Plan du cours 2008 : Information Quantique

Philippe Grangier, Institut d'Optique
Frédéric Magniez, Laboratoire de Recherche en Informatique

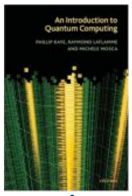
http://www.enseignement.polytechnique.fr/informatique/INF587

9 séances (13h45 - 17h30) PC 40, divisisées en

1. 21/01 (FM) : Introduction, notion de qubit, rappels de cryptographie classique, protocoles de distribution de clé
2. 28/01 (PG) : Shannon et cryptographie quantique
3. 04/02 (FM) : Paradoxe EPR, Téléportation, surperdense coding, tirage à pile ou face, mise en gage de bit avec 2 prouveurs
4. 11/02 : PAS DE COURS
5. 18/02 (PG) : Paradoxe EPR : mise en œuvre pratique
6. 03/03 (FM) : Circuits quantiques, algorithmes élémentaires, algorithme de Grover (recherche dans une liste)
7. 11/03 (FM) : Transformée de Fourier quantique, algorithme de Shor (factorisation et logarithme discret)
   (mardi, 13h45 - 17h30, s 72)
8. 13/03 (PG) : Décohérence, codes quantiques de correction d'erreurs
   (jeudi, 8h30 - 12h15, s 72)
9. 17/03 (FM/PG)

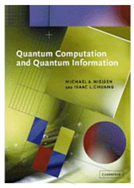
Un peu de bibliographie

An Introduction to Quantum Computing



- Auteurs : Phillip Kaye, Raymond Laflamme, Michele Mosca
- Editeur : Oxford University Press

Quantum Computation and Quantum Information



- Auteurs : Michael A. Nielsen, Isaac L. Chuang
- Editeur : Cambridge University Press

Classical and Quantum Computation

- Auteurs : A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi
- Editeur : Amer Mathematical Society
- Collection : Graduate Studies in Mathematics

Lecture Notes for Quantum Computation

- Auteur : John Preskill
- Lien URL : http://www.theory.caltech.edu/~preskill/ph229/

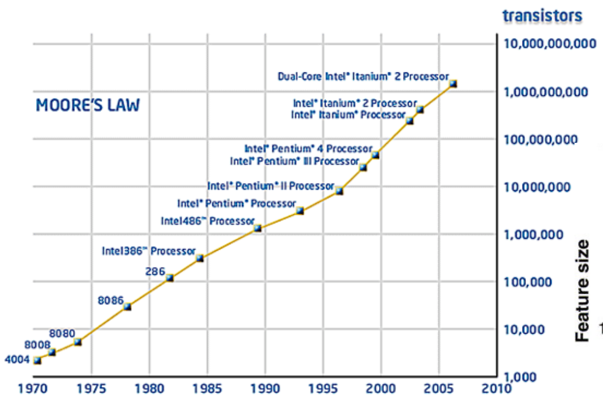
Information Quantique

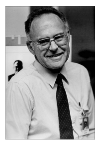
Frédéric Magniez

Cours I :
Introduction, notion de qubit
Rappels de cryptographie classique
Distribution quantique de clés
Systèmes à *n*-qubits

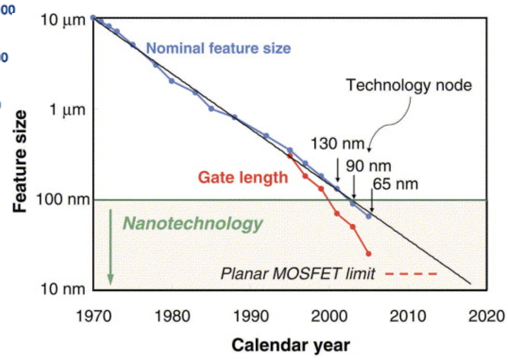
Vers la nanotechnologie

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...

