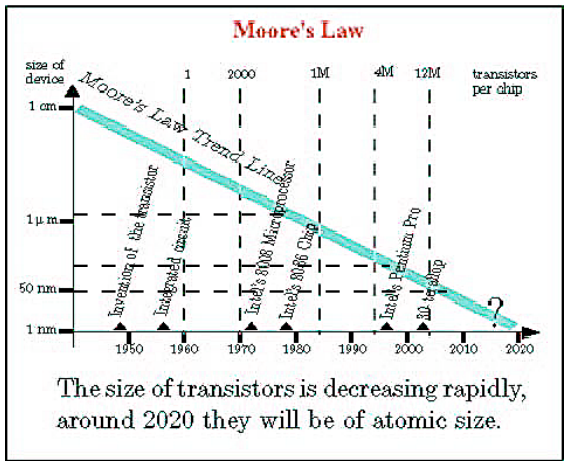
Information Quantique

Frédéric Magniez

Cours 1 :
Introduction, notion de qubit
rappels de cryptographie classique
protocoles élémentaires

Vers la nanotechnologie

Fin de la loi de Moore ?



"No exponential is forever. Your job is to delay forever.", Andrew Gordon Moore Feb. 2003.

Phénomènes quantiques vers 2020...

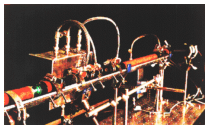
- Approche actuelle : les supprimer
- Informatique quantique : les utiliser !

La supériorité de l'informatique quantique

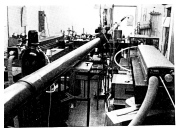
Cryptographie

- Distribution de clés secrètes [Bennett-Brassard 1984]

  Implémentation : ~100 km



Information quantique



- Paradoxe EPR [Einstein-Podolsky-Rosen 1935]

  Réalisation : 1982 [Orsay]

- Téléportation [Bennett-Brassard-Crépeau-Jozsa-Peres-Wootters 1993]

  Réalisation : 1997 [Innsbruck]

Algorithmique

- Calcul de périodes [Simon, Shor 1994] ⇨ Factorisation, log. discret...
- Recherche dans une liste non triée [Grover 1996]

  Implémentation sur combien de qubits ?

  1995 : 2 [ENS], 1998 : 3,

  2000 : 5 [IBM] - 7 [Los Alamos]

  2005 : 10 [Waterloo]

Comment programmer en quantique ?

Rappels

- Machine de Turing, calculabilité, universalité : [Turing 1936]
- Proposition : EDVAC (Electronic Discrete VAriable Computer) [von Neumann 1945]
- Premier ordinateur : Mark I [Robinson-Tootill-Williams 1949]

Calcul quantique

- Idée : simulation de systèmes quantiques [Feynman 1982]
- Modèles :

  Machine de Turing : [Deutsch 1985,1989], [Bernstein-Vazirani 1993]

  Circuits quantiques : [Yao 1993]

  Automates cellulaires, Automates finis...
- Technologie:

  Première porte : 2 qubits [ENS (Haroche) 1995]

  Premier circuit : 5 qubits [IBM (Chuang) 2000]

Bit classique

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

Bit probabiliste

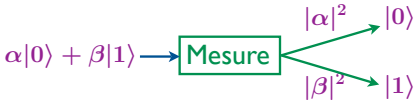
- Distribution probabiliste : $d = \begin{pmatrix} p \\ q \end{pmatrix}$ $\quad p, q \in [0, 1]$ $\quad p + q = 1$

Bit quantique (qubit)

- Etat = vecteur complexe de dimension 2 normé

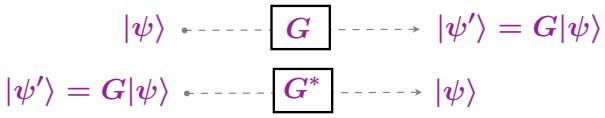
$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

