

Informatique quantique IFT6155

Pseudo Télépathie

Spooky action at a distance
Spukhafte Fernwirkungen

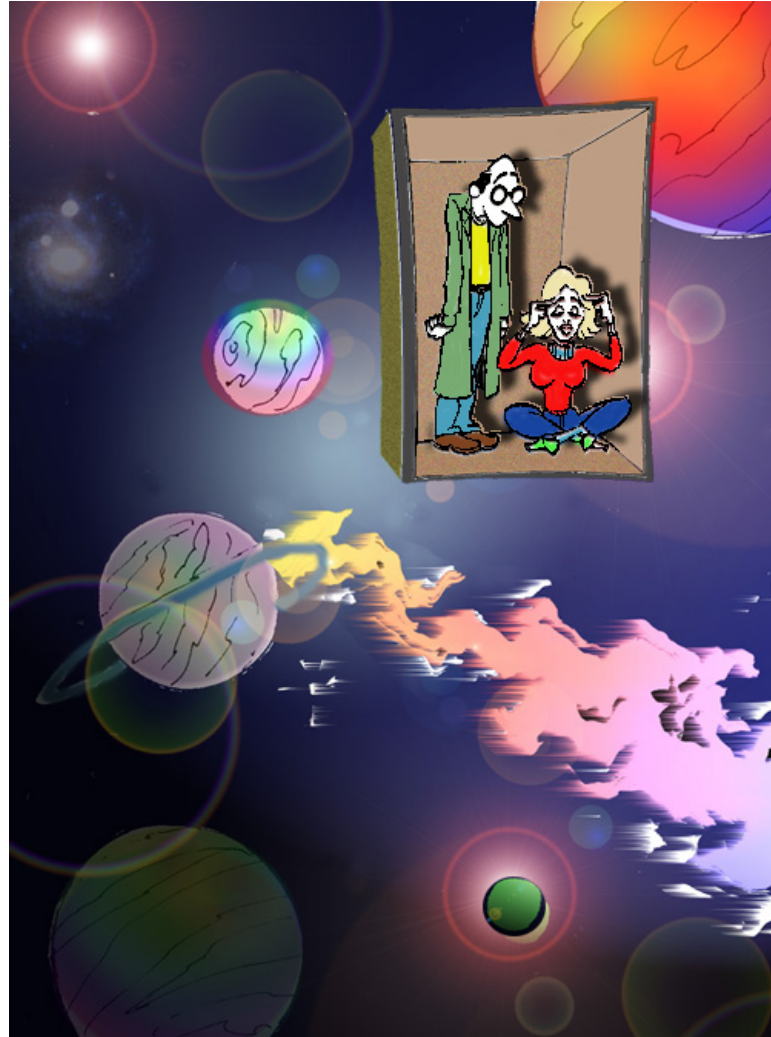
Pseudo-Télépathie?

La capacité d'accomplir une tâche nécessitant une certaine quantité de communications sans communiquer.

Pseudo-Télépathie



Pseudo-Télépathie



Mermin-GHZ

Alice, Bob et Charlie sont physiquement séparés par une *très* grande distance.

Chacun aura pour question un bit: x_A, x_B et x_C .

On leur promet que: $x_A \oplus x_B \oplus x_C = 1$.

Ils répondent un bit: y_A, y_B et y_C .

Pour gagner, il faut que: $y_A \oplus y_B \oplus y_C = x_A \wedge x_B \wedge x_C$.

Voici un tableau des questions possibles et de leurs réponses gagnantes.

001	:	000	011	101	110
010	:	000	011	101	110
100	:	000	011	101	110
111	:	111	100	010	001

Gagner est impossible

Les stratégies peuvent être probabilistes, mais, sans perte de généralité, les trois participants doivent avoir une réponse pour chacune des deux questions.

Alice: $y_A[0]$ et $y_A[1]$.

Bob: $y_B[0]$ et $y_B[1]$.

