Table des matières

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DE JIJEL
FACULTE DES SCIENCES
DEPARTEMENT DE PHYSIQUE

N° d'ordre :

Série :

MEMOIRE

présenté pour obtenir le diplôme de

MAGISTER

Spécialité : Physique

Option : Physique Théorique

par

Saoudel Nadia

THEME

Introduction à L'information Quantique

Soutenu le : 16 /12 /2008

Devant le Jury :

Président :	Kh. Nouicer	Prof.	Univ. Jijel
Rapporteur :	T. Boudjedaa	Prof.	Univ. Jijel
Examinateurs :	L. Chetouani	Prof.	Univ. Mentouri
	A. Lecheheb	Prof.	Univ. Mentouri
	A. Boutaghou	MC	Univ. Jijel

Remerciements

Tout mes remerciements vont tout premièrement à Dieu tout puissant pour la volonté la santé et la patience qu'il m'a données pour terminer ce mémoire

Je tiens à remercier mon encadreur Mr. T. Boudjedaa, Professeur à l'université de Jijel, pour m'avoir confié ce sujet et pour l'aide et le temps et la disponibilité qu'il a bien voulu me consacrer.

Mes remerciements vont ensuite au Jury de ma thèse, Mr. Kh. Nouicer , Professeur à l'université de Jijel pour l'honneur qu'il m'a fait en acceptant de présider le jury, et les examinateurs : Mr. L. Chetouani *, professeur à l'université de Mentouri Constantine , Mr.* A. Lecheheb*, Professeur à l'université Mentouri de Constantine, et Mr. A.*Boutaghou *. Maître de conférences à l'université de Jijel , qui ont bien accepté de juger ce travail.*

Je voudrais exprimer ma profonde gratitude envers tous les enseignants de la post graduation de physique théorique. En particulier Mrs : A. Bounames, Professeurs à l'université de Jijel,A. F. Benamira, professeur à l'université de Mentouri Constantin , Mr. M. Maameche Professeurs à l'université de Sétif , Mr.M.Merad, Professeurs à l'université de Oum El Boiguie.

Je remercie, encore tous mes collègues de la promotion 2004/2005, et ceux de la promotion qui nous ont précèdé 2003/2004, et 2002/2003 .

Enfin, j'adresse mes plus sincères remerciements à ma famille et en particulier ma mère, et mon père qui m'ont toujours soutenue et encouragée au cours de la réalisation de ce mémoire.

Nadia

Chapitre 1

Introduction générale

La mécanique quantique a révolutionné notre vie par son développement technologique en maitrisant la matière dans ses états microscopiques et continue encore à nous révolutionner par ses concepts en s'immisçant encore plus conceptuellement dans nos créations de tous les jours. De nos jours, on s'intéresse de plus en plus à son développement donnant naissance à des nouvelles disciplines de la science. Les physiciens expérimentent à outrance ses recoins et ses paradoxes pour en tirer profit pour une nouvelle phase de ses applications dite : Information quantique.

L'information quantique exploite essentiellement les effets de superposition et de mesure dans les domaines tels que l'informatique et la cryptographie. La superposition et la mesure, deux canaux complémentaires de la mécanique quantique, l'un enrichissant l'évolution et l'autre la limitant. Cette manière de voir la distingue énormément de la mécanique classique qui se définit complètement déterministe. Dans ce dernier cas l'état du système physique à n'importe quel instant est complètement déterminé par la donnée initiale et en plus la mesure permet de déterminer cette dernière d'une manière parfaite. On dit que la mesure peut être idéalisée en la négligeant ou en la compensant. Cette vision de voir les choses interdit une superposition possible des états et ne l'autorise que dans le cas des phénomènes ondulatoires se propageant dans l'espace-temps. Par contre en mécanique quantique on admet et on généralise ce principe de superposition à tous les systèmes physiques mais on confère à la mesure un statut particulier qui délimite l'effet de cette superposition. La mécanique quantique par son étrangeté et son

mystère a permis à la physique une avancée irréprochable qui s'est confirmée en sondant la matière dans ses états microscopiques d'une manière extraordinaire. Certes la mécanique classique permettait aussi de sonder la nature convenablement mais s'est butée au problème d'interaction de la lumière avec la matière au niveau microscopique : pour ne citer que le rayonnement du corps noir et le spectre des atomes. Les bases de la nouvelle mécanique ont permis un sondage presque parfait de ce phénomène d'interaction matière-rayonnement et une technologie nouvelle s'est bâtie dessus. Un développement proliférant en informatique et en télécommunication a vu le jour. Par ailleurs, depuis son avènement une opposition à ces idées nouvelles s'est formée essayant de remettre en cause les principes de bases de cette mécanique quantique. Plusieurs de ses fondateurs tels Einstein, de Broglie et Schrödinger ne l'ont pas acceptée comme théorie complète et ont essayé de construire des modèles physiques montrant son incomplétude. Deux exemples très connus sont le paradoxe EPR et le chat de Schrödinger. Ces derniers exploitent le principe de superposition dans sa version la plus profonde : les états intriqués (non séparables). Ces modèles suppose alors l'existence de variables cachées dont la mécanique quantique ne tient pas compte. Les inégalités de Bell, dues à J. S. Bell, sont les relations auxquelles obéissent les mesures sur des états intriqués dans l'hypothèse d'une théorie déterministe à variables cachées locales (complète selon l'argument EPR). L'expérience Alain Aspect a démontré que les inégalités de Bell sont violées, et elle nous force à renoncer encore une fois à une physique causale et locale au même temps. J. S. Bell plaide alors pour une physique déterministe non locale à l'image de la mécanique déterministe de Bohm. Le statut de la mécanique quantique reste souverain et les physiciens de la nouvelle génération ont préféré mener encore ce débat philosophique dans une ambiance plus défiante qui est celui des expérimentations. On assiste maintenant à une nouvelle ère de technologie de dimension nanométrique permettant par sa petitesse infime de s'assurer encore plus de la validité des concepts quantiques et de nous mener à des exploits inouïs telle que la téléportation quantique. En plus, les scientifiques ont commencé à imaginer les retombées de ces réalisations miniaturisées de la mécanique quantique et on voit naitre des sciences nouvelles comme l'informatique quantique et la cryptographie quantique permettant un pouvoir sans précédent en comparaison avec ce qui a été fait auparavant. L'objectif de ce mémoire est une introduction à l'information quantique par ces principes de base et de ces développements florissants et il est de nature pédagogique.

