COL·LECCIÓ JOVES INVESTIGADORS

Non-localité quantique et intrication

ou Pourquoi Dieu jue-t-il aux dés

Pablo Cerrato Serrano

19
PREMI DE RECERCA
MIQUEL SEGURA

PREMI DE RECERCA
MIQUEL SEGURA
19

Non-localité quantique et intrication

ou Pourquoi Dieu jue-t-il aux dés

Pablo Cerrato Serrano

Ajuntament de Rubí

RUBÍ educació

Autor:
Pablo Cerrato Serrano

Edita:
Ajuntament de Rubí

Correcció del francès:
Annick Delplace

Disseny i maquetació:
Masdisseny

Edició digital:
juny 2019

SOMMAIRE

És un honor, com a alcaldessa de Rubí, poder presentar-vos el treball de recerca guanyador del Premi Miquel Segura. Estem davant de la 19a edició d'aquest premi, que l'Ajuntament de Rubí atorga a les millors investigacions realitzades pels alumnes de batxillerat de la nostra ciutat.

És un reconeixement que constitueix un referent per al jovent dels centres educatius de Rubí, i suposa un incentiu a l'hora de desenvolupar les seves recerques. Aquests alumnes ens demostren, amb els nombrosos treballs presentats, la diversitat de temàtiques escollides i la qualitat del contingut.

Exemple d'aquesta qualitat és el treball que llegireu a continuació, que correspon al guanyador d'aquesta edició. La temàtica del treball és física quàntica i està fet en francès per l'alumne Pablo Cerrato Serrano. Amb una breu introducció al món quàntic, que inclou la no localització quàntica i l'entrellaçament, acaba amb el desenvolupament d'un sistema d'encriptació, que a priori sembla que no es pot desxifrar.

En nom de la ciutat que represento, vull felicitar l'autor pel seu afany i perseverança, així com també la resta de joves que van participar en aquest premi, que fan que l'aposta de la ciutat per l'educació combini coneixement, treball pràctic i ànim de crítica. A més, i com no pot ser d'una altra manera, vull expressar el meu agraïment als tutors que dia a dia treballen per guiar l'alumnat en la seva formació acadèmica i personal.

Us animo a endinsar-vos en la lectura d'aquest llibre.

Ana María Martínez
Alcaldessa de Rubí

PRÒLEG

El treball que teniu a les mans és el resultat de l'esforç i la perseverança de Pablo Cerrato, un alumne brillant que es va entusiasmar per la física quàntica el dia que va assistir a una conferència sobre el tema en el marc del programa "Bojos per la física" de la Fundació Catalunya-La Pedrera. Aquell dia, en Pablo va esdevenir un "boig per la física quàntica": de manera gairebé autodidacta, va començar a fer recerca sobre el tema i es va proposar demostrar-ne alguns dels principis. El seu gran interès per la física quàntica va fer que aconseguís implicar tot el seu entorn, família, amics i companys d'institut, que van fer el test de Bell tantes vegades com ell els ho va demanar.

Aquest treball té la gran virtut de fer atractiu i entenedor un tema que d'entrada pot semblar avorrit i difícil: l'entrellaçament quàntic. L'autor fa una introducció a la física quàntica molt didàctica on utilitza un llenguatge planer i posa exemples quotidians que acosten aquest àmbit al lector. Així mateix, els dos experiments que va fer permeten entendre molt bé què està entrellaçat i què no ho està.

Espero que gaudiu de la lectura.

Montserrat Mas LLorens
Professora de Física i Química
Tutora del Treball de Recerca

REMERCIEMENTS

Je voudrais remercier toutes les personnes qui ont rendu ce travail possible et qui m'ont soutenu et aidé tout au long du travail. Je commencerai par mes tutrices. Merci à Montse Mas pour avoir accepté de superviser mon travail, car sans elle il n'aurait pas été possible de le faire, et merci pour sa patience à mon égard, car je n'ai pas parlé autant que je ne l'aurais souhaité. Merci à Anne Forêt, qui devra lire tout le travail sur la physique quantique, malgré la complexité du sujet. J'espère que ça se passera bien ou tout du moins qu'il s'agira d'une expérience intéressante. Et merci à Magali Chane, pour son engagement et ses efforts pour comprendre toutes les théories quantiques, malgré leur complexité.

Je tenais également à remercier les chercheurs du *Grup d'informació quàntica (GIQ)* de l'UAB pour la séance Del BIT al QUBIT : *Criptografia quàntica i el test de Bell*, dédiée à la cryptographie, aux lois quantiques et au test de Bell. Sans eux, je n'aurais surement pas pu commencer le travail. Ils m'ont donné l'information dont j'avais besoin d'une manière simple et compréhensible. De plus, ils m'ont aidé à faire l'expérience sur l'ordinateur quantique d'IBM.

Je remercie ma famille pour toutes les heures où j'ai dû m'enfermer dans ma chambre pour faire le travail au lieu d'être en leur compagnie. Pour tout le soutien qu'ils m'ont apporté tout au long du travail de recherche. Pour les bêtises quantiques que je leur ai expliquées et qu'ils ont dû supporter. Pour tous les gouters qu'ils m'ont préparés et apportés. Et pour toutes les heures où je n'ai pas pu jouer avec mon frère.

Enfin, je souhaite remercier mes amis. Pour toutes les fois où je leur ai dit de faire le test de Bell. Merci à eux pour m'avoir apporté tous ces moments heureux lorsque j'avais besoin de déconnecter. Merci pour avoir fait l'effort de comprendre la physique quantique lorsque je la leur expliquais.

Merci à toutes et à tous de votre intérêt pour ce travail de recherche.

1 INTRODUCTION

1.1 Justification du choix

J'ai choisi ce travail de recherche pour plusieurs raisons, et notamment pour la passion que j'éprouve à l'égard de la physique. Sans passion ni curiosité, aucun travail de ce genre ne serait facile à faire. De plus, j'ai très envie de continuer à apprendre de nouvelles choses et de comprendre le monde qui nous entoure.

Pour moi, la physique est un outil très intéressant dont on se sert pour mieux comprendre le monde et l'Univers. Les formules et les théories sont toutes d'une grande utilité. Néanmoins, ma fascination pour la physique vient de personnes qui sont en amont, de toutes les heures passées à développer des théories fantaisistes. Lorsque j'apprends une nouvelle théorie ou une formule, je pense à ceux qui se sont demandés le pourquoi ou le comment des choses. Je m'étonne toujours du pouvoir de la pensée humaine. Celle qui recherche les mécanismes et les manières de faire les choses facilement et celle qui a réussi à trouver des liens entre les éléments les moins attendus.

Le domaine quantique, c'est ce que j'aime le plus. La physique quantique m'étonne parce que l'on ne peut pas toujours voir ce que l'on théorise. Accéder à un niveau si haut d'abstraction, je pense, est une réussite admirable.

J'ai choisi ce thème parce qu'il y a quelque temps, j'ai lu un article qui parlait de photons qui communiquaient à une vitesse plus élevée que celle de la lumière (Or, selon Einstein, rien ne peut dépasser la vitesse de la lumière). Ce thème m'a interpelé et beaucoup intéressé.

Ce travail de recherche me donnait l'opportunité d'en savoir plus sur ce sujet et de commencer à me poser les questions qui constitueraient le fil conducteur de mes recherches.

1.2 Objectifs

Mon objectif est d'apprendre et de continuer à m'intéresser au monde de la physique. J'aimerais être capable d'expliquer ces connaissances de façon simple et intelligible à des néophytes.

Toujours dans la limite d'un bachelier, je voudrais tester toutes les théories, les phénomènes et les expériences ayant trait au thème de mon travail. Je pourrai ainsi mettre en pratique l'objet de mes études. Concrètement, j'ai l'intention de tester les théories suivantes :

• L'inégalité de Bell. D'un côté, je testerai les cas où elle s'accomplit, de l'autre, j'utiliserai un ordinateur quantique pour tester la violation de cette inégalité.

• Le fonctionnement des filtres polarisateurs. J'essaierai de vérifier les théories concernant la probabilité et les filtres polarisateurs.

• Le masque jetable. Je ferai une expérience réelle de la méthode de chiffrement par *masque jetable*, d'abord sans *espion* et puis avec une *espionne*.

1.3 Méthodologie

En ce qui concerne la méthodologie, j'ai l'intention de demander des informations sur l'expérience *Big Bell Test* menée le 30 novembre 2016 par les scientifiques de l'ICFO (Institut des sciences photoniques). D'autre part, j'utiliserai l'ordinateur quantique d'IBM mis à la disposition du public afin de vérifier certaines théories quantiques dont il sera question dans ce travail. Enfin, j'ai prévu de mener une petite étude quantique, et plus exactement de faire un test de Bell, en vue de confirmer un théorème quantique.

La plupart des informations dont je dispose provient des conférences données par les scientifiques engagés dans le programme *Bojos per la física* (dingues pour la physique), auquel j'ai la chance d'appartenir. J'ai aussi consulté la thèse doctorale de Félix Bussières[1], ainsi que des vidéos et des informations sur Internet.

[1] BUSSIÈRES, Félix, Intrication temporelle et communication quantique, École polytechnique de Montréal, octobre 2009.

2 INTRODUCTION AU MONDE QUANTIQUE

Souvent le mot *physique* nous rebute, sans doute pour la complexité des formules, les lettres bizarres qui ne nous inspirent rien du tout… Si on posait la question « Pouvez-vous me nommer un physicien célèbre ? », en général, on obtiendrait presque toujours les mêmes réponses, à savoir Einstein, Stephen Hawking, Newton, Tesla peut-être… On craint la physique.

Mais heureusement, la physique est bien plus que toutes ces formules. La physique est une manière de comprendre le monde qui nous entoure. Aussi, au cours de ce travail, nous examinerons les phénomènes du monde d'un point de vue quantique.

2.1. Physique quantique

« Si vous croyez comprendre la mécanique quantique,
c'est que vous ne la comprenez pas. »
Richard Feynman

Je suis sûr qu'au moins un fois dans votre vie, même involontairement, vous avez entendu le mot *physique*. Peut-être suivi de *quantique*. Si tel est votre cas, alors, c'est parfait. Sinon, il y a quelques notions que vous devez connaitre avant de commencer à lire ce travail.

La physique est l'étude de tout ce qui passe dans l'univers, absolument tout : depuis les choses les plus grandes, comme les planètes ou les galaxies, jusqu'aux choses les plus petites, comme les atomes, les électrons ou les quarks[2].

Le mot *quantique* se réfère à la taille des objets que l'on étudie. Les phénomènes quantiques se manifestent à partir de l'échelle *nanométrique* (10^{-9}), celle des atomes.

Quand on parle de la *physique quantique*, on se réfère à ce qui se déroule à l'échelle des atomes.

Ce travail traite tout particulièrement d'une particule : le *photon* (γ). Il s'agit de la particule qui conduit la lumière (entre autres) et d'une particule élémentaire, c'est-à-dire d'une unité élémentaire, le photon n'est pas composé d'éléments plus petits. Sa charge n'est ni positive ni négative, le photon est neutre. Et le plus surprenant, c'est que le photon n'a pas de masse et peut se comporter comme une particule ou comme une onde[3]. Toutes ces caractéristiques sont très importantes. Nous les examinerons plus loin.

2.2. État quantique

Pour comprendre le sujet principal du travail, soit la non-localité et l'intrication, il faut connaitre au préalable quelques concepts *élémentaires*, qui seront expliqués dans le cadre de ce chapitre. Cela est

[2] Un quark est une particule élémentaire ou fondamentale, tous les protons et neutrons sont composés de quarks.
[3] Dualité onde-particule. Phénomène quantique selon lequel les particules se comportent comme si elles étaient des ondes. Cela nous permet d'utiliser les formules d'onde pour décrire le comportement de ces particules.

essentiel pour comprendre ce qui va suivre. À présent, partons à la découverte du monde fascinant de la physique et abordons quelques détails plus techniques.

Si je vous disais le mot *état*, à quoi penseriez-vous ? Peut-être à un pays, l'État français, l'État espagnol, les États-Unis… ou à l'état de *WhatsApp*. Ou peut-être à un aliment en mauvais état ou à une personne en état d'ivresse. Si vous penchez plutôt pour ce dernier cas, vous êtes dans le bon !

Un état correspond à la situation ou aux valeurs des variables qui peuvent définir un système. Par exemple, comme nous le disions précédemment, un aliment en mauvais état n'est pas frais, ce qui signifie qu'il a une *valeur de fraicheur* très basse. Ou encore, une personne qui court se trouve dans un *état de mouvement*, tandis qu'une personne qui est assise se trouve dans un *état de repos*.

Ces exemples correspondent à des états physiques. Mais les états que nous allons utiliser sont quantiques. Les états quantiques sont représentés d'une manière spéciale. Par exemple, si l'on veut écrire l'état *assis*, on écrit |*assis*⟩, si l'on veut écrire l'état courant, on écrit |*courant*⟩. En général, on écrit les états |A⟩ et |B⟩ pour faire référence à deux cas ou états possibles. Au fil de ce travail, nous allons surtout utiliser ces quatre états : $|0\rangle$ et $|1\rangle$ pour les *qubits* et $|\leftrightarrow\rangle$ et $|\updownarrow\rangle$ (avec leurs variantes) pour parler de la direction d'oscillation.

