Mécanique Quantique 1 —– CORRIGÉ

Séance d'éxercices 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 potentiellement un avantage important à la manipulation de l'information quantique. Une raison principale 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 un tel état à 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 1. 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.*
Pour un système classique de n bits, il existe $M = 2^n$ combinaisons différentes de 0 et de 1.
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 mots, 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.*
Une transformation unitaire $\hat{U}$ (par définition telle que $\hat{U}^\dagger = \hat{U}^{-1}$) dans un espace de Hilbert de dimension $M = 2^n$ est nécessairement représentée par une matrice $2^n \times 2^n$. Les éléments de la matrice étant complexes, on en déduit que le nombre de paramètres réels indépendants est donné par 2.2^{2n}. Pour 200 qubits, on a $2.2^{2.200} \approx 2.10^{120}$ paramètres nécessaires pour écrire une transformation unitaire (sans prendre en compte la condition d'unitarité ou de normalisation). Sachant que $10^{120} \gg 10^{80}$, on voit que le nombre de paramètres qu'il faudrait manipuler pour écrire ce genre de transformation est en fait gigantesque.
D'un autre coté, une opération unitaire peut être directement réalisée 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. Cette comparaison permet de cerner le potentiel computationnel d'un système quantique, grâce au parallélisme évoqué. Un exemple de ce potentiel est illustré par l'algorithme de Shor : En utilisant des opérations unitaires il est possible de factoriser de grands nombres, en un nombre d'étapes élémentaires (portes logiques quantiques) qui augmente seulement comme 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*)

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 :

$$\begin{aligned} U|0\rangle|0\rangle &= |0\rangle|0\rangle \\ U|1\rangle|0\rangle &= |1\rangle|1\rangle \end{aligned} \tag{2}$$

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 du non clonage quantique 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* (2) *de l'action de* U *sur les états de deux qubits et la linéarité de l'opérateur.* On a

$$\begin{aligned} U|\varphi\rangle|0\rangle &= U\left(\alpha|0\rangle + \beta|1\rangle\right)|0\rangle \\ &= \alpha U|0\rangle|0\rangle + \beta U|1\rangle|0\rangle \\ &= \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \\ &\neq |\varphi\rangle|\varphi\rangle \end{aligned}$$

ce qui montre que, malgré que l'opérateur U permette de copier les états d'une base orthogonale, il ne permet pas de copier un état $|\varphi\rangle$ étant une superposition des états de la base.

On voit donc 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 de cet état que l'on veut.
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 connaître 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 connaît 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 connaître 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 pour lesquelles on peut utiliser la mécanique quantique pour sécuriser la transmission de l'information. En 1983, un premier protocole quantique (BB84) à été proposé, permettant de distribuer une clé secrète entre deux parties A (Alice) et B (Bob) tout en assurant une sécurité en principe absolue.

Intrication et téléportation quantique

Une ressource importante pour l'information quantique réside dans la notion *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 :

$$(\alpha_1 |0\rangle + \beta_1 |1\rangle)\ (\alpha_2 |0\rangle + \beta_2 |1\rangle). \tag{3}$$

Dans cette dernière expression, le premier facteur $\alpha_1 |0\rangle + \beta_1 |1\rangle$ caractérise le premier système (premier qubit), alors que le second facteur $\alpha_2 |0\rangle + \beta_2 |1\rangle$ caractérise le second système (second qubit). On voit donc que dans l'expression (5), on a pu "séparer" les deux systèmes (on parle en toute généralité d'état séparable).
Exemple : *Les états de Bell*, définis comme

$$\begin{aligned} |\Phi^+\rangle &= (|0\rangle |0\rangle + |1\rangle |1\rangle)/\sqrt{2} \\ |\Phi^-\rangle &= (|0\rangle |0\rangle - |1\rangle |1\rangle)/\sqrt{2} \\ |\Psi^+\rangle &= (|0\rangle |1\rangle + |1\rangle |0\rangle)/\sqrt{2} \\ |\Psi^-\rangle &= (|0\rangle |1\rangle - |1\rangle |0\rangle)/\sqrt{2} \end{aligned} \tag{4}$$

sont intriqués parce qu'ils ne peuvent pas être représentés comme des états produits de la forme (5).

