Mécanique quantique I

Séance d'exercices n°8 : Information Quantique

L'unité de base d'information est le *bit* qui peut prendre deux valeurs : conventionnellement 0 et 1. Pour le traitement et le transfert de l'information, les *bits* sont encodés dans des systèmes physiques à 2 états comme par exemple deux valeurs différentes d'une tension ou d'une charge, ou deux directions de magnétisation. On peut faire de même au niveau quantique : encoder le 0 et le 1 dans les états notées $|0\rangle$ et $|1\rangle$ d'un système quantique à 2 niveaux. Un tel système est appelé un *quantum bit* ou *qubit*. Ceci donne un avantage important à l'information quantique. La raison principale en est la possibilité pour un *qubit* $|\phi\rangle$ d'être dans une superposition cohérente des états $|0\rangle$ est $|1\rangle$, c'est-à-dire qu'il peut se trouver dans un état de la forme

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{1}$$

où α et β sont des nombres complexe avec la contrainte de normalisation $|\alpha|^2 + |\beta|^2 = 1$.

Parallélisme quantique

Encodons une séquence de n bits dans un système de n spins 1/2 dans lequel les spins sont orientés suivant l'axe z et où la direction *up* est associé à 0 et la direction *down* est associé à $1s$. On suppose que l'état initial est dans un état produit, par exemple de la forme $|0\rangle|0\rangle|1\rangle...|0\rangle|1\rangle$.

Question 1 : Combien de combinaisons différentes possibles de 0 et de 1 existe-t-il dans un système classique de n bits ? Appelons ce nombre M.

Un système classique de n bits a donc M états distincts, chacun étant décrit par une chaîne de n valeurs binaires. D'autre part, chaque qubit est un vecteur dans un espace complexe bidimensionnel. Pour un système de n qubits, on a donc M états quantiques distincts correspondant aux M chaînes de n bits possibles. Ces M états sont décrits par M vecteurs orthogonaux, qui forment la base de l'espace de Hilbert total. Un état quelconque est alors une superposition cohérente de ces M vecteurs de base.

En d'autres termes, un état quantique dans l'espace complexe M-dimensionnel nécessite M nombres complexes indépendants pour sa description (à la normalisation près). Si on souhaite simuler un tel état avec des bits classiques (sur un PC par exemple) et que l'on essaye de décrire l'application d'une transformation unitaire, il devient nécessaire de manipuler un nombre de paramètres réels bien au-delà de ce qu'il est en fait possible de réaliser avec les ordinateurs actuels.

Question 2 : Calculez le nombre de paramètres réels nécessaires pour écrire une transformation unitaire dans un espace de Hilbert de dimension M. Que vaut ce nombre pour un système de 200 qubits ? En utilisant l'approximation $10^3 \approx 2^{10}$, comparez ce nombre avec le nombre de particules élémentaires dans l'univers, évalué à 10^{80} particules.

Notez toutefois qu'une opération unitaire peut être réalisée directement (et en une seule fois) sur le système de qubits, car cela correspond simplement à l'évolution temporelle donnée par l'équation de Schrödinger, par exemple en jouant sur un champ électromagnétique externe. C'est ce qu'on appelle le parallélisme quantique et c'est là que réside une des grande force du calcul

http ://quic.ulb.ac.be, ahertz@ulb.ac.be

quantique. Le parallélisme permet de réduire de façon exponentielle le nombre d'opérations à effectuer et rend donc les algorithmes quantiques plus puissants. Comme exemple d'algorithme quantique connu plus puissant que son homologue classique, on peut citer l'algorithme de Shor. En utilisant des opérations unitaires cet algorithme permet de factoriser de très grands nombres, en un nombre d'étapes élémentaires (portes logiques quantiques) qui augmente seulement de façon polynomiale (c'est proportionnel à une puissance de la taille du nombre à factoriser). Ceci est très intéressant car le meilleur algorithme classique connu réalise la même opération en un nombre d'étapes (donc en un temps) qui est exponentiel en la taille du nombre.

