CHAPITRE

10 Information quantique

« Je crois pouvoir dire sans risque de me tromper que personne ne comprend la mécanique quantique. »

— Richard Feynman

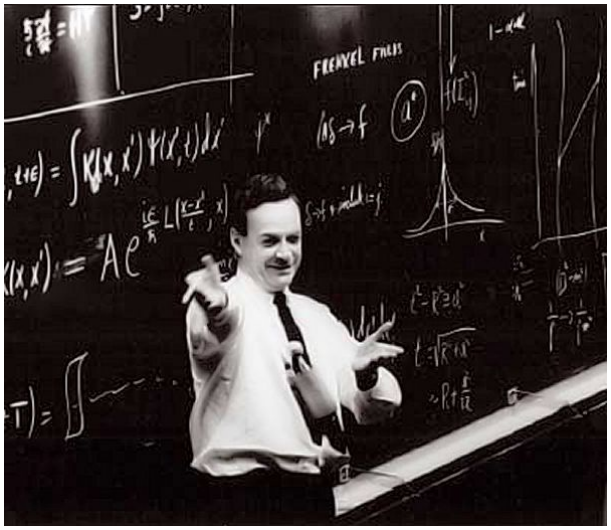

FIGURE 10.1 – Richard Feynman, ici en 1965 après avoir reçu son prix Nobel, est l'un des pères fondateurs de la théorie des ordinateurs quantiques (source © IOP, Cern).

Sommaire

10.1 Introduction **204**
10.2 Préliminaires **205**
10.3 Sur les inégalités de Bell **223**
10.4 Téléportation **229**
10.5 Jeu CHSH **230**
10.6 Jeu GHZ **237**
10.7 Le modèle φ-LOCAL **239**

Bibliographie 242

L'objectif de ce chapitre est de donner quelques intuitions sur l'information quantique, même si l'intuition est *a priori* difficile à percevoir, de montrer comment exploiter la non localité de l'information dans le monde quantique. Nous montrerons la différence subtile qu'il existe en calcul distribué entre des ressources aléatoires partagées (*shared randomness*) et des ressources quantiques intriqués (*entangled qubits*).

Mots clés et notions abordées dans ce chapitre :

- principe de causalité, principe de localité
- qubits, superposition, intrication, notation de Dirac
- expérience de Bell, jeu CHSH, jeu GHZ

Notons aussi qu'il existe des tentative de langages dédiés au calcul quantique, comme QCL (Quantum Computation Language [1]), dont on ne parlera pas.

10.1 Introduction

Ils existent deux principes fondamentaux en physique :

- le principe de *causalité*, et
- le principe de *localité*.

Le principe de causalité exprime le fait que la cause précède toujours la conséquence. Un événement ne peut avoir de conséquences que sur des événements futurs. En terme de calcul, cela signifie aussi que le résultat d'un calcul ne peut dépendre que de données déterminées avant le résultat. (Pour calculer $y := f(x)$, il faut que la donnée x soit déterminée. Le calcul de y ne peut pas déterminer x.)

Le principe de localité (parfois appelé principe de séparabilité) exprime le fait que des entités suffisamment éloignées (dans le temps et l'espace) ne peuvent interagir instantanément.

Des expériences reproductibles ont montré que ces deux principes fondamentaux ne peuvent être vrais tous les deux. Plus précisément, Alain Aspects a montré expérimentalement en 1982 que les inégalités de Bell étaient violées, ce qui implique la non localité de la physique quantique en supposant vrai le principe de causalité. Ce fait est utilisé dans certains protocoles de cryptographie quantique où la lecture d'un message par un espion est détectée par le fait que ces inégalités ne sont plus violées une fois les effets quantiques dissipés. Car l'acquisition d'information, comme la lecture, dissipe par nature les effets de superposition quantique.

La réalité physique du monde est donc différente de ce qu'on s'imagine *a priori*, tout au moins à l'échelle microscopique. Ces effets ont été vérifiés pour les particules élé-

1. http://tph.tuwien.ac.at/~oemer/qcl.html

mentaires (photons, électrons) mais aussi pour des atomes et même pour des molécules de plus en plus complexes [2]

La physique quantique manipule des états (ou particules quantiques) qui remettent en cause *a priori* le principe de localité, car des deux principes fondamentaux on s'accorde plutôt pour penser que c'est celui de causalité qui est vrai, c'est-à-dire celui qui est le plus en accord avec le monde réel. Des travaux récents en physique mathématique [DHFRW20] tendent à montrer que les *ensembles causaux* [3] pourrait être une base solide et plus fondamentale à la fois pour la physique quantique et la théorie de la gravitation.

Concernant l'information, remettre en cause la localité signifie qu'un bit d'information n'est pas forcément localisé en un lieu bien déterminé (sur une particule par exemple), mais peut être en même temps dans plusieurs endroit à la fois. C'est ce genre de propriété que l'on tente d'exploiter dans le calcul distribué quantique.

Contrairement à la théorie de la relativité, la physique quantique ne se déduit pas de manière logique à partir d'axiomes évidents ou faciles à admettre, comme par exemple le principe d'invariance (les lois sont les mêmes quel que soit le repère) et de causalité. D'ailleurs de ces deux principes on peut en déduire qu'il existe une vitesse limite c pour la propagation des ondes électromagnétiques. Du coup, la façon d'aborder la physique quantique est différente et moins intuitive. Comme Richard Feymann aimait à le dire « [...] personne ne comprend la mécanique quantique. »

10.2 Préliminaires

10.2.1 Information élémentaire

On pourra aussi se reporter aux articles [BCMdW10][RP00]. En première approximation un bit quantique, ou qubit, est une extension du bit probabiliste. Il est donc important de bien comprendre en premier lieu ce qu'est un bit classique déterministe, puis un bit probabiliste.

Bit déterministe B : représenté par une valeur $B \in \{0, 1\}$.

Bit probabiliste P : représenté par un vecteur P de deux réels $\begin{pmatrix} p \\ q \end{pmatrix}$ où p représente la probabilité d'obtenir la valeur 0 et q celle d'obtenir 1. Bien sûr pour être des probabilités, il faut avoir $0 \leqslant p, q \leqslant 1$ et $p + q = 1$.

2. Le record (fin 2019) est une molécule de 2 000 atomes observée en état de superposition en observant des franges d'interférence [FGZ+19].

3. En gros, ils s'agit de graphes orientés où les arcs correspondent aux liens de causalité. Émergent alors les notions de positions, d'espace, de temps (local), de gravité, de champs quantique... Je vous conseille vivement la vidéo de Passe-science #20 (causal sets) sur ce sujet.

En notant la valeur 0 par le vecteur $\begin{pmatrix}1\\0\end{pmatrix}$ et la valeur 1 par le vecteur $\begin{pmatrix}0\\1\end{pmatrix}$, on peut aussi représenter le bit probabiliste P comme une somme vectorielle des vecteurs de base :

$$P \;=\; p\begin{pmatrix}1\\0\end{pmatrix} + q\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}p\\q\end{pmatrix}.$$

Cette représentation arbitraire à juste pour vocation de donner un cadre plus formelle qui va se généraliser aux bits quantiques. C'est une façon de préparer le terrain.

Bit quantique (ou qubit) Q : representé par un vecteur Q de deux complexes $\begin{pmatrix}\alpha\\\beta\end{pmatrix}$ où $|\alpha|^2$ représente la probabilité d'observer 0 et $|\beta|^2$ celle d'observer 1. Bien sûr, comme le bit probabiliste il faut $|\alpha|^2 + |\beta|^2 = 1$.

On parle d'*état* $\begin{pmatrix}\alpha\\\beta\end{pmatrix}$ pour un qubit Q, puisque les nombres α, β ne sont pas à proprement parler des probabilités. On garde le terme de *probabilités* pour un bit probabiliste P et de *valeur* pour le bit déterministe B.

Pour récupérer l'information « utile » d'un bit B, P ou Q, il faut faire :

- une *lecture* de sa valeur pour B ;
- un *tirage* aléatoire pour P ;
- une *mesure* de l'état pour Q (voir le paragraphe 10.2.6).

La présence de nombres complexes pour décrire l'état d'un qubit Q s'explique par la nature ondulatoire des particules quantiques. Chaque coefficient α ou β représente l'amplitude et la phase d'une onde qui est de manière générale un nombre complexe selon la théorie ondulatoire classique[4]. La probabilité est proportionnelle à l'intensité de l'onde (disons lumineuse) observée/mesurée (disons sur un écran). Et dans la théorie ondulatoire l'intensité (ou taux d'énergie) n'est rien d'autre que le carré du module de l'amplitude.

Comme précédemment, en notant la valeur 0 par le vecteur $\begin{pmatrix}1\\0\end{pmatrix}$ et la valeur 1 par le vecteur $\begin{pmatrix}0\\1\end{pmatrix}$, on peut aussi représenter le bit quantique Q comme une somme vectorielle des vecteurs de base :

$$Q \;=\; \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha\\\beta\end{pmatrix}.$$

On rappelle que $|z|$ représente le module du complexe $z \in \mathbb{C}$. Si $z = x + iy$ alors son module z est $|z| = \sqrt{x^2 + y^2}$ et $z = |z| \cdot (\cos\varphi + i \sin\varphi)$ où $\varphi = \arg(z)$ est l'argument de z. La formule de De Moivre énonce que $\cos\varphi + i\sin\varphi = e^{i\varphi}$.

4. Pour faire simple, une onde transporte de l'énergie sans transporter de matière. C'est une perturbation locale et réversible du milieu physique.

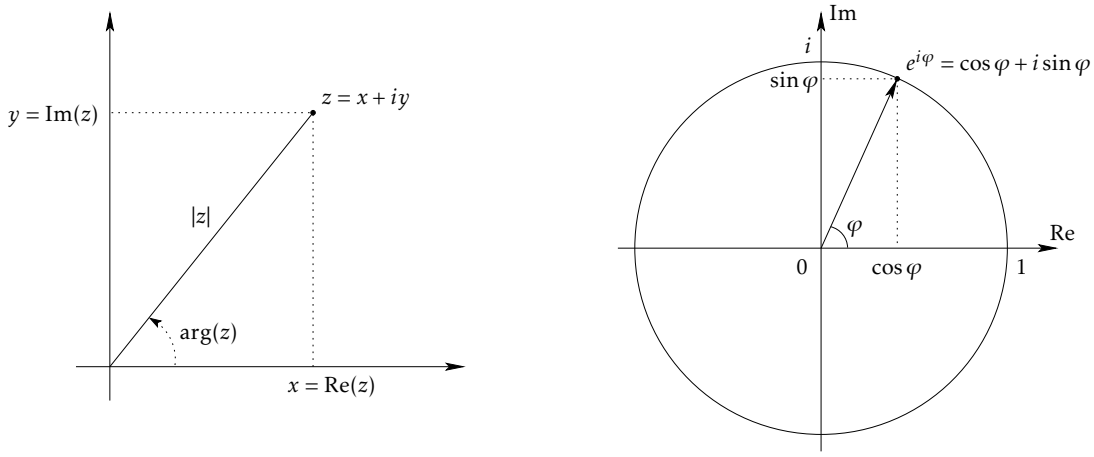

FIGURE 10.2 – Interprétation géométrique d'un nombre complexe $z \in \mathbb{C}$.

Un qubit est implémenté par une particule physique [5] : un photon, un électron, un atome. La mesure d'un qubit correspond, par exemple, à la mesure de la polarisation d'un photon, le spin [6] d'un électron ou le niveau d'énergie d'un atome. Polarisation, spin ou énergie, mais aussi position, vitesse ou impulsion [7], est ce qui s'appelle un *observable*.

Généralement ces particules sont refroidies par laser afin de contrôler et limiter leurs interactions avec l'environnement. Car dès qu'une particule interagit avec l'environnement, l'état du système ⟨particule,environnement⟩ change, en particulier l'état de la particule. Par exemple observer la position d'une particule modifie non seulement l'état de l'observateur (qui sait maintenant où elle se situe) mais aussi celui de la particule observée (par exemple en modifiant sa position ou sa vitesse).

Le formalisme mathématique de la théorie quantique n'a pour vocation que de prédire les états quantiques et de calculer les probabilités d'obtenir tels ou tels résultats. Le point est que jusqu'à présent, les prédictions selon cette théorie (et donc des calculs de probabilités qui en découlent) se sont toujours révélées exactes.

La théorie quantique affirme (c'est en fait l'un de ses axiomes) que des états colinéaires (plus précisément des états dont les vecteurs d'ondes sont colinéaires [8]) sont

5. De même qu'un bit a un support physique : le transistor.

6. Chaque particule possède un *spin* qui est un peu son moment magnétique, comme si la particule était un petit aimant tournant sur lui-même (ce qu'elle ne fait pas). Malheureusement, cette propriété n'a pas d'équivalent dans le monde classique, contrairement aux propriétés comme la charge électrique, la masse, la position, la vitesse, etc. Son intérêt est qu'elle est quantifiée (prend des valeurs discrètes) et facilement observable. Pour la mesurer on fait passer un jet de particules semblables horizontalement à travers un champs magnétique perpendiculaire et chaque particule est alors déviée aléatoirement vers le haut (+1) ou vers le bas (-1) exactement du même angle.

7. C'est une notion proche de celle de quantité de mouvement, soit le produit de la masse par la vitesse.

8. On parle de vecteurs colinéaires $\vec{u}, \vec{v} \in \mathbb{C}^2$, c'est-à-dire tels qu'il existe $\lambda \in \mathbb{C}^*$ avec $\vec{u} = \lambda \cdot \vec{v}$.