Souvent les états n'apparaissent pas seuls et nous allons travailler avec des particules qui peuvent se trouver dans 2 états. La particule aura une certaine probabilité d'être dans un état donné et une autre probabilité d'être dans l'autre état. On peut représenter ces deux états et les probabilités correspondantes par le biais de la *fonction d'onde* :

$$|\psi\rangle=\alpha|A\rangle+\beta|B\rangle$$

On peut observer qu'il ne s'agit pas d'une fonction *normale*. Elle est composée de plusieurs parties. Voici les différentes parties et leur signification :

$|\psi\rangle$ Psi : cela signifie simplement qu'il s'agit d'une fonction d'onde
α Alpha : la probabilité d'être dans l'état A
β Bêta : la probabilité d'être dans l'état B
$|A\rangle$ A : l'état A
$|B\rangle$ B : l'état B
$|\ \rangle$ Kets : la manière employée pour symboliser un état (notation de Dirac)

À présent, je vais vous présenter quelques exemples pour vous aider à mieux comprendre.
Voici la fonction d'onde d'une personne sportive :

$$|p.sportive\rangle = 75\ \%|courant\rangle + 25\ \%|assise\rangle$$

Selon la fonction d'onde, une personne sportive court 75 % du temps et est assise 25 % du temps. Ici, on observe l'une des caractéristiques de la fonction : l'addition des probabilités doit donner 100 %. C'est logique, car si l'addition donnait 95 %, cela signifierait que pendant 5 % du temps, on ne saurait pas ce que la personne fait.

Les pourcentages sont corrects, mais il y a une façon mathématique de les représenter sans utiliser le symbole % : il suffit d'écrire un zéro, une virgule et après le nombre (ou la fraction correspondante) ou il suffit tout simplement de diviser par 100. Voici un exemple d'une personne fainéante :

$$|p.fainéante\rangle = 0{,}75\ |assise\rangle + \frac{1}{4}|courant\rangle$$

Ici, on peut observer qu'une personne fainéante est assise 75 % du temps (0,75) et *court* le reste du temps, soit 25 % du temps ($\frac{1}{4} = 0{,}25$).. Si on fait l'addition des probabilités, nous obtenons 1. Si on dit qu'on a une probabilité égale à 1, c'est comme si on disait 100 %.

En réalité, le nombre que l'on veut n'est pas la probabilité (chiffre décimal), mais la racine carrée de cette probabilité. Voici l'exemple d'une pièce de monnaie :

$$|pièce\rangle = \frac{1}{\sqrt{2}}|pile\rangle + \frac{1}{\sqrt{2}}\,|face\rangle$$

Pour découvrir la probabilité de se trouver dans l'état pile, nous devons prendre le nombre $\frac{1}{\sqrt{2}}$, l'élever au carré $(\frac{1}{2})$ et multiplier par 100 (50). La probabilité d'obtenir pile est de 50 % et celle d'obtenir face est de 50 %.

Pour faire l'opération inverse, c'est très facile. D'abord, on doit prendre la probabilité, par exemple 10 %. Ensuite, on la divise par 100 $(\frac{10}{100} = \frac{1}{10})$ et on la laisse sous forme de fraction. Finalement, on prend la racine carrée de la fraction $(\sqrt{\frac{1}{10}} = \frac{1}{\sqrt{10}})$. Et voilà, la probabilité est prête à être utilisée dans notre fonction !

2.3 Les particules de la lumière

Après cette petite introduction consacrée au photon et à la représentation des états en physique quantique, nous allons examiner plus en détails le comportement du protagoniste de ce travail, le photon, mais aussi découvrir quelques caractéristiques des particules quantiques.

Commençons par le photon. Il s'agit d'une particule qui n'a ni poids ni volume, cela signifie que l'on ne peut pas *voir* un photon car il n'a pas de dimension. Néanmoins, on peut mesurer les interactions entre particules provoquées par le photon et ainsi savoir ce qu'il fait. Pendant ces interactions, le photon se comporte comme une onde (dualité onde-particule).

Le photon est représenté par la lettre gamma (γ). C'est lui qui conduit le rayonnement électromagnétique. Mais ne vous inquiétez pas, les rayonnements ne sont pas toujours *mauvais*. L'un des types de rayonnements qu'il conduit est la lumière. Oui, on peut voir grâce au photon, remerciez-le.

Comme nous le disions, le photon est une particule élémentaire, il n'est pas composé d'autres choses plus petites, il n'a pas non plus de structure interne.

Toutes les ondes ont une direction de propagation, un sens de propagation et une direction d'oscillation. Voici une onde isolée (Fig. 1).

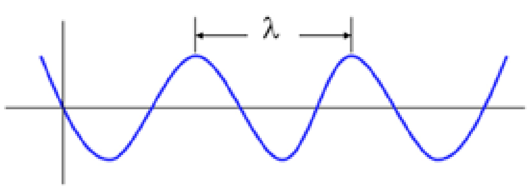


Fig. 1 : Onde isolée

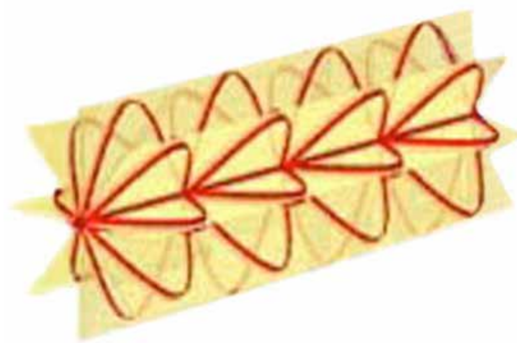


Fig. 2 : Ondes non-polarisées

Les ondes associées aux photons ne sont pas toujours isolées. Souvent, elles proviennent d'une source de photons comme le soleil, où les ondes sortent dans toutes les directions, tous les sens et toutes les orientations possibles (Fig. 2).

Toutes les particules élémentaires se caractérisent par une rotation sur un axe qui coupe la particule en deux moitiés. Il s'agit du *spin* (Fig. 3). Cette rotation est équivalente à celle d'une toupie (Fig. 4) ou à celle d'un *spinner* (Fig. 5).

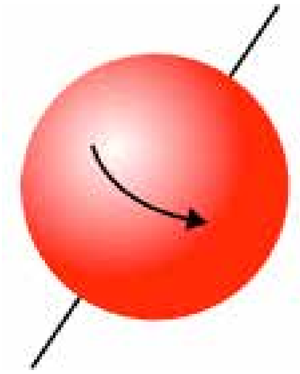


Fig. 3 : Spin

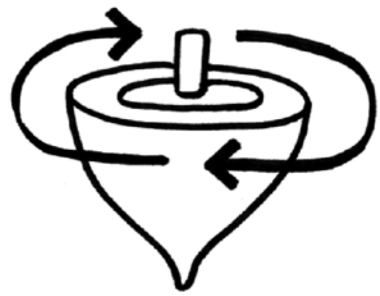


Fig. 4 : Toupie

Fig. 5 : Spinner

2.4 Mesure quantique

Tout ce que nous avons vu jusqu'ici correspond à la partie théorique, maintenant, nous allons aborder la partie expérimentale.

Vous vous rappelez de l'état et de la fonction d'état ? Très bien, nous pouvons utiliser ces notions dans le cas des photons et de leurs caractéristiques.

Comme nous le disions, les photons sont des ondes caractérisées par une direction de propagation, un sens de propagation et une direction d'oscillation. Laissons de côté la direction et le sens de propagation pour l'instant et concentrons-nous sur la direction d'oscillation.

Si nous coupons ce dessin d'ondes (Fig. 6) de manière perpendiculaire à leur direction de propagation, nous obtiendrons un autre dessin comme celui de la Fig. 7 :

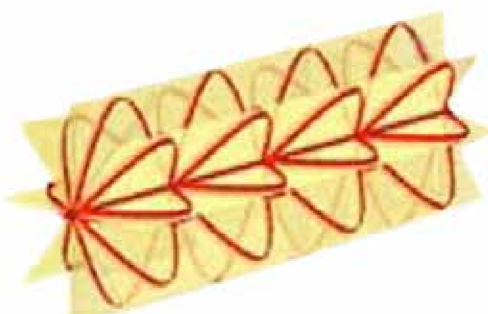


Fig. 6 : Ondes non-polarisées

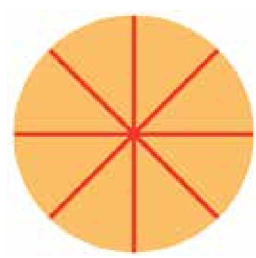


Fig. 7 : Directions d'oscillation des ondes

Nous travaillerons désormais sur ce type de dessins et toutes les transformations concerneront la direction d'oscillation des ondes.

Pour employer les fonctions d'onde, il faut avoir 2 états bien différenciés, ces deux états vont former une *base*. Par exemple, parmi les états les plus communs, on peut mentionner |↔⟩ et |↕⟩. Ceux deux états forment la *base* +. Pourquoi la base + et non pas une autre ? Tout simplement en raison de la direction d'oscillation des photons (horizontale et verticale). Nous allons aussi utiliser la *base X*. Cette base correspond aux états |⤡⟩ et |⤢⟩.

Par ailleurs, nous allons employer le *polarisateur*. Il s'agit tout simplement d'un verre qui ne laisse passer la lumière que dans une seule direction d'oscillation ou polarisation. Ci-après, on peut observer deux polarisateurs. Le premier polarisateur a une polarisation verticale, cela veut dire qu'il ne laisse passer que la lumière avec une polarisation de 90° (Fig. 8). Ensuite, il y a un autre polarisateur qui ne va laisser passer que la lumière avec une polarisation de 0°.

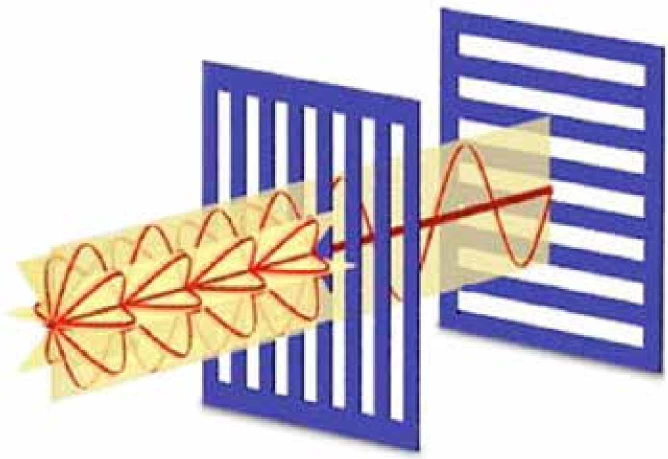


Fig. 8 : Filtre polarisateur

Ainsi, nous pouvons déduire que l'une des deux caractéristiques de la mesure quantique est son caractère *invasif*. En d'autres termes, quand nous prenons une mesure avec le polarisateur, quelques ondes sont détruites et ne peuvent pas être récupérées, donc l'état a changé indéfiniment. L'autre caractéristique est l'inexactitude des résultats, c'est-à-dire que l'onde a une probabilité de se trouver dans un état ou dans l'autre, mais on ne connait pas le résultat. Approfondissons à présent cette deuxième caractéristique et voyons comment cela influence les résultats.

Nous pouvons jouer avec le polarisateur et représenter d'une manière physique les états quantiques et les fonctions d'onde. Essayons de nous rappeler. Une fonction d'onde a des états et des probabilités. L'addition des probabilités au carré devait être égale à 1. En plus, nous pouvons seulement changer l'angle de polarisation de l'onde. À partir de ces données et d'un peu de trigonométrie, on peut conclure que :

$$\sin^2\theta+\cos^2\theta=1$$

Cette lettre *θ (theta)* a la valeur de l'angle de polarisation de l'onde associée au photon. Si nous substituons cette équation dans la formule de la fonction d'onde, nous obtiendrons une équation comme celle-ci :

$$|\psi\rangle=\sin\theta\ |A\rangle+\cos\theta\ |B\rangle$$

C'est ainsi que nous pouvons déterminer la probabilité des états pour toutes les ondes possibles. Par exemple, si nous avons un état en base X, où θ=45°, la fonction d'onde serait la suivante :

$$|\psi\rangle=\sin 45°\ |A\rangle+\cos 45°\ |B\rangle$$

Nous savons que sin 45°= $\frac{1}{\sqrt{2}}$, alors nous pouvons écrire la fonction comme ci-dessous :

$$|\psi\rangle=\frac{1}{\sqrt{2}}|A\rangle\ +\frac{1}{\sqrt{2}}\ |B\rangle$$

Supposons que deux individus échangent des photons. Nous les appelons *Alice* et *Bob*. Ces noms deviennent les lettres A et B pour faire référence à chacune des personnes ou lieux.

Imaginons qu'Alice veut envoyer un photon à Bob dans la base + et veut que ce photon soit dans l'état |↕⟩. Pour ce faire, elle va prendre un filtre polarisateur et va le placer de telle manière que la polarisation soit verticale, puis elle va mettre une source de photons derrière le filtre. De cette façon, elle va envoyer des photons dans l'état |↕⟩ à Bob.

Bob, par contre, devra *lire* ou mesurer ces photons reçus pour savoir ce qu'Alice a envoyé. Pour lire les photons, Bob prendra aussi un filtre polarisateur et une base aléatoire, par exemple la base X. Bob va prendre des mesures dans les deux états possibles. Il ne verra aucune différence entre les deux états, dans les deux cas il verra un peu de lumière passer à travers le filtre. Cela signifie qu'il a choisi la mauvaise base. Ensuite, il va essayer avec la base +. Il remarque une différence entre les 0° et les 90°: horizontalement, la lumière ne passe pas à travers le filtre, tandis que verticalement, toute la lumière passe. Il peut alors être sûr qu'Alice a envoyé un photon dans l'état |↕⟩.