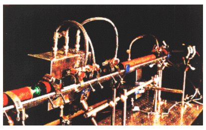
- Approche actuelle : les supprimer
- Informatique quantique : les utiliser !

La supériorité de l'informatique quantique

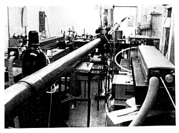
Cryptographie

- Distribution de clés secrètes [Bennett-Brassard 1984]

  Implémentation : ~100 km



Information quantique

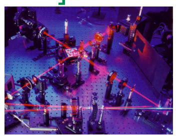


- Paradoxe EPR [Einstein-Podolsky-Rosen 1935]

  Réalisation : 1982 [Orsay]

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

  Réalisation : 1997 [Innsbruck]



Algorithmique

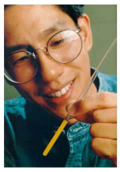
- Calcul de périodes [Simon, Shor 1994] ⇨ Factorisation, log. discret...
- Recherche dans une liste non triée [Grover 1996]

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

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

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \boxed{\text{Mesure}} \begin{cases} \xrightarrow{|\alpha|^2} |0\rangle \\ \xrightarrow{|\beta|^2} |1\rangle \end{cases}$$

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

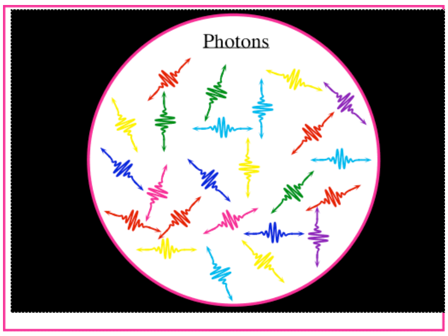
  définition: $G \in \mathbb{C}^{2\times 2}$ tq $G^*G = \mathrm{Id}$

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

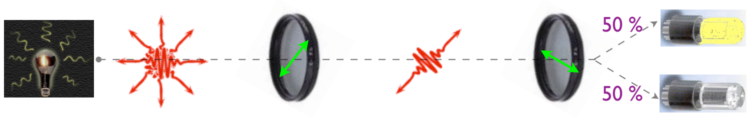
$$|\psi'\rangle = G|\psi\rangle \dashrightarrow \boxed{G^*} \dashrightarrow |\psi\rangle$$

Caractéristiques

- direction
- longueur d'onde
- polarisation



Filtre polarisant



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

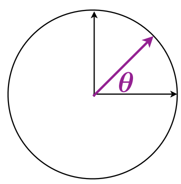
- Mélange statistique : NON
- Superposition quantique !

Le qubit : point de vue optique

Etat polarisation

- superposition : vecteur à 2 dimensions

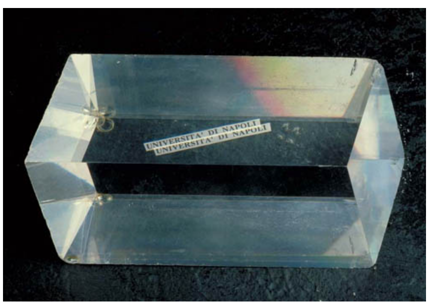
$$|\theta\rangle = \cos\theta|\rightarrow\rangle + \sin\theta|\uparrow\rangle$$

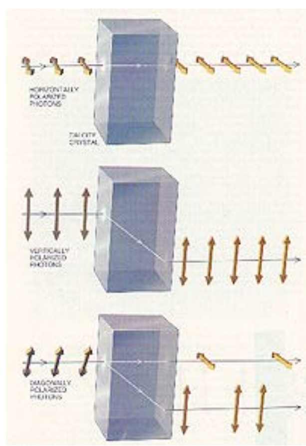


STOP

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

Cristal de Calcite (filtre amélioré)

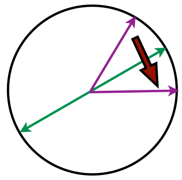




Transformations qui préservent la superposition ?

