INF581: Du calcul probabiliste au calcul quantique **Hiver 2011**

Cours 6 — 14 février

Enseignant : Frédéric Magniez *Rédacteur : Pierre Lorenzi*

Introduction au calcul quantique, premiers exemples.

6.1 Photon – polarisation

L'état d'un photon contient plusieurs paramètres physiques :
- longueur d'onde (= énergie = quantité de mouvemement),
- polarisation,
- axe de déplacement.

On ne considère que la polarisation.

Définition 6.1. *une polarisation est un angle complexe ($\in \mathbb{C}$), ou de manière équivalente un vecteur unitaire de $\mathbb{C}^2$.*

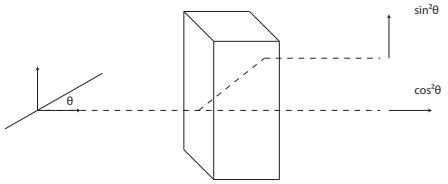
Pour cette leçon on se restreint à un angle dans $\mathbb{R}$.

Définition 6.2. *Si $\theta \in \mathbb{R}$ est un angle, $|\theta\rangle$ est son vecteur unitaire associé dans $\mathbb{R}^2$.*

Définition 6.3. *Un filtre a une sortie polarisée selon un axe.*

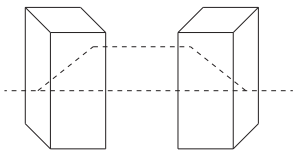
Cas probabiliste : sur un filtre d'angle 0, un faisceau polarisé à θ a un chance de $\cos^2(\theta)$ de passer et $\sin^2(\theta)$ d'être absorbé.

Définition 6.4. *Le cristal de calcite laisse passer les faisceaux horizontaux et dévie les faisceaux verticaux.*



Un faisceau de polarisation θ passe en horizontal avec une probabilité de $\cos^2(\theta)$ et est dévié avec une probabilité de $\sin^2(\theta)$.

On superpose maintenant un cristal de calcite avec un symétrique, le second redévie les faisceaux verticaux vers le bas.



On pourrait penser qu'on obtient des polarisations soit horizontales soit verticales. Mais si on met à la fin du dispositif un filtre de même angle θ que la lumière incidente, il laisse passer avec une probabilité 1, ce qui signifie que la lumière sortante a aussi une polarisation θ. Si elle s'était divisée en photons horizontaux et verticaux, il aurait filtré avec une probabilité $\cos^4(\theta) + \sin^4(\theta)$.

En revanche, si on ajoute un filtre en haut et en bas, on obtient bien $|0\rangle$ avec une probabilité $\cos^2(\theta)$ et $|\frac{\pi}{2}\rangle$ avec une probabilité $\sin^2(\theta)$.

Définition 6.5. *Une lame 1/2-onde effectue une symétrie axiale de la polarisation selon un axe quelconque.*

Cela fait qu'avec deux lames on peut obtenir une rotation quelconque de la polarisation.

6.2 Bit quantique – qubit

Définition 6.6. *Bit logique :* $b \in \{0, 1\}$

Définition 6.7. *Bit probabiliste :* $\begin{pmatrix} p \\ q \end{pmatrix}$ *avec* $p, q \geq 0$ *et* $p + q = 1$

On choisit $\binom{1}{0} = 0$ *et* $\binom{0}{1} = 1$.

Définition 6.8. *Bit quantique :* $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2$, *avec* $|\alpha|^2 + |\beta|^2 = 1$

On choisit $\binom{1}{0} = |0\rangle$ *et* $\binom{0}{1} = |1\rangle$.
Alors en général :

$$\boxed{|\psi\rangle = \alpha|0\rangle + \beta|1\rangle}$$

Cette formule est une superposition. α *et* β *sont les amplitudes*

Mesure pour $|\psi\rangle$, on obtient $|0\rangle$ avec une probabilité $|\alpha|^2$, $|1\rangle$ avec une probatilité $|\beta|^2$. On remarque qu'en passant au carré on obtient un bit probabiliste.

Évolution matrice unitaire U 2×2 (une matrice unitaire est telle que $U^* U = I_2$)

$$|\psi\rangle \text{ —— } \boxed{U} \text{ —— } U|\psi\rangle$$

Comme une matrice unitaire est inversible, toute transformation est réversible. À noter que transformation unitaire et mesure ne commutent pas, ce qui donne des résultats contre-intuitifs.

Dans le cas des bits probabilistes, l'évolution est une matrice stochastique, c'est-à-dire que la somme de chaque colonne vaut 1. Ainsi les transformations ne sont pas réversibles et l'évolution et la mesure commutent, ce qui diminue beaucoup la variété des situations.

