Causalité informationnelle : l'information est-elle un bon fondement pour la physique quantique?

Mathys Rennela
Sous la direction de Iordanis Kerenidis (CNRS)

Master 1 Informatique 2011-2012
Université Paris 7 Diderot

Résumé

Dans la théorie de la communication quantique, on considère des échanges entre deux individus, que l'on nomme Alice et Bob. Ces échanges se font via des dispositifs expérimentaux dont les possibilités sont prédéfinies.

Lors d'une communication quantique, Alice partage avec Bob un dispositif exploitant la physique quantique. Par ce dispositif, tout en étant éloigné géographiquement, Alice et Bob peuvent tenter de communiquer pour atteindre un objectif commun, comme le calcul du résultat d'une fonction ou l'échange de données.

Le principe de causalité informationnelle est un nouveau principe physique qui stipule que Bob ne peut pas acquérir plus d'information (en quantité) que ce qu'Alice lui a envoyé. Étant donné que ce principe permet de distinguer la théorie quantique des théories qui ne respectent pas tous les principes de la mécanique quantique, il semble qu'il s'agit d'un des principes qui régit la physique.

L'objectif des chercheurs en informatique quantique travaillant sur ce principe est de s'en servir pour faire découler de la notion d'information des éléments fondamentaux de la physique quantique. Néanmoins, on peut imaginer un certain nombre de théories différentes de la théorie quantique et pour lesquelles on ne sait pas si le principe de causalité informationnelle est respecté.

Durant ce stage, nous avons cherché à effectuer une présentation claire de l'état de la recherche sur le principe de causalité informationnelle et à identifier les limites des différentes approches proposées.

Table des matières

Introduction

La mécanique quantique est sans doute, de toutes les théories physiques actuelles, celle dont la formulation mathématique paraît la plus mystérieuse [1]. En particulier, la mécanique quantique est décrite par son formalisme mathématique et il n'existe actuellement pas de principe qui permettrait de caractériser cette théorie. De nombreux physiciens tels que Roger Penrose [2] avancent l'idée que la théorie quantique est incomplète. D'un formalisme simple, les fondements de la mécanique quantique semblent contre-intuitifs et la théorie quantique de l'information a au départ été développée pour permettre une meilleure compréhension de la mécanique quantique.

Le développement du concept de causalité informationnelle (*information causality*) relève d'une tentative de décrire la mécanique quantique grâce à la théorie de l'information, autant que d'une tentative de justifier l'existence de limites lors d'une communication quantique.

L'interprétation de la mécanique quantique en terme d'information offre aux informaticiens la possibilité de s'approprier la théorie quantique avec leurs outils et aux physiciens la possibilité d'appréhender la mécanique quantique comme une théorie de l'information. Depuis son apparition en 2009 dans [Paw10], le principe de causalité informationnelle a suscité beaucoup d'engouement, avec pas moins d'une quinzaine d'articles pré-publiés sur `arXiv.org`.

Au cours de cette étude, après un exposé des concepts fondamentaux de la théorie de la communication quantique, nous avons étudié l'état des recherches sur le principe de causalité informationnelle et tenté d'en faire une synthèse. A partir des résultats du corpus d'articles étudié, nous avons simplifié et étoffé les résultats établis, pour en fournir pour la première fois une présentation claire. Je m'appuierai principalement sur [Paw10], [Bra05], [All09], [Paw11]. [3]

1 Théorie classique de l'information

La théorie classique de l'information porte sur des entités probabilistes, les variables aléatoires qui permettent d'associer des probabilités aux résultats possibles d'une expérience aléatoire.

L'entropie (*entropy*) conceptualise la mesure de l'information. Elle mesure la quantité d'information que l'on acquière en connaissant la valeur d'une variable aléatoire ou de manière équivalente, elle évalue l'incertitude sur une variable aléatoire avant que l'on connaisse sa valeur.

L'information mutuelle (*mutual information*) mesure la quantité d'information dont une variable dispose sur une autre. Elle conceptualise la réduction de l'incertitude sur une variable aléatoire du fait que l'on a des informations sur une autre variable aléatoire. On peut aussi dire que l'information mutuelle

1. Jean Bricmont, Hervé Zwirn, *Philosophie de la mécanique quantique*, 2009
2. Roger Penrose, *The Emperor's new mind : Concerning computers, minds and the laws of physics*, Oxford University Press, 1989
3. Les articles de recherches dans ce domaine étant exclusivement en anglais, j'ai pris le soin de traduire les termes et d'indiquer systématiquement en italique le terme anglais d'origine.

mesure une dépendance entre deux variables aléatoires.

Il existe deux types de définitions de ces deux notions, formulées respectivement par Claude Shannon pour les variables aléatoires et John Von Neumann pour les états quantiques.

1.1 Entropie

L'entropie $H(X)$ mesure l'incertitude sur $X = x$. En effet si un événement $X = x$ a une probabilité $p(x)$, alors si $p(x)$ faible, x est peu probable et $X = x$ apporte beaucoup d'informations (de par sa singularité, sa rareté).

Définition 1 (Alphabet)**.** *On désigne par χ et on appelle alphabet l'ensemble des résultats possibles d'une expérience aléatoire*

Définition 2 (Entropie)**.** $H(X) = -\sum_{x \in \chi} p(x) \log p(x)$ *où χ est un alphabet et $p(x) = P(X = x)$.*

Proposition 1 (Encadrement de l'entropie)**.** $\forall X, 0 \leq H(X) \leq \log |\chi|$

On dit qu'une variable aléatoire a une distribution uniforme si chacun de ses événement est équiprobable. Si X une variable aléatoire ayant une distribution uniforme, alors $H(X) = \log |\chi|$. En particulier, quand X est un bit, $H(X) = \log |\chi| = \log |\{0, 1\}| = \log 2 = 1$.

On dit qu'une variable aléatoire X est déterministe, quand il existe un x_0 tel que $X = x_0$ presque sûrement. Si X est une variable aléatoire déterministe, alors $H(X) = 0$.

L'entropie conjointe (*joint entropy*) est une définition de l'entropie pour deux variables. On la note $H(X, Y)$ ou plus rarement $H(X \wedge Y)$.

Définition 3 (Entropie conjointe)**.** *Soient X et Y deux variables aléatoires.*

$$H(X, Y) = -\sum_{x,y} p(x, y) \log(p(x, y))$$

On peut généraliser la définition de l'entropie conjointe à un nombre quelconque de variables.

Définition 4 (Entropie conjointe généralisée)**.** *Soit $n \in \mathbb{N}$. Soient $(X_i)_{1 \leq i \leq n}$ une famille de n variables aléatoires.*

$$H(X_1, \cdots, X_n) = \sum_{i=1}^{n} H(X_i | X_{i-1}, \cdots, X_1)$$

On utilise généralement cette définition pour le cas n=3

Définition 5 (Entropie conjointe de 3 variables)**.** *Soient X, Y et Z trois variables aléatoires.*

$$\forall X, Y, Z, H(X, Y, Z) = H(X) + H(Y|X) + H(Z|X, Y)$$

On peut donner une définition conditionnelle de l'entropie.

Définition 6 (Entropie conditionnelle)**.** *Soient X et Y deux variables aléatoires.*
$H(Y|X) = \sum_{x\in\chi} p(x)H(Y|X=x) = -\sum_{x,y\in\chi} p(x,y)\log p(y|x)$.