Dans le deuxième chapitre, nous présentons les concepts fondamentaux de la mécanique quantique. Nous donnons quelques définitions, ses développements historiques et son écriture mathématique. La mécanique quantique est présentée comme un système complet de postulats et les notions d'opérations quantiques et de mesure sont introduites. Nous évoquons aussi le grand débat de la mécanique quantique. Nous présentons le contenu d'un article connu sous le nom du Paradoxe EPR, ce dernier est suivi d'une réponse à base du principe de complémentarité donné par Bohr. La causalité et en conséquence la localité "rigide" est présentée suivant le schéma de Bohm et enfin les inégalités de Bell sont déduites. Le troisième chapitre introduit le calcul quantique et ses algorithmes quantiques via les opérations quantiques sur les qubits et les portes logiques quantiques. La généralisation de la transformée de Fourier est présentée. Des exemples sur la téléportation sont évoqués. Nous présenterons l'algorithme de Deutsch et de Schor. Nous examinons également la réalisation physique du qubit. par ailleurs, on présente une introduction de l'information quantique en présentant quelques notions sur l'entropie et la cryptographie quantique.À la fin on va donner une conclusion générale.

Chapitre 2

Fondements de la mécanique quantique

2.1 Evolution des idées quantiques

La physique recherche les lois de la nature ; quelle nature ; celle de la matière inerte, faite d'après la théorie atomiste, des atomes qui sont la brique de ce monde macroscopique. Mais aussi cherche à les exprimer au moyen de lois plus simples, celles des constituants de ces atomes qui sont les particules : électrons, protons, neutrons etc. Ce schéma atomique s'étend formidablement aux confins de la matière mais bien sûr inextricablement quand on s'enfonce plus loin encore. Faute de prolonger et manipuler aussi, ce schéma a montré ses limites. Sans nul doute les atomes "existent" et ont apporté leur fruit à l'humanité. Sans rentrer dans les détails des méandres qui ont poussé les physiciens modernes à changer leurs positions et leurs stratégies d'exploration de recherche de ces lois, nous admettons qu'une théorie quantique est bien fondée depuis au moins un siècle. Avant d'exposer son axiomatique et ses fondements rappelons d'abord le contexte dans lequel la physique d'avant les idées de la quantique, dite classique, s'est développée.

La physique classique commença avec Galilée qui remarqua que les lois de la physique sont invariantes par rapport à une classe de référentiels dits inertiels ou Galiléens. Au début du XVII^{e}siècle, les savants se référaient aux théories d'Aristote et leurs prolongements pour expliquer les lois du mouvement. Galilée a effectué plusieurs expériences physiques mettant à défaut ces anciennes théories et se rallia à son prédécesseur Copernic. Il ouvra alors une voie nouvelle pour la science en basant les lois du mouvement sur la notion relative de mesure dans l'espace

et le temps. Il a ainsi proclamé que tout processus physique s'effectue dans l'espace-temps. Ce dernier est un concept introduit insidieusement dans notre raisonnement pour nous permettre de comprendre le déroulement de ce processus. Insidieusement, parce que bien qu'il paraisse évident, omniprésent, palpable par nos sens immédiat, il est avant tout une philosophie, une approche ni plus ni moins. C'est une philosophie parce que le déterminisme l'habite et le hante ; c'est une approche parce que la localité s'impose comme propriété physique du phénomène. Le contexte mathématique de ses idées a été élaboré par Isaac Newton dans ses "Principes Mathématiques de la philosophie naturelle" dans lesquelles il a développé les analyses de Galilée en les mathématisant et permit ainsi à la physique de faire un saut en passant du cadre phénoménologique et descriptif à un cadre théorique où l'on a été capable d'expliquer, de prédire et de généraliser. La mécanique classique de Newton est foncièrement déterministe et affirme que la dynamique de la particule est entièrement déterminée si l'on connait à chaque instant sa position x et sa quantité de mouvement p. On dit alors que c'est une théorie déterministe. Cette approche conçue dans le cadre de la mécanique s'est généralisée à toute la physique allant de la gravitation " force d'interaction des masses" jusqu'à l'électrodynamique enceinte théorique des interactions des charges via des champs électromagnétiques. Au cours de son développement, cette approche a buté sur deux problèmes fondamentaux celui de la "relativité des temps" en relation avec l'hypothèse de l'Ether et celui du rayonnement du corps noir en relation avec l'existence du quantum de Planck. Ces deux problèmes ont été à l'origine de l'introduction respective de deux constantes fondamentales en physique théorique : la célérité de la lumière et la constante de Planck. Elles ont été unifiées ensemble dans un schéma théorique élégant mais aussi , qui est l'électrodynamique quantique. La constante de Gravitation les rejoint dans un objet d'unification des champs quantiques. La situation est ambigüe et la solution est loin d'être espérée.

Le phénomène quantique par son trait essentiel de l'atomiticité s'avère dès son apparition un élément inintelligible du point de vue classique. Par exemple, aux quanta de lumière on incompatible ne pourrait associer une trajectoire bien définie au sens de la physique classique. Ce fait reflète le caractère complémentaire de la continuité spatiale de la propagation et du trait d'atomiticité. Situation qui nous oblige à renoncer à une description causale complète du phénomène physique et nous contenant des lois de probabilité fondées sur correspondance

intime entre les lois classiques et le quantum d'action de Planck.

Dans ce qui suit, nous allons présenter les principes de la mécanique quantique en commençant par le principe d'incertitude ou dans sa forme la plus générale le principe de complémentarité. Les postulats de la mécanique quantique ne sont autres que des énoncés logiques et adéquats assurant l'essence de cette complémentarité.

2.1.1 Développement de la mécanique quantique

Le développement de la physique quantique commença avec l'attitude qu'a pris Max Planck (1901) devant l'abandon de certains des principes classiques de la description des phénomènes de la nature en introduisant l'hypothèse du quantum universel d'action. Cette attitude nouvelle du trait d'atomicité nous apprend que les théories classiques sont des simples idéalisations qui ont des limites dans leurs applications dans les phénomènes quantiques. Leurs ambiguïtés de représentations ne s'effacent que dans le cas où les actions mises en jeu dans le phénomène physique sont grandes par rapport à ce quantum universel. Le terrain de conflit est celui de renoncer à une causalité "rigide" de la physique classique au profit d'un "indéterminisme" pour contenir le trait d'atomiticité ; une sorte de généralisation de causalité classique en une causalité quantique. C'est en partant de la relation intime entre la thermodynamique et les régularités statistiques présentes dans les systèmes mécaniques à très grand nombre de degré de liberté que Planck se laisse guider dans son analyse du rayonnement thermique et se trouve devant le fait d'accepter cette hypothèse du quantum universel pour dépasser les ambiguïtés inhérentes aux représentations classiques. Ces considérations bornées à la résolution du problème du rayonnement du corps noir sont en fait la première démarcation par rapport à l'esprit classique de la physique d'avant la quantique puisqu'elle contenait une discontinuité des échanges d'énergie entre la matière et le rayonnement. Cet écart s'est accentué avec Einstein (1905) qui admît hardiment que ses échanges d'énergie sont l'œuvre de quanta de la lumière qui sont les photons dont l'énergie et l'impulsion sont intimement liés aux propriétés π du rayonnement lui même que sont la fréquence et la longueur d'onde via ce quantum d'action universel. Cette image corpusculaire est inconciliable avec le phénomène ondulatoire de la lumière. La physique classique a aussi échoué dans l'explication de la stabilité de l'atome de Rutherford (1911) et c'est encore l'hypothèse de ce quantum universel introduite par Niels Bohr (1913) qui est venue rendre

compte de cette stabilité d'atome aussi bien que des lois empiriques qui décrivent le spectre des atomes en supposant que le spectre est émis d'une manière discontinue suite à des transitions entre des états quantiques stationnaires. Une fois encore cette hypothèse vient par son contenu renoncer à la description causale "rigide" de la physique classique. Ces états stationnaires ne laissent place qu'à la notion de probabilité dont l'évaluation dépend du principe de correspondance selon lequel la description classique doit se retrouver dans le cas où les actions mises en jeu sont grandes par rapport au quantum universel.