C'est ainsi que l'on mesure l'état d'un ou de plusieurs photons.

2.5 Principe de superposition

Peut-être avez-vous entendu parler du *chat de Schrödinger*, le pauvre chat qui est à la fois vivant et mort. Oui, cela parait un peu bizarre, mais c'est de la physique quantique. Ce chat en particulier explique très bien ce qu'est le principe de superposition.

L'histoire du célèbre chat de Schrödinger est très simple. Schrödinger, un physicien autrichien, décide d'enfermer son chat avec un flacon rempli de venin et un marteau dans une boite bien fermée et insonorisée, afin qu'il ne puisse rien écouter de ce qui se passe dans la boite. Le marteau ne peut casser le flacon, qui renversera le venin qui tuera le chat qu'avec une probabilité de 50 %. Imaginons qu'un ami joue à pile ou face. Si la monnaie tombe sur le côté pile, le chat survit. En revanche, s'il obtient face, le chat meurt. Schrödinger ne connait pas le résultat du jeu, de sorte qu'il ne sait pas si le chat est vivant ou mort. Ensuite, il fait la réflexion suivante : « Je ne sais pas si mon chat est vivant ou mort, par conséquent, il *est à la fois vivant et mort* ».

En somme, ce que cette histoire démontre, en termes généraux, c'est qu'un système (le chat) peut se trouver à la fois dans les deux états (vivant ou mort), tant qu'on ne mesure pas l'état dans lequel il se trouve (ouvrir la boite). Il s'agit du *principe de superposition* (superposition des états vivant et mort).

Prenons un exemple du principe de superposition dans le cas d'un photon. Si nous avons un photon en base X et que nous voulons le mesurer en base +, il y a une superposition des états |↔ et |↕, car la probabilité d'avoir ces deux états est de 50 % pour chacun d'eux. Ce photon avec la superposition d'états s'appelle *qubit* et se trouve à la base de l'informatique quantique. Ce n'est que lorsque l'on mesure ce qubit que l'on pourra déterminer l'état dans lequel il se trouve.

3 PARADOXE EPR ET TEST DE BELL

Sans aucun doute, on peut considérer Einstein comme l'un des physiciens les plus importants et célèbres. Grâce à lui, la physique a beaucoup avancé au début du XX[e] siècle. Il a créé la théorie de la relativité, laquelle nous permet de déterminer, par exemple, les mouvements des planètes, ou de comprendre le comportement des objets qui vont très vite.

Incontestablement, il a fait une contribution essentielle à la physique classique, qui se consacre à l'étude des objets plus grands que les atomes. Dans cette longue section consacrée au paradoxe EPR et au test de Bell, nous allons découvrir comment Einstein a réagi face à la mécanique quantique, une théorie complètement différente de la physique classique.

3.1 Le principe d'incertitude

« Quel est le son d'une seule main qui applaudit ? »
Kōan du XVIIe siècle

Werner Heisenberg, un physicien allemand né en 1901, énonça le *principe d'incertitude* en 1927. Il s'agit de l'une des règles primordiales en physique quantique. D'ailleurs, la théorie quantique est entièrement construite à partir de ce principe.

Le principe d'incertitude établit qu'il n'est pas possible de déterminer avec certitude deux variables complémentaires[4]. En d'autres termes, il n'est pas possible de connaitre en même temps à 100 % la vitesse d'un objet et sa position. Plus on connait sa vitesse, moins on connait sa position. L'incertitude d'une mesure n'est pas aléatoire. De fait, il y a une formule pour déterminer jusqu'à quel point il est possible de mesurer avec précision une grandeur physique.

Cette formule, proposée par Heisenberg en 1927, établit une limite à l'incertitude d'une variable donnée :

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}$$

Où $\Delta \mathrm{x}$ est l'incertitude sur la position, $\Delta \mathrm{p}$ l'incertitude sur la quantité de mouvement ($\mathrm{m} \cdot \Delta \mathrm{v}$, produit de la masse par vitesse) et $\hbar$ la constante de Planck réduite ($\mathrm{h}/2\pi \approx 1{,}0546 \cdot 10^{(-34)}\ \mathrm{J} \cdot \mathrm{s}$).

Cette formule peut être utilisée avec des objets et situations communes, mais elle n'a pas autant d'effet que si nous l'appliquons au monde quantique. Voilà quelques exemples d'application qui permettent de mieux comprendre l'importance et la différence entre le monde quantique et celui qui nous est plus familier.

Imaginons un match de baseball. Le lanceur lance la balle (150 g = 0,15 kg) et nous mesurons une vitesse de 100 km/h ($\approx 27{,}77\ \mathrm{m/s}$) avec une erreur de 0,5 km/h ($\approx 0{,}14\ \mathrm{m/s}$). Si nous voulons savoir où se trouve la balle au même moment, cela est possible avec l'erreur suivante :

[4] Deux variables complémentaires sont celles qui ne peuvent pas être mesurées simultanément comme la quantité de mouvement (produit de la masse par la vitesse) et la position.

$$\Delta x \cdot m \cdot \Delta v \geq \frac{\hbar}{2}$$
$$\Delta x \cdot 0{,}15 \text{ kg} \cdot 0{,}14 \text{ m/s} \geq \frac{1{,}0546 \cdot 10^{-34} \text{ J} \cdot \text{s}}{2}$$
$$\Delta x \geq \frac{1{,}0546 \cdot 10^{-34} \text{ J} \cdot \text{s}}{2 \cdot 0{,}14 \text{ m/s} \cdot 0{,}15 \text{ kg}}$$
$$\Delta x \geq 2{,}53104 \cdot 10^{-33} \text{ m}$$

Nous pourrons déterminer la position de la balle avec une erreur minimale de $2{,}53 \cdot 10^{(-33)}$, soit cent billions de fois plus petite qu'un proton (un 1 et 23 zéros plus petit qu'un atome), soit pratiquement 0. Voyons à présent ce qui se passe avec un proton de masse $1{,}67 \cdot 10^{-27}$ kg et une incertitude sur la vitesse de 0,5 km/h (≈ 0,14 m/s) :

$$\Delta x \cdot m \cdot \Delta v \geq \frac{\hbar}{2}$$
$$\Delta x \cdot 1{,}67 \cdot 10^{-27} \text{ kg} \cdot 0{,}14 \text{ m/s} \geq \frac{1{,}0546 \cdot 10^{-34} \text{ J} \cdot \text{s}}{2}$$
$$\Delta x \geq \frac{1{,}0546 \cdot 10^{-34} \text{ J} \cdot \text{s}}{2 \cdot 0{,}14 \text{ m/s} \cdot 1{,}67 \cdot 10^{-27} \text{ kg}}$$
$$\Delta x \geq 227 \cdot 10^{-9} \text{ m}$$

Pour le proton, nous avons trouvé une incertitude de 227 nm. À l'échelle humaine, il s'agit d'une valeur négligeable, mais pour un proton, il s'agit d'une distance considérablement grande (une différence d'au moins la distance de 2 000 atomes).

Ces deux exemples nous permettent, une fois de plus, d'observer qu'il y a une énorme différence entre l'échelle quantique et l'échelle humaine. De sorte que l'erreur sur la balle est négligeable, tandis que l'erreur sur le proton représente une différence de 2 000 atomes, avec dans les deux cas une même incertitude sur la vitesse (0,5 km/h).

En somme, le principe d'incertitude a apporté à la physique quantique l'une de ses caractéristiques élémentaires : la probabilité. Cette théorie nous empêche de déterminer avec certitude les résultats, par conséquent, nous devons faire des estimations pour essayer de deviner où la particule se trouve.

3.2 Paradoxe EPR

« Dieu ne joue pas aux dés avec l'Univers. »
Albert Einstein

L'une des raisons pour lesquelles on considère Albert Einstein comme l'un des physiciens les plus célèbres et les plus importants de l'histoire est la *théorie de la relativité*. Vous en avez surement entendu parler, mais de quoi s'agit-il ? La théorie de la relativité comprend deux parties : *la relativité restreinte* (1905), où Einstein explique sa théorie sans la gravitation, et la *relativité générale* (1915-1916), où Einstein ajoute la gravitation à sa théorie.

La *relativité restreinte* est la première à avoir été publiée, entre juin et novembre 1905, par le biais de 4 articles. L'impact fut si grand pour la physique de l'époque que ces articles ont été baptisés Annus Mirabilis Papers (les articles de l'année miraculeuse). Ils ont été publiés dans la revue scientifique Annalen der Physik.

Le premier article apparait le 9 juin 1905 sous le nom de « Un point de vue euristique concernant la production et la transformation de la lumière ». Il y expose sa théorie sur l'effet photoélectrique[5]. C'est grâce à cet article qu'il recevra le prix Nobel en 1921.

Le deuxième article, intitulé « Sur le mouvement de petites particules en suspension dans un liquide immobile, comme requis par la théorie cinétique moléculaire de la chaleur », est publié le 18 juillet 1905. Einstein y explique le comportement des particules immergées dans un liquide immobile. En outre, il donne des arguments mathématiques en faveur de l'existence de l'atome (avant cette date, les scientifiques avaient déjà utilisé l'atome comme un concept utile, mais ils n'étaient pas certains à 100 % que les atomes existaient).

L'article « De l'électrodynamique des corps en mouvement » est le troisième à avoir été publié, le 26 septembre 1905. Il s'agit de la *théorie de la relativité restreinte* elle-même. Einstein établit une limite physique pour la vitesse de tous les objets, qui est aussi celle de la lumière (300 000 km/s).

Le dernier article d'Einstein publié en 1905, « L'inertie d'un corps dépend-elle de l'énergie qu'il contient ?», date du 21 novembre. C'est là que l'on trouve la célèbre formule d'Einstein $E = mc^2$. Mais malgré sa célébrité, cette formule n'est pas l'authentique. En réalité, la forme originale est un peu plus complexe : $E^2 = m^2c^4 + p^2c^2$. Actuellement, nous en utilisons une autre qui rend les calculs plus faciles : $\frac{m \cdot c^2}{\sqrt{1 - \frac{v^2}{c^2}}}$ où *E* est l'énergie, m la masse, c la vitesse de la lumière $(3 \cdot 10^8 \text{ m/s})$ et *v* la vitesse de l'objet.

En novembre 1915, Einstein fait diverses conférences à l'académie prussienne des sciences et parle de la *relativité générale*. Lors de sa dernière conférence, il présente l'équation qui remplacera la gravitation de Newton. La gravitation n'est plus une force qui nous attire vers le centre d'une planète, mais bien la courbure de l'espace-temps.

De la *théorie de la relativité*, nous retiendrons seulement deux concepts : la lumière est composée de photons et rien ne peut pas dépasser la vitesse de la lumière.

En 1935, Erwin Schrödinger (oui, le monsieur du chat), en faisant des expériences, s'aperçut qu'il se passait quelque chose d'étrange lorsque deux particules étaient en contact. Il observa que lorsque les particules avaient été en contact et puis séparées, elles semblaient se comporter comme si elles avaient été la même particule, elles faisaient la même chose au même instant. Il baptisa cet effet l'*intrication*.

Einstein et d'autres scientifiques ne comprenaient pas ce qui se passait avec les particules et avaient une attitude plutôt hostile à l'égard de l'intrication. Cet effet semblait aller à l'encontre de certaines théories établies, et notamment à l'encontre du principe d'incertitude et de la théorie de la relativité d'Einstein, les deux bases des deux grandes théories.

Einstein pensait que si on laissait deux électrons interagir entre eux, au bout d'un certain temps, il y aurait une corrélation très élevée en raison du principe de conservation de la quantité de mouvement. De sorte que les deux électrons seraient identiques. Mais alors, Einstein arriva à la conclusion que l'on pourrait, lorsque les électrons étaient identiques, mesurer la vitesse de l'un et la position de l'autre en vue de déterminer la position et la vitesse des deux électrons. Cet argument soulevait une grande controverse parmi les scientifiques, car selon le principe d'incertitude, nous ne pouvons pas connaitre avec certitude ces deux caractéristiques. Cela signifiait-il que le principe d'incertitude était faux ? Bien sûr que non ! Le principe d'incertitude était démontré ! Si le principe d'incertitude était correct, alors, la seule option était de supposer que les électrons sont capables de *communiquer* entre eux, de sorte que lorsque nous prenons une mesure sur un électron, l'autre obéit au principe et a la même incertitude que le premier. En définitive, les deux électrons se comportent comme un seul, *ce que l'on fait à l'un, c'est*

[5] L'effet photoélectrique établit (en termes généraux) qu'un matériau peut émettre des électrons quand il reçoit un photon avec suffisamment d'énergie.

ce que l'autre fait aussi. Cette communication doit être instantanée, sinon on pourrait violer le principe. Mais tout ce raisonnement présentait encore un autre problème.

Si ces deux électrons sont capables de communiquer instantanément et que nous les séparons d'une distance d'1 million de kilomètres et nous faisons une mesure, la communication aurait une vitesse supérieure à celle de la lumière (300 000 km/s) et ce n'est pas possible !

