Introduction au calcul et à la cryptographie quantiques

Une personne travaillant en cryptographie peut être ammenée à s'intéresser au monde quantique pour au moins trois raisons. (1) L'existence de protocoles cryptographiques (échange de clés) dont la sécurité repose sur les postulats de la physique quantique. (2) On a découvert des algorithmes pour (d'hypothétiques) ordinateurs quantiques, résolvant la factorisation et le logarithme discret, en temps polynomial. (3) La génération d'aléa vrai est possible dans un monde quantique.

On ne peut pas prévoir si tous ces aspects auront des développements utiles un jour. Mais ils font intervenir de façon cruciale les étrangetés du monde quantique, que l'on peut étudier avec des outils de mathématiques discrètes. L'objectif peut être aussi et surtout de mieux comprendre certains aspects fondamentaux de la théorie quantique.

■ **Introduction au calcul et à la cryptographie quantiques**

1. — Fondements 1
2. — Intrication 6
3. — Incompatibilité quantique / classique 8
4. — L'intrication comme outil 10
5. — Echange de clés 12
6. — Portes et circuits quantiques 14
7. — Transformée de Fourier (quantique) 17
8. — Supériorité quantique 20
9. — Factorisation 21
10. — Algorithme de Grover 22

Progrès des ordinateurs quantiques

• 2000 : IBM 5 qubits. • 2017 : IBM 50 qubits. • 2018 : Atos 41 qubits. • 2018 : Intel 49 qubits. • 2018 : Google Sycamore 53 qubits. • 2020 : IBM Hummingburd 65 qubits. • 2023 : IBM Condor 1121 qubits (bruité), Heron 133 puis 156 qubits avec erreurs atténuées. Aussi Atom 1125 qubits. • 2029 : Calcul tolérant aux fautes (prévision IBM, 200 qubits logiques). • 2033+ : 2000 qubits logiques ? (prévision IBM).

1. Fondements

Qubits

L'unité d'information (classique) est le bit. C'est l'information que peut stocker un dispositif ayant seulement deux états possibles. La mécanique quantique introduit le principe de superposition. Un qubit est une superposition des états 0 et 1 :

$$\alpha|0\rangle + \beta|1\rangle \qquad \text{où } \alpha, \beta \in \mathbb{C} \text{ (avec redondance).} \tag{1}$$

Cette notation étrange est équivalente à :

$$|0\rangle = \binom{1}{0}, \qquad |1\rangle = \binom{0}{1}, \qquad |\psi\rangle = \binom{\alpha}{\beta}.$$

Mais la mesure d'un qubit donne un bit classique (0 avec probabilité $|\alpha|^2$ et 1 avec probabilité $|\beta|^2$). On a jamais directement accès à α et β. L'aléa est un ingrédient fondamental de la théorie quantique.

Exemples de supports pour les qubits : fentes d'Young, spin 1/2, polarisation, Mach-Zehnder,...

Pour $\lambda \neq 0$, les états $\binom{\alpha}{\beta}$ et $\binom{\lambda\alpha}{\lambda\beta}$ sont physiquements indiscernables. Un qubit est donc de façon plus élégante un point $(\alpha : \beta)$ de la *sphère de Riemann* $\mathbb{C} \cup \{\infty\}$ (la droite projective complexe). Les points $(\alpha : \beta) = (1 : \beta/\alpha)$ avec $\alpha \neq 0$ sont associés au complexe β/α, tandis que le point $|1\rangle = (0 : 1)$ est associé à ∞.

Espaces de Hilbert

1.1. — Postulat 1. *L'état d'un système quantique isolé est entièrement défini par un vecteur dans un espace de Hilbert.*

Vecteur $\binom{\alpha}{\beta}$ dans l'espace de Hilbert $\mathbb{C}^2$ (plus généralement $\mathbb{C}^d$). On utilise le produit hermitien usuel $\langle x \,|\, y\rangle = \sum_{i=1}^n x_i^* y_i$.

Forme *hermitienne* en général : linéaire à droite, tordue-symétrique (donc tordue-linéaire à gauche). Définie positive : $\langle x \,|\, x\rangle \geqslant 0$ et nul seulement pour $x = 0$. On dit parfois *produit scalaire complexe*.

Utilisation de bases orthonormées (mesures projectives). Exemple

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

Paradoxe des trois filtres polarisants

Certains effets quantiques sont observables avec des outils simples. Si on filtre de la lumière avec deux filtres polarisants successifs tels que l'axe du deuxième soit tourné de $\pi/2$ par rapport au premier, tous les photons sont bloqués. Si on insère un filtre supplémentaire entre les deux premiers, avec un axe orienté dans une direction intermédiaire $\pi/4$ alors un photon sur huit est transmis. L'insertion de cet obstacle supplémentaire améliore la transparence du dispositif — phénomène que la physique classique peine à expliquer mais qui est une conséquence immédiate des postulats quantiques.

Dualité

L'espace de Hilbert est isomorphe à son dual :

$$\mathcal{U} : \mathcal{H} \ni y \longmapsto u_y \in \mathcal{H}^* \qquad \text{avec } u_y(x) = \langle y \,|\, x\rangle.$$

L'application $\mathcal{U}$ est linéaire tordue, injective parce que $\langle \cdot \,|\, \cdot \rangle$ est défini positif, et surjective parce que, pour $u \in \mathcal{H}^*$, on a $u(x) = x_1 u(e_1) + \cdots x_n u(e_n)$ donc $u = u_y$ avec $y_i = u(e_i)^*$.

Notation de Dirac

Soit $\mathcal{H}$ un espace de Hilbert. Les vecteurs sont notés par des *ket* : $|x\rangle$, $|y\rangle\ldots$ Un vecteur représentera un état quantique. L'usage représente les vecteurs par des colonnes. Souvent, la base canonique est notée $(|0\rangle, |1\rangle, \ldots, |d-1\rangle)$, mais parfois le label a une autre signification (l'issue d'une mesure).

Autre exemple : en dimension 4, mais vue comme celle de deux qubits. La base canonique est notée $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$. Un état général de deux qubits est de la forme $(\alpha, \beta, \gamma, \delta)^t$ ou encore

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \qquad \text{avec } \alpha, \beta, \gamma, \delta \in \mathbb{C} \text{ vérifiant } |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

On note $\langle y|$ l'application qui à $|x\rangle$ associe $\langle y \,|\, x\rangle$. Le symbole est un *bra*. Avec cette notation, $\langle y| \cdot |x\rangle = \langle x \,|\, y\rangle$. Matriciellement, $\langle y \,|\, x\rangle = y^\dagger x$. Un *bra* est un vecteur ligne. Si $|y\rangle = \sum_i y_i |i\rangle$ (dans la base canonique) alors $\langle y| = \sum_i y_i^* \langle i|$.

D'autre part, $|y\rangle\langle x|$ représente l'application $|z\rangle \mapsto \langle x \,|\, z\rangle |y\rangle$. Pour des vecteurs normés, c'est l'application qui envoie $|x\rangle$ sur $|y\rangle$, et l'orthogonal de $|x\rangle$ sur 0. En particulier $|x\rangle\langle x|$ est la projection orthogonale sur la droite engendrée par $|x\rangle$.

En général, si $(|0\rangle, \ldots, |d-1\rangle)$ est la base canonique (donc orthonormée) de $\mathbb{C}^d$, alors $\sum_{i,j=0}^{d-1} a_{i,j} |i\rangle\langle j|$ représente l'application de matrice $A = \big(a_{i,j}\big)_{0 \leqslant i,j \leqslant d-1}$ dans cette base :

$$\Big(\sum_{i,j=0}^{d-1} a_{i,j}|i\rangle\langle j|\Big)\Big(\sum_{i=0}^{d-1} x_j |j\rangle\Big) = \sum_{i=0}^{d-1} \Big(\sum_{j=0}^{d-1} a_{i,j} x_j\Big)|i\rangle$$

Par abus, $\sum_{i,j=0}^{d-1} a_{i,j}|i\rangle\langle j|$ représente aussi la matrice dans cette base canonique.

Pour $x = \sum_j x_j|j\rangle$ et $y = \sum_i y_i|i\rangle$, l'application $|y\rangle\langle x|$ est

$$|y\rangle\langle x| = \Big(\sum_i y_i|i\rangle\Big)\Big(\sum_j x_j^*\langle j|\Big) = \sum_{i,j} y_i x_j^*|i\rangle\langle j|$$

et a pour matrice $\big(y_i x_j^*\big)_{i,j}$ dans la base canonique. Cette matrice est obtenue en effectuant le produit matriciel $yx^\dagger$.

Opérateurs

On note $A^\dagger$ la matrice obtenue à partir de la matrice A par conjugaison et transposition. En fait, $A^\dagger$ est la matrice adjointe de A :

$$\langle y \,|\, Ax\rangle = y^\dagger Ax = (A^\dagger y)^\dagger x = \langle A^\dagger y \,|\, x\rangle.$$

Les isométries, c'est-à-dire les opérateurs U tels que $\langle Ux \,|\, Uy\rangle = \langle x \,|\, y\rangle$ pour tous x,y sont les opérateurs unitaires : $UU^\dagger = U^\dagger U = I$. Elles transforment les bases orthonormales en bases orthonormales.

1.2. — Postulat 2. *L'évolution d'un état quantique isolé (donc hors mesure) est unitaire (donc inversible).*

Exemples pour les qubits : $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ est la porte *non*, $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ déphase, $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ échange $|0\rangle$ avec $|+\rangle$ d'une part, et $|1\rangle$ avec $|-\rangle$ d'autre part (transformée de Walsh-Hadamard). Plus généralement, les opérateurs unitaires sur $\mathbb{C}^2$ sont les opérateurs de la forme

$$\theta \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \qquad \text{avec } \alpha, \beta, \theta \in \mathbb{C} \text{ tels que } |\theta| = 1 \text{ et } |\alpha|^2 + |\beta|^2 = 1.$$

Projection stéréographique

On peut identifier la droite projective complexe avec la *sphère de Bloch* (sphère unité de $\mathbb{R}^3$) par projection stéréographique. Pour un point $M = (x, y, z)$ sur la sphère, on considère la droite passant M par $P = (0, 0, -1)$ (lorsque $M \neq P$) :

$$\Big\{\big(tx, ty, tz - (1-t)\big) \big| t \in \mathbb{R}\Big\}.$$

Cette droite coupe le plan équatorial pour $t = 1/(1+z)$. Donc l'identification est donnée par les formules

$$(x, y, z) \longmapsto \frac{x + iy}{1 + z} \qquad \text{et } (0, 0, -1) \mapsto \infty.$$

Les états $|0\rangle$ et $|1\rangle$ sont les deux pôles. Les états $\frac{1}{\sqrt{2}}(|0\rangle + \mathsf{exp}(i\varphi)|1\rangle)$ forment l'équateur.

Attention : le point orthogonal à $\left(\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right)$ est $\left(\begin{smallmatrix} \beta^* \\ -\alpha^* \end{smallmatrix}\right)$. Sur la sphère de Bloch, ils sont diamétralement opposés car :

$$\left\langle \left(\frac{x+iy}{1+z}, 1\right) \middle| \left(\frac{-x-iy}{1-z}, 1\right) \right\rangle = -\frac{x^2+y^2}{1-z^2} + 1 = 0.$$

En coordonnées polaires, la projection stéréographique peut s'écrire

$$\mathbb{R}^3 \ni (\cos\varphi\ \sin\theta, \sin\varphi\ \sin\theta, \cos\theta) \longmapsto \big(\mathsf{exp}(i\varphi/2)\ \mathsf{sin}(\theta/2) : \mathsf{exp}(-i\varphi/2)\ \mathsf{cos}(\theta/2)\big) \in \mathbb{P}_1(\mathbb{C}).$$

Dans l'autre sens, pour $(a : b)$ que l'on peut supposer vérifier $|a|^2 + |b|^2 = 1$, on peut poser

$$a = \mathsf{sin}(\theta/2)\,\mathsf{exp}(i\alpha), \qquad b = \mathsf{cos}(\theta/2)\,\mathsf{exp}(i\beta), \qquad \varphi = \alpha - \beta.$$

On a alors

$$\begin{aligned}\mathbb{P}_1(\mathbb{C}) \ni (a : b) &= \big(\mathsf{exp}(i\varphi)\,\mathsf{sin}(\theta/2) : \mathsf{cos}(\theta/2)\big) = \big(\mathsf{exp}(i\varphi)\,\mathsf{sin}\,\theta : 1 + \mathsf{cos}\,\theta\big) \\ &\longmapsto (\cos\varphi\ \sin\theta, \sin\varphi\ \sin\theta, \cos\theta) \in \mathbb{R}^3.\end{aligned}$$

Plus généralement, lorsque $|\alpha|^2 + |\beta|^2 = 1$, on peut formuler la projection stéréographique inverse par

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle \longmapsto \big(\langle q|X|q\rangle, \langle q|Y|q\rangle, \langle q|Z|q\rangle\big) = \big(2\,\mathsf{re}(\alpha^*\beta), 2\,\mathsf{im}(\alpha^*\beta), |\alpha|^2 - |\beta|^2\big) \in \mathbb{R}^3.$$

Lien avec $\mathsf{SO}(3)$

L'opérateur X fait basculer la sphère de Bloch autour de l'axe des x, car $X\binom{\alpha}{\beta} = \binom{\beta}{\alpha}$, ce qui correspond à $\tau \mapsto 1/\tau$, c'est-à-dire à $(x+iy)/(1+z) \mapsto (x-iy)/(1-z)$. L'opérateur Z fait basculer la sphère autour de l'axe des z. L'opérateur $Y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right) = iXZ = -iZX$ autour de l'axe des y. Plus généralement, l'opérateur $xX + yY + zZ$ (avec $x^2+y^2+z^2 = 1$) fait basculer d'un angle π la sphère autour de l'axe dirigé par le vecteur (x, y, z) (c'est l'action par conjugaison du quaternion canonique iR).