Intrication et téléportation quantique

Une ressource importante pour l'information quantique réside dans la notion *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 :

$$(\alpha_1 |0\rangle + \beta_1 |1\rangle)\ (\alpha_2 |0\rangle + \beta_2 |1\rangle). \tag{5}$$

Dans cette dernière expression, le premier facteur $\alpha_1 |0\rangle + \beta_1 |1\rangle$ caractérise le premier système (premier qubit), alors que le second facteur $\alpha_2 |0\rangle + \beta_2 |1\rangle$ caractérise le second système (second qubit). On voit donc que dans l'expression (5), on a pu "séparer" les deux systèmes (on parle en toute généralité d'état séparable).
Exemple : *Les états de Bell*, définis comme

$$\begin{aligned} \left|\Phi^+\right\rangle &= (|0\rangle |0\rangle + |1\rangle |1\rangle)/\sqrt{2} \\ \left|\Phi^-\right\rangle &= (|0\rangle |0\rangle - |1\rangle |1\rangle)/\sqrt{2} \\ \left|\Psi^+\right\rangle &= (|0\rangle |1\rangle + |1\rangle |0\rangle)/\sqrt{2} \\ \left|\Psi^-\right\rangle &= (|0\rangle |1\rangle - |1\rangle |0\rangle)/\sqrt{2} \end{aligned} \tag{6}$$

sont *intriqués* parce qu'ils ne peuvent pas être représentés comme des états produits de la forme (5).

Question 4.

(a) *Prouvez que les états de Bell* $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Phi^-\rangle$, *définis par le système* (6), *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, par exemple,*

$$\left|\Phi^+\right\rangle = (|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)/\sqrt{2}. \tag{7}$$

(b) *Que se passe-t-il si on applique un opérateur d'inversion de bit* σ_x *(voir* (42) *et* (43) *dans le Rappel) ou d'inversion de signe* σ_z *(voir équation (7) dans le Rappel) sur le qubit de Alice ou le qubit de Bob dans l'état* $|\Phi^+\rangle$.

(a) Les etats de Bell forment une base si et seulement si

$$\begin{cases} \langle\Phi^+|\Phi^+\rangle = 1 \\ \langle\Phi^-|\Phi^-\rangle = 1 \\ \langle\Psi^+|\Psi^+\rangle = 1 \\ \langle\Psi^-|\Psi^-\rangle = 1 \end{cases} \text{ et } \begin{cases} \langle\Phi^+|\Phi^-\rangle = 0 \\ \langle\Phi^+|\Psi^+\rangle = 0 \\ \langle\Phi^+|\Psi^-\rangle = 0 \\ \langle\Phi^-|\Psi^+\rangle = 0 \\ \langle\Phi^-|\Psi^-\rangle = 0 \\ \langle\Psi^+|\Psi^-\rangle = 0 \end{cases} \tag{8}$$

On a

$$\begin{aligned} \langle\Phi^+|\Phi^+\rangle &= (\langle 0|\langle 0| + \langle 1|\langle 1|)(|0\rangle |0\rangle + |1\rangle |1\rangle)/2 \\ &= \left(\underbrace{\langle 0|0\rangle\langle 0|0\rangle}_{=1} + \underbrace{\langle 0|1\rangle\langle 0|1\rangle}_{=0} + \underbrace{\langle 1|0\rangle\langle 1|0\rangle}_{=0} + \underbrace{\langle 1|1\rangle\langle 1|1\rangle}_{=1}\right)/2 \\ &= 1 \end{aligned} \tag{9}$$

