Intrication quantique : mythe ou réalité ?

Zeno Toffano

AFSCET

Res-Systemica
Revue Française de Systémique
Fondée par Evelyne Andreewsky

Intrication quantique : mythe ou réalité ?

Zeno Toffano [a,b]

[a] *Professeur de Physique Quantique à CentraleSupélec, Dép. des Télécommunications,*
[b] *Laboratoire de Signaux et Systèmes (L2S, UMR8506) CNRS-CentraleSupelec-Université Paris Sud*
3 rue Joliot Curie, 91192 Gif-sur-Yvette cedex, France
zeno.toffano@centralesupelec.fr

31 janvier 2015[1]

Résumé.

On s'intéresse au concept d'intrication quantique en partant de l'histoire et des postulats de la Physique Quantique. Le débat sur l'intrication est ensuite présenté à travers l'argument EPR et le théorème de Bell. Les premières expériences montrant l'intrication sont discutées. Des applications technologiques de l'intrication quantique sont décrites: la téléportation quantique en cryptographie, l'ordinateur quantique et une application en Recherche d'Information. On analysera aussi l'évolution du concept d'intrication dans le cadre de l'émergence du nouveau domaine interdisciplinaire de l'information quantique ainsi que les discussions récentes autour du sujet.

Mots-clés : physique quantique, intrication quantique, inégalités de Bell, information quantique, non-localité, cryptographie quantique, codes stabilisateurs, ordinateur quantique, recherche d'information.

[1] Communication présentée lors de la réunion du groupe « Modelisation des Systemes Complexes – Afscet » le 16 juin 2014 au CNAM à Paris.

Quantum Entanglement: Myth or Reality?

Abstract

We are interested in the concept of quantum entanglement, starting from the history and postulates of Quantum Physics. The debate on entanglement is then introduced through the EPR argument and Bell's theorem and the first experiments showing entanglement are discussed. Technological applications of quantum entanglement are described: quantum teleportation in cryptography, quantum computer and an application in Information Retrieval. We also analyze the evolution of the concept of entanglement in the context of the emergence of new interdisciplinary field of quantum information and recent discussions around the subject.

Key Word : quantum physics, quantum entanglement, Bell inequalities, quantum information, nonlocality, quantum cryptography, stabilizer codes, quantum computing, information retrieval.

Introduction : bref historique de la physique quantique

a) Les débuts

Le 14 décembre 1900, pour expliquer les résultats expérimentaux sur le rayonnement du corps noir (le Soleil par exemple), Max Planck propose que la matière ne puisse émettre ou absorber des radiations que par multiple entier de la fréquence, la constante de proportionnalité étant h , baptisée depuis constante de Planck ($h = 6{,}626 \ldots . 10^{-34}$ Joule. sec).

Cinq ans plus tard, en 1905, Albert Einstein propose que les radiations elles-mêmes aient des propriétés « quantiques » et introduit le concept de photon. C'était la naissance de la physique quantique.

En 1913, Niels Bohr invente une description, certes incohérente, mais qui donne, sans coup férir, le spectre de toutes les raies d'émission de l'atome d'hydrogène. Cette description est étendue aux autres atomes par Arnold Sommerfeld. Niels Bohr énonce le principe de complémentarité concernant les propriétés des particules.

En 1924 Louis de Broglie postule qu'il existe aussi une longueur d'onde associée aux particules possédant une masse : les ondes de matière.

En 1925 Wolfgang Pauli découvre le principe d'exclusion pour deux électrons identiques occupant le même niveau quantique.

b) Non commutativité, relation d'incertitude et fonction d'onde

La même année Werner Heisenberg découvre la non-commutativité des quantités physiques de position x et d'impulsion p (vitesse multipliée par la masse d'une particule).

(1) $$[x, p] = x \cdot p - p \cdot x = ih/2\pi$$

Une des conséquences de la non-commutativité est la relation d'incertitude qui fixe une limite sur la connaissance (incertitude) simultanée de la position Δx et de l'impulsion Δp.

(2) $$\Delta x \cdot \Delta p \geq h/4\pi$$

L'algèbre linéaire est alors presque inconnue des physiciens, sauf de Max Born qui comprend que la relation ci-dessus est une relation entre matrices. Werner Heisenberg, Max Born et Pascual Jordan construisent une mécanique de quantités non commutatives où les quantités physiques sont des matrices. Partant de de la non-commutativité Pauli réussit le tour de force de calculer le spectre de l'atome d'hydrogène.

En 1926 Erwin Schrödinger trouve l'équation décrivant la fonction d'onde électronique $\psi(r, t)$. Max Born donne l'interprétation de la fonction d'onde en l'associant à la probabilité de trouver une particule dans une région donnée de l'espace. L'équation de Schrödinger est telle qu'une somme de fonctions d'onde est aussi une fonction d'onde. C'est cela qui est à la base des interférences quantiques d'électrons.

En 1928, Paul Dirac donne ce qui est la formulation actuelle de la mécanique quantique. En « notation de Dirac » l'état quantique, aussi appelé « Ket » s'écrit :

(3) $$|\psi>$$

Paul Dirac et Wolfgang Pauli, indépendamment, découvrent ensuite le spin.

c) Les postulats

A la fin de cette période la théorie est établie et stabilisée et conduit à l'énonciation des trois postulas fondamentaux dont le but est :

i) de décrire l'état d'un système quantique à un instant donnée.

ii) de prévoir le résultat d'une mesure d'une grandeur quantique (une «observable»).

iii) de décrire l'évolution dans le temps d'un système quantique.

Le postulat qui est le plus problématique pour l'interprétation est celui de la mesure qui stipule que si l'on effectue une mesure sur un état quantique le résultat ne peut être qu'une des valeurs associées (valeur propre) à l'observable de mesure, mais qu'on ne peut pas à priori savoir avec certitude laquelle. On ne peut connaître que les probabilités associées. En plus, juste après la mesure, il y a en général un changement d'état. Ce phénomène est appelé la réduction du paquet d'onde ou de la fonction d'onde. Si on effectue une deuxième mesure avec une grandeur qui est incompatible avec la première, c'est à dire qu'elle ne commute pas, alors on change à nouveau d'état. Ce mécanisme par « sauts » aléatoires, montre le caractère fondamentalement indéterministe des phénomènes quantiques.

d) « Sens » de la superposition quantique

On va discuter le phénomène de «superposition quantique» : observons l'image de la figure 1 que nous nommons « ma femme / ma belle-mère ».