Encore plus généralement, $\exp\big(i(\theta/2)R\big) = \cos(\theta/2)I + i\sin(\theta/2)R$ fait tourner la sphère d'un angle θ. Par exemple,

$$\exp\left(i\frac{\theta}{2}Z\right) \cdot X \cdot \exp\left(i\frac{\theta}{2}Z\right)^\dagger = \cos(\theta)X - \sin(\theta)Y,$$
$$\exp\left(i\frac{\theta}{2}Z\right) \cdot Y \cdot \exp\left(i\frac{\theta}{2}Z\right)^\dagger = \cos(\theta)Y + \sin(\theta)X,$$
$$\exp\left(i\frac{\theta}{2}Z\right) \cdot Z \cdot \exp\left(i\frac{\theta}{2}Z\right)^\dagger = Z.$$

Produit tensoriel

Produit tensoriel d'espaces vectoriels : pour E de base $(e_1, \dots, e_m)$ et F de base $(f_1, \dots, f_n)$, le produit $E \otimes F$ a pour base la famille $(e_i \otimes e_j)_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$.

Produit tensoriel de vecteurs : pour $a = (a_i)_i$ et $b = (b_i)_i$, on a $a \otimes b = (a_i b_{i'})_{(i,i)'}$ avec un double indice que l'on classe par ordre lexicographique. Produit tensoriel de matrices :

$$A = (A_{i,j})_{0 \leqslant i \leqslant m-1, 0 \leqslant j \leqslant n-1} \quad B = (B_{i',j'})_{0 \leqslant i' \leqslant m'-1, 0 \leqslant j' \leqslant n'-1} \qquad (A \otimes B)_{(i,i'),(j,j')} = A_{i,j} B_{i',j'}.$$

Plein de propriétés. Exemple utile :

$$(A \otimes B)(a \otimes b) = Aa \otimes Bb.$$

1.3. — Postulat 4. *L'espace des états d'un système quantique composé s'obtient comme produit tensoriel des espaces d'états de ses composantes.*

Lorsque le système est composé de parties indépendantes, l'état global est le produit tensoriel de ceux des parties. Mais l'espace des états contient des états non produits. En effet, pour un état produit :

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle.$$

Le déterminant des quatre coefficients est nul.

Les états non produits sont dits *intriqués*. Par exemple $\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$ est (maximalement) intriqué. L'intrication est aussi et surtout caractérisée par des corrélations entre les mesures des différentes parties.

Mesures projectives (ou observations)

L'issue d'une mesure quantique est probabiliste (le vecteur d'état ne permet pas de prévoir l'issue, mais seulement les probabilités). Répéter la mesure (plus généralement obtenir une information que l'on peut déduire des observations déjà faites) donne un résultat cohérent.

En physique, une observable est une variable que l'on peut mesurer. En physique quantique, une *observable* est représentée par un opérateur normal : $AA^\dagger = A^\dagger A$ (voire hermitien). C'est équivalent à dire qu'il est diagonalisable par une matrice unitaire (voire à vp réelles) :

1.4. — Théorème (spectral) [NS p.72]. *Un opérateur est normal ssi il est diagonalisable dans une base orthonormale.* □

Un opérateur normal est donc caractérisé par ses valeurs propres $\lambda \in \Lambda$, et par les espaces propres E_λ correspondants. Soient $P_\lambda = |\lambda\rangle\langle\lambda|$ les projecteurs associés. Ce sont des projecteurs orthogonaux :

$$E_\lambda^2 = E_\lambda \qquad \text{et} \qquad E_\lambda E_\mu = 0 \quad \text{pour } \lambda \neq \mu.$$

On a de plus

$$I = \sum_\lambda P_\lambda, \qquad \text{et} \qquad A = \sum_\lambda \lambda P_\lambda.$$

Inversement, pour toute famille $\{P_\lambda\}_\lambda$ de projecteurs orthogonaux, l'opérateur $\sum_\lambda \lambda P_\lambda$ est normal.

1.5. — Postulat 3. *Toute mesure quantique (projective) est décrite par une observable normale A. Les valeurs propres de A sont les issues de la mesure. La probabilité $p(\lambda)$ que l'issue soit λ lors de la mesure d'un état $|q\rangle$ est donnée par*

$$p(\lambda) = \langle q|P_\lambda|q\rangle.$$

L'état après mesure est alors

$$|q'\rangle = \frac{P_\lambda|q\rangle}{\sqrt{p(\lambda)}}.$$

1.6. — Exemples (Mesure d'un qubit). Pour une mesure dans la base $\big(|0\rangle, |1\rangle\big)$, on a

$$P_+ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad P_- = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \qquad P_+ + P_- = I, \qquad P_+ - P_- = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = Z.$$

Pour une mesure dans la base $\big(|+\rangle, |-\rangle\big)$, l'observable est $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, et :

$$P_+ = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \qquad P_- = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \qquad P_+ + P_- = I, \qquad P_+ - P_- = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X.$$

Dans la base $\big(|i\rangle, |-i\rangle\big)$, l'observable est $Y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$:

$$P_+ = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}, \qquad P_- = \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}, \qquad P_+ + P_- = I, \qquad P_+ - P_- = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = Y.$$

Plus généralement l'observable $S = xX + yY + zZ = \left(\begin{smallmatrix} z & x-iy \\ x+iy & -z \end{smallmatrix}\right)$ correspond au spin dans une direction quelconque où les réels x, y, z vérifient $x^2 + y^2 + z^2 = 1$. Les vecteurs $|s_+\rangle = \left(\begin{smallmatrix} 1+z \\ x+iy \end{smallmatrix}\right)$ et $|s_-\rangle = \left(\begin{smallmatrix} 1-z \\ -x-iy \end{smallmatrix}\right)$ associés à (x, y, z) et $(-x, -y, -z)$ par la projection stéréographique sont les vecteurs propres pour les valeurs propres ± 1. On a bien $P_+ + P_- = I$ et $P_+ - P_- = S$ avec

$$P_+ = \frac{1}{2+2z}|s_+\rangle\langle s_+| = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \quad \text{et} \quad P_- = \frac{1}{2-2z}|s_-\rangle\langle s_-| = \frac{1}{2}\begin{pmatrix} 1-z & -x+iy \\ -x-iy & 1+z \end{pmatrix}.$$

1.7. — Proposition. *L'espérance et la variance de la mesure $\mathcal{A}$ (d'observable A normale) ont pour expression*

$$E(\mathcal{A}) = \langle q|A|q\rangle \qquad\qquad \mathsf{Var}\,\mathcal{A} = \langle q|A^\dagger A|q\rangle - \big|\langle q|A|q\rangle\big|^2.$$

Démonstration — Pour la première formule, on diagonalise A dans une base orthogonale :

$$A = \sum_{i=1}^{n} \lambda_i |\lambda_i\rangle\langle\lambda_i|$$

où les λ_i sont les valeurs propres et les $|\lambda_i\rangle$ les vecteurs propres correspondants. Pour un état $x = \sum x_i|\lambda_i\rangle$ décomposé dans la base propre, on a

$$\langle x|A|x\rangle = \Big(\sum_j x_j^*\langle\lambda_j|\Big)\Big(\sum_k \lambda_k|\lambda_k\rangle\langle\lambda_k|\Big)\Big(\sum_i x_i|\lambda_i\rangle\Big) = \sum_k x_k^* x_k \lambda_k = E(\mathcal{A})$$

puisque $|x_k|^2$ est la probabilité d'obtenir l'issue λ_k. • Pour la deuxième, on remarque que $A^\dagger$ se diagonalise dans la même base : $A^\dagger = \sum_{i=1}^n \lambda_i^*|\lambda_i\rangle\langle\lambda_i|$. On a alors :

$$\begin{aligned}\langle Ax\,|\,Ax\rangle = \langle x\,|\,A^\dagger Ax\rangle &= \Big(\sum_j x_j^*\langle\lambda_j|\Big)\Big(\sum_k \lambda_k^*|\lambda_k\rangle\langle\lambda_k|\Big)\Big(\sum_l \lambda_l|\lambda_l\rangle\langle\lambda_l|\Big)\Big(\sum_i x_i|\lambda_i\rangle\Big) \\ &= \sum_k |x_k|^2|\lambda_k|^2 = E(|\mathcal{A}|^2) = \mathsf{Var}(\mathcal{A}) + \big|E(\mathcal{A})\big|^2\end{aligned}$$

puisque, par définition, la variance d'une variable complexe $\mathcal{X}$ est donnée par $E\big(|\mathcal{X}^2|\big) - \big|E(\mathcal{X})\big|^2$. □

1.8. — Définition. On dit que deux mesures sont *compatibles* lorsque leurs observables commutent (elles admettent une base commune de diagonalisation).

Principe d'incertitude

1.9. — Lemme (Cauchy-Schwarz). *Pour tous $x, y \in \mathcal{H}$, on a l'inégalité*

$$\big|\langle x \,|\, y\rangle\big|^2 \leqslant \langle x \,|\, x\rangle\langle y \,|\, y\rangle.$$

Démonstration — On a

$$\begin{aligned} 0 \leqslant \langle y \,|\, y\rangle\left\langle x - \frac{\langle y \,|\, x\rangle}{\langle y \,|\, y\rangle}y \middle| x - \frac{\langle y \,|\, x\rangle}{\langle y \,|\, y\rangle}y \right\rangle &= \langle y \,|\, y\rangle\langle x \,|\, x\rangle - \langle y \,|\, x\rangle\langle x \,|\, y\rangle - \langle y \,|\, x\rangle^*\langle y \,|\, x\rangle + \frac{\langle y \,|\, x\rangle^*\langle y \,|\, x\rangle}{\langle y \,|\, y\rangle}\langle y \,|\, y\rangle \\ &= \langle y \,|\, y\rangle\langle x \,|\, x\rangle - \langle y \,|\, x\rangle\langle x \,|\, y\rangle. \end{aligned}$$

Mais $\langle y \,|\, x\rangle\langle x \,|\, y\rangle = \langle x \,|\, y\rangle^*\langle x \,|\, y\rangle = \big|\langle x \,|\, y\rangle\big|^2$. □

1.10. — Théorème (Heisenberg). *Soient $|\psi\rangle \in \mathcal{H}$ et A, B deux observables (donc des opérateurs normaux). On a l'inégalité*

$$\mathsf{Var}\, A\ \mathsf{Var}\, B \geqslant \Big|\langle \psi, A^\dagger B\psi\rangle\Big|^2.$$

Démonstration — Supposons que $\langle A\rangle = \langle B\rangle = 0$ (quitte à remplacer A par $A - \langle A\rangle$ et idem pour B). On a alors

$$\begin{aligned} \mathsf{Var}\, A\ \mathsf{Var}\, B &= \langle A\psi, A\psi\rangle\langle B\psi, B\psi\rangle \\ &\geqslant \big|\langle A\psi, B\psi\rangle\big|^2 \quad \text{d'après Cauchy-Schwarz} \\ &= \Big|\langle \psi, A^\dagger B\psi\rangle\Big|^2. \end{aligned}$$