De même,

$$\langle\Phi^-|\Phi^-\rangle = \left(\underbrace{\langle 0|0\rangle\langle 0|0\rangle}_{=1} - \underbrace{\langle 0|1\rangle\langle 0|1\rangle}_{=0} - \underbrace{\langle 1|0\rangle\langle 1|0\rangle}_{=0} + \underbrace{\langle 1|1\rangle\langle 1|1\rangle}_{=1}\right)/2 = 1, \tag{10}$$

$$\langle\Psi^+|\Psi^+\rangle = \left(\underbrace{\langle 0|0\rangle\langle 1|1\rangle}_{=1} + \underbrace{\langle 0|1\rangle\langle 1|0\rangle}_{=0} + \underbrace{\langle 1|0\rangle\langle 0|1\rangle}_{=0} + \underbrace{\langle 1|1\rangle\langle 0|0\rangle}_{=1}\right)/2 = 1, \tag{11}$$

et

$$\langle\Psi^-|\Psi^-\rangle = \left(\underbrace{\langle 0|0\rangle\langle 1|1\rangle}_{=1} - \underbrace{\langle 0|1\rangle\langle 1|0\rangle}_{=0} - \underbrace{\langle 1|0\rangle\langle 0|1\rangle}_{=0} + \underbrace{\langle 1|1\rangle\langle 0|0\rangle}_{=1}\right)/2 = 1. \tag{12}$$

D'autre part,

$$\langle\Phi^+|\Phi^-\rangle = \left(\underbrace{\langle 0|0\rangle\langle 0|0\rangle}_{=1} - \underbrace{\langle 0|1\rangle\langle 0|1\rangle}_{=0} + \underbrace{\langle 1|0\rangle\langle 1|0\rangle}_{=0} - \underbrace{\langle 1|1\rangle\langle 1|1\rangle}_{=1}\right)/2 = 0, \tag{13}$$

$$\langle\Phi^+|\Psi^+\rangle = \left(\underbrace{\langle 0|0\rangle\langle 0|1\rangle}_{=0} + \underbrace{\langle 0|1\rangle\langle 0|0\rangle}_{=0} + \underbrace{\langle 1|0\rangle\langle 1|1\rangle}_{=0} + \underbrace{\langle 1|1\rangle\langle 1|0\rangle}_{=0}\right)/2 = 0, \tag{14}$$

$$\langle\Phi^+|\Psi^-\rangle = \left(\underbrace{\langle 0|0\rangle\langle 0|1\rangle}_{=0} - \underbrace{\langle 0|1\rangle\langle 0|0\rangle}_{=0} + \underbrace{\langle 1|0\rangle\langle 1|1\rangle}_{=0} - \underbrace{\langle 1|1\rangle\langle 1|0\rangle}_{=0}\right)/2 = 0, \tag{15}$$

$$\langle\Phi^-|\Psi^+\rangle = \left(\underbrace{\langle 0|0\rangle\langle 0|1\rangle}_{=0} + \underbrace{\langle 0|1\rangle\langle 0|0\rangle}_{=0} - \underbrace{\langle 1|0\rangle\langle 1|1\rangle}_{=0} - \underbrace{\langle 1|1\rangle\langle 1|0\rangle}_{=0}\right)/2 = 0, \tag{16}$$

$$\langle\Phi^-|\Psi^-\rangle = \left(\underbrace{\langle 0|0\rangle\langle 0|1\rangle}_{=0} - \underbrace{\langle 0|1\rangle\langle 0|0\rangle}_{=0} - \underbrace{\langle 1|0\rangle\langle 1|1\rangle}_{=0} + \underbrace{\langle 1|1\rangle\langle 1|0\rangle}_{=0}\right)/2 = 0, \tag{17}$$

et

$$\langle\Psi^+|\Psi^-\rangle = \left(\underbrace{\langle 0|0\rangle\langle 1|1\rangle}_{=1} - \underbrace{\langle 0|1\rangle\langle 1|0\rangle}_{=0} + \underbrace{\langle 1|0\rangle\langle 0|1\rangle}_{=0} - \underbrace{\langle 1|1\rangle\langle 0|0\rangle}_{=1}\right)/2 = 0. \tag{18}$$