Exemples

- $\frac{1}{\sqrt{2}}(\,|0\rangle + |1\rangle\,)$——mesure$\langle \begin{matrix} 0 & p=1/2 \\ 1 & p=1/2 \end{matrix}$
- identité $|b\rangle$ ——Id—— $|b\rangle$
- négation $|b\rangle$ ——Nég—— $|1-b\rangle$
- matrice de Hadamard : $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

  $H^2 = I_2$, il s'agit en fait d'une symétrie sur l'axe d'angle $\pi/8$

Exercice soit une matrice stochastique P telle que

$$P\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1/2\\1/2\end{pmatrix} \quad \text{et} \quad P^2\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$$

Montrer que P n'existe pas.

On pose $P = \begin{pmatrix}a & c\\ b & d\end{pmatrix}$ et on trouve une contradiction

Exercice Soit P stochastique telle que

$$P^2\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \quad \text{et} \quad P^2\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}$$

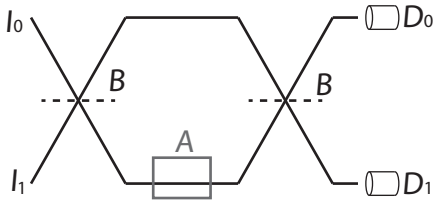
Montrer que P n'existe pas.

On voit que $P^2 = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$, donc $\det(P^2) = -1 = \det(P)^2$, ce qui est impossible sur $\mathbb{R}$.

Exercice Trouver U unitaire telle que $U^2 =$NOT au signe près.

On s'inspire de la matrice de Hadamard. On prend $U = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$, et alors $U^2 = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$

Exercice Soit le montage suivant :



I_0 et I_1 sont des sources de photons. En B se trouvent des miroirs semi-réfléchissants (*beam splitter*) qui laissent passer un photon ou le réfléchissent avec une probabilité 1/2. D_0 et D_1 sont des détécteurs de photons.

L'état est la direction des photons : haut $\begin{pmatrix}1\\0\end{pmatrix}$ bas $\begin{pmatrix}0\\1\end{pmatrix}$

On a $B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$

1. Si un photon est émis depuis I_1, quelle est la probabilité de le voir en D_0 ?
2. On met en A une bombe censée exploser au passage d'un photon. Si elle est défectueuse elle laisse passer le photon sans interaction. Proposer un test pour vérifier que la bombe fonctionne. Calculer la probabilité d'observer un photon en D_1 si la bombe fonctionne et n'explose pas.

---

1. Elle est égale à 1. $B^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, donc $B^2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$, donc probabilité de 1 d'être en haut.
2. Test : on envoie un photon. La bombe explose avec une probabilité de 50%. Sinon, le photon a 25% d'arriver en D_0 et 25% d'arriver en D_1. Dans ce dernier cas, la bombe n'a pas explosé mais on sait qu'elle fonctionne.

6.3 Applications cryptographiques

6.3.1 Incertitude sur la mesure

Soit les deux bases :

$+$ base normale, vecteurs $|0\rangle$, $|1\rangle$

$\times$ base diagonale, vecteurs $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

Si on fait une mesure d'un photon sur un vecteur, on ne peut savoir s'il appartient à l'une ou à l'autre base.

6.3.2 Protocole de distribution de clés secrètes

Définition 6.9. *One-time pad*

A et B partagent un secret $k \in \{0,1\}^*$

A veut transmettre $x \in \{0,1\}^*$ à B

Protocole :

- *A envoie $(y_i = x_i \oplus k_i)$*
- *B reçoit y_i et réapplique le xor.*

Le one-time pad est l'algorithme le plus sûr existant, il est théoriquement impossible à casser. Cependant il ne peut pas fonctionner dans un grand réseau parce que chaque pair de participants doit partager un secret.

Alternative 1 AES, c'est un bon algorithme de cryptage à la complexité prouvée.

Alternative 2 Permettre à A et B de générer un secret. Il y a RSA et Hoffman, mais ce dernier n'est pas prouvé.

Alternative 3 Utiliser l'incertitude de la mesure : QUANTUM KEY DISTRIBUTION, trouvée par Bennett et Brassard en 1984.

6.3.3 Quantum Key Distribution

Contexte

- A et B se parlent sur un canal authentifié et public.
- A et B peut s'échanger des qubits sur un canal tel qu'il n'y a aucune erreur si le canal n'est pas attaqué.

Protocole pour 1 bit de clé secrète

- Alice tire $a \in \{0, 1\}$
- Alice tire $c \in \{0, 1\}$ et envoie $H^c|a\rangle = |\psi\rangle$
- Bob tire $d \in \{0, 1\}$, il reçoit $|\psi\rangle$,
- Bob observe le bit $b = H^d|\psi\rangle$
- Alice et Bob annoncent c et d et gardent leur bit a et b si $c = d$.

