Les maths des jeux quantiques

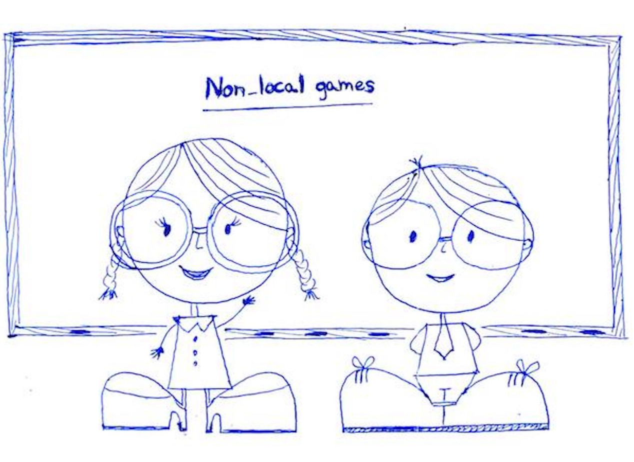
Écrit par **Rubén Martos**

Publié le 6 septembre 2023

DOI : 10.60868/y8by-1816 — CC BY-NC-ND 4.0

≥ 30 min

CRYPTOGRAPHIE PHYSIQUE



Les jeux quantiques sont des expériences de pensée destinées à mettre en évidence les effets de la mécanique quantique sur l'information. Dans cet article, nous nous intéresserons à l'un de ces jeux en particulier, dans lequel deux joueurs, Alice et Bob, élaborent ensemble une stratégie commune pour gagner le jeu, puis sont séparés et questionnés par un maître du jeu. Leurs réponses déterminent leur gain commun. L'objectif des physicien en inventant ces « jeux » est de montrer que les stratégies possibles dans le monde de la physique classique peuvent être battues en exploitant les effets quantiques.

Plan de l'article

Nous allons chercher à comprendre comment cela est possible dans le cas du jeu CHSH (inventé par Clauser, Horne, Shimony et Hett). La physique quantique va nous amener à faire un peu de géométrie complexe, c'est-à-dire à nous placer dans des espaces dont les coordonnées peuvent prendre des valeurs complexes. Le but de cet article est de montrer comment les nombres complexes, inventés par les algébristes du XVI[e] siècle, se mettent au service du physicien d'aujourd'hui.

Nous allons montrer qu'une stratégie classique déterministe permet de gagner à ce jeu dans 75% des cas tandis qu'une stratégie quantique permet d'améliorer ce score et de gagner dans plus de 85% des cas !

Avant-propos

Nous voulons utiliser les règles de la mécanique quantique dans le traitement de l'information. Le lien entre la mécanique quantique et la théorie de l'information apparaît à partir de l'observation suivante. L'unité minimale d'information dans un ordinateur est le *bit*, qui peut adopter seulement deux valeurs : soit 0 soit 1. Nous pouvons penser à introduire un « bit quantique », un *qubit*. Il devra suivre les règles de la mécanique quantique. En particulier, le *principe de superposition* permettrait au qubit d'adopter une *infinité* d'états possibles et non seulement 0 ou 1. L'état du qubit dans la réalité est indéterminé, mais lors d'une mesure explicite, nous le forcerions à se définir soit en 0 soit en 1. De manière générale, un qubit a une certaine probabilité p de valoir 1 et une probabilité $1-p$ de valoir 0. Nous allons voir comment Alice et Bob vont utiliser ce phénomène afin d'élaborer une stratégie quantique pour le jeu CHSH.

Un autre phénomène de la mécanique quantique qu'Alice et Bob vont exploiter pour la conception de leur stratégie quantique est l'*enchevêtrement quantique* (terminologie introduite par Schrödinger). Ce phénomène est interprété comme une *apparente communication* entre Alice et Bob pendant le jeu quantique malgré la séparation des joueurs. L'origine physique de cette observation se trouve dans le *paradoxe EPR* (introduit par Einstein, Podolsky et Rosen). Le paradoxe met en évidence qu'en physique quantique mesurer telle information sur une particule permet d'obtenir *instantanément et indépendamment des distances* une information sur une *autre* particule, ce qui contredit le fait que rien ne va plus vite que la vitesse de la lumière !

Pour ce qui concerne la mécanique quantique, ses principes et ses rapports avec la théorie de l'information nous renvoyons aux excellents articles [1-3] de Stephan De Bièvre.

Le jeu CHSH

Le jeu CHSH est considéré comme un précurseur du calcul quantique. En effet, en utilisant cette expérience de pensée, on peut se questionner sur l'utilité de la mécanique quantique pour améliorer les tâches de traitement de l'information. Cette perspective impose une séparation conceptuelle entre la tâche en soi (qui est toujours classique) et les méthodes ou la stratégie pour la résoudre (qui peut être quantique).

