Information Quantique

Frédéric Magniez

Cours 1 :
Paradoxe EPR
Superdence coding
Téléportation

Le qubit : point vue informatique

Bit classique

- Elément déterministe : $b \in \{0,1\}$

Bit probabiliste

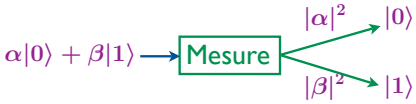
- Distribution probabiliste : $d = \begin{pmatrix} p \\ q \end{pmatrix}$ $\quad p,q \in [0,1]$, $p+q=1$

Bit quantique (qubit)

- Etat = vecteur complexe de dimension 2 normé

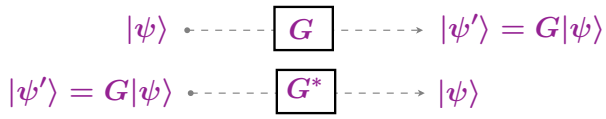
$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

- Observation = projection orthogonale probabiliste



- Evolution = transformation unitaire (donc réversible) $G \in \mathcal{U}(2)$

définition: $G \in \mathbb{C}^{2\times 2}$ tq $G^*G = \mathrm{Id}$



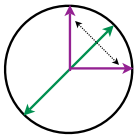
Transformation classique réversible

- Identité

$$|b\rangle \dashrightarrow \boxed{\text{Id}} \dashrightarrow |b\rangle$$

- Négation

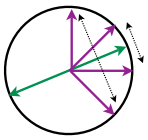
$$|b\rangle \dashrightarrow \boxed{\text{NOT}} \dashrightarrow |1-b\rangle$$



Transformation de Hadamard

- Définition : lame demi-onde à 22,5° $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$

$$|b\rangle \dashrightarrow \boxed{H} \dashrightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$$



- Propriétés : pile ou face quantique

$$|0\rangle \to \boxed{H} \to \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \to \boxed{\text{Mesure}} \xrightarrow{\frac{1}{2}} |0\rangle \quad \xrightarrow{\frac{1}{2}} |1\rangle$$

$$|b\rangle \to \boxed{H} \to \boxed{H} \to \boxed{\text{Mesure}} \to |b\rangle$$

La mesure ne commute pas !

Base orthonormée: $|\psi_0\rangle, |\psi_1\rangle : \langle\psi_i|\psi_j\rangle = \delta_i(j)$

Mesure souhaitée

$$|\psi\rangle \dashrightarrow \boxed{\text{Mesure}(|\psi_0\rangle, |\psi_1\rangle)} \xrightarrow{|\langle\psi_0|\psi\rangle|^2} |\psi_0\rangle \quad \xrightarrow{|\langle\psi_1|\psi\rangle|^2} |\psi_1\rangle$$

Porte changement de base

$$|b\rangle \dashrightarrow \boxed{M} \dashrightarrow |\psi_b\rangle$$

$$M = \begin{pmatrix}\langle 0|\psi_0\rangle & \langle 0|\psi_1\rangle\\ \langle 1|\psi_0\rangle & \langle 1|\psi_1\rangle\end{pmatrix}$$

Réalisation

$$\dashrightarrow \boxed{\text{Mesure}(|\psi_0\rangle, |\psi_1\rangle)} \dashrightarrow \quad \equiv \quad \dashrightarrow \boxed{M^*} \boxed{\text{Mesure}} \boxed{M} \dashrightarrow$$

En optique : tourner le filtre

Définition

- $|\psi\rangle \in \mathbb{C}^{\{0,1\}^n}$ tel que $\||\psi\rangle\| = 1$

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \qquad \text{avec} \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$$

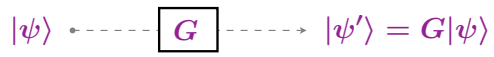
$$\mathbb{C}^{\{0,1\}^2} = \mathbb{C}^{\{0,1\}} \otimes \mathbb{C}^{\{0,1\}} \neq \mathbb{C}^{\{0,1\}} \times \mathbb{C}^{\{0,1\}}$$