Figure 1. Image « ma femme / ma belle-mère »

Que voyons-nous ? En fait après un certain temps on «observe» deux images… Par une impression « complexe », on pourrait être amené à penser que les deux personnes sont superposées sur l'image, c'est à dire, qu'elles existent simultanément au même endroit et au même moment. On peut concevoir la superposition au niveau de la pensée, mais ceci n'est plus vrai au niveau de la vision (mesure par l'œil); parce que l'image se «réduit» toujours dans l'une ou l'autre personne. Dans la réalité on ne peut pas vraiment définir une combinaison linéaire (superposition) du type :

(4) $$|\Psi> = a|ma\ femme> + b|ma\ belle\text{-}mère>$$

En mécanique quantique, l'opérateur de mesure se comporte de la même façon, il divise la fonction d'onde en ses composantes. Dans cet exemple, le «prisme» séparerait l'image qui est décrite par l'état (4) en ses composantes $|ma\ femme>$ et $|ma\ belle\text{-}mère>$.

La probabilité avec laquelle nous allons voir l'une ou l'autre image est fonction des coefficients de l'éq. (4). Plus spécifiquement la probabilité de voir la première image sera $P_1 = |a|^2$ et $P_2 = |b|^2$ pour la deuxième. En Physique Quantique on normalise la fonction d'onde (4) ce qui a comme conséquence que $|a|^2 + |b|^2 = 1$ de façon à être compatible avec le fait que la probabilité totale doit être égale à 1.

Nombreuses interprétations sont actuellement proposées pour rendre compte de la nature insolite de la physique quantique.

e) Principales interprétations de la physique quantique

Bien sûr le fait que les postulats ne soient pas démontrés a conduit à plusieurs interprétations de la physique quantique. Ni l'origine de la fonction d'onde, ni sa structure sous-jacente n'est décrite dans les lois de la mécanique quantique. En particulier, les mécanismes de superposition, d'intrication et de mesure ne sont pas clarifiés.

Sans rentrer dans le détail des différentes interprétations on peut citer celles qui sont les plus connues.

- L'interprétation de Copenhague est l'interprétation standard de la mécanique quantique formulée par Niels Bohr et Werner Heisenberg en incluant aussi l'interprétation probabiliste de la fonction d'onde initialement proposé par Max Born. L'interaction d'un observateur ou d'un appareil de mesure qui est externe au système quantique est la cause de la réduction de la fonction d'onde.

- La théorie des « univers multiples » de Hugh Everett est une interprétation de la physique quantique dans laquelle une fonction d'onde universelle obéit aux mêmes lois déterministes, réversibles à tout moment; en particulier il n'y a pas de réduction de la fonction d'onde associée à la mesure. A chaque évènement une nouvelle entité (univers) est créé. Dans cette interprétation la fonction d'onde a une réalité objective.

- L'interprétation en «histoires cohérentes» de la mécanique quantique est basée sur un critère qui permet à l'histoire d'un système d'être décrit de telle sorte que les probabilités pour chaque histoire obéissent à des règles de somme des probabilités classiques. Selon Robert Griffiths, son promoteur, il n'est pas nécessaire alors d'interpréter la physique quantique en termes de mesures.

- La théorie de Broglie-Bohm de la physique quantique part de la théorie développée par Louis de Broglie avec une extension proposée par David Bohm afin d'y inclure les mesures. Les particules, sont « pilotées » par la fonction d'onde qui obéit à l'équation de Schrödinger. La théorie est considérée comme une théorie à variables cachées mais qui prend en compte la non-localité et satisfait donc à l'inégalité de Bell (voir plus loin).

- Interprétation de la réduction objective de la fonction d'onde. La réduction se produit au hasard par localisation spontanée. Le mécanisme de la réduction n'est pas défini par la théorie quantique standard, qui doit être étendue si cette approche s'avère correcte. Dans cette ligne on peut citer l'interprétation de Roger Penrose qui conjecture que la réduction de la fonction d'onde pourrait être due à la gravité.

- L'idée principale derrière l'interprétation de la mécanique quantique relationnelle, développée par Carlo Rovelli, est que différents observateurs peuvent donner différents récits de la même série d'évènements. Par exemple, pour un observateur en un point donné dans le temps, un système pourrait être dans un seul état propre réduit, tandis que pour un autre observateur, il pourrait être dans une superposition de deux ou plusieurs états. Par conséquent, si la physique quantique doit être une théorie complète, elle doit faire valoir que la notion d'état ne décrit pas le système observé lui-même, mais la relation, ou la corrélation, entre le système et son observateur. Cette dernière interprétation est à mettre en parallèle avec les récents développements qui font un lien entre physique quantique et la théorie de l'information.

1) L'intrication quantique

Il s'agit d'un «état étrange» dans lequel deux particules (ou plus) sont si profondément liées qu'elles partagent la même existence, même à grande distance. Si une mesure est faite sur l'une, l'état de l'autre est changé aussi, instantanément, afin d'être compatible avec la mesure de la première.

a) L'argument EPR

Albert Einstein a appelé cette action-à-distance « fantasmagorique » (« spooky action at distance »). Dans un article de 1935 [1] Albert Einstein, Boris Podolsky et Nathan Rosen énoncent: «Si, sans pour autant perturber un système, nous pouvons prédire avec certitude, c'est à dire, avec une probabilité égale à l'unité, la valeur d'une grandeur physique, alors il existe un élément de la réalité physique correspondant à cette grandeur physique». C'est l'argument EPR qui conteste la possibilité de corrélation à distance entre particules en faisant l'hypothèse d'une interprétation manquante pouvant résoudre ce paradoxe. Selon l'argument EPR la physique quantique n'est pas une théorie complète et toute théorie physique satisfaisante pour être correcte doit être complète.

b) Théorème de Bell

Mercredi 4 Novembre 1964, un papier [2] par le physicien John Bell arrive à la revue Physics. Simplement intitulé «Sur le paradoxe Einstein Podolsky et Rosen», il montre que, dans le cadre de la physique quantique, le réglage d'un appareil de mesure peut

influer sur la lecture d'un autre instrument, même à grande distance - et que cela se produit instantanément. L'argument utilise le spin quantique, au lieu de la position et de l'impulsion, utilisées dans l'argument EPR, et montre que la corrélation entre deux spins est soumise à une inégalité qui peut être violée si les postulats de la physique quantique sont vrais. Cet article était passé un peu inaperçu dans les premières années après sa parution, en effet le phénomène d'intrication ne faisait pas partie des domaines enseignés dans les milieux académiques et était cantonné aux problèmes d'interprétation. À l'époque les physiciens étaient plus occupés à développer des modèles et des technologies, surtout nucléaires, et la physique quantique n'offrait un intérêt que si liée à ces développements, comme le souligne David Keiser dans un livre décrivant l'historique du sujet [3].

