i : H \otimes R \to H$ définie par

$$E_i\left(\sum_j \lambda_j\,|q_j\rangle \otimes |j\rangle\right) := \lambda_i\,|q_i\rangle$$

où $\lambda_j \in \mathbf{C}$ et $|q_j\rangle \in H$ sont quelconques. On définit $\mathcal{E}$ par $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^*$. Par (7.3) c'est bien une opération quantique $\mathcal{E} : L(H \otimes R) \to L(H)$. En plus

$$\mathcal{E}(\rho \otimes |j\rangle \langle j'|) = \rho\delta_{jj'} = tr_R(\rho \otimes |j\rangle \langle j'|)$$

pour ρ un opérateur hermitien quelconque sur H et $\{|j\rangle\}$ une base orthonormée sur R. Par la linéarité de $\mathcal{E}$ et tr_R on voit que $\mathcal{E}$ est bien tr_R.

Exemple 2. On se rappelle qu'un seul qubit s'exprîme comme un point sur la sphère (de Bloch) :

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{\mathrm{i}\varphi}\sin\frac{\theta}{2}\,|1\rangle \in H \quad (|\alpha|^2 + |\beta|^2 = 1)\,.$$

Pour un état pûr (voir page 3), $\rho = |\psi\rangle \langle\psi|$. Dans ce cas un calcule montre que

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2}\,,$$

où $\vec{r} = (\sin\theta\,\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$ et $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ où σ_j sont les matrices de Pauli :

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Plus généralement, on peut voir que pour un état ρ pas nécessairement pûr on a

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2}\,,$$

avec $\vec{r} \in \mathbf{R}^3$ tel que $||\vec{r}|| \leq 1$ – le vecteur de Bloch associé à l'état ρ.

Le canal "bit flip" qui interchange $|0\rangle$ et $|1\rangle$ avec probabilité $1-p$ est représenté par l'opération quantique $\mathcal{E}$ déterminé par les opérateurs : $E_0 = \sqrt{p}\,I = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $E_1 = \sqrt{1-p}\,X = \sqrt{1-p}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. On peut calculer explictement que

$$\mathcal{E}(\rho) = \frac{1}{2}\left\{\begin{pmatrix} 1-r_3 & r_1 + \mathrm{i}r_2 \\ r_1 - \mathrm{i}r_2 & 1+r_3 \end{pmatrix} + p\begin{pmatrix} 2r_3 & -2\mathrm{i}r_2 \\ 2\mathrm{i}r_2 & -2r_3 \end{pmatrix}\right\}.$$

Par exemple, si $p = 1/2$ on obtient $\mathcal{E}(\rho) = \frac{1}{2}\begin{pmatrix} 1 & r_1 \\ r_1 & 1 \end{pmatrix}$.

La matrice d'un processus quantique : On a un isomorphisme entre $L(L(H_1), L(H_2))$ et $L(H_1) \otimes L(H_2) = L(H_1 \otimes H_2)$ (l'isomorphisme de Choi). En effet on suppose qu'on a choisit des bases pour H_1 et H_2. Soit $\varphi : L(H_1) \to L(H_2)$ linéaire et soit E_{ij} la base canonique de $L(H_1)$ donnée par les matrices avec 1 dans la place ij et 0 ailleurs. On définit la matrice de Choi :

$$C_\varphi = \sum_{i,j} E_{ij} \otimes \varphi(E_{ij}) \in L(H_1) \otimes L(H_2)\,.$$

Reciproquement, donné $\sum_{i,j} E_{ij} \otimes A_{ij} \in L(H_1) \otimes L(H_2)$ ($A_{ij} \in L(H_2)\ \forall i, j$), on définit φ par $\varphi(E_{ij}) = A_{ij}$.