(b) Nous allons voir qu'il est en fait possible de retrouver, à partir d'un état de Bell (nous prenons $|\Phi^+\rangle$ ici) les 3 autres états de la base des états de Bell, en appliquant les opérations de bit flip et sign flip à l'un ou l'autre des qubits d'Alice ou Bob. Si nous appliquons l'opération de bit flip (correspondant à σ_x) au qubit d'Alice, on a

$$\begin{aligned}(\sigma_x \otimes \mathbb{I})\left|\Phi^+\right\rangle &= \sigma_x \otimes \mathbb{I}\left(\frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}}\right)\\ &= \frac{(\sigma_x|0\rangle)|0\rangle + (\sigma_x|1\rangle)|1\rangle}{\sqrt{2}}\\ &= \frac{|1\rangle|0\rangle + |0\rangle|1\rangle}{\sqrt{2}}\\ &= \left|\Psi^+\right\rangle\end{aligned} \tag{19}$$

De même, si nous appliquons l'opération de bit flip au qubit de Bob cette fois, on a

$$\begin{aligned}(\mathbb{I} \otimes \sigma_x)\left|\Phi^+\right\rangle &= \mathbb{I} \otimes \sigma_x\left(\frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}}\right)\\ &= \frac{|0\rangle(\sigma_x|0\rangle) + |1\rangle(\sigma_x|1\rangle)}{\sqrt{2}}\\ &= \frac{|0\rangle|1\rangle + |1\rangle|0\rangle}{\sqrt{2}}\\ &= \left|\Psi^+\right\rangle\end{aligned} \tag{20}$$

Il suffit donc d'appliquer un bit flip sur n'importe lequel des systèmes (celui d'Alice ou celui de Bob) à l'état $|\Phi^+\rangle$ afin d'obtenir l'état $|\Psi^+\rangle$. Si maintenant on applique l'opération de sign flip à l'un des qubit de $|\Phi^+\rangle$, on a

$$(\sigma_z \otimes \mathbb{I}) \left|\Phi^+\right\rangle = \left|\Phi^-\right\rangle \tag{21}$$

et

$$(\mathbb{I} \otimes \sigma_z) \left|\Phi^+\right\rangle = \left|\Phi^-\right\rangle \tag{22}$$

Si on cherche à obtenir l'etat $|\Psi^-\rangle$, on peut par exemple appliquer un sign flip au qubit d'Alice dans $|\Psi^+\rangle$, et donc par exemple effectuer une opération telle que

$$(\sigma_z \otimes \sigma_x) \left|\Phi^+\right\rangle = \left|\Psi^-\right\rangle . \tag{23}$$

Les états de Bell sont des états avec une intrication *maximale*. En particulier, ils saturent une mesure quantitative de l'intrication.
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.
On voit que si l'on permute les qubit d'Alice et Bob dans $|\Phi^+\rangle$, $|\Phi^-\rangle$ ou $|\Psi^+\rangle$, on obtient les mêmes états, ce qui veut dire qu'on a une symétrie par rapport aux deux systèmes (celui d'Alice et celui de Bob). Si l'on effectue cette permutation dans $|\Psi^-\rangle$, on voit qu'on obtient l'opposé de l'état d'origine. Les 3 états $|\Phi^+\rangle$, $|\Phi^-\rangle$ et $|\Psi^+\rangle$ sont donc symétriques et constituent les états triplets, alors que l'état $|\Psi^-\rangle$ est antisymétrique et constitue l'état singulet.
Remarquez 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. Il est possible de voir que cette propriété permet la *téléportation* d'un état inconnu d'un système quantique d'un endroit à un autre endroit arbitrairement éloigné. Ce protocole utilise un état intriqué comme ressource.
Supposons que Alice et Bob partagent le même état de Bell, disons $|\Phi^+\rangle_{AB}$, de sorte que le premier qubit appartienne à Alice et le deuxième à Bob. Techniquement, ceci peut par exemple 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 maintenant montrer que si Alice a un troisième photon qui est dans un état inconnu $|\phi\rangle_{A'}$, donné par