- Observation = projection orthogonale probabiliste



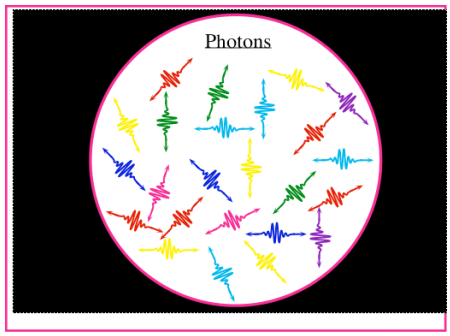
- Evolution = transformation unitaire (donc réversible) $G \in \mathcal{U}(2)$

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



Caractéristiques

- direction
- longueur d'onde
- polarisation



Sortie d'un filtre polarisant

- Lumière polarisée selon la direction du filtre.
- Lumière parallèle au filtre passe.
- Lumière orthogonale au filtre ne passe pas.

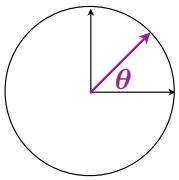
Polarisation diagonale

- Mélange statistique : NON
- Superposition quantique !

Etat polarisation

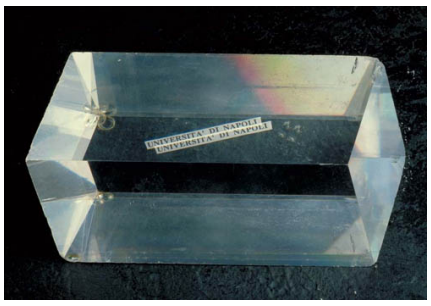
- superposition : vecteur à 2 dimensions

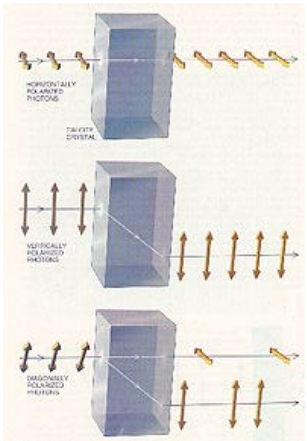
$$|\theta\rangle = \cos\theta|\rightarrow\rangle + \sin\theta|\uparrow\rangle$$



$$|0\rangle = |\rightarrow\rangle$$
$$|1\rangle = |\uparrow\rangle$$

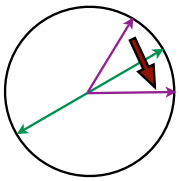
Cristal de Calcite (filtre amélioré)





Transformations qui préservent la superposition ?

- Condition nécessaire : isométrie
- Une transformation connue : la lame demi-onde
  symétrie orthogonale par rapport à son axe



- Transformation orthogonales : $G \in \mathcal{O}(2)$
  $G \in \mathbb{R}^{2\times 2}$ telle que ${}^tGG = \mathrm{Id}$

STOP Orthogonale $\Longrightarrow$ Réversible

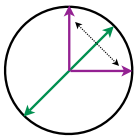
Transformation classique réversible

- Identité

$|b\rangle$ ------ Id ------ $|b\rangle$

- Négation

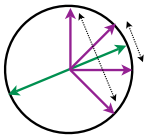
$|b\rangle$ ------ NOT ------ $|1-b\rangle$



Transformation de Hadamard

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

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



- Propriétés : pile ou face quantique

$|0\rangle \to H \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \to$ Mesure $\to$ $\frac{1}{2}$ $|0\rangle$, $\frac{1}{2}$ $|1\rangle$

$|b\rangle \to H \to H \to$ Mesure $\to |b\rangle$

STOP La mesure ne commute pas !

Exercice 1

- Montrer qu'il n'existe pas de transformation classique 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

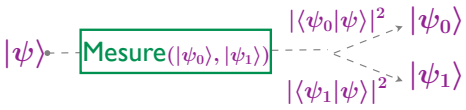
- Trouver une transformation quantique G telle que G^2 se comporte comme la porte NOT (au signe près)

  Indication : modifier légèrement la porte H

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

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

Mesure souhaitée



Porte changement de base

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

Réalisation

STOP En optique : tourner le filtre

Cryptage à l'aide d'une clé privée

One-time pad

Message :	0	1	1	0	0	1	0	1	1	1	0
Clé privée :	1	1	0	1	0	0	1	0	1	0	0
XOR bit à bit :	1	0	1	1	0	1	1	1	0	1	0

- Théorème : sécurité parfaite si chaque bit de clé est utilisé une seule fois !