On a obtenu une borne inférieure au produit des deux variances. □

On peut noter en plus que $A^\dagger B = \frac{1}{2}(A^\dagger B + B^\dagger A) + \frac{1}{2}(A^\dagger B - B^\dagger A)$, le premier terme étant hermitien et le second anti-hermitien. L'espérance $\langle \psi, (A^\dagger B + B^\dagger A)\psi\rangle$ est un nombre réel x alors que $\langle \psi, (A^\dagger B - B^\dagger A)\psi\rangle$ est un imaginaire pur iy. On obtient alors

$$\mathsf{Var}\, A\ \mathsf{Var}\, B \geqslant |x + iy|^2 = x^2 + y^2.$$

2. Intrication

Etats de Bell

Les états de Bell sont les quatres états

$$|\mathcal{B}_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \qquad |\mathcal{B}_x\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\mathcal{B}_z\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |\mathcal{B}_y\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Les états de Bell forment une base propre commune aux opérateurs (compatibles 2 à 2, puisque X, Y et Z anticommutent)

$$X \otimes X = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \qquad Y \otimes Y = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix} \qquad Z \otimes Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

et les valeurs propres sont indiquées dans le tableau suivant

	$X \otimes X$	$Y \otimes Y$	$Z \otimes Z$
$\lvert\mathcal{B}_x\rangle$	-1	1	1
$\lvert\mathcal{B}_y\rangle$	1	-1	1
$\lvert\mathcal{B}_z\rangle$	1	1	-1
$\lvert\mathcal{B}_-\rangle$	-1	-1	-1

Si j'utilise les notations $|\mathcal{B}_?^X\rangle$ pour les mêmes expressions dans la base $(|+\rangle, |-\rangle)$, et aussi $|\mathcal{B}_?^Y\rangle$ pour celles dans la base $(|i\rangle, |-i\rangle)$, j'obtiens les identités :

$$\begin{array}{ll} |\mathcal{B}_-\rangle = -|\mathcal{B}_-^X\rangle = i|\mathcal{B}_-^Y\rangle & |\mathcal{B}_y\rangle = |\mathcal{B}_y^X\rangle = |\mathcal{B}_z^Y\rangle \\ |\mathcal{B}_z\rangle = |\mathcal{B}_x^X\rangle = -i|\mathcal{B}_x^Y\rangle & |\mathcal{B}_x\rangle = |\mathcal{B}_z^X\rangle = |\mathcal{B}_y^Y\rangle \end{array}.$$

Concurrence

Pour un état

$$|q\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \tag{2}$$

de deux qubits, on note $C = 2|\alpha\delta - \beta\gamma| \in [0,1]$. Si on exprime $|q\rangle$ dans la base de Bell :

$$\begin{aligned} |q\rangle &= \lambda|\mathcal{B}_x\rangle + i\mu|\mathcal{B}_y\rangle + \nu|\mathcal{B}_z\rangle + i\tau|\mathcal{B}_-\rangle \qquad \text{avec } |\lambda|^2+|\mu|^2+|\nu|^2+|\tau|^2 = 1 \\ &= \frac{1}{\sqrt{2}}\big((\lambda+i\mu)|00\rangle + (\nu+i\tau)|01\rangle + (\nu-i\tau)|10\rangle - (\lambda-i\mu)|11\rangle\big) \end{aligned} \tag{3}$$

on obtient une autre expression de la concurrence :

$$C = \big|(\lambda+i\mu)(-\lambda+i\mu) - (\nu+i\tau)(\nu-i\tau)\big| = \big|\lambda^2+\mu^2+\nu^2+\tau^2\big| \leqslant |\lambda|^2+|\mu|^2+|\nu|^2+|\tau|^2 = 1.$$

La concurrence est une mesure de l'intrication des états sur deux qubits. Elle vaut 0 pour les états produits et elle vaut 1 pour les états *maximalement* intriqués, comme les états de Bell, ou plus généralement pour les états (3) avec $\big|\lambda^2+\mu^2+\nu^2+\tau^2\big| = 1$.

De plus, pour $S = \lambda X - \mu Y - \nu Z$ avec λ, μ, ν (et τ) réels, on a

$$\langle q|S\otimes S|q\rangle = -(\lambda^2+\mu^2+\nu^2) = \tau^2 - 1$$

donc, pour $\tau = 0$, on observe une corrélation maximale lors d'une paire de mesures dans la direction $(\lambda, -\mu, -\nu)$.

Lorsque $\tau \neq 0$, par exemple pour $|q\rangle = \frac{1}{\sqrt{2}}\big(|\mathcal{B}_y\rangle + |\mathcal{B}_-\rangle\big) = \frac{1}{2}\big(|00\rangle + |01\rangle - |10\rangle + |11\rangle\big)$, On observe les corrélations maximales suivantes :

$$\langle q|X\otimes Z|q\rangle = -1, \qquad \langle q|Y\otimes Y|q\rangle = -1, \qquad \langle q|Z\otimes X|q\rangle = +1.$$

On a un autre exemple de corrélation maximale $\langle q|S\otimes S|q\rangle = -1$ pour l'état

$$|q\rangle = \frac{1}{2}\big(|\mathcal{B}_x\rangle + i|\mathcal{B}_y\rangle + |\mathcal{B}_z\rangle + i|\mathcal{B}_-\rangle\big) = \frac{1}{2}\big(\zeta|00\rangle + \zeta|01\rangle + \zeta^*|10\rangle - \zeta^*|11\rangle\big)$$

où $\zeta = \mathsf{exp}(i\pi/4)$, avec $S = \frac{1}{\sqrt{3}}(X - \zeta Y - Z)$ qui n'est pas à coefficients réels. On a aussi $\langle q|Z\otimes X|q\rangle = 1$.

Concurrence et densité

La matrice densité de la partie gauche de (2) est

$$\rho = |q\rangle\langle q| = \begin{pmatrix} |\alpha|^2+|\beta|^2 & \alpha\gamma^*+\beta\delta^* \\ \alpha^*\gamma+\beta^*\delta & |\gamma|^2+|\delta|^2 \end{pmatrix} = \frac{1}{2}\big(I + x_1X + y_1Y + z_1Z\big) = \frac{1}{2}\begin{pmatrix} 1+z_1 & x_1-iy_1 \\ x_1+iy_1 & 1-z_1 \end{pmatrix}$$

où

$$x_1 = 2\,\mathsf{re}(\alpha\gamma^*+\beta\delta^*) \qquad y_1 = 2\,\mathsf{im}(\alpha\gamma^*+\beta\delta^*) \qquad z_1 = |\alpha|^2+|\beta|^2-|\gamma|^2-|\delta|^2.$$

On a aussi

$$\rho^2 = \frac{1}{2}\left(\frac{1+r^2}{2}I + x_1X + y_1Y + z_1Z\right) \qquad \text{où } r^2 = x_1^2+y_1^2+z_1^2$$

donc $\mathsf{tr}(\rho^2) = \frac{1}{2}(1+r^2)$. On vérifie que

$$\begin{aligned} C^2 + r^2 &= 4|\alpha\delta-\beta\gamma|^2 + 4|\alpha\gamma^*+\beta\delta^*|^2 + \big(|\alpha|^2+|\beta|^2-|\gamma|^2-|\delta|^2\big)^2 \\ &= \big(|\alpha|^2+|\beta|^2+|\gamma|^2+|\delta|^2\big)^2 = 1. \end{aligned}$$

Donc

$$C = \sqrt{1-r^2} = \sqrt{2(1-\mathsf{tr}\,\rho^2)}. \tag{4}$$

Mesure et intrication

En tenant compte du fait que l'appareil de mesure est lui aussi quantique, la mesure (associée aux projecteurs P_λ) d'un état $|\psi\rangle$ est une opération qui transforme un état produit en un état intriqué :

$$|\psi\rangle \otimes |s\rangle = \Big(\sum_\lambda P_\lambda|\psi\rangle\Big) \otimes |s\rangle \longmapsto \sum_\lambda P_\lambda|\psi\rangle \otimes |\lambda\rangle$$

où $|s\rangle$ est l'état initial de l'appareil de mesure, et $|\lambda\rangle$ son état indiquant l'issue λ.

3. Incompatibilité quantique / classique

Inégalité CHSH

Alice et Bob réalisent des expériences sur (des échantillons de) deux systèmes $\mathcal{A}$ et $\mathcal{B}$ (dont les propriétés sont peut-être corrélées). Alice a le choix entre deux mesures sur $\mathcal{A}$, et Bob a le choix entre deux mesures sur $\mathcal{B}$. Les mesures sont notées A_1,A_2,B_1,B_2 et leurs issues ± 1.

Réalisme Local. Objectivisme : les grandeurs physiques sont définies indépendamment de leur observation. Localité : des parties distantes peuvent être séparées causalement.

Dans un cadre réaliste local, la mesure ne fait que révéler une grandeur qui existe indépendamment de la mesure. Cette grandeur ne dépend que du système (et peut-être de l'expérimentateur). Mais (par exemple) la valeur de A_1 ne dépend pas du fait que Bob mesure (ou ne mesure pas) B_1 ou B_2. Dans ce cadre la quantité

$$T := A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2$$

est parfaitement définie. On voit facilement qu'elle ne peut prendre que les valeurs ± 2. Pour plusieurs échantillons préparés de façon similaire, on a donc $E(T) \in [-2, 2]$. Si on veut confirmer $E(T)$ expérimentalement, on prendra soin de ne faire qu'une seule mesure sur chaque particule, puisque la deuxième mesure pourrait être faussée. Ainsi $E(T)$ est mesuré sous la forme $E(A_1B_1) + E(A_1B_2) + E(A_2B_1) - E(A_2B_2)$.

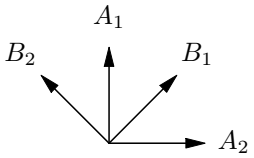


Figure 1. Les directions des mesures de spin

Dans un cadre quantique, considérons deux particules de spin 1/2 dans l'état $\mathcal{B}_- = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Si Alice et Bob mesurent les spins de leurs particules dans les directions respectives $\overrightarrow{u} : (x, y, z)$ et $\overrightarrow{u}' : (x', y', z')$ (avec $x^2 + y^2 + z^2 = x'^2 + y'^2 + z'^2 = 1$) alors la mesure est décrite par l'opérateur observable

$$S = (xX + yY + zZ) \otimes (x'X + y'Y + z'Z)$$

Dans le calcul de l'espérance $\langle \mathcal{B}_-|S|\mathcal{B}_-\rangle$ de cette mesure, seuls les termes diagonaux sont non nuls (par exemple $\langle \mathcal{B}_-|(X \otimes Z)|\mathcal{B}_-\rangle = 0$ et il reste

$$\begin{aligned}\langle \mathcal{B}_-|S|\mathcal{B}_-\rangle &= xx'\langle \mathcal{B}_-|(X \otimes X)|\mathcal{B}_-\rangle + yy'\langle \mathcal{B}_-|(Y \otimes Y)|\mathcal{B}_-\rangle + zz'\langle \mathcal{B}_-|(Z \otimes Z)|\mathcal{B}_-\rangle \\ &= -(xx' + yy' + zz') = -\overrightarrow{u} \cdot \overrightarrow{u}'.\end{aligned}$$

Pour la configuration de la figure 1, on a

$$T = -\overrightarrow{a}_1 \cdot \overrightarrow{b}_1 - \overrightarrow{a}_1 \cdot \overrightarrow{b}_2 - \overrightarrow{a}_2 \cdot \overrightarrow{b}_1 + \overrightarrow{a}_2 \cdot \overrightarrow{b}_2 = -\sqrt{2}/2 - \sqrt{2}/2 - \sqrt{2}/2 - \sqrt{2}/2 = -2\sqrt{2} < -2.$$

Le cadre quantique et le cadre réaliste local sont donc **incompatibles**.

Toutes les expériences réalisées confirment les prédictions quantiques. Elles montrent donc que la nature ne respecte pas la propriété de réalisme local. Ce travail expérimental a été couronné par le prix Nobel de physique en 2022 (Aspect/Clauser/Zeilinger).

L'argument GHZ

Les quatre opérateurs de Pauli sur 3 qubits :

$$M_0 = X \otimes X \otimes X, \qquad M_1 = X \otimes Y \otimes Y, \qquad M_2 = Y \otimes X \otimes Y, \qquad M_3 = Y \otimes Y \otimes X,$$

ont pour valeurs propres ± 1 (leurs carrés sont I). Ils commutent deux-à-deux, donc admettent une base de diagonalisation simultanée. L'état GHZ

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

est l'un des vecteurs propres simultané pour les quatres opérateurs. On a $M_0|\psi\rangle = |\psi\rangle$ et $M_i|\psi\rangle = -|\psi\rangle$ pour $i = 1, 2, 3$.