L'idée générale du jeu est la suivante. Alice et Bob se placent dans deux salles séparées de sorte qu'ils ne peuvent pas communiquer. Rappelons qu'un bit est l'unité minimale d'information qui peut valoir soit 0 soit 1. L'arbitre envoie à chacun un bit, disons x et y respectivement. Ces bits sont choisis de manière aléatoire et ils représentent les *questions* de l'arbitre. Ensuite, Alice et Bob doivent chacun *répondre* en transmettant un autre bit à l'arbitre, disons a et b, respectivement. La règle pour gagner le jeu, c'est-à-dire la condition de réussite d'Alice et Bob est que les bits-questions x et y avec les bits-réponses a et b doivent vérifier les conditions suivantes :

— si x ou y est le bit 0, alors a et b doivent être égaux ;
— si $x = 1$ et $y = 1$, alors a et b doivent être différents.

En utilisant la règle d'addition des bits, nous pouvons coder ces deux conditions avec l'équation suivante $a + b = xy$. Rappelons que les bits s'additionnent entre eux de la manière suivante :

+	0	1
0	0	1
1	1	0

Afin de gagner le jeu, Alice et Bob ont le droit de se mettre d'accord en amont sur une stratégie à suivre et ils peuvent partager des informations communes dès le départ afin de concevoir une stratégie conjointe. En pratique, l'information commune qu'Alice et Bob vont partager n'est pas quelque chose de tangible ; ce n'est pas non plus une donnée explicite de la part du maître du jeu. Il s'agit plutôt d'une conséquence des règles de la mécanique quantique, notamment de l'enchevêtrement quantique.

Formalisation mathématique du jeu

Décrivons ce jeu de manière plus mathématique. Toutes les questions et réponses du jeu étant des bits, elles appartiennent à l'ensemble $\{0,1\}$. Notons I_A et I_B les ensembles des questions pour Alice et Bob. De même notons O_A et O_B les ensembles respectifs des réponses d'Alice et Bob. On a donc

$$I_A = \{0,1\},\ O_A = \{0,1\},\ I_B = \{0,1\},\ O_B = \{0,1\}$$

Dire que l'arbitre choisit de manière aléatoire *uniformément* et *indépendamment* les bits qu'il envoie à Alice et à Bob, signifie qu'il utilise la loi de distribution uniforme sur $I_A \times I_B$. Autrement dit, l'arbitre sélectionne une question pour Alice et une autre pour Bob de manière aléatoire et chacune des questions a la même probabilité de se réaliser.

La règle pour gagner le jeu CHSH se traduit en disant que

— si $(x,y) \in \{(0,0),(0,1),(1,0)\}$, alors il faut $a = b$;
— si $(x,y) \in \{(1,1)\}$, alors $a \neq b$.

Nous allons encoder cette règle avec une fonction mathématique, disons R. La fonction R est une fonction à quatre variables : les deux questions envoyées par l'arbitre à Alice et Bob et les réponses respectives. La fonction R prend deux valeurs : 1 si Alice et Bob ont gagné ou 0 sinon. Plus précisément, si Alice et Bob répondent respectivement les bits a et b après avoir reçu respectivement les questions x et y, alors Alice et Bob gagnent le jeu avec la paire de réponses (a,b) étant donnée la paire de questions (x,y), c'est-à dire $R(a,b \mid x,y) = 1$, si $a+b = xy$. Sinon, Alice et Bob perdent le jeu avec la paire de réponses (a,b) étant donnée la paire de questions (x,y), c'est-à dire $R(a,b \mid x,y) = 0$.

Stratégie classique

Alice et Bob peuvent mettre en place deux types de stratégie commune avant d'être questionnés par le maître du jeu. Le premier type de stratégie consiste à répondre complètement au hasard aux questions, quelles qu'elles soient, en espérant que les réponses données conduisent à la victoire. Mais l'on sent bien que cette stratégie est pour le moins... hasardeuse (on pourrait même se demander s'il s'agit véritablement de stratégie, qui est l'art de coordonner ses actions en vue d'atteindre un but). Le second type de stratégie consiste au contraire à donner une réponse obéissant à des règles précises. Par exemple, répondre toujours 1 quelle que soit la question, ou bien donner une réponse *en fonction* de la question posée (comme répondre le même bit que celui envoyé dans la question). Ce second type de stratégie est appelé stratégie classique (ou déterministe). Contrairement au type de « stratégie hasardeuse » précédent, il nécessite l'élaboration d'un algorithme. La question que doivent se poser Alice et Bob est : quel algorithme de réponses à donner maximise les chances de gagner ?