- 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 ${}^t GG = \mathrm{Id}$

Orthogonale $\Longrightarrow$ Réversible

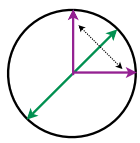
Transformation classique réversible

- Identité

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

- Négation

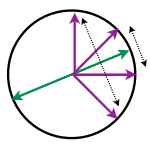
  $|b\rangle \dashrightarrow \boxed{\mathrm{NOT}} \dashrightarrow |1-b\rangle$



Transformation de Hadamard

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

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



- Propriétés : pile ou face quantique

  $|0\rangle \rightarrow \boxed{H} \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow \boxed{\text{Mesure}} \begin{cases} \xrightarrow{\frac{1}{2}} |0\rangle \\ \xrightarrow{\frac{1}{2}} |1\rangle \end{cases}$

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

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

$$|\psi\rangle \longrightarrow \boxed{\text{Mesure}(|\psi_0\rangle, |\psi_1\rangle)} \begin{cases} \xrightarrow{|\langle\psi_0|\psi\rangle|^2} |\psi_0\rangle \\ \xrightarrow{|\langle\psi_1|\psi\rangle|^2} |\psi_1\rangle \end{cases}$$

Porte changement de base

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

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

Réalisation

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

STOP En optique : tourner le filtre

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...

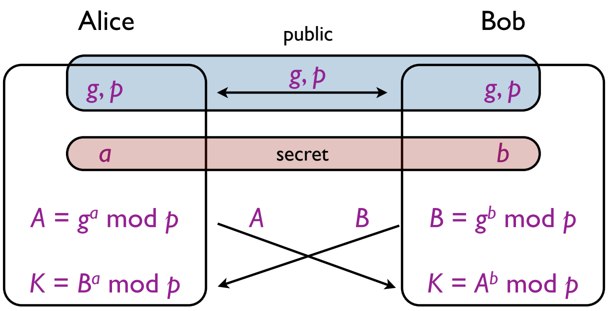
DES

- 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

Idée : fonction à sens unique

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

Protocole



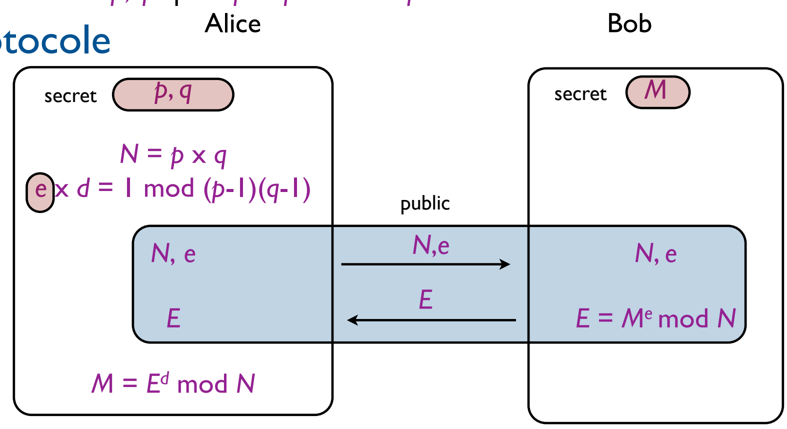
Exemple

- 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 mod p = 36 mod 23 = 16
- Bob choisit à son tour un nombre secret b=15
- Bob envoie à Alice la valeur g^b mod p = 315 mod 23 = 12
- Alice peut calculer la clé secrète : (g^b mod p)a mod p = 126 mod 23 = 9
- Bob obtient la même clé qu'Alice : (g^a mod p)b mod p = 1615 mod 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 $e \times d = 1 (\bmod 20)$ 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) :

  3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723286782437916272838
  033415471073108501919548529007337724822783525742386454014691736602477652346609