Proposition 2 (Règle de la chaîne (*Chain rule*))**.** *Soient X et Y deux variables aléatoires.*
$H(X,Y) = H(X) + H(Y|X)$.

Corollaire 1. *Soient X, Y et Z trois variables aléatoires.*
$H(X,Y|Z)) = H(X|Z) + H(Y|X,Z)$.

Proposition 3. *Pour toute variable aléatoire X, $H(X|X) = 0$*

Proposition 4 (Majoration de l'entropie conditionnelle)**.** *Pour toutes variables aléatoires X et Y, $H(X|Y) \leq H(X)$*

Il découle de cette proposition que toute information supplémentaire réduit l'incertitude.

Définition 7. *On définit une variable aléatoire X qui peut prendre les valeurs suivantes :*

$$\begin{cases} 1 & \textit{avec une probabilité } p \\ 0 & \textit{avec une probabilité } (1-p) \end{cases}$$

On notera $H(p)$ l'entropie de $H(X)$.

Proposition 5. *Soit $p \in [0;1]$ une probabilité. $H(p) = -p\log p - (1-p)\log(1-p)$*

Définition 8 (Indépendance)**.** *Deux variables aléatoires sont dites indépendantes quand elles n'ont aucune influence l'une sur l'autre.*

Proposition 6. *Soient X et Y sont deux variables aléatoires indépendantes.*

$$H(X,Y) = H(X) + H(Y)$$
$$H(X|Y) = H(X)$$
$$H(Y|X) = H(Y)$$

1.2 Information mutuelle

L'information mutuelle $I(X:Y)$ mesure la quantité d'information moyenne sur X que l'on peut espérer récupérer lorsqu'on connaît Y.

Définition 9 (Information mutuelle)**.** *Soient X et Y deux variables aléatoires.*

$$I(X:Y) = \sum_{x,y\in\chi} p(x,y)\log\frac{p(x,y)}{p(x)p(y)}$$

Proposition 7. *Soient X et Y deux variables aléatoires.*

$$H(X,Y) = H(X|Y) + I(X:Y) + H(Y|X)$$

Corollaire 2. *Soient X et Y deux variables aléatoires.*

$$\begin{aligned} I(X:Y) &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \\ &= H(X) + H(Y) - H(X,Y) \\ I(X:Y) &\leq \min\{H(X), H(Y)\} \end{aligned}$$

Tout comme pour l'entropie, on peut donner une définition conditionnelle de l'information mutuelle.

Définition 10 (Information mutuelle conditionnelle)**.** *Soient X, Y et Z des variables aléatoires.*

$$I(X:Y|Z) = H(X|Z) - H(X|Y,Z)$$

Il en découle une forme généralisée de l'information mutuelle.

Définition 11 (Information mutuelle généralisée)**.** *Soit $(X_i)_{1\leq i\leq n}$ une famille de n variables aléatoires.*

$$I(X_1, \cdots, X_n : Y) = \sum_{i=1}^{n} I(X_i : Y | X_{i-1}, \cdots, X_1)$$

Proposition 8 (Propriété de l'information mutuelle)**.** *Soient X, Y et Z trois variables aléatoires.*

$$I(X:Y) \geq 0$$
$$I(X:Y|Z) \geq 0$$
Si X et Y sont indépendants, $I(X:Y) = 0$
Si X et Y ne dépendent pas de Z, $I(X:Y|Z) = 0$

Proposition 9. $I(X:Y) = H(X) - H(X|Y) = H(Y) + H(Y|X) = I(Y:X)$

Cette proposition exprime le fait que X en dit autant sur Y que Y en dit sur X.

Corollaire 3. $I(X:X) = H(X) - H(X|X) = H(X)$

Ce corollaire nous permet de voir l'entropie comme une version réflexive de l'information mutuelle (*self-information*).

Théorème 1 (Majoration de l'entropie conjointe (*independance bound on entropy*))**.**

$$\forall X_1, \cdots, X_n, H(X_1, \cdots, X_n) \leq \sum_{i=1}^{n} H(X_i)$$

Théorème 2 (Théorème du traitement des données)**.**

$$X \to Y \to Z \implies I(X:Y) \geq I(X:Z)$$

Ce théorème traduit mathématiquement l'idée que tout traitement supplémentaire peut faire perdre de l'information, mais ne permet pas d'en gagner.

2 Théorie quantique de l'information

2.1 Formalisme mathématique de l'information quantique

Notation 1 (Vecteur-ket de Dirac)**.** *On se donne une base en posant les vecteurs* $|0\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ *et* $|1\rangle = \begin{pmatrix}1\\0\end{pmatrix}$.

Définition 12 (Bit quantique)**.** *On définit un bit quantique ou qubit*[4] *par la formule* $|\phi\rangle = \alpha\cdot|0\rangle + \alpha\cdot|1\rangle$ *où* α *et* β *sont deux nombres complexes tels que* $|\alpha|^2 + |\beta|^2 = 1$

Contrairement au bit qui ne peut valoir que deux états 0 ou 1, la valeur d'un qubit est une superposition quantique de l'état $|0\rangle$ et de l'état $|1\rangle$. Lorsqu'on mesure la valeur d'un qubit, on obtient 0 avec une probabilité $|\alpha|^2$ et 1 avec une probabilité $|\beta|^2$

Définition 13 (Produit de Kronecker)**.**
Soient deux matrices $A = (a_{i,j})_{1\leq i\leq m, 1\leq j\leq n}$ *et* $B = (b_{i,j})_{1\leq i\leq p, 1\leq j\leq q}$.
On pose $A\otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}$.
En particulier, $\forall a,b,c,d\in\mathbb{C}, \begin{pmatrix}a & b\end{pmatrix}\otimes\begin{pmatrix}c\\d\end{pmatrix} = \begin{pmatrix}ac & bc\\ad & bd\end{pmatrix}$

Notation 2. *Par commodité, on a tendance à écrire* $|\phi\rangle\,|\phi'\rangle$ *ou* $|\phi,\phi'\rangle$ *à la place de* $|\phi\rangle\otimes|\phi'\rangle$.

On a les propriétés suivantes, quand la taille des lignes et colonnes permettent la multiplication de matrice :

Proposition 10.

$$(A\otimes B)(C\otimes D) = (AC)\otimes(BD)$$
$$A\otimes(B+C) = A\otimes B + A\otimes C$$
$$tr(A\otimes B) = tr(A)\cdot tr(B) \text{ (A et B matrices carrées)}$$

2.2 Principes de l'information quantique

2.2.1 Impossibilité du clonage quantique

Un qubit est fragile face aux mesures : le fait de mesurer un état le détruit. On ne peut dupliquer un qubit car il faudrait avoir α et β pour créer un autre qubit dans le même état $\alpha\cdot|0\rangle + \beta\cdot|1\rangle$, or :

4. Par la suite, le terme bit désignera uniquement les bits classique.

(i) Lire un qubit fige son état (après mesure, il est dans l'état mesuré).

(ii) Une mesure ne donne pas α ou β mais $|0\rangle$ ou $|1\rangle$ avec une probabilité $|\alpha|^2$ et $|\beta|^2$ respectivement.