Face à ces problèmes, en 1935, Albert Einstein, Boris Podolsky et Nathan Rosen, écrivirent un article qui fut publié le 25 mars dans le journal américain *Physical Review*. Cet article est connu sous le nom de « Paradoxe EPR », mais son titre d'origine est « *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete* ». Dans cet article, ils exposent trois conditions à remplir pour avoir une bonne théorie :

Localité : Deux objets éloignés n'interfèrent pas entre eux à une vitesse plus élevée que celle de la lumière

Réalité : Si on ne modifie pas un système et que nous pouvons mesurer avec certitude la valeur d'une grandeur physique, il y a un élément de la réalité associé à cette valeur.

Complétude : Une théorie doit parler de tous les éléments de la réalité.

Dans le cas de cette paire d'électrons intriqués, la théorie quantique ne respecte pas la condition de localité. En conséquence, Einstein, Podolsky et Rosen définirent la théorie quantique comme une théorie incomplète. Tout au long des 4 pages de l'article, ils démontrent avec des formules et des arguments pourquoi la théorie quantique n'est pas complète, en supposant que le principe de Heisenberg et surtout la théorie de la relativité soient corrects.

En général, Einstein n'aimait pas trop la théorie quantique, les probabilités le dérangeaient, il défendait l'exactitude et le déterminisme de la physique. D'où sa célèbre phrase : « Dieu ne joue pas aux dés avec l'Univers », ce qui signifie que les phénomènes de l'Univers ne peuvent pas être décrits par des probabilités. En conséquence, Einstein croyait en l'existence de *variables cachées*, de paramètres. Mais tant que ces variables cachées ne sont pas connues, les probabilités de la physique quantique resteront en place.

Cet article fut bien accepté par de nombreux scientifiques, cependant, la raison pour laquelle la paire d'électrons pouvait communiquer à distance reste un mystère. Non seulement cela pouvait être des électrons, mais aussi des photons (communication à travers le spin).

3.3 Théorème et test de Bell

« Einstein, cessez de dire à Dieu ce qu'il doit faire. »
Niels Bohr

John Steward Bell, né en Irlande en 1928, fut un physicien très célèbre pour sa contribution à la physique quantique et pour la résolution du problème que supposait le paradoxe EPR.

En 1964, il présente le théorème de Bell selon lequel *une théorie physique de variables cachées ne peut pas reproduire toutes les prédictions de la mécanique quantique*. Avec cet argument, il nie l'hypothèse d'Einstein des variables cachées pour l'intrication.

Bell élabore une sorte de jeu pour démontrer sa théorie. Nous allons en expliquer une adaptation pour que ce soit plus facile à comprendre. Alice et Bob ont été séparés dans des salles où ils ne peuvent pas communiquer entre eux. On leur a donné une fiche avec une couleur aléatoire : vert ou rouge. Ils devront choisir entre 0 ou 1 et appuyer sur un bouton. Ils voient sur un écran une personne qui jette un dé chaque fois qu'on leur donne une nouvelle fiche. Tous les deux voient le même résultat du dé. L'objectif du jeu, c'est d'obtenir le plus de points possibles (+1 si on gagne, -1 si on perd) de la façon suivante :

• Si au moins l'un des deux candidats a une fiche de couleur verte, les numéros doivent être les mêmes.

• Si les deux candidats ont une fiche rouge, les numéros doivent être différents.

• La communication pendant le jeu est interdite.

• Les deux candidats peuvent développer une stratégie pour gagner le plus grand nombre de parties possibles avant de commencer.

Voici la grille de correction :

	VV	VR	RV	RR
00	√	√	√	X
01	X	X	X	√
10	X	X	X	√
11	√	√	√	X

Fig. 9 : Grille de correction pour le test de Bell

	VV	VR	RV	RR
00	√	√	√	X

Fig. 10 : Stratégie 75 %

	VV	VR	RV	RR
01	X	X	X	√

Fig. 11 : Stratégie 25 %

Les numéros à gauche sont les choix d'Alice.
Les numéros à droite sont les choix de Bob.
Dans chaque colonne nous avons :
La couleur à gauche est la couleur de la fiche d'Alice.
La couleur à droite est la couleur de la fiche de Bob.

Si nous appelons *variables cachées* la stratégie employée, nous aurons un système intriqué de photons (personnes) qui suivent les variables cachées et ne peuvent pas communiquer. Ces conditions simulent un scénario réel où les photons sont envoyés trop loin pour communiquer et doivent forcément utiliser les variables cachées. Dans le cas où les photons utilisent vraiment les variables cachées, le résultat d'une expérience sera le même que le résultat obtenu avec la meilleure stratégie suivie par une personne.

Avec un peu attention, nous pouvons conclure que l'une des meilleures stratégies est celle où l'on met partout 0 ou partout 1, car si toutes les couleurs sont aléatoires, toutes les combinaisons sortiront avec la même probabilité et nous aurons 75 % de probabilité de gagner. Si l'on faisait l'inverse, le résultat minimum serait de 25 %.

Ces résultats peuvent être vérifiés à l'aide d'un tableau *Excel* où l'on programme les couleurs pour qu'elles soient aléatoires et puis toutes les réponses 0. De cette manière, nous obtenons un pourcentage très proche de 75 % chaque fois qu'on fait le test. Avec un peu plus d'1 million de chiffres, nous obtenons 74,981 % ; avec 16 millions, 74,991 % ; avec 56 millions, 74,992 %... Plus nous utilisons un nombre élevé de chiffres, plus nous serons proche du 75 %.

Beaucoup de tests de Bell ont été réalisés au fil de l'histoire depuis son invention. Moi, j'ai mené une petite étude portant sur plus de 100 personnes qui ont fait le test.

J'ai proposé le même jeu que celui décrit ci-dessus, les candidats ont dû écrire des 0 et des 1 en suivant une stratégie ou aléatoirement. L'objectif de l'étude était de vérifier que les candidats ne peuvent pas avoir un taux de réussite de plus de 75 % ni de moins de 25 %. Si on les oblige à suivre une stratégie, ils vont se comporter comme des photons avec des variables cachées. En revanche, si on leur dit « Écrivez des numéros aléatoires », ils vont se comporter comme des photons sans variables cachées et avec intrication (ou pas). En conséquence, si les numéros sont aléatoires, nous pouvons aussi vérifier si les personnes ont une sorte de communication *télépathique*, par rapport aux photons intriqués.

Voici les résultats obtenus :

Parties gagnées: 2 265

Parties perdues: 2 078

Ratio: 0,5215289

Cent trente-deux personnes ont participé à cette étude et ont généré 8 686 numéros à partir desquels nous sommes arrivés aux résultats et conclusions suivants. Nous pouvons observer que 52,15 % des parties ont été gagnées. Cela signifie que le théorème de Bell s'est accompli et que, en général, nous, les êtres humains, nous ne sommes pas des *êtres non-locaux*, en d'autres termes, nous ne pouvons pas communiquer plus vite que la vitesse de la lumière. Si vous le préférez, nous n'avons pas de faculté télépathique. Cependant, il y a des cas où le pourcentage de parties « gagnées » de façon aléatoire a dépassé le pourcentage maximum attendu avec des variables cachées. Il y a eu seulement 8 cas (sur 174) de *communication* entre les participants, nous allons les analyser ensuite :

Premier cas[6] :

	RR	RV	VR	VV
00	1	3	4	2
01	1	0	0	0
10	1	0	0	0
11	4	4	2	4

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
21	5	0,807692308	0,307692308

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,730769231	0,230769231	0,076923077

SCORE MAX. Pourcentage maximum attendu de parties gagnées si la stratégie parfaite avait été suivie.

VAR. SCORE MAX. Variation du SCORE MAX. par rapport à 50 % en valeur absolue. (|SCORE MAX. – 0,5|)

DÉVIATION. La variation du ratio par rapport à 50 % moins la VAR. SCORE MAX. Si le résultat est positif, il est possible qu'il y ait eu une communication entre les participants. (VARIATION–VAR. SCORE MAX.)

[6] Premier cas (Annexe 1).

Longueur du test : 26 questions
Participants : Homme (27 ans environ) et Pablo Cerrato (17 ans).
Stratégie : Choisir 0 lorsque les numéros de dés sont pairs et 1 lorsque les numéros de dés sont impairs.
Pourquoi ? : L'homme a suivi la stratégie sauf dans 2 cas où il a changé, mais il a réussi.
Même s'ils suivaient tous les deux une stratégie, l'homme a ajouté quelques numéros aléatoires, ce qui a rendu sa partie aléatoire, tandis que Pablo a maintenu sa stratégie. C'est pour cette raison qu'ils ont eu un résultat plus élevé que celui que l'on attendait.

Deuxième cas[7] :

	RR	RV	VR	VV
00	0	0	4	0
01	0	0	1	5
10	8	0	0	0
11	2	5	0	0

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
17	8	0,68	0,18

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,6	0,1	0,08

Longueur du test : 25 questions
Participants : Marta Moreno (15 ans) et Víctor Cerrato (15 ans).
Stratégie : Marta a mis 0 aux fiches vertes et 1 aux rouges, par contre Víctor a joué sa partie d'une façon complètement aléatoire.
Pourquoi ? : Le caractère aléatoire des numéros de Víctor a fait que le pourcentage final soit plus grand. Il s'agit d'une situation similaire au premier cas. L'un a écrit les numéros de façon aléatoire et l'autre a suivi une stratégie. Ils ont eu de la chance, Víctor aurait pu mettre des numéros complètement différents et avoir eu un résultat moins bon. On pourrait dire que ce cas est celui des photons avec intrication. Mais cela ne veut pas dire que Marta et Víctor ont communiqué par télépathie ! Ils devraient faire beaucoup plus de tests avec une note égale ou supérieure pour vraiment vérifier l'existence d'une communication télépathique.

Troisième cas[8] :

	RR	RV	VR	VV
00	1	1	3	0
01	0	0	4	4
10	3	3	1	1
11	4	0	0	0

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
7	18	0,28	0,22

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,68	0,18	0,04

Longueur du test : 25 questions.
Participants : Marta Moreno (15 ans) et Pablo Cerrato (17 ans).
Stratégie : Tous les deux ont fait le test aléatoirement.
Pourquoi ? : De la chance.

[7] Deuxième cas (Annexe 2).
[8] Troisième cas (Annexe 3).

Quatrième cas[9] **:**

	RR	RV	VR	VV
00	1	3	1	2
01	4	1	1	0
10	2	0	3	0
11	0	2	3	2

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
19	6	0,76	0,26

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,72	0,22	0,04

Longueur du test : 25 questions.
Participants : Carla Encrenaz (7 ans) et Céline Encrenaz (7 ans).
Stratégie : Carla et Céline ont suivi chacune une stratégie différente, mais Carla a changé un numéro et a réussi.
Pourquoi ? : Exactement pour la même raison que dans le premier cas, de la chance.

Cinquième cas[10] :

	RR	RV	VR	VV
00	0	6	0	8
01	7	0	4	0
10	0	0	0	0
11	0	0	0	0

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
21	4	0,84	0,34

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,72	0,22	0,12

Longueur du test : 25 questions.
Participants : Rosa Galdeano (18 ans) et Pablo Cerrato (17 ans).
Stratégie : Rosa a mis des zéros et Pablo a fait le test aléatoirement.
Pourquoi ? : Probablement de la chance et la distribution des fiches.
Il s'agit du test pour lequel la déviation a été la plus grande (12 %).

Sixième cas[11] :

	RR	RV	VR	VV
00	5	1	2	0
01	3	3	2	0
10	2	1	2	0
11	2	1	1	0

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
10	15	0,4	0,1

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,52	0,02	0,08

Longueur du test : 25 questions.
Participants : Fernando del Castillo (56 ans) et Iván Cubero (18 ans).
Stratégie : Chacun a suivi une stratégie différente.
Pourquoi ? : La distribution des couleurs n'a pas été égale, on peut observer qu'il n'y a pas eu vert-vert.

[9] Quatrième cas (Annexe 4).
[10] Cinquième cas (Annexe 5).
[11] Sixième cas (Annexe 6).

Septième cas[12] :

	RR	RV	VR	VV
00	2	1	1	2
01	3	1	0	2
10	3	1	1	0
11	1	2	2	3

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
17	8	0,68	0,18

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,64	0,14	0,04

Longueur du test : 25 questions.
Participants : Anna Bárcena (17 ans) et Oriol González (17 ans).
Stratégie : Ils ont choisi des numéros de manière aléatoire.
Pourquoi ? : De la chance.

Huitième cas[13] :

	RR	RV	VR	VV
00	2	1	1	0
01	5	0	1	2
10	3	1	0	3
11	2	2	1	1

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
14	11	0,56	0,06

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,52	0,02	0,04

Longueur du test : 25 questions.
Participants : Francisco Serrano (66 ans) et Josefa Laynez (67 ans).
Stratégie : Ils ont choisi des numéros de manière aléatoire.
Pourquoi ? : Le pourcentage maximum était très petit, seulement le 52 %. Avec un pourcentage très bas, ils ont pu dépasser facilement le maximum établi pour une stratégie.

3.4 Inégalité de Bell

« Non seulement Dieu joue aux dés, mais il les jette parfois où ils ne peuvent pas se voir. »
Stephen Hawking

Au point précédent, nous avons découvert l'une des contributions à la physique de John Steward Bell, le test de Bell, et nous savons à présent de quoi il s'agit. En outre, nous avons observé les résultats que des êtres humains, c'est-à-dire des *êtres locaux*, obtiennent en faisant le test de Bell.