Supposons Alice et Bob font des expériences dans leurs laboratoires respectifs. Aux expériences de Alice. on associe des espaces d'Hilbert d'entrées H^{A_1} et de sorties H^{A_2} ; de même pour Bob on a H^{B_1} et H^{B_2}. Pour simplicité on suppose que ces espaces ont tous la même dimension. L'ensemble de tous les eventualités des expériences dans le laboratoire d'Alice est l'ensemble des CP–applications $\{\mathcal{M}_i^{A_1A_2}\}_{i=1}^n$. Par l'isomorphisme ci-dessus, on a

$$\mathcal{M}_i^{A_1A_2} : L(H^{A_1}) \to L(H^{A_2}) \quad \longleftrightarrow \quad M_i^{A_1A_2} \in L(H^{A_1} \otimes H^{A_2})$$

où $M_i^{A_1A_2}$ est non-négative. De même pour Bob.

La *probabilité non-contextuel* associée à deux mesures des sorties dans les deux laboratoires s'exprîme comme une fonction bilinéaire sur les opérateurs de Choi corresondants (rappel : le Théorème de Gleason (Th 1.2) exprîme la probabilité comme une trace) :

$$p(\mathcal{M}_i^{A_1A_2}, \mathcal{M}_j^{B_1B_2}) = \mathrm{tr}\,[W^{A_1A_2B_1B_2}(M_i^{A_1A_2} \otimes M_j^{B_1B_2})]$$

où $W^{A_1A_2B_1B_2} \in L(H^{A_1} \otimes H^{A_2} \otimes H^{B_1} \otimes H^{B_2})$ est fixé pour toute répétition de l'expérience. Ce formalisme suppose l'existence d'une structure de causalité globale incorporant les deux laboratoires.

8. **Les inégalités de Bell revisitées et les boites de Popescu-Rohrlich**

L'inégalité CHSH (Clauser-Horne-Shimony-Holt (1969)). Deux particules sont préparées dans un état intriqué, par example $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, et se déplacent vers deux appareils de mesure aux emplacements 1 et 2. Ces deux appareils mesurent une propriété des particules avec des paramètres de détection réglables a et b respectivement. Par exemple, on peut interpréter les paramètres comme la direction dans laquelle on mesure le spin.

Borne de Tirelson. On pose la question : par combien peut-on depasser l'inégalité de Bell ? Response : la borne de Tirelson pour l'inégalité de Bell en question.

Borne de Tirelson pour l'inégalité CHSH : Soient A, A', B, B' des observables pour Alice et Bob tel que $[A, B] = [A, B'] = [A', B] = [A', B'] = 0$ et avec mesures possibles $\in \{\pm 1\}$. Alors on a vu que

$$\mathbb{E}[AB] + \mathbb{E}[AB'] + \mathbb{E}[A'B] - \mathbb{E}[A'B'] \leq 2\sqrt{2}\,.$$

(Dans le cas classique la borne est 2).

Preuve : On définit l'observable $D = AB + AB' + A'B - A'B'$. Puisque les résultats de toute mesure correspond à un opérateur de projection, on a $A^2 = A'^2 = B^2 = B'^2 = \mathbb{I}$, d'où

$$D^2 = 4\mathbb{I} - [A, A'][B, B']\,.$$

Si $[A, A'] = 0$ ou $[B, B'] = 0$ on est dans le cas classique et $\mathbb{E}[D] \leq 2$. Dans le cas quantique

$$||[A, A']|| \leq 2||A||\,||A'|| \leq 2$$

et on obtient la borne $\mathbb{E}[D] \leq 2\sqrt{2}$. □

En 1994, Popescu et Rohrlich ont formulé un ensemble de mesures corrélées (sans signalement) qui donnent $S_{CHSH} = 4$ (le maximum algébrique). La formulation de ces expérience s'appellent des boites non-locales, ou des boites PR (de Popescu-Rohrlich). Ces expérience hypothétiques indiquent l'existence des théories raisonables de la nature qui sont en violation avec la théorie quantique.