Le principe d'impossibilité du clonage (*no-cloning principle*) veut qu'on ne peut produire l'état quantique $|\phi\rangle\,|\phi\rangle$ à partir de l'état $|\phi\rangle$ sans connaître les coefficients α et β qui le déterminent. Autrement dit, on ne peut construire un dispositif capable de faire une copie exacte de n'importe quel état quantique. On peut le reformuler de manière mathématique :

Théorème 3 (Théorème d'impossibilité du clonage quantique)**.** *Soit $|\phi\rangle$ un état quantique quelconque. Il n'existe pas d'opérateur unitaire*[5] *U tel que $U\,|\phi, 0\rangle = |\phi, \phi\rangle$*

Démonstration. Raisonnons par l'absurde et supposons qu'un tel opérateur unitaire U existe.

Soit $|\phi\rangle$, $|\psi\rangle$ deux états quantiques quelconques.

$$U\,|\phi, 0\rangle = |\phi, \phi\rangle$$
$$U\,|\psi, 0\rangle = |\psi, \psi\rangle$$

U étant un opérateur unitaire, il préserve le produit scalaire donc :

$$\langle\phi|\psi\rangle = \langle 0| \cdot \langle\phi|\psi\rangle \cdot |0\rangle \underset{U}{=} \langle\phi| \cdot \langle\phi|\psi\rangle \cdot |\psi\rangle$$

De fait on a $\langle\phi|\psi\rangle = (\langle\phi|\psi\rangle)^2$. Donc $\langle\phi|\psi\rangle \in \{0, 1\}$ et de fait, $|\phi\rangle$ et $|\psi\rangle$ sont soit orthogonaux, soit égaux. U ne peut donc cloner que des états quantiques qui sont orthogonaux deux à deux et n'est donc pas un moyen général de cloner un état quantique, ce qui va à l'encontre de notre hypothèse de départ. □

Il en découle qu'il y a une quantité limitée d'information que l'on peut apprendre d'un état quantique inconnu et qu'il n'existe pas de dispositif quantique qui permet de dupliquer tout état quantique.

On peut cependant nuancer ces constatations. Tout d'abord, le théorème démontre l'impossibilité de faire une copie exacte d'états quantiques non-orthogonaux mais la copie d'états quantiques orthogonaux reste possible. Ensuite, bien qu'un clonage parfait soit impossible, il est possible de réaliser des copies imparfaites en modifiant l'état de telle façon à ce que sa copie se rapproche de l'original.

2.2.2 Intrication quantique

Deux systèmes sont dit séparés quand, étant éloignés, les observations faites sur l'un ne dépendent pas du tout de celles faites sur l'autre : il n'y a pas d'interaction.

5. Un opérateur unitaire est un opérateur linéaire U tel que $U^*U = UU^* = I$, où I est l'opérateur identité et $U*$ l'adjoint de U.

Quand deux systèmes ne sont pas séparés, on dit qu'ils sont intriqués. La théorie quantique stipule qu'il existe des systèmes qui restent corrélés, même s'ils se trouvent suffisamment distants pour qu'aucune information ne puisse être transmise entre eux. C'est pour cela que l'on qualifie la théorie quantique comme une théorie non-locale (*nonlocal theory*) car elle ne tient pas compte de la localité. On retrouve cette notion dans la formalisation mathématique suivante.

Définition 14. *On dit qu'un état $|u\rangle$ est intriqué s'il n'existe pas d'états $|x\rangle$ et $|y\rangle$ tels que $|u\rangle = |x\rangle \otimes |y\rangle$*

2.2.3 Localité, signalement et information

Le postulat d'Einstein ou principe de non-signalement (*no-signaling principle*) stipule que l'information ne peut aller plus vite qu'une vitesse limite, qui est celle de la lumière. Tout dispositif respectant le postulat d'Einstein est dit sans signalement (*no-signaling*) et nier ce postulat revient à rendre triviale tout communication puisque la transmission d'informations peut se faire de manière instantanée.

Les inégalités de Clauser-Horne-Shimony-Holt (*CHSH inequalities*), qui sont une simplification des inégalités de Bell (*Bell inequalities*), permettent de distinguer les théories locales des théories non-locales [6] et sont à la base de tous les protocoles de communication dont il sera question ici.

2.3 De l'information classique à l'information quantique

On peut considérer la théorie quantique de l'information comme une extension de la théorie classique de l'information, qui prend en compte les spécificités de la communication quantique.

John Von Neumann a défini une théorie de l'information sur des définitions de bases différentes de celle de Shannon mais dont les propriétés sont similaires. La théorie de l'information de Von Neumann se base sur la notion de densité de probabilité plutôt que sur celle de variable aléatoire. Un opérateur densité (*density operator*), aussi appelé matrice densité (*density matrix*), réunit les états quantiques possibles d'un système physique à un instant donné.

Définition 15 (Opérateur densité)**.** *Pour tout système quantique dans lequel tout état $|\phi_i\rangle$ est associé à une probabilité p_i, on définit l'opérateur densité ou matrice densité comme la matrice $\rho = \sum_i p_i |\phi_i\rangle \langle\phi_i|$*

Example 1. *Le qubit $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ a pour opérateur densité $\rho = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$*

On définit l'entropie de Von Neumann, qui est l'équivalent quantique de l'entropie de Shannon, de la manière suivante en la notant S pour la différencier.

6. Pour être plus précis, les inégalités de Bell ont permis aux physiciens de distinguer la physique quantique (théorie non-locale) de la physique classique (théorie locale). En effet, alors que ces inégalités doivent toujours être vérifiées selon la physique classique, la physique quantique permet d'envisager des protocoles expérimentaux pour violer ces inégalités. Par leur construction, ces inégalités sont respectées si la théorie est locale et ne sont pas respectées si la théorie est non-locale.

Définition 16 (Entropie de Von Neumann)**.** $S(\rho) = -\mathrm{Tr}\rho\log\rho = -\sum_{i=1}^{n}\lambda_i \log\ \lambda_i$ *où* ρ *est un opérateur densité d'un espace de Hilbert à n dimensions.* $(\lambda_i)_{1\leq i\leq n}$ *est la famille de ses valeurs propres.*

Proposition 11 (Propriétés de l'entropie au sens de Von Neumann)**.**

$$S\Big(\sum_{i=1}^{k}\lambda_i\,\rho_i\Big)\ \geq\ \sum_{i=1}^{k}\lambda_i\,S(\rho_i)$$
$$S(\rho_A\otimes\rho_B) = S(\rho_A) + S(\rho_B)$$
$$|S(\rho_A)\ -\ S(\rho_B)|\ \leq\ S(\rho_{AB})\ \leq\ S(\rho_A)\ +\ S(\rho_B)$$

Définition 17 (Information mutuelle de Von Neumann)**.**

$$I(A:B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$$
$$I(A:B|C) = S(\rho_{AC}) + S(\rho_{BC}) - S(\rho_{ABC}) - S(\rho_C)$$

Il existe un théorème qui va maintenant nous permettre d'évaluer quelle quantité d'information on a réussi à encoder.

Théorème 4 (Théorème d'Holevo [7])**.**

$$\boxed{I(X:Y) \leq S(\rho) - \sum_i p(i)S(\rho_i)}$$

Le théorème d'Holevo permet de donner une borne supérieure à l'information qui est accessible.