  Preuve : trouver un bit du message est équivalent à trouver un bit de la clé. Si ce bit est aléatoire, alors proba de deviner = 1/2 pour chaque bit, *i.e.* identique à tirer à pile ou face !
- Pour une sécurité parfaite, la clé doit être aussi longue que le message...

DES

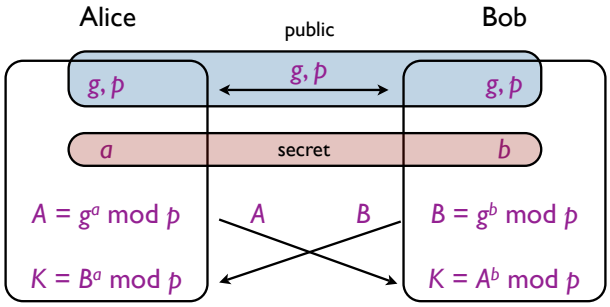
- Cryptage plus evolué qui permet d'utiliser plusieurs fois une même et plus petite clé
- Sécurité combinatoire : pas de preuve de sécurité mais toujours non cassé
- En pratique, très sûr si la clé n'est pas trop utilisée...
- Habituellement, la clé privée est générée à l'aide d'un protocole à clé publique, RSA ou Diffie-Hellman

Diffie-Hellman (1976) : distribution de clé privée

Idée : fonction à sens unique

- Calculer $g^a \bmod p$ se fait en $\log a$ multiplications
- Trouver a tq $A = g^a \bmod p$ se fait en a multiplications

Protocole



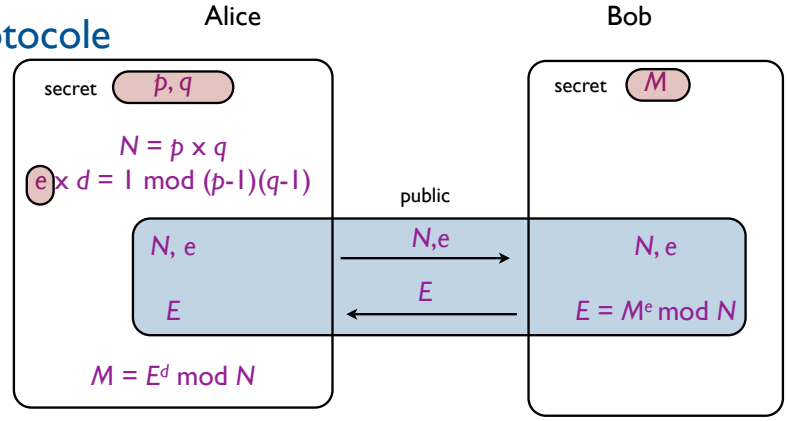
Exemple

- Alice et Bob choisissent un nombre premier p=23 et un générateur g=3
- Alice choisit un nombre secret a=6
- Alice envoie à Bob la valeur $g^a \bmod p = 36 \bmod 23 = 16$
- Bob choisit à son tour un nombre secret b=15
- Bob envoie à Alice la valeur $g^b \bmod p = 315 \bmod 23 = 12$
- Alice peut calculer la clé secrète : $(g^b \bmod p)a \bmod p = 126 \bmod 23 = 9$
- Bob obtient la même clé qu'Alice : $(g^a \bmod p)b \bmod p = 1615 \bmod 23 = 9$

Idée : fonction à sens unique

- Calculer $p \times q$ se fait en $\log p$ additions
- Trouver p, q tq $N = p \times q$ se fait en p divisions

Protocole



Théorème

- Le groupe multiplicatif de Z_N est cyclique et de cardinal $(p-1)(q-1)$
- Pour tout M (même non inversible) $M^{ed} = M \bmod N$