Exemple : $|00\rangle + |01\rangle = |0\rangle \otimes (|0\rangle + |1\rangle)$

$|00\rangle + |11\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$

Transformations unitaires : $G \in \mathcal{U}(2^n)$

$G \in \mathbb{C}^{2^n \times 2^n}$ tq $G^*G = \mathrm{Id}$



Mesure

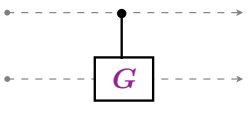
Définition

$$\mathrm{c\text{–}NOT}|0b\rangle = |0b\rangle$$
$$\mathrm{c\text{–}NOT}|1b\rangle = |1\rangle|(1-b)\rangle$$
$$\mathrm{c\text{–}NOT}|ab\rangle = |a\rangle|a \oplus b\rangle$$

$$\mathrm{c\text{–}NOT} = \begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix}$$

Représentation

Généralisation



$$\mathrm{c\text{–}}G|0b\rangle = |0b\rangle$$
$$\mathrm{c\text{–}}G|1b\rangle = |1\rangle G|b\rangle$$

Exercice 1

- Montrer qu'il n'existe pas de transformation stochastique PF telle que

  sur le bit 0 : la sortie de PF est un bit probabiliste uniforme $\begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$

  sur le bit 0 : deux applications de PF redonne le bit 0

Exercice 2

- Trouver une transformation quantique G telle que G^2 se comporte comme la porte NOT (au signe près)

  Indication : modifier légèrement la porte H

- Existe-t-il une telle transformation stochastique ? Pourquoi ?

Exercice 3

- Montrer qu'il n'existe pas de transformation quantique à 2-qubit telle que

$$G|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$$

Exercice 4

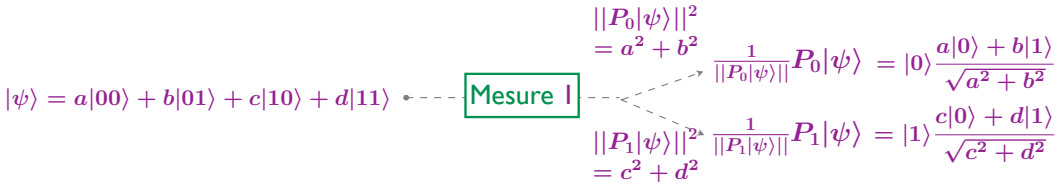
- Montrer que

- Réaliser un SWAP avec des c-NOT.

Mesure du premier bit

- Projecteurs $P_0 = |00\rangle\langle 00| + |01\rangle\langle 01| = |0\rangle\langle 0| \otimes \mathbf{I_2}$
  $P_1 = |10\rangle\langle 10| + |11\rangle\langle 11| = |1\rangle\langle 1| \otimes \mathbf{I_2}$
  $P_0 \overset{\perp}{\oplus} P_1 = Id$

- Mesure du premier bit



Commentaires

- Résultat de la mesure : mélange statistique d'états quantiques
- Représentation : matrice densité

Définition : $\rho = \begin{pmatrix} p & \alpha \\ \alpha^* & q \end{pmatrix}$

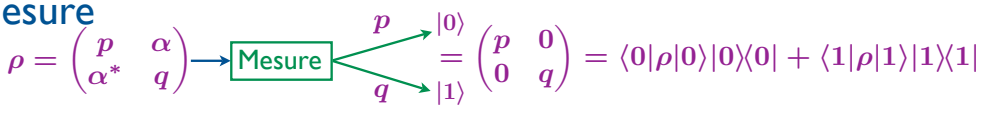
- Etat quantique (pur) : $|\psi\rangle = a|0\rangle + b|1\rangle \mapsto \rho = |\psi\rangle\langle\psi| = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}$
- Etat probabiliste : $d = \begin{pmatrix} p \\ q \end{pmatrix} \mapsto \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}$
- Etat mélangé : mélange statistique d'états quantiques

$$(|\psi_i\rangle, p_i)_{i\in I} \mapsto \sum_{i\in I} p_i |\psi_i\rangle\langle\psi_i|$$

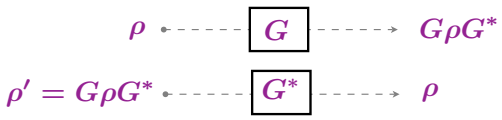
Théorème

- Deux systèmes de même matrice densité sont indistincts

Mesure



Transformation unitaire



Autres possibilités...