Définition 18 (Information d'Holevo)**.** *La limite* $\chi = S(\rho) - \sum_i p(i)S(\rho_i)$ *définit par le théorème d'Holevo est appelée information d'Holevo.*

Corollaire 4 (Théorème faible d'Holevo [8])**.**

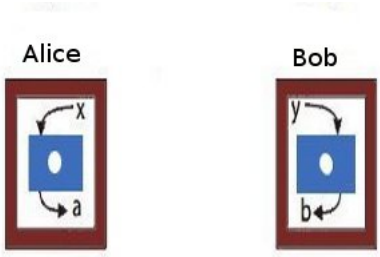
$$\boxed{I(A:B) \leq S(\rho) \leq \log\ n}$$

Le théorème d'Holevo nous dit que la quantité d'information accessible est limitée par l'information d'Holevo χ. Autrement dit, il implique que n qubits ne peuvent représenter qu'au plus n bits classiques. Ce qui peut être surprenant compte tenu de la puissant des bits quantiques par rapport aux bits classiques.

2.4 Jeu de Clauser-Horne-Shimony-Holt

Les recherches en théorie quantique de l'information qui nous intéressent ici concernent essentiellement des expériences de pensée que nous allons maintenant expliciter.

7. [Ved06], p.71-73 ; [Nie00], pp.528-536
8. [Tim04], pp. 25



Dans le jeu de Clauser-Horne-Shimony-Holt [9] (*Clauser-Horne-Shimony-Holt game*), abrégé jeu de CHSH (*CHSH game*), Bob doit essayer de deviner ce qu'a écrit Alice. On cherche à déterminer la probabilité avec laquelle Bob devine le bon résultat et cette probabilité dépend de la théorie considérée, qui détermine les corrélations qui peuvent exister entre les informations dont disposent Alice et Bob avant de commencer à jouer.

D'une manière totalement équivalente, on peut considérer qu'Alice et Bob souhaitent échanger des informations mais qu'Alice ne peut en envoyer qu'une partie à Bob, qui souhaite déterminer la probabilité que les informations qu'il a après l'échange sont correctes.

On considère dans ce jeu la théorie classique de l'information, la théorie quantique de l'information mais aussi des théories hypothétiques, au delà de la théorie quantique, qui permettent par exemple des corrélations plus fortes ou une communication instantanée.

L'exemple extrême de dispositif aux corrélations plus fortes que la théorie quantique sont appelés boîtes de Popescu-Rohrlich (*Popescu-Rohrlich box*). Dans le cas des boîtes de Popescu-Rohrlich, il suffit qu'Alice transmette un seul et unique bit pour que Bob ait accès à tous les bits d'Alice. Bob gagne à tous les coups. Autrement dit, la communication est triviale, ce qui n'est jamais le cas en mécanique quantique et qui ne semble pas non plus être le cas dans la nature.

La probabilité de gain dépend de la stratégie choisie par Alice et Bob. On la définit d'une manière générale de la manière suivante.

Définition 19 (Probabilité de gain)**.**

$$\boxed{p_{CHSH} = \frac{1}{4} \sum_{x,y=0}^{1} P(a \oplus b = xy | x, y)}$$

Il est possible de démontrer que selon la théorie choisie, il existe des stratégies optimales. Par définition, la probabilité p_{PR} de gagner avec une boîte de Popescu-Rohrlich est de 1.

Si Alice et Bob ne communiquent pas, Bob n'a aucun moyen de gagner de l'information de la part d'Alice et doit donc choisir entre répondre 0 et répondre 1. La meilleure stratégie pour Bob est de ré-

9. Ce jeu doit son nom au fait qu'il permet de distinguer les théories locales des non-locales, puisque par construction il limite les possibilités de gain si l'on joue en utilisant une théorie locale.

pondre systématiquement 0, on a $b = 0$ et donc $p_{CHSH} = \frac{1}{4}\sum_{x,y=0}^{1} P(a = xy|x, y)$. Si $a = 0$, dans $\frac{3}{4}$ des cas, x ou y est nul. Avec cette stratégie, Bob gagne dans $p_C = \frac{3}{4} \approx 75\%$ des cas.

On peut démontrer que dans le cas de la théorie quantique, on a une stratégie optimale si Alice et Bob disposent de boîtes qui leur permettent de partager un état intriqué $\frac{|00\rangle - |11\rangle}{\sqrt{2}}$ aussi appelé état de Bell (*Bell state*). De telles systèmes quantiques sont appelés boîtes de Einstein-Podolsky-Rosen (*EPR pairs*) et permettent de donner une probabilité de gain optimale $p_Q = cos^2(\frac{\pi}{8}) = \frac{2+\sqrt{2}}{4} \approx 85\%$ [10]. Cette valeur est aussi appelée limite de Tsirelson[Tsi80].

2.5 Boîtes non-locales, boîtes sans signalements

Une boîte (*box*) est un dispositif imaginaire avec un port entrée-sortie qu'un individu cherche à utiliser pour communiquer avec un autre individu éloigné géographiquement mais qui possède lui aussi une boîte. Les possibilités d'interaction dépendent de la théorie choisie [11].

En théorie de l'information quantique, les boîtes de Popescu-Rohrlich sont l'exemple paradigmatique de dispositif permettant une communication triviale. Elles font parties de la famille bien plus large des boîtes non-locales (*nonlocal boxes*), c'est à dire des boîtes respectant les principes d'une théorie qui ne tient pas compte de la localité de l'information. Les boîtes non-locales sont elles-même incluses dans une famille bien plus large, celle des boîtes sans signalement (*no-signalling boxes*), c'est à dire de toutes les boîtes qui respectent le postulat d'Einstein.

Si l'on joue au jeu de CHSH en définissant la probabilité de gain par exemple $p_{CHSH} = \frac{1}{4}\sum_{x,y=0}^{1} P(a \oplus b = xy \oplus x|x, y)$ ou $p_{CHSH} = \frac{1}{4}\sum_{x,y=0}^{1} P(a \oplus b = xy \oplus 1|x, y)$, on peut définir deux nouvelles formes de boîtes non-locales, différentes des boîtes de Popescu-Rohrlich mais qui permettent aussi une communication triviale.

3 Information et fondements de la théorie quantique

3.1 Définition du principe de causalité informationnelle

La physique quantique est décrite par son formalisme. Il existe des théories plus fortes que la théorie quantique qui violent les inégalités de Clauser-Horne-Shimony-Holt tout en respectant le postulat d'Einstein. Des phénomènes "typiquement quantiques" se retrouvent aussi dans ces théories mais seule une nouvelle notion que l'on se propose ici d'étudier, la causalité informationnelle, est validée par la théorie

10. [Nie00], pp.111-119

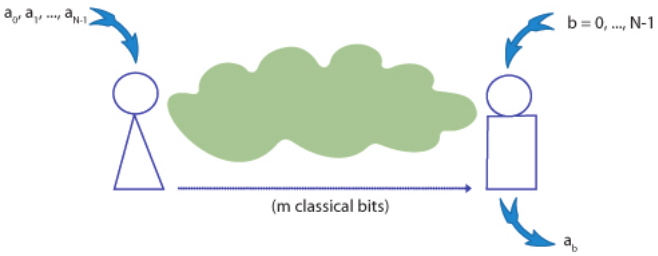
11. En fait, ce dispositif est parfaitement réalisable dans le cas de la théorie classique et de la théorie quantique : l'existence de ce document en est la preuve.

classique et la théorie quantique, et uniquement par ces deux théories.