Les issues des quatres mesures sont ± 1. En supposant un cadre réaliste local, le produit des trois mesures $i = 1, 2, 3$ fait disparaître les $Y = \pm 1$, qui sont au carré. On devrait donc avoir l'identité $M_0 = M_1 M_2 M_3$. Pour l'état $|\psi\rangle$, les résultats observés des quatre M_i sont respectivement $1, -1, -1, -1$ et l'identité précédente deviendrait $1 = -1$.

En mécanique quantique, les M_i définissent quatres observations compatibles. On a $M_1 M_2 M_3 = -M_0$, conformément aux résultats expérimentaux.

Inégalité Leggett-Garg

Une mesure physique dichotomique est (potentiellement) effectuée à trois instants $t_1 < t_2 < t_3$. Les issues associées sont $a_1, a_2, a_3 \in \{\pm 1\}$. Si a_1, a_2 et a_3 sont définis (réalisme) alors l'expression $T := a_1 a_2 + a_2 a_3 - a_1 a_3$ vaut -3 lorsque $a_1 = -a_2 = a_3$, et vaut 1 dans tous les autres cas. Donc $-3 \leqslant T \leqslant 1$.

On note $Q_{i,j}$, pour $(i, j) = (1, 2)$, $(2, 3)$ ou $(1, 3)$, les corrélations

$$Q_{i,j} = \mathsf{prob}\{a_i a_j = 1\} - \mathsf{prob}\{a_i a_j = -1\}.$$

On a alors

$$K := Q_{1,2} + Q_{2,3} - Q_{1,3} = 1 - 4\big(\mathsf{prob}\{a_1, a_2, a_3 = + - +\} + \mathsf{prob}\{a_1, a_2, a_3 = - + -\}\big)$$

et donc l'inégalité $-3 \leqslant K \leqslant 1$.

Supposons au contraire que le système est un qubit, qui évolue en passant par les états $|q_i\rangle$ aux instants t_i, pour $i = 1, 2, 3$, avec

$$|q_1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + e^{-i\theta}|1\rangle\big), \qquad |q_2\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big), \qquad |q_3\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\theta}|1\rangle\big)$$

avec $\theta \in \mathbb{R}$. Supposons aussi que la mesure effectuée est celle dans la base $(|+\rangle, |-\rangle)$. On a alors

$$\mathsf{prob}\{a_1 = 1\} = \frac{1 + \cos\theta}{2}, \qquad \mathsf{prob}\{a_2 = 1\} = 1, \qquad \mathsf{prob}\{a_3 = 1\} = \frac{1 + \cos\theta}{2}.$$

On en déduit, puisque $\mathsf{prob}\{a_2 = -1\} = 0$,

$$Q_{1,2} = \mathsf{prob}\{a_1 = 1\} - \mathsf{prob}\{a_1 = -1\} = \cos\theta$$

et, de façon similaire, on trouve cette même valeur pour $Q_{2,3}$. En invoquant une « hypothèse de stationnarité » : la corrélation ne dépend pas de l'état de départ mais seulement de l'évolution, on peut montrer que $Q_{1,3} = \cos(2\theta) = 2\cos^2\theta - 1$. On obtient finalement

$$Q_{1,2} + Q_{2,3} - Q_{1,3} = 1 + 2\cos\theta - 2\cos^2\theta.$$

Cela peut dépasser la borne 1 ; on obtient même la valeur maximale $3/2$ pour $\theta = \pi/3$.

4. L'intrication comme outil

Téléportation

Les matrices de passage de la base canonique $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$ à la base de Bell $(|\mathcal{B}_y\rangle, |\mathcal{B}_x\rangle, |\mathcal{B}_z\rangle, |\mathcal{B}_-\rangle)$ et son inverse sont respectivement

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\\ 1 & -1 & 0 & 0\end{pmatrix} \quad \text{et} \quad \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0 & 1\\ 1 & 0 & 0 & -1\\ 0 & 1 & 1 & 0\\ 0 & 1 & -1 & 0\end{pmatrix}.$$

On a donc, pour un qubit $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ quelconque

$$\begin{aligned}|q\rangle|\mathcal{B}_-\rangle &= \frac{1}{\sqrt{2}}\big(\alpha|001\rangle - \alpha|010\rangle + \beta|101\rangle - \beta|110\rangle\big)\\ &= \frac{1}{2}\Big(\alpha\big(|\mathcal{B}_y\rangle + |\mathcal{B}_x\rangle\big)|1\rangle - \alpha\big(|\mathcal{B}_z\rangle + |\mathcal{B}_-\rangle\big)|0\rangle + \beta\big(|\mathcal{B}_z\rangle - |\mathcal{B}_-\rangle\big)|1\rangle - \beta\big(|\mathcal{B}_y\rangle - |\mathcal{B}_x\rangle\big)|0\rangle\Big)\\ &= \frac{1}{2}\Big(|\mathcal{B}_y\rangle\big(\alpha|1\rangle - \beta|0\rangle\big) + |\mathcal{B}_x\rangle\big(\alpha|1\rangle + \beta|0\rangle\big) + |\mathcal{B}_z\rangle\big(\beta|1\rangle - \alpha|0\rangle\big) - |\mathcal{B}_-\rangle\big(\alpha|0\rangle + \beta|1\rangle\big)\Big)\\ &= \frac{1}{2}\big(|\mathcal{B}_y\rangle XZ|q\rangle + |\mathcal{B}_x\rangle X|q\rangle - |\mathcal{B}_z\rangle Z|q\rangle - |\mathcal{B}_-\rangle|q\rangle\big).\end{aligned} \tag{5}$$

Donc, si Alice et Bob disposent d'un état de Bell $|\mathcal{B}_-\rangle$ partagé, on peut réaliser la téléportation d'un qubit $|q\rangle$ initialement possédé par Alice :

- Alice mesure les deux qubits en sa possession dans la base de Bell.
- Elle transmet à Bob le résultat de sa mesure (2 bits **classiques**).
- Bob applique la correction correspondante sur sa partie.

Téléportation en arrière

Le même protocole permet de téléporter un qubit en « remontant dans le temps ». La procédure est d'abord identique sauf que le qubit initial $|q\rangle$ d'Alice est non spécifié. Après l'étape de correction, Bob post-sélectionne son qubit sur l'état $\langle q'|$: il fait une mesure dans la base $(|q'\rangle, |q'^{\perp}\rangle)$ et ignore l'expérience si le résultat ne correspond pas à $|q'\rangle$. On peut alors en déduire que le qubit initial $\langle q|$ d'Alice était $\langle q'|$.

Codage super-dense

Si Alice et Bob disposent d'un état de Bell $|\mathcal{B}_-\rangle$ partagé, alors Alice peut transmettre à Bob deux bits d'information classique en envoyant à Bob un seul qubit.

Pour cela, elle sélectionne A l'un des quatre opérateurs I, X, Z, XZ en fonction des deux bits classiques qu'elle veut transmettre. Elle applique alors cet opérateur au composant de $|\mathcal{B}_-\rangle$ qu'elle possède, et envoie le qubit résultant à Bob. L'état transformé $(A\otimes I)|\mathcal{B}_-\rangle$ est alors l'un des quatre états de Bell, et caractérise A puisque

$$(I\otimes I)|\mathcal{B}_-\rangle = |B_-\rangle, \qquad (X\otimes I)|\mathcal{B}_-\rangle = |B_x\rangle, \qquad (Z\otimes I)|\mathcal{B}_-\rangle = |B_z\rangle, \qquad (XZ\otimes I)|\mathcal{B}_-\rangle = |B_y\rangle.$$

Bob n'a plus qu'à mesurer cet état dans la base de Bell pour savoir quelle transformation A Alice a appliquée. Il pourra alors en déduire les deux bits classiques choisis par Alice.

Si un attaquant intercepte le qubit envoyé par Alice à Bob, ce qubit n'est qu'une partie d'un état maximalement intriqué. Donc ce qubit ne porte à lui seul aucune information sur l'état quantique composé, ni sur les bits classiques encodés. La transmission selon ce protocole est donc sécurisée.

Non-signaling

Lorsque Alice et Bob partagent un état intriqué, les résultats de leurs mesures respectives sont corrélés, c'est-à-dire que le résultat obtenu par Alice peut dépendre du **résultat** obtenu par Bob. On pourrait penser que cela permet de transmettre de l'information de façon instantanée entre les deux parties. Il n'en est rien, comme le montre le résultat suivant qui précise que le résultat obtenu par Alice ne dépend pas de l'**action** effectuée par Bob. Une mesure projective arbitraire effectuée par Alice (ou Bob) est ici décrite par une transformation U_A (ou U_B) suivie d'une mesure dans la base canonique.

4.1. — Théorème. *Soit $|q\rangle$ un état partagé par Alice et Bob. Ils effectuent chacun la transformation U_A ou U_B sur leur partie respective et effectuent une mesure dans une base fixe. Les différentes probabilités des issues que peut obtenir Alice ne dépendent pas de la transformation U_B appliquée par Bob.*

Démonstration — On a

$$\begin{aligned}
\mathsf{prob}(x \mid U_A \otimes U_B) &= \sum_y \mathsf{prob}(x, y \mid U_A \otimes U_B) \\
&= \sum_y \langle q \mid (U_A^\dagger \otimes U_B^\dagger)(P_x \otimes P_y)(U_A \otimes U_B) \mid q\rangle \\
&= \sum_y \langle q \mid (U_A^\dagger P_x U_A) \otimes (U_B^\dagger P_y U_B) \mid q\rangle \\
&= \langle q \mid (U_A^\dagger P_x U_A) \otimes (U_B^\dagger \textstyle\sum_y P_y U_B) \mid q\rangle \\
&= \langle q \mid (U_A^\dagger P_x U_A) \otimes (U_B^\dagger I U_B) \mid q\rangle \\
&= \langle q \mid (U_A^\dagger P_x U_A) \otimes I \mid q\rangle
\end{aligned}$$

ce qui est indépendant de ce que fait Bob. □

On peut imaginer des dispositifs physiques respectant la condition de *non-signaling* mais ne respectant pas les postulats quantiques (donc ces dispositifs resteront à priori imaginaires). L'un d'eux est une *boîte non locale* qui permettrait de gagner systématiquement au jeu de Bell. Dans ce jeu, Alice et Bob reçoivent respectivement les inputs x et y et doivent répondre respectivement a et b tels que $a \oplus b = xy$ (avec $x, y, a, b \in \{0, 1\}$) pour marquer un point.

- Une stratégie classique permet de gagner avec probabilité maximum $3/4$.
- Une stratégie quantique permet de gagner avec probabilité maximum $\mathsf{cos}^2(\pi/8) \simeq 0.85$.
- Une stratégie utilisant une boîte non locale permet de gagner avec probabilité 1. Voici l'une de ces boîtes :
  - Lorsque $xy = 0$, la boîte répond $(a, b) = (0, 0)$ ou $(a, b) = (1, 1)$, chaque possibilité ayant probabilité $1/2$.
  - Lorsque $xy = 1$, la boîte répond $(a, b) = (0, 1)$ ou $(a, b) = (1, 0)$, chaque possibilité ayant probabilité $1/2$.
  - Cette boîte respecte *non-signaling* puisque l'observation de la réponse a (qui vaut 0 avec probabilité $1/2$ et 1 avec aussi probabilité $1/2$) n'apporte pas d'information sur l'input y. De façon symétrique, l'observation de la réponse b n'apporte pas d'information sur x.

Symétrie induite par un singlet

On partage un singlet $|\mathcal{B}_-\rangle = \frac{1}{\sqrt{2}}\big(|10\rangle - |01\rangle\big)$ entre Alice et Bob. Si Alice fait ensuite une mesure qui projette sa partie dans l'état $|a\rangle = \alpha|0\rangle + \beta|1\rangle$ alors on obtient

$$\big(|a\rangle\langle a| \otimes I\big)|\mathcal{B}_-\rangle = \frac{1}{\sqrt{2}}|a\rangle \otimes |b\rangle$$

où la partie de Bob est $|b\rangle = -\beta^*|0\rangle + \alpha^*|1\rangle = |a^\perp\rangle$. Le coefficient $1/\sqrt{2}$ exprime que la probabilité qu'Alice obtienne $|a\rangle$ lors de sa mesure est $1/2$.