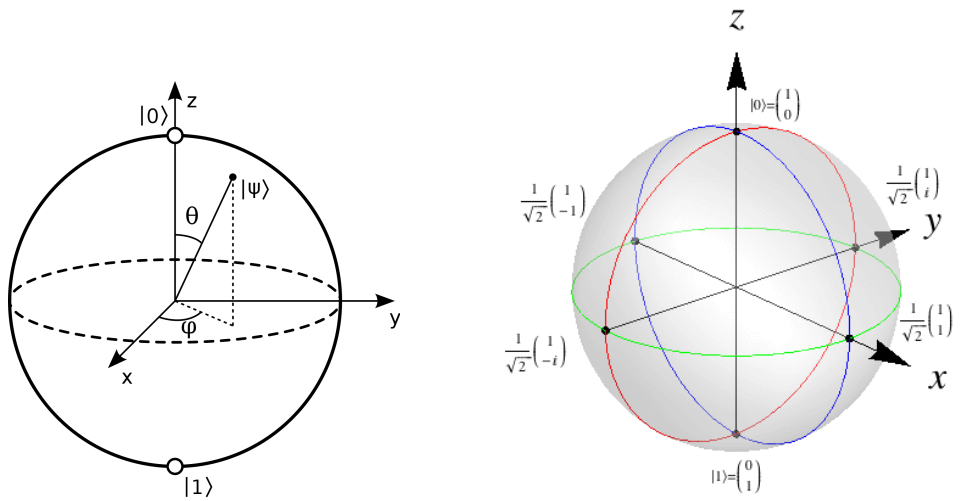

FIGURE 10.3 – Sphère de Bloch : un point de la sphère représente l'état quantique d'une particule.

indiscernables – les projections lors des mesures seront les mêmes. Du coup, l'état d'un qubit est bien un point de la surface unité d'une sphère : les coefficients complexes α, β nous donnent *a priori* 4 degrés de liberté ; la condition $|\alpha|^2 + |\beta|^2 = 1$ fait que le qubit évolue dans un espace isomorphe à $\mathbb{R}^3$; et finalement la co-linéarité fait qu'on peut normaliser les vecteurs à l'unité. D'où la sphère unité de $\mathbb{R}^3$ comme sur la figure 10.3.

10.2.2 Superposition, interférence et décohérence

La *superposition* exprime le fait qu'un qubit peut être dans la superposition de plusieurs états. On l'exprime formellement en écrivant que l'état d'un qubit Q vaut :

$$Q = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Dans le monde physique, cela traduit la dualité onde-corpusculaire. Par exemple, un photon individuel va passer par les deux fentes de Young et les probabilités d'observer un résultat sur l'écran vont dépendre des longueurs des deux chemins utilisés avec un effet constructif ou destructif comme une onde (voir la figure 10.4(c)). Le photon est alors dans un état dit de *superposition*. Il passe réellement par les deux fentes à la fois, comme le ferai une onde. Quant au résultat observé, c'est comme si le photon interfèrerait avec lui-même par recombinaison. D'un autre coté on n'observe jamais un photon à deux endroits à la fois.

Il est important de noter que ce phénomène d'*interférence* se produit pour *une seule* particule. Ce n'est pas un phénomène lié à un flux de particules. Cela a été testé physiquement pour des photons individuels par Alain Aspect dans les années 1980, puis sur

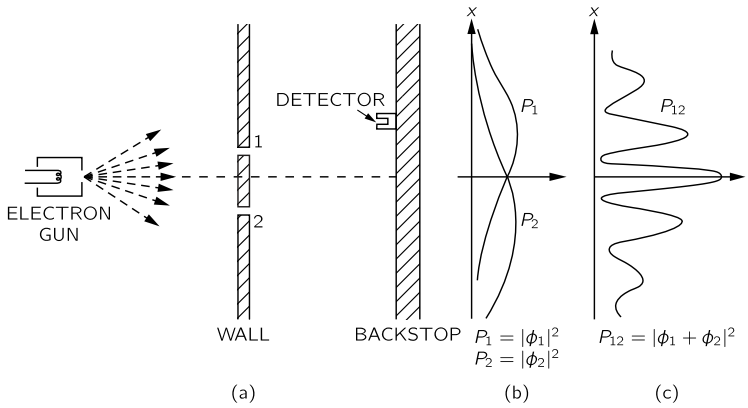

FIGURE 10.4 – Le détecteur permet de capter ou non un électron individuel à une position déterminée (axe x). Pour obtenir la distribution P_1 par exemple (fente 1 ouverte), il faut déplacer uniformément le détecteur et compter. La ditribution P_{12} est celle observée lorsque les fentes 1 et 2 sont ouvertes simultanément. Extrait des cours de Richard Feymann (caltech.edu).

des électrons, protons, neutrons et même des atomes et plus récemment des molécules. C'est bien une seule particule qui passe par les deux fentes à la fois.

Si l'on obstrue une des deux fentes (figure 10.4(b)), la distribution devient quasiment uniforme sur l'écran : on observe une tâche diffuse. Après l'observation, l'état de superposition est détruit, car dans la réalité telle qu'on la conçoit on observe jamais le même photon à deux endroits à la fois.

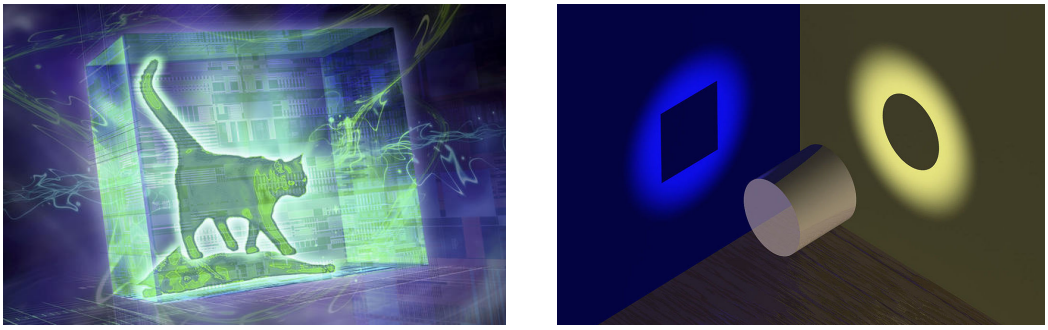

FIGURE 10.5 – Illustration du phénomène de superposition par le Chat de Schrödinger (source © H. Ritsch/Science Photo Library), et la métaphore du cylindre (source Wikipédia).

La métaphore du cylindre (voir figure 10.5) est l'exemple d'un objet ayant des propriétés (comme être un cercle ou un carré) apparemment inconciliables. Mais une projection peut nous faire apparaître l'une ou l'autre de ces propriétés. Pour une particule dans un état quantique c'est la même chose : onde et particule sont deux facettes (ob-

servations) d'une même réalité mais pas la réalité elle-même. Notons que la notion de *mesure* d'un état quantique revient à faire aussi une projection (cf. paragraphe 10.2.6). Voir aussi l'extrait de la BD sur la figure 10.6.

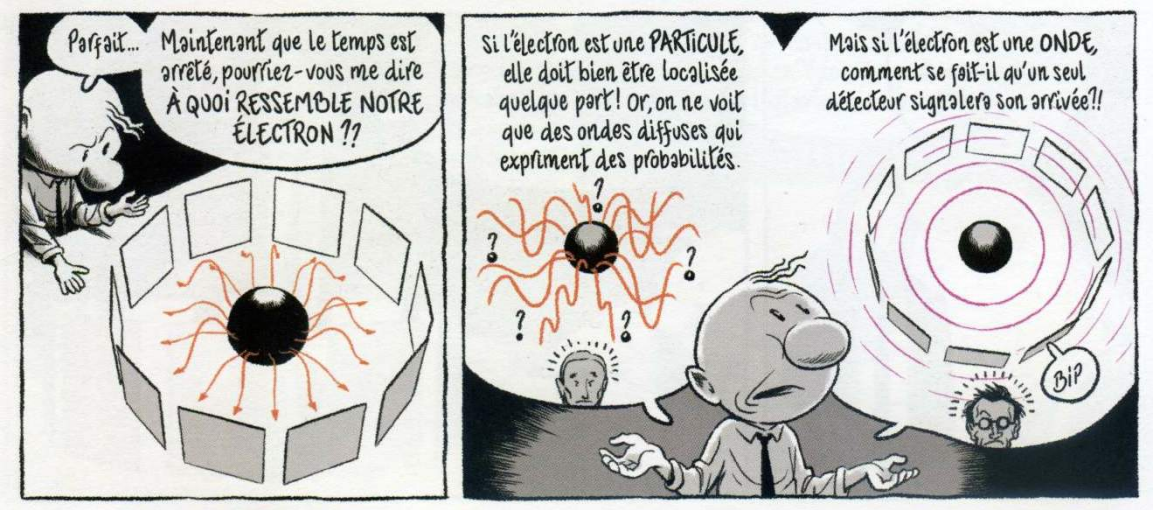

FIGURE 10.6 – « Le Mystère du Monde Quantique » par T. Damour et M. Burniat © Dargaud 2016.

La *décohérence* est le fait une particule dans un état de superposition va au bout d'un moment devenir une simple particule probabiliste à cause des interaction avec l'extérieur au système. Dans l'expérience de Young, si le photon interagit avec les atomes près d'un des deux parcours possibles, alors le choix de la trajectoire devient simplement aléatoire et plus superposé.

10.2.3 Système à plusieurs qubits

Pour l'instant il n'y a pas de différence fondamentale entre un bit probabiliste $P = p\begin{pmatrix}1\\0\end{pmatrix}+q\begin{pmatrix}0\\1\end{pmatrix}$ et un qubit $Q = \alpha\begin{pmatrix}1\\0\end{pmatrix}+\beta\begin{pmatrix}0\\1\end{pmatrix}$ hormis que α, β peuvent être complexes. Dans les deux cas, les coefficients donnent la probabilité d'observer 0 (p ou $|\alpha|^2$) et la probabilité d'observer 1 (q ou $|\beta|^2$). Il va en être autrement lorsqu'on considère des systèmes de plusieurs bits et qubits.

En déterministe un système composé d'une paire de valeurs v_1, v_2 se représente tout simplement par un couple (v_1, v_2), un vecteur ligne $(\,v_1\ v_2\,)$ ou encore un vecteur colonne ${}^t(\,v_1\ v_2\,) = \begin{pmatrix}v_1\\v_2\end{pmatrix}$.

On pourrait représenter deux bits probabilistes (P_1, P_2) par un couple de vecteurs ou

encore un vecteur colonne à quatre composantes :

$$(P_1, P_2) = \left(\begin{pmatrix} p_1 \\ q_1 \end{pmatrix}, \begin{pmatrix} p_2 \\ q_2 \end{pmatrix}\right) \quad \text{ou} \quad \begin{pmatrix} p_1 \\ q_1 \\ p_2 \\ q_2 \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} p_1 p_2 \\ p_1 q_2 \\ q_1 p_2 \\ q_1 q_2 \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}$$

Ces représentations sont en fait toutes équivalentes, ce qui nécessite un effort de vérification pour la dernière. En utilisant le fait que $p_1 + q_1 = 1$ et que $a/c = p_1/q_1$, on déduit que $p_1 = a/(a+c)$ et $q_1 = c/(c+a)$. De la même manière, $p_2 + q_2 = 1$ et $a/b = p_2/q_2$ impliquent que $p_2 = a/(a+b)$ et $q_2 = b/(b+a)$. On peut donc facilement passer d'une représentation à n'importe qu'elle autre.

La dernière représentation a l'avantage de donner les probabilités d'obtenir chacune des quatre paires de valeurs $(0,0)$, $(0,1)$, $(1,0)$ et $(1,1)$. De plus elle correspond à un produit *tensoriel*, opération vectorielle notée $\otimes$, appelé aussi *produit de Kronecker*. De manière générale, si $A = (a_{i,j})$ et B sont deux matrices de dimensions respectives $r_A \times s_A$ et $r_B \times s_B$, alors $A \otimes B = (a_{i,j}B)$ est une matrice $r_A r_B \times s_A s_B$.

Ainsi,

$$\begin{pmatrix} p_1 \\ q_1 \end{pmatrix} \otimes \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} = \begin{pmatrix} p_1 \cdot \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} \\ q_1 \cdot \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} p_1 p_2 \\ p_1 q_2 \\ q_1 p_2 \\ q_1 q_2 \end{pmatrix}.$$

Notez en passant que ce produit n'est pas commutatif en général, car par exemple si $p_2 q_1 \neq p_1 q_2$, alors

$$\begin{pmatrix} p_2 \\ q_2 \end{pmatrix} \otimes \begin{pmatrix} p_1 \\ q_1 \end{pmatrix} = \begin{pmatrix} p_2 p_1 \\ \boxed{p_2 q_1} \\ q_2 p_1 \\ q_2 q_1 \end{pmatrix} \neq \begin{pmatrix} p_1 p_2 \\ \boxed{p_1 q_2} \\ q_1 p_2 \\ q_1 q_2 \end{pmatrix} = \begin{pmatrix} p_1 \\ q_1 \end{pmatrix} \otimes \begin{pmatrix} p_2 \\ q_2 \end{pmatrix}.$$

On remarque que ce produit tensoriel se décompose en une combinaison linéaire de quatre vecteurs unitaires coefficientés par les probabilités d'obtenir les valeurs $(0,0)$, $(0,1)$, $(1,0)$ et $(1,1)$.

$$\begin{pmatrix} p_1 \\ q_1 \end{pmatrix} \otimes \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} = \begin{pmatrix} p_1 p_2 \\ p_1 q_2 \\ q_1 p_2 \\ q_1 q_2 \end{pmatrix} = p_1 p_2 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + p_1 q_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + q_1 p_2 \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + q_1 q_2 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

D'ailleurs on vérifie que la somme $p_1 p_2 + p_1 q_2 + q_1 p_2 + q_1 q_2 = (p_1 + q_1)(p_2 + q_2) = 1$ puisque $p_1 + q_1 = p_2 + q_2 = 1$. Ainsi le produit tensoriel permet une simple généralisation du bit probabiliste $P = \begin{pmatrix} p \\ q \end{pmatrix} = p \begin{pmatrix} 1 \\ 0 \end{pmatrix} + q \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ a un système qui se décomposent en une somme de vecteur unitaires coefficientés par des probabilités.