Charlie: $y_C[0]$ et $y_C[1]$.

Pour pouvoir gagner avec certitude on doit avoir:

$$y_A[0] \oplus y_B[0] \oplus y_C[1] = 0$$

$$y_A[0] \oplus y_B[1] \oplus y_C[0] = 0$$

$$y_A[1] \oplus y_B[0] \oplus y_C[0] = 0$$

$$y_A[1] \oplus y_B[1] \oplus y_C[1] = 1$$

Donc...

$$\begin{aligned} & (y_A[0] \oplus y_B[0] \oplus y_C[1]) \oplus (y_A[0] \oplus y_B[1] \oplus y_C[0]) \oplus \\ & (y_A[1] \oplus y_B[0] \oplus y_C[0]) \oplus (y_A[1] \oplus y_B[1] \oplus y_C[1]) = \\ & 0 \oplus 0 \oplus 0 \oplus 0 \oplus 1 \end{aligned}$$

$$\begin{aligned} & (y_A[0] \oplus y_A[0]) \oplus (y_B[0] \oplus y_B[0]) \oplus (y_C[0] \oplus y_C[0]) \oplus \\ & (y_A[1] \oplus y_A[1]) \oplus (y_B[1] \oplus y_B[1]) \oplus (y_C[1] \oplus y_C[1]) = 1 \end{aligned}$$

$$0 = 1 \quad !!!$$

Gagner est impossible?

Il est relativement facile de démontrer que peu importe leurs stratégies, si les questions sont posées de façon aléatoire uniforme, alors la probabilité de commettre une erreur est d'au moins 25%.

Les arbitres acceptent de faire l'expérience à plusieurs reprises, disons 100 fois. La probabilité que les joueurs réussissent à tous les coups est donc $(3/4)^{100} = 0.000000000000032072$.

Le problème est en fait que les joueurs réussissent à gagner à coup sûr!

Quelle sera la conclusion des Arbitres?

Télépathie!?!

La localité d'Einstein: Aucune influence de quelque sorte ne peut se propager plus vite que la lumière.

Chose certaine, on peut conclure que des expériences effectuées à une distance arbitraire peuvent engendrer des résultats corrélés dont la seule explication classique requiert de la communication. L'univers n'est pas *local*.

Gagner est possible

La solution qui permet à nos trois joueurs de gagner est simple.

Pour chaque exécution future du jeu, ils possèdent un état:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |001\rangle + |010\rangle + |100\rangle - |011\rangle - |101\rangle - |110\rangle - |111\rangle)$$

Leur stratégie consiste à faire H si la question est 1 puis de mesurer et de donner comme réponse le bit obtenu.

Pour voir que ça fonctionne, il suffit de constater que:

$$(H \otimes I \otimes I)|\psi\rangle = \frac{1}{2}(|000\rangle - |011\rangle + |101\rangle + |101\rangle)$$

$$(I \otimes H \otimes I)|\psi\rangle = \frac{1}{2}(|000\rangle + |011\rangle - |101\rangle + |101\rangle)$$

$$(I \otimes I \otimes H)|\psi\rangle = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle - |101\rangle)$$

$$(H \otimes H \otimes H)|\psi\rangle = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle - |111\rangle)$$

Localité

Le déterminisme d'Einstein: Dieu ne joue pas aux dés.

La mécanique quantique est fondamentalement probabiliste.

Le monde est-il déterministe ?

Existe-t-il une théorie déterministe qui décrit le monde qui serait plus précise que la mécanique quantique ?

Supposons qu'une telle théorie existe et que chaque particule ait un comportement déterministe. Chaque particule sait comment elle va réagir à n'importe quelle mesure, c'est seulement nous qui ne le savons pas.

Ceci nous donnerait une stratégie classique pour gagner à ce jeu, mais c'est impossible alors il n'existe pas de théorie déterministe qui décrit le monde.

Dieu joue aux dés!!!

Carré Magique

Analysons maintenant un jeu à deux participants.