Exemple

- Choix des facteurs $p = 3$ et $q = 11$
- $N = p \times q = 3 \times 11 = 33$
- $(p-1) \times (q-1) = 2 \times 10 = 20$
- Choix de e premier avec 20, par ex. $e = 7$. Ce sera la clé publique.
- Calcul de la clé privée d : comme $e \times d = 1 \pmod{20}$ on trouve $d = 3$
- Encodage d'une valeur $M = 5$: $5^7 = 78125 = 2367*33+14$. Donc $E = 14$
- Déchiffrement de $E = 14$: $14^3 = 2744 = 83*33+5$. Donc $M = 5$

Commentaires

- Toute le monde peut chiffrer avec la connaisance de N et e
- Pour déchiffrer, il faut connaître/trouver d

  En particulier, il suffit de factoriser N

RSA Challenges

- http://www.rsasecurity.com/rsalabs

Challenge Number	Prize ($US)	Status	Submission Date	Submitter(s)
RSA-576	$10,000	Factored	December 3, 2003	J. Franke et al.
RSA-640	$20,000	Factored	November 2, 2005	F. Bahr et al.
RSA-704	$30,000	Not Factored		
RSA-768	$50,000	Not Factored		
RSA-896	$75,000	Not Factored		
RSA-1024	$100,000	Not Factored		
RSA-1536	$150,000	Not Factored		
RSA-2048	$200,000	Not Factored		

- RSA-640 (193 chiffres) :

3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782439716272838033415471073108501919548529007337724822783525742386454014691736602477652346609

=

163473364580925384844313388386509085984178367003309231218111085238933310010450851212118167511579

×

190087128166482211312685157393541397547189678996851549366663853908802710380210449895719126146557l

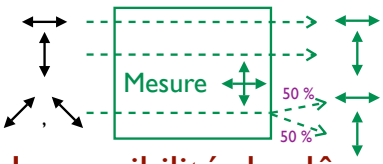
Problème

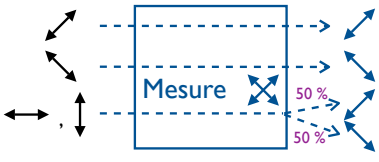
- Initialement : aucune information secrète entre Alice et Bob
- A la fin : une clé secrète connue uniquement d'Alice et de Bob

Situation en classique

- Tâche impossible, car toute l'information est sur le canal
- Cependant il est possible (outils probabilistes) de :
  - Amplifier le secret d'une clé imparfaite, en la réduisant
  - Identifier un message avec une clé secrète

Incertidude liée à la mesure

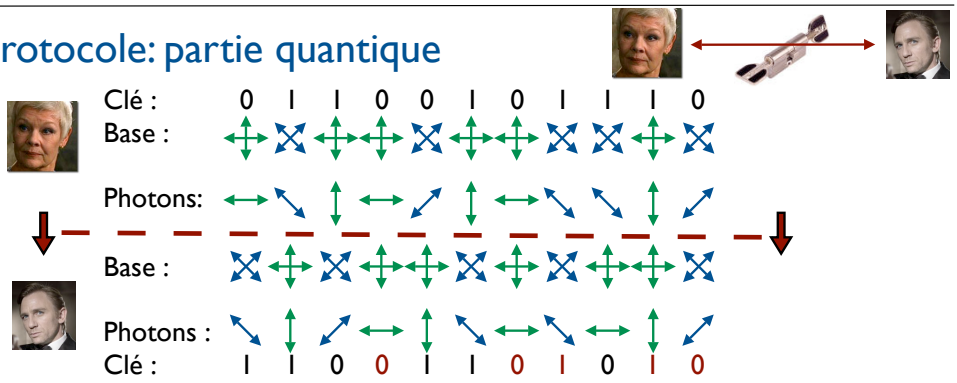




Impossibilité de clôner

- Impossible de dupliquer un état inconnu
- Preuve utilisant la linéarité des transformations

Protocole: partie quantique



Protocole : partie classique

- Révélation : Alice et Bob révèle publiquement leurs choix de base
  A&B ne conserve que les bits avec même choix de base (proba. 1/2)
  Aucune observation de la communication $\Longrightarrow$ A&B ont la même clé !
- Sécurité : A&B vérifient quelques bits à des positions aléatoires
- Amplification de secret : En utilisant des techniques classiques de cryptographie, la clé est rendue sûre avec grande probabilité en sacrifiant encore quelques bits

