TD 3. Superdense-coding, téléportation, cryptographie

FIGURE 1 – PAULI MATRICES

$$\sigma_0 = \mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Exercice 0.1: Base de Bell Comme au TD1, on introduit la notation $|\beta_i\rangle = (\sigma_i \otimes \mathbf{I})|\beta_0\rangle$. Montrer que ces états forment une base de $\mathbb{C}^4$. En conclure que $\{|\beta_i\rangle\langle\beta_i|\}_{i=0...3}$ est la description d'une mesure $\mathcal{M}$.

1 Superdense-coding

Exercice 1.1: Supposons qu'Alice et Bob partagent une paire d'états enchevêtrés $|\beta_0\rangle = (1/\sqrt{2})(|0\rangle^{\text{Alice}} \otimes |0\rangle^{\text{Bob}} + |1\rangle^{\text{Alice}} \otimes |1\rangle^{\text{Bob}})$.
Montrer qu'Alice peut transformer $|\beta_0\rangle$ en $|\beta_j\rangle$ sans l'aide de Bob.
Proposer un protocole qui permet à Alice de communiquer vers Bob 2 bits d'information classique en effectuant un unique envoi de 1 qubit.
Résumer le protocole de superdense coding à l'aide d'un circuit.

2 Teleportation

Exercice 2.1: Classiquement Combien faut-il d'information classique pour qu'Alice envoie à Bob la description complète d'un qubit ?

Exercice 2.2: Teleportation
Supposons qu'Alice et Bob partagent l'état

$$|\beta_0\rangle = (1/\sqrt{2})(|0\rangle^{\text{Alice}} \otimes |0\rangle^{\text{Bob}} + |1\rangle^{\text{Alice}} \otimes |1\rangle^{\text{Bob}}).$$

Alice souhaite envoyer un troisième qubit, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ à Bob. Nous allons montrer qu'elle peut accomplir cela avec juste deux bits d'information classique. Considérons le qubit à envoyer, avec la paire de Bell :

$$|\psi\rangle \otimes |\beta\rangle = (1/\sqrt{2})(|\psi\rangle^{\text{Alice}} \otimes |0\rangle^{\text{Alice}} \otimes |0\rangle^{\text{Bob}} + |\psi\rangle^{\text{Alice}} \otimes |1\rangle^{\text{Alice}} \otimes |1\rangle^{\text{Bob}})$$

Vérifier que cet état est égal à

$$(1/2) \sum_i |\beta_i\rangle^{\text{Alice}} \otimes \sigma_i |\psi\rangle^{\text{Bob}}.$$

Alice mesure $\mathcal{M}$ sur les deux qubits, qu'elle détient : $\{(|\beta_i\rangle\langle\beta_i|) \otimes \mathbf{I}\}_{i=0...3}$. Quelles sont les quatre états post-mesure possibles, et leurs probabilités respectives ? Montrer que si le résultat i advient, alors l'état pose-mesure sera

$$|\beta_i\rangle^{\text{Alice}} \otimes \sigma_i |\psi\rangle^{\text{Bob}}.$$

Dès lors, Bob à 'reçu' $|\psi\rangle$, mais ce $|\psi\rangle$ est masqué par σ_i. Maintenant, si Alice envoie i, le résultat de sa mesure, à Bob (sur 2 bits classiques), Alors Bob pourra révéler $|\psi\rangle$ en appliquant σ_i à son qubit (Montrer que les matrices de Pauli sont leurs propre inverse).
Résumer la téléportation quantique à l'aide d'un circuit.

3 BB84

Exercice 3.1: Base canonique et base diagonale Soient $\mathcal{M} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ la mesure correspondant à la base canonique et $\mathcal{M}' = \{|+\rangle\langle +|, |-\rangle\langle -|\}$ la mesure correspondant à la base diagonale.
Si Alice envoie un bit d'information encodé dans l'une des bases, et que Bob le mesure dans cette même base, Bob apprend-t-il queque chose sur le qubit originellement envoyé ?
Si Alice envoie un bit d'information encodé dans l'une des bases, mais que Bob le mesure dans l'autre base, Bob apprend-t-il quelque chose sur le qubit originellement envoyé ?
Si Alice envoie un bit d'information encodé dans l'une des bases, que Eve l'intercepte et le mesure dans cette même base, puis que Bob le mesure dans cette même base, Bob apprend-t-il queque chose sur le qubit originellement envoyé ?
Si Alice envoie un bit d'information encodé dans l'une des bases, que Eve l'intercepte et le mesure dans l'autre base, puis que Bob le mesure dans la base d'Alice, Bob apprend-t-il queque chose sur le qubit originellement envoyé ?

Exercice 3.2: BB84 Alice et Bob souhaitent se mettre d'accord sur une clé partagée (une chaîne de bits, secrète). Ils sont à leur disposition :
- un canal quantique non-sécurisé
- un canal classique où ils peuvent broadcaster de l'information publique, mais inaltérable.

Utiliser les remarques de l'exercice précédent pour proposer un protocole de mise en place de cette clé.
Comment cette clé peut-elle être utilisée par la suite pour encrypter de l'information classique de manière inconditionnellement sûre ?