Question: $x_A \in \{1, 2, 3\}$ et $x_B \in \{1, 2, 3\}$.

Réponse: $y_A \in \{0, 1\}^3$ et $y_B \in \{0, 1\}^3$.

Promesse: aucune.

Condition gagnante:

- 1) $y_A(x_A) = y_B(x_B)$,
- 2) $y_A(1) \oplus y_A(2) \oplus y_A(3) = 0$ et
- 3) $y_B(1) \oplus y_B(2) \oplus y_B(3) = 0$.

Il est facile de voir que toute stratégie classique échouera avec probabilité au moins $1/9$. Si on regarde les trois triplets de bits que peut répondre Alice comme les lignes d'un tableau et les trois triplets de bits que Bob peut répondre comme les colonnes d'un tableau, la condition 1 demande que les deux tableaux soient identiques. La condition 2 exige que la parité de chaque ligne soit paire et la condition 3 que la parité des colonnes soit impaire. On se rend rapidement compte que c'est impossible.

Carré Magique

Si Alice et Bob partagent l'état

$$|\psi\rangle = \frac{1}{2}(|0011\rangle - |0110\rangle - |1001\rangle + |1100\rangle) \equiv \left(\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\right)^{\otimes 2}$$

Selon x_A , Alice effectuera une des trois transformations suivantes puis elle mesurera deux bits a_1 et a_2 , sa réponse sera $(a_1, a_2, a_1 \oplus a_2)$.

$$A_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} i & 0 & 0 & 1 \\ 0 & -i & 1 & 0 \\ 0 & i & 1 & 0 \\ 1 & 0 & 0 & i \end{pmatrix} \quad A_2 = \frac{1}{2} \begin{pmatrix} i & 1 & 1 & i \\ -i & 1 & -1 & i \\ i & 1 & -1 & -i \\ -i & 1 & 1 & i \end{pmatrix} \quad A_3 = \frac{1}{2} \begin{pmatrix} -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{pmatrix}$$

Selon x_B , Bob effectuera une des trois transformations suivantes puis il mesurera deux bits b_1 et b_2 , sa réponse sera $(b_1, b_2, 1 \oplus b_1 \oplus b_2)$.

$$B_1 = \frac{1}{2} \begin{pmatrix} i & -i & 1 & 1 \\ -i & -i & 1 & -1 \\ 1 & 1 & -i & i \\ -i & i & 1 & 1 \end{pmatrix} \quad B_2 = \frac{1}{2} \begin{pmatrix} -1 & i & 1 & i \\ 1 & i & 1 & -i \\ 1 & -i & 1 & i \\ -1 & -i & 1 & -i \end{pmatrix} \quad B_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix}$$

Les calculs montrant que le jeu sera gagné pour toutes les questions sont laissés en exercice.

BCT99

Entrée: (2^n bits)

Alice: a

Bob: b

Sortie: (n bits)

Alice: y

Bob: z

Contraintes:

$$a = b \Rightarrow y = z$$

$$D(a, b) = \frac{2^n}{2} \Rightarrow y \neq z$$

Note: Savoir que $D(a, b) = 2^n/2$ ne donne que $\frac{n}{2}$ bits d'information à Alice sur b .

Solution classique

Toute solution au problème **BCT99** nécessite $\Omega(2^n)$ bits de communication.
Pour $n = 1, 2, 3$ on peut tricher, mais pas pour $n = 4$.

On obtient ce résultat en regroupant des énoncés (dont la preuve est non triviale) de Brassard, Buhrman, Cleve, Galliard, Tapp, Wigderson et Wolf.

Protocole avec intrication

- Alice et Bob partagent n paires dans l'état $|\varphi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- Alice reçoit la question a ;
Bob reçoit la question b .
- Alice applique $U_A : |i\rangle \rightarrow (-1)^{a_i} |i\rangle$.
Bob applique $U_B : |i\rangle \rightarrow (-1)^{b_i} |i\rangle$.
- Ils appliquent H à chaque qubit.
- Ils mesurent;
Alice produit y et
Bob produit z .