Nous avons constaté que, en moyenne, on peut obtenir un pourcentage maximum de 75 % et un pourcentage minimum de 25 %. Aussi, nous pouvons dire :

$$25\ \% \leq \textit{Pourcentage obtenu} \leq 75\ \%$$

Ce résultat peut aussi s'écrire comme suit :

$$-2 \leq \frac{g}{\frac{n}{4}} \leq 2$$

[12] Septième cas (Annexe 7).
[13] Huitième cas (Annexe 8).

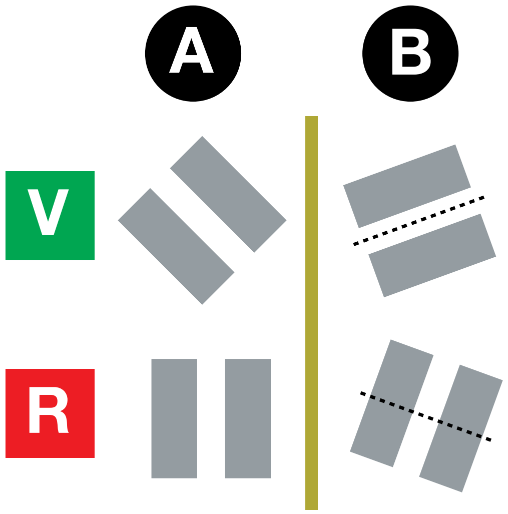
Où *g* sont les points obtenus (+1 si on gagne, -1 si on perd) et *n* sont les numéros écrits. Il s'agit de ladite *inégalité de Bell*, proposée par Bell en 1964. Cette équation est vérifiée pour tous les êtres locaux. Mais par contre, si nous faisons passer un test de Bell à un être non-local, l'inégalité sera violée, c'est-à-dire que l'équation donnera plus que 2 ou moins que -2.

Nous ne pouvons pas faire l'expérience nous-mêmes, parce que l'on aurait besoin de photons intriqués et d'une façon de les mesurer. Ces processus sont difficiles à réaliser et les matériaux sont chers. Alors, il ne nous reste que deux options : utiliser les mathématiques ou utiliser un ordinateur quantique. Moi, j'ai employé les deux méthodes.

Commençons par les mathématiques. Dans l'introduction, nous disions que si un photon a un état de polarisation déterminé, nous pouvons utiliser un filtre polarisateur pour mesurer son état. Nous savons que si l'état de polarisation du photon correspond à la direction du filtre, il passe avec une probabilité égale à 1 (100 %). Dans tous les autres cas, la probabilité de traverser le filtre est égale à $\cos^2 \theta$. Nous pouvons alors mesurer le pourcentage que l'on obtiendrait dans le cas de deux photons intriqués. Il faut tenir compte du fait que si les photons sont intriqués, celui que reçoit Bob aura une polarisation orientée de 90° par rapport à celui d'Alice.

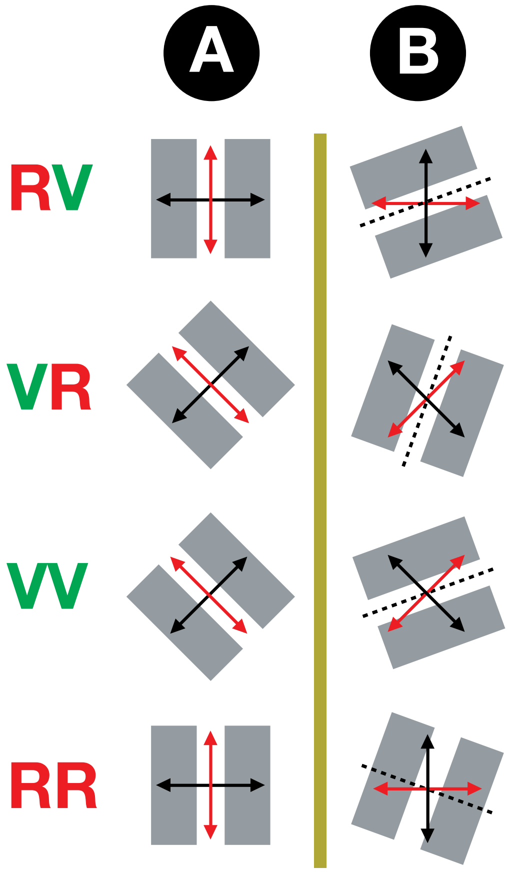
Pour réaliser cette expérience mathématique, imaginons qu'Alice et Bob font le test de Bell avec des filtres polarisateurs. Ils décident que s'ils reçoivent une fiche d'une couleur, ils disposeront leur filtre d'une certaine façon, tandis que s'ils reçoivent une fiche de l'autre couleur, ils le feront tourner de 45°.

Voici la position des polarisateurs en fonction de la couleur de la fiche :



Quand la fiche est verte, Alice orientera son filtre à 45° et Bob à 22,5°.

Quand la fiche est rouge, Alice orientera son filtre à 90° et Bob à 67,5°



$$\left.\begin{aligned} P_{00} &= \tfrac{1}{2} \cdot \cos^2 22{,}5^\circ = 0{,}427 \\ P_{11} &= \tfrac{1}{2} \cdot \sin^2 67{,}5^\circ = 0{,}427 \end{aligned}\right\} P = 0{,}854$$

$$\left.\begin{aligned} P_{00} &= \tfrac{1}{2} \cdot \sin^2 67{,}5^\circ = 0{,}427 \\ P_{11} &= \tfrac{1}{2} \cdot \cos^2 22{,}5^\circ = 0{,}427 \end{aligned}\right\} P = 0{,}854$$

$$\left.\begin{aligned} P_{00} &= \tfrac{1}{2} \cdot \sin^2 67{,}5^\circ = 0{,}427 \\ P_{11} &= \tfrac{1}{2} \cdot \cos^2 22{,}5^\circ = 0{,}427 \end{aligned}\right\} P = 0{,}854$$

$$\left.\begin{aligned} P_{01} &= \tfrac{1}{2} \cdot \sin^2 67{,}5^\circ = 0{,}427 \\ P_{10} &= \tfrac{1}{2} \cdot \cos^2 22{,}5^\circ = 0{,}427 \end{aligned}\right\} P = 0{,}854$$

Maintenant, nous pouvons calculer la probabilité de gagner pour chaque combinaison de couleurs.

Si nous additionnons les probabilités (en moyenne), nous obtenons un pourcentage de 85,4 %($\frac{2+\sqrt{2}}{4}$ plus exactement). Et donc :

$$25\,\% \leq 85{,}4\,\% \nleq 75\,\%$$

Voilà une preuve mathématique de la non-localité des photons intriqués.

Comme nous le disions, on peut également tester l'inégalité de Bell à l'aide d'un ordinateur quantique. Nous en reparlerons au chapitre V, ainsi que de la computation quantique. Voyons à présent où il est possible de trouver un ordinateur quantique et quels sont les résultats obtenus.

En mars 2017, IBM a créé un ordinateur quantique public grâce auquel on peut mener des expériences quantiques tout simplement en les proposant sur leur site Internet. C'est exactement ce que j'ai fait, j'ai visité leur site et j'ai proposé une expérience où les photons violent l'inégalité de Bell. Cette expérience a été réalisée avec 8 192 photons intriqués. Voici les résultats obtenus pour toutes les combinaisons de couleurs :

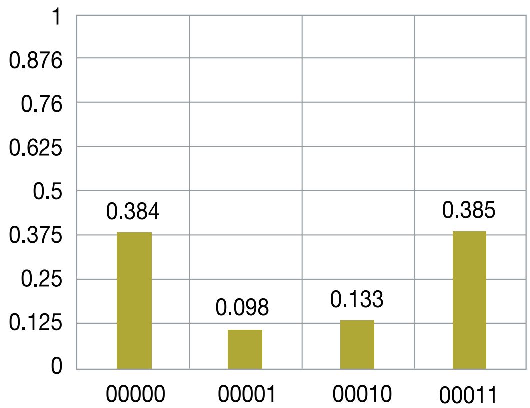


Fig. 12 : Résultats RV

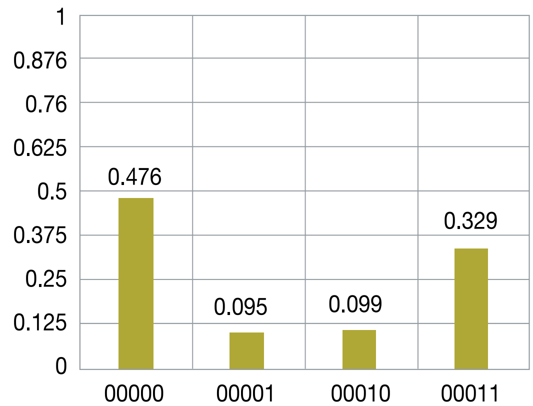


Fig. 13 : Résultats VR

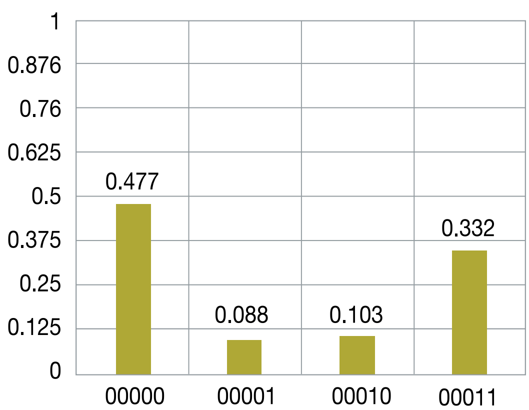


Fig. 14 : Résultats VV

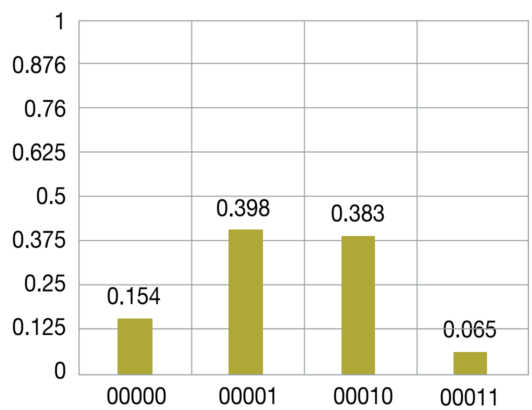


Fig. 15 : Résultats RR

Si nous faisons le calcul, le résultat est de 79,1 %, ce qui est en dehors de la limite de 75 % que l'inégalité établit.

Nous avons vu jusqu'ici tout ce que j'ai fait pour vérifier la violation de l'inégalité de Bell dans le cas des photons intriqués et sa confirmation dans le cas des *êtres locaux* ou qui suivent des stratégies ou variables cachées. Mais bien entendu, il y a d'autres institutions et des laboratoires qui ont aussi effectué des expériences en vue d'étudier l'inégalité de Bell.

Ainsi, l'Institut de sciences photoniques (ICFO) a dirigé une étude à l'échelle mondiale appelée *Big Bell Test*. Comme son nom l'indique, il s'agit d'un test de Bell où des personnes du monde entier ont généré des 1 et 0 de manière aléatoire pour faire cette grande expérience. Le 30 novembre 2016, plus de 100000 personnes de 190 pays se sont connectées pour générer plus de 90 millions de numéros aléatoires qui ont été analysés par 15 institutions au moyen de différentes expériences. Ils ont tous pu confirmer que l'inégalité de Bell était violée et que les photons intriqués avaient une nature non-locale.

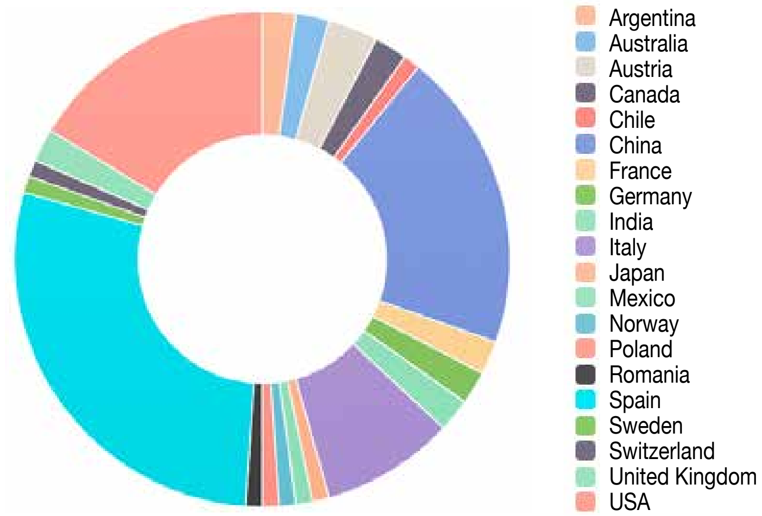


Fig. 16 : Top 20 des pays les plus participatifs au Big Bell Test

Nous pouvons donc affirmer que les photons intriqués n'ont pas de variables cachées et ne suivent pas le principe de localité, c'est-à-dire le principe que devrait avoir, selon Einstein, toute bonne théorie. D'où Einstein avait très probablement tort en disant que les photons ont des variables qui leur disent comment agir.

4 NON-LOCALITÉ QUANTIQUE ET INTRICATION

Tout au long du travail, nous avons parlé du mot « non-local » et de la possibilité de communiquer plus rapidement que la vitesse de la lumière, mais qu'est-ce que cela signifie vraiment ? Dans ce chapitre, nous examinerons l'évolution du monde par rapport à la physique quantique et ce qu'il est possible de faire avec toutes ces théories extravagantes et théorèmes complexes.