De même, un système (A,B) composé de deux qubits A et B se représentera comme une combinaison linéaire des 4 vecteurs unitaires

$$(A,B) = \begin{pmatrix} c_{00} \\ c_{01} \\ c_{10} \\ c_{11} \end{pmatrix} = c_{00}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + c_{01}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + c_{10}\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + c_{11}\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

avec $c_{ij} \in \mathbb{C}$ et $\sum_{ij} |c_{ij}|^2 = 1$, la probabilité d'observer $A = i \in \{0,1\}$ et $B = j \in \{0,1\}$ étant contrôlée par $|c_{ij}|^2$. Pour un système à 3 qubits, on aurait une description décrivant la combinaison linéaire des 8 vecteurs de base (soit une superposition)

$$(A,B,C) = \begin{pmatrix} c_{000} \\ c_{001} \\ c_{010} \\ c_{011} \\ c_{100} \\ c_{101} \\ c_{110} \\ c_{111} \end{pmatrix} = c_{000}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + c_{001}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \cdots + c_{110}\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + c_{111}\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

L'état du système (A,B,C) donné par l'equation précédente est déterminé par les coefficients (*a priori* complexes) $c_{000},\ldots,c_{111}$. Si l'on fait une mesure sur chacun des trois qubits (mesure simultanée ou pas), la probabilité d'observer par exemple $A = 1$, $B = 0$ et $C = 1$ sera $|c_{101}|^2$.

Plus généralement l'état d'un système à n qubits se décrit comme la combinaison linéaire de 2^n vecteurs de taille 2^n. De même pour un système de n bits probabilistes. Bien sûr, si certains bits sont indépendants, ce n'est pas la façon la plus compacte de faire. S'ils sont tous indépendants par exemple, alors la suite $p_1,\ldots,p_n$ des probabilités suffit à décrire le système.

10.2.4 Intrication

Le point important est qu'on peut avoir des systèmes à $n > 1$ qubits qui sont dans des états qui ne peuvent correspondre à aucun produit tensoriel. On parle d'états non séparables ou *intriqués*. Inversement on dira que l'état (A,B) d'un système est *séparable* si $(A,B) = A \otimes B$ ce qui revient à dire que le système est composé de deux sous-systèmes indépendants. Deux particules intriquées forment donc un système unique, solidaire, inséparable (cf. figure 10.7).

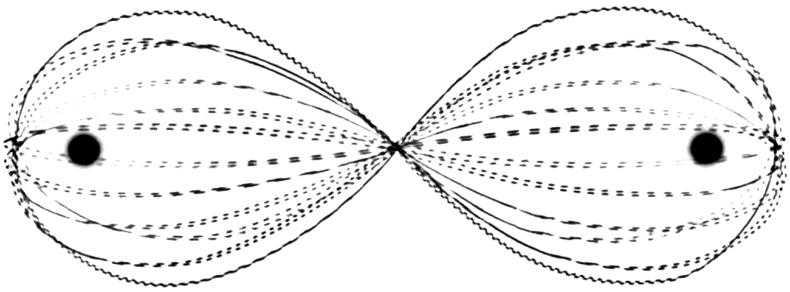

FIGURE 10.7 – Illustration d'un système de deux particules intriquées.

Par exemple prenons un système (A, B) de deux qubits défini [9] par :

$$(A,B) \;=\; \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Cet état signifie que la probabilité d'obtenir $(0,0)$ est $|1/\sqrt{2}|^2 = 1/2 = 50\%$, soit la même que d'obtenir $(1,1)$. Il n'est pas possible d'obtenir $(1,0)$ ou $(0,1)$. Le résultat de la mesure des qubits A et B est bien aléatoire mais corrélé.

Ce système n'est pas séparable. S'il l'était alors on aurait :

$$(A,B) = \begin{pmatrix}\alpha_0\\\beta_0\end{pmatrix} \otimes \begin{pmatrix}\alpha_1\\\beta_1\end{pmatrix} \quad \Rightarrow \quad (A,B) = \alpha_0\alpha_1\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \beta_0\alpha_1\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + \alpha_0\beta_1\begin{pmatrix}0\\0\\1\\0\end{pmatrix} + \beta_0\beta_1\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

pour $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{C}$ à déterminer. Or il faut $\alpha_0\alpha_1 = \beta_0\beta_1 = 1/\sqrt{2} \neq 0$ et $\beta_0\alpha_1 = \alpha_0\beta_1 = 0$, ce qui n'est pas possible, même dans $\mathbb{C}$.

Remarques. Pour générer un système de qubits intriqués, les particules support doivent préalablement interagir. En pratique on peut récupérer deux photons issus d'une même « cascade atomique », comme l'a fait Alain Aspect dans sa célèbre expérience. On excite un atome, par exemple de calcium, à un niveau d'énergie élevé avec un laser. Lorsque les électrons reviennent au niveau fondamental, en passant par un niveau d'énergie intermédiaire, deux photons intriqués sont émis (un pour chaque niveau). Leur polarisation est alors corrélées et on peut leur faire prendre des directions différentes et contrôlées (voir [Teo16]). Un même système peut avoir une propriété en état d'intrication

9. On aurait pu prendre un système $(P_1, P_2) = {}^t(p_1p_2, 0, 0, q_1q_2)$ de deux bits probabilistes corrélés. La non séparabilité n'est pas le propre de la mécanique quantique.

(ici la polarisation) et une autre dans un état classique (ici la position). Il se trouve aussi que les deux électrons de l'atome d'hélium sont toujours dans un état intriqué. De manière générale, deux éléments quantiques indiscernables ou issus d'un même processus sont intriqués tant que les éléments n'ont pas subi de mesure qui détruit l'état quantique. Par exemple, un photon qui passe à travers un cristal non linéaire va être coupé en deux photons intriqués (voir figure 10.8).

La propriété d'intrication a été vérifiée, non seulement pour des systèmes de deux particules, mais aussi des systèmes de deux objets macroscopiques (faisceaux de silicium de la taille d'une bactérie) d'une dizaine de milliards d'atomes et espacés de 20 cm, l'effet pouvant être maintenu pendant plusieurs minutes.

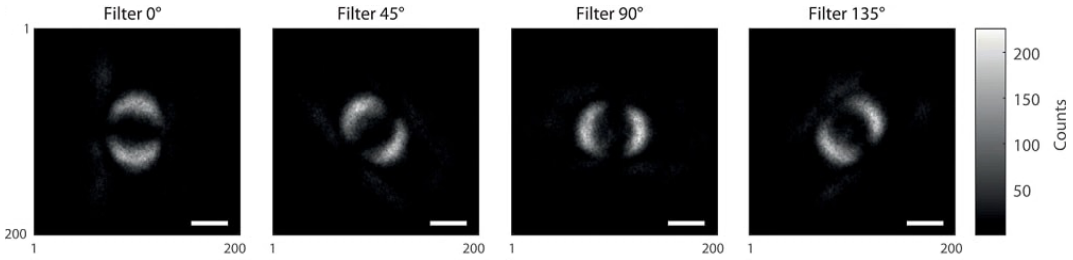

FIGURE 10.8 – Premières photos de photons intriqués (juillet 2019). Il s'agit de flux de photons intriqués selon différents filtres, l'image résultante étant la superposition de chacun des deux flux.

Actuellement, on est capable de construire des systèmes jusqu'à plusieurs dizaines [10] de qubits intriqués (cf. figure 10.9). La question de savoir s'il sera possible un jour de construire des ordinateurs généraliste avec beaucoup plus de qubits est largement débattue [Kal19]. Les effets non locaux d'intrications (cf. paragraphe 10.2.10) ont été testés jusqu'à des distances supérieures à plusieurs centaines de kilomètres en conditions extérieures [11] et même dans l'eau.

10.2.5 Notation de Dirac

Comme on vient de le voir, lorsqu'on considère des systèmes à n qubits on est amené à manipuler des vecteurs de dimension 2^n qui ont tendances à être très peu denses. En

10. IBM a annoncé en mai 2017 un processeur à 17 qubits, et à moyen terme l'objectif d'un processeur à 50 qubits avec 90 microsecondes de temps quantique.
11. Le record en 2017 était de 1 200 km détenu par la Chine (voir l'article).

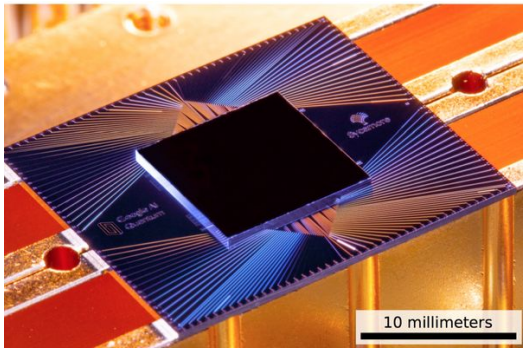

FIGURE 10.9 – Cryostat d'IBM câblé pour le processeur de 50 qubits, et le processeur Sycamore de 54 qubits de Google. © IBM & Google.

particulier, les 2^n vecteurs de la base de calcul

$$\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix},\begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix},\ldots,\begin{pmatrix}0\\\vdots\\1\\0\end{pmatrix},\begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}$$

contiennent qu'une seule valeur non nulle pour 2^n composantes. On utilise donc la notation de Dirac ou notation « bra-ket », qui pour les vecteurs de la base utilise n caractères au lieu de 2^n. Le vecteur de base pour la dimension $i = 0,\ldots,n-1$, donc celui ayant un seul « 1 » à la ligne i, est simplement noté $|\text{bin}_n(i)\rangle$ où $\text{bin}_n(i)$ est l'écriture binaire de l'entier i sur n bits.

Par exemple, $|0\rangle$, $|01\rangle$ et $|111\rangle$ représenteront respectivement les vecteurs

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

ce qui pour $n = 3$ représente un gain de place non négligeable.

Aussi, on notera l'état d'un système S, composé d'un ou plusieurs qubits, par $|S\rangle$ qui est donc un vecteur d'une certaine dimension (2^n si S est composé de n qubits). Pour

$n = 2$, on pourra par exemple écrire :

$$|S\rangle \;=\; \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\0\\1\end{pmatrix} \;=\; \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \;=\; \begin{pmatrix}2^{-1/2}\\0\\0\\2^{-1/2}\end{pmatrix}.$$

Il est facile de voir que, pour tout mot binaire $w \in \{0,1\}^+$,

$$|0\rangle \otimes |w\rangle \;=\; \begin{pmatrix}1\\0\end{pmatrix} \otimes |w\rangle \;=\; \begin{pmatrix}1\cdot|w\rangle\\0\cdot|w\rangle\end{pmatrix} \;=\; \begin{pmatrix}|w\rangle\\0\\\vdots\\0\end{pmatrix} \;=\; |0w\rangle\,.$$

De même, $|1\rangle \otimes |w\rangle = |1w\rangle$, si bien que, plus généralement, on a $|v\rangle \otimes |w\rangle = |vw\rangle$ pour tout mot binaire v. (Cela se montre par induction sur la longueur du mot v et par l'associativité de $\otimes$.)

On note la transposition d'un vecteur $|A\rangle$ non pas par ${}^t|A\rangle$ mais par $\langle A|$. [*Cyril.* À revoir. En fait $\langle A|$ est le trans-conjugué, c'est-à-dire la matrice transposée où chaque élément complexe de A est remplacé par son conjugué : $a + ib \mapsto a - ib$. On note que $(a+ib)\cdot(a-ib) = a^2 - (ib)^2 = a^2 + b^2$.] Si bien que $|A\rangle \cdot \langle B|$ représente le produit scalaire de $|A\rangle$ par $|B\rangle$. Comme on va le voir bientôt, le produit scalaire représentera l'application d'opérateur sur les qubits. Produit scalaire et vecteur à coefficients complexes font que l'état d'un système quantique S à n qubits est finalement représenté par un vecteur de l'espace de Hilbert de dimension 2^n.

10.2.6 Mesure

Faire une mesure d'un système S consiste à observer son état. En terme informatique, c'est produire le résultat d'un calcul. En fait, une mesure produit deux effets : 1) elle modifie le système qui se trouve alors dans un état particulier ; et 2) elle permet de récupérer une probabilité d'observer ce nouvel état.

Prenons un exemple déjà rencontré d'un système S composé de deux qubits dans l'état

$$|S\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\,.$$

Après la mesure du système S, on obtient $|00\rangle$ ou $|11\rangle$ avec probabilité $\frac{1}{2}$. Plus généralement, la mesure d'un système S de n qubits initialement dans l'état :

$$|S\rangle = \sum_{i=0}^{2^n-1} \alpha_i \cdot |\mathrm{bin}_n(i)\rangle$$

à pour effet : 1) de modifier S qui passe alors dans un état $|S'\rangle = |\text{bin}_n(i)\rangle$ qui est déterminé (la probabilité que l'état de S' soit $|\text{bin}_n(i)\rangle$ est précisément de $|1|^2 = 1$) ; et 2) de fournir à l'expérimentateur l'indice i en question. Et donc la probabilité que cela se produise est $|\alpha_i|^2$. Dans ce cas les valeurs des n qubits deviennent déterminées à 0 ou à 1 suivant la chaîne $\text{bin}_n(i)$.

À vrai dire il est possible d'effectuer d'autres sortes de mesures sur un état $|S\rangle$, comme par exemple mesurer un seul ou une partie des n qubits. Les mesures précédentes sont dites selon la « base de calcul ». Un des axiomes de la mécanique quantique stipule que pour toute base orthogonale $|B_i\rangle$, la mesure de l'état $|S\rangle = \sum_i \beta_i \cdot |B_i\rangle$ fait passer S dans un état $|B_i\rangle$ avec la probabilité connue $|\beta_i|^2$.

10.2.7 Opérateurs

De manière générale, l'évolution d'un système quantique suit l'équation d'Erwin Schrödinger (1925) qui est très jolie mais dont on ne parlera pas trop dans ce cours [12] :

$$i\hbar \cdot \frac{\partial}{\partial t}|\Psi(r,t)\rangle \;=\; \hat{H} \cdot |\Psi(r,t)\rangle\,.$$

En gros, les états successifs (dérivée selon le temps) s'obtiennent en appliquant une certaine opération $\hat{H}$ (qu'on appelle hamiltonien du système). C'est l'évolution de l'équation d'onde d'un système quantique Ψ.