$$|\phi\rangle_{A'} = \alpha |0\rangle + \beta |1\rangle , \tag{24}$$

il lui est possible de le transmettre à Bob, sans pour autant le mesurer (et donc sans connaitre les valeurs de α et β) en effectuant par contre une mesure sur son autre qubit, et en envoyant le résultat (donné par deux bits classiques) à Bob. Ce dernier peut en effet reconstruire *parfaitement* l'état $|\phi\rangle$ à partir de l'information envoyée par Alice. En résumé, $|\phi\rangle$ reste complètement inconnu d'Alice, et 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 :

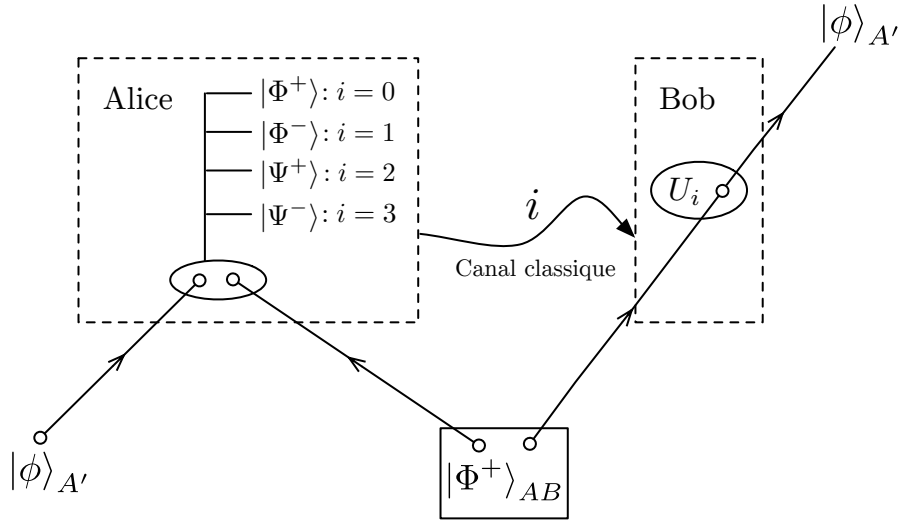

FIGURE 1 – Téléportation quantique.

Question 6.

On suppose que

$$|\Psi\rangle_{A'AB} = |\phi\rangle_{A'} \left|\Phi^+\right\rangle_{AB} \tag{25}$$

où $|\phi\rangle_{A'}$ *est l'état d'un qubit défini dans l'équation* (24) *et* $|\Phi^+\rangle_{AB}$ *est l'état de Bell défini dans l'équation* (7).

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

$$|\Psi\rangle_{A'AB} = \frac{1}{2}\left[\left|\Phi^+\right\rangle_{A'A}|\phi_0\rangle_B + \left|\Phi^-\right\rangle_{A'A}|\phi_1\rangle_B + \left|\Psi^+\right\rangle_{A'A}|\phi_2\rangle_B + \left|\Psi^-\right\rangle_{A'A}|\phi_3\rangle_B\right], \tag{26}$$

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

(b) *Montrez qu'en appliquant une séquence appropriée d'opérations d'inversions de bits ou de signe (voir équations* (42) *et* (42) *dans le Rappel)), on peut transformer chacun de ces états* $|\phi_i\rangle$ *en l'état* $|\phi\rangle$.