4.1 Vers un monde non-local

« Photons that did tango can never untangle. »
Alejandro Martínez Gallardo

Nous avons vu que les photons intriqués possèdent une nature non-locale. Cela veut dire qu'ils peuvent communiquer entre eux plus rapidement que la vitesse de la lumière. Plus exactement, ils peuvent communiquer entre eux instantanément, et ce où qu'ils soient, à 2 millimètres ou à 3 000 millions d'années-lumière. Ce qui signifie que nous pourrions communiquer avec un ami qui habite en Chine ou avec un extraterrestre qui habite à l'autre bout de l'Univers avec la même vitesse (c'est-à-dire instantanément).

Cela étant dit, quelle serait la façon de communiquer ? De fait, la façon de communiquer serait très semblable à celle d'un *ordinateur classique* (ordinateur normal), avec des bits d'information, c'est-à-dire des 0 et des 1. Alors, pourquoi ne sommes-nous pas encore capables de communiquer instantanément ? Parce qu'un bit normal n'est pas le même qu'un bit quantique ou *qubit*. Un bit classique peut être un 0 ou un 1, nous pouvons avoir trois bits avec la combinaison 011. La différence entre un bit et un qubit, c'est que le qubit n'est pas un 0 ni un 1, mais les deux à la fois ! Ce n'est qu'au moment de la mesure que le bit se décide pour un 0 ou 1. Alors si nous avons trois qubits, les combinaisons possibles sont 000, 001, 010, 011, 100, 101, 110 et 111. Toutes ces options sont possibles avec seulement trois qubits. Plus on a de qubits, plus on a de combinaisons. Nous pouvons observer que le nombre de combinaisons possibles augmente de façon exponentielle, selon la fonction suivante :

$$q=2^n$$

Où *q* est le nombre de combinaisons et *n* le nombre de qubits. Voici quelques exemples : avec 2 qubits, nous aurons 4 combinaisons ; avec 3, nous en aurons 8 ; avec 5, nous en aurons 32 ; avec 8, 256 ; avec 10, 1 024 ; avec 15, 32 768 ; avec 20 qubits, nous aurons 1 048 576 possibilités… Ce nombre augmente très rapidement. La différence entre le bit et le qubit est évidente, alors que 8 bits classiques peuvent exprimer un résultat (10010111 par exemple), 8 bits quantiques peuvent exprimer 256 résultats, toutes les combinaisons possibles.

Les qubits sont une superposition des états $|0\rangle$ et $|1\rangle$, où l'état $|0\rangle$ se donnera avec une certaine probabilité α et l'état $|1\rangle$ se donnera avec une probabilité β, tel que $\alpha^2 + \beta^2 = 1$, comme nous l'avons vu aux points 2.2 *État quantique* et 2.4 *Mesure quantique*. L'état de superposition peut être écrit de la façon suivante :

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$$

De plus, si les qubits sont intriqués, nous avons une autre expression pour les représenter d'une façon telle que le changement de l'un implique le changement de l'autre.

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Quand on mesure un qubit, il ne sera plus dans un état de superposition, il deviendra un bit classique, peu importe combien de fois nous recommençons la mesure, dorénavant, il sera toujours le même, soit un 0, soit un 1.

Il en va de même lorsque deux photons sont intriqués, quand on mesure l'un, il devient un bit classique et, comme les deux sont intriqués, l'autre devient aussi un bit classique, le même que le premier photon.

Alors, nous pouvons imaginer le futur de la communication. Alice et Bob, séparés par des millions de kilomètres, pourront communiquer entre eux instantanément avec ce système. Alice pourrait envoyer un message de manière à ce que les photons en superposition intriqués avec ceux de Bob deviennent des bits classiques. Ensuite, Bob les mesurerait aussi et obtiendrait le résultat des bits classiques d'Alice.

Par exemple, Alice veut dire *bonjour* à Bob. Imaginons que *bonjour* en binaire soit 101. Bob et Alice ont chacun 3 photons intriqués en état de superposition. Alice mesure le premier et obtient le bit classique 1. Elle fait de même avec le deuxième et obtient 0, puis avec le troisième et obtient 1. Ensuite, Bob mesure les bits et obtient les mêmes résultats que ceux d'Alice. Voilà la méthode de fonctionnement. Mais ils pourraient faire l'inverse, Bob pourrait mesurer les photons d'abord pour envoyer un message à Alice.

4.2 Théorème de non-communication

« La science peut ne jamais arriver à un meilleur système de communication de bureau que la pause-café. »
Earl Wilson

Earl Wilson fut le célèbre joueur de baseball qui laissa cette citation à l'histoire de la science et du bureau. Il a surement dit cela sans avoir de connaissances en physique quantique, mais avec sa citation, il a prédit un théorème quantique.

Effectivement, le théorème de non-communication ne se limite pas seulement au bureau, mais concerne aussi l'Univers. La pause-café et la communication en vis-à-vis resteront toujours le meilleur système de communication.

Le théorème de non-communication établit qu'on ne peut pas communiquer avec une autre personne par la méthode d'intrication de photons sans avoir un signal classique ou local. Cela veut dire que nous ne pouvons pas communiquer avec une autre personne en utilisant la méthode de l'intrication de photons sans l'avoir appelée auparavant.

Mais alors, pourquoi avons-nous besoin d'un signal qui voyage au maximum à la vitesse de la lumière pour ensuite communiquer à une vitesse supérieure à la lumière ? La réponse parait un peu surprenante, mais si l'on réfléchit un peu, c'est évident. Nous avons dit qu'une fois que le photon en état de superposition est mesuré, il restera toujours dans le même état et il n'y aura plus de superposition. Donc Bob ne peut pas savoir si Alice a envoyé un message. Voici un exemple.

Imaginons qu'Alice a le photon suivant en état de superposition intriqué avec un autre photon de Bob. Le photon d'Alice a une probabilité de 1/2 (50 %) d'être dans l'état $|0\rangle$ et une probabilité de 1/2 (50 %) d'être dans l'état $|1\rangle$.

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Alors, Alice prend la mesure et obtient l'état $|0\rangle$. En conséquence, l'état d'intrication sera le suivant :

$$|\beta_{-00}\rangle=1|00\rangle+0|11\rangle$$

Les photons ont une probabilité de 1 (100 %) d'être dans l'état $|0\rangle$ et une probabilité de 0 (0 %), d'être dans l'état $|1\rangle$. Nous pouvons écrire la fonction de la manière suivante :

$$|\beta_{-00}\rangle=|00\rangle$$

On voit clairement que les deux photons sont dans l'état $|0\rangle$ et qu'il n'y a pas d'autre possibilité. L'état $|11\rangle$ n'apparait même pas, parce que c'est impossible de changer l'état.

Bob fait ensuite la mesure de son photon intriqué $|\beta_{-00}\rangle=|00\rangle$ et obtient évidemment l'état $|0\rangle$. Ce que l'on vient de voir est un cas où il y a une intention communicative d'Alice et une intention réceptive de Bob. Voyons à présent ce qu'il se passe lorsqu'il n'y a pas de communication d'Alice mais que, par contre, il y a une intention réceptive de Bob.

Recommençons : Alice a le photon suivant en état de superposition intriqué avec un autre photon de Bob.

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Alice ne veut rien dire, alors, elle ne prend aucune mesure, car ce n'est pas nécessaire. En conséquence, la fonction d'onde des photons reste la même :

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Bob veut savoir ce qu'Alice a dit, mais il ne sait pas si Alice a dit quelque chose, ils sont séparés. Il décide de mesurer le photon. Il prend la mesure du photon dans cet état, où il va obtenir avec la même probabilité l'état $|0\rangle$ et l'état $|1\rangle$.

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Bob obtient l'état $|1\rangle$, mais Alice n'a rien envoyé. Si Bob pense qu'Alice a envoyé un message, il recevra un faux message.

Si au lieu d'avoir un photon, il y en a trois. Bob pourra mesurer les états 101 et interpréter qu'Alice lui a dit *bonjour*. Il pourra aussi lire 011 qui signifie *poisson* ou 111 qui signifie *montre*[14].

Pour éviter ce problème, il faut qu'Alice envoie d'abord un signal d'appel à Bob et puis qu'elle envoie le message. Mais on revient au même problème, Bob ne peut pas savoir avec certitude si Alice est en train d'appeler, il pourrait mesurer les photons et arriverait à la conclusion qu'Alice est en train de l'appeler alors qu'Alice ne l'a pas fait.

Le théorème dit alors que pour toute communication non-locale, il faut une communication locale. C'est-à-dire que pour pouvoir communiquer avec les photons intriqués, il faut d'abord envoyer un signal d'appel avec des photons qui voyagent à la vitesse de la lumière ou employer une autre méthode qui suit le principe de localité. À partir du moment où ils ont communiqué classiquement, ils pourront communiquer avec des photons intriqués librement.

[14] Il faut remarquer que j'ai complètement inventé la relation entre les nombres binaires et les mots, 101 ne veut pas dire bonjour. J'ai fait ça en vue de rendre plus facile l'explication.

5 COMPUTATION QUANTIQUE

Tout au long du travail, nous avons parlé du mot *non-local* et de la possibilité de communiquer plus rapidement que la vitesse de la lumière, mais qu'est-ce que cela signifie vraiment ? Le monde connait une énorme avancée technologique et scientifique grâce aux ordinateurs quantiques.

Dans ce chapitre, nous allons découvrir les ordinateurs quantiques, ce qu'il est possible de faire avec eux et comment ils nous protègent d'un intrus qui essayerait de nous voler des informations quantiques.

5.1 Liste de courses quantique

« La physique est le système d'exploitation de l'Univers. »
Steven R. Garman

Nous savons que les qubits constituent le fondement d'un ordinateur quantique. Un ordinateur quantique est presque identique à un ordinateur classique, mais il utilise des qubits comme unité minimale d'information.

Nous savons aussi qu'un qubit est un mélange (superposition) des états $|0\rangle$ et $|1\rangle$ en même temps. Cela nous permet de calculer très rapidement. Un ordinateur classique peut donner une seule combinaison avec *n* bits ordonnés, tandis qu'un ordinateur quantique peut donner 2^n combinaisons avec *n* qubits ordonnés ou pas. De plus, un ordinateur quantique peut faire des calculs qu'un ordinateur classique ne peut pas faire, et notamment déchiffrer le code d'accès d'un ordinateur classique avec une certaine facilité et relativement vite.

Alors, que peut-on faire ? En tout cas, nous pouvons élaborer une énorme liste de courses. Énorme veut dire vraiment énorme, gigantesque. Un ordinateur classique pourrait trouver ce que l'on doit acheter très rapidement, mais un ordinateur quantique peut faire la même chose en $\sqrt{n}$ pas, où n est le nombre de démarches qu'un ordinateur classique doit suivre. Cela représente une énorme différence. Si nous avons une liste de 4 294 967 296 choses à acheter et que nous voulons savoir si nous avons déjà acheté du lait, un ordinateur devrait faire 4 294 967 296 pas pour trouver le lait (au pire des cas, lorsque le lait se trouve au bout de la liste). En revanche, un ordinateur quantique devrait faire seulement 65 536 pas pour trouver le lait. Si les deux ordinateurs avaient le même taux de bits/s (bits traités chaque seconde), l'ordinateur quantique irait 65 536 fois plus vite qu'un ordinateur classique. Ce cas concret correspond à un algorithme de recherche quantique dénommé le *Grover's search algorithm*.

Maintenant que nous savons un peu ce qu'est un ordinateur quantique, nous allons aborder le système de sécurité des données quantiques.

5.2 Cryptographie

« Le génie de la cryptographie est hors de la bouteille. »
Jan Koum

L'un des problèmes sans cesse mentionné tout au long de l'histoire est la protection de l'information. C'est pour y faire face que la cryptographie fut inventée.

Les origines de la cryptographie remontent à 4500 av. J.-C., lorsque les Égyptiens écrivirent des hiéroglyphes non standards. Puis la cryptographie a évolué au fil du temps jusqu'à nos jours. Elle passa de la substitution de lettres à d'autres méthodes telles que la scytale, le code de César…

En 1882, Frank Miller inventa un système de cryptographie indéchiffrable, le *masque jetable*. En 1919, Gilbert Vernam breveta le système. Il s'agit d'un système indéchiffrable, parce que si nous essayons de le déchiffrer, nous obtiendrons toutes les combinaisons possibles. Le système du *masque jetable* fonctionne de la manière suivante. Imaginons que deux personnes (Alice et Bob) veulent échanger un message, mais sans que personne ne sache ce qui est écrit. Alice et Bob partagent un masque, c'est-à-dire, un code qui sert à chiffrer et déchiffrer le message. Alice prend son message, y ajoute le masque et envoie le résultat à Bob. Bob reçoit le message et soustrait le masque, pour obtenir le message original.

Voici un exemple. Alice veut envoyer à Bob le message *Bonjour.* Alice sépare les lettres et écrit le numéro qui correspond à chaque lettre de l'alphabet.
2 (B) 15 (O) 14 (N) 10 (J) 15 (O) 21 (U) 18 (R)

Tous les deux partagent un masque :
16 (P) 12 (L) 15 (O) 3 (C) 17 (Q) 23 (W) 4 (D) …

Alice additionne le message et le masque pour obtenir le message chiffré.