La même expérience faite en remplacant $|\mathcal{B}_-\rangle$ par un autre état de Bell $|\mathcal{B}_w\rangle$ avec $w = x$, y ou z donne $|b\rangle$ symétrique de $|a\rangle$ dans la direction w.

Mesures non locales instantanées (ou pas)

Dans l'espace de deux qubits $|AB\rangle$, partagés par Alice et Bob, les états

$$|00\rangle, \qquad |01\rangle, \qquad |1+\rangle, \qquad |1-\rangle$$

forment une base orthonormale. Une mesure M dans cette base selon le formalisme de von Neumann est donc possible.

Effectivement, Alice peut mesurer sa partie selon Z, puis indiquer le résultat a à Bob. Ce dernier peut alors compléter la mesure M en mesurant sa partie dans la base Z si $a = 0$, ou dans la base X si $a = 1$. On peut noter que cette procédure ne peut pas être réalisée en temps arbitrairement petit puisqu'il faut un délai pour acheminer l'information classique a entre Alice et Bob.

D'ailleurs Vaidman montre plus généralement que toute mesure instantanée et globale de M permettrait de transmettre de l'information instantanément :

• Alice prépare un état $|a\rangle$ avec $a = 0$ ou 1 au dernier moment, alors que Bob prépare à l'avance l'état $|0\rangle$.

• La mesure M est effectuée (et selon l'hypothèse, le collapse est instantané et global).

• Bob effectue une mesure Z sur sa partie : il obtient b.

Si $a = 0$, l'état de Bob reste $|0\rangle$ après la mesure M et l'issue $b = 0$ de sa mesure est certaine. Si $a = 1$, l'état après mesure M est $|1+\rangle$ ou $|1-\rangle$ et l'issue b obtenue est 0 ou 1 de façon équiprobable. Le choix d'Alice aurait donc constitué un signal instantanément détectable par Bob, contredisant le *non-signaling*, prouvé dans le formalisme de von Neumann.

Pourtant, la procédure suivante peut être réalisée en temps arbitrairement court :

• En plus de l'état $|AB\rangle$, Alice et Bob disposent d'un état partagé $|\mathcal{B}_-\rangle$ préparé à l'avance.

• Alice mesure ses deux qubits dans la base de Bell. D'après (5), la partie de Bob est alors dans l'état $|A'\rangle = W|A\rangle$ où W est l'une des quatre matrices de Pauli, spécifiée par la valeur a obtenue par Alice.

• Sans attendre de connaître a, Bob effectue alors la mesure M sur les qubits $|A'B\rangle$. Il obtient une issue b.

La mesure M est considérée par Vaidman comme effectuée dans le sens où les issues a et b suffisent en principe à déterminer l'état initial $|AB\rangle$. Mais la mesure (et le collapse associé) n'est pas globale, dans le sens où les issues a et b ont été obtenues dans des lieux distincts. Bien sûr, pour qu'Alice, Bob ou une autre entité locale sache quel était l'état initial, il faudrait attendre que les deux valeurs a et b soient rassemblées en un lieu unique.

5. Echange de clés

BB84

Les qubits sont portés par des photons polarisés (par exemple). La polarisation horizontale et la polarisation verticale correspondent à deux états orthogonaux, que nous désignons arbitrairement $|0\rangle$ et $|1\rangle$, et qui forment la *base droite*. Les états de polarisation oblique $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ forment une deuxième base, dite *oblique*.

Si (par exemple) on mesure dans la base droite un photon polarisé obliquement, l'issue est totalement incertaine. On dit que les deux bases sont mutuellement sans biais.

• Alice choisit les n bits a_i à transmettre. Elle choisit aussi n autres bits r_i.

• Elle encode les a_i en utilisant la base droite ou la base oblique selon la valeur de r_i. Les photons polarisés sont envoyés vers Bob.

• Bob choisit n bits s_i (qui sont chacun un choix de base).

• Bob mesure les photons reçus en utilisant les bases désignées par les s_i. Il obtient des bits b_i qui sont les a_i choisis par Alice lorsque $r_i = s_i$ et des bits aléatoires lorsque $r_i \neq s_i$. De plus, certains photons sont tout simplement perdus.

• Par un canal classique, Alice et Bob s'échangent et comparent les r_i et les s_i. Les bits qui n'ont pas été mesurés dans la base initiale sont définitivement écartés. Les bits restants, si personne d'autre n'est intervenu sur le canal, sont corrects ($a_i = b_i$).

• Alice et Bob peuvent convenir de comparer, sur le canal classique, une certaine proportion des bits échangés. Une discordance est le signe d'une tentative d'interception. Si Eve tente d'intercepter le bit a_i, elle modifie sa polarisation si elle mesure avec une base différente de r_i. Si cette base est $\overline{r_i}$ alors la valeur b_i qu'obtiendra Bob est uniformément aléatoire. Ainsi, la tentative d'Eve fait que $a_i \neq b_i$ avec probabilité 1/4.

On peut améliorer ce protocole en utilisant 3 bases sans biais, au lieu de 2. Cette troisième base est donnée par $(|0\rangle + i|1\rangle, |0\rangle - i|1\rangle)$ et correspond à une polarisation circulaire. Les trois bases ont donc pour matrices $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, $\frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1&1\\1&-1\end{smallmatrix}\right)$ et $\frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1&i\\1&-i\end{smallmatrix}\right)$. On a $|\langle e_i, f_j\rangle|^2 = 1/2$ pour des vecteurs pris dans des bases différentes. On peut aussi le concevoir avec des qutrits (et 4 bases). Voici les caractéristiques des trois variantes, où n est le nombre de qubits ou qutrits utilisés :

Variante	Probabilité de discordance si interception par Eve	Probabilité que Eve obtienne une valeur correcte	Taille de la clé obtenue
2 bases	1/4	3/4	$n/2$ qubits
3 bases	1/3	2/3	$n/3$ qubits
qutrits	1/2	1/2	$n/4$ qutrits

B92

C'est une sorte de simplification de BB84. On fixe deux d'états qubits $|u\rangle$ et $|v\rangle$ non orthogonaux. (par exemple $u = |0\rangle$ et $v = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Alice choisit des bits aléatoires $b_i \in \{0, 1\}$ (pour $1 \leqslant i \leqslant n$) et encode chaque bit 0 par un $|u\rangle$, et chaque bit 1 par un $|v\rangle$. Bob choisit au hasard entre deux mesures projectives : celle dans la base $\mathcal{U} = (|u\rangle, |u^\perp\rangle)$ ou celle dans la base $\mathcal{V} = (|v\rangle, |v^\perp\rangle)$. S'il utilise la base $\mathcal{U}$ et qu'il obtient l'issue $u^\perp$, il est sûr qu'Alice a envoyé $|v\rangle$, donc encodé un 1. S'il utilise la base $\mathcal{V}$ et qu'il obtient une issue $v^\perp$, il est sûr qu'Alice a encodé un 0. En retour, Bob envoie à Alice les numéros des bits qu'il a ainsi obtenus.

Cela peut être interprété en termes de POVM. Posons $c = \langle u, v\rangle$, et définissons les trois opérateurs

$$E_{u^\perp} = \frac{|u^\perp\rangle\langle u^\perp|}{1+|c|}, \qquad E_{v^\perp} = \frac{|v^\perp\rangle\langle v^\perp|}{1+|c|}, \qquad E_0 = I - E_{u^\perp} - E_{v^\perp}.$$

On a alors

$$\begin{array}{lll} \langle u|E_{u^\perp}|u\rangle = 0, & \langle u|E_{v^\perp}|u\rangle = 1-|c|, & \langle u|E_0|u\rangle = |c|, \\ \langle v|E_{u^\perp}|v\rangle = 1-|c|, & \langle v|E_{v^\perp}|v\rangle = 0, & \langle v|E_0|v\rangle = |c|. \end{array}$$

Si Bob utilise ce POVM pour faire une mesure, l'issue $u^\perp$ signifie que l'état transmis est v, l'issue $v^\perp$ signifie que l'état transmis est u, l'issue 0 ne signifie rien de certain.

Bob obtient un bit de clé lorsque la base de mesure est différente de celle d'encodage et que l'issue est $|u^\perp\rangle$ ou $|v^\perp\rangle$. Cela arrive avec probabilité $(1 - |c|^2)/2$.

Ekert 91

Alice et Bob utilisent une source de paires de qubits intriqués, disons dans l'état $(|01\rangle - |10\rangle)/\sqrt{2}$. La sécurité de cette source n'est pas nécessaire, elle peut même être controlée par l'attaquant. Dans le protocole original, Alice et Bob utilisent chacun trois bases de mesure. L'exemple donné est celui de particules de spin 1/2 avec des mesures selon les directions d'angles $0, \pi/4, \pi/2$ pour Alice, et $\pi/4, \pi/2, 3\pi/4$ pour Bob. Je préfère attribuer à chaque partie 4 bases de mesure, notées A_k et B_k ($0 \leqslant k \leqslant 3$), repérées par les angles $k\pi/4$.

Par exemple, on utilisera les bases de mesure d'observables respectives

$$A_0 = B_0 = Z, \qquad A_1 = B_1 = H = \frac{Z+X}{\sqrt{2}}, \qquad A_2 = B_2 = X, \qquad A_3 = B_3 = \frac{Z-X}{\sqrt{2}}$$

dont les vecteurs propres sont respectivement

$$|0\rangle \text{ et } |1\rangle, \qquad c|0\rangle + s|1\rangle \text{ et } -s|0\rangle + c|1\rangle, \qquad |+\rangle \text{ et } |-\rangle, \qquad c|0\rangle - s|1\rangle \text{ et } s|0\rangle + c|1\rangle,$$

où $c = \mathsf{cos}(\pi/8) = \frac{1}{2}\sqrt{2+\sqrt{2}}$ et $s = \mathsf{cos}(\pi/8) = \frac{1}{2}\sqrt{2-\sqrt{2}}$.

Alice et Bob choisissent chacun indépendamment, et pour chaque paire reçue, une base de mesure. Notons A_a et B_b les bases choisies. Les (mesures des) paires pour lesquelles $a = b$ sont retenues pour former les bits de clé. Les paires pour lesquels a et b sont de parité contraire serviront à vérifier la qualité de la source en utilisant (deux fois) CHSH :

$$E(A_0B_1) + E(A_0B_3) + E(A_2B_1) - E(A_2B_3) = E(A_1B_0) + E(A_1B_2) + E(A_3B_0) - E(A_3B_2) = -2\sqrt{2}.$$

Les paires pour lesquelles a et b sont différents mais de même parités sont ignorées. En résumé, en notant k les configurations participant directement à la clé et c les configurations utilisées pour vérification par CHSH, on peut les représenter par la matrice

$$\begin{pmatrix} k & c & & c \\ c & k & c & \\ & c & k & c \\ c & & c & k \end{pmatrix}.$$

Si les a et b sont choisis avec probabilités uniformes, la proportion de paires utilisées pour k et c sont respectivement 1/4 et 1/2 (contre 2/9 et 4/9 dans le protocole original).

Sécurité

Si Eve veut distinguer deux états quantiques $|x\rangle$ et $|y\rangle$ sans perturbation. Elle doit utiliser une opération unitaire U (et un état initial $|s\rangle$) telle que

$$U(|x\rangle \otimes |s\rangle) = |x\rangle \otimes |u\rangle \qquad \text{et} \qquad U(|y\rangle \otimes |s\rangle) = |y\rangle \otimes |v\rangle$$

avec $|u\rangle \neq |v\rangle$ pour qu'une mesure puisse les distinguer. Mais alors, par conservation du produit hermitien, on a

$$\langle x \,|\, y\rangle = \langle x \,|\, y\rangle\langle u \,|\, v\rangle.$$

Puisqu'on a supposé $|u\rangle = |v\rangle$, on obtient que $|x\rangle$ et $|y\rangle$ sont orthogonaux.