Discussion par moyen d'un exemple : Alice appuie sur l'un de deux boutons $A0$ ou $A1$ de son appareil. Sur l'appareil de Bob, il observe l'un de deux indicateurs $b0$ et $b1$ s'allumer. Il y a alors quatre evenements possibles : $(A0, b0), (A0, b1), (A1, b0), (A1, b1)$. On suppose que les quatre evenements ont lieu avec probabilités conditionnelles : $p(b0|A0), p(b1|A0) = 1 - p(b0|A0), p(b0|A1), p(b1|A1) = 1 - p(b0|A1)$. Si $p(b0|A0) \neq p(b0|A1)$ alors le choix de Alice a un effet sur l'espérance du resultat de Bob et par suite il est possible pour Alice de communiquer avec Bob avec petite probabilité d'erreur. Par exemple, si $p(b0|A0) = 1/2$ et $p(b0|A1) = 2/3$, alors après cent répétitions d'appuyer sur le même bouton, Bob peut savoir avec grande certitude le bouton que Alice a poussé en regardant combien de fois $b0$ s'est allumé. On va compliquer la situtation.

Alice appuie sur l'un de $A0$ et $A1$ et Bob appuie sur l'un de $B0$ et $B1$. Alice observe l'un de deux eventualités $a0$ et $a1$ et Bob observe l'un de $b0$ et $b1$. Cette fois-ci, il y a $2^4 = 16$ possibilités : (AX, BY, ax, by) $(X, Y, x, y \in \{0, 1\})$. On suppose qu'en fait il n'y a que huit possibilités qui surviennent avec probabilités conditionnelles :

$$p(ax, by|AX, BY) = \begin{cases} \frac{1}{2} & \text{si } x \oplus y = XY \\ 0 & \text{sinon} \end{cases}$$

Si on appuie sur $A1$ et $B1$ $(XY = 1)$, les résultats avec probabilités non-nulles $((x \oplus y = 1 \Rightarrow x \neq y)$ sont les événements équiprobables $(a0, b1)$ ou $(a1, b0)$ (anti-corrélation). Dans les autres cas $(XY = 0)$, les deux résultats avec probabilités non-nulles $(x \oplus y = 0 \Rightarrow x = y)$ sont les événements

équiprobables $(a0, b0)$ ou $(a1, b1)$ (corrélation). Ces corrélations sont connus sous le nom : *boites de Popescu–Rohrlich* (1994).

Est-ce-que ces résultats impliquent qu'il existe une infuence A sur B ou B sur A ? D'abord, Alice ne peut pas envoyer un message à Bob en appuyant sur $A0$ ou $A1$ (ni Bob à Alice) car $p(bx|A0) = p(bx|A1)$ pour $x = 0$ et $x = 1$. L'ensemble des probabilités est sans signalement (no signaling). D'autre part, il est impossible de simuler ce résultat quand les deux participants ne peut pas communiquer entre eux.

En effet, Alice et Bob ont deux boites noires qui corrésondent à leurs laboratoires respectifs. L'entrée de Alice est $A0$ ou $A1$ qui donne des instructions sur l'expérience à faire ; les sorties pour Alice sont $a0$ ou $a1$. De même pour Bob. Est-ce-que les deux peuvent s'arranger d'avance afin que les résultats ci-dessus se produisent ?

Sans perdre la généralité, supposons que Alice et Bob s'arrangent d'avance que si $X = 0$ alors $x = 0$. Dans ce cas, lorsque $X = 0$ et $Y = 0$, il faut s'arranger que la boite noire de Bob produit $y = 0$ lorsque $Y = 0$ (corrélation). De plus, il faut que lorsque $X = 0$ et $Y = 1$, la boite de Bob produit $y = 0$ lorsque $Y = 1$ (corrélation). Puisque la boite de Bob produira $y = 0$ lorsque $Y = 0$, afin de guarantir success lorsque $X = 1$ et $Y = 0$, il faut que la boite de Alice produit $x = 0$ lorsque $X = 1$ (corrélation). Mais maintenant on a fixé tous les résultats des deux boites pour toute entrée et un problème est survenu : si $X = Y = 1$, les sorties seront $x = y = 0$ et il faut anti-corrélation dans ce cas ! Autrement dit, dans un cas sur quatre, l'expérience ne produira pas le résultat. Si les entrées sont aléatoires, 0 et 1 avec probabilité uniforme, alors la probabilité de succès (de reproduire ce qu'il faut) est au plus 3/4.