2 (B)	15 (O)	14 (N)	10 (J)	15 (O)	21 (U)	18 (R)	Massage
+ 16 (P)	12 (L)	15 (O)	3 (C)	17 (Q)	23 (W)	4 (D)	Masque
18 (R)	27 (?)	29 (?)	13 (M)	32 (?)	44 (?)	22 (V)	Massage chiffré

Nous pouvons observer que certains nombres dépassent 26 (Z). Pour associer une lettre à ces numéros, nous allons recommencer l'alphabet avec 27 (A). En conséquence, le message chiffré sera le suivant :
18 (R) 27 (A) 29 (C) 13 (M) 32 (F) 44 (R) 22 (V)

Alice envoie le message chiffré à Bob et il le reçoit. Alors, Bob déchiffre le message avec le même masque qu'Alice.

18 (R)	27 (A)	29 (C)	13 (M)	32 (F)	44 (R)	22 (V)
- 16 (P)	12 (L)	15 (O)	3 (C)	17 (Q)	23 (W)	4 (D)
2 (B)	15 (O)	14 (N)	10 (J)	15 (O)	21 (U)	18 (R)

Voilà le message que Bob a déchiffré. Il correspond au message original.

Alors, pourquoi dit-on que ce système est indéchiffrable ? Nous avons dit que l'on pourrait trouver toutes les combinaisons possibles. Prenons l'exemple d'une espionne appelée Ève. L'espionne essaiera de déchiffrer le message envoyé par Alice. Mais Ève ne connait pas le masque. Voyons ce qui se passerait dans ce cas.

Ève prend le message envoyé par Alice et le déchiffre avec son propre masque, un masque qu'elle a elle-même inventé :

18 (R)	27 (A)	29 (C)	13 (M)	32 (F)	44 (R)	22 (V)
- 12 (L)	9 (I)	14 (N)	26 (Z)	5 (E)	11 (K)	17 (Q)
6 (F)	18 (R)	15 (O)	-13 (M)	27 (A)	33 (G)	5 (E)

Nous pouvons observer qu'avec le même message envoyé par Alice, une personne qui ne connait pas le masque pourrait obtenir le mot *fromage*. Ève pourrait tout aussi bien avoir obtenu le mot *portable,* *montrez, biscuit* ou même *sqwldn* ou *onebci*. Ève ne peut pas déterminer quel est le masque utilisé par Alice et Bob.

Si nous utilisons des bits binaires, il suffit de faire l'addition, car additionner deux fois en binaire, c'est comme si on n'avait rien fait[16]. Voici un exemple :

$$
\begin{array}{rcccccc}
 & 0 & 0 & 1 & 1 & 0 & 1 \\
+ & 0 & 1 & 0 & 1 & 0 & 0 \\
\hline
 & 0 & 1 & 1 & 0 & 0 & 1
\end{array}
\qquad\qquad
\begin{array}{rcccccc}
 & 0 & 1 & 1 & 0 & 0 & 1 \\
+ & 0 & 1 & 0 & 1 & 0 & 0 \\
\hline
 & 0 & 0 & 1 & 1 & 0 & 1
\end{array}
$$

Résultat : 0 1 1 0 0 1

Nous pouvons observer que nous obtenons le même message en additionnant deux fois le masque quand on additionne en binaire.

Nous avons vu que le système du *masque jetable* est excellent pour chiffrer nos messages si l'on souhaite que personne ne comprenne rien. Toutefois, malgré l'efficacité de cette méthode, il faut qu'Alice et Bob se donnent rendez-vous pour définir le masque, car s'ils procèdent autrement, Ève peut les épier et prendre aussi possession du masque.

Par conséquent, elle pourra les épier sans être découverte. Donc, la meilleure manière de définir un masque est de se donner rendez-vous. Ainsi, Ève n'aura pas la possibilité d'intervenir et d'écouter le masque.

5.3. Sécurité quantique

En dépit de ce que l'on vient de dire, il existe une manière de définir un masque sans qu'Ève ne puisse aussi l'avoir, ou tout au moins sans qu'on ne le sache. L'évolution de la technologie quantique permet d'utiliser une méthode telle que, si Ève a épié, nous le saurons.

Grâce à la propriété invasive de la mesure quantique, on peut savoir si Ève a essayé d'épier le masque. Voici comment procèdent Bob et Alice.

Bob et Alice veulent créer un masque sans se donner rendez-vous, car ils habitent chacun à l'autre bout du monde. Ils vont s'envoyer des bits, ou plus exactement des photons polarisés dans des bases aléatoires que chacun choisira. Pour cette expérience, nous les laisserons choisir entre les bases + et X. Attribuons un bit à chacun des états de chaque base. Pour la base +, $|\leftrightarrow\rangle$ sera 0 et $|\updownarrow\rangle$ sera 1. Pour la base X, $|\nearrow\rangle$ sera 0 et $|\searrow\rangle$ sera 1. Alice commence à choisir des bases aléatoires, Bob le fait aussi

CAHIER D'ALICE			
Numéro	Base (+,X)	Bit (0,1)	Polarisation ($\leftrightarrow,\updownarrow,\searrow,\nearrow$)
1	+		
2	x		
3	x		
4	x		
5	+		
6	+		
7	x		
8	x		
9	+		
10	+		

CAHIER DE BOB				
Base (+,X)	Bit (0,1)	Base égale	Bit (0,1)	Erreur
x				
x				
+				
x				
x				
+				
+				
+				
x				
+				

16 0+0=0; 0+1=1; 1+0=1; 1+1=0

Puis, Alice choisit des bits au hasard et note la position du polarisateur pour envoyer les photons à Bob :

CAHIER D'ALICE			
Numéro	Base (+,X)	Bit (0,1)	Polarisation (↔,↕,⤡,⤢)
1	+	1	↕
2	x	1	⤡
3	x	0	⤢
4	x	1	⤡
5	+	1	↕
6	+	1	↕
7	x	1	⤡
8	x	0	⤢
9	+	0	↔
10	+	0	↔

CAHIER DE BOB				
Base (+,X)	Bit (0,1)	Base égale	Bit (0,1)	Erreur
x				
x				
+				
x				
x				
+				
+				
+				
x				
+				

Alice envoie les photons polarisés et Bob les mesure avec la base qu'il a choisie. Si la base est la même, le bit reçu par Bob doit être le même envoyé par Alice. Par contre, si la base est différente, la probabilité de passer le filtre est le 50 %, en conséquent, il peut mesurer un 0 ou un 1. Voici les résultats obtenus :

CAHIER D'ALICE			
Numéro	Base (+,X)	Bit (0,1)	Polarisation (↔,↕,⤡,⤢)
1	+	1	↕
2	x	1	⤡
3	x	0	⤢
4	x	1	⤡
5	+	1	↕
6	+	1	↕
7	x	1	⤡
8	x	0	⤢
9	+	0	↔
10	+	0	↔

CAHIER DE BOB				
Base (+,X)	Bit (0,1)	Base égale	Bit (0,1)	Erreur
x	0			
x	1			
+	0			
x	1			
x	1			
+	0			
+	0			
+	0			
x	1			
+	0			

Maintenant, Alice dit à Bob les bases qu'elle a utilisées. S'ils ont utilisé la même, Bob mettra un ✓ à côté du bit et écrira le bit qu'il a reçu.

CAHIER D'ALICE			
Numéro	Base (+,X)	Bit (0,1)	Polarisation (↔,↕,⤡,⤢)
1	+	1	↕
2	x	1	⤡
3	x	0	⤢
4	x	1	⤡
5	+	1	↕
6	+	1	↕
7	x	1	⤡
8	x	0	⤢
9	+	0	↔
10	+	0	↔

CAHIER DE BOB				
Base (+,X)	Bit (0,1)	Base égale	Bit (0,1)	Erreur
x	0			
x	1	✓	1	
+	0			
x	1	✓	1	
x	1			
+	0	✓	1	
+	0			
+	0			
x	1			
+	0	✓	0	

Finalement, ils choisissent la moitié des bits pour lesquels les bases ont été les mêmes et ensuite les comparent. Si le bit envoyé par Alice n'est pas le même que celui que Bob a reçu, Ève aura épié. En revanche, si tous les bits envoyés coïncident avec les bits reçus, l'autre moitié des bits sera le masque.

CAHIER D'ALICE			
Numéro	Base (+,X)	Bit (0,1)	Polarisation (↔,↕,⤡,⤢)
1	+	1	↕
2	x	1	⤡
3	x	0	⤢
4	x	1	⤡
5	+	1	↕
6	+	1	↕
7	x	1	⤡
8	x	0	⤢
9	+	0	↔
10	+	0	↔

CAHIER DE BOB				
Base (+,X)	Bit (0,1)	Base égale	Bit (0,1)	Erreur
x				
x	1	✓	1	
+	0			
x	1	✓	1	
x	1			
+	0	✓	1	
+	0			
+	0			
x	1			
+	0	✓	0	

Ils comparent les bits numéro 2 et 6. Ils sont les mêmes, alors, le masque est 1 0. On peut dire qu'Ève n'a pas épié. Voyons à présent un autre cas.

CAHIER D'ALICE			
Numéro	Base (+,X)	Bit (0,1)	Polarisation (↔,↕,⤡,⤢)
1	+	1	↕
2	x	1	⤡
3	x	0	⤢
4	x	1	⤡
5	+	1	↕
6	+	1	↕
7	x	1	⤡
8	x	0	⤢
9	+	0	↔
10	+	0	↔

CAHIER DE BOB				
Base (+,X)	Bit (0,1)	Base égale	Bit (0,1)	Erreur
x				
x	1	✓	1	
+	0			
x	1	✓	1	
x	1			
+	0	✓	0	
+	0			
+	0			
x	1			
+	0	✓	0	

Ce cas est très similaire au précédent. Ils leur reste à vérifier les bits.

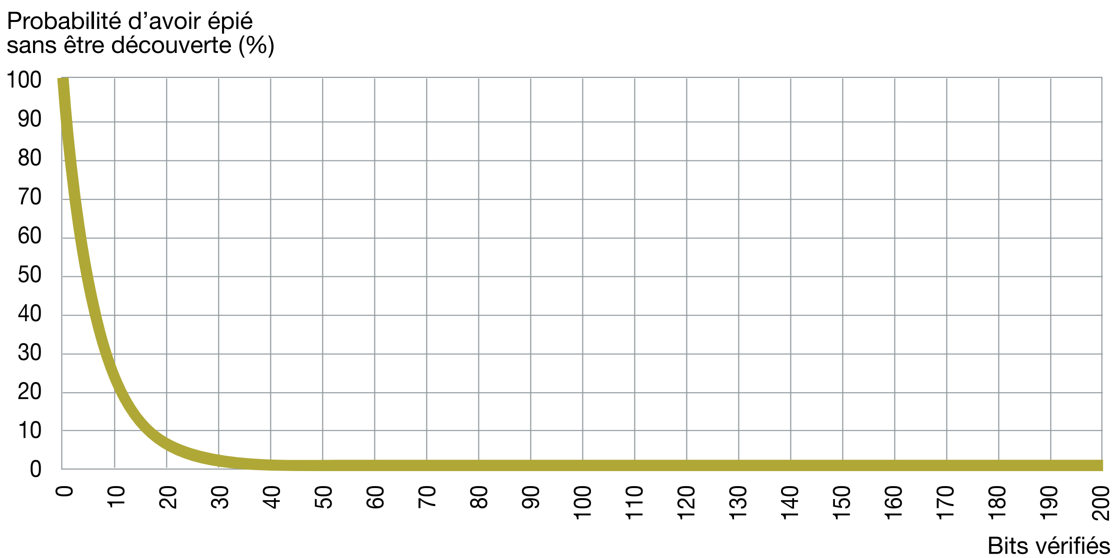
CAHIER D'ALICE			
Numéro	Base (+,X)	Bit (0,1)	Polarisation (↔,↕,⤡,⤢)
1	+	1	↕
2	x	1	⤡
3	x	0	⤢
4	x	1	⤡
5	+	1	↕
6	+	1	↕
7	x	1	⤡
8	x	0	⤢
9	+	0	↔
10	+	0	↔

CAHIER DE BOB				
Base (+,X)	Bit (0,1)	Base égale	Bit (0,1)	Erreur
x				
x	1	✓	1	
+	0			
x	1	✓	1	
x	1			
+	0	✓	0	X
+	0			
+	0			
x	1			
+	0	✓	0	

Le bit 6 n'est pas le même ! Donc, on sait qu'Ève a épié et connait le masque. Alors, il faut recommencer l'expérience.

Si nous savons qu'il y a deux bases possibles et deux bits pour chaque base, nous savons qu'il y a 4 possibilités d'états que l'on peut envoyer, soit |↔⟩, |↕⟩, |⤢⟩ et |⤡⟩. Si Ève positionne son polarisateur aléatoirement, elle aura 1 possibilité sur 4 de deviner la polarisation correcte. Donc, on peut dire qu'Ève modifiera le masque avec une probabilité de $p = \frac{3}{4}$.

La probabilité qu'Ève ait pu épier sans être découverte suit la fonction $p = (\frac{3}{4})^{\frac{n}{2}}$. Voici la représentation de la fonction.



Nous pouvons voir qu'elle décroit très rapidement car la probabilité d'être découverte augmente très rapidement.

6 CONCLUSIONS

Ayant terminé toutes mes recherches et obtenu toute l'information nécessaire, je suis prêt à faire une évaluation générale du travail.