Une voie encore plus riche fut frayée par Louis de Broglie (1925) quand il reconnut que la dualité onde-corpuscule n'est pas seulement une propriété de la lumière mais plutôt aussi de la matière. Cette idée fut aussitôt confirmée par des expériences d'interférence des électrons. Dans un même ordre d'idée, Schrödinger (1926) montra comment les états stationnaires des atomes ainsi que leurs spectres peuvent être déduits d'une équation d'onde qu'il déduit à partir d'une analogie déjà établie entre la mécanique et l'optique. Vers la même année, Heisenberg proposa une mécanique des matrices et des développements très rapides ont conquis la physique quantique. Dans ce schéma, les orbites stationnaires ne font plus partie du décor et les équations de mouvement gardent leurs formes où l'on remplace les grandeurs cinématiques et dynamiques classiques par des symboles qui ne commutent pas et la constance de Planck n'entre qu'à travers une relation cinématique de commutation. Cette représentation a permis d'expliciter le principe de correspondance formellement et le passage du quantique au classique se voit éclairer. Peu après, Schrödinger montra l'équivalence des deux approches, ondulatoire et matricielle, et les physiciens de ce temps se sont acharnés à élaborer un formalisme abstrait de cette physique quantique qui tiendrait compte des différentes représentations et de son interprétation. Malgré le succès retentissant de ce formalisme subsistait un malaise relatif à celui de la mesure quantique dont une clarification a vu le jour avec l'essai de l'expérience du microscope de Heisenberg postulée comme un principe d'incertitude.

Dans ce qui suit, nous présentons ce principe d'indétermination de la mesure dans un exposé simple et nous le prolongeons par le principe qui l'englobe qui est celui de la complémentarité. La démonstration de ce principe résulte des postulats de la mécanique quantique ce qui démontre que le formalisme est cohérent et complet, et contient comme il se doit un postulat de mesure.

2.1.2 Le principe d'incertitude

Ce principe stipule que la connaissance qu'on pourrait avoir d'un système quantique contient toujours une indétermination. Toute mesure de la position d'un électron à l'aide d'un appareil quelconque (le microscope par exemple) utilisant le rayonnement devra selon la dualité onde-particule être accompagnée d'un échange d'impulsion entre l'électron et l'appareil de mesure. Cet échange d'impulsion est beaucoup plus grand que la précision sur la position sera plus grande. Suivant le formalisme, cette dualité onde-particule se manifeste dans la mesure par une limitation sur la précision de chacune de deux variables conjuguées. Dans le cas de la position et de l'impulsion on a la relation suivante

$$\Delta x \Delta p \sim \hbar$$

où Δx et Δp sont des incertitudes définies sur la détermination des ces variables. Ces relations d'incertitudes permettent d'expliquer et d'élucider les paradoxes qui surgissent au cours d'une analyse d'effets quantiques au moyen des images habituelles de la physique classique en basant sur la connexion intime entre la description statistique de la mécanique quantique et les possibilités effectives de mesure. Là encore et avec plus de détermination, on voit que l'hypothèse de l'atomicité remets en cause d'une manière plus directe le cadre de causalité "rigide" de la mécanique quantique. Plus général est alors le principe de complémentarité qui permet de tenir compte de cette hypothèse d'atomiticité et de l'exigence de la finitude du quantum universel. Il est important de reconnaitre alors que, " d'aussi loin que les phénomènes puissent transcender le domaine des explications de la physique classique, la description de tous les résultats d'expérience doivent être exprimés en termes classiques" parce que dans une expérience nous nous référons à des situations où nous pouvons dire ce que nous avons fait et ce qu'e nous avons appris. Cette connaissance se fait au moyen des images classiques dénués d'ambiguïtés en se servant convenablement de la terminologie de la physique classique et implique avec elle "l'impossibilité de toute séparation nette entre le comportements des objets atomiques et leur interaction avec les instruments de mesure servant à définir les conditions sous lesquelles le phénomène se manifeste". Tout essai de subdivision du phénomène exigera un changement du dispositif expérimental qui permettra de nouvelles possibilités d'interactions non contrôlables en principe et "les résultats obtenus dans des conditions expérimentales différentes ne peuvent être

englobés en une seule image, mais doivent être considérés comme complémentaires en ce sens que, seule, la totalité des phénomènes épuise l'information possible sur les objets". "Ce principe de la complémentarité peut être considéré comme une généralisation rationnelle de l'idéal même de la causalité". Cette manière nouvelle de voir les choses a suscité d'ardentes discussions et une controverse s'est installée parmi les physiciens de cette époque. Le paradoxe EPR figure parmi ces tentatives de démonstration de l'incomplétude du formalisme quantique. Son contenu a été publié dans la prestigieuse revue Physical Review sous le titre "Can quantum-mecahnical description be considered complete" .

Dans ce qui suit, nous allons présenter les principes de base du formalisme quantique, parmi ces principes figure le postulat de la mesure qui stipule un effondrement de l'état physique sur l'état de la mesure. Nous abordons alors juste après utilisant ce postulat de mesure l'argument de l'incomplétude proposé par Einstein-Podolsky-Rosen puis brièvement nous exposerons l'objection de Bohr à cet argument et l'absorption de son conflit dans un cadre de complémentarité.

2.1.3 Les principes de la mécanique quantique

Expérience de fentes de Young

En 1801, le physicien Thomas Young montra la nature ondulatoire de la lumière lors d'une expérience demeurée célèbre. Soit une mince fente percée dans un écran opaque et placée derrière une lampe à vapeur de sodium. La fente diffracte la lumière qui s'étale sur écran muni de deux étroites fentes. Les deux faisceaux obtenus se superposent, donnant lieu à un phénomène d'interférence de franges visibles sur écran situé au-delà du dispositif. Des franges sombres, chacune d'elle correspondent aux régions où les deux ondes se construisent ou se détruisent.