Vérification

- Alice et Bob sacrifient et vérifient une partie aléatoire de leur clé
- Dans un monde idéal (sans bruit), Alice et Bob rejettent leur clé s'il y a UNE erreur
- Dans le monde réel, Ils rejettent leur clé si la proportion d'erreurs est supérieure au bruit du canal (qui doit être < 11 %)

Authentification

- Génération de clé sans secrêt initial sur une ligne authentifiée
- Petite clé secrète $\Longrightarrow$ grande clé secrète (authentifiée)

Utilisation I

- Avec la clé obtenue, on peut encoder un texte de même longueur en utilisant le codage "one-time pad"
- Une foie utilisée, la clé est jetée...

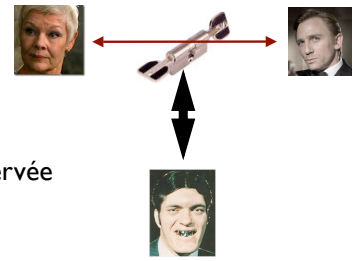
Utilisation II

- Utiliser la clé secrête dans des applications cryptographiques qui utilisent la clé plusieurs fois (ex: ssh, netscape,...)
- Attention : la sécurité n'est plus inconditionnelle

Exercice 1 : Analyse d'une attaque (sur un photon)

Question 1

- En supposant qu'aucun bit de la clé ne soit sacrifié, quelle est la longueur moyenne de la clé si N photons ont été échangés ?



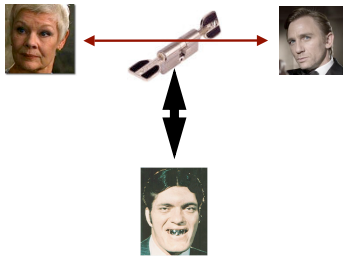
Stratégie 1

- Eve observe le photon dans une base 
- Eve renvoie le photon dans la polarisation observée

Question 2

- On suppose que 10 % des bits de la clé sont sacrifiés pour vérifier l'absence d'espionnage. On suppose aussi qu'on est dans un monde parfait (sans bruit).
- Quelle est la probabilité qu'Eve soit détectée.
- Généraliser avec k photons interceptés par Eve.

Exercice 2 : Analyse générale d'attaque (sur un photon)



Stratégie 2

- Identique à la Stratégie 1, mais toujours une base fixé d'angle θ

Question

- Reprendre la question 2 de l'exercice 1
- Calculer l'angle θ qui optimise la probabilité que l'espion trouve le bon bit.

Théorème [2000]

- Le protocole quantique de distribution de clé est inconditionnellement sûr, même sur un canal de communication bruitée (si les loies de la Mécanique Quantique sont correctes)

Systèmes à n-qubit

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 $G^*G = \mathrm{Id}$

$$|\psi\rangle \dashrightarrow \boxed{G} \dashrightarrow |\psi'\rangle = G|\psi\rangle$$

Mesure

$$\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \dashrightarrow \boxed{\text{Mesure}} \xrightarrow{|\alpha_x|^2} |x\rangle$$

Mesures partielles : cas du 2-qubit

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

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \dashrightarrow \boxed{\text{Mesure 1}} \begin{cases} \xrightarrow{||P_0|\psi\rangle||^2 = a^2+b^2} \frac{1}{||P_0|\psi\rangle||} P_0|\psi\rangle = |0\rangle \frac{a|0\rangle + b|1\rangle}{\sqrt{a^2+b^2}} \\ \xrightarrow{||P_1|\psi\rangle||^2 = c^2+d^2} \frac{1}{||P_1|\psi\rangle||} P_1|\psi\rangle = |1\rangle \frac{c|0\rangle + d|1\rangle}{\sqrt{c^2+d^2}} \end{cases}$$

Commentaires

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

Matrice densité d'un qubit

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

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

Mesure

$\rho = \begin{pmatrix} p & \alpha \\ \alpha^* & q \end{pmatrix}$ → Mesure → p : $|0\rangle$, q : $|1\rangle$ $= \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix} = \langle 0|\rho|0\rangle |0\rangle\langle 0| + \langle 1|\rho|1\rangle |1\rangle\langle 1|$

Transformation unitaire

ρ — G → $G\rho G^*$

$\rho' = G\rho G^*$ — G^* → ρ

Autres possibilités...