Exemple On note $R = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$:

a	0	$\boxed{0}$	1	$\boxed{1}$
c	0	1	1	0
$\|\psi\rangle$	$\|0\rangle$	$H\|0\rangle$	$H\|1\rangle$	$\|1\rangle$
d	1	1	0	0
b	R	$\boxed{0}$	R	$\boxed{1}$

Efficacité Probabilité pour obtenir un bit de clé : 1/2.
Si on veut N bits de clé, en moyenne $2N$ itérations.

Non-clonage Attaque possible : Ève se met entre A et B sur le canal quantique.
Protocole :

- garder le photon d'Alice, en envoyer un autre $|\theta\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$
- mesurer le photon d'Alice et, en fonction du résultat, annoncer une certaine base à Bob.

Parade Test d'attaque : lorsqu'après l'annonce $c = d$, Alice et Bob vérifient que $a = b$ avec une probabilité p en s'échangeant a et b sur le canal public.
Il faut donc $\frac{2N}{1-p}$ itérations pour transmettre le message.
S'il n'y a aucune erreur, on en déduit que Ève a lu et corrompu peu de bits.

Définition 6.10. *Réconciliation : éliminer le bruit restant.*

Définition 6.11. *Privacy amplification : diminuer l'information d'Ève (le bruit est dû à Ève mais aussi au canal*

Dans ces deux cas la clé est plus petite mais correcte et secrète.

Théorème 6.12. *si la fréquence des erreurs est inférieure à 11%, alors on peut extraire une clé secrète de taille $\Theta(N)$, avec N le nombre d'itérations.*

Preuve: On admet ce résultat. □

Exercice Efficacité du non-clonage
Ève apprend a de manière certaine si Alice et Bob annoncent la même base.
Quelle est la probabilité que $a = b$? Quel est le choix optimal pour θ ?

Faisons un tableau :

c	0	0	1	1
a	0	1	0	1
$\mathbb{P}_r(a=b)$	$\cos^2(\theta)$	$\sin^2(\theta)$	$\cos^2(\theta-\frac{\pi}{4})$	$\sin^2(\theta-\frac{\pi}{4})$

Comme chaque cas est équiprobable, il vient : $\mathbb{P}_r(a=b) = \frac{1}{2}$. Il n'y a donc pas de θ optimal. On détecte Ève avec une probabilité $\frac{p}{2}$.

Exercice On change un peu le protocole.

- Ève observe le bit d'Alice sur la base $|\theta\rangle$, $|\theta+\frac{\pi}{2}\rangle$. Elle choisit $e=0$ pour $|\theta\rangle$ et $e=1$ pour $|\theta+\frac{\pi}{2}\rangle$.
- Elle envoie le qubit mesuré à Bob.

1. $\mathbb{P}_r(e=a)$? Quel est le choix optimal pour θ ?
2. si $c=d$, $\mathbb{P}_r(a=b)$?

---

1. Refaisons le tableau :

c	0	0	1	1
a	0	1	0	1
$\mathbb{P}_r(e=a)$	$\cos^2(\theta)$	$\cos^2(\theta)$	$\cos^2(\theta-\frac{\pi}{4})$	$\cos^2(\theta-\frac{\pi}{4})$

On a donc $\mathbb{P}_r(e=a) = \frac{1}{2}(\cos^2(\theta)+\cos^2(\theta-\frac{\pi}{4}))$
Comme $\cos^2$ est concave, le θ optimal est la moyenne de 0 et $\frac{\pi}{4}$, c'est-à-dire $\frac{\pi}{8}$. On a alors $\mathbb{P}_r(e=a) = \cos^2(\frac{\pi}{8}) \approx 85\%$.
2. On a $\theta = \frac{\pi}{8}$ et $c=d$. Calculons :
$\mathbb{P}_r(a=b|a=e) = \mathbb{P}_r(b=c|a=e) = \cos^2\frac{\pi}{8}$
$\mathbb{P}_r(a=b|a\neq e) = \mathbb{P}_r(b=e|a\neq e) = \sin^2\frac{\pi}{8}$
Ainsi en utilisant la réponse précédente on trouve $\mathbb{P}_r(a=b) = \cos^4(\frac{\pi}{8}) + \sin^4(\frac{\pi}{8}) = \frac{3}{4}$
Ève se fait prendre à chaque fois avec une probabilité $\frac{1}{4}$, donc en tout avec une probabilité $\frac{p}{4}$.