On modifie l'état d'un système S par l'application d'un *opérateur* qui n'est rien d'autre que le produit du vecteur d'état $|S\rangle$ par une matrice U d'un espace de Hilbert de dimension 2^n pour un système de n qubits.

$$|S'\rangle \;=\; U \cdot |S\rangle\,.$$

Les opérateurs sont des matrices carrées *unitaires* $2^n \times 2^n$ à coefficients dans $\mathbb{C}$, c'est-à-dire un opérateur U vérifiant $U^* \cdot U = U \cdot U^* = \text{Id}_{2^n}$ où U^* est l'adjoint de U et Id_{2^n} est la matrice identité de dimension 2^n. Ce sont aussi les matrices de changement de base. Notons que la matrice nulle (avec des zéros partout) par exemple n'est pas un opérateur, elle n'est pas unitaire. En quelque sorte, on doit toujours pouvoir revenir à l'état initial, car :

$$U^* \cdot |S'\rangle \;=\; U^* \cdot U \cdot |S\rangle \;=\; |S\rangle\,.$$

Les calculs quantiques doivent donc être réversibles, sinon il s'agit d'une mesure. Dans ce cas le système perd de l'information qui est transférée à l'expérimentateur.

Pour $n = 1$, les opérateurs sont des matrices 2×2. Par exemple :

$$\text{NOT} := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{NOT} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \;=\; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \;=\; \begin{pmatrix} \beta \\ \alpha \end{pmatrix}.$$

12. $\hbar \approx 1.054\,571\,800 \times 10^{-34} J \cdot s$ est la constante de Planck réduite, r le vecteur de position, t le temps, et $\hat{H}$ est l'hamiltonien du système, son énergie totale.

Il suit que $\text{NOT} \cdot |0\rangle = |1\rangle$ et $\text{NOT} \cdot |1\rangle = |0\rangle$. C'est donc l'opérateur NOT classique lorsque l'entrée est 0 ou 1, mais de manière générale il s'agit d'un échange de coordonnées. Sur la sphère de Bloch, cela correspond à la symétrie centrale autour de l'origine. En classique et pour $n = 1$, c'est, avec l'identité, le seul opérateur réversible. En quantique par contre, dès $n = 1$ il existe déjà une infinité d'opérateurs comme cette famille paramétrée par $\theta \in \mathbb{R}$:

$$R(\theta) := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}. \tag{10.1}$$

Cet opérateur revient à faire une rotation du vecteur représentant l'état du qubit, qui on le rappelle est un vecteur. On a aussi des opérateurs plus exotiques comme (ici i est le nombre complexe tel que $i^2 = -1$)

$$\sqrt{\text{NOT}} := \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

son nom étant justifié par le fait que $\sqrt{\text{NOT}} \cdot \sqrt{\text{NOT}} = \text{NOT}$. Si l'opérateur NOT pouvait être vu comme une symétrie ou rotation du vecteur d'état sur la surface de Bloch, $\sqrt{\text{NOT}}$ peut être vu comme une rotation intermédiaire.

Et pour $n = 2$, on a par exemple l'opérateur *Controlled-Not* :

$$\text{CNOT} := \begin{pmatrix} \text{Id}_2 & 0 \\ 0 & \text{NOT} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

L'effet de cet opérateur sur un système composé de deux qubits $|x\rangle \otimes |y\rangle = |x, y\rangle$ est le suivant : $\text{CNOT} \cdot |x, y\rangle = |x, x \oplus y\rangle$ (voir figure 10.10). Donc si $x = 1$, y est inversé sinon il est laissé tel quel. Notons que pour être réversible il faut garder en mémoire (dans la sortie) x et/ou y. Ici c'est x qui est conservé.

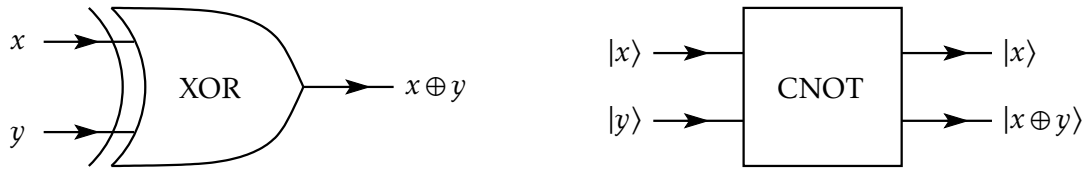

FIGURE 10.10 – Opérateurs classique XOR et quantique CNOT.

En fait, tous les circuits booléens classiques peuvent être construits par un circuits quantiques à la différence que les opérateurs doivent avoir une ou plusieurs entrées supplémentaires pour les rendre réversibles. La porte universelle classique comme NAND (pour *Not-And*) peut être réalisée par un opérateur sur 3 qubits, donc par une matrice 8×8. C'est l'opérateur *Toffoli* appelé aussi CCNOT (pour *Controlled-Controlled-Not*). Cet opérateur se comporte ainsi : $\text{CCNOT} \cdot |x, y, z\rangle = |x, y, z \oplus (x \wedge y)\rangle$. En particulier $\text{CCNOT} \cdot |x, y, 1\rangle = |x, y, \neg(x \wedge y)\rangle = |x, y, \text{NAND}(x, y)\rangle$. Mais aussi $\text{CCNOT} \cdot |1, y, z\rangle =$

$|1,y,z\oplus y\rangle = |1,\mathrm{CNOT}\cdot|y,z\rangle\rangle$. Enfin, $\mathrm{CCNOT}\cdot|1,1,z\rangle = |1,1,\neg z\rangle$. Il peut aussi être défini par :

$$\mathrm{CCNOT} := \begin{pmatrix} \mathrm{Id}_6 & 0 \\ 0 & \mathrm{NOT} \end{pmatrix} = \begin{pmatrix} 1&0&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0&0&0\\ 0&0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&0&1&0 \end{pmatrix}$$

10.2.8 Commutation des opérations locales

Certains opérateurs quantiques binaires précédents, comme par exemple CNOT, ne sont pas locaux dans le sens où il faut avoir accès à la fois au qubit $|x\rangle$ et au qubit $|y\rangle$ pour calculer $\mathrm{CNOT}\cdot|x,y\rangle$. Intuitivement, les entrées doivent passer dans le même lieu au même moment. Dans un certain nombre de cas, les qubits sont très éloignés (Alice possède $|x\rangle$ et Bob $|y\rangle$) et on veut pouvoir effecter une certaine opération sur le système $|x,y\rangle$ seulement en interagissant sur $|x\rangle$ ou sur $|y\rangle$. Il s'agit alors d'une opération « locale » réalisée par Alice (disons l'opération A) ou par Bob (disons l'opération B). Dans le premier cas, l'opérateur appliqué sur le système est $A\otimes\mathrm{Id}$. Dans le second cas, il s'agit de l'opérateur $\mathrm{Id}\otimes B$. Si Alice et Bob appliquent simultanément [13] leur propre opération, il s'agit de l'opérateur $A\otimes B$.

Si Alice et Bob appliquent leurs opérateurs localement chacun sur leur qubit, on obtient *a priori* trois évolutions possibles du système $|x,y\rangle$, en se rappelant que le produit de matrice est associatif mais pas commutatif. Plus précisément, le système devient :

$$\begin{aligned} (\mathrm{Id}\otimes B)\cdot(A\otimes\mathrm{Id})\cdot|x,y\rangle &\qquad \text{(Alice, puis Bob)}\\ (A\otimes\mathrm{Id})\cdot(\mathrm{Id}\otimes B)\cdot|x,y\rangle &\qquad \text{(Bob, puis Alice)}\\ (A\otimes B)\cdot|x,y\rangle &\qquad \text{(Alice et Bob).} \end{aligned}$$

Une propriété importante du produit tensoriel qui va nous servir est que

$$(A\otimes X)\cdot(Y\otimes B) \;=\; (A\cdot Y)\otimes(X\cdot B)$$

[*Cyril*. À vérifier sur des matrices (blocs) 2×2.] En particulier, si $X = Y = \mathrm{Id}$, alors

$$\begin{aligned} (A\otimes\mathrm{Id})\cdot(\mathrm{Id}\otimes B) &= (A\cdot\mathrm{Id})\otimes(\mathrm{Id}\cdot B) = A\otimes B\\ &= (\mathrm{Id}\cdot A)\otimes(B\cdot\mathrm{Id})\\ &= (\mathrm{Id}\otimes B)\cdot(A\otimes\mathrm{Id})\,. \end{aligned}$$

13. Pour peu que cela ait un sens, cf. la figure 1.11.

Et donc les opérations « locales » appliquées à un système binaire, soient $(A \otimes \mathrm{Id})$ et $(\mathrm{Id} \otimes B)$, commutent. L'état du système résultant ne dépend pas de l'ordre d'application des opérations. C'est d'ailleurs le même résultat que d'appliquer simultanément l'opération $A \otimes B$ sur le système.

On peut déduire de cette propriété de commutation des opérateurs locaux une propriété fondamentale de la théorie quantique. C'est une théorie dite *non-signalling* ou non signalante (Voir [Bar06, Corollaire 1, pp. 5].) Cela serait très gênant si cela n'était pas le cas, car on violerait le principe de causalité. On y reviendra plus tard.

10.2.9 Copie et effacement

En admettant le principe que l'on peut copier que ce que l'on connaît, il devient alors évident que les bits probabilistes et quantiques ne peuvent pas être copiés. Seuls les bits déterministes (donc connus) le peuvent. Plus formellement, on peut montrer qu'il n'existe pas d'opérateur unitaire U permettant de passer d'un état[14] $|\psi, 0\rangle$ à un état $|\psi, \psi\rangle$, soit

$$U \cdot |\psi, 0\rangle \; = \; |\psi, \psi\rangle$$

à condition bien sûr que $|\psi\rangle$ soit une superposition d'états, c'est-à-dire un vecteur $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ dont les coefficients vérifient $0 < |\alpha|^2, |\beta|^2 < 1$, puisque les états dont les coordonnées sont 0 ou 1 sont déterminées de manière certaine et donc copiables. Pour la même raison il n'est pas possible d'« effacer » un qubit : il n'y a pas d'opérateur unitaire U tel que $U \cdot |\psi\rangle = |0\rangle$ pour un vecteur $|\psi\rangle$ en état de superposition.

Le principe de copier seulement que ce que l'on connaît peut se voir aussi comme le principe suivant : « pour copier il faut mesurer ». Or faire une mesure change l'état du système. En particulier, la mesure d'un qubit à pour effet de fixer sa valeur, désormais on la connaît. De même un appel à une fonction `random()` aura pour effet de fixer la valeur d'un bit aléatoire. Maintenant, pour les opérations, c'est différent. Bien entendu il faut admettre qu'on puisse modifier un état sans forcément en connaître sa valeur. Lorsqu'on fait `NOT(x)` par exemple, on ne dit pas qu'on connaît `x`. Cette opération pourrait correspondre à la rotation d'une boîte spéciale contenant `x` telle que si on l'ouvre par le haut on lit `x` et si c'est par le bas on lit `NOT(x)`. Donc tant que la boîte n'est pas ouverte, on ne sait pas si l'on va lire un 0 ou un 1, l'état de `x` n'est pas connue (et potentiellement elle n'est peut-être même pas encore fixée). Par contre, en inversant le haut et le bas on sait que l'on lira 0 si `x` était dans l'état 1 et 0 si `x` était dans l'état 1.

On pourrait imaginer copier un bit probabiliste P généré par une certaine fonction `random()` en copiant le code source du générateur, ainsi que l'initialisation de sa graine `seed`. Mais dans ce cas, le bit P serait déterminé par la donnée (`seed`, `random`) ce qui contredit le fait que P soit aléatoire (on parle de nombre pseudo-aléatoire). Si P est

14. On peut remplacer $|\psi, 0\rangle$ par $|\psi, b\rangle$ où b est une constante arbitraire indépendante de ψ.

réellement aléatoire alors au moins un des deux éléments `seed` ou `random` ne peut avoir de description finie (comme un entier de 128 bits ou un programme `C` de 10 Ko).

10.2.10 Impact non local d'actions locales

Pour illustrer les notions rencontrées, nous allons considérer un système composé de deux qubits (A, B) dans l'état suivant :

$$|A,B\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$$

Dans cet état, et après mesure suivant la base de calcul, on a donc la probabilité $|1/2|^2$ d'observer $|00\rangle$, $|1/2|^2$ d'observer $|01\rangle$, $|1/2|^2$ d'observer $|10\rangle$ et $|-1/2|^2$ d'observer $|11\rangle$. Bref, il y a exactement une chance sur quatre d'observer chacune des quatre possibilités.

On peut supposer que le qubit A est à disposition d'Alice et que le qubit B à disposition de Bob, Alice et Bob étant arbitrairement éloignés l'un de l'autre et dans l'incapacité de communiquer pendant le temps de l'expérience. En particulier, Alice a exactement une chance sur deux d'observer 0. Idem pour Bob, et pour la valeur 1.

Supposons que Bob décide d'appliquer l'opérateur $R(-\pi/4)$ à son qubit. Alice, quant à elle ne fait rien. Formellement elle applique l'opérateur Id_2. C'est une action locale qui se traduit par l'application de l'opérateur $\mathrm{Id}_2 \otimes R(-\pi/4)$ sur l'état $|A,B\rangle$.

Par définition de R (équation 10.1), on a :

$$R(-\pi/4) = \begin{pmatrix} \cos(-\pi/4) & -\sin(-\pi/4) \\ \sin(-\pi/4) & \cos(-\pi/4) \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \tag{10.2}$$

L'opérateur appliqué au système est :

$$\mathrm{Id}_2 \otimes R(-\pi/4) = \begin{pmatrix} R(-\pi/4) & 0 \\ 0 & R(-\pi/4) \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix}$$

Il suit qu'après la rotation de Bob, l'état du système devient :

$$|A,B\rangle' = (\mathrm{Id}_2 \otimes R(-\pi/4)) \cdot |A,B\rangle = \frac{1}{2} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$$

$$= \frac{1}{2\sqrt{2}} \begin{pmatrix} 2 \\ 0 \\ 0 \\ -2 \end{pmatrix} = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \,.$$

La probabilité qu'a Alice d'observer 1 vaut $|-1/\sqrt{2}|^2 = 1/2$, comme Bob. Alice et Bob ont aussi toujours une chance sur deux d'observer 0. En fait, la probabilité qu'a Alice d'observer une valeur donnée ne peut pas être influencée par l'action locale de Bob. Sinon, il y aurait transmission d'information [15]. Avant la mesure, et quoi qu'ait fait Bob localement, Alice ignore toujours l'information aléatoire codé par le qubit de Bob. D'ailleurs, peut-être que Bob a déjà fait la mesure sur son qubit... et Alice ne le sait pas.