U_A , U_B et H

L'opérateur U_A pour $n = 2$ et $a = 1011$.

$$\begin{aligned}
 U_A &= \begin{pmatrix} (-1)^{a_1} & 0 & 0 & 0 \\ 0 & (-1)^{a_2} & 0 & 0 \\ 0 & 0 & (-1)^{a_3} & 0 \\ 0 & 0 & 0 & (-1)^{a_4} \end{pmatrix} \\
 &= \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}
 \end{aligned}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} (-1)^{x \cdot y} |y\rangle$$

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n \text{ mod } 2$$

Analyse

$$|\psi_0\rangle = \left(\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_A |x\rangle_B$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{a_x} (-1)^{b_x} |x\rangle_A |x\rangle_B$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{a_x+b_x} |x\rangle_A |x\rangle_B$$

$$|\psi_2\rangle = \frac{1}{2^{3n/2}} \sum_{x=0}^{2^n-1} (-1)^{a_x+b_x} \left(\sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle_A \right) \left(\sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle_B \right)$$

$$= \sum_{y,z=0}^{2^n-1} \frac{1}{2^{3n/2}} \left(\sum_{x=0}^{2^n-1} (-1)^{a_x+b_x+x \cdot (y \oplus z)} \right) |y\rangle_A |z\rangle_B$$

Cas d'égalité: $a = b$

Supposons que $a = b$.

L'amplitude α de $|y\rangle_A|z\rangle_B$ dans $|S_2\rangle$ est

$$\begin{aligned}\alpha &= \frac{1}{2^{3n/2}} \sum_{x=0}^{2^n-1} (-1)^{a_x+b_x+x \cdot (y \oplus z)} \\ &= \frac{1}{2^{3n/2}} \sum_{x=0}^{2^n-1} (-1)^{x \cdot (y \oplus z)} \\ &= 0 \quad (\text{lorsque } y \oplus z \neq 0)\end{aligned}$$

Donc la probabilité qu'Alice et Bob observent $y \neq z$ est 0.

Cas balancé: $D(a, b) = 2^n/2$

L'amplitude α de $|y\rangle_A|z\rangle_B$ dans $|S_2\rangle$ est

$$\begin{aligned}\alpha &= \frac{1}{2^{3n/2}} \sum_{x=0}^{2^n-1} (-1)^{a_x+b_x+x \cdot (y \oplus z)} \\ &= \frac{1}{2^{3n/2}} \sum_{x=0}^{2^n-1} (-1)^{a_x+b_x} \quad (\text{lorsque } y = z) \\ &= 0\end{aligned}$$

Donc la probabilité qu'Alice et Bob observent $y = z$ est 0.

Interprétation

Théorème (BCT99):

La simulation classique de n états intriqués nécessite $\Omega(2^n)$ bits de communication.

$$n \text{ Ebits} \succeq 2^n \text{ Bits}$$

Mermin-GHZ Généralisé

Nous allons étudier une généralisation du jeu Mermin-GHZ pour n participants avec $n \geq 3$. La présentation est basée sur [Brassard, Broadbent, Tapp: 2004].

Question: $x_i \in \{0, 1\}$ pour $i = 1 \dots n$.

Réponse: $y_i \in \{0, 1\}$ pour $i = 1 \dots n$.

Promesse: $\sum_i x_i = 0 \pmod{2}$

Condition gagnante: $\frac{1}{2} \sum_i x_i = \sum_i y_i \pmod{2}$

Mermin-GHZ Généralisé

Lemme:

Soit $|\Phi_n^\pm\rangle = \frac{1}{\sqrt{2}}(|0\dots 0\rangle \pm |1\dots 1\rangle)$, $P = \{x | \sum_j x[j] = 0 \pmod{2}\}$ et $I = \{x | \sum_j x[j] = 1 \pmod{2}\}$ alors

$$H^{\otimes n}|\Phi_n^+\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in P} \alpha_x |x\rangle$$

$$H^{\otimes n}|\Phi_n^-\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in I} \alpha_x |x\rangle$$

$$|\alpha_x| = 1$$

Preuve:

Exercice...