(a) On a

$$\begin{aligned} |\Psi\rangle_{A'AB} &= |\phi\rangle_{A'} \left|\Phi^+\right\rangle_{AB} \\ &= \frac{1}{\sqrt{2}}\left(\alpha|0\rangle_{A'} + \beta|1\rangle_{A'}\right)\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right) \\ &= \frac{\alpha}{\sqrt{2}}\left(|0\rangle_{A'}|0\rangle_A|0\rangle_B + |0\rangle_{A'}|1\rangle_A|1\rangle_B\right) + \frac{\beta}{\sqrt{2}}\left(|1\rangle_{A'}|0\rangle_A|0\rangle_B + |1\rangle_{A'}|1\rangle_A|1\rangle_B\right) \end{aligned} \tag{27}$$

Or, à partir des définitions des états de Bell, on trouve aisément les identités suivantes :

$$\begin{aligned} |0\rangle|0\rangle &= \left(\left|\Phi^+\right\rangle + \left|\Phi^-\right\rangle\right)/\sqrt{2} \\ |0\rangle|1\rangle &= \left(\left|\Psi^+\right\rangle + \left|\Psi^-\right\rangle\right)/\sqrt{2} \\ |1\rangle|0\rangle &= \left(\left|\Psi^+\right\rangle - \left|\Psi^-\right\rangle\right)/\sqrt{2} \\ |1\rangle|1\rangle &= \left(\left|\Phi^+\right\rangle - \left|\Phi^-\right\rangle\right)/\sqrt{2} \end{aligned} \tag{28}$$

Si on réécrit $|\Psi\rangle_{A'AB}$ en recombinant cette fois les deux qubits d'Alice, on obtient

$$\begin{aligned} |\Psi\rangle_{A'AB} &= \frac{1}{2}\left|\Phi^+\right\rangle(\alpha|0\rangle+\beta|1\rangle)+\frac{1}{2}\left|\Psi^+\right\rangle(\alpha|1\rangle+\beta|0\rangle) \\ &+ \frac{1}{2}\left|\Phi^-\right\rangle(\alpha|0\rangle-\beta|1\rangle)+\frac{1}{2}\left|\Psi^-\right\rangle(\alpha|1\rangle-\beta|0\rangle), \end{aligned} \tag{29}$$

et on trouve donc bien que l'état des trois particules peut se représenter comme une superposition de quatre termes, chaque terme représentant un état donc les deux premiers qubits forment un état de Bell. En fait, les deux premiers qubites correspondent aux deux états d'Alice, tandis que le troisième correspond à l'état de Bob. On comprend donc que si Alice mesure ses deux qubits, son résultat est forcement un des autres états de Bell. Des lors, en fonction de l'état de Bell obtenu, on sait que est l'état de Bob :

i. Si Alice mesure $|\Phi^+\rangle$ pour ses deux états, alors on sait que Bob est déjà dans l'état inconnu $|\phi\rangle = \alpha|0\rangle+\beta|1\rangle$, et il ne doit donc pas effectuer de transformation pour l'atteindre.

ii.] Si Alice mesure $|\Psi^+\rangle$, alors on sait que Bob est dans l'état $\alpha|1\rangle+\beta|0\rangle$, et il doit effectuer une transformation pour obtenir l'état $|\phi\rangle$.

iii. Si Alice mesure $|\Phi^-\rangle$, alors on sait que Bob est dans l'état $\alpha|0\rangle-\beta|1\rangle$.

iv. Si Alice mesure $|\Psi^-\rangle$, alors on sait que Bob est dans l'état $\alpha|1\rangle-\beta|0\rangle$.

Il suffit donc à Alice d'envoyer le résultat de sa mesure à Bob afin que ce dernier sache quel transformation effectuer sur l'état dont il dispose afin d'obtenir l'état $|\phi\rangle$.