Bien evidemment, si on avait communication entre les boites, on pouvait toujours produire les résultats souhaités, par exemple, la boite de Alice dirait à la boite de Bob : mon entrée était $X = 0$ avec sortie $x = 0$, alors faites attention à ce que tu fais ! Le point important est que les boites sont séparées dans l'espace et un tel signal devrait se propager d'une vitesse plus grande que la lumière. La borne supérieure de success de 3/4 est une inégalité de type Bell : si les boites contiennent des particules quantiques préparées dans un état intriqué, et si on fait une expérience appropriée, on peut s'arranger pour que la probabilité de succès est plus grand que 3/4. Pourtant, dans le formalisme de la mécanique quantique, Tsirelson a montré que la probabilité de succès de ce jeu est au plus $(2 + \sqrt{2})/4 \sim 0,85$ (1980). En principle on peut attendre 1 et donc la question se pose (non-résolue !) : pourquoi la borne supérieure ? - est-ce-que c'est une propriété fondamentale de la nature ou est-ce-qu'il existe des cas où de telles bornes sont violées (pas encore observés).

Encore Bell : Alice mesure dans la direction A et Bob mesure dans la direction B. Les résultats a et b prennent les valeurs ± 1. Pour chaque mesure A et B, le *corrélateur* $\mathbb{E}[A, B]$ est défini comme l'espérance du produit ab :

$$\mathbb{E}[A, B] := \sum_{a,b} ab\, p(a, b|A, B)\,.$$

Notons que $ab = 1$ si Alice et Bob obtiennent le même résultat et -1 si ils obtiennent des résultats différents. Donc on peut interpréter $\mathbb{E}[A, B]$ comme l'espérance que les résultats de Alice et Bob sont corrélés.

Lorsque Alice fait un choix de deux possibilités $A0$ et $A1$ et Bob de $B0$ et $B1$, la valeur CHSH pour la probabilité jointe est par définition

$$S_{CHSH} := \mathbb{E}[A0, B0] + \mathbb{E}[A0, B1] + \mathbb{E}[A1, B0] - \mathbb{E}[A1, B1]\,.$$

On compare avec $x \oplus y = XY$ ci'dessus : La valeur CHSH comprend une contribution négative lorsque $A1$ et $B1$ sont choisies ($x = y$ lorsque $XY = 1$) et une contribution positive dans tous les autres cas ($x \neq y$ lorsque $XY = 0$).

– si la probabilité distribution jointe est décrite par des stratégies locales alors $-2 \leq S_{CHSH} \leq 2$.

– sinon, si on adopte les règles de la mécanique quantique, un paire intriqué peut atteindre $S_{CHSH} = 2\sqrt{2}$ (confirmé par l'expérience):

Preuve : On prépare l'état intriqué $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ où $|0\rangle$ et $|1\rangle$ sont les états propres pour $\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Aux choix de mesures A et B on associe des vecteurs $\vec{x}$ et $\vec{y}$ tels que $\vec{x} \cdot \vec{\sigma}$ est la mesure sur le premier qubit et $\vec{y} \cdot \vec{\sigma}$ la mesure sur le deuxième, où $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ est le vecteur des matrices de Pauli. D'aprés les règles de la théorie quantique on a

$$\mathbb{E}[A, B] = -\vec{x} \cdot \vec{y}\,.$$

On suppose que les deux choix de mesures pour A corréspondent aux mesures dans les directions orthogonales $\vec{e}_1$ et $\vec{e}_2$ réspectivement et que pour B ils corréspondent aux mesures dans les directions orthogonales $-\frac{1}{\sqrt{2}}(\vec{e}_1 + \vec{e}_2)$ et $\frac{1}{\sqrt{2}}(-\vec{e}_1 + \vec{e}_2)$. Dans ce cas on a

$$\mathbb{E}[A0, B0] = \mathbb{E}[A0, B1] = \mathbb{E}[A1, B0] = \frac{1}{\sqrt{2}} \quad \text{et} \quad \mathbb{E}[A1, B1] = -\frac{1}{\sqrt{2}}$$

d'où $S = 2\sqrt{2} > 2$. □

Boites non-locales : La boite de Popescu-Rohrlich est un exemple d'une boite non-locale. En général, une telle boite est caractérisée par la probabilité des sorties a et b donnée les entrées A et B : $p(a, b|A, B)$. Il faut que

$$p(a, b|A, B) \geq 0,\ \forall a, b, A, B \quad \text{et} \quad \sum_{a,b} p(a, b|A, B) = 1,\ \forall A, B\,.$$