Décrivons une telle stratégie classique de manière plus mathématique. D'une part, le bit-réponse d'Alice sera une fonction de son bit-question $f(x)$. D'autre part, le bit-réponse de Bob sera une fonction de son bit-question $g(y)$. La question est donc : quelles sont les meilleures fonctions pour avoir $f(x) + g(y) = xy$ le plus souvent possible ?

Étant donné que les questions sont des bits, c'est-à-dire $x, y \in \{0,1\}$, il y a plus de possibilités que les questions soient telles que $xy = 0$ qu'elles soient telles que $xy = 1$. En effet, il y a trois combinaisons de zéro et un qui font $xy = 0$ et il y en a une qui fait $xy = 1$. Ensuite, selon la règle d'addition des bits que nous avons rappelée précédemment, la condition $a + b = 0$ est possible uniquement lorsque $a = b$. Par conséquent, conformément à la règle du jeu CHSH, il est plus avantageux qu'Alice et Bob s'accordent pour répondre tous les deux le même bit toujours (soit 0 soit 1) quelle que soit la question qu'ils reçoivent. Par exemple, une stratégie classique où $f(x) = 0$ pour toute question x envoyée à Alice et $g(y) = 0$ pour toute question y envoyée à Bob, définirait un algorithme avec lequel Alice et Bob pourraient gagner le jeu très souvent. De plus, observons que de toutes les configurations possibles pour les questions x, y, la seule combinaison qui fait $xy = 1$ est $x = 1$ et $y = 1$. Donc, avec l'algorithme ci-dessus Alice et Bob perdraient le jeu uniquement lorsque l'arbitre envoie la question $x = 1$ à Alice et la question $y = 1$ à Bob. Ceci veut dire qu'Alice et Bob perdraient le jeu uniquement 1 fois sur 4 ! Autrement dit, Alice et Bob gagneraient le jeu CHSH dans 75% des fois en utilisant cette stratégie.

Pour ce jeu, nous pouvons écrire explicitement toutes les fonctions possibles, c'est-à-dire tous les algorithmes possibles. En effet, il y a 16 configurations différentes qu'Alice et Bob peuvent adopter envers leur stratégie conjointe. Il est possible également de calculer les probabilités de réussite de chacune de ces stratégies. Ces calculs montrent que, effectivement, la stratégie que nous avons décrite ci-dessus est la meilleure qu'Alice et Bob puissent adopter. En conclusion, Alice et Bob peuvent gagner le jeu CHSH avec une probabilité de 75% en utilisant une stratégie classique déterministe :

$$P(\text{gagner CHSH, classique}) = \frac{3}{4}$$

Les 16 stratégies classiques pour CHSH

Fin provisoire de l'article

Pour des raisons techniques, la version complète de cet article est disponible seulement au format paginé à retrouver sur la page 10.60868/y8by-1816.

Références

[1] S. De Bièvre. « À la découverte de la cryptographie quantique ». *Images des mathématiques* (7 juill. 2021). URL : https://images.math.cnrs.fr/a-la-decouverte-de-la-cryptographie-quantique/.

[2] S. De Bièvre. « Subtile mécanique quantique ». *Images des mathématiques* (10 avr. 2021). URL : https://images.math.cnrs.fr/subtile-mecanique-quantique/.

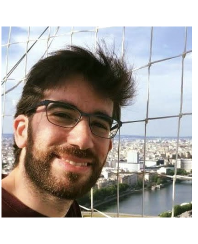
[3] S. De Bièvre. « Surprenant hasard quantique ». *Images des mathématiques* (5 mars 2021). URL : https://images.math.cnrs.fr/surprenant-hasard-quantique/.

Remerciements

J'ai commencé la rédaction de cet article pendant ma période post-doctorale à l'Université de Copenhague financée par une Marie Skłodowska-Curie Individual Fellowship. Les groupes de travail animés par Laura Mančinska et David E. Roberson sont à l'origine de ma motivation et de mon intérêt vers la théorie quantique de l'information et ses rapports avec les algèbres d'opérateurs.

J'aimerais remercier Pooneh Afsharijoo pour le dessin sympathique d'Alice et Bob qui présente cet article. J'aimerais remercier Stéphane Sirejacob pour sa relecture attentive, ses commentaires et ses suggestions qui ont, sans doute, amélioré qualitativement la rédaction de l'article. J'aimerais remercier les éditeurs Aurélien Alvarez et Jérôme Buzzi pour leur intérêt sur le sujet et, surtout, par leurs successives remarques, propositions et relectures qui ont profilé le texte progressivement. Enfin, j'aimerais remercier les relecteurs Clément Caubel, Aziz El Kacimi, Shalom Eliahou, Pierre-Antoine Guihéneuf, Sébastien Kernivinen, pour leur intérêt et leurs commentaires.