6. Portes et circuits quantiques

Impossibilité du clonage

On ne peut pas cloner un état quantique. C'est une conséquence du postulat de linéarité. En effet, il faudrait un opérateur unitaire U tel que, pour deux états $|x\rangle$ et $|y\rangle$,

$$U|x0\rangle = |xx\rangle, \qquad U|y0\rangle = |yy\rangle, \quad \text{et} \quad U|(ax+by)0\rangle = |(ax+by)(ax+by)\rangle \quad \text{pour } |a|^2 + |b|^2 = 1.$$

Mais les deux premières identités entraînent $U|(ax+by)0\rangle = a|xx\rangle + b|yy\rangle$ par linéarité alors que la dernière implique $U|(ax+by)0\rangle = a^2|xx\rangle + ab(|xy\rangle + |yx\rangle) + b^2|yy\rangle$, ce qui n'est en général pas la même chose. **Il est plus simple de reprendre la démonstration précédente avec $|u\rangle = |x\rangle$ et $|v\rangle = |y\rangle$.**

Par contre, à partir d'un état (par exemple un qubit) $a|0\rangle + b|1\rangle$, il est possible d'obtenir $a|00\rangle + b|11\rangle$ (par la transformation unitaire envoyant la base $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$ sur la base $(|00\rangle, |01\rangle, |11\rangle, |10\rangle)$). Cette confusion a été à l'origine d'une controverse (initiée par Nick Herbert) sur la possibilité d'une communication à vitesse supra-luminique par laser : Alice fait une mesure dans la base droite ou bien oblique (selon la valeur du bit qu'elle veut transmettre) sur une composante d'un état de Bell. On a pu croire que Bob pourrait déterminer exactement l'état de sa composante (et donc le bit d'Alice) par tomographie après amplification laser.

Portes quantiques

Portes sur un qubit

Les portes les plus courantes sont les suivantes :

$$X, Y, Z, \quad H : \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S : \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad T : \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{pmatrix}.$$

Pour x, y, z réels tels que $x^2 + y^2 + z^2 = 1$ la porte $R = xX + yY + zZ$ représente sur la sphère de Bloch la rotation d'angle π autour de l'axe dirigé par (x, y, z). On a $R^2 = I$, donc

$$\exp\left(i\frac{\theta}{2}R\right) = \cos\left(\frac{\theta}{2}\right)I + i\sin\left(\frac{\theta}{2}\right)R$$

qui est la rotation de même axe et d'angle θ. La porte de Hadamard est un exemple ; son axe est $(x, y, z) = \frac{1}{\sqrt{2}}(1, 0, 1)$ et son angle est $\theta = \pi$.

Une porte générale sur un qubit est un opérateur unitaire, que l'on peut supposer de déterminant 1 en ignorant la phase globale. L'ensemble des portes s'identifie donc au groupe SU(2), qui est représenté par les matrices

$$\begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \qquad \text{avec } \alpha, \beta \in \mathbb{C} \text{ tels que } |\alpha|^2 + |\beta|^2 = 1. \tag{6}$$

Ce sont aussi les portes de la forme

$$tI + ixX + iyY + izZ \qquad \text{avec coefficients réels tels que } t^2 + x^2 + y^2 + z^2 = 1,$$

la correspondance étant donnée par $t = \operatorname{re}\alpha$, $x = \operatorname{re}\beta$, $y = -\operatorname{im}\beta$ et $z = \operatorname{im}\alpha$.

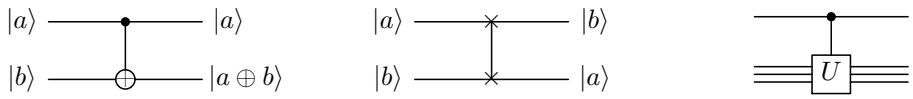
Dans la forme (6), posons $\alpha = \rho^* c$ et $\beta = \sigma^* s$ avec $|\rho| = |\sigma| = 1$ et $c, s \in \mathbb{R}$. puis $-\rho\sigma = \exp(i\varphi)$ et $-\rho\sigma^* = \exp(i\lambda)$. On a

$$\rho\begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} = \begin{pmatrix} c & \rho\sigma^* s \\ -\rho\sigma s & \rho^2 c \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} & -e^{i\lambda}\sin\frac{\theta}{2} \\ e^{i\varphi}\sin\frac{\theta}{2} & e^{i(\varphi+\lambda)}\cos\frac{\theta}{2} \end{pmatrix}$$

où $c = \cos(\theta/2)$ et $s = \sin(\theta/2)$. Cette forme de droite paramétrée par trois angles θ, φ, λ est par exemple celle utilisée dans le langage de programmation quantique `qiskit`.

Portes sur deux qubits

La porte *CNOT* (non contrôlé), la porte *SWAP*, le U contrôlé.



Leurs matrices dans la base canonique sont données par :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \left(\begin{array}{c|c} I & O \\ \hline O & U \end{array}\right).$$

Voir aussi la porte Z controlée (qui est symétrique).

6.1. — Proposition. *On peut fabriquer n'importe quel état $|\Psi\rangle$ sur 2 qubits à partir de $|00\rangle$ à l'aide d'une unique porte* CNOT *et d'opérations sur 1 qubit.*

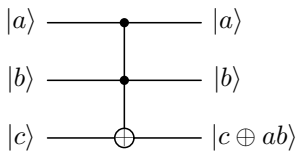
Démonstration — Il existe des opérations u et v sur un seul qubit telles que $(u \otimes v)|\Psi\rangle$ soit sous forme de Smith :

$$\lambda|00\rangle + \mu|11\rangle \qquad \text{avec } |\lambda|^2 + |\mu|^2 = 1.$$

Soit w une opération telle que $w|0\rangle = \lambda|0\rangle + \mu|1\rangle$. On a $|\Psi\rangle = (u^\dagger \otimes v^\dagger) \circ \text{CNOT} \circ (w \otimes I)|00\rangle$. □

Porte sur trois qubits

La porte de Toffoli (*CCNOT* ou *CCX*) :



$$\left(\begin{array}{c|c|c|c} I & O & O & O \\ \hline O & I & O & O \\ \hline O & O & I & O \\ \hline O & O & O & X \end{array}\right).$$

Implémentation de fonctions classiques

Un ordinateur quantique est souvent amené à évaluer des fonctions classiques (sur des états superposés). En général, la construction $|x\rangle \mapsto |f(x)\rangle$ est impossible puisque toute évolution quantique est réversible. Pour $f : \{0,1\}^n \to \{0,1\}$, on utilise souvent l'une des deux formes suivantes (où $b \in \{0,1\}$) :

$$U_f : |x\rangle \otimes |b\rangle \longmapsto |x\rangle \otimes |b \oplus f(x)\rangle \qquad \text{ou} \qquad P_f : |x\rangle \longmapsto (-1)^{f(x)}|x\rangle$$

qui sont réversibles. En fait, la deuxième peut être réalisée à partir de la première puisque $U_f(|x\rangle \otimes |-\rangle) = P_f(|x\rangle) \otimes |-\rangle$.

Rebond de phase

Considérons l'action d'une porte *bit-flip* controlé C-X :

$$|x\rangle \otimes |y\rangle \longmapsto |x\rangle \otimes |x \oplus y\rangle.$$

Le qubit de contrôle (à gauche) semble inchangé par définition. Pourtant, si on exprime $|x\rangle$ et $|y\rangle$ dans la base $(|+\rangle, |-\rangle)$ on observe :

$$|++\rangle \longmapsto |++\rangle, \qquad |+-\rangle \longmapsto |--\rangle, \qquad |-+\rangle \longmapsto |-+\rangle, \qquad |--\rangle \longmapsto |+-\rangle$$

et donc que le qubit de droite semble inchangé, mais contrôle un *phase-flip* sur le qubit de gauche. Les termes de qubit « de contrôle » et de qubit « contrôlé » sont donc quelque peu trompeurs et ne sont justifiés que relativement au choix de la base canonique utilisée pour définir les portes.

Quant à la porte C-Z : $|x\rangle \otimes |y\rangle \longmapsto (-1)^{xy}|x\rangle \otimes |y\rangle$, elle est symétrique. Donc les rôles des deux qubits et les termes pour les désigner sont interchangeables.

Portes de Clifford

Le groupe $\mathcal{P}_n$ de Pauli sur n qubits est l'ensemble des opérateurs de la forme $zP_1 \otimes \ldots \otimes P_n$ où $z \in \{\pm 1, \pm i\}$ et $P_i \in \{I, X, Y, Z\}$. Si n éléments de $\mathcal{P}_n$ commutent deux-à-deux et laissent stable un unique (à phase près) état $|q\rangle$, on dit que $|q\rangle$ est un état *stabilisateur*. Par exemple, les états stabilisateurs pour un unique qubit sont les états $|0\rangle, |1\rangle, |+\rangle, |-\rangle, |i\rangle|-i\rangle$ qui forment un octaèdre sur la sphère de Bloch.

Les portes de Clifford sont celles qui laissent $\mathcal{P}_n$ invariant par conjugaison. Elles forment un sous-groupe du groupe des unitaires, engendré par les portes H, $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$ et CNOT. Le théorème de Gottesman-Knill montre que le calcul de tout circuit utilisant seulement des portes de Clifford est simulable efficacement par un ordinateur classique. Pour profiter du potentiel supra-classique des ordinateurs classiques, on doit donc nécessairement introduire des portes non-Clifford, par exemple $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \zeta \end{smallmatrix}\right)$ avec $\zeta = (1+i)/\sqrt{2}$.

7. Transformée de Fourier (quantique)

Il s'agit de la transformée discrète habituelle. Soit $\omega = \mathsf{exp}(2i\pi/d)$. La transformée est l'application linéaire de $\mathbb{C}^d$ dans lui-même, dont la matrice dans la base canonique est $H_d = \frac{1}{\sqrt{d}} \sum_{s,t=0}^{d-1} \omega^{st} |s\rangle\langle t|$. À un état $|x\rangle = \sum_{t=0}^{d-1} x_t |t\rangle$, elle associe donc un état $\mathsf{QFT}\,|x\rangle = \sum_{s=0}^{d-1} \hat{x}_s |s\rangle$ dont les coordonnées sont données par :

$$\hat{x}_s = \frac{1}{\sqrt{d}} \sum_{t=0}^{d-1} \omega^{st} x_t \qquad \text{et inversement} \quad x_t = \frac{1}{\sqrt{d}} \sum_{s=0}^{d-1} \omega^{-st} \hat{x}_s.$$

C'est une transformation unitaire, d'après la relation de Parseval (ou parce que $H_d H_d^\dagger = I$).

Le cas le plus courant est celui de la transformée sur n qubits, c'est-à-dire où $d = 2^n$. L'identification $\mathbb{C}^{2^n} \simeq \mathbb{C}_2^{\otimes n}$ permet d'écrire les vecteurs $(|t\rangle)_{0 \leqslant t \leqslant d-1}$ de la base canonique sous deux formes au choix :

$$|t\rangle \sim |t_{n-1}\rangle \otimes \cdots \otimes |t_0\rangle \qquad \text{où } (t_{n-1}, \ldots, t_0)_2 \text{ est le développement binaire de } t.$$

L'image $\mathsf{QFT}\,|t\rangle = \frac{1}{\sqrt{d}} \sum_{s=0}^{d-1} \omega^{st} |s\rangle$ s'exprime alors sous la forme d'un état produit :

$$\begin{aligned}
\mathsf{QFT}\,\big(|t_{n-1}\rangle \cdots |t_0\rangle\big) &= \frac{1}{\sqrt{2^n}} \sum_{s=0}^{2^n-1} \omega^{st} |s_{n-1}\rangle \cdots |s_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{s=0}^{2^n-1} \Big(\prod_{k=0}^{n-1} \omega^{2^k s_k t} \Big) |s_{n-1}\rangle \cdots |s_0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{s=0}^{2^n-1} \Big(\bigotimes_{k=n-1}^{0} \omega^{2^k s_k t} |s_k\rangle \Big) = \bigotimes_{k=n-1}^{0} \frac{1}{\sqrt{2}} \big(|0\rangle + \omega^{2^k t} |1\rangle\big) = \bigotimes_{k=n-1}^{0} |\omega^{2^k t}\rangle
\end{aligned}$$

avec $s = \sum_{k=0}^{n-1} 2^k s_k$ et $|s\rangle = \bigotimes_{k=n-1}^{0} |s_k\rangle$, en notant $|\omega^u\rangle = \frac{1}{\sqrt{2}} \big(|0\rangle + \omega^u |1\rangle\big)$.

Cette formule mène à une réalisation de la QFT d'ordre 2^n avec un circuit à $n(n+1)/2$ portes, que nous détaillons plus bas pour $n = 4$.