c) Expériences sur l'intrication

Mais John Clauser sous l'impulsion de David Bohm et Charles Townes (qui était son directeur de thèse) et avec l'aide de Stuart Jay Freedman réalisent une première expérience afin de vérifier le théorème de Bell en 1972 [4] à l'aide de photons polarisés. Ensuite en 1982 à Orsay sous le conseil de Bernard d'Espagnat [5] reprenant le schéma de John Clauser, Alain Aspect en collaboration avec Philippe Grangier et Gérard Roger, en utilisant des photons polarisés émis par une source de Calcium, font la preuve définitive de la violation de l'inégalité de Bell donc de l'intrication des particules [6]. Cette dernière expérience est basée sur la forme de l'inégalité de Bell dite de CHSH proposée par John Clauser, Michael Horne, Abner Shimony et Richard Holt en 1969 [7]. Elle consiste à effectuer deux mesures incompatibles conjointes parmi quatre sur deux particules. On désigne les mesures A et C sur la particule 1 et B et D sur la particule 2. Le schéma est illustré sur la figure 2. Chaque mesure ne peut donner que les résultats ± 1. L'inégalité de Bell s'exprime donc en combinant les quatre valeurs moyennes suivant l'ordre suivant :

(5) $$| < AB > \; - \; < AD > \; - \; < CB > \; - \; < CD > | \; \leq \; 2$$

On peut vérifier aisément que si l'on identifie les valeurs des résultats de mesure ± 1 séparément pour chaque particule il y'a $2^4 = 16$ possibilités de combinaisons. Si l'on remplace ces valeurs dans l'expression (5) qui prend alors la forme (6), on trouve toujours 2 (± 2 si on enlève la valeur absolue). Donc on ne viole jamais l'inégalité de Bell si les résultats de mesure sont attribués à l'une ou à l'autre particule.

(6) $$A, B, C, D = \pm 1 \qquad \left|(A - C)B \; - \; (A + C)D\right| \; = \; 2$$

Dans le cadre de mesures quantiques on évalue maintenant les valeurs moyennes des 4 mesures conjointes mais sans spécifier les mesures individuelles et on cherche à vérifier dans quel cas la combinaison (5) est supérieure à 2 ce qui correspond à la violation de l'inégalité de Bell.

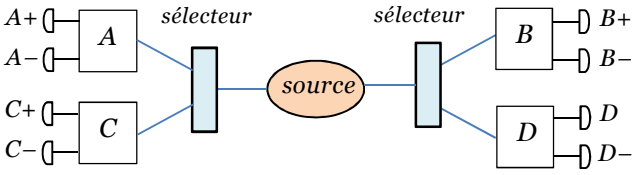

Figure 2. Configuration d'une expérience de Bell-CHSH avec deux photons polarisés.

Par le formalisme quantique on montre que l'inégalité est violée à l'aide d'un état quantique intriqué. Plus précisément on peut atteindre une valeur maximale de $2\sqrt{2}$, dite de Tsirelson, mise en évidence par Boris Tsirelson en 1980 [8]. Cette valeur maximale est atteinte avec l'état quantique appelé « singulet » qui correspond à une combinaison linéaire d'états de spin anticorrélés comme décrit par (7):

(7) $$|\psi>_s = \frac{1}{\sqrt{2}}(|-1,+1> - |+1,-1>)$$

2) L'information quantique

L'intrication est au cœur de ce domaine, en effet elle est considérée comme une «ressource» [9] pour les algorithmes pouvant diminuer leur complexité et aussi pour le codage de l'information dans des applications de cryptographie.

a) Le qubit

Le «qubit» constitue l'élément d'information élémentaire. Il permet, par le principe de superposition quantique, l'utilisation simultanée de deux états quantiques $|0>$ et $|1>$. Les valeurs sont exprimées suivant la notation informatique d'un bit {0,1}. Le qubit peut être représenté par un vecteur comme illustré sur la figure 3.

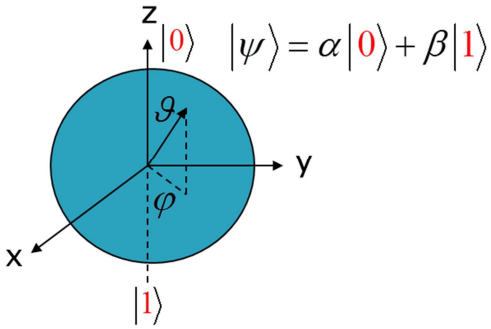

Figure 3. Représentation vectorielle d'un qubit dans l'espace de Hilbert.

Le vecteur évolue dans un espace vectoriel et en général les coefficients α et β sont des nombres complexes on appelle cet espace vectoriel l'espace de Hilbert d'après le mathématicien David Hilbert. Mais c'est en utilisant plusieurs qubits qu'on peut exploiter pleinement les propriétés quantiques notamment pour obtenir des états intriqués.

Afin d'effectuer des opérations sur les qubits on a imaginé des « portes quantiques » qui sont l'équivalent des portes logiques en électronique mais sont ici des opérateurs unitaires réversibles. On peut citer par exemple la porte CNOT agissant sur deux qubits et dont le fonctionnement est illustré à la figure 4. Grâce à la porte CNOT et à l'inversion on peut obtenir toutes les fonctions logiques et ainsi concevoir une « machine universelle ». En électronique classique la porte « NAND » (opération logique NON-ET) constitue une porte universelle.

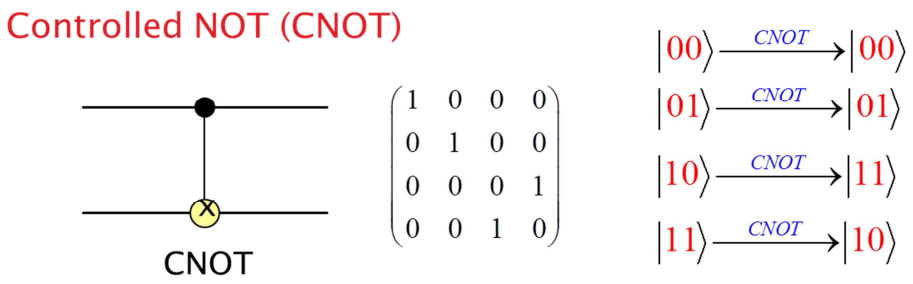

Figure 4. Porte quantique unitaire et réversible CNOT pour deux qubits.