6.4 2-qubit et plus

Définition 6.13. *Produit tensoriel*

Soit V et W deux espaces vectoriels. On note $V \otimes W$ l'espace vectoriel libre généré par

$$Vec(v \otimes w, v \in V, w \in W)$$

avec la relation d'équivalence

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$$

$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$$

$$(\lambda v) \otimes w = v \otimes (\lambda w) = \lambda(v \otimes w)$$

Si $(e_i)_{i\in I}$ est une base de V et $(f_j)_{j\in J}$ de W, $(e_i \otimes f_j)_{i\in I, j\in J}$ est une base de $I \otimes J$. Ainsi $\dim V \otimes W = \dim V \cdot \dim W$.

Transformation linéaire Soit deux applications linéaires $S : V \to X$ et $T : W \to Y$. On définit l'application

$$\begin{array}{rl} S \otimes T : & V \otimes W \to X \otimes Y \\ & V \otimes W \mapsto Sv \otimes Tw \end{array}$$

on l'étend sur tout l'espace par linéarité.

Application Distribution de probabilités jointes, soit A et B deux ensembles finis

$\mathcal{D}(A)$	l'espace des distributions de probabilité dans A
$\mathcal{D}(B)$	l'espace des distributions de probabilité dans B
$\mathcal{D}(A \times B)$	$= \mathcal{D}(A) \otimes \mathcal{D}(B) \quad \neq \mathcal{D}(A) \times \mathcal{D}(B)$

Preuve: On donne un exemple pour montrer que $\mathcal{D}(A) \otimes \mathcal{D}(B) \neq \mathcal{D}(A) \times \mathcal{D}(B)$.

On prend $A = B = \{0, 1\}$, et la distribution d sur $(A \times B)$ tq $d(0, 0) = 1/2$ et $d(1, 1) = 1/2$. Elle appartient bien à $\mathcal{D}(A) \otimes \mathcal{D}(B)$ car $d = \frac{1}{2}d_0 \otimes d_0 + \frac{1}{2}d_1 \otimes d_1$, avec $d_0(0) = 1, d_0(1) = 0$, de même pour d_1. Or elle ne se décompose pas dans $\mathcal{D}(A) \times \mathcal{D}(B)$ car si on écrit d_A et d_B les probabilités sur chaque coefficient, on a $d_A = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$ et $d_B = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$, mais $(d_A, d_B) = (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}) \neq (\frac{1}{2}, 0, 0, \frac{1}{2})$.

□

Ainsi quand on joint plusieurs qubits, ils ne se comportent pas comme s'ils étaient indépendants, alors qu'une chaîne de n bits a 2^n valeurs possibles.

Définition 6.14. *Un n-qubit : $|\psi\rangle \in \mathbb{C}^{2n}$ tel que $\| |\psi\rangle \|_2 = 1$*

Base :

$$\begin{cases} |x\rangle, x \in \{0, 1\}^n \\ |\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \end{cases}$$

Mesure

$$|\psi\rangle = \sum \alpha_x |x\rangle \text{ ——[mesure]—— } x, \quad p = \alpha_x$$

Évolution Matrice unitaire U de taille $2^n \times 2^n$.

$$|\psi\rangle \text{ ——[}U\text{]—— } U|\psi\rangle$$

Exemple État de Bell : $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ $\quad (\neq |\psi_1\rangle \otimes |\psi_2\rangle$ comme on a vu)

$$\mathbb{C}^4 = \mathbb{C}^{\{0,1\}^2} = \mathbb{C}^{\{0,1\}} \otimes \mathbb{C}^{\{0,1\}} = \mathbb{C}^2 \otimes \mathbb{C}^2$$

$$\frac{1}{\sqrt{2}}(\,|00\rangle + |11\rangle\,) \text{——[mesure]} \begin{cases} |00\rangle & p = 1/2 \\ |11\rangle & p = 1/2 \end{cases}$$

On peut même séparer les deux photons et les conserver dans le même état global.

Paradoxe EPR

- A et B ne communiquent pas, mais ils peuvent partager une information initiale.
- A reçoit un bit aléatoire $x \in \{0,1\}$, de la part d'un tiers
- B reçoit un bit aléatoire $x \in \{0,1\}$, de la part d'un tiers
- A renvoie au tiers $a \in \{0,1\}$
- B renvoie au tiers $b \in \{0,1\}$

A et B cherchent à maximiser $p = \mathbb{P}_{x,y}(a \oplus b = x \wedge y)$.

Stratégie déterministe : $a = b = 0$! probabilité de $3/4$, et cette valeur est optimale (on l'admet). Il peut exister d'autres façons (comme $a = x$ et $b = \bar{y}$).

Stratégie probabiliste : A et B donnent un bit au hasard. On peut montrer qu'il y a une probabilité optimale de $3/4$, même si l'aléa est partagé.