A l'origine, la causalité informationnelle a été définie en ces termes :

> « Le gain d'information que Bob peut obtenir d'un ensemble inconnu de données d'Alice est limité à m bits en utilisant toutes les ressources locales de Bob et les m bits transmis par Alice » [12]

Si Alice transmets m bits à Bob, il ne peut acquérir une quantité d'information sur les données d'Alice supérieure à m. Ainsi la causalité informationnelle généralise le postulat d'Einstein, qui est en fait le principe de causalité informationnelle pour $m = 0$.



Alice reçoit un message $\overrightarrow{a} = a_0 \cdots a_{N-1}$. Dans un autre lieu, Bob reçoit une variable aléatoire $b \in \{0, \cdots, N-1\}$. Alice envoie m bits à Bob qui doit essayer de deviner a_b. Le principe de causalité informationnelle limite les capacités de Bob.

On pose $\mathrm{I} \equiv \sum_{K=0}^{N} I(a_K : \beta | b = K)$ (information mutuelle entre a_K et β, réponse de Bob, sachant que l'entrée est K). On définit alors le principe de causalité informationnelle de la façon suivante :

$$\boxed{\mathrm{I} \leq m}$$

L'idée fondamentale du principe de causalité informationnelle est que si on peut avoir une certitude sur m bits, il y a $N - m$ bits où l'on ne peut qu'essayer de deviner aléatoirement. Bob ne peut donner une valeur correcte que pour au plus m bits. S'il peut parfaitement deviner a_b pour $b \in \{0, \cdots, m-1\}$, il doit faire un choix complètement aléatoire pour $b \in \{m, \cdots, N-1\}$. Si Alice envoie m bits, Bob ne peut avoir accès qu'à une sous-séquence de bits : $N - m$ bits lui restent inaccessibles.

Le principe de causalité informationnelle permet d'affirmer l'impossibilité que Bob dispose de plus d'informations que ce qui lui a été envoyé. En d'autres termes, il fixe une limite aux effets (augmentation de l'information) d'une cause (transmission d'information), d'où le terme de causalité informationnelle[Paw10].

Les ressources échangées respectent le postulat d'Einstein car sinon cela signifie que l'on ouvre d'autres voies de communication alors que l'on autorise qu'un unique échange d'information entre Alice et Bob. Appelons boîtes sans signalement (*no-signaling boxes*) les dispositifs théoriques que l'on vient de construire. On les considère comme perméables à toute forme de corrélation sans signalement, même des corrélations plus fortes que ce que la théorie quantique permet. Le principe de causalité informationnelle permet de distinguer les corrélations quantiques des corrélations qui sont en dehors de la théorie quantique.

12. « Information gain that Bob can reach about previously unknown to him data set of Alice, by using all his local ressources and m classical bits communicated by Alice is at most m bits »[Paw10]

3.2 Démonstration du principe de causalité informationnelle

On partira des trois postulats suivants pour la démonstration du principe de causalité informationnelle :

Proposition 12 (Consistance (1))**.** *Si A et B sont des variables aléatoires classiques, alors $I(A : B)$ est l'information mutuelle entre A et B, au sens de Shannon.*

Proposition 13 (Inégalité du traitement de l'information (2))**.** *Soient A, B et B' trois variables aléatoires.*

$$B \longrightarrow B' \implies I(A : B) \geq I(A : B')$$

Proposition 14 (Règle de la chaîne (3))**.** *Soient A, B et C trois variables aléatoires.*

$$I(A : B, C) = I(A : C) + I(A : B|C)$$

Corollaire 5 (3')**.** *Soient A, B et C trois variables aléatoires.*

$$I(A : B, C) - I(A : C) = I(A : B|C) = I(A, C : B) - I(B : C)$$

Proposition 15 (α)**.** *Soient A et B deux variables aléatoires. $I(A : B) = 0$ quand A et B sont indépendants.*

On peut maintenant démontrer le principe de causalité informationnelle $\mathrm{I} = \sum_{K=0}^{N} I(a_K : \beta|b = K) \leq m$

Démonstration. $\overrightarrow{a} = a_0 \cdots a_{N-1}$ désigne la chaîne de tous les bits $a_0, \cdots, a_{N-1}$ contenant les données d'Alice, $\overrightarrow{x}$ désigne le message qu'elle transmet et B désigne la part de Bob avant l'échange (autrement dit, son choix de b).

En utilisant la propriété (3), on a $I(\overrightarrow{a} : \overrightarrow{x}, B) = I(a_0, \cdots, a_{N-1} : \overrightarrow{x}, B) = I(a_0 : \overrightarrow{x}, B) + I(a_1, \cdots, a_{N-1} : \overrightarrow{x}, B|a_0)$

On pose $I(\overrightarrow{a} : \overrightarrow{x}, B) = I(a_0 : \overrightarrow{x}, B) + \mathrm{I}'$ où $\mathrm{I}' = I(a_1, \cdots, a_{N-1} : \overrightarrow{x}, B|a_0)$

On a par le corollaire (3') : $I' = I(a_1, \cdots, a_{N-1} : \overrightarrow{x}, B, a_0) - I(a_1, \cdots, a_{N-1} : a_0)$.

Or pour $i \neq j$, a_i et a_j sont indépendants donc par (α), on a $I' = I(a_1, \cdots, a_{N-1} : \overrightarrow{x}, B, a_0)$.

En utilisant la proposition (2), on a $I' \geq I(a_1, \cdots, a_{N-1} : \overrightarrow{x}, B)$ (perte de l'information a_0).

Donc $I(\overrightarrow{a} : \overrightarrow{x}, B) \geq I(a_0 : \overrightarrow{x}, B) + I(a_1, \cdots, a_{N-1} : \overrightarrow{x}, B)$. En répétant ce processus, on a $I(\overrightarrow{a} : \overrightarrow{x}, B) \geq \sum_{K=0}^{N-1} I(a_K : \overrightarrow{x}, B)$.

β est obtenu à partir de b, $\overrightarrow{x}$ et B. Donc par (2), $I(a_K : \beta | b = K) \leq I(a_K : \overrightarrow{x}, B)$. D'où $I(\overrightarrow{a} : \overrightarrow{x}, B) \geq \sum_{K=0}^{N-1} I(a_K : \overrightarrow{x}, B) \geq \sum_{K=0}^{N} I(a_K : \beta | b = K) \equiv I$

On a majoré I, il faut maintenant majorer $I(\overrightarrow{a} : \overrightarrow{x}, B)$:

$$I(\overrightarrow{a} : \overrightarrow{x}, B) \underset{(3)}{=} \underbrace{I(\overrightarrow{a} : B)}_{=0 \text{ par } (\alpha)} + I(\overrightarrow{a} : \overrightarrow{x} | B) \underset{(3')}{=} I(\overrightarrow{x} : \overrightarrow{a}, B) - I(\overrightarrow{x} : B) \leq I(\overrightarrow{x} : \overrightarrow{a}, B)$$

Or $I(\overrightarrow{x} : \overrightarrow{a}, B) = H(\overrightarrow{x}) - H(\overrightarrow{x} | \overrightarrow{a}, B) \leq H(\overrightarrow{x})$ et $H(\overrightarrow{x}) \leq m$.

D'où $I \leq I(\overrightarrow{a} : \overrightarrow{x}, B) \leq I(\overrightarrow{x} : \overrightarrow{a}, B) \leq m$ □

Les trois postulats qui ont servi de base à cette démonstration sont vraies pour la théorie classique et la théorie quantique, ce qui de fait rend le principe de causalité informationnelle valable dans ces deux théories.