Théorème du non-clonage quantique (*No-cloning theorem*)

Le théorème de non-clonage s'exprime ainsi : *il est impossible de créer des copies parfaites d'un état quantique inconnu tiré d'un ensemble d'états non-orthogonaux.*

Supposons qu'il existe un opérateur unitaire, qui produit des copies parfaites des états $|0\rangle$ et $|1\rangle$. Les états de sortie d'une telle opération sont des états à deux qubits, un pour conserver l'original et un pour recevoir la copie. Cependant pour assurer l'unitarité de l'opérateur on a aussi besoin d'un second système d'entrée, arbitraire mais qui est le même pour tous les états et qui ne ne doit pas dépendre de l'état d'entrée. En tout généralité on peut choisir cet état qui joue le rôle d'une *page blanche* comme l'état $|0\rangle$. Dans ces conditions l'opérateur en question U agit de la manière suivante :

$$\begin{aligned} U|0\rangle|0\rangle &= |0\rangle|0\rangle \\ U|1\rangle|0\rangle &= |1\rangle|1\rangle \end{aligned}$$

Cet opérateur existe parce qu'il ne viole pas le théorème de non-clonage : il fait des copies parfaites d'états orthogonaux. Mais comment cet opérateur agit-il sur un état arbitraire $|\varphi\rangle$? Est-ce qu'on aura toujours un clonage parfait :

$$U|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle \quad ?$$

Question 3 : Prouvez le théorème en faisant agir l'opérateur U sur l'état général superposé $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ qui n'est pas orthogonal à $|0\rangle$ et $|1\rangle$. Pour cela, utilisez la définition (présentée au-dessus) de l'action de U sur les états de deux qubits et la linéarité de l'opérateur.

Notez que la condition selon laquelle l'état doit être tiré d'un ensemble d'états non-orthogonaux est essentielle. En effet, si on sait que l'état qu'on veut cloner fait partie d'un ensemble donné d'états orthogonaux les uns aux autres, on peut construire une observable pour laquelle ces états seront les états de base. Dans ce cas la mesure de cette observable nous donnerait l'information complète sur l'état. Si on sait quel est l'état en question, en principe on peut recréer autant de copies que l'on veut. Toutefois, puisque seul des copies des états orthogonaux sont possible, on n'a pas une opération universelle (c'est-à-dîre une opération qui permet de cloner n'importe quel état).

L'impossibilité de copier un état quantique inconnu peut être exploitée pour la distribution d'une clé secrète (une séquence aléatoire de bits 0 et 1) entre deux parties A (Alice) et B (Bob) pour la protection de l'information transmise dans un canal de communication. Si la clé est encodée dans des états quantiques, pour connaitre la valeur des bits de la clé transmise par le canal, l'espion éventuel doit copier des états inconnus, ce qui en vertu du théorème est impossible (évidemment les états doivent être tirés d'un ensemble qui contient des états non-orthogonaux). L'espion peut choisir quand-même d'intercepter les signaux quantiques, de

les mesurer puis d'en créer de nouveaux à partir des mesures pour les renvoyer à la bonne destination. Comme l'état est inconnu, l'espion ne connait pas la base dans laquelle sa mesure donne un résultat déterministe, cette mesure ne peut donc pas être toujours parfaite. Ainsi l'espion ne peut pas parfaitement connaitre l'état inconnu et s'il envoie dans le canal quantique des états qu'il a reconstruit sur la base de l'information incomplète il va créer les erreurs. On peut créer des protocoles de communication où ces erreurs (et de ce fait l'espion lui-même) peuvent toujours être détectées, indiquant que la clé distribuée n'est pas sécurisée. On abandonne alors cette clé et comme aucune information n'a été transmise la sécurité est toujours assurée. Si on conclut qu'il n'y a pas eu l'intervention d'un espion dans la transmission, on peut utiliser la clé distribuée en toute sécurité. Ceci est totalement différent de ce qui ce passe dans un protocole classique où il est impossible de savoir si l'espion a observé le signal transmis par le canal. C'est une vision un peu simpliste mais elle présente les raisons de pourquoi on peut utiliser la mécanique quantique pour sécuriser la transmission de l'information. En 1983, un premier protocole quantique (BB84) à été proposé, pouvant distribuer une clé secrète entre deux parties A (Alice) et B (Bob) en assurant une sécurité en principe absolue.

