Plan du cours 05/06 Information Quantique

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

9 séances (13:45 - 18:00) divisées en

7 séances de cours

1. (FM) Notion de qubit, circuits et protocoles élémentaires
2. (PG) "Paradoxe EPR", intrication, théorème de Bell
3. (FM) Algorithmes élémentaires, algorithme de Grover (recherche dans une liste)
4. (PG) Décohérence, codes quantiques de correction d'erreurs
5. (FM) Transformée de Fourier quantique et premières applications
6. (FM) Algorithmes de Shor (factorisation, log discret) et autres récents algorithmes
7. (PG) Mises en œuvre pratique : de la cryptographie au calcul quantique

2 séances de présentation de projets

basés sur des articles et individuels

Information Quantique

Frédéric Magniez

Cours 1 :
notion de qubit, circuits, protocoles élémentaires

Plan du cours d'aujourd'hui

Partie I

- Présentation générale
- Qubit - réalisation avec des photons
- Portes, premières contradictions
- Protocole d'échange de clés (Bennett-Brassard'84)

Partie II

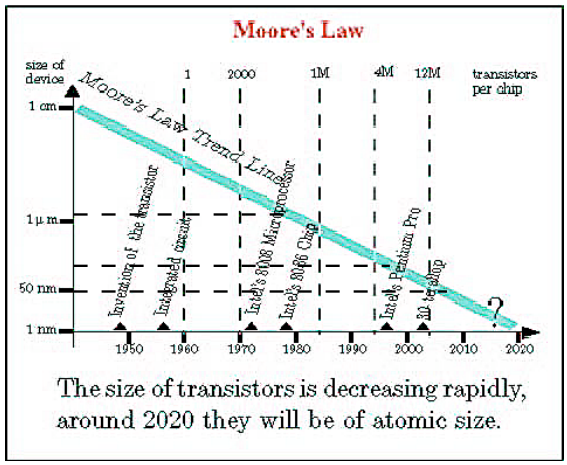
- *n*-qubit
- Porte c-Not, Circuits
- Mesures de Bell
- Superdense coding
- Téléportation

Partie III

- Paradoxe EPR
- Paradox GHZ
- Tirage à pile ou face à distance

Vers la nanotechnologie

Fin de la loi de Moore ?



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

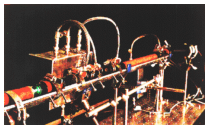
Phénomènes quantiques vers 2020...

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

La puissance du calcul quantique

Cryptographie


- Distribution de clés secrètes [Bennett-Brassard 1984]
  Implémentation : ~100 km

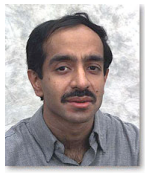


Information quantique

- 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]
  2001 : 8 [IBM]


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

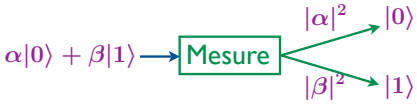
- Distribution probabiliste : $d = \begin{pmatrix} p \\ q \end{pmatrix}$ $\quad p, q \in [0, 1]$ $\quad p + q = 1$

Bit quantique (qubit)

- Etat = vecteur complexe de dimension 2 normé

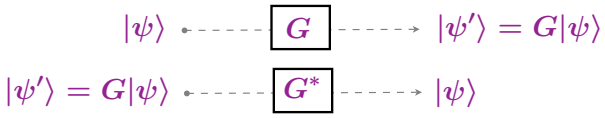
$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

- Observation = projection orthogonale probabiliste



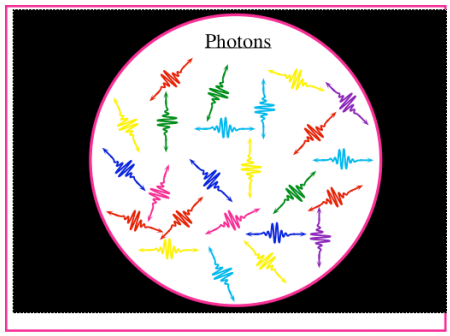
- Evolution = transformation unitaire (donc réversible) $G \in \mathcal{U}(2)$

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



Caractéristiques

- direction
- longueur d'onde
- polarisation

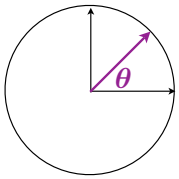


Etat polarisation

- superposition : vecteur à 2 dimensions

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

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



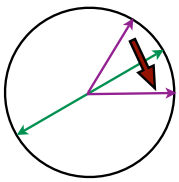
Polariseur

- mesure : projection orthonormée

L'observation perturbe le système

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 ${}^tGG = \mathrm{Id}$

Orthogonale $\Longrightarrow$ Réversible

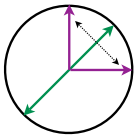
Porte classique réversible

- Identité

$|b\rangle$ ⋯ I_2 ⋯ $|b\rangle$

- Négation

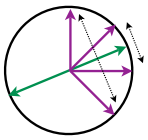
$|b\rangle$ ⋯ NOT ⋯ $|1-b\rangle$



Porte 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 $\to |0\rangle$ (½), $|1\rangle$ (½)

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

La mesure ne commute pas !