3.3 Limites du gain d'information lors d'une communication quantique

Le principe de causalité informationnelle limite la capacité de Bob à obtenir les informations d'Alice aux m bits transmis par celle-ci. Il nous reste à démontrer que, quand le principe de causalité informationnelle est validée, Bob ne peut obtenir tout le message d'Alice à moins que cette dernière ne lui envoie le message en totalité. Mathématiquement, cette idée se formalise par le théorème suivant si l'on appelle P_K la probabilité que Bob devine correctement a_K, l'un des bits envoyés par Alice.

Théorème 5.

$$\boxed{\sum_{K=0}^{N} h(P_K) \geq N - m}$$

Démonstration. Par définition, $\forall 0 \leq K < N, P_K = p(a_K \oplus \beta = 0 | b = K)$. D'après les définitions de l'entropie d'une probabilité, on a $h(P_K) = -P_K \log P_K - (1 - P_K) \log(1 - P_K)$

$$\begin{aligned} \forall K,\ I(a_K : \beta | b = K) &= H(a_K) - H(a_K | \beta, b = K) \\ &= 1 - H(a_K | \beta, b = K) \\ &\geq 1 - H(a_K | b = K) = 1 - h(P_K) \end{aligned}$$

En sommant de 0 à $N-1$, on obtient $\mathrm{I} \geq N - \sum_{K=0}^{N} h(P_K)$ et comme par le principe de causalité informationnelle on a $\mathrm{I} \leq m$, on a de fait $\sum_{K=0}^{N} h(P_K) \geq N - m$. □

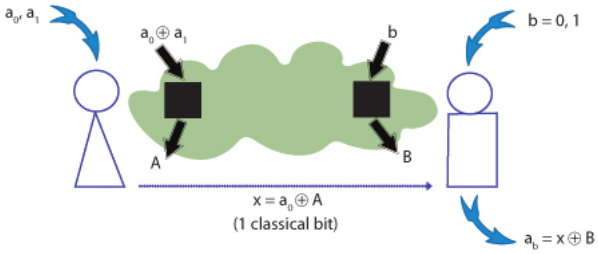
Si l'on suppose que Bob devine toujours juste, on a toujours $P_K = 1$ et donc $h(P_K) = 0$. En utilisant le théorème que l'on vient de démontrer, il en ressort que $\sum_{K=0}^{N} h(P_K) = 0 \geq N - m$ et donc $N = m$. On a ainsi démontré que si Bob veut obtenir tout le message par une méthode qui respecte le principe de causalité informationnelle, Alice doit lui envoyer le message en totalité.

3.4 Conditions de non-respect du principe de causalité informationnelle

L'intérêt principal du principe de causalité informationnelle est qu'il est en accord avec la physique classique et la physique quantique. On se propose ici pour le prouver d'expliquer à quelles conditions le principe de causalité informationnelle n'est plus respecté.

Notation 3. *On désignera par* $\oplus$ *l'addition modulo 2 i.e.* $a \oplus b \equiv a + b \mod 2$

On réalise une expérience de pensée avec deux boîtes sans signalement partagées par Alice et Bob.



Protocole de Van Dam : On considère deux boîtes dont les états quantiques sont corrélés. Alice et Bob dispose d'une boîte chacun. Alice rentre $a_0 \oplus a_1$ dans sa boîte et obtient A en sortie puis envoie le message $x = a_0 \oplus A$ à Bob. Bob rentre 0 ou 1 dans sa boîte et obtient B. Au final, grâce au message d'Alice, Bob calcule $a_b = x \oplus B$.

Alice dispose de deux bits a_0 et a_1 mais ne peut en envoyer qu'un. Les probabilités $P(A \oplus B = ab|a, b)$ décrivent les corrélations entre les entrées $a, b \in \{0, 1\}$ et les sorties $A, B \in \{0, 1\}$.

Notons P_K la probabilité que Bob ait une valeur correcte de a_K. La probabilité que Bob ait la valeur correcte de a_0 est $P_0 = \frac{1}{2} \cdot [P(A \oplus B = 0|0, 0) + P(A \oplus B = 0|1, 0)]$. La probabilité que Bob ait la valeur correcte de a_1 est $P_1 = \frac{1}{2} \cdot [P(A \oplus B = 0|0, 1) + P(A \oplus B = 1|1, 1)]$

On a $P(A \oplus B = ab|a, b) = \frac{1}{2}(1 + E)$ avec $0 \leq E \leq 1$. Cette probabilité dépend de la quantité d'information E que l'on peut acquérir avec la meilleure stratégie. $E = 1$ pour une boîte de Popescu-Rohrlich (par définition) et $E = 0$ quand les états quantiques sont non-corrélés (théorie classique). $E = \frac{1}{\sqrt{2}}$ pour une boîte d'Einstein-Podolsky-Rosen.

Dans le cas d'une boîte de Popescu-Rohrlich, Bob a tout à coup sûr : $P_0 = P_1 = 1$, $I = 2$, $m = 1$ donc le principe de causalité informationnelle n'est pas respecté.

Démonstration.

$$\begin{aligned}\mathrm{I} &= I(a_0 : a_0|b=0) + I(a_1 : a_1|b=1)\\ &= H(a_0|b=0) - H(a_0|a_0, b=0) + H(a_1|b=1) - H(a_1|a_1, b=1)\\ &= H(a_0) - H(a_0|a_0) + H(a_1) - H(a_1|a_1)\end{aligned}$$

D'où $\mathrm{I} = H(a_0) - 0 + H(a_1) - 0 = 1 + 1 = 2 > 1 = m$ □

Si une théorie satisfait le principe de causalité informationnelle, alors elle respecte la limite de Tsirelson. De fait si une théorie dépasse cette limite, elle viole le principe de causalité informationnelle. Nous allons maintenant montrer un théorème qui concerne cette fois-ci toutes les théories post-quantiques, c'est à dire toutes les théories qui possèdent des corrélations plus fortes que ce que permet la théorie quantique. [13]

Théorème 6. *Si une théorie possède des corrélations plus fortes que la théorie quantique pour le jeu de CHSH, alors elle viole le principe de causalité informationnelle.*

Démonstration. [14] Alice dispose d'un message $\overrightarrow{a}$ de taille $N = 2^n$ ($n \in \mathbb{N}$) mais ne peut en communiquer qu'un seul bit à Bob. Considérons un extension du jeu de CHSH, le n-jeu de CHSH, où Alice et Bob doivent utiliser une combinaison de n de couples de boîtes sans signalement pour jouer.