En revanche, ce qui a changé c'est que conjointement Alice et Bob ne peuvent observer que 00 ou 11. Si Bob fait une mesure locale et observe 1, Alice mesurera également 1 de manière certaine. Ce n'était pas le cas pour l'état initial $|A,B\rangle$ où 01 et 10 pouvaient être observés. Bob a fait quelque chose qui fait qu'Alice et Bob observeront à coup sûr la même valeur. C'est donc les corrélations qui ont changées. Notons que le changement de corrélation est opérationnel dès que l'action de Bob sur son qubit est achevée, indépendamment de la distance séparant Alice de Bob.

Pour illustrer la situation, on pourrait imaginer qu'un grand nombre de particules intriquées, dans l'état ci-dessus, soit générées successivement. Pour fixer les idées supposons que les particules sont des pièces quantiques enfermées dans des boîtes, donnant pile ou face aléatoirement lorsqu'Alice et Bob ouvre leur boîte respectivement. On pourrait alors vérifier au fur et à mesure des générations de pièces intriquées que, quelle que soit la distance séparant les pièces quantiques, les quatre sorties possibles se produisent uniformément : PP, PF, FP, FF. Cependant, a un moment donné, Bob pourrait effectuer une opération sur sa pièce lui permettant d'affirmer à Alice : « cette fois je suis sûr certain que tu auras le même résultat que moi ». Cela paraît bien évidemment étonnant.

Pour résumer, une action locale peut changer les corrélations de manière instantanées [16] sans permettre de transmission d'information entre les parties du système. On dit parfois que le calcul quantique est *contextuel* : le calcul d'un système (ici réduit à

15. Alice, en mesurant ou estimant la probabilité, pourrait déterminer si Bob a appliqué son opérateur ou pas, et ce instantanément quelque soit la distance.

16. On a pu tester expérimentalement dans [SBB+08] « l'instantanéité » de ce changement et vérifier qu'il se produisait à une vitesse supérieur à 10^4 fois la vitesse de la lumière.

Alice) quantique peut être influencé par des actions locales extérieures à ce système (ici Bob). Cela ne peut pas se produire dans le cas de calcul classique.

10.3 Sur les inégalités de Bell

Les inégalités de John Stewart Bell prédisent les résultats d'une expérience, en terme de seuil de probabilité, pour que la théorie des variables locales cachées soit valide. On va revenir sur ces expériences qui ont été réalisées par Alain Aspect en 1982. Elles confirment que les inégalités de Bell sont effectivement violées, que la théorie des variables locales cachées ne peut expliquer les résultats expérimentaux.

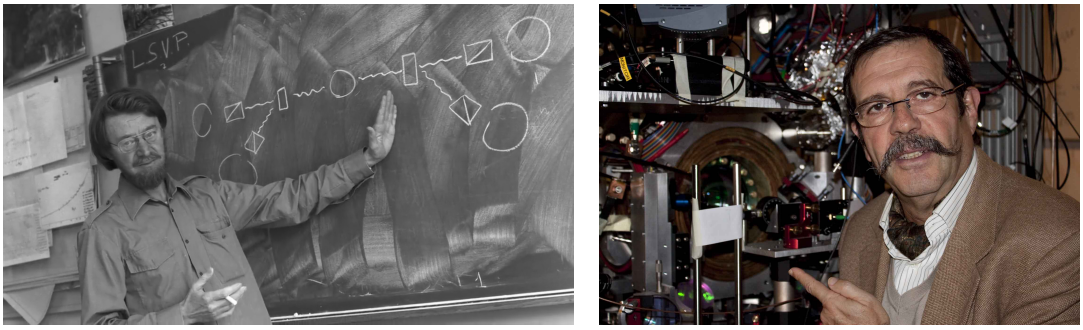

FIGURE 10.11 – John Bell et Alain Aspect.

Les expériences d'Alain Aspect ont été successivement améliorées afin d'éliminer tous les « échappatoires[17] « (*loophole*) possibles à la non localité des effets quantiques, et en 2015 on considérait que tous les échappatoires avait été éliminés [HBD+15]. De très bonnes vidéos (part. 1 | part. 2 | part. 3 | part. 4) réalisées par L'Institut d'Optique retracent l'histoire de l'intrication quantique et revient sur ces découvertes.

10.3.1 L'expérience de pensée

Dans l'expérience de pensée (cf. figure 10.12 de gauche) un générateur C produit deux particules (des photons intriqués dans l'expérience d'Alain Aspect) qui partent en direction opposée vers des détecteurs A et B. Elles partent à une vitesse qui rend impossible toute communication entre elles pendant leur parcours. Les détecteurs, qui sont typiquement des polariseurs comme sur la figure 10.13, sont indépendants, sans lien de communication. Ils sont orientés selon les positions à 1, 2 ou 3 de façon aléatoire, indépendante et uniforme. Au passage d'une particule émise depuis C, chaque détecteur émet un flash soit rouge (R) soit vert (V). Il est important de remarquer que le choix du

17. Comme la certification de la source aléatoire ou l'effet de la distance (6m pour Alain Aspect), etc.

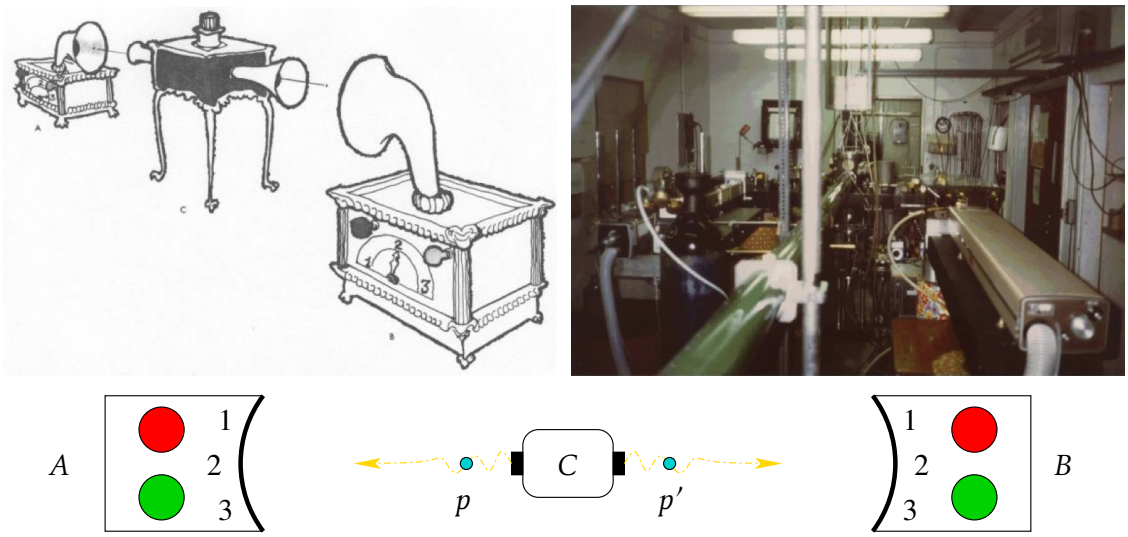

FIGURE 10.12 – Le choix 1-2-3 des détecteurs A et B (angle des polariseurs) est déterminé par le libre choix de l'expérimentateur après le départ des particules depuis le générateur C. Dans l'expérience réelle d'Alain Aspect en 1982 (à droite) le choix est déterminé par un générateur aléatoire quantique. Source [Mer85].

positionnement est fait après la génération des particules en C. Il n'y a donc pas de lien de causalité entre la position des détecteurs A et B, et la génération des particules en C.

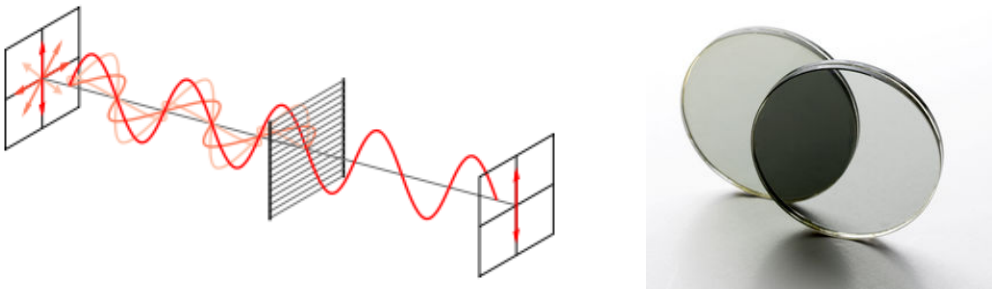

FIGURE 10.13 – Un polariseur permet de ne garder que les particules/ondes d'une orientation (polarité) donnée.

La table 10.1 présente les résultats hypothétiques d'une telle série d'expériences. Par exemple « 12VR » dans la table signifie que le réglage du détecteur A était sur 1 et a flashé V, et que le détecteur B était sur 2 et a flashé R.

12VR	32RV	32VR	22RR	33RR	12RV	22VV	13RV	21RV
22VV	11VV	31RV	22RR	21RV	21VV	21VR	11VV	13VR
11VV	31RV	32RV	21VR	31VR	31RV	12VR	23RV	11RR
21VR	13VR	13RV	33VV	21RR	12RV	33RR	23RV	23VR
33VV	33RR	12RR	21RV	31VR	32VR	23RR	13VV	23VV
33RR	12VR	12RV	31VV	33VV	13VV	32VR	32RR	23RV
11RR	31VR	22RR	11RR	23VR	23VR	22VV	13RR	33VV
22VV	11VV	12VR	32RV	32VV	31RR	13RV	22RR	11RR

TABLE 10.1 – Résultats d'une expérience de pensée[18] comme schématisée sur la figure 10.12 comportant 72 détections. La distribution des 9 paires de positions possibles (11, 12, ..., 33) est uniforme, soit 8 fois chacune. La distribution des flashs (RR, RV, VR, VV) est uniforme, soit 18 fois chacune. En particulier, 50% des détections (36 fois sur 72) flashent de la même couleur (RR ou VV). Les corrélations (mêmes positions et mêmes flashes) sont soulignées.

Les données ont deux caractéristiques (vérifiées pour la table 10.1) :

1. **Corrélation.** Lorsque les détecteurs sont sur les mêmes positions, leurs flashs sont toujours de couleur identique : 22VV, 33RR, 22RR, etc.
2. **Uniformité.** Lorsqu'on ne considère que les flashs, faisant abstraction de la position des détecteurs, le résultat est aléatoire uniforme. En particulier, la moitié du temps les flashs sont de la même couleur, la moitié du temps les flashs sont de couleur différente.

Il faut bien réalisé que de vraies expériences physiques montrent que ces deux caractéristiques se trouvent être réalisées simultanément. On donnera plus loin au paragraphe 10.3.2 une explication de cette observation grâce au formalisme quantique.

> **Hypothèse.** Supposons que ce que mesurent les détecteurs est une propriété intrinsèque des particules qui est fixée avant d'être détectée.

Cette propriété pourra être fixée par exemple lorsque les particules sont créées en C ou un peu plus tard pendant leur parcours de C aux détecteurs. En fait on supposera que la propriété est fixée avant de positionner les détecteurs (le choix de la mesure). C'est l'hypothèse de la théorie des variables locales cachées : les particules possèdent une propriété préexistante qui n'est accessible aux expérimentateurs seulement au moment de réaliser la mesure.

18. Il est assez facile de générer une telle distribution, et donc de se convaincre que la table 10.1 n'est pas qu'un accident ou juste impossible. Il suffit d'une part de générer le même nombre de chaque paire de positions (un multiple de 9), et d'autre part de générer le même nombre de chaque paire de flashs (un multiple de 4). Lorsque ces deux quantités de paires sont identiques (disons $9\times4 = 36$), il suffit d'apparier les paires de positions et paires de flashs de façon à respecter la corrélation.

Sous cette hypothèse et à cause de la caractéristique (1) des données, pour que les détecteurs flashent de la même couleur lorsqu'ils sont réglés de la même façon, il faut que les deux particules possèdent une propriété commune indiquant comment les détecteurs doivent se comporter. Si cela n'était pas le cas, puisqu'on génère suffisamment de particules et effectue suffisamment de détections avec des positions aléatoires, on devrait observer une différence de flash pour un même positionnement de détecteur (qui on le rappelle a lieu après la génération). Or cela n'arrive jamais. Les propriétés qu'on observent sont donc les mêmes pour chaque paire de particules. Entre deux générations successives, ces propriétés sont évidemment arbitraires mais identiques pour p et p'.

Un détecteur ne peut distinguer que 8 possibilités, et donc 8 propriétés d'une particule : un flash R ou V en position 1, un flash R ou V en position 2, et un flash R ou V en 3. Par exemple, une particule qui flasherait R en position 1, d'après notre hypothèse, possède cette propriété (de flasher R en position 1) avant la mesure. Si elle flashe V en position 2, c'est qu'elle possède aussi cette propriété. Enfin, si elle flashe R en position 3, c'est qu'elle possède cette propriété supplémentaire. Comme le détecteur est positionné après la génération, une telle particule doit posséder ces trois propriétés qu'on notera par RVR dans ce cas-ci. On dira plus simplement que la particule est de type RVR. Encore une fois, à cause de la caractéristique (1) des données les deux particules doivent avoir le même type, RVR par exemple, puisque sinon au bout d'un certain nombre de mesures les détecteurs pareillement positionnés mesureraient une différence. Il est exclus que le générateur C génère un même type seulement lorsque les détecteurs ont la même position car le positionnement est déterminé après la génération des particules. Encore une fois, sous notre hypothèse, chaque particule générée possède un type déterminé mais absolument inaccessible avant la mesure. Le type est aléatoire et gardé secret jusqu'à la mesure.