Remarques

- Une matrice densité est hermitienne, semi-positive, de trace 1,

  donc diagonalise en base orthonormée et ses vp sont ≥ 0 et somment à 1
- Tout qubit peut se représenter comme le mélange de deux états purs

Exercice 1

- Montrer que les statistiques de l'observation d'un qubit dans une base quelconque s'exprime uniquement en fonction de sa matrice densité

Exercice 2

- Soit la paire EPR $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Montrer qu'effectuer une transformation unitaire U sur le premier qubit de $|\psi\rangle$ est équivalent à effectuer la transformation U^t sur le deuxième qubit.

Exercice 3

- Considérer la paire EPR $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

  La probabilité d'observer 0 ou 1 sur le premier qubit est 1/2

  Quand est-il dans une autre base ?
- Intuitivement, quelle est la matrice densité représentant l'état du 1er qubit ?

  Justifier en procédant à une mesure dans une base quelconque du 1er qubit.

Définition informelle

- Matrice densité du qubit restant après l'observation de l'autre qubit (et en en oubliant le résultat) (peut importe la base !)

Exemples (à verifier)

- Etats séparés : $\mathbf{Tr_2}(|\psi_1\rangle|\psi_2\rangle) = |\psi_1\rangle\langle\psi_1| \approx |\psi_1\rangle$
- Paire EPR : $\mathbf{Tr_2}(|\mathbf{EPR}\rangle) = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{1}{2}\mathbf{Id}$

Définition formelle

$$_2\langle b|\psi\rangle_{12} = (\langle 0b|\psi\rangle)|0\rangle + (\langle 1b|\psi\rangle)|1\rangle$$

$$\mathbf{Tr_2}(|\psi\rangle) = {}_2\langle 0|\psi\rangle\langle\psi|0\rangle_2 + {}_2\langle 1|\psi\rangle\langle\psi|1\rangle_2$$

Définition

- Soit ρ une matrice densité sur n-qubit
- Soit $|\psi\rangle$une superposition sur $(n+m)$-qubit, avec $m \geq 0$
- L'état pur $|\psi\rangle$ purifie l'état mélangé ρ si

$$\mathbf{tr}_S|\psi\rangle\langle\psi| = \rho$$

où S représente les m derniers qubits de $|\psi\rangle$

Théorème

- Si $2^m \geq \text{rang}(\rho)$ alors il existe une purification de ρ

Exercice

- Prouver le théorème de purification en diagonalisant ρ

Jeu

- Alice et Bob partagent une information initiale mais ne communiquent pas
- Alice, resp. Bob, reçoit un bit aléatoire x, resp. y
- Alice, resp. Bob, retourne un bit a, resp. b

- Objectif : maximiser $p = \Pr_{x,y}(a \oplus b = x \wedge y)$

$\wedge$	0	1
0	0	0
1	0	1

$\oplus$	0	1
0	0	1
1	1	0

Classiquement

Exercice :
- Meilleur stratégie déterministe : $a = b = 0 \implies p = \frac{3}{4}$

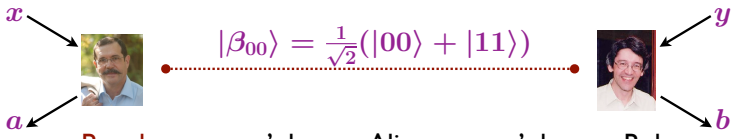
Exercice :
- Théorème : la meilleure stratégie probabiliste n'est pas meilleure que la meilleure stratégie déterministe

Rappel

- Objectif : maximiser $p = \Pr_{x,y}(a \oplus b = x \wedge y)$

Quantiquement

- Alice et Bob partagent une paire EPR



Paradoxe : ce qu'observe Alice = ce qu'observe Bob

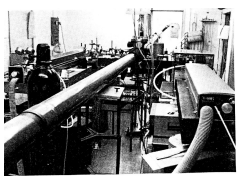
- Bob effectue une rotation d'angle $\frac{\pi}{8}$
- Si $x = 1$, Alice effectue une rotation d'angle $\frac{\pi}{4}$
- Si $y = 1$, Bob effectue une rotation d'angle $-\frac{\pi}{4}$

y\x	0	1
0	$\|\beta_{0,\frac{\pi}{8}}\rangle$	$\|\beta_{\frac{\pi}{4},\frac{\pi}{8}}\rangle$
1	$\|\beta_{0,-\frac{\pi}{8}}\rangle$	$\|\beta_{\frac{\pi}{4},-\frac{\pi}{8}}\rangle$

- Alice et Bob observent leur qubit et renvoie la valeur obtenue

Exercice :
- Théorème : $p = \cos^2(\frac{\pi}{8}) \approx 0.85$

Réalisation : [Aspect-Grangier-Roger-Dalibard: Orsay'82]