Une boite est *locale*, ou admet un *modèle local de variable cachée* si les probabilités de sorties sont caractérisées par

$$p(a, b|A.B) = \sum_{\lambda} p(\lambda) p(a|A, \lambda) P(b|B, \lambda)\,,$$

où $p(a|A, \lambda)$ et $p(b|B, \lambda)$ sont les probabilité d' entrée/sortie des systèmes de Alice et Bob, et λ et choisit au hasard suivant une distribution de probabilité fixée $p(\lambda)$ – intuitivement λ corréspond à une variable cachée. Si une boite ne réspecte pas cette condition alors elle est non-locale.

Boites sans signalement : ni Alice, ni Bob peuvent signaler leur choix d'entrée à l'autre. Cette condition est formalisée par les équations :

$$\begin{aligned}\sum_b p(a,b|A,B) &= \sum_b p(a,b|A,B') := p(a|A) \quad \forall a,A,B,B' \\ \sum_a p(a,b|A,B) &= \sum_a p(a,b|A',B) := p(b|B) \quad \forall b,B,A,A'\end{aligned}$$

Cadre général : En général, si les entrées de Alice et Bob $A, B \in \{1,\ldots,m\}$ et les sorties $a, b \in \{1,\ldots,K\}$ (ce sont que des conventions - dans le cas binaire on prend plutot $A, B \in \{0,1\}$ et $a, b \in \{-1,+1\}$). Un scenario de Bell est caractérisé par les K^2m^2 probabiltiés $p(a,b|A,B)$, une pour chaque paire d'entrées et sorties. D'aprés Tirelson, on appelle l'ensemble $\mathcal{P} := \{p(a,b|A,B)\}$ un *comportement* (a behaviour). Un comportement corréspond alors à un point $\mathbf{p} \in \mathcal{S} \subset \mathbf{R}^{K^2m^2}$ déterminé par les contraintes : $p(a,b|A,B) \geq 0$ et $\sum_{a,b=1}^{K} p(a,b|A,B) = 1$, d'où $\dim \mathcal{S} = (K^2 - 1)m^2$.

On peut montrer que l'ensemble des comportements sans signalement est un sous-espace affine de $\mathbf{R}^{K^2m^2}$ de dimension $t := 2(K-1)m + (K-1)^2m^2$. En effet, une parametrisation est donnée par $\{p(a|A), p(b|B), p(a,b|A,B)\}$ où $a, b \in \{1,\ldots,K-1\}$ et $A, B \in \{1,\ldots,m\}$.

Comportement local Une autre contrainte concernent les comportements locaux, pour lesquels

$$p(a,b|A,B) = \int_\Lambda p(a|A,\lambda)p(b|B,\lambda)p(\lambda)\mathrm{d}\lambda\,,$$

où la variable cachée λ prend ses valeurs dans un espace Λ. Tout comportement local est sans signalement, mais pas reciproquement lorsque $K \geq 2$ et $m \geq 2$.

Explication : On introduit une variable cachée hypothétique λ avec distribution de probabilité $p(\lambda)$. On suppose que A et B représentent les resultats des mesures aux emplacements 1 et 2. Dans sa forme générale

$$A = A(a,b,\lambda), \quad B = B(a,b,\lambda)\,.$$

Si on accepte *réalisme local* : la mesure à l'emplacement 1 n'a pas d'influence sur la mesure à l'emplacement 2 et reciproquement, on aura

$$A = A(a,\lambda), \quad B = B(b,\lambda)\,.$$

La supposition de localité entraîne qu'on peut identifier des facteurs dans le passé, décrites par des variables λ, qui ont une influence causale sur les deux resultats, et qui expliquent la dépendance entre A et B. Lorsqu'on a pris en compte toutes ces facteurs, l'indétermination sur les résultats devaient découpler, c'est à dire les probabilités pour A et B devraient se factoriser :

$$p(A,B|a,b,\lambda) = p(A|a,\lambda)p(B|b,\lambda)\,.$$

Cette factorisation exprîme le fait qu'on a trouvé une explication d'après laquelle la probabilité pour A ne dépend que sur la variable λ et sur la mesure locale a, et pas sur la mesure distante b et son résultat.