Pour le type RVR, les deux particules flasheront de la même couleur si les détecteurs sont en position 11, 22 ou 33, 13 ou 31. Ils flasheront de couleurs différentes pour les positions 12, 21, 23 et 32. Puisque les positions des détecteurs sont fixées indépendamment, aléatoirement et uniformément, chacune des 9 paires de positions (11, 12, 13, 21, ..., 33) se produit avec la même fréquence, soit 1/9. Donc les mêmes couleurs devraient flasher $5/9 = 1/2 + 1/18 > 55\%$ du temps pour le type RVR. Cela reste valable pour les six types ayant exactement deux lettres identiques, soient RRV, RVR, VRR, VVR, VRV, RVV. Pour les deux types restant RRR et VVV, les mêmes couleurs devraient flasher 100% du temps. Voir la table 10.2.

Au final, quelque soit la distribution du type des particules générées en C au cours de l'expériences, les détecteurs devraient flasher de la même couleur au moins 55% du temps. C'est incompatible avec la caractéristique (2) des données. Les distributions des résultats vérifiant (1) et (2) violent les inégalités de Bell.

Il suit que les résultats de cette expérience de pensée, qui ont été, et c'est le point fondamental, réellement vérifiés par Alain Aspect, sont incompatibles avec l'hypothèse que les particules possèdent, avant la mesure, une quelconque propriété. La propriété

type	positions	proba
RVR	11,22,33,13,31	5/9
VRV	11,22,33,13,31	5/9
RRV	11,22,33,12,21	5/9
VVR	11,22,33,12,21	5/9
VRR	11,22,33,13,31	5/9
RVV	11,22,33,23,32	5/9
VRR	11,22,33,23,32	5/9
RRR	toutes	9/9
VVV	toutes	9/9

TABLE 10.2 – Table donnant, en fonction du type de la particule, les positions des détecteurs qui aboutissent à un flash de la même couleur, ainsi que la probabilité de cet évènement.

de la particule est déterminée seulement au moment de sa mesure en A et est de plus corrélée au résultat de B.

Une présentation similaire de la même expérience de pensée peut-être trouvé sur le site de l'écrivain et astrophysicien Adam Becker. Cette fois il s'agit de jeu de roulettes dans un casino, cf. figure 10.14.

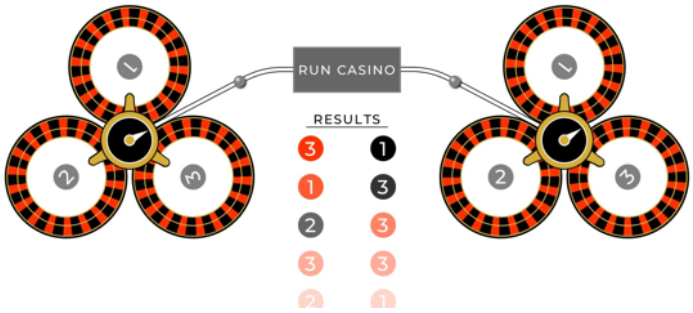

FIGURE 10.14 – Application interactive sur freelanceastro.github.io/bell permettant de simuler un lancer de billes intriquées dans un casino avec un système de tables de roulettes sélectionnables, dont le résultat est soit rouge soit noir.

Notons que c'est cette combinaison (propriété indéterminée et corrélation) qui est difficile à expliquer. La corrélation seule pourrait être expliquée par des variables locales cachées : quand on met un gant issu d'une même paire chacun dans une boîte fermée alors si on observe un gant droit dans l'une, on observera de façon certaine un gant gauche dans l'autre. De même il est concevable que la propriété mesurée ne soit pas déterminée avant la mesure, comme par exemple une pièce de monnaie tournante

sur une table qui se fixerait sur pile ou face quand elle n'aurait plus assez d'énergie (cf. figure 10.15) ou quand l'expérimentateur le déciderait.

FIGURE 10.15 – Pièce de monnaie dont l'état « pile » ou « face » n'est pas encore déterminé.

L'expérience de pensée que l'on vient de décrire ressemble en certains points au *Free Will Theorem* de John Conway *et al.* [CK06]. Sur la base de trois axiomes de physique assez simples (appelés SPIN[19], TWIN[20] et FIN[21]), il est démontré que si le choix de la mesure (la direction du spin d'une particule) est libre (*Free Will*), c'est-à-dire n'est pas fonction d'une information pré-déterminée accessible aux expérimentateurs (par exemple le passé de l'Univers), alors la réponse de la particule n'est pas non plus fonction d'une information pré-déterminée accessible aux particules. Dit autrement, si l'expérimentateur a le choix de la mesure, la particule a le choix du résultat : le résultat d'une mesure n'est pas pré-déterminé, la propriété mesurée n'existe pas avant sa mesure.

Ce phénomène de non déterminisme des propriétés quantiques des particules peut donc se déduire d'expériences de pensées basées sur des axiomes qui sont plus simples à admettre que le formalisme de la physique quantique.

10.3.2 L'explication

[*Cyril*. À FINIR]

On va maintenant vérifier par le calcul qu'en effet l'expérience de pensée, si on la réalise, produira des données vérifiant à la fois la propriété de corrélation et d'uniformité des flashs comme présentée ci-dessus.

Notons par X et Y les deux particules générées par C, juste après leur création mais avant leur détection en A et B. Ce sont des qubits et ils forment un système quantique

19. Quand l'expérimentateur fait trois mesures de directions mutuellement orthogonales, il obtient les résultats $1, 0, 1$ dans un ordre quelconque.
20. Si les expérimentateurs A et B font la même mesure de direction sur deux particules intriquées/jumelées, le résultat sera identique.
21. La vitesse de transmission de l'information est finie.

dans l'état intriqués suivant :

$$|X,Y\rangle \;=\; \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \;=\; \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}.$$

Le choix de l'orientation effectuée dans les détecteurs revient à une mesure locale sur chacune des particules selon une base qui a été tournée d'un angle de 0°, 120° ou 240°.

[*Cyril*. À FINIR. On pourrait définir un jeu non-local, avec comme entrée $x, y \in \{1,2,3\}$ et comme sortie $a, b \in \{0,1\}$. Objectif : montrer qu'on obtient bien l'uniformité et la corrélation comme annoncé.]

[*Cyril*. D'ailleurs on pourrait introduire d'autres jeux non-locaux : $x, y \in \{0,1\}$ et $a, b \in \{0,1\}$ tels que si $x = y$ alors $a \neq b$ et sinon la sortie est aléatoire uniforme. Avec un état de $|01\rangle + |10\rangle$ on va pouvoir le faire, avec une mesure identique (selon la base de calcul $|0\rangle$ ou $|1\rangle$ suivant l'entrée) donc si $x = y$ ce qui va donner 01 ou 10 avec proba 1/2. Sinon, on aura des sorties aléatoires. Mais on peut le faire sans aucun effet quantique : Alice lit x et fait un xor avec un bit aléatoire r_i. Bob lit y et fait xor avec le bit aléatoire $1 - r_i$. Il semble que l'on ne peut pas le faire avec du non-shared randomness. NB : Dans les jeu non-locaux, c'est-à-dire sans communication entre les joueurs, partager un état quantique intriqué ou shared-randomness, partagent le fait que Alice et Bob, pour disposer de ces ressources, ont du de rencontrer.]

10.4 Téléportation

Il est possible de téléporter des états quantiques. Mais il faut bien l'avouer, les explications des réalisations expérimentales laissent perplexe (voir figure 10.16).

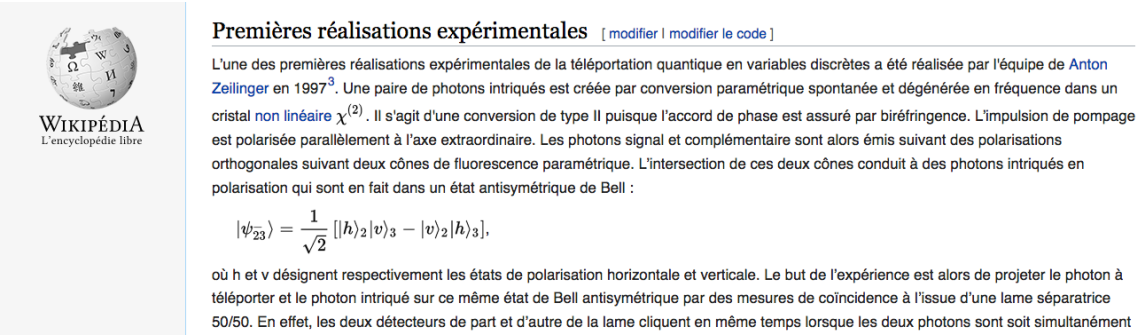

FIGURE 10.16 – Extrait, plutôt cryptique, de la page Wikipédia sur les expériences de téléportations quantiques.

Le principe est pourtant assez simple. [*Cyril*. À FINIR... Il faut qu'Alice fasse un CNOT entre le qubit dont elle veut téléporter l'état et son qubit intriqué avec celui

de Bob. Elle fait ensuite un Hadamard et une mesure qu'elle transmet à Bob par voie classique. Bob effectue alors un Hadamard en fonction du résultat d'Alice. Le qubit de Bob est alors dans le même état que celui d'Alice.] Pour cela il faut une paire de particules intriquées, donc *a priori* indiscernables et qui ont précédemment interagi. La téléportation est instantanée[16] quelle que soit la distance. Il faut bien noter que c'est l'état qu'on téléporte d'une particule à une autre. En rien on ne téléporte une particule, de l'énergie ou une information (voir figure 10.17).

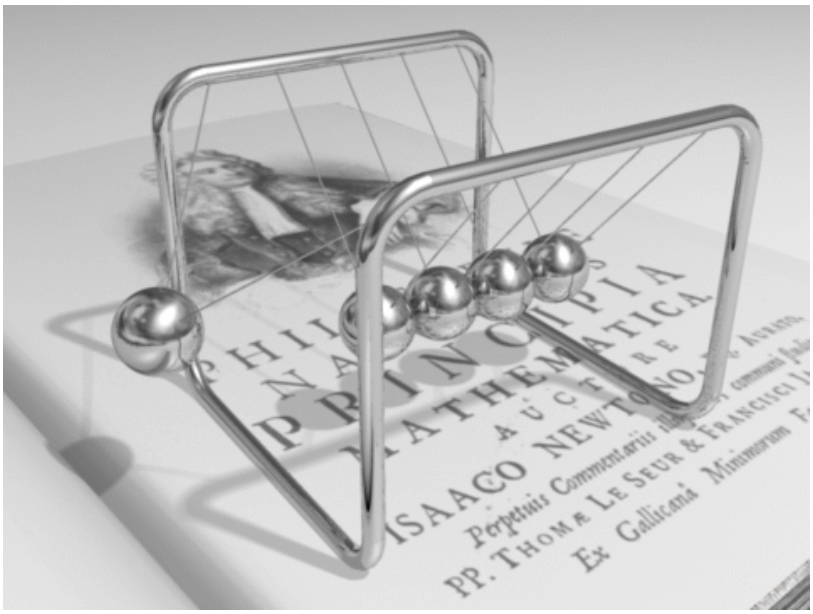

FIGURE 10.17 – Analogie avec le pendule de Newton pour comprendre que ce n'est pas la particule, support du qubit, qui se téléporte, mais son état (ici la quantité de mouvement de la bille à l'extrémité). On remarquera que : 1) les deux billes extrémités doivent être indiscernables vis à vis de l'observable (ici la masse pour préserver la quantité de mouvement) ; et 2) l'état initial qui est « téléporté » est aussi détruit. Bien évidemment, pour le pendule, il s'agit d'une transmission, et non d'une téléportation, de la quantité de mouvement qui ne se détruit pas mais plutôt s'annule. Voir l'animation.

10.5 Jeu CHSH

On va expliquer, grâce à une expérience de pensée (un jeu), la différence entre ressource aléatoire (partagée) et ressource quantique (intriquée). Ce jeu fait écho à l'expérience de pensée de Bell et l'expérience bien réelle d'Alain Aspect. Ce type de jeu, tout comme celui de la section 10.6, est parfois appelé jeu *pseudo-télépathique*, les joueurs semblant deviner comme par magie les cartes des autres joueurs.

Dans ce jeu, du noms des auteurs, Clauser-Horne-Shimony-Holt [CHSH69], il y a deux joueurs : Alice (A) et Bob (B) et ils ne peuvent pas communiquer (cf. figure 10.18). Il s'agit pour les joueurs de calculer un bit de sortie a et b en fonction d'un bit d'entrée x et y, et d'éventuellement de ressources extérieures accessibles seulement par les joueurs. Plus précisément, pour qu'Alice et Bob gagnent, if faut $a \oplus b = x \wedge y$. Dit autrement, il faut que $a = b$, sauf si $x = y = 1$.

Dans le cas déterministe, la ressource est réduite à l'algorithme seul. Dans le cas probabiliste, la ressource (en plus de l'algorithme) est alors une source de bits aléatoires partagées (*shared randomness*) inconnue de l'expérimentateur (secrète donc). Et dans le cas quantique, la ressource sont des qubits dans un état intriqué (*entangled qubits*).

Les physiciens nomment plus communément la source de bits aléatoires partagées par *variable locale cachée*, une quantité constante déterminée inaccessible aux expérimentateurs mais connues de toutes les particules.