  =

  1634733645809253848443133883865090859841783670033092312181110852389333100104508151212118167511579

  x

  1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

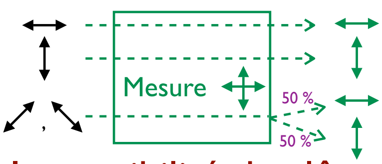
Problème

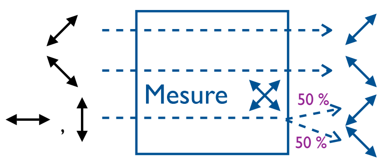
- Initialement : aucune information secrète entre Alice et Bob
- A la fin : une clé secrète connue uniquement d'Alice et de Bob

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



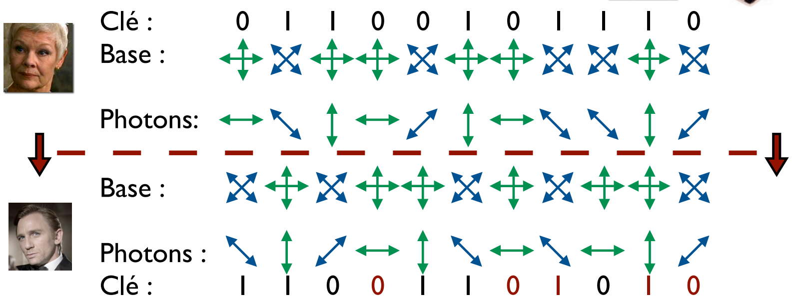


Impossibilité de clôner

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

Le protocole BB84 [Bennett-Brassard 84]

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 ⟹ 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

Cas pratique et applications

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

- ligne authentifiée : Génération de clé sans secrêt initial
- ligne non-authentifiée : Petite clé secrète ⇒ grande clé secrète

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...

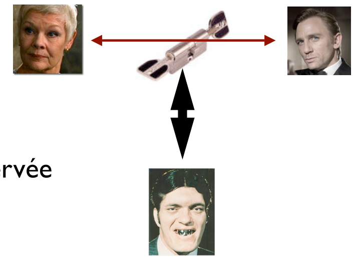
Utilisation II

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

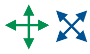
Exercice 1 : Analyse d'une attaque (sur un photon)

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 ?



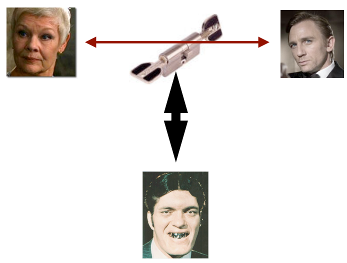
Stratégie 1

- Eve observe un 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)

Définition

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

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

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

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

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

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

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \dashrightarrow \boxed{\text{Mesure 1}}$$

$$\xrightarrow{||P_0|\psi\rangle||^2 = a^2+b^2} \frac{1}{||P_0|\psi\rangle||} P_0|\psi\rangle = |0\rangle \frac{a|0\rangle + b|1\rangle}{\sqrt{a^2+b^2}}$$

$$\xrightarrow{||P_1|\psi\rangle||^2 = c^2+d^2} \frac{1}{||P_1|\psi\rangle||} P_1|\psi\rangle = |1\rangle \frac{c|0\rangle + d|1\rangle}{\sqrt{c^2+d^2}}$$

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

$$\rho = \begin{pmatrix} p & \alpha \\ \alpha^* & q \end{pmatrix} \longrightarrow \boxed{\text{Mesure}} \begin{cases} \xrightarrow{p} |0\rangle \\ \xrightarrow{q} |1\rangle \end{cases} = \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix} = \langle 0|\rho|0\rangle |0\rangle\langle 0| + \langle 1|\rho|1\rangle |1\rangle\langle 1|$$

Transformation unitaire

$$\rho \dashrightarrow \boxed{G} \dashrightarrow G\rho G^*$$

$$\rho' = G\rho G^* \dashrightarrow \boxed{G^*} \dashrightarrow \rho$$

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