Jeu

- Alice, Bob et Charlie partagent une information initiale mais ne communiquent pas
- Alice, Bob et Charlie reçoivent un bit aléatoire : x, y, z
- Contrainte : $x \oplus y \oplus z = 0 \quad \Longrightarrow \quad xyz \in \{000, 011, 101, 110\}$
- Alice, Bob et Charlie renvoient un bit : a, b, c
- Objectif : maximiser $a \oplus b \oplus c = x \vee y \vee z$

Classiquement

- Impossible avec une certitude absolue
- Exercice : Montrer que la probabilité de succès maximale est 3/4

Quantiquement

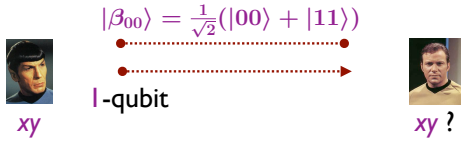
- Alice, Bob et Charlie partagent $\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$
- Protocole pour Alice/Bob/Charlie :

  Si le bit détenu est 1 alors appliquer la porte Hadamard

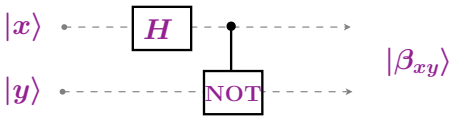
  Observer et renvoyer le bit obtenu
- Exercice : Montrer que ce protocole gagne le jeu avec certitude.

Problème

- Alice & Bob partagent une paire EPR
- Alice veut transmettre deux bits xy à Bob
- Mais alice ne peut envoyer qu'un seul bit à Bob, mais quantique



Changement de base de Bell



$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Exercice 1

- Montrer comment passer d'un état de Bell à un autre en appliquant une porte quantique sur un seul des qubits

Exercice 2

- En déduire un protocole qui permet à Bob de retrouver la valeur des bits *xy* en ne recevant qu'1-qubit d'Alice à l'aide d'une paire EPR partagée entre Alice et Bob.

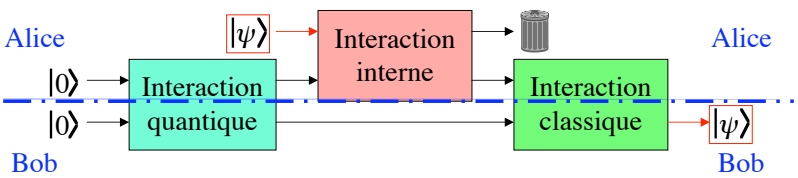
Exercice 3

- Montrer que le qubit envoyé par Alice ne révèle rien sur *xy* s'il est intercepté par une tierce personne.

Problème

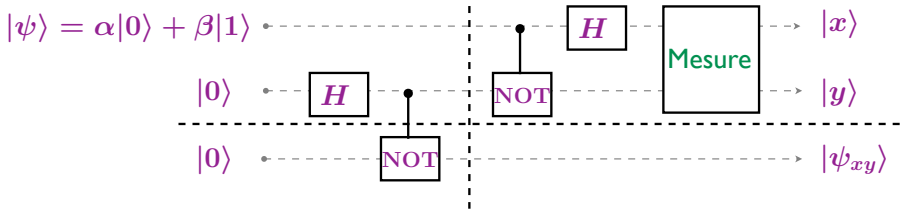
- Alice veut transmettre un qubit $|\psi\rangle$ à Bob
- Bob : position éloignée et inconnue d'Alice

Réalisation



La communication classique ne révèle rien sur $|\psi\rangle$!

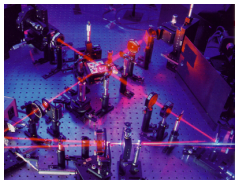
Circuit



Exercice

- Calculer l'état du système avant mesure
- Ecrire l'état du qubit $|\psi_{xy}\rangle$ en fonction des valeurs *x,y* observées
- Quelle est la matrice densité correspondant au troisième qubit ?
- Expliquer la fin du protocole

Réalisations



- 1 photon [Zeilinger et al : Innsbruck'97]
- 1 photon, 6 km [Gisin et al : Genève'02]
- 1 atome [Blatt et al : Innsbruck'04]
- Vidéo YouTube'06 : http://www.youtube.com/watch?v=6_5KKeEq-FU