Proposition 10.1 *Aucun algorithme déterministe ne permet à Alice et Bob de gagner au jeu CHSH à tous les coups.*

Preuve. Supposons qu'il existe un tel algorithme, et soient $a(x)$ et $b(y)$ les fonctions calculées par Alice et Bob ; dans le cas déterministe ces fonctions ne dépendent que des l'entrées, Alice et Bob ne pouvant pas communiquer. Pour gagner, il faut $a(x) \oplus b(y) = x \wedge y$. Les fonctions doivent donc vérifier les quatre équations suivantes, une pour chacune entrée (x, y) possibles :

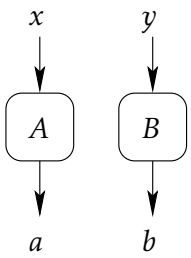

FIGURE 10.18 – Le jeu CHSH : pour gagner, le OU-exclusif de la sortie doit être égale au ET de l'entrée, soit $a \oplus b = x \wedge y$. Autrement dit, on doit avoir les mêmes sorties, sauf si les deux entrées sont à 1.

$$
\begin{aligned}
a(0) \oplus b(0) &= 0 \\
a(0) \oplus b(1) &= 0 \\
a(1) \oplus b(0) &= 0 \\
a(1) \oplus b(1) &= 1
\end{aligned}
$$

En utilisant le fait que $a \oplus b \equiv a + b \pmod 2$, la somme modulo deux, on peut transformer ces équations en sommes classiques et considérer le résultat modulo 2. La somme des termes des membres à gauche fait $2 \cdot (a(0) + a(1) + b(0) + b(1))$ ce qui est nécessairement paire. Malheureusement, la somme des termes des membres de droite est impaire. Il n'existe donc pas de fonctions $a(x)$ et $b(y)$ satisfaisant ces quatre contraintes. Il n'existe donc pas d'algorithme déterministe qui permet de gagner au jeu CHSH à tous les coups. □

En revanche, comme on va le voir, il existe un algorithme probabiliste qui résout CHSH avec une probabilité de 75% si Alice et Bob partagent un secret aléatoire. Notez bien qu'il faut arriver à gagner avec cette probabilité quelle que soit la distribution des entrées. Par exemple, répondre toujours 0, qui satisfait les contraintes dans $\frac{3}{4}$ des cas, ne marche que si la distribution des entrées est uniforme (même chance d'obtenir les quatre entrées (x, y) possibles). Alice et Bob se battent donc contre un adversaire (en fait l'expérimentateur) qui connaît par avance leur stratégie, et qui dans ce cas là proposera toujours $x = y = 1$ pour faire échouer à coup sûr l'algorithme d'Alice et Bob. Notez qu'on admet que l'adversaire, aussi fort soit-il, n'a pas accès à la ressource aléatoire commune (variables locales cachées).

Proposition 10.2 *Si Alice et Bob partagent des bits secrets aléatoires, alors il peuvent gagner au jeu CHSH dans* 75% *des cas, et ce quel que soit l'adversaire.*

Preuve. Pour atteindre 75% de réussite, il suffit que les joueurs, avant la proposition de chaque entrée (x,y) proposée par l'adversaire, se mettent d'accord sur une des quatre équations à ne pas satisfaire (en utilisant une même paire de bits aléatoires partagés), choix inconnu de l'adversaire. Il est alors toujours possible de résoudre le système composé des trois équations restantes.

Par exemple, s'ils décident de ne pas satisfaire la 4e équation soit $a(1) \oplus b(1) = 0$ au lieu de $a(1) \oplus b(1) = 1$, alors $a(x) = b(y) = 0$ est une solution. Ainsi, les joueurs perdent seulement si l'adversaire propose l'entrée (x,y) correspondant à l'équation choisie (ici $x = y = 1$), soit seulement dans $\frac{1}{4}$ des cas.

On peut alors vérifier que s'ils choisissent de ne pas satisfaire l'équation correspondant à l'entrée (x,y) :

- $(0,0)$, alors $a(x) = \neg x$ et $b(y) = y$ est une solution.
- $(0,1)$, alors $a(x) = 0$ et $b(y) = y$ est une solution.
- $(1,0)$, alors $a(x) = x$ et $b(y) = 0$ est une solution.
- $(1,1)$, alors $a(x) = 0$ et $b(y) = 0$ est une solution.

Donc quels que soient les choix de l'adversaire, Alice et Bob gagneront dans $\frac{3}{4}$ des coups. □

Mais peut-on faire mieux ? Et bien non.

Proposition 10.3 *Aucun algorithme probabiliste ne peut gagner au jeu CHSH avec plus de 75% de chance.*

Preuve. Un algorithme probabiliste est un algorithme qui, pour chaque entrée, fait un certain nombre de tirages aléatoires avant de renvoyer sa sortie. Ces choix aléatoires sont autant d'exécutions et de sorties possibles. En fait on peut regrouper les sorties possibles et voir un algorithme probabiliste comme un algorithme qui affiche chaque sortie avec une certaine probabilité.

Il y a au plus quatre fonctions $a(x)$ à une variable binaire[22] qui sont $0, 1, x, \neg x$. De même pour $b(y)$, si bien qu'Alice et Bob ont a leur disposition au plus 16 algorithmes ou paires de fonctions $(a(x), b(y))$. En fait, certaines paires de fonctions ont toujours les mêmes sorties, en particulier à cause de la symétrie de la formule $a(x) \oplus b(y)$ qui définit la sortie de l'algorithme. Mais pas seulement. Par exemple, la paire de fonctions $(a(x), b(y)) = (\neg x, \neg y) = (x, y)$ puisque $\neg x \oplus \neg y = x \oplus y$.

Ainsi, on peut vérifier qu'il n'existe que 8 fonctions de sorties différentes, qui sont (cf. la table ci-dessous) : 0, 1, x, $\neg x$, y, $\neg y$, $x \oplus y$, $\neg x \oplus y$.

22. De manière générale il y a 2^{2^n} fonctions $f : \{0,1\}^n \to \{0,1\}$ à n variables, cf. [Gav25, Section 2.6].

	0	1	x	$\neg x$
0	0	1	x	$\neg x$
1	1	0	$\neg x$	x
y	y	$\neg y$	$x \oplus y$	$\neg x \oplus y$
$\neg y$	$\neg y$	y	$\neg x \oplus y$	$x \oplus y$

L'algorithme probabiliste d'Alice et Bob choisit donc une de ces sorties suivant une certaine distribution de probabilité $p_1, \ldots, p_8$, p_i étant la probabilité de choisir la i-ème sortie. On a bien sûr que $\sum_i p_i = 1$. La distribution $p_1, \ldots, p_8$ détermine entièrement l'algorithme probabiliste d'Alice et Bob qui cherchent à optimiser les p_i pour maximiser leurs chances de succès quel que soit l'adversaire.

On notera P_{xy} la probabilité de succès de cet algorithme pour l'entrée (x, y). La table ci-dessous résume les différentes probabilités.

x	y	$x \wedge y$	0	1	x	$\neg x$	y	$\neg y$	$x \oplus y$	$\neg x \oplus y$	probabilité de succès
0	0	0	p_1	0	p_3	0	p_5	0	p_7	0	$P_{00} = p_1 + p_3 + p_5 + p_7$
0	1	0	p_1	0	0	p_4	p_5	0	0	p_8	$P_{01} = p_1 + p_4 + p_5 + p_8$
1	0	0	p_1	0	p_3	0	0	p_6	0	p_8	$P_{10} = p_1 + p_3 + p_6 + p_8$
1	1	1	0	p_2	p_3	0	p_5	0	0	p_8	$P_{11} = p_2 + p_3 + p_5 + p_8$

L'objectif est de montrer que, quel que soit le choix des probabilités $p_1, \ldots, p_8$, la probabilité de succès de l'algorithme d'Alice et Bob ne dépassera pas 75% pour les quatre entrées possibles. Dit autrement on veut montrer que :

$$\min\{P_{00}, P_{01}, P_{10}, P_{11}\} \leqslant \frac{3}{4}.$$

Pour cela on va calculer la somme $S = P_{00} + P_{01} + P_{10} + P_{11}$ et montrer que $S \leqslant 3$ ce qui permettra de conclure que le plus petit des quatre termes de la somme est $\leqslant 3/4$. C'est immédiat car :

$$S = 3p_1 + p_2 + 3p_3 + p_4 + 3p_5 + p_6 + p_7 + 3p_8 \leqslant 3 \cdot (p_1 + \cdots + p_8) = 3$$

ce qui termine la preuve. On notera que pour maximiser la probabilité de succès, Alice et Bob ont intérêt à choisir $p_1 = p_3 = p_5 = p_8 = 1/4$ et $p_2 = p_4 = p_6 = p_7 = 0$, ce qui revient à choisir aléatoirement une des quatre paires de fonctions : $0 = 0 \oplus 0$, $x = x \oplus 0$, $y = 0 \oplus y$ et $\neg x \oplus y$. C'est précisément la solution présentée dans la proposition 10.2. Dans ce cas on a $P_{00} = P_{01} = P_{10} = P_{11} = 3/4$. □

On va maintenant montrer que s'ils possèdent chacun un qubit formant un système dans un état intriqué alors ils peuvent gagner avec une probabilité strictement supérieure à 75%.

Proposition 10.4 *Si Alice et Bob disposent de ressources quantiques, alors ils peuvent gagner au jeu CHSH avec une probabilité de* $\cos^2(\pi/8) = (1+1/\sqrt{2})/2 > 85\%$.

Preuve. Cette fois-ci, Alice et Bob partagent des paires de qubits intriqués, une paire pour chaque nouvelle entrée de l'adversaire. Alice possède un qubit $|A\rangle$ et Bob un qubit $|B\rangle$. Les qubits ont interagit dans le passé, avant bien sûr que n'ai été fixée l'entrée (x,y) de l'adversaire, pour former le système :

$$|A,B\rangle \;=\; \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) .$$

L'algorithme, pour Alice, consiste à appliquer une rotation $R(\theta) = \begin{pmatrix}\cos\theta & -\sin\theta \\ \sin\theta & \cos\theta\end{pmatrix}$ suivant un angle θ de $-\pi/16$ si $x=0$ et $3\pi/16$ si $x=1$, soit de manière générale un angle de $\theta_A = (4x-1)\pi/16$. La stratégie est identique pour Bob avec une rotation de $\theta_B = (4y-1)\pi/16$.

Une fois cette opération effectuée sur chacun de leur propre qubit, Alice et Bob affiche le résultat de la mesure dans la base de calcul, soit 0 ou 1 suivant que l'état devient $|0\rangle$ ou $|1\rangle$.

En terme de calcul, l'action d'Alice se traduit par l'application de l'opérateur $R(\theta_A)\otimes \mathrm{Id}_2$ (soit une matrice 4×4) à l'état $|A,B\rangle$ représentant l'état initial du système. De même pour Bob, son action va se traduire par l'application de l'opérateur $\mathrm{Id}_2 \otimes R(\theta_B)$ à $|A,B\rangle$.

Chacune des opérations de rotation affecte non seulement le qubit sur laquelle elle est effectuée mais le système en entier. On peut montrer que l'ordre d'application des opérateurs n'a pas d'influence sur l'état du système final (cf. paragraphe 10.2.8) si bien qu'on peut appliquer directement l'opérateur $R(\theta_A)\otimes R(\theta_B)$ à $|A,B\rangle$. L'état du système devient :

$$(R(\theta_A)\otimes R(\theta_B))\cdot|A,B\rangle \;=$$

$$\begin{pmatrix} \cos\theta_A \cdot \begin{pmatrix}\cos\theta_B & -\sin\theta_B \\ \sin\theta_B & \cos\theta_B\end{pmatrix} & -\sin\theta_A \cdot \begin{pmatrix}\cos\theta_B & -\sin\theta_B \\ \sin\theta_B & \cos\theta_B\end{pmatrix} \\ \sin\theta_A \cdot \begin{pmatrix}\cos\theta_B & -\sin\theta_B \\ \sin\theta_B & \cos\theta_B\end{pmatrix} & \cos\theta_A \cdot \begin{pmatrix}\cos\theta_B & -\sin\theta_B \\ \sin\theta_B & \cos\theta_B\end{pmatrix} \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$$

En utilisant les formules

$$\begin{cases} \cos(x+y) \;=\; \cos x\cos y - \sin x \sin y \\ \sin(x+y) \;=\; \sin x \cos y + \cos x \sin y \end{cases}$$

l'état se simplifie en :

$$\begin{aligned}(R(\theta_A)\otimes R(\theta_B))\cdot|A,B\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix}\cos\theta_A\cos\theta_B-\sin\theta_A\sin\theta_B\\ \cos\theta_A\sin\theta_B+\sin\theta_A\cos\theta_B\\ \sin\theta_A\cos\theta_B+\cos\theta_A\sin\theta_B\\ \sin\theta_A\sin\theta_B-\cos\theta_A\cos\theta_B\end{pmatrix} = \frac{1}{\sqrt{2}}\cdot\begin{pmatrix}\cos(\theta_A+\theta_B)\\ \sin(\theta_A+\theta_B)\\ \sin(\theta_A+\theta_B)\\ -\cos(\theta_A+\theta_B)\end{pmatrix}\\ &= \frac{1}{\sqrt{2}}(\cos(\theta_A+\theta_B)(|00\rangle-|11\rangle)+\sin(\theta_A+\theta_B)(|01\rangle+|10\rangle))\end{aligned}$$

Il faut maintenant vérifier que la probabilité de succès, c'est-à-dire d'avoir $a\oplus b = x\wedge y$, est bien de $\cos^2(\pi/8)$.

La probabilité d'obtenir $a\oplus b = 0$ est la probabilité d'obtenir $|00\rangle$ ou $|11\rangle$, soit

$$2\cdot\left(\frac{1}{\sqrt{2}}\cos(\theta_A+\theta_B)\right)^2 = \cos^2(\theta_A+\theta_B)\,.$$

Si l'entrée est $x=0$ et $y=0$, alors la probabilité d'avoir $a\oplus b = x\wedge y = 0$ vaut $\cos^2(-2\pi/16)=\cos^2(\pi/8)$.

Si l'entrée est $x=1$ et $y=0$ (ou $x=0$ et $y=1$, les formules sont symétriques en x et y), alors la probabilité d'avoir $a\oplus b = x\wedge y = 0$ vaut $\cos^2(3\pi/16-\pi/16)=\cos^2(\pi/8)$.

La probabilité d'obtenir $a\oplus b = 1$ est la probabilité obtenir $|01\rangle$ ou $|10\rangle$, soit $\sin^2(\theta_A+\theta_B)$.