Le principe de la superposition

Le principe de superposition affirme que l'état physique des systèmes quantiques : atome, particule, photon etc. admet la règle de combinaison des vecteurs. Quand un système a plusieurs états possibles, la somme de tous ces états est également un état possible. On dit que le système se trouve alors dans une superposition d'états. C'est grâce à ce principe qu'on puisse génèrer

les multiples représentations classiques qui sont en dualité quantique Ce phénomène est bien sur impensable dans l'univers classique des particules bien qu'il soit déjà présent dans l'image ondulatoire des ondes. Mais revu dans sa dualité, il nous permet d'accéder aux propriétés étranges du monde quantique. La mesure fait disparaître la superposition d'états au profit d'un seul état et on parle alors de la réduction du paquet d'ondes. la superposition d'états et la théorie quantique nous montre comment calculer la probabilité qu'on a de mesurer chaque état dans cette superposition.

La représentation d'un état quantique

Avant d'exposer l'axiomatique de la mécanique quantique, voyons d'abord comment se décrit l'état d'un système physique suivant cette nouvelle approche du principe de complémentarité généralisant la notion de causalité au niveau microscopique. L'état physique du système contient toute l'information. Il décrit, par exemple un atome préparé dans un niveau d'énergée bien défini ou un éléctron localisé à une certaine position dans l'éspace. Mathématiquement (choix de l'école de Copenhague) l'état est un objet mathématique qui donne le maximum d'information possible sur le système dans le but de prévoir les résultats des expériences que l'on peut réaliser. Cet élément, est un vecteur de l' espace de Hilbert. Le choix de cet espace est motivé par l'approche probabiliste qui nous permet de nous ramener aux situations classiques via le principe de correspondance. Ce choix permet une superposition des états qui est en principe fondamental agençant les possibilités des phénomènes qui émergent en expérience.

La notation de Dirac

Il est devenu habituel mais aussi par souci de représentation on notera l'état du système représenté par un vecteur normé $|> \in$ H, avec $|>$ est appelé " ket " et on notera $<|$ appelé "bra " , le vecteur dual $\in \mathcal{H}^*$

Comme on va le voir les grandeurs physiques seront des opérateurs hermitiens complets, puisque une mesure complète sur cette grandeur doit la déterminer réellement et complètement et la valeur moyenne de l'observable A dans l'état $|\psi\rangle$ sera notée $\langle\psi| A \ |\psi\rangle$

La définition de fonction d'onde de Schrodinger

La fonction d'onde de Schrödinger est la représentation de l'état quantique dans la base de dimension infinie relative à l'observable position. La probabilité de présence des particules représentées par cet état quantique est alors directement liée au carré de la norme de cette fonction d'onde. La fonction d'onde est calculée à l'aide de l'équation de Schrödinger, ce qu'on appelle l'évolution de l'état physique. Comme on l'a dit précédemment, la fonction d'onde fut introduite par Louis de Broglie dans sa thèse de la dualité onde-particule. Elle est issue de la dualité onde-particule et donne à toute particule les propriétés d'interférence typique d'une onde.

L'espace de Hilbert

Il est utile de rappeler les propriétés mathématiques de cet espace de Hilbert enceinte mathématique des calculs quantiques.

Définition

Un espace de Hilbert $\mathcal{H}$ est un espace vectoriel doté d'un produit scalaire hermitien et dont les propriétés de convergence sont complète, ceci permet et garantit la traduction des propriétés quantiques en valeurs mathématiques d'une manière univoque. En fait, l'interprétation probabiliste use du carré du module t par conséquent les phases laissées libres vont jouées un rôle important dans la description quantique : on appelle ça phénomène d'interférence et plus profond encore intrication des états. La dimension de cet espace est quelconque en général et comme on va voir dans le prochaine chapitre que l'information quantique utilise des espaces de dimension finie de valeurs deux pour un qubit et de valeurs 2^n pour un n-qubit.

Il est vrai que cet état des choses peut être représenté dans d'autres représentations, ce qu'on a cité auparavant pour la mécanique des matrices, mais au fait les résultats physiques sont indépendants du choix de représentation. Une généralisation aux systèmes composés, vue dans l'approche de la matrice densité, est aussi donnée.

Les postulats de la mécanique quantique

Postulat 1 : On associe à chaque système physique fermé un espace linéaire complexe muni d'un produit hermitien complet qu'on nomme espace de Hilbert. L'état du système est alors décrit par un vecteur de norme égale à l'unité appartenant à cet espace de Hilbert qu'on note$|\psi\rangle$.
Exemple : le qubit de l'information quantique

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \quad \text{avec} \qquad |a|^2 + |b|^2 = 1$$

C'est l'état fondamental de l'information quantique. Il appartient à un espace complexe de dimension 2. Il est abstrait mais il peut être réalisé physiquement de différentes manières : des états d'atomes de spin, de photons, etc.

Postulat 2 : Une observable (qui peut être aussi une grandeur physique) est une propriété du système quantique qui en principe peut être mesurée. Une observable est un opérateur auto-adjoint dont la base propre. Cet opérateur agit sur l'espace des états du système quantique

$$\begin{aligned} A \quad &: \quad |\psi\rangle \rightarrow A\,|\psi\rangle \\ A\left(a\,|\psi\rangle + b\,|\varphi\rangle\right) \quad &= \quad a\left(A\,|\psi\rangle\right) + b\left(A\,|\varphi\rangle\right) \\ \left\langle A^{+}\phi\right|\psi\rangle \quad &= \quad \langle\phi|\,A\psi\rangle \end{aligned}$$

Cet opérateur auto-adjoint peut être développé comme

$$A = \sum_n a_n P_n$$

Où a_n est une valeur propre et P_n le projecteur sur le sous espace propre correspondant à la valeur propre et s'écrivant

$$P_n = \sum_n |v_n\rangle\,\langle v_n|$$

Cet ensemble de projecteurs vérifie

$$P_n P_m = \delta_{nm} P_n;\ P_n^{+} = P_n;\ \sum_n P_n = I$$

Comme

$$P_n^2 = P_n \text{ et } P_n = P_n^{+}$$

On peut alors écrire

$$\sum_n P_n^+ P_n = I$$

D'habitude on définit la mesure quantique à partir de cet ensemble de projecteurs mais il est plus intéressant d'utiliser un ensemble d'opérateurs plus général.