Quand $n > 1$, on divise le message $\overrightarrow{a}$ en deux sous-messages $\overrightarrow{a}'$ et $\overrightarrow{a}''$ de taille 2^{n-1} tels que $\overrightarrow{a} = \overrightarrow{a}'\overrightarrow{a}''$. On définit la fonction suivante, donnant le résultat du n-jeu de CHSH : $f_n(\overrightarrow{a}, b) \equiv a_b$. La stratégie de jeu consiste à considérer le problème de manière récursive et à obtenir les résultats pour le jeu à n couples de boites à partir des résultats du jeu à $n-1$ couples de boîtes :

$$f_n(\overrightarrow{a}, b) = f_{n-1}(\overrightarrow{a}', b') \oplus b_{n-1}[f_{n-1}(\overrightarrow{a}', b') \oplus f_{n-1}(\overrightarrow{a}'', b'')]$$

En réutilisant dans le n-jeu de CHSH la définition de E que l'on a utilisé précédemment, on a $E_j = 2P_j - 1$ où P_j désigne la probabilité de trouver a_j. Il est démontré dans [Paw10] que $P_K = \frac{1}{2}(1 + E_0^{n-k}E_1^k)$. On a démontré précédemment que $I = N - \sum_{K=1}^{N} h(P_K) = \sum_{K=1}^{N}[1 - h(P_K)]$. Il existe de plus une propriété de l'entropie qui veut que $1 - h(\frac{1+y}{2}) \geq \frac{y^2}{2\ln 2}$.

$$\begin{aligned}I &= \sum_{K=1}^{N}[1 - h(P_K)] = \sum_{k=0}^{n}\binom{n}{k}\left[1 - h(\frac{1 + E_0^{n-k} + E_1^k}{2})\right]\\ &\leq \frac{\sum_{k=0}^{n}\binom{n}{k}(E_0^2)^{n-k} + (E_1^2)^k}{2\ln 2} = \frac{(E_0^2 + E_1^2)^n}{2\ln 2}\end{aligned}$$

13. Il est à noter que lorsque l'on parle de théorie post-quantique, nous faisons référence à des théories fictives et que l'on ne peut observer que par des expériences de pensée.

14. Par soucis de concision et de clarté, nous avons simplifié et omis certains détails de la démonstration de [Paw10]

Ainsi, si l'on peut deviner plus que l'un des deux premiers bits du message d'Alice, $E_0^2 + E_1^2 > 1$, alors il existe un entier k tel que dans le n-jeu de CHSH à k couples de boîtes, $I > 1 = m$. Le principe de causalité informationnelle n'est donc pas respecté.

□

Si l'on considère enfin que Bob peut deviner chaque bit avec la même probabilité dans le n-jeu de CHSH, on obtient que $2 \cdot E^2 > 1$ et donc que $E > \frac{1}{\sqrt{2}}$. On retrouve ainsi la limite de Tsirelson car $\frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) = \frac{2+\sqrt{2}}{4}$

4 Tentatives de définitions des limites quantiques en terme de théorie de l'information

4.1 Limites des corrélations quantiques et principe de causalité informationnelle

On peut imaginer des théories post-quantiques, c'est à dire des théories dont les corrélations sont plus fortes que celles de la théorie quantique. Ces théories physiques permettent parfois de rendre les communications triviales, c'est à dire de retrouver la totalité d'un message à partir d'une partie seulement de ce message. En informatique quantique, il y a toujours une complexité de communication (*communication complexity*) et intuitivement, on peut raisonnablement penser qu'il en va de même dans la nature.

Pour un certain nombre de théories post-quantiques, on ne sait pas si la complexité de communication s'effondre ou non. Comme toutes les corrélations qui dépassent la limite de Tsirelson violent le principe de causalité informationnelle, la causalité informationnelle semble être un bon outil pour distinguer le quantique du post-quantique. Les auteurs de [All09] ont constaté que le principe de causalité informationnelle ne permet actuellement que de définir en partie les limites des corrélations quantiques (*quantum boundary*) imposées par la théorie quantique.

Le point de départ est la constatation que l'ensemble des corrélations des théories non-locales que l'on peut imaginer peut être représenté par un polytope à 8 dimensions et 24 sommets, dans lequel l'ensemble des corrélations quantiques est contenu[Bar05]. Parmi ces 24 sommets, on compte 8 boîtes non-locales et 16 boîtes locales. Les boîtes non-locales correspondent à une violation maximale des inégalités de Clauser-Horne-Shimony-Holt et les boîtes locales correspondent aux limites auxquels les inégalités de Clauser-Horne-Shimony-Holt sont respectées. De manière équivalente, on peut définir les 8 boîtes non-locales comme les dispositifs permettant de gagner à coup sûr au jeu de Clauser-Horne-Shimony-Holt avec $p_{CHSH} = \frac{1}{4}\sum_{x,y=0}^{1} P(a \oplus b = xy \oplus \mu x \oplus \nu y \oplus \sigma | x, y)$ avec $\mu, \nu, \sigma \in \{0, 1\}$. La boîte de Popescu-Rohrlich est donc l'une d'entre elles ($\mu = \nu = \sigma = 0$).

L'ensemble des corrélations des théories non-locales est obtenu en combinant différentes boîtes dont on peut faire varier l'importance en y rajoutant une pondération. Bien que l'on réussisse à retrouver les

corrélations quantiques à partir du principe de causalité informationnelle quand l'on combine une boîte non-locale et une boîte de Popescu-Rohrlich, ce n'est pas forcément le cas. Par exemple, en combinant une boîte de Popescu-Rohrlich avec une boîte locale, on peut produire des corrélations post-quantiques qui sont sous la limite du principe de causalité informationnelle.

4.2 Corrélations quantiques, non-localité et complexité de communication

Bien que les capacités en terme d'information et de communication de la théorie quantique soient plus fortes que celles de la théorie classique, elles n'en sont pas pour autant parfaites et doivent respecter la limite de Tsirelson. Des travaux ont été effectués pour légitimer cette limite[Bra05], en prenant encore pour base que la complexité de communication ne peut être triviale.

Les auteurs de [Bra05] ont démontré que toute boîte non-locale qui fonctionne avec une probabilité d'obtenir un résultat correct supérieure à $\frac{3+\sqrt{6}}{6} \approx 90.8\%$ permet d'exécuter n'importe quelle fonction booléenne avec une complexité de communication triviale, c'est à dire d'après la définition de l'article, sans communication.

Cet article fournit déjà une limite en terme de ce qui est possible en physique mais reste supérieur à la limite de Tsirelson qui n'est que de $\frac{2+\sqrt{2}}{4} \approx 85\%$. Savoir comment améliorer cette limite est une question ouverte auquel nous n'avons pu répondre puisqu'elle nécessiterait de déterminer la manière dont on pourrait utiliser l'intrication quantique pour déterminer si le résultat était optimal.

Pour faire simple, le cœur de la démonstration vient d'un lemme qui établit que si la probabilité de gagner au jeu de la majorité non-locale (*nonlocal majority*) [15] est de plus de $\frac{5}{6}$, la complexité de communication de toute fonction est triviale. De cette fraction découle la limite d'environ 90.8%.

On peut tout de même faire quelques constatations en modifiant quelque peu les méthodes utilisées pour démontrer les lemmes. La limite de $\frac{3+\sqrt{6}}{6} \approx 90.8\%$ apparaît dans la situation où l'on considère qu'une complexité de communication triviale est un cas où il n'y a pas besoin de communication pour obtenir un résultat. Mais étant donné que certaines fonctions, comme le produit scalaire, obligent Alice à transmettre à Bob tout son message pour qu'il puisse obtenir un résultat, on peut relâcher quelque peu la notion de complexité triviale. Si Alice dispose de données de taille n, on peut considérer que la complexité de communication est triviale si on arrive à calculer n'importe quelle fonction alors qu'Alice n'a envoyé qu'au plus $n-1$ bits.

