

TD3 : Sphère de Bloch, matrices de Pauli, cryptographie quantique

1 Sphère de Bloch, matrices de Pauli

Dans cet exercice nous allons considérer les propriétés moyennes des états de spin-1/2, et le fait qu'on peut les représenter en termes d'un vecteur sur une sphère unitaire (la sphère de Bloch).

On rappelle d'abord les matrices de Pauli, représentées sur la base des vecteurs propres de σ^z

$$\sigma^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (1)$$

En particulier les trois opérateurs de spin-1/2, $\hat{S}^\mu$ ($\mu = x, y, z$) peuvent être écrits en termes des matrices de Pauli quand on les représente sur la base des états propres de $\hat{S}^z$, $\{|\tau_z\rangle : \tau = \uparrow, \downarrow\}$:

$$\langle \tau_z | \hat{S}^\mu | \tau'_z \rangle = \frac{\hbar}{2} \sigma_{\tau\tau'}^\mu \quad (2)$$

où $\sigma_{\tau\tau'}^\mu$ est un élément de la matrice de Pauli σ^μ , en prenant $\uparrow = 1$ et $\downarrow = 2$ comme indices. L'écriture rapide de l'identité ci-dessus est $\hat{S}^\mu \rightarrow (\hbar/2)\sigma^\mu$.

On rappelle aussi les opérateurs de montée et descente du spin

$$\sigma^+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \sigma^- = (\sigma^+)^\dagger = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}. \quad (3)$$

1.1

En introduisant les opérateurs $\hat{S}^\pm \rightarrow \hbar\sigma^\pm$, déterminer leur action sur les états $|\tau_z\rangle$, et leur lien avec les opérateurs $\hat{S}^x$ et $\hat{S}^y$.

1.2

Justifier qu'on peut écrire un état arbitraire du spin-1/2 dans la forme

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right) |\uparrow_z\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right) |\downarrow_z\rangle. \quad (4)$$

Déterminer l'intervalle de valeurs possibles pour θ, ϕ tel à reproduire un état arbitraire normalisé de type $a|\uparrow_z\rangle + b|\downarrow_z\rangle$ ($a, b \in \mathbb{C}$), à un terme de phase global ($e^{i\gamma}$) près.

1.3

Calculer la valeur moyenne des trois composantes de spin sur l'état arbitraire $|\psi\rangle$, et montrer que

$$\langle \psi | \mathbf{S} | \psi \rangle = \frac{\hbar}{2} \mathbf{n} \quad (5)$$

où $\mathbf{n}$ est un vecteur sur la sphère unitaire (qu'on appelle la sphère de Bloch) à déterminer.

Repérer sur la sphère de Bloch les points correspondants aux vecteurs propres de $\hat{S}^x, \hat{S}^y, \hat{S}^z$.

Suggestion : utiliser les opérateurs de montée/descente.

Maintenant on se concentre sur quelques propriétés remarquables des matrices de Pauli. Pour mener les calculs on peut re-écrire les matrices de Pauli à partir des opérateurs $|\tau_z\rangle\langle\tau'_z|$, qui engendrent tout opérateur qui agit sur l'espace de Hilbert des spins-1/2.

1.4

Montrer que $(\sigma^\mu)^2 = \mathbb{1}$; et que $\text{Tr}(\sigma^\mu) = 0$.

1.5

Montrer que, si $\mu \neq \nu$, alors $\sigma^\mu \sigma^\nu = -\sigma^\nu \sigma^\mu$ (les matrices de Pauli anti-commutent).

Suggestion : on peut se limiter à montrer cette propriété pour une paire ou deux d'indices μ, ν .

1.6

Montrer que

$$\sigma^\mu \sigma^\nu = i \sum_{\gamma} \epsilon_{\mu\nu\gamma} \sigma^\gamma + \delta_{\mu\nu} \mathbb{1} \quad (6)$$

où $\epsilon_{\mu\nu\gamma}$ est appelé le tenseur complètement antisymétrique, à savoir il vaut 1 si $\mu\nu\gamma$ est une permutation paire de xyz (à savoir xyz, yzx, zxy) ; il vaut -1 si permutation impaire ; et 0 dans tout autre cas.

Suggestion : on peut se limiter à montrer cette propriété pour une paire ou deux d'indices μ, ν .

1.7

Conclure que les règles de commutation suivantes valent pour les opérateurs de spin-1/2 :

$$[\hat{S}^x, \hat{S}^y] = i\hbar \hat{S}^z \quad [\hat{S}^y, \hat{S}^z] = i\hbar \hat{S}^x \quad [\hat{S}^z, \hat{S}^x] = i\hbar \hat{S}^y. \quad (7)$$

Considérons maintenant un spin-1/2 dans un état aligné avec la direction $\mathbf{m}$ arbitraire de l'espace (où $\mathbf{m}$ est un vecteur unitaire), $|\psi\rangle = |\uparrow_{\mathbf{m}}\rangle$. On imagine donc d'envoyer ce spin dans un appareil Stern-Gerlach avec gradient de champ magnétique selon la direction $\mathbf{n}$.