Postulat 3 : Une mesure quantique est décrite par un ensemble d'opérateurs de mesure $\{M_n\}$. Ces opérateurs agissent sur l'espace des états du système physique. Notons (n) le résultat de mesure. Si le système physique est dans l'état $|\psi\rangle$ juste avant la mesure alors la probabilité d'avoir (n) comme résultat de mesure est

$$P(n) = \left\langle \psi \mid M_n^+ M_n \right| \psi\rangle$$

pour qu'on ait $\sum_n P(n) = 1$ l'ensemble des opérateurs $\{M_n\}$ vérifie

$$\sum_n M_n^+ M_n = I$$

Juste après la mesure, si le résultat de mesure est (n), l'état du système quantique (réduction du paquet d'ondes) est

$$|\,\widetilde{\psi}\rangle = \frac{M_n \mid \psi >}{\sqrt{\langle \psi \mid M_n^+ M_n |\, \psi\rangle}}$$

Postulat 4 : L'évolution d'un système quantique fermé est décrite par une opération unitaire comme

$$|\psi(t_2)\rangle = U(t_2, t_1)\,|\psi(t_1)\rangle$$

L'opérateur $U(t_2, t_1)$ est unitaire $U^+(t_2, t_1)U(t_2, t_1) = I$ et plus précisemment, l'évolution en temps continu est décrite par l'équation de Schrodinger

$$i\hbar \frac{\partial}{\partial t}\,|\psi(t)\rangle = H\,|\psi(t)\rangle$$

Où H est l'opérateur hamiltonien du système ; autrement dit, $U(t_2, t_1) = \exp\left[\dfrac{-i}{\hbar} H(t_2 - t_1)\right]$

En mécanique quantique, il n'existe aucune mesure qui puisse distinguer deux états quantiques non orthogonaux. En effet, soient $|\psi_1\rangle$ et $|\psi_2\rangle$ deux états non orthogonaux et $\{M_n\}$ un ensemble d'opérateurs de mesures quantiques. Notons respectivement

$$E_1 = \sum_{n,(1)} M_n^+ M_n \text{ et } E_2 = \sum_{n,(2)} M_n^+ M_n$$

l'ensemble qui donne l'état (1) et respectivement l'état (2), nous avons alors respectivement

$$\langle\psi_1 \mid E_1 \mid \psi_1\rangle = 1 \text{ et } \langle\psi_2 \mid E_2 \mid \psi_2\rangle = 1$$

Et en plus

$$E_1 + E_2 = I$$

Alors on a

$$\langle\psi_1 \mid E_2 \mid \psi_1\rangle = 0$$

Comme E_i est hermétique et est défini positif, définissons alors $\sqrt{E_i}$ et par conséquent $\sqrt{E_2} \mid \psi_1\rangle = 0$. Sachant que $|\psi_1\rangle$ et $|\psi_2\rangle$ sont deux états non orthogonaux, écrivons

$$|\psi_2\rangle = \alpha \mid \psi_1\rangle + \beta \mid \varphi\rangle \quad \text{où} \quad \mid \varphi\rangle \perp \mid \psi_1\rangle \text{ et } \mid \beta \mid < 1$$

On a alors

$$\sqrt{E_2} \mid \psi_2\rangle = \beta\sqrt{E_2} \mid \varphi\rangle$$

Nous déduisons alors que

$$\langle\psi_2 \mid E_2 \mid \psi_2\rangle = \mid \beta \mid^2 < 1$$

En contradiction avec l'hypothèse

$$\langle\psi_2 \mid E_2 \mid \psi_2\rangle = 1$$

D'où le résultat.

Mesures projectives

L'ensemble $\{M_n\}$des opérateurs de mesure admet un cas particulier intéressant qui est celui des mesures projectives. Une mesure projective est décrite par une observable M dont l'ensemble des projecteurs est $\{P_n\}$ avec

$$M = \sum_n a_n P_n \equiv \sum_n (n) P_n$$

P_n est le projecteur sur le sous espace de la valeur propre a_n. La probabilité d'avoir a_n est

$$P(a_n) \equiv P(n) = \langle\psi \mid P_n \mid \psi\rangle = \left\langle\psi \mid P_n^+ P_n\right| \psi\rangle$$

Et on a

$$\sum_n P_n = \sum_n P_n^+ P_n = I$$

Juste après la mesure on a

$$|\widetilde{\psi}\rangle = \frac{P_n \mid \psi >}{\sqrt{P_n}}$$

Ces projecteurs de mesure vérifient aussi

$$P_n P_m = \delta_{nm} P_n;\ P_n^+ = P_n;\ P_n^2 = P_n \text{ et } P_n = P_n^+$$

On voit bien que cet ensemble de mesure est un cas spécial de l'ensemble $\{M_n\}$ des opérateurs de mesure.

Valeur moyenne d'une mesure projective et principe d'incertitude

Soit M l'observabe de mesure. La moyenne de cette observalble de mesure est

$$\mathcal{E}(M) = \sum_n a_n P(n) = \sum_n a_n \langle \psi \mid P_n \mid \psi \rangle =< \psi \mid \sum_n a_n P_n \mid \psi \rangle =< \psi \mid M \mid \psi \rangle =< M >_\Psi$$

L'écart quadratique de M est défini par

$$\Delta(M) = \sqrt{< M^2 >_\Psi - < M >_\Psi^2}$$

Et il n'est pas difficile de s'assurer qu'on le pricipe d'incertitude de Heisenberg suivant et dont nous avons déjà donné une interprétation physique

$$\Delta(M)\Delta(M') \geq \frac{|< [M, M'] >_\Psi|}{2}$$

Les mesures POVM (Positif-Operator-Valued-Measure)

A partir de l'ensemble $\{M_n\}$ on peut aussi construire un ensemble d'opérateurs de mesure définis positifs. En effet, définissons

$$E_n = M_n^+ M_n$$

E_n est défini positif et on a

$$P(n) =< E_n >_\Psi \text{ et } \sum_n E_n = I$$

On appelle cet ensemble $\{E_n\}$ l'ensemble des opérateurs de mesure définis positifs (POVM). Les mesures projectives forment un ensemble POVM.

Systèmes composées

Postulat : L'espace des états d'un système composé est le produit tensoriel des espaces des états de chacune des parties du système total. En plus si les parties de ce système sont préparées dans les états suivants : $\mid \psi_i\rangle \quad i = 1 - N$ alors l'état du système total est

$$\mid \psi_1\rangle \otimes \mid \psi_2\rangle \otimes ... \otimes \mid \psi_N\rangle$$

Application : Soit Q l'espace des états d'un système quantique et $\{M_n\}$ un ensemble d'opérateurs de mesure agissant sur Q.Introduisons un système auxilliaire $\mathcal{M}$ qui a une base orthonormé $\{|n\rangle\}$où n sont les différents résultats de mesure données par l'ensemble $\{M_n\}$ .Fixons d'abord l'état de $\mathcal{M}$ à $|0\rangle$ et définissons l'opérateur U agissant sur $|\psi\rangle \otimes |0\rangle$, où $|\psi\rangle$ est l'état du système physique, par

$$U |\psi\rangle |0\rangle \equiv \sum_n M_n |\psi\rangle |n\rangle .$$

Comme

$$\sum_n M_n^+ M_n = I.$$

On a

$$\begin{aligned} \langle\varphi| \langle 0| U^+ U |\psi\rangle |0\rangle &= \sum_{n,n\prime} \langle\varphi| M_n^+ M_{n\prime} |\psi\rangle \langle n \mid n'\rangle \\ &= \sum_n \langle\varphi| M_n^+ M_n |\psi\rangle = \langle\varphi \mid \psi\rangle \\ &= (\langle\varphi| \langle 0|)(|\psi\rangle |0\rangle) \end{aligned}$$

ie, U conserve le produit scalaire des vecteurs de la forme $|\psi\rangle |0\rangle$ .Or $|\psi\rangle |0\rangle$ constitue un s-espace de l'espace $Q \otimes \mathcal{M}$ où $\mathcal{M}$ est l'espace généré par $\{|n\rangle\}$. Donc d'aprés les propriétés algèbrique on peut étendre U sur tout l'espace $\phi \otimes M$ en conservant son unitarité.