Le fait que les portes quantiques soient unitaires offre un avantage conséquent par rapport aux portes classiques, il s'agit du fait qu'elles ne consomment aucune énergie ! Les portes quantiques ont le même nombre de sorties que d'entrées alors que les portes classiques à deux entrées possèdent une seule sortie. Cette réduction a comme conséquence de provoquer une augmentation d'entropie et donc un échauffement d'une unité d'énergie thermique kT à chaque opération, ce phénomène a été révélé par Rolf Landauer [10] en 1961. Bien que kT soit une énergie très faible, et négligeable par rapport à la consommation des portes logiques actuelles elle pourrait constituer dans le futur une limite ultime dans les performances des ordinateurs classiques.

b) Non clonage et non suppression

Que les opérateurs quantiques soient unitaires, présente deux autres conséquences inhabituelles. La première est que si on ne connait pas l'état d'un système quantique, alors on ne peut pas faire une copie exacte de celui-ci. Ceci est connu comme le théorème de non-clonage [11]. L'autre est que si un système quantique ne subit pas de réduction, on ne peut pas supprimer des informations dans ce système. Ceci est connu comme le théorème de non-suppression [12]. On montre que ces résultats sont directement liés au phénomène d'intrication quantique.

L'association de plusieurs qubits correspond à l'association physique de plusieurs états de particules différentes et ceci peut être décrit mathématiquement par l'opération de produit tensoriel.

c) Codes quantiques

Ces dernières années des évolutions importantes ont eu lieu et qui semblent prometteuses au niveau du codage de l'information quantique notamment pour corriger les erreurs lors d'un transfert d'états quantiques intriqués dans les systèmes cryptographiques.

Un grand travail théorique a porté à définir des nouvelles familles de codes comme par exemple les codes stabilisateurs [13], inventés par Daniel Gottesman, qui utilisent les algèbres des opérateurs de Pauli X, Y et Z qui représentent les observables de spin ½. Leur action sur un qubit est illustré à la figure 5.

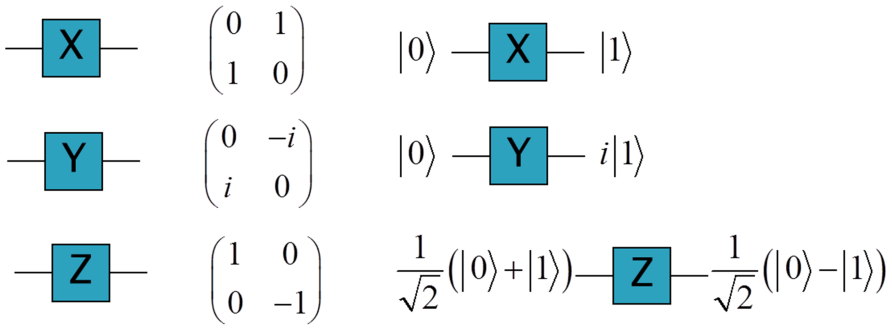

Figure 5. Opérateurs de Pauli *X*, *Y* et *Z* et leur action sur un qubit.

En combinant ces opérateurs par des produits tensoriels on forme un Groupe de Pauli G_n.

(8) $$G_n = \{E_1 \otimes E_2 \otimes \ldots \otimes E_n | E_i \in G_1\} \equiv \{I, X, Y, Z\}^n \mathrm{x} \{\pm 1, \pm \mathrm{i}\}$$

C'est en utilisant ces opérateurs pour coder l'information quantique que les algorithmes quantiques de correction d'erreurs sont capables de détecter si les qubits individuels ont été « surveillés » par des observateurs malveillants. Ces algorithmes quantiques utilisent d'une façon très fine les phénomènes de superposition quantique, d'intrication quantique et de mesure.

d) Jeux quantiques

Une des applications des opérateurs décrits plus haut est dans la théorie des jeux quantiques. Un jeu appelé carré magique ou jeu de Mermin a été proposé par David Mermin [14].

$I \otimes Z$	$Z \otimes I$	$Z \otimes Z$
$X \otimes I$	$I \otimes X$	$X \otimes X$
$X \otimes Z$	$Z \otimes X$	$Y \otimes Y$

Figure 6. Jeu quantique « boîte magique » avec observables quantiques correspondantes.

Un carré magique est constitué d'un tableau de $3\mathrm{x}3 = 9$ cases. Chaque case peut être remplie soit par un $+1$ ou un -1. Pour gagner à ce jeu il faut que le produit des entrées dans chaque ligne soit égal à -1, et le produit des entrées dans chaque colonne à $+1$. On peut montrer que ceci n'est pas possible dans tous les cas, plus précisément il existe des stratégies classiques qui permettent de gagner 8 fois sur 9.

Mais il s'avère qu'il existe une stratégie gagnante à tous les coups à l'aide de la mécanique quantique ! La démonstration effectuée par Padmanabhan Aravind fait appel à des états intriqués à 4 particules [15].

Dans le tableau de la figure 6 chaque case contient une observable quantique qui est le produit tensoriel de deux opérateurs de Pauli (et aussi l'opérateur identité I faisant aussi partie du groupe). Chacune de ces neuf observables, quand mesurée, donne soit la valeur $+1$ soit -1. Les trois observables dans chaque ligne et dans chaque colonne commutent entre elles. Il s'ensuit, d'après le second postulat, qu'elles peuvent être mesurées simultanément. On peut aussi montrer que dans chaque ligne et chaque colonne, chaque observable est égale au produit des deux autres, à l'exception de la troisième colonne, où chaque observable est le produit des deux autres changée de signe.

Supposons maintenant qu'on connaisse la valeur mesurée correspondante à chaque observable. Appelons ces valeurs suivant les trois lignes a, b, et c par: a_1, a_2, a_3, b_1, b_2, b_3, c_1, c_2 et c_3.

Puisque les observables dans chaque ligne et chaque colonne du tableau commutent, nous nous attendons que les valeurs correspondantes dans chaque ligne et dans chaque colonne satisfassent les mêmes règles de multiplication que les observables correspondantes.

En d'autres termes, nous nous attendons, par exemple, à ce que les équations suivantes soient vérifiées :

(9)
$$a_1a_2a_3 = +1 \qquad b_1b_2b_3 = +1 \qquad c_1c_2c_3 = +1$$
$$a_1b_1c_1 = +1 \qquad a_2b_2c_2 = +1 \qquad a_3b_3c_3 = -1$$

Mais il est facile de montrer que cela est impossible: si le produit des trois premières de ces six équations est égal à $+1$ (suivant la règle où chaque élément d'une ligne est le produit des deux autres on obtient donc un carré), le produit des trois dernières ne peut pas vérifier simultanément la condition.