Mermin-GHZ Généralisé

Stratégie quantique. Soit P tel que $P|0\rangle = |0\rangle$ et $P|1\rangle = i|1\rangle$. Les participants partagent de façon naturelle l'état $|\Phi_n^+\rangle$. Chaque participant j applique P si $x_j = 1$ puis applique H , mesure et retourne le résultat.

Peu importe quel participant applique P l'état sera transformé en

$$\frac{1}{\sqrt{2}}(|0\dots 0\rangle + i|1\dots 1\rangle)$$

si exactement k participants appliquent P on aura

$$\frac{1}{\sqrt{2}}(|0\dots 0\rangle + i^k|1\dots 1\rangle)$$

si le nombre de 1 est congru à 0 mod 4

(la réponse doit être paire)

alors on aura pour un certain l

$$\frac{1}{\sqrt{2}}(|0\dots 0\rangle + (i^4)^l|1\dots 1\rangle) = |\Phi_n^+\rangle$$

et donc si on applique H et mesure on aura un résultat pair. Sinon, si le nombre de 1 est congru à 2 mod 4 alors on aura pour un certain l

$$\frac{1}{\sqrt{2}}(|0\dots 0\rangle + i^2(i^4)^l|1\dots 1\rangle) = |\Phi_n^-\rangle$$

et après avoir appliqué H on obtiendra un résultat impair.

Mermin-GHZ Généralisé

Il n'existe aucune stratégie classique permettant de résoudre le problème à coup sûr.

Si $n = 3$ on a exactement Mermin-GHZ.

Si $n > 3$, supposons qu'on a une solution qui marche à coup sûr. En particulier, elle marchera si les participants 4 à n ont comme question 0. Mais dans ce cas, les trois premiers participants se retrouvent à essayer de résoudre Mermin-GHZ.

Mermin-GHZ Généralisé

Théorème: Dans le jeu Mermin-GHZ généralisé, la proportion maximale de bonnes réponses est $\frac{1}{2} + \frac{1}{2^{\lfloor n/2 \rfloor}}$.

Preuve:

Soit $S_{ij} = 1$ si la réponse du joueur i à la question j est 0 et $S_{ij} = -1$ si la réponse du joueur i à la question j est 1. Notez qu'une parité paire correspond à un produit 1 et une parité impaire à un produit -1.

Soit $\delta(x)$ le nombre de 1 dans x et s défini par

$$s = \prod_{j=1}^n (S_{j0} + iS_{j1}) = \sum_{x \in \{0,1\}^n} \left(i^{\delta(x)} \prod_{j=1}^n S_{jx_j} \right)$$

où la deuxième équation est obtenue en faisant l'expansion du produit en une somme de termes. Chaque terme correspond à une question possible (respectant la promesse ou non).

Chaque terme de la somme prend pour valeur $1, -1, i$ ou $-i$.

Mermin-GHZ Généralisé

$$s = \prod_{j=1}^n (S_{j0} + iS_{j1}) = \sum_{x \in \{0,1\}^n} \left(i^{\delta(x)} \prod_{j=1}^n S_{jx_j} \right)$$

Si la question ne respecte pas la promesse alors le nombre de 1 sera impair et le terme aura comme valeur i ou $-i$.

Si $\delta(x) \equiv 0 \pmod{4}$ et que la réponse est paire (bonne réponse) alors le terme aura comme valeur 1.

Si $\delta(x) \equiv 0 \pmod{4}$ et que la réponse est impaire (mauvaise réponse) alors le terme aura comme valeur -1.

Si $\delta(x) \equiv 2 \pmod{4}$ et que la réponse est paire (mauvaise réponse) alors le terme aura comme valeur -1.