Associons maintenant à cet opérateur unitaire U la mesure projective $\{P_n\}$ defini par

$$P_n = I_Q \otimes |n\rangle \langle n| .$$

On a

$$\begin{aligned}\langle\psi|\langle 0|U^{+}\,P_nU\,|\psi\rangle|0\rangle &= \sum_{n\prime,n\prime\prime}\langle\psi|\,M^{\ +}_{n\prime}\ \ \langle n'|\,I_Q\otimes|n\rangle\langle n|\,M_{n\prime\prime}\,|\psi\rangle\,|n''\rangle \\ &= \sum_{n\prime,n\prime\prime}\langle\psi|\,M^{\ +}_{n\prime}\ \ M_{n\prime\prime}\,|\psi\rangle\,\delta_{n\prime,n}\delta_{n\prime\prime,n} \\ &= \langle\psi|\,M^{\ +}_{n}\ \ M_n\,|\psi\rangle = P(n).\end{aligned}$$

Et

$$\frac{P_nU\,|\psi\rangle\,|0\rangle}{\sqrt{\langle\psi|\langle 0|U^{+}\,P_nU\,|\psi\rangle|0\rangle}} = \frac{M_n\,|\psi\rangle\,|n\rangle}{\sqrt{\langle\psi|\,M^{\ +}_{n}\ \ M_n\,|\psi\rangle}}$$

L'état du système physique est alors

$$\frac{M_n\,|\psi\rangle}{\sqrt{\langle\psi|\,M^{\ +}_{n}\ \ M_n\,|\psi\rangle}}$$

Et le probabilité avant la mesure est

$$P\,(n) = \langle\psi|\,M^{\ +}_{n}\ \ M_n\,|\psi\rangle$$

Apartir de$\{P_n\}$ et U on retrouve l'ensemble $\{M_n\}$ via le système auxilliaire.

Opérateur densité (la matrice de densité)

La mécanique quantique peut être formulée dans un formalisme dit formalisme de la matrice densité qui est plus convenable et plus compatible avec presque tous les scénarios qu'on puisse rencontrés.

Supposons que l'état du système n'est pas complètement connu. Précisemment, qu'il peut être dans différents états $|\psi_i\rangle$ avec des probabilité P_i.

On appelle l'ensemble$\{P_i,\ \ |\psi_i\rangle\}$ ensemble d'états purs. Nous définissons l'opérateur densité ou la matrice densité par

$$\rho = \sum_i P_i\,|\psi_i\rangle\langle\psi_i|$$

Soit $\mathcal{U}$ un opérateur unitaire d'évolution du système, alors ρ évolue comme

$$\begin{aligned} \rho \quad &\rightarrow \quad \rho^{(U)} = \sum_i P_i U \left|\psi_i\right\rangle \left\langle\psi_i\right| U^+ \\ &= \quad U\ \rho U^+ \end{aligned}$$

Si l'état du système est initialement $|\psi_i\rangle$ la probabilité d'avoir le résultat (m) est

$$P\left(m \mid i\right) = \left\langle\psi_i\right| M_m^+ M_{\ m} \left|\psi_i\right\rangle$$

$\{M_m\}$ est un ensemble d'opérateurs de mesure. Ou bien on peut écrire

$$\begin{aligned} P\left(m \mid i\right) &= \sum_\lambda \left\langle\psi_i\right| \lambda \left\rangle \left\langle\lambda\right| M_m^+ M_{\ m} \left|\psi_i\right\rangle \right. \\ &= \sum_\lambda \left\langle\lambda\right| M_m^+ M_{\ m} \left|\psi_i\right\rangle \ \left\langle\psi_i\right| \lambda \left\rangle \right. \\ &= Tr\left(M_m^+ M_{\ m} \left|\psi_i\right\rangle \left\langle\psi_i\right|\right) \end{aligned}$$

Si l'état initial n'est pas complètement connu, la probabilité d'avoir le résultat (m) est

$$\begin{aligned} p\left(m\right) &= \sum_i p_i\ p\left(m \mid i\right) \\ &= \sum_i p_i\ Tr\left(M_m^+ M_{\ m} \left|\psi_i\right\rangle \left\langle\psi_i\right|\right) \\ &= Tr\left(M_m^+ M_{\ m} \rho\right) \end{aligned}$$

Si $|\psi_i\rangle$ est l'état avant la mesure, alors

$$\left|{\psi_i}^m\right\rangle = \frac{M_m \left|\psi_i\right\rangle}{\sqrt{\left\langle\psi_i\right| M_m^+ M_{\ m} \left|\psi_i\right\rangle}}$$

est l'état juste aprés la mesure. Soit la probabilité $p\left(m \mid i\right)$ de i sachant que le résultat est (m), on sait que (d'après la théorie des probabilités conditionnelles)

$$p\left(m \mid i\right) = \frac{p\left(m \mid i\right) p_i}{p(m)}$$

Juste aprés la mesure pour un système décrit par la matrice densité on a une matrice densité

$$\begin{aligned}
\rho_{(m)} &= \sum_i p\left(m \mid i\right) |\psi_i{}^m\rangle \langle\psi_i^m| \\
&= \sum_i p\left(m \mid i\right) \frac{M_{\ m} |\psi_i\rangle \langle\psi_i| M_m^+}{\langle\psi_i| M_m^+ M_{\ m} |\psi_i\rangle} \\
&= \frac{p\left(m \mid i\right) p_i}{p(m)} \frac{M_{\ m} |\psi_i\rangle \langle\psi_i| M_m^+}{p\left(m \mid i\right)} \\
&= \frac{M_{\ m} \rho M_m^+}{Tr\left(M_m^+ M_{\ m} \rho\right)}
\end{aligned}$$