Comportements quantiques : Enfin, on considère les comportements quantiques qui corréspondent aux éléments de $\mathcal{S}$ qui s'écrivent sous la forme

$$p(a,b|A,B) = \mathrm{tr}\left(\rho M_{a|A} \otimes M_{b|B}\right),$$

où ρ est un opérateur densité défini sur un espace de Hilbert $H^{Alice} \otimes H^{Bob}$ qui reprśente les systèmes combinés de Alice et Bob, et $M_{a|A}$ est un opérateur CP défini sur H^{Alice} qui corréspond aux expériences de Alice (d'où $M_{a|A} \geq 0$ et $\sum_{a=1}^{K} M_{a|A} = Id$) ; de même pour $M_{b|B}$.

L'ensemble $\mathcal{S}$ est un polytôpe, ainsi que les sous-ensembles des comportements sans signalement (NS) et locaux (L). On a $L \subset Q \subset NS \subset \mathcal{S}$ (inclusions strictes) où Q est l'ensembles des comportements quantiques. L'ensemble Q est convexe mais pas un polytôpe. Les hyperplans qui délimitent l'ensemble L corréspondent aux inégalités de Bell.

9. **Jeux de causalité**

On essaie de reconstruire la mécanique quantique à partir des principes information-théorique (L. Hardy, 2001). On rencontre alors des problèmes lorsqu'on veut imposer une structure de causalité.

Dans le cadre d'un processus quantique, on peut formuler un jeux dans lequel les processus locaux corréspondent aux opérateurs CP, mais aucune structure de causalité globale est supposée.

Le jeu (O. Oreshkov, F. Costa et C. Brukner, Nat. Comm. 3 (2012), 1092.) : Alice et Bob ont tous les deux un système dans leurs laboratoires respéctifs. D'abord on décrit le jeu de manière intuitive. Chacun lance une piece dont la valeur (pile ou face) est notée a pour Alice et b pour Bob. Les deux partagent un bit aléatoire c : si $c = 0$ alors Bob doit communiquer b à Alice ; si $c = 1$, alors Bob doit deviner la valeur de a. Les deux joueurs proposent une proposition du résultat de l'autre: x pour Alice et y pour Bob. Les bits a, b et c sont tous aléatoires.

L'objectif du jeu est de maximiser la probabilité de succès :

$$P_{succes} = \frac{1}{2}\{p(x = b|c = 0) + p(y = a|c = 1)\,,$$

c'est à dire, Alice doit deviner le résultat de Bob, ou reciproquement, dépendant de la valeur de c. Si tous les événements se passent dans une suite causale, alors

$$P_{succes} \leq \frac{3}{4}\,.$$

En effet, soit Alice ne peut pas signaler à Bob soit Bob ne peut pas signaler à Alice. Considérons ce dernier cas. Si $c = 1$, Alice et Bob pouvaient en principe atteindre $p(y = a|c = 1) = 1$. Pourtant, si $c = 0$, Alice ne peut que faire une proposition au hasard avec probabilité de succès $p(x = b|c = 0) = \frac{1}{2}$. Le même argument s'applique si Alice ne peut pas signaler à Bob.

Version quantique du jeu : Alice et Bob sont dans leurs laboratoires réspectifs. Les opérations dans chaque laboratoire sont décrites par des applications CP, mais à l'extérieur de chaque laboratoire

aucune structure causale est supposée. Un état quantique x entre dans le laboratoire d'Alice sur lequel elle effectue une mesure ; Alice prépare l'état a. De même pour Bob et même sous une stratégie mixte, c'est à dire par rapport à un mélange de structures causales (voir ci-dessous).