Supposons, par exemple, que huit des neuf valeurs prédéfinies du tableau soient les suivantes: : $a_1 = +1$, $a_2 = +1$, $a_3 = +1$, $b_1 = +1$, $b_3 = -1$, $c_1 = +1$, $c_2 = +1$ et $c_3 = +1$. Si l'observable avec la valeur prédéfinie b_2 est mesurée conjointement avec les observables ayant les valeurs prédéfinies $b_1 = +1$ et $b_3 = -1$, alors $b_2 = -1$, puisque on doit avoir $b_1b_2b_3 = +1$. Mais si le même observable est mesurée avec les observables ayant les valeurs préexistantes $a_2 = +1$ et $c_2 = +1$, on obtient $b_2 = +1$, puisque on doit respecter aussi $a_2b_2c_2 = +1$, d'où l'impossibilité.

Ce que nous appelons le résultat d'une mesure d'une observable ne peut pas en général dépendre uniquement de l'observable et du système sur lequel la mesure est effectuée. Elle dépendra aussi des autres mesures qui sont effectuées conjointement avec la mesure de l'observable. La mesure est dite « contextuelle ».

e) Téléportation et cryptographie quantique

Dans une configuration typique de téléportation quantique les parties séparées dans l'espace effectuent des opérations, puis communiquent les résultats d'une manière classique. Les ressources classiques sont considérés comme réalistes et locales. L'intrication partagée est considérée comme une ressource supplémentaire qui n'est pas disponible sur les calculateurs classiques.

L'équipe de Nicolas Gisin [16] de l'université de Genève a réussi une première dans le domaine de la téléportation quantique: transporter l'état quantique d'un photon sur une distance de 25 km de fibre optique. Concrètement, l'expérience consiste à envoyer deux photons provenant d'une même source liés par l'intrication quantique sur deux supports différents. Le premier, A (Alice), part dans une fibre optique longue de 12,5 km tandis que le second B (Bob) est stocké dans un cristal. Un troisième photon C, ayant parcouru 12,5 km dans une autre fibre optique, rencontre A. Cette « rencontre » anéantit les deux photons A et C. Mais l'état de C se retrouve alors dans B à cause de l'intrication. Et cela fonctionne même à 25 km de distance ! Ce système permet d'élaborer des codes secrets: en observant l'un des photons intriqués, toute interception d'un message codé avec l'autre photon, sera aussitôt visible sur le premier… c'est la base de la cryptographie quantique.

Ce mécanisme de cryptographie est appelé BB84 [17] d'après son invention par Charles Bennett et Gilles Brassard en 1984. En pratique, Bob mesure et note les valeurs 0 ou 1 mesurées et obtient une suite de bits. Ensuite sur un canal classique, pouvant être espionné, Alice et Bob comparent la liste des bases utilisées pour les différents polariseurs et analyseurs : horizontal/vertical correspondant aux états $\{|0>, |1>\}$ d'angles 0° et 90° respectivement, et diagonaux $\{|-45°>, |+45°>\}$. Si les deux bases de Alice et Bob coïncident, le bit est choisi pour faire partie de la clé. Sinon il est détruit car inutilisable. Finalement ce mécanisme permet d'obtenir deux clés identiques chez Alice et chez Bob. La procédure est schématisée sur la fig. 7.

Polariseur d'Alice	Bit correspondant	Analyseur de Bob	Bit mesuré	Bit retenu ?
$\|0\rangle$	0	Horizontal	0	OUI
$\|0\rangle$	0	Diagonal	??	NON
$\|1\rangle$	1	Horizontal	1	OUI
$\|1\rangle$	1	Diagonal	??	NON
$\|-45°\rangle$	0	Horizontal	??	NON
$\|-45°\rangle$	0	Diagonal	0	OUI
$\|+45°\rangle$	1	Horizontal	??	NON
$\|+45°\rangle$	1	Diagonal	1	OUI

Figure 7. Table de vérité et principe du protocole de cryptographie BB84 avec photons polarisés intriqués mesurés à l'aide de deux bases de polarisation.

3) Vers l’ordinateur quantique

Le grand physicien américain Richard Feynman, a imaginé en 1982 [18] une machine capable de « simuler la physique » en tirant avantage des propriétés quantiques. Son intérêt: s'affranchir des limites mécaniques de la gravure qui restreignent la miniaturisation et la performance des puces telles qu'on les connaît actuellement.

C'est dans la première moitié des années 1990 que deux résultats théoriques majeurs ont donné le véritable signal de départ aux recherches aujourd'hui foisonnantes sur l'information quantique et son traitement: l'algorithme quantique de Peter Shor [19] pour la factorisation des entiers, et l'algorithme quantique de Lov Grover [20] pour la recherche d'un élément dans une base de données non ordonnée.

L’intérêt technologique pourra vraiment être apprécié le jour où l’on disposera d’une machine, l’ordinateur quantique, pouvant travailler avec des états formés d’un nombre important de qubits.

a) Premières réalisation expérimentales

Alors que nous sommes encore à des nombreuses années de la construction d'ordinateurs quantiques à grande échelle, beaucoup de progrès ont été réalisés. Par exemple les circuits supraconducteurs ont été utilisés pour mettre en œuvre des algorithmes quantiques. Aussi des qubits réalisés à l’aide de spins nucléaires et des photons uniques ont été utilisés pour démontrer certaines formes simples de correction d'erreur quantique et aussi pour réaliser la simulation quantique.

Mais les progrès les plus impressionnants ont été réalisés avec les systèmes à ions piégés. Ces systèmes ont été utilisés pour mettre en œuvre à l’aide de deux et trois qubits de nombreux algorithmes, par exemple l'algorithme de recherche quantique et la transformée de Fourier quantique. Les ions piégés ont également été utilisés pour démontrer les prémices d’une communication quantique, y compris la correction d'erreur quantique et la téléportation quantique. Le prix Nobel a été décerné en 2012 à Serge Haroche pour ces travaux.

b) Nouvelles méthodes de calcul quantique

Des progrès importants ont été réalisés dans la compréhension des ressources physiques nécessaires pour le calcul quantique.

Peut-être la percée la plus étonnante a été la découverte démontrant que le calcul quantique peut être effectué par la seule mesure. Pendant de nombreuses années, on croyait que la dynamique unitaire de superposition, préservant la cohérence quantique, était une partie essentielle pour la puissance des ordinateurs quantiques. Cette idée a été invalidée montrant que le calcul quantique pouvait être réalisé sans dynamique unitaire. La seule ressource nécessaire devient alors la mémoire quantique, c’est à dire, la capacité de stocker de l'information quantique.