Article édité par Jérôme Buzzi.



Rubén Martos
Post-doctorant – Université de Lille
https://sites.google.com/view/ruben-martos/home

Compléments

Les 16 stratégies classiques pour CHSH

Les 16 configurations différentes qu'Alice et Bob peuvent adopter envers leur stratégie classique conjointe pour le jeu CHSH sont définies par les fonctions suivantes :

$$\begin{array}{rccl} f_1,f_2,f_3,f_4 : & I_A & \longrightarrow & O_A \\ & x & \overset{f_1}{\longmapsto} & f_1(x) := x \\ & x & \overset{f_2}{\longmapsto} & f_2(x) := x+1 \\ & x & \overset{f_3}{\longmapsto} & f_3(x) := 0 \\ & x & \overset{f_4}{\longmapsto} & f_4(x) := 1 \end{array}$$

$$\begin{array}{rccl} g_1,g_2,g_3,g_4 : & I_B & \longrightarrow & O_B \\ & y & \overset{g_1}{\longmapsto} & g_1(y) := y \\ & y & \overset{g_2}{\longmapsto} & g_2(y) := y+1 \\ & y & \overset{g_3}{\longmapsto} & g_3(y) := 0 \\ & y & \overset{g_4}{\longmapsto} & g_4(y) := 1 \end{array}$$

Conformément à la règle du jeu, les configurations (f_3, g_3) et (f_4, g_4) s'avèrent être les bons candidats pour fournir une stratégie optimale comme on a expliqué précédemment. Nous pouvons calculer les probabilités gagnantes de chacune des configurations et garder celle qui donne la probabilité la plus haute. En guise d'exemple, calculons la probabilité gagnante de la stratégie (f_1, g_1) et de la stratégie (f_3, g_3).

Stratégie (f_1, g_1)

Étant donnés $x, y \in \{0,1\}$, voyons quand l'équation $a + b = xy$ est satisfaite lorsque Alice choisit sa réponse a en utilisant la fonction f_1 et Bob choisit sa réponse b en utilisant la fonction g_1.

— Si $(x,y) = (0,0)$, alors $a = f_1(x) = 0$ et $b = g_1(y) = 0$. On a $0 + 0 = 0 \cdot 0$
— Si $(x,y) = (0,1)$, alors $a = f_1(x) = 0$ et $b = g_1(y) = 1$. On a $0 + 1 \neq 0 \cdot 1$
— Si $(x,y) = (1,0)$, alors $a = f_1(x) = 1$ et $b = g_1(y) = 0$. On a $1 + 0 \neq 1 \cdot 0$
— Si $(x,y) = (1,1)$, alors $a = f_1(x) = 1$ et $b = g_1(y) = 1$. On a $1 + 1 \neq 1 \cdot 1$

Avec cette stratégie, Alice et Bob gagneraient le jeu seulement 1 fois sur 4 :

$$P(\text{gagner CHSH}), (f_1, g_1)) = \frac{1}{4} R(0,0 \mid 0,0) = \frac{1}{4}$$

Stratégie (f_3, g_3)

Étant donnés $x, y \in \{0,1\}$, voyons quand l'équation $a + b = xy$ est satisfaite lorsque Alice choisit sa réponse a en utilisant la fonction f_3 et Bob choisit sa réponse b en utilisant la fonction g_3.

— Si $(x,y) = (0,0)$, alors $a = f_3(x) = 0$ et $b = g_3(y) = 0$. On a $0 + 0 = 0 \cdot 0$
— Si $(x,y) = (0,1)$, alors $a = f_3(x) = 0$ et $b = g_3(y) = 0$. On a $0 + 0 = 0 \cdot 1$
— Si $(x,y) = (1,0)$, alors $a = f_3(x) = 0$ et $b = g_3(y) = 0$. On a $0 + 0 = 1 \cdot 0$
— Si $(x,y) = (1,1)$, alors $a = f_3(x) = 0$ et $b = g_3(y) = 0$. On a $0 + 0 \neq 1 \cdot 1$

Avec cette stratégie, Alice et Bob gagneraient le jeu 3 fois sur 4. Nous pouvons montrer, avec des calculs similaires, que la stratégie (f_4, g_4) donne la même probabilité gagnante que (f_3, g_3) et que le reste des stratégies donnent toujours une probabilité inférieure.

$$P(\text{gagner CHSH, classique}) = P(\text{gagner CHSH}, (f_3, g$$

$$= \frac{1}{4}(R(0,0 \mid 0,0) + R(0,0 \mid 0,1) + R(0,0 \mid 1,0)) = \frac{3}{4}$$