Dans la mesure où l'objectif principal de mon travail était de confirmer les principales théories et théorèmes de la physique quantique, ainsi que d'apprendre de quoi il s'agit, je peux affirmer qu'il a été accompli de manière satisfaisante. Néanmoins, la difficulté du thème choisi et le manque d'informations disponibles sur Internet ont parfois rendu ce travail un peu difficile. Dans presque tous les cas, je ne trouvais que des documents spécialisés, dépourvus d'explications générales et accessibles pour un public désinformé ou sans connaissances approfondies des méthodes mathématiques. Étant donné que les mathématiques ont été mon principal outil de démonstration, j'ai rencontré des difficultés à comprendre le processus à suivre et parfois la notation était complètement nouvelle pour moi. Néanmoins, j'ai tenté d'expliquer la théorie le plus simplement possible, sans perdre pour autant l'essence du travail.

Quant à la partie expérimentale, il m'a été plutôt facile de la mener à terme. Au départ, je ne connaissais pas l'existence de l'ordinateur quantique d'IBM, ni même celle du test de Bell. Grâce à la séance de *Bojos per la Física* dédiée à la cryptographie quantique et au test de Bell, j'ai pu orienter mon travail et concevoir l'expérience quantique que j'ai menée (test de Bell). Les gens se sont montrés très aimables et collaboratifs à l'égard de mon expérience. Malgré le thème fort compliqué, la physique quantique, les gens s'y sont quand même intéressés. Certaines personnes ont compris le fonctionnement du monde quantique et s'en sont émerveillées.

Presque tous les objectifs initiaux ont été accomplis. J'ai fait une petite étude avec une participation de 132 personnes en vue de vérifier l'inégalité de Bell, ainsi qu'une expérience avec un total de 32 768 photons au moyen de l'ordinateur quantique d'IBM en vue de démontrer la violation de l'inégalité. En outre, j'ai aussi mené à bien l'expérience sur la méthode de chiffrement par *masque jetable* et j'ai pu observer les effets provoqués par une *espionne*. Néanmoins, je n'ai pas pu tester la probabilité concernant les filtres polarisateurs. J'ai essayé de construire un simulateur d'ordinateur quantique qui émulait l'intrication de photons et faisait des calculs de probabilité en relation avec les expériences quantiques, mais malheureusement, alors que j'étais sur le point de terminer, un Arduino a cessé de fonctionner et donc je n'ai pas encore pu l'achever.

J'aimerais conclure en disant que j'ai eu beaucoup de plaisir à faire ce travail. J'ai pu écrire et travailler sur un sujet qui me passionne. Apprendre de nouvelles choses a été une expérience vraiment réjouissante. J'ai eu l'opportunité de connaitre des scientifiques qui m'ont aidé et ont répondu à mes questions. Cela a aussi été l'occasion de faire connaitre autour de moi une très petite partie du vaste domaine qu'est la physique quantique en tentant de simplifier en toute humilité les explications.

7 SITOGRAPHIE

Mardi, 21 février 2017
http://www.nationalgeographic.es/noticias/ciencia/salud-y-cuerpo-humano/sincronizacion-corazones-seres-queridos - La synchronisation des cœurs. Étude de l'accélération du rythme cardiaque en fonction de la situation des êtres chers.
http://www.elmundo.es/elmundosalud/2013/07/16/corazon/1373987296.html - La synchronisation des cœurs. Étude de l'interaction entre le rythme cardiaque et de la musique.
https://fr.wikipedia.org/wiki/Intrication_quantique - Intrication quantique

Vendredi, 10 mars 2017
https://publications.polymtl.ca/215/ - Intrication temporelle et communication quantique

Dimanche, 19 mars 2017
http://francis.naukas.com/2013/01/10/carnaval-de-fisica-la-produccion-de-pares-de-fotones-entrelazados/ - Introduction à l'intrication de photons
https://es.wikipedia.org/wiki/%C3%93ptica_no_lineal#cite_note-1 - L'optique non-linéaire
https://es.wikipedia.org/wiki/Estado_cu%C3%A1ntico#Estados_degenerados_y_no-degenerados - États quantiques

Mardi, 9 mai 2017
https://www.youtube.com/watch?v=NTuOLfqCdXI - Espace d'Hilbert
https://www.youtube.com/watch?v=3r06XLVEFcE - Introduction à la mécanique quantique

Mardi, 11 juillet 2017
https://es.wikipedia.org/wiki/Estado_cu%C3%A1ntico - État quantique
https://es.wikipedia.org/wiki/Estado_f%C3%ADsico - État physique
https://es.wikipedia.org/wiki/Experimento_de_Young - Expérience de Young

Mercredi, 12 juillet 2017
https://es.wikipedia.org/wiki/Fot%C3%B3n - Photon

Jeudi, 30 novembre 2017
https://es.wikipedia.org/wiki/Albert_Einstein - Albert Einstein

Vendredi, 1 décembre 2017
https://fr.wikipedia.org/wiki/Principe_de_compl%C3%A9mentarit%C3%A9 - Principe de complémentarité
https://fr.wikipedia.org/wiki/Principe_d%27incertitude - Principe d'incertitude
https://fr.wikipedia.org/wiki/Constante_de_Planck - Constante de Planck
https://ioc.xtec.cat/campus/mod/assign/view.php?id=461444 - Idée d'une balle de baseball
https://respuestas.tips/medidas-y-peso-de-la-pelota-de-bisbol/ - Poids d'une balle de baseball

Samedi, 2 décembre 2017
http://cesire.cat.mialias.net/recursos/context/fisica/unitat%208/241_la_relativitat_especial.html - Vie d'Einstein
https://en.wikipedia.org/wiki/Annalen_der_Physik - Annelen der Physik (revue dans laquelle fut publiée la relativité restreinte)
https://fr.wikipedia.org/wiki/Annus_mirabilis_d%27Albert_Einstein - Annus mirabilis d'Albert Einstein
https://es.wikipedia.org/wiki/Entrelazamiento_cu%C3%A1ntico#Motivaci.C3.B3n_y_antecedentes_hist.C3.B3ricos – Histoire de l'intrication quantique
https://es.wikipedia.org/wiki/Paradoja_EPR - Paradoxe EPR
https://en.wikipedia.org/wiki/No-communication_theorem - Théorème de non-communication
https://en.wikipedia.org/wiki/John_Stewart_Bell - J. S. Bell
https://es.wikipedia.org/wiki/Teorema_de_Bell - Théorème de Bell

Mardi, 5 décembre 2017
https://es.wikipedia.org/wiki/C%C3%BAbit - Qubit

Samedi, 9 décembre 2017
https://es.wikipedia.org/wiki/Computaci%C3%B3n_cu%C3%A1ntica - Computation quantique
https://en.wikipedia.org/wiki/One-time_pad - OTP (masque jetable)

8 ANNEXES

Annexe 1 : Premier cas

	PABLO (16 ans)		Nom:? (27 ans)	
Numéro	COULEUR	BIT	COULEUR	BIT
1		0		0
2		1		1
3		1		1
4		0		0
5		0		1
6		1		1
7		1		1
8		1		1
9		0		0
10		0		0
11		1		1
12		0		0
13		1		1
14		1		1
15		0		0
16		1		1
17		0		0
18		1		1
19		1		1
20		0		0
21		1		1
22		1		1
23		1		1
24		0		0
25		1		0
26		0		0
27				
28				
29				
30				

	RR	RV	VR	VV
00	1	3	4	2
01	1	0	0	0
10	1	0	0	0
11	4	4	2	4

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
21	5	0,807692308	0,307692308

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,730769231	0,230769231	0,076923077

STRATÉGIE	
Numéro Dé pair --> 0	Numéro Dé impair -->1

Annexe 2 : Deuxième cas

	MARTA (15 ans)		VÍCTOR (15 ans)	
Numéro	COULEUR	BIT	COULEUR	BIT
1		1		0
2		1		0
3		1		1
4		0		0
5		0		1
6		0		1
7		1		0
8		0		0
9		1		1
10		0		0
11		1		0
12		1		1
13		1		0
14		1		1
15		1		0
16		0		1
17		0		1
18		0		0
19		1		0
20		0		1
21		1		1
22		1		0
23		1		1
24		0		1
25		1		1
26				
27				
28				
29				
30				

	RR	RV	VR	VV
00	0	0	4	0
01	0	0	1	5
10	8	0	0	0
11	2	5	0	0

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
17	8	0,68	0,18

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,6	0,1	0,08

STRATÉGIE	
Rouge --> 1	Vert --> 0

Annexe 3 : Troisième cas

	MARTA (15 ans)		PABLO (17 ans)	
Numéro	COULEUR	BIT	COULEUR	BIT
1		0		0
2		0		1
3		0		1
4		1		0
5		1		0
6		0		0
7		1		1
8		0		1
9		1		1
10		0		1
11		1		0
12		1		1
13		0		1
14		1		0
15		1		0
16		0		0
17		0		1
18		1		0
19		1		1
20		0		1
21		1		0
22		0		0
23		1		0
24		0		1
25		0		0
26				
27				
28				
29				
30				

	RR	RV	VR	VV
00	1	1	3	0
01	0	0	4	4
10	3	3	1	1
11	4	0	0	0

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
7	18	0,28	0,22

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,68	0,18	0,04

STRATÉGIE
Aléatoire

Annexe 4 : Quatrième cas

	Carla (7 ans)		Céline (7 ans)	
Numéro	COULEUR	BIT	COULEUR	BIT
1		1		1
2		0		0
3		0		1
4		1		0
5		1		1
6		0		0
7		0		1
8		1		0
9		1		1
10		0		0
11		0		1
12		1		0
13		1		1
14		0		0
15		0		1
16		1		0
17		1		1
18		0		0
19		0		1
20		1		0
21		1		1
22		0		0
23		0		1
24		0		0
25		1		1
26				
27				
28				
29				
30				

	RR	RV	VR	VV
00	1	3	1	2
01	4	1	1	0
10	2	0	3	0
11	0	2	3	2

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
19	6	0,76	0,26

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,72	0,22	0,04

STRATÉGIE
Aléatoire

Annexe 5 : Cinquième cas

	ROSA (18 ans)		PABLO (17 ans)	
Numéro	COULEUR	BIT	COULEUR	BIT
1		0		0
2		0		1
3		0		1
4		0		0
5		0		0
6		0		0
7		0		1
8		0		0
9		0		0
10		0		0
11		0		1
12		0		0
13		0		1
14		0		0
15		0		1
16		0		0
17		0		1
18		0		0
19		0		0
20		0		1
21		0		0
22		0		1
23		0		1
24		0		0
25		0		1
26				
27				
28				
29				
30				

	RR	RV	VR	VV
00	0	6	0	8
01	7	0	4	0
10	0	0	0	0
11	0	0	0	0

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
21	4	0,84	0,34

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,72	0,22	0,12

STRATÉGIE
Aléatoire

Annexe 6 : Sixième cas

	FERNANDO (56 ans)		IVÁN (16 ans)	
Numéro	COULEUR	BIT	COULEUR	BIT
1		1		0
2		0		1
3		0		0
4		1		1
5		0		0
6		0		1
7		1		0
8		0		1
9		0		0
10		1		1
11		0		0
12		0		1
13		1		0
14		0		1
15		0		0
16		1		1
17		0		0
18		0		1
19		1		0
20		0		1
21		0		0
22		1		1
23		0		0
24		0		1
25		1		0
26				
27				
28				
29				
30				

	RR	RV	VR	VV
00	5	1	2	0
01	3	3	2	0
10	2	1	2	0
11	2	1	1	0

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
10	15	0,4	0,1

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,52	0,02	0,08

STRATÉGIE
Aléatoire

Annexe 7 : Septième cas

	ANNA (17 ans)		ORIOL (17 ans)	
Numéro	COULEUR	BIT	COULEUR	BIT
1		0		0
2		1		1
3		1		1
4		0		0
5		1		1
6		0		0
7		1		1
8		1		0
9		0		0
10		1		1
11		1		0
12		1		1
13		1		0
14		1		1
15		0		0
16		0		1
17		1		1
18		0		1
19		0		1
20		0		0
21		0		1
22		1		0
23		0		1
24		1		0
25		0		1
26				
27				
28				
29				
30				

	RR	RV	VR	VV
00	2	1	1	2
01	3	1	0	2
10	3	1	1	0
11	1	2	2	3

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
17	8	0,68	0,18

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,64	0,14	0,04

STRATÉGIE
Aléatoire

Annexe 8 : Huitième cas

	FRANCISCO (66 ans)		JOSEFA (67 ans)	
Numéro	COULEUR	BIT	COULEUR	BIT
1		1		0
2		1		0
3		0		1
4		1		0
5		0		1
6		0		1
7		0		1
8		1		0
9		1		0
10		1		1
11		0		0
12		1		1
13		1		1
14		0		1
15		0		0
16		1		1
17		0		1
18		1		0
19		1		1
20		0		1
21		1		0
22		0		0
23		0		0
24		1		1
25		0		1
26				
27				
28				
29				
30				

	RR	RV	VR	VV
00	2	1	1	0
01	5	0	1	2
10	3	1	0	3
11	2	2	1	1

PARTIES GAGNÉES	PARTIES PERDUES	RATIO	VARIATION
14	11	0,56	0,06

SCORE MAX.	VAR. SCORE MAX.	DÉVIATION
0,52	0,02	0,04

STRATÉGIE
Aléatoire

COL·LECCIÓ JOVES INVESTIGADORS

Ajuntament de Rubí

RUBÍ
educació