(b) Il reste encore à définir les transformations que Bob doit appliquer une fois qu'il connait l'état de sa particule :

i. Si Alice a mesuré $|\Phi^+\rangle$, alors Bob sait que sa particule est dans l'état $|\phi\rangle$, et il ne doit donc appliquer aucune transformation.

ii. Si Alice a mesuré $|\Phi^-\rangle$, alors Bob sait que sa particule est dans l'etat $\alpha|0\rangle-\beta|1\rangle$. Il lui suffit donc d'appliquer un sign flip (σ_z) afin d'obtenir ϕ.

iii. Si Alice a mesuré $|\Psi^+\rangle$, alors Bob sait que sa particule est dans l'etat $\alpha|1\rangle+\beta|0\rangle$. Il lui suffit donc d'appliquer un bit flip (σ_x) afin d'obtenir ϕ.

iv. Si Alice a mesuré $|\Psi^-\rangle$, alors Bob sait que sa particule est dans l'etat $\alpha|1\rangle-\beta|0\rangle$. Il lui suffit donc d'appliquer un bit flip (σ_x) suivi d'un sign flip (σ_z) afin d'obtenir ϕ.

Finalement, on voit donc que si Bob sait (grâce aux informations d'Alice) de quel état il dispose, et est donc capable de retrouver l'état $|\phi\rangle$ d'origine. Insistons sur le fait qu'il n'a jamais fallu mesurer ce dernier durant le processus de téléportation.

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

(a) 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 $|\Phi^+\rangle$.

(b) Alice reçoit un troisième qubit qui est dans un état inconnu $|\phi\rangle$.

(c) 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).

(d) Le résultat est transmis à Bob par un canal classique.

(e) 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

La mécanique quantique interdit de mesurer simultanément *deux observables $\hat{A}$ et $\hat{B}$ avec une précision arbitraire, si ils ne commutent pas :*

$$\langle \hat{A}^2 \rangle \langle \hat{B}^2 \rangle \geq \frac{1}{4} |\langle [\hat{A}, \hat{B}] \rangle|^2. \tag{30}$$

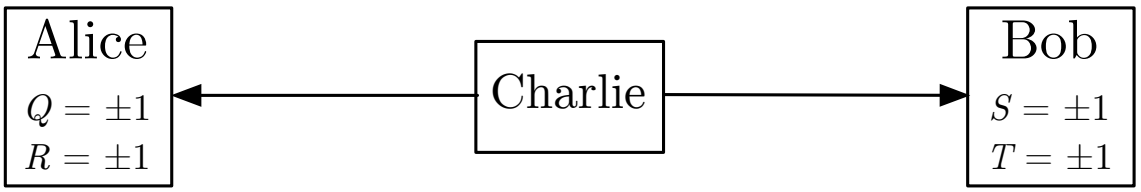

FIGURE 2 – Schéma expérimental.

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.

Calculer les valeurs que peut prendre la quantité $QS + RS + RT - QT$.
Sachant que $Q = \pm 1$, $S = \pm 1$, $R = \pm 1$ et $T = \pm 1$, on en déduit aisément que

$$QS + RS + RT - QT = \pm 2. \tag{31}$$

Question 8.

Supposons que $p(q, r, s, t)$ est 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. Trouvez une borne supérieure pour $E(QS) + E(RS) + E(RT) - E(QT)$, où $E(.)$ est l'espérance mathématique.* Indice : Utilisez la linéarité de l'espérance.
Par linéarité de l'espérance, on a

$$\begin{aligned} E(QS) + E(RS) + E(RT) - E(QT) &= E(QS + RS + RT - QT) \\ &= \sum_{q,r,s,t} p(q, r, s, t)(QS + RS + RT - QT) \end{aligned} \tag{32}$$

En utilisant alors l'inégalité (31), on voit que

$$E(QS) + E(RS) + E(RT) - E(QT) \leq 2 \sum_{q,r,s,t} p(q, r, s, t) = 2. \tag{33}$$

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)

$$\left|\Psi^-\right\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{34}$$

Ensuite Alice et Bob mesurent les *observables* données par

$$\begin{cases} \hat{Q} = Z_1 \\ \hat{R} = X_1 \end{cases} \quad \text{et} \quad \begin{cases} \hat{S} = \dfrac{-Z_2 - X_2}{\sqrt{2}} \\ \hat{T} = \dfrac{Z_2 - X_2}{\sqrt{2}} \end{cases} \tag{35}$$