Le jeu de la majorité non-locale peut se jouer à l'aide de deux boîtes non-locales. Dans la première, Alice et Bob insèrent respectivement $x' = \overline{x_1} \oplus x_2$ et $y' = y_1 \oplus y_2$, obtenant en sortie a' et b'. Dans

15. C'est une variante du jeu de CHSH où Alice et Bob disposent respectivement de 3 bits x_1, x_2, x_3 et y_1, y_2, y_3 et doivent calculer par des boîtes non-locales a et b, de telle façon à ce que $a \oplus b = Maj(x_1 \oplus y_1, x_2 \oplus y_2, x_3 \oplus y_3)$ où $Maj(u,v,w) = \lfloor \frac{u+v+w}{2} \rfloor$

la deuxième boîte, Alice et Bob insèrent respectivement $x'' = \overline{x_2} \oplus x_3$ et $y'' = y_2 \oplus y_3$, obtenant en sortie a'' et b''. Bob n'a besoin que de deux bits, x' et x'', pour effectuer à coup sur le calcul seul. La complexité de communication de ce jeu est donc de 2 bits. Si l'on dispose d'un protocole qui en utilise moins de 2, alors la complexité de communication est triviale.

Nous allons maintenant réécrire le protocole proposé par l'article en prenant en compte cette constatation. Appelons p la probabilité que la boîte non-locale donne le résultat attendu. Si l'on nomme q la probabilité que la majorité soit calculée avec deux boîtes, on a $q = p^2 + (1-p)^2$, exprimant le fait que le résultat n'est bon que si les deux boîtes donnent un bon résultat ou si elles se trompent toutes les deux. Maintenant, au lieu de considérer qu'aucune communication n'est possible, nous allons remplacer l'une des boîtes non-locales par une boîte qui, avec une probabilité γ transmette l'entrée d'Alice à Bob, qui peut dès lors calculer directement le résultat de la fonction [16], et fonctionne comme les boîtes non-locales utilisées dans l'ancien protocole sinon. Si l'on appelle q' la probabilité de réussite au jeu de majorité non-locale d'une boîte non-locale fonctionnant sur ce principe, on a alors $q' = \gamma \cdot (1 \cdot p) + (1-\gamma)[p^2 + (1-p)^2]$

On a de fait $\gamma = \dfrac{q' - p^2 - (1-p)^2}{p - p^2 - (1-p)^2}$, qui est le minimum de communication à ajouter pour gagner, en fonction de p et en espérance. Ainsi communiquer permet de baisser les exigences de performance en termes de corrélations du système. Si l'on pose $p = \dfrac{2+\sqrt{2}}{4}$, on a $\gamma \approx 0.805$. C'est le minimum de communication qui est nécessaire pour pouvoir gagner ce jeu en ne dépassant pas la limite de Tsirelson. On a ainsi établit un lien entre la complexité de communication et les limites de la théorie quantique.

Conclusion

Le principe de causalité informationnelle pose le problème de savoir si l'on peut concevoir la mécanique quantique comme une théorie de l'information. Le fait que ce principe permet de distinguer ce qui est possible dans le monde physique de ce qui ne l'est pas, peut laisser penser qu'il s'agit d'un principe fondamental qui régit notre univers. Claude Shannon mettait déjà en garde en 1956 sur le caractère explicatif de sa théorie de l'information.

> « It will be all too easy for our somewhat artificial prosperity to collapse overnight when it is realized that the use of a few exciting words like information theory, entropy, redundancy, do not solve all our problems (...) The establishing of such applications is not a trivial matter of translating words to a new domain, but rather the slow tedious process of hypothesis and experimental validation. »[Sha56]

L'idée que la notion d'information pourrait être à la base de la physique revient régulièrement dans la formulation des théories physiques. Les constatations de l'article d'origine [Paw10] semblent difficile à améliorer et il reste encore à fournir une présentation claire qui permettrait de comprendre les fondements de la mécanique quantique, d'autant que rien n'indique qu'un principe tel que le principe de causalité informationnelle permettrait d'éclairer les scientifiques dans leur compréhension de la phy-

16. Cela revient également à ce qu'Alice puisse transmettre instantanément son message à Bob.

sique, quand bien même il s'agirait d'un principe fondamental.

Il faut aussi rappeler qu'il ne s'agit pas de la première tentative d'établir la mécanique quantique comme une théorie de l'information, même si pour la première fois on a réussit à faire découler la limite de Tsirelson d'un principe informationnel. Il existe de nombreuses tentatives de reformulation de la mécanique quantique dans la théorie de l'information quantique. La réussite de cette entreprise permettait d'établir les lois de la physique en les faisant dériver de la notion d'information.

Le principe de causalité informationnelle est un modèle *ad hoc* qui force à penser la dimension entropique et causale de la physique, sans pour autant fournir aucun élément explicatif de la théorie quantique et n'a aucune capacité prédictive. Il n'en reste pas moins que les informaticiens travaillant actuellement sur la communication quantique sont en mesure de percevoir la physique quantique sous un angle informationnel grâce au principe de causalité informationnelle.

Références

[All09] J. Allcock, N. Brunner, M. Pawlowski, V. Scarani, "Recovering part of the quantum boundary from information causality", arXiv :0906.3464v3, 2009.

[Asl10] Claude Aslangul, *Mécanique quantique*, 2010.

[Bar05] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, D. Roberts, "Nonlocal correlations as an information-theoretic resource", PhysRevA.71.022101, American Physical Society, 2005.

[Bar09] H. Barnum, J. Barrett, L. Orloff Clark, M. Leifer, R. Spekkens, N. Stepanik, A. Wilce, R. Wilke, "Entropy and Information Causality in General Probabilistic Theories", arXiv :0909.5075v1, 2009.

[Bra05] G. Brassard, H. Buhrman, N. Linden, A. A. Methot, A. Tapp, F. Unger, "A limit on nonlocality in any world in which communication complexity is not trivial", arXiv :quant-ph/0508042v1, 2005.

[Cor11] Charles Corge, *L'informatique quantique : qu'est-ce et pour quoi faire ?*, 2011.

[Cov06] Thomas Cover, *Elements of Information Theory*, 2006.

[Gui68] Silviu Guiasu, Radu Theodorescu, *La théorie mathématique de l'information*, 1968.

[Har01] Yorick Hardy, Willi-Hans Steek, *Classical and quantum computing*, 2001.

[Kay07] Philip Kaye, *An Introduction to Quantum Computing*, 2007.

[Nie00] Michael A. Nielsen, Isaac L. Chuang, *Quantum computation and quantum information*, 2000.

[Paw10] M. Pawlowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, M. Zukowski, « Information Causality as a Physical Principle », arXiv :0905.2292v3, 2009.

[Paw11] M. Pawłowski, V. Scarani, « Information Causality », 2011, arXiv :1112.1142v1

[Rio07] Olivier Rioul, *Théorie de l'information et codage*, Lavoisier, 2007.

[Sha56] Claude Shannon, « The Bandwagon », 1956.

[Sag11] Sagawa, Yoshida, *Fundamentals of quantum information*, 2011.

[Tim04] Christopher Gordon Timpson, *Quantum Information Theory and The Foundations of Quantum Mechanics*, arXiv :quant-ph/0412063v1, 2004.

[Ved06] Vlatko Vedral, *Introduction to Quantum Information Science*, 2006.

[Wil12] Mark M. Wilde, « From Classical to Quantum Shannon Theory », arXiv :1106.1445v3, 2012.

[Tsi80] B.S. Tsirelson. « Quantum generalizations of Bell's inequality », *Lett. Math. Phys.*, 4 :93, 1980.