1.8

Soit β l'angle formé entre $\mathbf{m}$ et $\mathbf{n}$. A la lumière de ce qu'on a vu jusque là, justifier qu'on puisse écrire

$$|\psi\rangle = \cos(\beta/2) |\uparrow_{\mathbf{n}}\rangle + \sin(\beta/2) e^{i\gamma} |\downarrow_{\mathbf{n}}\rangle \quad (8)$$

où γ est un angle arbitraire (dans le sens qu'on ne peut pas le déterminer avec les informations qu'on a fourni).

1.9

Conclure alors que la probabilité P que le spin-1/2 traverse l'appareil SG en sortant du bras correspondant à l'état $|\uparrow_{\mathbf{n}}\rangle$ s'écrit comme

$$P = \frac{1}{2} (1 + \mathbf{n} \cdot \mathbf{m}). \quad (9)$$

1.10

De façon générale, on peut attribuer à chaque état $|\psi\rangle$ un opérateur (qu'on appelle "matrice densité") correspondant au projecteur sur $|\psi\rangle$, $\hat{\rho}_{|\psi\rangle} = |\psi\rangle\langle\psi|$. On peut montrer que, quand on le représente dans la base propre de $\hat{S}^z$, l'opérateur $\hat{\rho}$ prend la forme

$$\hat{\rho}_{|\psi\rangle} \rightarrow \frac{1}{2} (1 + \mathbf{m} \cdot \boldsymbol{\sigma}) \quad (10)$$

où $\mathbf{m}$ est le vecteur de Bloch de l'état $|\psi\rangle$, et $\boldsymbol{\sigma} = (\sigma^x, \sigma^y, \sigma^z)$ est le vecteur de matrices de Pauli.

Ici on se limitera à montrer que $P = \langle \uparrow_{\mathbf{n}} | \hat{\rho}_{|\psi\rangle} | \uparrow_{\mathbf{n}} \rangle = \text{Tr}(\hat{\rho}_{|\uparrow_{\mathbf{n}}\rangle} \hat{\rho}_{|\psi\rangle})$ prend la même forme que ce qu'on a obtenu au point précédent.

2 Distribution quantique de clé

Si on veut envoyer un message secret à quelqu'un, une façon de procéder c'est de l'envoyer dans un code secret, ou "crypté". Tout message peut être décomposé en code binaire comme séquence de 0 et 1, du type 010001011101... La *clé* de cryptage pour transformer un tel message en un message secret est aussi une séquence binaire *aléatoire*, par exemple 101100011010.... ; pour construire le message crypté il suffit de sommer les deux séquences avec les règles : $0 \oplus 0 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$, $1 \oplus 1 = 0$. Par exemple

$$\begin{array}{rcl} \text{(message)} & 010001011101... & \oplus \\ \text{(clé)} & 101100011010... & = \\ \text{(message crypté)} & 111101000111... & \end{array}$$

Du coup le message crypté apparaît comme complètement aléatoire si on ne connaît pas la clé, donc il ne contient en soit aucune information pour quelqu'un qui puisse l'intercepter.

2.1

Proposez une expérience avec photons et polariseurs qui vous permet de réaliser un générateur de clés parfaitement aléatoires.

Le problème de la cryptographie est donc celui de partager une clé secrète entre l'expéditeur A (ou Alice) et le destinataire B (ou Bob), sans que un espion E (ou Ève) puisse l'intercepter. Une fois que A et B ont la clé secrète en commun, ils peuvent l'utiliser pour plusieurs envois de message.

La mécanique quantique peut être utilisée pour mettre en place un système de distribution de clé qui est intrinsèquement sécurisé, c'est à dire qu'il ne peut pas être espionné sans que la clé que A essaie d'envoyer à B ne soit pas altéré par l'acte même de l'espionnage.

Le premier protocole de distribution quantique de clé (*quantum key distribution, QKD*) fut proposé par Bennet et Brassard en 1984, et il porte le nom BB84. On va l'explorer dans la suite de cet exercice.

Dans ce protocole, A est une source de photons uniques polarisés suivant 4 possibles directions, correspondantes à deux bases possibles. L'état de polarisation du photon envoyé encode un bit (0 ou 1) de la clé qu'on veut communiquer.

$$\begin{array}{ll} \text{Base 1) } H, V : & |H\rangle \rightarrow 1 \quad |V\rangle \rightarrow 0 \\ \text{Base 2) } +, - : & |+\rangle = (|H\rangle + |V\rangle)/\sqrt{2} \rightarrow 1 \quad |-\rangle = (|H\rangle - |V\rangle)/\sqrt{2} \rightarrow 0 \end{array}$$

Ici on imagine $\langle H|H\rangle = \langle V|V\rangle = 1$.