En effet, les deux joueurs partagent une boite noire et un bit c. Alice et Bob introduisent a et b dans la boite, qui ensuite sort les bits x et y dans leurs laboratoire réspectifs. Si une structure causale globale existe comprennant les deux laboratoires, alors $P_{succes} \leq 3/4$.

Déscription comme un processus quantique : On se rappelle que pour deux CP-applications $\mathcal{M}^{A_1A_2}$: $L(H^{A_1}) \to L(H^{A_2})$ et $\mathcal{M}^{B_1B_2} : L(H^{B_1}) \to L(H^{B_2})$, la probabilité d'obtenir deux resultats des mesures de Alice et Bob et donné par une fonction bilinéaire sur les CP-applications qui s'exprîme sous la forme :

$$p(\mathcal{M}^{A_1A_2}, \mathcal{M}^{B_1B_2}) = \mathrm{tr}\left\{W(M^{A_1A_2} \otimes M^{B_1B_2})\right\},$$

où $W \in L(H^{A_1} \otimes H^{A_2} \otimes H^{B_1} \otimes H^{B_2})$ (La matrice du processus) ne dépend que de la choix de la mesure, et $M^{A_1A_2} \in L(H^{A_1} \otimes H^{A_2})$ est l'opérateur corréspondant à $\mathcal{M}^{A_1A_2}$ par l'isomorphisme de Choi-Jamiolkowsky.

Dans le cadre du jeu ci-dessus, il exite un processus pour lequel on a $P_{succes} > 3/4$: on prend les CP-applications suivantes :

$$\begin{aligned} M^{A_1A_2}(x,a,c) &= \frac{1}{2}\{I + (-1)^x\sigma_3\}^{A_1} \otimes \{I + (-1)^a\sigma_3\}^{A_2} \\ M^{B_1B_2}(y,b,c) &= cM_1^{B_1B_2}(y,b,c) + (c \oplus 1)M_2^{B_1B_2}(y,b,c), \end{aligned}$$

où

$$M_1^{B_1B_2}(y,b,c) = \frac{1}{2}\{I + (-1)^y\sigma_3\}^{B_1} \otimes I^{B_2},$$

et

$$M_2^{B_1B_2}(y,b,c) = \frac{1}{2}\{I^{B_1 \otimes B_2} + (-1)^b(\sigma_1^{B_1} \otimes \sigma_3^{B_2})\}.$$

Un calcul montre que pour ce processus:

$$P_{succes} = \frac{2+\sqrt{2}}{4} > \frac{3}{4}.$$

Conclusions : Il s'agit d'un processus causal non-séparable, c'est à dire d'un processus quantique qu'on ne peut pas exprîmer comme un mélange de processus causaux :

$$W \neq \lambda W^{A \preceq B} + (1-\lambda)W^{B \preceq A},$$

où $0 \leq \lambda 1$ et $W^{A \preceq B}$ resprésente un processus pour lequel Alice ne peut pas signaler à Bob. "Ne peut pas signaler" s'interprète comme soit les canaux vont dans l'autre sens, soit les deux joueurs partagent un état biparti du type $\sum_{i,j} a_{ij} |i\rangle_A \otimes |j\rangle_B$.

Réalisme causal : $p(x, y|a, b)$ est un mélange convexe d'ordres causaux : l'ordre causal est prédéfini, même si on ne le connait pas avec certitude :

$$p(x, y|a, b) = p(A \preceq B)p(c|A \preceq B) \sum_c p(x|a, c, A \preceq B)p(y|a, b, c, A \preceq B)$$
$$+p(A \not\preceq B)p(c|A \not\preceq B) \sum_c p(y|b, c, A \not\preceq B)p(x|a, b, c, A \not\preceq B)\,.$$

L'inégalité causale joue un rôle analogue aux inégalités de Bell en invalidant le réalisme local. Problème : comment exclure ces boites (analogies des boites-PR) qui représentent un scenario causal réalist.

Paul Baird