Formulations covariante et contravariante

La formulation usuelle de la transformée de Fourier discrète (DFT) est contravariante : $y = Hx$, avec $x, y \in \mathbb{C}^d$. Celle de la QFT est plus naturellement covariante : à un élément d'une base, elle associe un élément d'une autre base : $f = eH$, ou de façon équivalente, elle associe une forme $\langle f|$ à une forme $\langle e|$, éléments de $\mathbb{C}^{*d}$. Avec la notation tensorielle pratiquée par les physiciens, on écrirait

$$y^s = \frac{1}{\sqrt{d}}\, \omega_t^s x^t \quad \text{(DFT)} \qquad \text{et} \qquad f_t = \frac{1}{\sqrt{d}}\, \omega_t^s e_s \quad \text{(QFT)}.$$

Cooley-Tukey quantique

On suppose $d = pq$, et que ω est une racine de l'unité d'ordre d. En posant $t = iq + j$, on peut décomposer un état $|x\rangle$ de $\mathbb{C}^d$ dans le produit tensoriel $\mathbb{C}^p \otimes \mathbb{C}^q$:

$$|x\rangle = \sum_{t=0}^{d-1} x_t |t\rangle = \sum_{i=0}^{p-1} \sum_{j=0}^{q-1} x_{iq+j} |i, j\rangle.$$

De même, en posant $s = k + \ell p$, on peut écrire $|s\rangle = |k, \ell\rangle \in \mathbb{C}^p \otimes \mathbb{C}^q$ et la matrice de Hadamard devient

$$\begin{aligned}
H_d &= \frac{1}{\sqrt{d}} \sum_{s,t=0}^{d-1} \omega^{st} |s\rangle\langle t| = \frac{1}{\sqrt{pq}} \sum_{k,i=0}^{p-1} \sum_{\ell,j=0}^{q-1} \omega^{(k+\ell p)(iq+j)} |k, \ell\rangle\langle i, j| \\
&= \frac{1}{\sqrt{pq}} \sum_{k,i=0}^{p-1} \sum_{\ell,j=0}^{q-1} (\omega^q)^{ki} (\omega^p)^{\ell j} \omega^{kj} |k, \ell\rangle\langle i, j| \\
&= \sum_{k,j=0}^{p-1,q-1} \omega^{kj} \Big(\frac{1}{\sqrt{p}} \sum_{i=0}^{p-1} (\omega^q)^{ki} |k\rangle\langle i| \Big) \otimes \Big(\frac{1}{\sqrt{q}} \sum_{\ell=0}^{q-1} (\omega^p)^{\ell j} |\ell\rangle\langle j| \Big).
\end{aligned}$$

On voit donc que la QFT d'ordre d s'exprime en combinant des QFT d'ordre p sur la partie gauche, des QFT d'ordre q sur la partie droite, et des *twiddle factors* ω^{kj}. Plus précisément :

$$\begin{aligned} H_d|x\rangle &= \frac{1}{\sqrt{pq}}\Big(\sum_{k,i=0}^{p-1}\sum_{\ell,j=0}^{q-1}(\omega^q)^{ki}(\omega^p)^{\ell j}\omega^{kj}|k,\ell\rangle\langle i,j|\Big)\sum_{i,j=0}^{p-1,q-1}x_{iq+j}|i,j\rangle \\ &= \frac{1}{\sqrt{q}}\sum_{\ell,j=0}^{q-1}(\omega^p)^{\ell j}\Big(\frac{1}{\sqrt{p}}\sum_{k=0}^{p-1}\Big[\sum_{i=0}^{p-1}(\omega^q)^{ki}x_{iq+j}\Big]\omega^{kj}|k\rangle\Big)|\ell\rangle. \end{aligned}$$

Implémentation pour $d = 16$

Ici, le ket $|t\rangle$, avec $t = (t_3, t_2, t_1, t_0)_2$, représente quatre qubits $|t_3\rangle \otimes |t_2\rangle \otimes |t_1\rangle \otimes |t_0\rangle$.

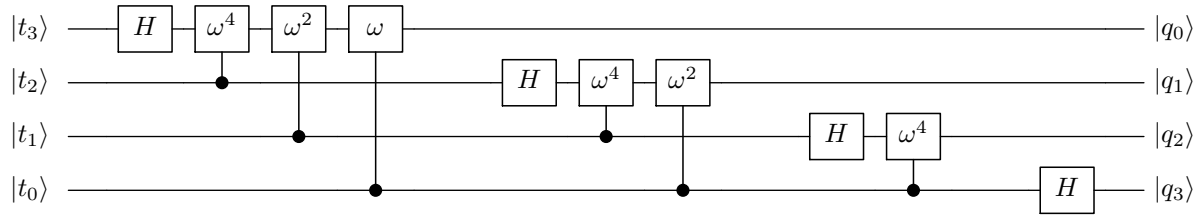
$$\begin{aligned} \mathsf{QFT}\,|t\rangle &= \frac{1}{4}\sum_{s=0}^{7}\omega^{st}|s\rangle \\ &= \frac{1}{\sqrt{2}}\big(|0\rangle + \omega^{8t}|1\rangle\big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + \omega^{4t}|1\rangle\big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + \omega^{2t}|1\rangle\big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + \omega^{t}|1\rangle\big) \\ &= |\omega^{8t}\rangle \otimes |\omega^{4t}\rangle \otimes |\omega^{2t}\rangle \otimes |\omega^{t}\rangle = |q_3\rangle \otimes |q_2\rangle \otimes |q_1\rangle \otimes |q_0\rangle. \end{aligned}$$

En particulier, on a

$$\begin{aligned} \mathsf{QFT}\,|0\rangle &= \frac{1}{4}\big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big) = |+\rangle|+\rangle|+\rangle|+\rangle \\ \mathsf{QFT}\,|8\rangle &= \frac{1}{4}\big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle - |1\rangle\big) = |+\rangle|+\rangle|+\rangle|-\rangle \\ \mathsf{QFT}\,|4\rangle &= \frac{1}{4}\big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle - |1\rangle\big) \otimes \big(|0\rangle + \omega^4|1\rangle\big) = |+\rangle|+\rangle|-\rangle|\omega^4\rangle \\ \mathsf{QFT}\,|2\rangle &= \frac{1}{4}\big(|0\rangle + |1\rangle\big) \otimes \big(|0\rangle - |1\rangle\big) \otimes \big(|0\rangle + \omega^4|1\rangle\big) \otimes \big(|0\rangle + \omega^2|1\rangle\big) = |+\rangle|-\rangle|\omega^4\rangle|\omega^2\rangle \\ \mathsf{QFT}\,|1\rangle &= \frac{1}{4}\big(|0\rangle - |1\rangle\big) \otimes \big(|0\rangle + \omega^4|1\rangle\big) \otimes \big(|0\rangle + \omega^2|1\rangle\big) \otimes \big(|0\rangle + \omega|1\rangle\big) = |-\rangle|\omega^4\rangle|\omega^2\rangle|\omega\rangle \end{aligned}$$

Cela s'implémente avec des portes de déphasage et de Hadamard :

$$[\omega] = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix} \qquad [\omega^2] = \begin{pmatrix} 1 & 0 \\ 0 & \omega^2 \end{pmatrix} \qquad [\omega^4] = \begin{pmatrix} 1 & 0 \\ 0 & \omega^4 \end{pmatrix} \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & \omega^8 \end{pmatrix}.$$



À noter que l'ordre des qubits de sortie est inversé par rapport à celui des qubits d'entrée.

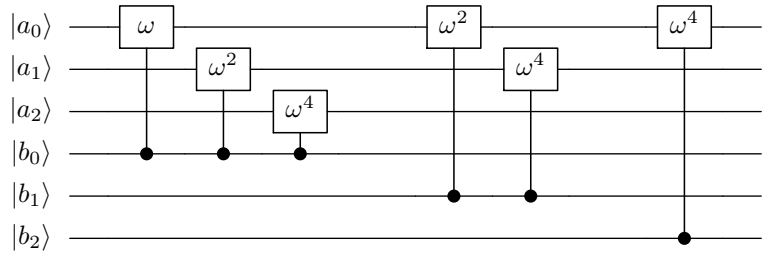
Arithmétique quantique

Soient $a = (a_{n-1}, \ldots, a_0)_2$ et $b = (b_{n-1}, \ldots, b_0)_2$ deux entiers représentables en binaire sur n digits. On peut les représenter sur un ordinateur quantique par les états :

$$|a\rangle = |a_0\rangle \otimes \cdots \otimes |a_{n-1}\rangle \qquad \text{et} \qquad |b\rangle = |b_0\rangle \otimes \cdots \otimes |b_{n-1}\rangle$$

de n qubits chacun.

Posons $\omega = \exp(2i\pi/2^n)$. Le circuit suivant (dessiné pour $n = 3$) :



où la porte de label ω^k représente $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \omega^k \end{smallmatrix}\right)$, implémente une porte C-Z généralisée :

$$|a\rangle \otimes |b\rangle \longmapsto \omega^{ab}|a\rangle \otimes |b\rangle.$$

Pour implémenter une addition (modulo 2^n), c'est-à-dire une porte C-X généralisée :

$$|a\rangle \otimes |b\rangle \longmapsto |a\rangle \otimes |a+b\rangle$$

on peut tirer parti de la transformée de Fourier (sur le deuxième registre) :

$$|a\rangle|b\rangle \overset{\mathsf{QFT}_2}{\longmapsto} \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{bk}|a\rangle|k\rangle \overset{\text{C-Z}}{\longmapsto} \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{(a+b)k}|a\rangle|k\rangle$$
$$\overset{\mathsf{QFT}_2^{-1}}{\longmapsto} \frac{1}{d} \sum_{k,\ell=0}^{d-1} \omega^{(a+b-\ell)k}|a\rangle|\ell\rangle = |a\rangle|a+b\rangle.$$

Cette méthode se généralise pour l'addition de $t > 2$ termes. Pour cela, il suffit d'utiliser successivement $t - 1$ portes C-Z généralisées. La QFT (directe et inverse) ne s'applique encore qu'à un seul registre, utilisé comme accumulateur. D'autre part, si on remplace ω par ω^γ dans la porte C-Z du circuit ci-dessus, on réalise le calcul de $\gamma a + b$. En particulier, pour $b = 0$, on réalise la multiplication par une constante γ. Enfin, la multiplication de a par b peut être traitée en multipliant a par chaque $2^i b_i$, où les b_i forment le développement binaire de b, et en additionnant les termes obtenus.

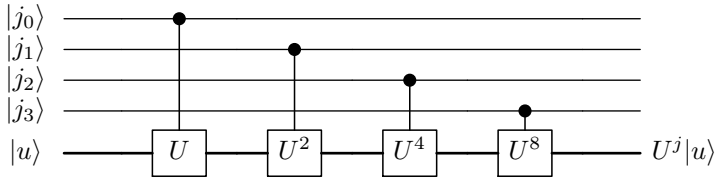
Estimation de phase

Soit U un opérateur quantique de vecteur propre $|u\rangle$ et de valeur propre $\theta = \exp(2i\pi\varphi)$, c'est-à-dire $U|u\rangle = \theta|u\rangle$. On peut expérimentalement obtenir une approximation de φ.

On utilise un registre de t qubits que l'on initialise tous dans l'état $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ (il suffit de partir de l'état $|0\rangle$ et d'appliquer une porte de Hadamard, décrite par la matrice $\frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$). On utilise aussi un système quantique dans l'état $|u\rangle$. L'état initial est alors

$$2^{-t/2} \sum_{j=0}^{2^t-1} |j\rangle \otimes |u\rangle.$$

On le fait parcourir un circuit implémentant les U^{2^i} contrôlés par chaque bit j_i de j :



On obtient alors

$$2^{-t/2}\sum_{j=0}^{2^t-1}|j\rangle\otimes U^j|u\rangle = 2^{-t/2}\sum_{j=0}^{2^t-1}\theta^j\,|j\rangle\otimes|u\rangle.$$

On applique alors une transformée de Fourier inverse d'ordre 2^t à la partie gauche pour obtenir (avec $\omega=\mathsf{exp}(2i\pi/2^t)$)

$$2^{-t}\sum_{j=0}^{2^t-1}\theta^j\sum_{k=0}^{2^t-1}\omega^{-kj}\,|k\rangle\otimes|u\rangle = 2^{-t}\sum_{k=0}^{2^t-1}\left(\sum_{j=0}^{2^t-1}\mathsf{exp}\left(2i\pi j(\varphi-k/2^t)\right)\right)|k\rangle\otimes|u\rangle.$$

Le coefficient de $|k\rangle\otimes|u\rangle$ est grand lorsque $k/2^t$ est proche de φ (modulo 1). Une mesure de (la partie gauche de) l'état obtenu permet d'obtenir ce tel k.