Intrication et téléportation quantique

Une ressource importante pour l'information quantique est *l'intrication quantique*. Un état de deux (ou plusieurs) qubits est intriqué si il ne peut pas être représenté comme un état produit, c'est-à-dire, un état de la forme :

$$(\alpha_1 |0\rangle + \beta_1 |1\rangle)\ (\alpha_2 |0\rangle + \beta_2 |1\rangle).$$

Exemple : *Les états de Bell*, définis dans le problème suivant sont intriqués parce qu'ils ne peuvent pas être représentés comme des états produits,

Question 4 : Prouvez que les états de Bell $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Phi^-\rangle$, définis par

$$\begin{aligned} |\Phi^+\rangle &= (|0\rangle |0\rangle + |1\rangle |1\rangle)/\sqrt{2} \\ |\Phi^-\rangle &= (|0\rangle |0\rangle - |1\rangle |1\rangle)/\sqrt{2} \\ |\Psi^+\rangle &= (|0\rangle |1\rangle + |1\rangle |0\rangle)/\sqrt{2} \\ |\Psi^-\rangle &= (|0\rangle |1\rangle - |1\rangle |0\rangle)/\sqrt{2} \end{aligned} \tag{2}$$

forment une base de l'espace de Hilbert de deux qubits. Pour souligner quel qubit appartient à Alice (A) et quel qubit appartient à Bob (B) on écrit aussi

$$|\Phi^+\rangle = (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)/\sqrt{2}. \tag{3}$$

Que se passe-t-il si on applique un opérateur d'inversion de bit σ_x (voir équation (6)) ou d'inversion de signe σ_z (voir équation (7)) sur le qubit de Alice ou le qubit de Bob dans l'état $|\Phi^+\rangle$.

Les états de Bell sont des états avec une intrication *maximale*. En particulier, ils saturent une mesure quantitative de l'intrication, l'entropie de Von Neumann.

Remarquez que trois des quatre états sont symétriques sous permutation du premier et deuxième qubit, et que le quatrième état est antisymétrique. De plus, comme un qubit correspond à un spin 1/2, deux qubits forment un système dont le spin total est soit $S = 0$, soit $S = 1$ (par les lois de composition d'un moment cinétique). Pour ces raisons les trois états symétriques forment un état *triplet* ($S = 1$) tandis que l'état antisymétrique forme un état *singulet* ($S = 0$).

Question 5 : Indiquez quels sont les états de Bell qui forment les états triplets et l'état singulet.

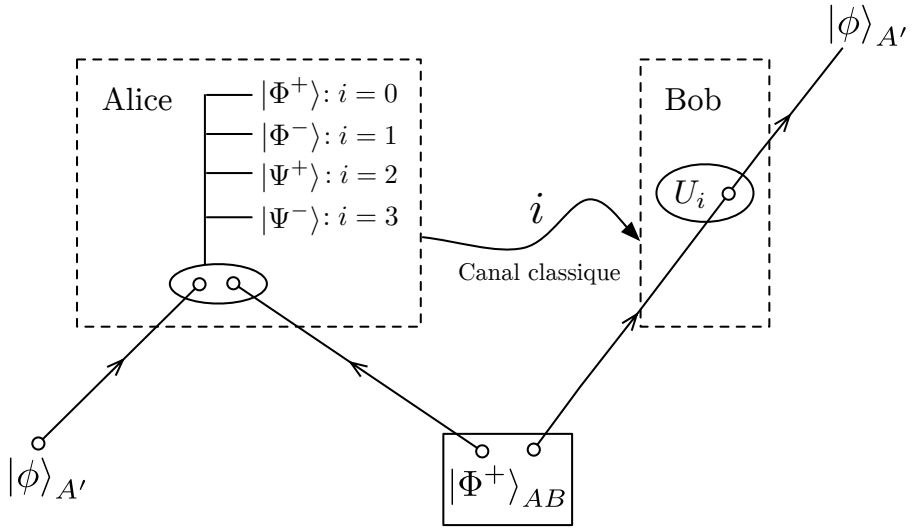

FIGURE 1 – Téléportation quantique.

Il est important de noter que l'état global de deux qubits peut rester inchangé même si les systèmes physiques correspondant sont séparés d'une grande distance, de sorte que des systèmes arbitrairement éloignés peuvent rester intriqués. Cette propriété nous permet la *téléportation* de l'état inconnu d'un système quantique d'un endroit à un autre endroit plus éloigné. Ce protocole utilise un état intriqué comme ressource.

Supposons que deux personnes, Alice et Bob, partagent le même état de Bell, disons $|\Phi^+\rangle_{AB}$, d'une manière que le premier qubit appartient à Alice et le deuxième à Bob. Techniquement, ceci peut-être réalisé expérimentalement en utilisant un état intriqué à deux photons, créé a partir d'un cristal non-linéaire. Un photon est envoyé par une fibre optique à Alice, l'autre photon est envoyé à Bob. Dans ce cas Alice et Bob partagent un état intriqué.