Juste après la mesure (m) sachant qu' avant la mesure le système est décrit par ρ on a

$$\rho_{(m)} = \frac{M_{\ m} \rho M_m^+}{Tr\left(M_m^+ M_{\ m} \rho\right)}$$

Si l'état du système est complètement déterminé $|\psi\rangle$ nous dirons que l'état est pur et on lui associe le matrice densité

$$\rho = |\psi\rangle \langle\psi|$$

Sinon il est dit un état mélange ou mixte

$$\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$$

avec p_i la probabilité de chaque état $|\psi_i\rangle$. Dans le cas pur on a :

$$\rho^2 = |\psi\rangle \langle\psi| \psi \rangle \langle\psi| = \rho$$

Et

$$\begin{aligned}
Tr\rho &= Tr\rho^2 = \sum_\lambda \langle\lambda| \psi \rangle \langle\psi| \lambda \rangle \\
&= \langle\psi| \sum_{\sum \lambda} |\lambda\rangle \langle\lambda| \psi \rangle \\
&= \langle\psi| \psi \rangle = 1
\end{aligned}$$

Dans le cas non pure

$$\begin{aligned}
\rho^2 &= \sum_i \sum_j P_i P_j |\psi_i\rangle \underbrace{\langle\psi_i| \psi_j \rangle}_{\delta_{ij}} \langle\psi_j| \\
&= \sum_i P_i^2 |\psi_i\rangle \langle\psi_i|
\end{aligned}$$

Et

$$\begin{aligned} Tr\rho^2 &= \sum_i P_i^2 \sum_\lambda \langle\lambda|\,\psi_i\,\rangle\,\langle\psi_i|\,\lambda\,\rangle \\ &= \sum_i P_i^2\,\langle\psi_i|\,\psi_i\,\rangle = \sum_i P_i^2 < 1 \end{aligned}$$

Car $\sum_i P_i = 1$ ($Tr\rho = 1$).En effet

$$\begin{aligned} Tr\rho &= \sum_i P_i \sum_\lambda \langle\lambda|\,\psi_i\,\rangle\,\langle\psi_i|\,\lambda\,\rangle \\ &= \sum_i P_i\,\langle\psi_i|\,\psi_i\,\rangle = \sum_i P_i = 1 \end{aligned}$$

ρ est un opérateur positif

$$\begin{aligned} \langle\varphi|\,\rho\,|\varphi\rangle &= \sum_i P_i\,\langle\varphi|\,\psi_i\,\rangle\,\langle\psi_i|\,\varphi\,\rangle \\ &= \sum_i P_i\,|\langle\varphi|\,\psi_i\,\rangle|^2 \geq 0 \end{aligned}$$

Propriètés :

1) ρ un opérateur densité associé à l'ensemble $\{P_i, |\psi_i\rangle\}$ si et seulement si $Tr\rho = 1$, ρ opérateur positif.

2) Deux ensembles $\{P_i\ , |\psi_i\rangle\}$ et $\{P_i',\ \ |\psi_i'\rangle\}$ génère la même matrice densité si et seulement si $|\psi_i'\rangle = U\,|\psi_i\rangle$ et U unitaire.

Si on suppose que le système peut être dans l'état mélange ρ_m avec une probabilité $p(m)$ la description se fait alors par

$$\begin{aligned} \rho &= \sum_m p\,(m)\,\rho_m \\ &= Tr\left(M_m^+ M_{\ m}\rho\right)\frac{M_{\ m}\rho M_m^+}{Tr\left(M_m^+ M_{\ m}\rho\right)} \\ &= \sum_m M_{\ m}\rho M_m^+ \end{aligned}$$

Si le système est composé et chaque composante est décrire par ρ_i alors ρ est décrit par

$$\rho_1 \otimes \rho_2 \otimes ... \otimes \rho_n.$$

2.1.4 Matrice densité réduite

Soit le système composé $\{AB\}$ décrit par la matrice densité ρ^{AB}ou peut décrire chacune des parties par une matrice densité

$$\begin{aligned} \rho^A &= Tr_B\left(\rho^{AB}\right) \\ \rho^B &= Tr_A\left(\rho^{AB}\right) \end{aligned}$$

Où Tr_B trace partielle sur B et Tr_A trace partielle sur A.

Exemple

$$\begin{aligned} Tr_B\left(|\psi_A\rangle\left\langle\widetilde{\psi}_A\right| \otimes |\psi_B\rangle\left\langle\widetilde{\psi}_B\right|\right) &= |\psi_A\rangle\left\langle\widetilde{\psi}_A\right| Tr_B\left(|\psi_B\rangle\left\langle\widetilde{\psi}_B\right|\right) \\ &= \left(\left\langle\widetilde{\psi}_B\middle|\,\psi_B\,\right\rangle\right)|\psi_A\rangle\left\langle\widetilde{\psi}_A\right| \end{aligned}$$

Et

$$Tr_B\left(|\psi_A\rangle\left\langle\widetilde{\psi}_A\right| \otimes |\psi_B\rangle\left\langle\widetilde{\psi}_B\right|\right) = \left(\left\langle\widetilde{\psi}_A\middle|\,\psi_A\,\right\rangle\right)|\psi_B\rangle\left\langle\widetilde{\psi}_B\right|$$

En effet cette trace partielle décrit correctement chacune des parties.

Si on suppose qu'on effectue une mesure sur A via l'observable M, Sur le produit tensoriel $A \otimes B$ on a l'observable

$$\overline{M} = M \otimes I_B$$

Et on a

$$\begin{aligned} Tr\left(M\rho^A\right) &= Tr\left(\overline{M}\rho^{AB}\right) \\ &= Tr\left(M \otimes I_B\right)\rho^{AB} \end{aligned}$$

On montre que la seule fonction ρ^A verifiant ce résultat est

$$\rho^A = Tr_B\left(\rho^{AB}\right)$$

Décomposition de Schmidt

Soit $|\psi\rangle$ un état pur d'un système composé AB. Alors il existe une base orthonormée $|i_A\rangle$ de A et une base orthonormée $|i_B\rangle$ de B telles que

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle$$

Où $\lambda_i \geq 0$ satisfaisant $\sum_i \lambda_i^2 = 1$.

Cette décomposition est dite de Schmidt et λ_i sont les coefficients de Schmidt.