Si l'entrée est $x=y=1$, alors la probabilité d'avoir $a\oplus b = x\wedge y = 1$ vaut $\sin^2(6\pi/16)=\sin^2(3\pi/8)=\cos^2(\pi/8)$, car sur le cercle unité on s'aperçoit que les angles $3\pi/8$ et $\pi/8$ sont symétriques par rapport à l'angle $\pi/4$ (voir figure 10.19). □

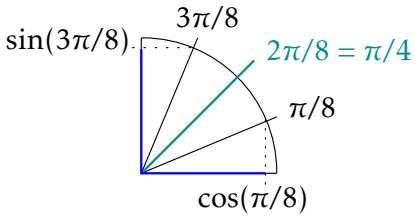

FIGURE 10.19 – Géométriquement, par symétrie autour de l'axe d'angle $\pi/4$, on remarque que $\cos(\pi/8)=\sin(3\pi/8)$.

On peut même montrer qu'aucun algorithme quantique ne peut le faire avec une probabilité plus grande que $\cos^2(\pi/8)$. C'est la borne de Tsirelson [Cir80]. Il faut pour cela utiliser de l'algèbre linéaire (et des valeurs propres) dans les espaces de Hilbert, et on ne le fera pas dans ce cours.

[*Exercice.* 1 Montrer qu'Alice et Bob peuvent gagner au jeu CHSH avec 50% de chance s'ils ont accès à une ressource probabilistes non partagées. 2* Montrer que 50% est la meilleure probabilité possible.]

10.6 Jeu GHZ

Il s'agit en fait d'une variante simplifiée du jeu GHZ, du nom des auteurs Greenberger-Horne-Zeilinger [GHZ89], voir aussi [Boy04]. Il y a maintenant trois joueurs : Alice (A), Bob (B) et Carole (C). On peut en fait le généraliser à n joueurs. Comme précédemment ils ne peuvent communiquer avant de recevoir les entrées qui sont des valeurs booléennes, respectivement x, y, z. Ils doivent sortir des valeurs a, b, c respectivement avec leurs propres resources, mais sans communiquer après l'arrivée des entrées (figure 10.20).

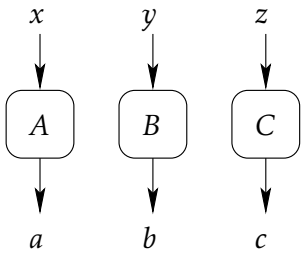

FIGURE 10.20 – Le jeu GHZ : pour gagner, la parité de la somme de la sortie doit être égale à la parité de la demi-somme de l'entrée, sachant que la somme de l'entrée est toujours paire. Ce jeu peut être généralisé à n joueurs.

Il y a une contrainte (promesse) sur les entrées : leur somme doit être paire. Pour gagner, il faut que la parité de la somme de la sortie soit égale à la parité de la demi-somme de l'entrée. Autrement dit, $x+y+z \in \{0,2\}$ et $a+b+c \equiv \frac{1}{2}(x+y+z) \pmod 2$. Pour résumer :

x	y	z	$\frac{1}{2}(x+y+z)$
0	0	0	0
1	1	0	1
1	0	1	1
0	1	1	1

ce qui revient aussi à distinguer le cas $xyz = 000$ des trois autres.

Soient $a(x)$, $b(y)$ et $c(z)$ les fonctions calculées par Alice, Bob et Carole. Alors, pour gagner, les fonctions doivent donc vérifier les quatre équations suivantes :

$$\begin{aligned} a(0)+b(0)+c(0) &\equiv 0 \\ a(1)+b(1)+c(0) &\equiv 1 \\ a(1)+b(0)+c(1) &\equiv 1 \\ a(0)+b(1)+c(1) &\equiv 1 \end{aligned}$$

De manière similaire au jeu précédent, la somme des termes de gauche fait $2\cdot(a(0)+a(1)+b(0)+b(1)+c(0)+c(1))$ ce qui est paire. Malheureusement, la somme des termes de droite est impaire. Il n'existe donc pas de fonctions $a(x), b(y), c(z)$ satisfaisant toutes les contraintes.

Une stratégie, similaire au jeu précédent, atteint 75% pour $n = 3$, où il suffit que tous les joueurs choisissent, conjointement via 2 bits aléatoires partagés, une des quatre contraintes à ne pas respecter, et résolvent ainsi le système modifié. Par exemple, si c'est la 3e équation que les joueurs décide de ne pas respecter, alors $a(x) = c(z) = 0$ et $b(y) = y$ est une solution. Et si c'est la 1ère, c'est encore plus simple, puisque $a(x) = b(y) = c(z) = 1$ est une solution.

De manière générale, on peut montrer qu'aucune stratégie, même celle utilisant des bits aléatoires partagées, ne peut gagner à ce jeu avec une probabilité plus grande que $\frac{1}{2}+\left(\frac{1}{2}\right)^{\lceil n/2\rceil}$ où n est le nombre de joueurs. Pour $n = 3$, cela fait $\frac{1}{2}+\left(\frac{1}{2}\right)^2 = \frac{3}{4} = 75\%$.

Si maintenant les trois participants Alice, Bob et Carole, possèdent chacun un qubit préalablement intriqués dans l'état

$$|A,B,C\rangle \;=\; \frac{1}{2}|000\rangle - \frac{1}{2}|011\rangle - \frac{1}{2}|101\rangle - \frac{1}{2}|110\rangle$$

alors ils peuvent gagner à 100% (cf. [BCMdW10, §A.]). L'algorithme consiste à faire une mesure sur chacun des qubits selon la base de calcul si l'entrée vaut 0 et selon la base d'Hadamard $\{H|0\rangle, H|1\rangle\} = \left\{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right\}$ si l'entrée vaut 1. Il se trouve que

$$H \;=\; \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \;=\; R(\pi/4) \qquad \text{(cf. l'équation (10.2).)}$$

On peut montrer que mesurer selon la base d'Hadamard revient en fait à appliquer H puis à effectuer une mesure selon la base de calcul.

Si $xyz = 000$, les trois mesures de l'état $|A,B,C\rangle$ se font selon la base de calcul et donc donneront $a+b+c \equiv 0$ dans 100% des cas car l'état est une superposition d'états ayant un nombre pair de 1. Si $xyz = 011$, cela revient à faire une mesure selon la base de calcul

sur l'état :

$$\begin{aligned}(I\otimes H\otimes H)\cdot|A,B,C\rangle &= (I\otimes H\otimes H)\cdot\left(\frac{1}{2}|000\rangle-\frac{1}{2}|011\rangle-\frac{1}{2}|101\rangle-\frac{1}{2}|110\rangle\right)\\ &= (I\otimes H\otimes H)\cdot\left(\frac{1}{2}|0\rangle(|00\rangle-|11\rangle)-\frac{1}{2}|1\rangle(|01\rangle+|10\rangle)\right)\\ &= \frac{1}{2}|0\rangle(|01\rangle+|10\rangle)-\frac{1}{2}|1\rangle(|00\rangle-|11\rangle)\\ &= \frac{1}{2}|001\rangle+\frac{1}{2}|010\rangle-\frac{1}{2}|100\rangle+\frac{1}{2}|111\rangle\end{aligned}$$

et donc $a+b+c\equiv 1$ après mesures dans 100% des cas, puisqu'il s'agit d'une superposition d'état ayant un nombre impair de 1. Les autres cas ($xyz=101$ et $xyz=110$) se traitent de manière similaire.

Il est à noter que le résultat n'est pas déterministe : pour les mêmes entrées la sortie peut être différente. Cependant les joueurs gagnent le jeu à coup sûr.

10.7 Le modèle φ-LOCAL

Dans un jeu à deux joueurs, l'hypothèse *non-signalling* signifie que le choix de mesure d'un joueur n'est pas *signalé* à l'autre. Et en physique le choix de la mesure est l'analogue de l'entrée en informatique, la donnée qui va déterminer le calcul. Donc dans un modèle de calcul multi-joueurs respectant l'hypothèse *non-signalling*, la sortie d'un joueur ne peut dépendre de l'entrée d'un autre sans communication. Il est par contre autorisé que les sorties soient corrélées. C'est précisément ce qu'il se passe dans le modèle quantique : il y a corrélation (entre sorties distantes) sans pour autant être *signalling* (entre entrées et sorties distantes).

Dans cette extension *non-signalling* du modèle local, nommée φ-LOCAL comme *physical locality*, on s'autorise toutes les correlations (potentiellement non locales) des résultats, sans toute fois autoriser celles qui découlent d'une communication instantanée à distance. Donc dans le modèle φ-LOCAL à distance t on s'autorise tout sauf de communiquer au-delà de nœuds à distance t en t unités de temps (ou rondes). La non communication entre deux nœuds quelconques suffisamment loin s'exprime par le fait que les sorties de l'un d'entre eux sont indépendantes des entrées de l'autre. Et plus généralement, les sorties conjointes d'un groupe de nœuds (on parle de distribution des marginales) sont indépendantes des entrées de tout groupe de sommets suffisamment éloignés.

Plus formellement, lorsque deux sommets A et B ne sont pas en mesure de communiquer, cela signifie que pour une entrée (x,y), le résultat (a,b) doit vérifier :

$$\Pr(a|x,y)=_{\text{def}}\sum_b \Pr(a,b|x,y)=\Pr(a|x)\quad\text{et}\quad \Pr(b|x,y)=_{\text{def}}\sum_a \Pr(a,b|x,y)=\Pr(b|y)\,.$$

Dit autrement, la première somme doit être indépendante de y alors que la seconde indépendante de x.

Par exemple, la distribution suivante vérifie cette propriété, étant sous-entendu que les lignes absentes arrivent avec une probabilité nulle comme par exemple $\Pr(a=0,b=1|x=0,y=0)=0$. Pour résumer la distribution, on sort 00 ou 11 avec probabilité 1/2 sauf lorsqu'on a $x=y=1$. Dans ce cas on sort 01 ou 10 avec probabilité 1/2.

x	y	a	b	Pr
0	0	0	0	1/2
		1	1	1/2
0	1	0	0	1/2
		1	1	1/2
1	0	0	0	1/2
		1	1	1/2
1	1	0	1	1/2
		1	0	1/2

En effet, $\Pr(a=0|x,y)=1/2$ quels que soient x et y. De même $\Pr(a=1|x,y)=1/2$. Donc $\Pr(a|x,y)=\Pr(a|x)$. Et de manière similaire, on vérifie que $\Pr(b=0|x,y)=\Pr(b=1|x,y)=1/2$ quels que soient x et y. Cette distribution est donc *non-signalling* : a et b sont corrélées, mais à partir de a on ne tire aucune information sur y, et à partir de b on ne tire aucune information sur x.

On remarquera que $a \oplus b = x \wedge y$. Autrement dit, dans ce modèle, Alice et Bob gagnent au jeu CHSH avec une probabilité de 100%.

[*Cyril*. À FINIR]

On peut vérifier que les distributions issues des propositions 10.2 et 10.4 sont également *non-signalling*.

...

On peut étendre la propriété de non communication (ou *non-signalling*) de la manière suivante. Tout d'abord une *tâche* sur un graphe G de sommets $v_1,\dots,v_n$ est une fonction faisant correspondre, pour tout sommet v_i, une entrée x_i avec une sortie a_i. On notera $\vec{x}=(x_1,\dots,x_n)$ et $\vec{a}=(a_1,\dots,a_n)$.

...

Bibliographie

[Bar06] J. Barrett, *Information processing in generalized probabilistic theories*, Tech. Rep. 0508211v3 [quant-ph], arXiv, November 2006.

[BCMdW10] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, *Nonlocality and communication complexity*, Reviews of Modern Physics, 82 (2010), pp. 665–697. doi : 10.1103/RevModPhys.82.665.

[Boy04] M. Boyer, *On Mermin's n-player games parity game*, August 2004. www.iro.umontreal.ca/~boyer/mermin.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Physical Review Letters, 23 (1969), pp. 880–883. doi : 10.1103/PhysRevLett.23.880.

[Cir80] B. Cirel'son, *Quantum generalizations of Bell's inequality*, Letters in Mathematical Physics, 4 (1980), pp. 93–100. doi : 10.1007/BF00417500.

[CK06] J. H. Conway and S. Kochen, *The free will theorem*, Foundations of Physics, 36 (2006), pp. 1441–1473. doi : 10.1007/s10701-006-9068-6.

[DHFRW20] E. Dable-Heath, C. J. Fewster, K. Rejzner, and N. Woods, *Algebraic classical and quantum field theory on causal sets*, Tech. Rep. 1908.01973v3 [math-ph], arXiv, February 2020.

[FGZ+19] Y. Y. Fein, P. Geyer, P. Zwick, F. Kiałka, S. Pedalino, M. Mayor, S. Gerlich, and M. Arndt, *Quantum superposition of molecules beyond 25 kDa*, Nature Physics, 15 (2019), pp. 1242–1245. doi : 10.1038/s41567-019-0663-9.

[Gav25] C. Gavoille, *Analyse d'algorithme – Cours d'introduction à la complexité paramétrique et aux algorithmes d'approximation*, 2025. !MYHTTP/UE-AA/cours.pdf. Notes de cours.

[GHZ89] D. M. Greenberger, M. A. Horne, and A. Zeilinger, *Going beyond Bell's Theorem*, in Bell's Theorem, Quantum Theory, and Conceptions of the Universe, Kluwer, 1989, pp. 69–72.

[HBD+15] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres*, Nature, 526 (2015), pp. 682–686. doi : 10.1038/nature15759.

[Kal19] G. Kalai, *The argument against quantum computers*, Tech. Rep. 1908.02499 [quant-ph], arXiv, August 2019.

[Mer85] N. D. Mermin, *Is the moon there when nobody looks ? Reality and the quantum theory*, Physics Today, 38 (1985), pp. 38–47. doi : 10.1063/1.880968.

[RP00] E. Rieffel and W. Polak, *An introduction to quantum computing for non-physicists*, ACM Computing Surveys, 32 (2000), pp. 300–335. doi : 10.1145/367701.367709.

[SBB+08] D. Salart, A. Baas, C. Branciard, N. Gisin, and H. Zbinden, *Testing the speed of 'spooky action at a distance'*, Nature, 454 (2008), pp. 861–864. doi : 10.1038/nature07121.

[Teo16] M. Teodorani, *Entanglement : l'intrication quantique, des particules à la conscience*, Macro Edition, 2016.