B est un filtre polariseur, qui mesure l'état de polarisation dans la base H, V ou $+, -$.

À chaque envoi, A choisit au hasard la base de polarisation de ses photons, et en suite elle envoie un photon polarisé au hasard (1 ou 0) dans cette base.

B choisit aussi au hasard une base de mesure entre H, V ou $+, -$, et il extrait donc un bit (1 ou 0) de la mesure. (Voire schéma dans la figure).

2.2

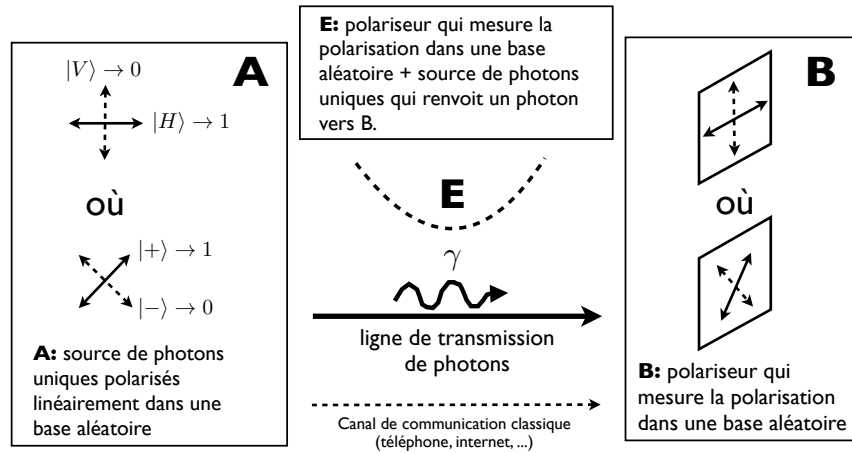
En utilisant les propriétés des polariseurs, justifier que la probabilité que un photon envoyé par A dans l'état $|\psi\rangle$ soit mesuré dans l'état $|\phi\rangle$ par B est donnée par $|\langle\psi|\phi\rangle|^2$. Quelle est la probabilité P que le bit mesuré par B coïncide avec celui envoyé par A ?

2.3

On généralise la base $+, -$ à la base $\theta+, \theta-$

$$\begin{array}{l} |\theta+\rangle = \cos\theta|H\rangle + \sin\theta|V\rangle \\ |\theta-\rangle = -\sin\theta|H\rangle + \cos\theta|V\rangle, \end{array}$$

et on établit la correspondance $|\theta+\rangle \rightarrow 1$, $|\theta-\rangle \rightarrow 0$. Que vaut dans ce cas la probabilité $P = P(\theta)$?



2.4

A envoie à B un nombre N de photons. En suite par le moyen d'un canal de communication classique non sécurisé (téléphone, internet, etc.) B envoie à A une fraction f de ces bits mesuré, correspondant à ses fN premiers bits, qui sont en suite éliminés de la clé (comme ils ont été rendus publiques). Si $fN \gg 1$, combien de bits de A et B devraient coïncider (dans le cas d'un θ générique) ?

2.5

Une espionne E prend possession du canal de transmission des photons, et son but est de capturer la clé transmise par A sans être aperçue ni par A ni par B. Donc elle doit mesurer le photon de A et en renvoyer un à B (dans la même base). Mais E ignore la base dans la quelle A envoie ses photons, et donc elle mesure et renvoie les photons dans une base aléatoire (mais toujours choisie parmi les deux bases de A).

Quelle est la probabilité que E mesure l'état du photon tel qu'il a été envoyé par A ?

(Cette probabilité correspond en suite à celle de E de renvoyer à B un photon exactement dans le même état que celui envoyé par A).

Quelle est la probabilité de mesurer correctement une clé composée par N photons ? En conclure sur la robustesse intrinsèque de la distribution quantique de clé dans la limite $N \gg 1$.

2.6

Quelle est la probabilité $P_E(\theta)$ que le bit de A et B coïncident en présence d'un espion ?

Suggestion : décomposer le problème dans le cas où les bases de A et E coïncident, et celui où les bases ne coïncident pas.

Pour $\theta = \pi/4$, quel est le nombre minimal N de photons nécessaires pour que A et B s'aperçoivent de la présence d'un espion ?

2.7

Si la présence d'un espion est détectée, la clé envoyée par A est abandonnée. Autrement A et B se communiquent par le canal d'information classique la séquence de bases qu'ils ont utilisé pour envoyer et mesurer le photon respectivement. Si les bases coïncident pour un photon donné, le bit correspondant est retenu dans la clé - pourquoi ? Autrement il est abandonné. Quelle est la longueur moyenne des clés qu'on peut produire de cette façon là ?