Si $\delta(x) \equiv 2 \pmod{4}$ et que la réponse est impaire (bonne réponse) alors le terme aura comme valeur 1.

On conclut donc que $Re(s)$ est le nombre de bonnes réponses moins le nombre de mauvaises réponses.

Notez que $S_{j0} + iS_{j1} = \sqrt{2}e^{ia_j\pi/4}$.

Si n est pair alors $s = \prod_{i=1}^n \sqrt{2}e^{ia_j\pi/4} \in \{2^{n/2}, -2^{n/2}, i2^{n/2}, -i2^{n/2}\}$ et donc $Re(s) \leq 2^{n/2}$.

Si n est impair alors $s = \prod_{i=1}^n \sqrt{2}e^{ia_j\pi/4} \in \{2^{n/2}(\pm \frac{1}{\sqrt{2}} \pm \frac{i}{\sqrt{2}})\}$ et donc $Re(s) \leq 2^{(n-1)/2}$.

QED

Mermin-GHZ Généralisé

Théorème: Dans le jeu Mermin-GHZ généralisé, la probabilité maximale de succès est $\frac{1}{2} + \frac{1}{2^{\lfloor n/2 \rfloor}}$.

Preuve

Une stratégie probabiliste correspond à une distribution probabiliste de stratégies déterministes. Soit p_i la probabilité que la stratégie i soit choisie et q_i la proportion pour cette stratégie.

Si p est la probabilité de succès alors $p = \sum_i p_i q_i$.

Clairement, toutes les q_i ne peuvent être inférieures à p .

Cette borne peut être atteinte avec une stratégie simple.

QED

Mermin-GHZ Généralisé

Si on réalise une expérience, il y aura nécessairement des erreurs expérimentales. Jusqu'à quel taux d'erreurs obtiendra-t-on des résultats ne pouvant pas être expliqués avec une théorie déterministe locale?

Nous allons utiliser un modèle d'erreur simple. Nous supposons que l'appareil effectue la mesure de façon parfaite, mais qu'il affichera le résultat avec probabilité p et le résultat inverse avec probabilité $1 - p$.

Théorème: Avec un taux d'efficacité de $p \leq \frac{1}{2} + \frac{\sqrt{2}}{4} \simeq 85\%$ (avec le modèle décrit plus haut) et n suffisamment grand, les résultats obtenus ne peuvent être expliqués par une théorie locale déterministe.

Mermin-GHZ Généralisé

Théorème: Avec un taux d'erreurs $p \leq \frac{1}{2} + \frac{\sqrt{2}}{4} \simeq 85\%$ (avec le modèle décrit plus haut) et n suffisamment grand, les résultats obtenus ne peuvent être expliqués par une théorie locale déterministe.

Preuve:

Il suffit de trouver pour quel p la probabilité de succès devient plus grande que $\frac{1}{2} + \frac{1}{2^{\lfloor n/2 \rfloor}}$ qui est la limite pour un protocole local.

La probabilité de réussite est donnée par la probabilité d'avoir un nombre pair d'erreurs. Cette probabilité est donnée par

$$p_n = \sum_{i \text{ pair}} \binom{n}{i} p^{n-i} (1-p)^i = \frac{1}{2} + \frac{(2p-1)^n}{2}.$$

Donc on obtient des résultats localement inexplicables si

$$p_n = \frac{1}{2} + \frac{(2p-1)^n}{2} > \frac{1}{2} + \frac{1}{2^{\lfloor n/2 \rfloor}}$$

Pour $n = 3$ on obtient $p > 89.7\%$, pour $n = 5$ on obtient $p > 87.9\%$ et en prenant la limite on obtient que pour tout ϵ il existe n suffisamment grand tel que $p > \frac{1}{2} + \frac{\sqrt{2}}{4} + \epsilon$ implique que les résultats ne peuvent pas être expliqués localement.

QED