8. Supériorité quantique

Algorithme de Simon

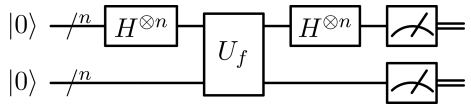
La supériorité du calcul quantique sur le calcul classique peut être constatée dans le cas du *problème de Simon*, pour lequel le gain quantique est exponentiel. Ce problème peut s'énoncer ainsi :

8.1. — Problème (Simon). Soit $f:\{0,1\}^n\to\{0,1\}^n$ une fonction booléenne admettant une unique période s :

$\exists! s\in\{0,1\}^n$ tel que, pour tous $x,y\in\{0,1\}^n$, on a $f(x)=f(y)$ si et seulement si $x=y$ ou $x\oplus s=y$.

Le problème est celui de déterminer s.

Résoudre ce problème par une méthode classique a nécessairement un coût en $O(2^{n/2})$ appels à l'oracle f. L'algorithme quantique de Simon est représenté par le circuit suivant qui utilise deux registres de n qubits chacun :



où le sous-circuit U_f réalise la transformation

$$U_f:\begin{cases}\mathbb{C}^{2^n}\otimes\mathbb{C}^{2^n}\longrightarrow\mathbb{C}^{2^n}\otimes\mathbb{C}^{2^n}\\ \quad|x\rangle\otimes|z\rangle\longmapsto|x\rangle\otimes|z\oplus f(x)\rangle\end{cases}$$

Les états quantiques obtenus aux différentes étapes de l'algorithme sont

$$|0^n\rangle\otimes|0^n\rangle\rightsquigarrow\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle\otimes|0^n\rangle\rightsquigarrow\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle\otimes|f(x)\rangle\rightsquigarrow\frac{1}{2^n}\sum_{x,y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle\otimes|f(x)\rangle.$$

À la dernière étape, le coefficient (amplitude) de $|y\rangle\otimes|f(x)\rangle$ est :

$$\frac{1}{2^n}\Big((-1)^{x\cdot y}+(-1)^{(x\oplus s)\cdot y}\Big)=\begin{cases}0 & \text{si } s\cdot y \text{ est impair,}\\ \pm1/2^{n-1} & \text{si } s\cdot y \text{ est pair.}\end{cases}$$

La mesure de $|y\rangle$ donne une issue y telle que $s\cdot y$ est pair (où $s\cdot y=\sum_{i=1}^n s_iy_i$). En utilisant ce circuit (environ) n fois, on obtient n contraintes linéaires, qui permettent de déterminer s. Le coût quantique est donc de $O(n)$ appels à l'oracle.

Détermination d'un réseau périodique

Soit $f : \{0,1\}^n \to \mathbb{Z}_N$ où le module N est un entier. L'ensemble des $z \in \mathbb{Z}^n$ qui sont des périodes de f forme un sous-groupe L de $\mathbb{Z}^n$. Une généralisation de l'algorithme de Simon permet de déterminer L (plus précisément une base du réseau dual L^*). En partant d'une superposition gaussienne approchée $\sum_{x\in\mathbb{Z}^n} \alpha_x|x\rangle$ avec α_x réels positifs tels que $\sum \alpha_x^2 = 1$, en appliquant U_f, puis une transformée de Fourier à gauche, on obtient

$$\frac{1}{\sqrt{N^n}} \sum_{x,y\in\mathbb{Z}^n} \alpha_x \omega^{x\cdot y}|y\rangle \otimes |f(x)\rangle \qquad \text{avec } \omega = \mathsf{exp}(2i\pi/N).$$

Lorsque $f(x) = f(x+s)$ c'est probablement que $s \in L$. Les termes $\alpha_x\omega^{x\cdot y}$ et $\alpha_{x+s}\omega^{(x+s)\cdot y}$ s'ajoutent lorsque $N \mid s\cdot y$. Une mesure de y donne donc (préférentiellement) un élément de L^*.

9. Factorisation

Le calcul quantique permet de factoriser les entiers en temps polymomial, grâce à l'algorithme de Shor. Rappelons que pour factoriser N, il suffit de savoir calculer l'ordre r d'un entier x modulo N car, en posant $r = 2^k q$ avec q impair, on peut trouver avec probabilité $\geqslant 1/2$ un i tel que $1 \leqslant i \leqslant k$ et

$$x^{2^i q} \equiv 1 \bmod N \qquad \text{mais} \quad x^{2^{i-1} q} \not\equiv \pm 1 \bmod N.$$

Calcul de l'ordre

On suppose x inversible modulo N (sinon, on sait factoriser N). On note encore r son ordre (inconnu), et n la longueur binaire de N. L'opération $|y\rangle \mapsto |xy \bmod N\rangle$ est une opération unitaire U_x sur n qubits (pour $y \geqslant N$, on pose $U_x|y\rangle = |y\rangle$). On peut la réaliser par un circuit quantique (c'est une permutation de la base canonique). On pose

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \theta^{-ks}\, |x^k \bmod N\rangle \qquad \text{où } \theta = \mathsf{exp}(2i\pi/r).$$

On a alors

$$\begin{aligned} U_x|u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \theta^{-ks}\, |x^{k+1} \bmod N\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{k=1}^{r} \theta^{-(k-1)s}\, |x^k \bmod N\rangle \\ &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \theta^{-(k-1)s}\, |x^k \bmod N\rangle \qquad \text{car } \theta^{-(r-1)s}|x^r \bmod N\rangle = \theta^s|1\rangle \\ &= \theta^s|u_s\rangle. \end{aligned}$$

Donc les $|u_s\rangle$ sont des vecteurs propres et leurs valeurs propres sont les θ^s.

On ne connaît pas les $|u_s\rangle$. Par contre, on a

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = \frac{1}{r} \sum_{k=0}^{r-1} \Big(\sum_{s=0}^{r-1} \theta^{-ks} \Big) |x^k \bmod N\rangle = |1\rangle.$$

La méthode de détermination de phase présentée plus tôt fonctionne encore (par linéarité) lorsque l'état $|u\rangle$ est une combinaison linéaire de vecteurs propres, mais il va approximer l'**une** des « phases » $\varphi_s = s/r$ de $\theta^s = \mathsf{exp}(2i\pi s/r)$.

On utilise pour cela un circuit à deux registres : un de longueur t (à ajuster en fonction de la précision souhaitée) et un de longueur n. On initialise le circuit dans l'état $|0\rangle^t \otimes |1\rangle$ (tous les qubits du circuit sont

à 0, sauf celui de poids faible dans le second registre, qui est à 1). Puis, avec des portes de Hadamard sur le premier registre, on fabrique l'état

$$2^{-t/2}\sum_{j=0}^{2^t-1}|j\rangle\otimes|1\rangle=\sqrt{\frac{2^{-t}}{r}}\sum_{j=0}^{2^t-1}\sum_{s=0}^{r-1}|j\rangle\otimes|u_s\rangle.$$

Avec des portes U_x controlées, on obtient alors

$$2^{-t/2}\sum_{j=0}^{2^t-1}|j\rangle\otimes|x^j \bmod N\rangle=\sqrt{\frac{2^{-t}}{r}}\sum_{j=0}^{2^t-1}\sum_{s=0}^{r-1}\theta^{js}|j\rangle\otimes|u_s\rangle.$$

Ensuite, la transformée de Fourier inverse d'ordre 2^t sur le registre de gauche permet d'obtenir

$$\frac{2^{-t}}{\sqrt{r}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^t-1}\sum_{k=0}^{2^t-1}\omega^{-kj}\theta^{js}|k\rangle\otimes|u_s\rangle=\frac{2^{-t}}{\sqrt{r}}\sum_{s=0}^{r-1}\sum_{k=0}^{2^t-1}\sum_{j=0}^{2^t-1}\exp\left(2ij\pi\left(\frac{s}{r}-\frac{k}{2^t}\right)\right)|k\rangle\otimes|u_s\rangle.$$

Par une mesure de ce registre, on obtient avec grande probabilité un entier k tel que $\left|\frac{k}{2^t}-\frac{s}{r}\right|\leqslant\frac{1}{2^{t+1}}$. Si $2^t\geqslant N^2\geqslant r^2$ alors,

$$\left|\tfrac{k}{2^t}-\tfrac{s}{r}\right|\leqslant\frac{1}{2^{t+1}}\leqslant\frac{1}{2r^2}.$$

Le développement de $k/2^t$ en fraction continue va nous donner s/r (en fraction réduite ; on obtient donc r ou un de ses diviseurs).

La condition $2^t\geqslant r^2$ est obtenue avec $t\geqslant 2n$. L'étape QFT a donc un coût en $O(n^2)$. L'étape consistant à appliquer U_x^j est coûteuse. Avec l'algorithme de multiplication standard, son coût est celui de n portes contrôlées de multiplication, c'est-à-dire $O(n^3)=O(\ln^3 N)$. Le coût de l'algorithme complet est alors celui de cette étape dominante. Mais en basant la multiplication sur QFT, on réduit le coût de l'algorithme de Shor à $O\big((\ln N)^2(\ln\ln N)(\ln\ln\ln N)\big)$.

10. Algorithme de Grover

On recherche dans une base de données un élément w satisfaisant une contrainte, exprimée par une fonction booléenne f :

$$f(w)=1\qquad\text{mais } f(x)=0 \text{ pour tout } x\neq w.$$

On suppose que le domaine des clés x est l'ensemble des entiers de 0 à 2^n-1, ou plutôt l'ensemble $\mathcal{X}$ de leurs développements binaires (les chaînes binaires de longueur n).

Une telle recherche par un algorithme classique a un coût moyen d'environ 2^{n-1} appels à l'oracle f. L'algorithme quantique de Grover va permettre de réaliser cette recherche avec un coût en $O(\sqrt{2^n})$.

Notons $\mathcal{H}(\mathcal{X})$ l'espace de n qubits, engendré par les $|x\rangle$, pour $x\in\mathcal{X}$. On commence par implémenter (avec un circuit essentiellement composé de portes X multi-controlées) l'opérateur U_f (sur $n+1$ qubits) :

$$U_f:\mathcal{H}(\mathcal{X})\otimes\mathbb{C}^2\ni|x\rangle\otimes|y\rangle\longmapsto|x\rangle\otimes|y\oplus f(x)\rangle.$$

La restriction de U_f aux états de la forme $|x\rangle\otimes|-\rangle$ peut alors s'exprimer simplement par (le deuxième facteur étant invariant) :

$$V_f|x\rangle=(-1)^{f(x)}|x\rangle\qquad\text{pour } x\in\mathcal{X}.$$

L'opérateur V_f est donc la symétrie orthogonale par rapport à l'hyperplan orthogonal à $|w\rangle$.

On implémente aussi la symétrie orthogonale $S=I-2|s^\perp\rangle\langle s^\perp|$, définie sur $\mathcal{H}(\mathcal{X})$ par rapport à la droite engendrée par $|s\rangle=|+\rangle^{\otimes n}$. Restreintes au plan engendré par $|s\rangle$ et $|w\rangle$, les applications V_f et S sont des symétries par rapport aux droites respectivement engendrées par $|w^\perp\rangle$ et par $|s\rangle$. Comme $\langle w\,|\,s\rangle=1/\sqrt{2^n}$,

$|w\rangle$ et $|s\rangle$ sont quasiment orthogonaux, et l'angle θ entre $|w^\perp\rangle$ et $|s\rangle$ est très proche de $\sin\theta = 1/\sqrt{2^n}$. Le produit SV_f est alors une rotation d'angle 2θ.

On part donc de l'état $|s\rangle$ et on applique k fois SV_f (ou bien de $|s\rangle \otimes |-\rangle$ et on applique k fois SU_f). L'angle entre le vecteur $|s'\rangle$ obtenu et $|w^\perp\rangle$ est alors $(2k+1)\theta$. Pour $k \simeq \sqrt{2^n}\pi/4$, l'angle obtenu est proche de $\pi/2$, ce qui signifie que $|s'\rangle$ est très proche de l'état $|w\rangle$ de la base canonique. Une mesure dans cette base permet donc d'obtenir w avec très grande probabilité.

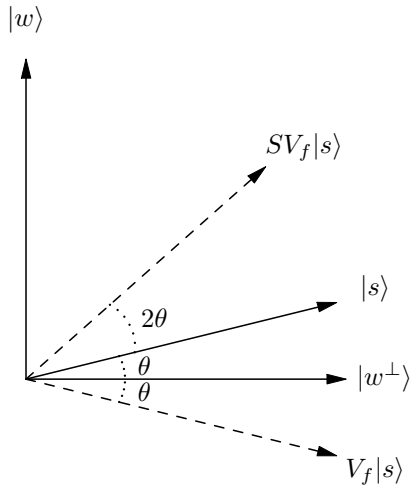


Figure 2. Géométrie de l'algorithme de Grover