Nous allons montrer maintenant que si Alice a un troisième photon qui est dans un état inconnu $|\phi\rangle_{A'}$, donné par

$$|\phi\rangle_{A'} = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{4}$$

en mesurant et en envoyant le résultat (donné par deux bits classiques) à Bob, Il peut reconstruire *parfaitement* l'état $|\phi\rangle$. Rappelons que $|\phi\rangle$ est complètement inconnu d'Alice, et qu'elle n'envoie pas à Bob l'état lui-même mais seulement le résultat des mesures qu'elle à pratiquée, c'est-à-dire de l'information classique et non quantique. Nous allons aussi voir que sans l'état intriqué $|\Phi^+\rangle_{AB}$, partagé par Alice et Bob, l'information classique envoyée par Alice ne permet pas de reconstruire $|\phi\rangle$.

Avant de traiter le protocole de téléportation quantique, nous allons résoudre le problème suivant :

Question 6 : On suppose que

$$|\Psi\rangle_{A'AB} = |\phi\rangle_{A'}\,|\Phi^+\rangle_{AB}$$

où $|\phi\rangle$ est l'état d'un qubit défini dans l'équation (1) **et $|\Phi^+\rangle$ est l'état de Bell défini dans l'équation** (2)**.**

Montrez que par des opérations algébriques on peut représenter $|\Psi\rangle_{A'AB}$ sous la forme suivante,

$$|\Psi\rangle_{A'AB} = \frac{1}{2}\left[|\Phi^+\rangle_{A'A}\,|\phi_0\rangle_B + |\Phi^-\rangle_{A'A}\,|\phi_1\rangle_B + |\Psi^+\rangle_{A'A}\,|\phi_2\rangle_B + |\Psi^-\rangle_{A'A}\,|\phi_3\rangle_B\right], \tag{5}$$

où les états $|\phi_i\rangle$ sont différents états du qubit de Bob.

Puis, montrez qu'en appliquant une séquence appropriée d'opérations d'inversions de bits ou de signe (voir équations (6) et (7) ci-dessous) on peut transformer chacun de ces états $|\phi_i\rangle$ en l'état $|\phi\rangle$.

La représentation obtenue permet à Alice et Bob d'effectuer le protocole de téléportation, représenté schématiquement sur la Fig. 1 :

1. Alice et Bob partagent un système à deux qubit intriqués, de telle manière qu'Alice possède le premier qubit et Bob le deuxième qubit. Cet état est l'état de Bell $|\Phi^+\rangle$.
2. Alice reçoit un troisième qubit qui est dans un état inconnu $|\phi\rangle$.
3. Alice applique une mesure jointe aux deux qubits qu'elle possède : le qubit dans l'état inconnu $|\phi\rangle$ et *sa moitié* de l'état de Bell $|\Phi^+\rangle$. Elle obtient un résultat qui indique dans quel état de Bell sont *ses deux qubits*. Ce résultat est encodé sous la forme d'un des nombres suivants $i = 0, 1, 2, 3$ (pouvant être représenté par 2 bits).
4. Le résultat est transmis à Bob par un canal classique.
5. En utilisant le résultat d'Alice, Bob *sait* quelle transformation unitaire (qui contient des inversions de bits et de signe) il doit appliquer à *sa moitié* de l'état de Bell $|\Phi^+\rangle$, et ainsi reconstruire l'état $|\phi\rangle$.

En conclusion, on voit que l'on peut parfaitement téléporter un état inconnu sans le mesurer. De plus, on remarque que l'information classique envoyée à Bob (2 bits) est insuffisante pour reconstruire toute seule l'état $|\phi\rangle$ (2 paramètres réels).

L'inégalité de Bell

On sait que la mécanique quantique interdit de mesurer *simultanément* deux observables $\hat{A}$ et $\hat{B}$ avec une précision arbitraire, s'ils ne commutent pas :

$$\langle(\Delta\hat{A})^2\rangle \, \langle(\Delta\hat{B})^2\rangle \geq \frac{1}{4} |\, \langle[\hat{A}, \hat{B}]\rangle \,|^2.$$

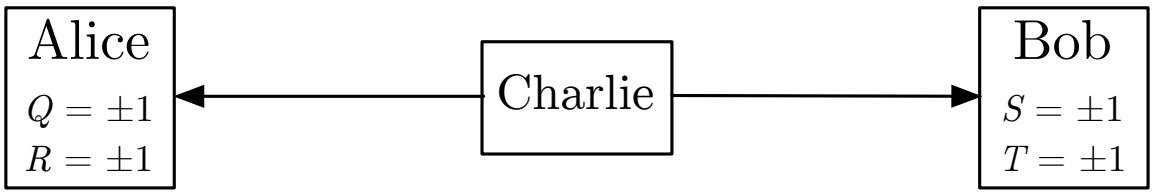

FIGURE 2 – Schéma expérimental.