Utilisation des matrices densités

Théorème

- Deux systèmes de même matrice densité sont indistincts

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

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

Exercice

- Est-ce que dans le protocole de distribution de clé, un espion Eve peut apprendre qqchose d'un photon d'Alice avant la révélation des bases ?

La transformation $\mathrm{c\text{–}NOT}$

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

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

Exercices

Exercice 1

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

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

Exercice 2

- Montrer que

- Réaliser un SWAP avec des c-NOT.

Exercice 3

- 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.

L'état singlet

Exercice 4

- Soit l'état singlet $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Montrer qu'effectuer une transformation unitaire U sur le premier qubit de $|\psi\rangle$ est équivalent à effectuer la transformation U^* sur le deuxième qubit (à une phase globale près)
- En déduire, que peut importe la base de mesure, le résultat d'une mesure sur le premier qubit est toujours opposé à celui de la mesure du deuxième qubit
- Que peut-on dire de similaire sur la paire EPR de l'exercice 3 ?

Exercice 5

- 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

Trace partielle d'un 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

- 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

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

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

Exercice

- Vérifier les exemples ci-dessus
- Pourquoi le nom de trace partielle ?

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 : $a = b = 0 \implies p = \frac{3}{4}$

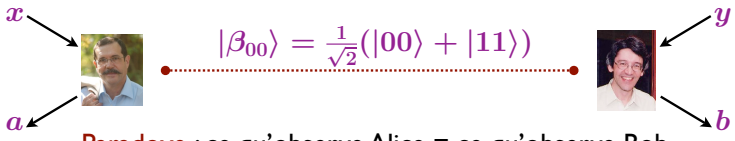
Exercice : - Théorème : la meilleure stratégie probabiliste n'est pas meilleure que la meilleure stratégie déterministe

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

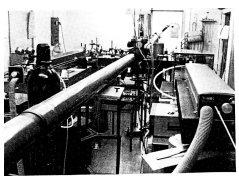
- Bob effectue une rotation d'angle $\frac{\pi}{8}$
- Si $x = 1$, Alice effectue une rotation d'angle $\frac{\pi}{4}$
- Si $y = 1$, Bob effectue une rotation d'angle $-\frac{\pi}{4}$

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]



Paradoxe GHZ

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

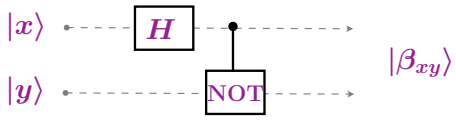
- Alice, Bob et Charlie partagent $\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$
- Protocole pour Alice/Bob/Charlie :

  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.

Application des mesures de Bell

Changement de base de Bell



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

Superdense coding

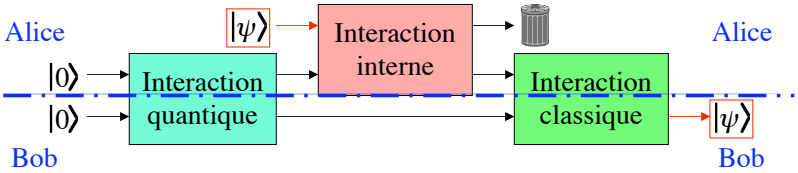
$$\mathrm{FLIP} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Alice et Bob partagent une paire EPR $|\beta_{00}\rangle$
- Alice veut envoyer à Bob deux bits x, y
- Alice effectuent les transformations locales $\mathrm{NOT}^y \times \mathrm{FLIP}^x$
- Alice envoie son qubit à Bob
- Bob fait une mesure de Bell et récupère x, y
- Conclusion : 1-qubit = 2 bits !