Ceci est remarquable: si on dispose d’un état quantique donné, le calcul quantique peut s’effectuer simplement en « observant » les qubits individuels par des moyens appropriés.

c) La simulation quantique

Un troisième domaine de progrès a été dans la simulation des systèmes quantiques. L'article pionnier de Richard Feynman en 1982 [18] sur l'informatique quantique a été motivé en partie par l'observation que les systèmes quantiques semblent souvent être difficiles à simuler sur les ordinateurs classiques.

Bien sûr, à l'époque il n'y avait qu'une compréhension limitée de la façon de simuler des systèmes quantiques sur les ordinateurs classiques. Mais dans les années 1990 et, surtout, dans les années 2000, on a beaucoup progressé afin de connaître quels systèmes quantiques sont faciles à simuler. Par exemple, il est connu depuis longtemps que les systèmes quantiques basés sur certains composants optiques linéaires peuvent être facilement simulés classiquement. On a découvert que l'addition de deux éléments optiques simples, sources de photons uniques et des photodétecteurs, permettent de donner à l'optique linéaire la pleine puissance du calcul quantique.

d) Les canaux de communication quantique

Un quatrième domaine de progrès a été dans la compréhension approfondie des canaux de communication quantique. Une théorie a été développée portant sur la façon dont les états intriqués peuvent faciliter la communication classique sur des canaux quantiques. Beaucoup de protocoles quantiques de communication ont été développés. Mais, malgré les progrès, il reste beaucoup de phénomènes non encore élucidés. Il a été découvert récemment que deux canaux quantiques, chacun avec une capacité quantique nulle, pouvaient acquérir une capacité quantique positive lorsqu'utilisés ensemble; le résultat analogue, avec des capacités classiques sur des voies de communication classiques, est impossible.

e) L'ordinateur quantique D-Wave

Selon la société canadienne D-Wawe Systems qui commercialise les premières machines prétendues quantiques, un ordinateur de 500 qubits pourrait effectuer en une fraction de seconde plus d'opérations qu'il y a d'atomes dans tout l'univers !

Ces ordinateurs fonctionnent à base de circuits électriques supraconducteurs refroidis à quelques degrés au-dessus du zéro absolu (−273°C). Google en association avec la NASA on fait l'acquisition d'une telle machine. Il faut souligner que cette machine n'est pas un ordinateur mais bien un calculateur quantique, qui ne peut pas être programmé pour effectuer n'importe quel algorithme. Il ne peut être utilisé que pour mettre en œuvre les calculs dits de « recuit simulé », des algorithmes d'optimisation utilisés par exemple pour la construction de circuits intégrés, le traitement des images et la résolution de problèmes de transports optimaux. Cela revient à trouver le minimum d'une fonction qui peut être associé à l'énergie d'un système physique.

La polémique est vive autour de cette machine et les avis dans la communauté scientifique sont partagés pour savoir si la machine D-Wave peut vraiment être qualifiée d'ordinateur quantique [21].

4) Applications en dehors de la Physique

a) « Quantum Interaction » et Recherche d'Information

Des communautés de chercheurs aux quatre coins du monde s'appliquent à essayer d'appliquer des principes de la théorie quantique à des domaines complètement éloignés de la physique, comme l'économie, l'étude du comportement humain, ou bien la modélisation sémantique. Ces efforts on fait émerger un nouveau domaine nommé « Quantum Interaction » [22].

TEXT example with a window spanning on 3 words ($l = 3$) : "THE COLOUR ORANGE TAKES ITS NAME FROM THE ORANGE FRUIT"

THE	16	3	5	1	1	2	3	2
COLOUR	3	8	3	2	1	0	0	0
ORANGE	5	3	16	3	2	2	2	3
TAKES	1	2	3	8	3	2	1	0
ITS	1	1	2	3	8	3	2	0
NAME	2	0	2	2	3	8	3	0
FROM	3	0	2	1	2	3	8	1
FRUIT	2	0	3	0	0	0	1	8

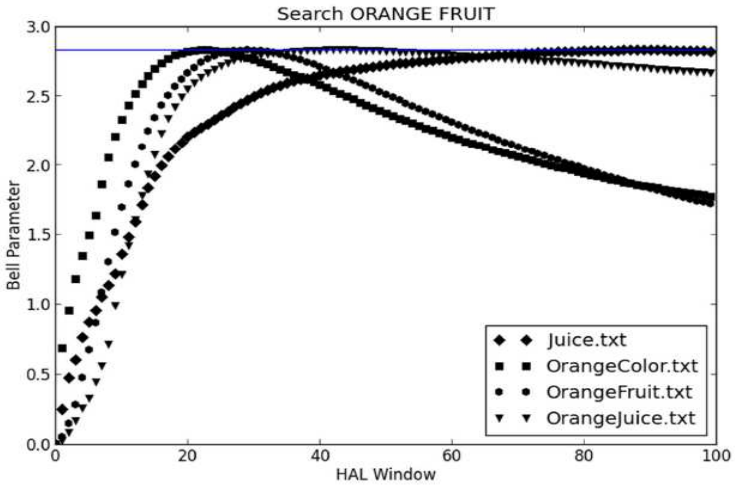

Figure 8. Cooccurrence des mots selon l'algorithme HAL. Test de corrélation intriquée.

Au travers de l'inégalité de Bell, nous nous sommes interrogés comment améliorer les algorithmes de recherche dans des listes de mots, comme des pages internet par exemple. Réussir à implémenter des algorithmes donnant des résultats pertinents lors de recherches sémantiques est devenu aujourd'hui un défi non seulement scientifique mais aussi économique.

Nous avons utilisé les méthodes LSA (« Latent Semantic Analysis ») à travers l'algorithme HAL (« Hyperspace Analogue to Language » [23]) donnant une représentation latente des co-occurrences entre mots dans un document. Des premiers résultats sur les corrélations entre deux mots montrent une mesure de pertinence qui s'apparente à l'intrication quantique [24].

b) Les boîtes « non-locales »

Depuis l'énoncé du théorème de Bell et la mise en évidence expérimentale de l'intrication quantique les débats autour de cette question n'ont pas cessé. La pierre d'achoppement se situe toujours à propos de la non-localité et du défaut de réalisme de la Physique Quantique.

Pour ne pas éclaircir la situation on s'est aperçu assez tôt que l'inégalité de Bell sous la forme CHSH donnée par l'équation (5) possède une autre borne au-delà de 2. Cette borne, dite de Tsirelson [8], limite, en cas de violation par un système quantique, la valeur appelée paramètre de Bell, au chiffre maximum de $2\sqrt{2} = 2{,}8284\ldots$. Au-delà de ce chiffre le paramètre de Bell, qui peut en principe d'après l'expression (5) aller jusqu'à la valeur 4, se trouve dans une zone qu'on qualifie de «supra-quantique».