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 $\langle\Psi^-|\,\hat{Q}\hat{S}\,|\Psi^-\rangle + \langle\Psi^-|\,\hat{R}\hat{S}\,|\Psi^-\rangle + \langle\Psi^-|\,\hat{R}\hat{T}\,|\Psi^-\rangle - \langle\Psi^-|\,\hat{Q}\hat{T}\,|\Psi^-\rangle$ *et interprétez le résultat.*
Aide : Utilisez les propriétés (42) *et* (42) *des matrices de Pauli (voir Rappel), ainsi que l'égalité suivante :*

$$(A \otimes B)(|x\rangle\,|y\rangle) = (A\,|x\rangle)(B\,|y\rangle), \quad x, y = 0, 1. \tag{36}$$

On a

$$\begin{aligned} \left\langle\Psi^-\right|\hat{Q}\hat{S}\left|\Psi^-\right\rangle &= \frac{1}{2}\Big(\langle 01| - \langle 10|\Big)\Big(\sigma_z \otimes \mathbb{I}\Big)\Big(\frac{-\mathbb{I}\otimes\sigma_z - \mathbb{I}\otimes\sigma_x}{\sqrt{2}}\Big)\Big(|01\rangle - |10\rangle\Big) \\ &= \frac{1}{2\sqrt{2}}\Big(\langle 01| - \langle 10|\Big)\Big(\sigma_z \otimes \mathbb{I}\Big)\Big(-\mathbb{I}\,|0\rangle\,\sigma_z\,|1\rangle + \mathbb{I}\,|1\rangle\,\sigma_z\,|0\rangle - \mathbb{I}\,|0\rangle\,\sigma_x\,|1\rangle + \mathbb{I}\,|1\rangle\,\sigma_x\,|0\rangle\Big) \\ &= \frac{1}{2\sqrt{2}}\Big(\langle 01| - \langle 10|\Big)\Big(\sigma_z \otimes \mathbb{I}\Big)\Big(|0\rangle\,|1\rangle + |1\rangle\,|0\rangle - |0\rangle\,|0\rangle + |1\rangle\,|1\rangle\Big) \\ &= \frac{1}{2\sqrt{2}}\Big(\langle 01| - \langle 10|\Big)\Big(|0\rangle\,|1\rangle - |1\rangle\,|0\rangle - |0\rangle\,|0\rangle - |1\rangle\,|1\rangle\Big) \\ &= \frac{1}{\sqrt{2}}. \end{aligned} \tag{37}$$

De même, on obtient

$$\left\langle\Psi^-\right|\hat{R}\hat{S}\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}, \tag{38}$$

$$\left\langle\Psi^-\right|\hat{R}\hat{t}\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}, \tag{39}$$

et

$$\left\langle\Psi^-\right|\hat{Q}\hat{T}\left|\Psi^-\right\rangle = -\frac{1}{\sqrt{2}}. \tag{40}$$

Finalement, on obtient

$$\left\langle\Psi^-\right|\hat{Q}\hat{S}\left|\Psi^-\right\rangle + \left\langle\Psi^-\right|\hat{R}\hat{S}\left|\Psi^-\right\rangle + \left\langle\Psi^-\right|\hat{R}\hat{T}\left|\Psi^-\right\rangle - \left\langle\Psi^-\right|\hat{Q}\hat{T}\left|\Psi^-\right\rangle = 2\sqrt{2}, \tag{41}$$

ce qui ne respecte pas l'inégalité de Bell (33).

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 :

(a) σ_x implémente une *inversion de bit* :

$$\sigma_x |0\rangle = |1\rangle \qquad \sigma_x |1\rangle = |0\rangle \tag{42}$$

(b) σ_z implémente une *inversion de signe* :

$$\sigma_z |0\rangle = |0\rangle \qquad \sigma_z |1\rangle = -|1\rangle \tag{43}$$

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