Problème

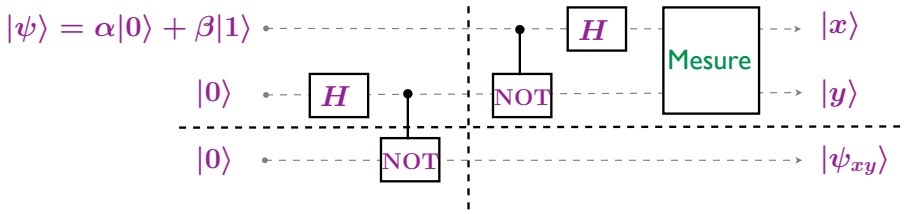
- Alice veut transmettre un qubit $|\psi\rangle$ à Bob
- Bob : position éloignée et inconnue d'Alice
- Communication possible : classique à sens unique Alice ⟶Bob

Réalisation



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

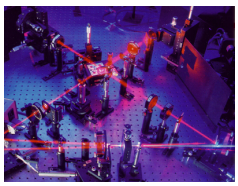
Circuit



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

Tirage à pile ou face

Problème

- Alice et Bob sont éloignés
- Ils veulent tirer à pile ou face de manière équitable

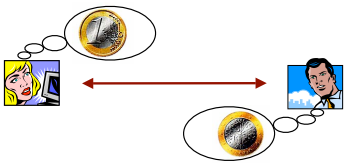
Classiquement

- Solutions basées sur des difficultés combinatoires
- Aucune solution inconditionnellement sure

Quantiquement

- Biais possible : 0,25 [Ambainis 2001]
- Biais impossible : 0,207 [Kitaev 2002]

Version faible : élection



- Alice voudrait pile
- Bob voudrait face
- Aucune impossibilité connue !
- Biais possible : 0,207 [Ambainis et al 2002]

Exercice

Essai de protocole

$$|\psi_{b,x}\rangle = \begin{cases} |0\rangle, & \text{si } b=0, x=0 \\ |1\rangle, & \text{si } b=0, x=1 \\ \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), & \text{si } b=1, x=0 \\ \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle), & \text{si } b=1, x=1 \end{cases}$$

- Alice choisit deux bits aléatoires b, x
- Alice envoie $|\psi_{b,x}\rangle$ à Bob
- Bob choisit un bit aléatoire b' qu'il envoie à Alice
- Alice envoie b, x à Bob qui vérifie l'état reçu
- Le résultat du protocole est $b \oplus b'$

Exercice

- Montrer que si Alice et Bob sont honnêtes, alors $\Pr_{x,b,b'}(b \oplus b' = 0) = \frac{1}{2}$
- Montrer que Bob ne peut pas tricher
- Montrer qu'Alice peut tricher avec certitude : biais = 0.5

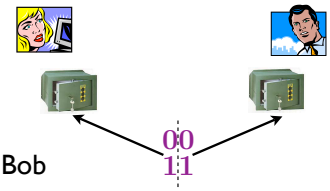
  Indication : utiliser une paire EPR

Solutions

- Ne pas prendre $|\psi_{b,0}\rangle \perp |\psi_{b,1}\rangle \implies$ biais ≤ 0.42
- Augmenter la dimension $\implies$ biais ≤ 0.25

D'où le quantique tire-t-il sa supériorité ?

De l'enchevêtrement ?



- L'"enchevêtrement probabiliste" existe
  - Tirer à pile ou face 00 ou 11
  - Partager chacun des bits entre Alice et Bob
  - Alice/Bob regarde son bit quand il le désire, son résultat est alors corrélé avec celui de Bob/Alice
- Mais l'enchevêtrement quantique est "plus fort"
  - Paradoxe EPR (violation des inégalites de Bell)

Des amplitudes complexes ?

- Non, on peut les simuler par des amplitudes réelles

$$\alpha|0\rangle + \beta|1\rangle \simeq \alpha_r|00\rangle + \alpha_i|01\rangle + \beta_r|10\rangle + \beta_i|11\rangle \qquad \mathcal{U}(2^n) \simeq \mathcal{O}(2^{2n})$$

Des amplitudes négatives ?

- Oui car possibilité d'interférences destructives

De la complexité des amplitudes ?

- Non, les amplitudes doivent être facilement calculables pour être physiquement réalisables