Exercice 1

- Montrer qu'il n'existe pas de porte 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

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

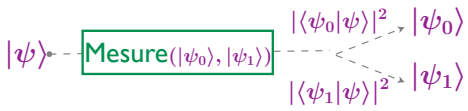
  Indication : modifier légèrement la porte H

- Montrer qu'il n'existe pas de telle porte classique

Mesure dans une autre base

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

Mesure souhaitée



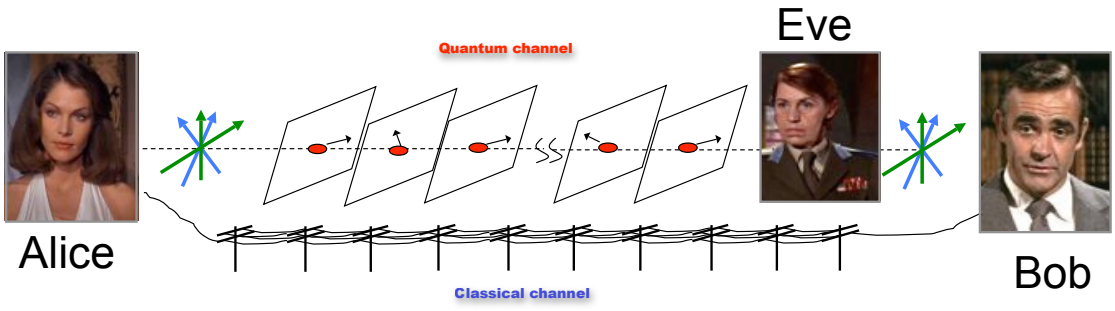
Porte changement de base

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

Réalisation

STOP En optique : tourner le polariseur

Distribution de clé quantique



Protocole de distribution de clé quantique :

* Alice code des bits sur des états non-orthogonaux d'impulsions « à un photon »
* Bob détecte les photons, puis Alice et Bob s'accordent sur la base de mesure.

* Toute tentative d'Eve pour détecter ou copier l'information sur le canal quantique va induire des perturbations (erreurs) qui seront évaluées par Alice et Bob

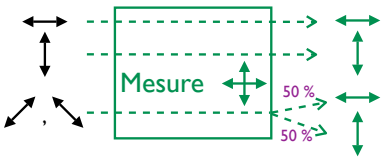
-> tant que le taux d'erreurs n'est pas trop grand, Alice et Bob peuvent obtenir une clé sans erreurs, et totalement inconnue d'Eve.

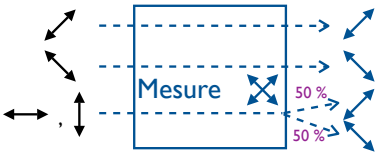
Distribution quantique de clés

Problème

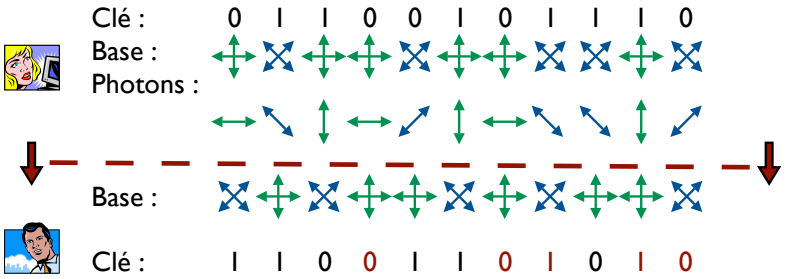
- Initialement : aucune information secrète entre Alice et Bob
- A la fin : une clé secrète connue uniquement d'Alice et de Bob

Incertitude de la mesure





Protocole



Fin du protocole

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 %)

Amplification du secret

- En utilisant des techniques classiques de cryptographie, la clé est rendue sûre avec grande probabilité en sacrifiant encore d'autre bits de la clé

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

Exercices sur la distribution de clés

Exercice 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 ?

Exercice 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).
- Si l'espion se contente de lire un photon dans une des deux bases et de renvoyer à Bob son photon résultat, quelle est la probabilité qu'il soit détecté.
- Généraliser avec k photons interceptés par l'espion.

Exercice 3

- Même question en supposant que l'espion lit et émet tous les photons reçus dans une base fixée d'angle θ.
- Calculer l'angle θ qui optimise la probabilité que l'espion trouve le bon bit.