Il n'y a pas vraiment de théorie pour les objets se trouvant dans cette zone, on les qualifie de « no-signalling - non-local boxes » une traduction serait : boîtes non-communicantes et non-locales.

Une réalisation inattendue est obtenue à partir d'une relation logique entre variables de sortie (a, b) et d'entrée (x, y) dans une « boîte PR ». Ce schéma a été trouvé par Sandu Popescu et Daniel Rohrlich en 1994 [25]. Dans une boîte PR on mesure les variables de sortie (a, b). Elles sont corrélées aux variables d'entrée (x, y) par la contrainte logique suivante :

(10) $$a \oplus b \ = \ x \wedge y$$

où $\oplus$ représente l'opérateur logique « OU EXCLUSIF » qui vaut 1 quand les entrées sont différentes et 0 sinon et $\wedge$ l'opérateur logique « ET » qui vaut 1 quand les deux entrées sont toutes deux égales à 1 et 0 sinon.

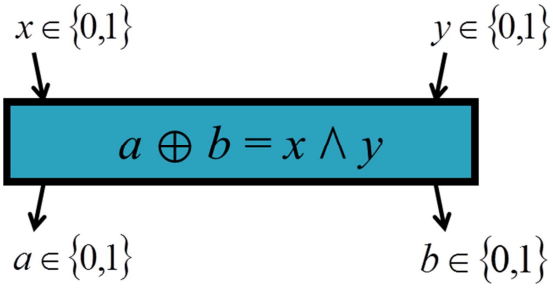

Figure 9. Boîte non-locale PR.

On peut écrire une inégalité de type Bell-CHSH pour 4 « expériences » sur la boîte PR correspondantes aux 4 différentes combinaisons du couple d'entrée (x, y) et en prenant comme « mesure », la valeur conjointe C_{xy} des variables dichotomiques de sortie A et B de valeur ± 1 (voir (11)). Ceci donne, en utilisant les probabilités conditionnelles par la contrainte logique (10) et en considérant les différents possibilités de sortie de a et b :

(11) $C_{xy} = \sum_{a,b} \mathrm{P}(a, b | a \oplus b = x \wedge y)\, A(a).B(b)$ avec $A(a) = 2a - 1$ et $B(b) = 2b - 1$

Par exemple si l'on fixe l'entrée $(x, y) = (0,0)$ alors à cause de la contrainte logique (10) on doit avoir $a = b$, c'est-à-dire pour (a, b) soit $(0,0)$ soit $(1,1)$, donc le produit $AB = (2a - 1)(2b - 1) = +1$. Les probabilités associées aux quatre résultats possibles pour la sortie (a, b) sont fixées puisque les cas a différent de b, soit $(0,1)$ soit $(1,0)$, est impossible ici, et les deux autres cas sont équiprobables avec une probabilité de ½.

Ceci donne pour $C_{00} = (½ + ½)(+1) = +1$. On obtient par le même raisonnement : $C_{01} = C_{10} = C_{00} = +1$. Le seul terme différent est C_{11} qui par la contrainte logique (10) impose maintenant a différent de b, ce qui donne $C_{11} = -1$.

Si on calcule l'inégalité de Bell (5) dans ce cas particulier on obtient :

(11) $$C_{00} + C_{01} + C_{10} - C_{11} = +4$$

L'inégalité de Bell donne ici une valeur de +4, qui est la valeur maximale possible bien au-delà du cas quantique qui est $2\sqrt{2}$!

5) Considérations et discussions récentes sur la notion d'intrication

Traditionnellement, l'intrication a été considérée comme une bizarrerie d'objets microscopiques défiant une explication à partir du sens commun. Depuis peu, cependant, l'intrication est reconnue pour être omniprésente et robuste même à des températures plus élevées, comme le souligne Vlatko Vedral [26]. Avec la prise de conscience que l'intrication peut se produire dans les systèmes macroscopiques, et avec le développement d'expériences visant à exploiter ce fait, de nouveaux outils s'avèrent nécessaires pour définir et quantifier l'intrication, au-delà du cadre microscopique original. L'intrication peut être mise en évidence par des observables macroscopiques spécifiques qu'on appelle «entanglement witnesses» (« témoins d'intrication »).

Il est clair que la notion même d'intrication est affectée par une certaine ambiguïté puisqu'elle est liée à la structure multipartite sélectionné pour l'état quantique. C'est la thèse que soutient Paolo Zanardi [27]. Les états quantiques qui sont considérés comme intriqués par rapport à une partition peuvent être considérés comme séparés par rapport à une autre partition. Inversement, les états quantiques d'un système considéré comme élémentaire peuvent être intriqués quand ce même système possède une structure multipartite. Dans ce cas, on est dans la situation quelque peu paradoxale d'un état intriqué apparemment sans intrication !

L'intrication est considérée comme la règle de l'étrangeté du monde quantique, mais un phénomène nouveau semble pouvoir nous offrir ses avantages mais avec moins de retentissement, comme le souligne un article récent [28]. Les chercheurs ont donné à ce phénomène le nom de discorde quantique (« quantum discord »), tout un programme !

Conclusion

Depuis 1964 les inégalités de Bell et le phénomène d'intrication ont fasciné de nombreux scientifiques à travers le monde. Un récit historique intéressant et amusant est l'ouvrage « How the Hippies Saved Physics » par David Kaiser [3] qui a reçu le prix du meilleur livre de vulgarisation en physique par la société Physics World en 2012. Beaucoup de débats ont eu lieu autour du comportement classique et non classique, de l'intrication, des propriétés locales et non-locales, de la contextualité, des boîtes non-locales et des théories supra-quantiques.

Depuis les premières expériences démontrant la violation de l'inégalité de Bell beaucoup d'autres systèmes présentant l'intrication ont été réalisés. Par exemple avec des spins grâce aux techniques de Résonance Magnétique Nucléaire (RMN) ou avec des méta-atomes froids de Rydberg ou encore à l'aide de matériaux supraconducteurs tout ceci nous rapproche de la réalisation pratique d'un ordinateur quantique. Un nouveau domaine scientifique a vu le jour: l'information quantique, l'intrication étant au cœur de ce domaine.

Au niveau de l'interprétation il n'est pas certain qu'on se soit libérés de l'aura mystérieuse entourant ce phénomène. Des études plus critiques faisant appel à l'épistémologie ou à la philosophie s'avèrent peut-être nécessaires par exemple autour de la notion de non-localité [29].