Considérons l'expérience suivante : un émetteur, Charlie, envoie une particule à Alice et une deuxième particule à Bob. Alice peut mesurer (sans savoir quelle mesure elle va effectuer) deux propriétés physiques Q et R de sa particule. Chaque propriété peut prendre les valeurs ± 1. De son coté, Bob peut mesurer deux autres propriétés S et T, qui peuvent aussi prendre les valeurs ± 1. Alice et Bob mesurent simultanément leurs particules. Le schéma expérimental est montré sur la Fig. 2.

Question 7 : Quelles valeurs peut prendre la quantité $QS + RS + RT - QT$.

Supposons que $p(q, r, s, t)$ soit la probabilité jointe qu'avant les mesures d'Alice et de Bob, le système soit *simultanément* dans l'état $Q = q, R = r, S = s, T = t$. L'existence simultanée des valeurs q, r, s et t et par conséquent l'existence de la probabilité jointe est une hypothèse habituelle de la physique classique.

Question 8 : Trouvez une borne supérieur pour $E(QS)+E(RS)+E(RT)-E(QT)$, où $E(.)$ est l'espérance mathématique. *Indice : Utilisez la linéarité de l'espérance.*

L'inégalité obtenue est appelée *inégalité de Bell* ou *inégalité de CHSH* d'après "John Clauser, Michael Horne, Abner Shimony and Richard Holt".

Supposant maintenant que Charlie envoie deux particules, où chaque particule possède un spin 1/2. L'état quantique global du système est donné par l'état intriqué suivant (état de Bell)

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Ensuite Alice et Bob mesurent les *observables* données par

$$\hat{Q} = Z_1, \quad \hat{S} = \frac{-Z_2 - X_2}{\sqrt{2}},$$
$$\hat{R} = X_1, \quad \hat{T} = \frac{Z_2 - X_2}{\sqrt{2}},$$

avec $X_1 = \sigma_x \otimes \mathbb{I}, X_2 = \mathbb{I} \otimes \sigma_x, Z_1 = \sigma_z \otimes \mathbb{I}, Z_2 = \mathbb{I} \otimes \sigma_z$, où $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ est l'identité et σ_x, σ_z sont les matrices de Pauli (voir ci-dessous).

Question 9 : Calculez $\langle\Psi^-| QS |\Psi^-\rangle + \langle\Psi^-| RS |\Psi^-\rangle + \langle\Psi^-| RT |\Psi^-\rangle - \langle\Psi^-| QT |\Psi^-\rangle$ et interprétez le résultat. *Aide : Utilisez les propriétés (6) et (7) des matrices de Pauli (voir ci-dessous), ainsi que l'égalité suivante :*

$$(A \otimes B)(|0\rangle |0\rangle) = (A |0\rangle)(B |0\rangle).$$

Rappel : Matrices de Pauli

Les trois matrices de Pauli sont :

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Elles vérifient les relations suivantes :

$$\sigma_x\sigma_y = i\sigma_z, \qquad \sigma_y\sigma_z = i\sigma_x, \qquad \sigma_z\sigma_x = i\sigma_y.$$

Ces matrices sont à la fois hermitiennes et unitaires. En tant que matrices hermitiennes, $\sigma_x/2$, $\sigma_y/2$ et $\sigma_z/2$ vérifient les opérations de commutation d'un moment cinétique, et représentent en effet l'opérateur de spin pour une particule de spin 1/2. En tant que matrices unitaires, elles correspondent à différentes opérations sur un qubit :

1. σ_x implémente une *inversion de bit* :

$$\sigma_x |0\rangle = |1\rangle \qquad \sigma_x |1\rangle = |0\rangle \tag{6}$$

2. σ_z implémente une *inversion de signe* :

$$\sigma_z |0\rangle = |0\rangle \qquad \sigma_z |1\rangle = -|1\rangle \tag{7}$$

3. σ_y implémente, à une phase globale prés, une inversion de signe suivie d'une inversion de bit (puisque $\sigma_y = i\sigma_x\sigma_z$)