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

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

Définition

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

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

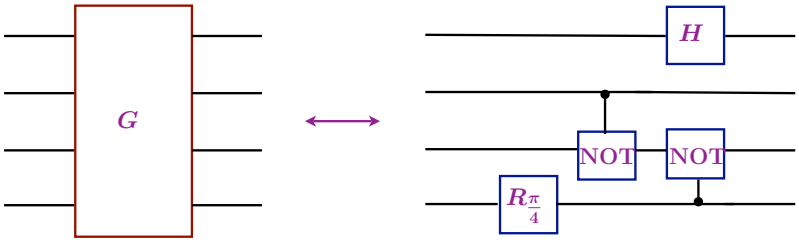
Représentation

Généralisation

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

Produit tensoriel de portes

Circuit



Théorème

- Il existe une famille universelle finie de portes à 1-qubit et 2-qubit

Exercice 1

- Montrer qu'il n'existe pas de porte 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 effectuer une transformation unitaire U sur le premier qubit de $|\psi\rangle$ est équivalent à effectuer la transformation U^t sur le deuxième qubit.

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

Classiquement

- Meilleur stratégie déterministe : $a = b = 0 \implies p = \frac{3}{4}$
- Exercice : Pourquoi ?
- Résultat : une stratégie probabiliste optimale est obtenue avec une stratégie déterministe optimale

Quantiquement

- Alice et Bob partagent une paire EPR
- 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 $-\frac{\pi}{4}$
- Alice et Bob observent leur qubit et renvoie la valeur obtenue
- Exercice : montrer que $p = \frac{2+\sqrt{2}}{4} \approx 0.85$

Paradoxe GHZ

Jeu

- Alic, 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

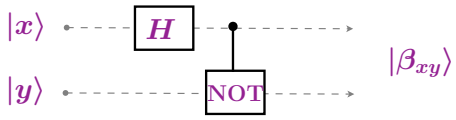
- Alice, Bob et Charlie partagent $\frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$
- Protocole pour Alice/Bob/Charlie :

  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

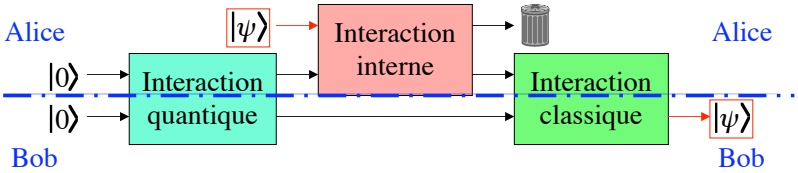
$$\mathrm{FLIP} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- 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 !

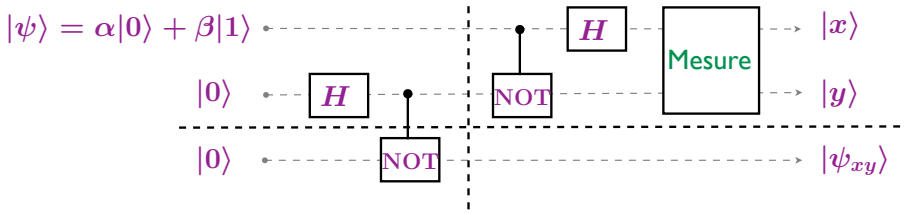
Problème

- 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



Circuit



Analyse

$$
\begin{aligned}
|\psi\rangle|0\rangle|0\rangle \mapsto & \tfrac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|0\rangle|0\rangle + |1\rangle|1\rangle) \\
= & \tfrac{1}{2}|\beta_{00}\rangle(\alpha|0\rangle + \beta|1\rangle) \\
& + \tfrac{1}{2}|\beta_{01}\rangle(\alpha|1\rangle + \beta|0\rangle) \\
& + \tfrac{1}{2}|\beta_{10}\rangle(\alpha|0\rangle - \beta|1\rangle) \\
& + \tfrac{1}{2}|\beta_{11}\rangle(\alpha|1\rangle - \beta|0\rangle)
\end{aligned}
$$

Fin du protocole

- Bob "corrige" son bit en fonction des bits reçus x, y

Tirage à pile ou face

Problème

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

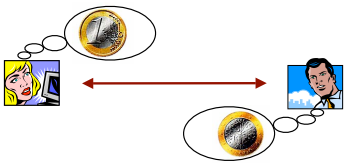
Classiquement

- 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

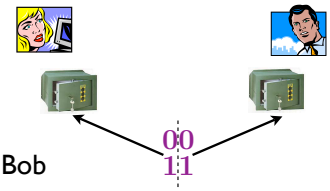
  Indication : utiliser une paire EPR

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