On peut citer Werner Heisenberg en 1956: « La science de la nature ne décrit ni explique simplement la nature; elle est une partie du rapport entre la nature et nous-mêmes; elle décrit la nature en tant qu'exposée à notre méthode d'interrogation ».

Quelle attitude philosophique adopter ? Ce pourrait être une attitude spéculative afin de formuler en langage ordinaire l'image métaphysique du monde qui rende raison de nos pratiques ordinaires et de la forme de nos théories scientifiques. Ou bien une attitude plus critique comme exprimée par le philosophe Ludwig Wittgenstein : « la philosophie des sciences est une lutte contre la fascination que d'anciens modes de théorisation exercent sur nous. Par exemple le mystère des corrélations EPR pourrait être lié à une fascination pour le mode classique de théorisation qui revient à connecter les phénomènes spatio-temporels par le biais de processus eux-mêmes spatio-temporels ».

De plus en plus d'interprétations font appel à d'autres disciplines en dehors de la physique comme par exemple la théorie de l'information. John Archibald Wheeler en 1988 [30] a été le premier à formuler un programme consistant à dériver le formalisme quantique à partir de principes informationnels. Les termes de la relation cognitive avec la nature pourraient être redéfinis en termes d'information.

Réferences

[1] A. Einstein, B. Podolsky et N. Rosen. "Can quantum-mechanical description of physical reality be considered complete?" Phys. Rev. 47 777, 1935.

[2] J.S. Bell. "On the Einstein Podolsky Rosen Paradox". Physics 1 (3): 195–200, 1964.

[3] D. Kaiser. How the Hippies saved Physics, W.W. Norton & Company, New York, 2012.

[4] S. J. Freedman et J. F. Clauser. “Experimental test of local hidden-variable theories”, Phys. Rev. Lett. 28, 938, 1972.

[5] B. D'Espagnat, “The Quantum Theory and Reality”, Scientific American, pp. 158-181, Nov. 1979.

[6] A. Aspect, P. Grangier et G. Roger. “Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities”, Phys. Rev. Lett. 49, 91, 1982.

[7] J.F. Clauser, M.A. Horne, A. Shimony et R.A. Holt. “Proposed experiment to test local hidden-variable theories”, Phys. Rev. Lett. 23 (15): 880–4, 1969

[8] B.S. Tsirelson. “Quantum generalizations of Bell's inequality”, Lett. Math. Phys. 4:2, 93-100, 1980.

[9] M. A. Nielsen et I. L. Chuang. Quantum Computation and Quantum Information, Cambridge University Press, New York, 2000.

[10] R. Landauer. “Irreversibility and heat generation in the computing process”, IBM Journal of Research and Development, vol. 5, pp. 183-191, 1961.

[11] W. K. Wootters. and W. H. Zurek. “A single quantum cannot be cloned”, Nature, Vol. 299, pp. 802-803, 1982,

[12] A. K. Pati et S. L. .Braunstein. “Impossibility of deleting an unknown quantum state”, Nature, Vol. 404, pp. 164-165, 2000.

[13] D. Gottesman, “Class of quantum error-correcting codes saturating the quantum Hamming bound”, Phys. Rev. A 54, 1862-1868, 1996.

[14] N. D. Mermin. “Simple unified form for the major no-hidden-variables theorems”, Phys. Rev. Lett. 65, pp. 3373-3376, 1990.

[15] P. K. Aravind. “A simple demonstration of Bell's theorem involving two observers and no probabilities or inequalities”, arXiv:quant-ph/0206070, 2002.

[16] N. Gisin. L'Impensable Hasard: Non-localité, téléportation et autres merveilles quantiques, Odile Jacob, 2012.

[17] C. H. Bennett et G. Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175, p. 8, 1984.

[18] R. P. Feynman. “Simulating physics with Computers”, International Journal of Theoretical Physics, Vol. 21, Issue 6-7, pp 467-488, 1982.

[19] P. W. Shor. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM J. Computing 26, pp. 1484-1509, 1997.

[20] L. K. Grover. “A fast quantum mechanical algorithm for database search”, Proceedings, 28th Annual ACM Symp. on the Theory of Computing, p. 212, 1996.

[21] P. Ball. “La mystérieuse boîte noire de D-Wave”, La Recherche, n°485, pp. 28, mars 2014.

[22] M. Buchanan. “Quantum minds: Why we think like quarks”, New Scientist, 2828, pp. 34-37, Sept. 2011.

[23] K. Lund et C. Burgess. “Producing high-dimensional semantic spaces from lexical co-occurrence. Behavior”, Research Methods Instruments and Computers 28, pp. 203-208, 1996.

[24] J. Barros, Z. Toffano, Y. Meguebli et B-L. Doan. “Contextual Query Using Bell Tests”, Quantum Interaction Lecture Notes in Computer Science 2014, pp 110-121, 2014.

[25] S. Popescu, D. Rohrlich. “Quantum nonlocality as an axiom”, Foundations of Physics, 24, p.379-385, 1994.

[26] V. Vedral. “Quantifying entanglement in macroscopic systems”, Nature, Vol 453, pp. 1004-1007, 2008.

[27] P. Zanardi. “Virtual Quantum Subsystems”, Phys. Rev. Lett., Vol 87, N° 7, 077901-1, 2001.

[28] M. Brooks. “Quantum control: How weird do you want it?”, New Scientist 2986 , pp. 34-37, Sept. 2014.

[29] R. Nadeau et M. Kafatos. The Non-Local Universe: The New Physics and Matters of the Mind, Oxford Univesity Press, 2001.

[30] J. A. Wheeler. “Information, Physics, Quantum: The Search for Links”, Proc. 3rd Int. Symp. Foundations of Quantum Mechanics, Tokyo, pp.354-368, 1989.

Zeno Toffano est titulaire d’un diplôme d’études approfondies (master) en physique des solides de l’université ParisSud à Orsay et d’un diplôme de spécialisation de l’École Supérieure d’Electricité (Supélec). Il est titulaire d’un doctorat en Physique effectué au CEA de Saclay en 1985 dans le domaine de l’étude à basse température par RMN de supraconducteurs organiques. Il est depuis 1987 à Supélec et effectue ses recherches dans le domaine des télécommunications optiques. Il est titulaire de l’habilitation à diriger des recherches (2004) et est depuis professeur. Il enseigne la physique quantique et l’optoélectronique. Il fait également partie du Laboratoire de Signaux et Systèmes L2S, groupe théorie de l’information, qui s’intègre dans la nouvelle université Paris-Saclay.