Exemple

Soit un système à deux qubits décrit par l'état pur

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{2}$$

La décomposition de Schmidt est

$$|\psi\rangle = \sum_i^2 \lambda_i |i_A\rangle |i_B\rangle , \qquad \lambda_i \geq 0, \qquad \sum_i \lambda_i^2 = 1.$$

Où $\{|i_A\rangle\}$ est orthonormée et

$$\langle 1_A | 1_A\rangle = \langle 2_A | 2_A\rangle = 1, \qquad \langle 1_A | 2_A\rangle = \langle 1_B | 2_B\rangle = 0$$

Evidemment on identifie

$$|1_A\rangle = |1_B\rangle = |0\rangle , \qquad |2_A\rangle = |2_B\rangle = |1\rangle$$

Alors

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|1_A\rangle |1_B\rangle + |2_A\rangle |2_B\rangle)$$

Avec

$$\lambda_1 = \lambda_2 = \frac{1}{\sqrt{2}}, \qquad \sum_i^2 \lambda_i^2 = 1$$

Même chose pour

$$\begin{aligned} |\psi\rangle &= \frac{|00\rangle + |11\rangle + |01\rangle + |10\rangle}{2} \\ &= \lambda_1 |1_A\rangle |1_B\rangle + \lambda_2 |2_A\rangle |2_B\rangle \end{aligned}$$

Avec

$$\begin{aligned} |1_A\rangle &= \alpha |0\rangle + \beta |1\rangle , \qquad |\alpha|^2 + |\beta|^2 = 1 \\ |2_A\rangle &= \gamma |0\rangle + \delta |1\rangle , \qquad |\gamma|^2 + |\delta|^2 = 1 \end{aligned}$$

$$\langle 1_A | 2_A\rangle = \alpha^* \gamma + \beta^* \delta = 0$$

Et aussi

$$\begin{aligned} |1_B\rangle &= \overline{\alpha} |0\rangle + \overline{\beta} |1\rangle , \qquad |\overline{\alpha}|^2 + \left|\overline{\beta}\right|^2 = 1 \\ |2_B\rangle &= \overline{\gamma} |0\rangle + \overline{\delta} |1\rangle , \qquad |\overline{\gamma}|^2 + \left|\overline{\delta}\right|^2 = 1 \end{aligned}$$

$$\langle 1_B | 2_B\rangle = \overline{\alpha}^* \overline{\gamma} + \overline{\beta}^* \overline{\delta} = 0$$

Elors

$$|\psi\rangle = \lambda_1 \left(\alpha |0\rangle + \beta |1\rangle\right) \left(\overline{\alpha} |0\rangle + \overline{\beta} |1\rangle\right) + \lambda_2 \left(\gamma |0\rangle + \delta |1\rangle\right) \left(\overline{\gamma} |0\rangle + \overline{\delta} |1\rangle\right)$$

d'où

$$\begin{aligned} \lambda_1 \alpha \overline{\alpha} + \lambda_2 \gamma \overline{\gamma} &= \frac{1}{2}, \qquad \lambda_1 \beta \overline{\alpha} + \lambda_2 \delta \overline{\gamma} = \frac{1}{2} \\ \lambda_1 \alpha \overline{\beta} + \lambda_2 \gamma \overline{\delta} &= \frac{1}{2}, \qquad \lambda_1 \beta \overline{\beta} + \lambda_2 \delta \overline{\delta} = \frac{1}{2}, \end{aligned}$$

De cette méthode de décomposition de Schmidt on peut definir une purification de l'état d'un système comme suit

Purification de Schmidt

Soit un système A décrit par

$$\rho^A = \sum_i P_i |i_A\rangle \langle i_A|$$

Purifiant A en le composant avec un système fictif R dont la base orthonormée est $|i_R\rangle$, l'état pur

$$|AR\rangle = \sum_i \sqrt{P_i}\,|i_A\rangle\,|i_R\rangle$$

et dit purifié de A.

Et on a

$$\rho^A = Tr_R\left(|AR\rangle\langle AR|\right)$$

En effet

$$\begin{aligned} Tr_R\left(|AR\rangle\langle AR|\right) &= \sum_{ij}\sqrt{P_iP_j}\,\left|i^A\right\rangle\left\langle j^A\right| Tr\left(\left|i^K\right\rangle\left\langle j^K\right|\right) \\ &= \sum_i \sqrt{P_iP_j}\,\left|i^A\right\rangle\left\langle j^A\right|\delta_{ij} \\ &= \sum_i P_i\left|i^A\right\rangle\left\langle i^A\right| = \rho^A \end{aligned}$$

2.1.5 Paradoxe EPR et inégalités de Bell

Problème de la complétude de la mécanique quantique : (Article d'Einstein-Podolsky-Rosen)

Dans cet article les auteurs ont voulu mettre à défaut la mécanique quantique en s'attaquant à sa complétude. L'argumentation est basée sur un critère de réalité adopté par les auteurs : "Si, sans perturber en aucune façon un système donné, nous pouvons prédire avec certitude (c'est à dire avec une probabilité égale à l'unité) la valeur d'une quantité physique,donc il existe un élément de réalité physique correspondant à cette quantité" .

Les auteurs exposent alors les conséquences du formalisme quantique sur un système constitué de deux parties qui ont agi l'une sur l'autre pendant un temps limité. Après ça, ils déduisent que des grandeurs physiques telles la position et l'impulsion qui sont incompatibles dans une des deux parties peuvent être prédites par des mesures effectuées sur l'autre partie du système. La conclusion est alors que la mécanique quantique "ne fournit pas une description complète de la réalité" et ils expriment leur croyance en une théorie plus complète. Exposons maintenant cette argumentation :

Soient deux systèmes I et II qui, nous supposons, ont interagi pendant un temps ($t = 0, t = T$). Après ce temps, on les suppose sans interaction et on suppose qu'on connait leurs états avant $t = 0$. Ainsi nous pouvons déterminer suivant l'équation de Schrödinger leur état composé $(I + II)$ à n'importe quel instant et en particulier à $t > T$.Soit Ψ la fonction d'onde du système composé $(I + II)$. L'état de chaque partie reste inconnu et ne peut se déterminer que par un processus de mesure impliquant une réduction du paquet d'ondes. Soient a une quantité physique de la partie A et $a_1 a_2 a_3$...des valeurs propres de A et $u_1 u_2 u_3$... les fonctions propres correspondantes. Comme cet ensemble est complet développant Ψ suivant ce système complet de fonctions propres

$$\Psi(x_1, x_2) = \sum_{n=1}^{\infty} \psi_n(x_2) u_n(x_1)$$

x_1 est la variable décrivant le premier système et x_2 est la variable décrivant le deuxième système. $\psi_n(x_2)$ sont dans ce cas les coefficients du développement de $\Psi(x_1, x_2)$ par rapport au système de fonctions orthogonal $u_n(x_1)$.

Supposons que nous avons effectué une mesure sur l'observable A et qu'on a trouvé la valeur a_k . D'après le postulat de la mesure de la mécanique quantique, le système I devrait se trouvé dans l'état défini par $u_k(x_1)$ et par conséquent le deuxième système est laissé en l'état données par la fonction d'onde $\psi_k(x_2)$ puisque par réduction du paquet d'ondes la série précédente sera réduite au terme $\psi_k(x_2)u_k(x_1)$. La base des fonctions $u_n(x_1)$ détermine le choix sur l'observable A.

Maintenant, si on suppose qu'on a effectué une mesure sur le système I de l'observable B définie par la base des fonctions $v_n(x_1)$ associées aux valeurs propres $b_1 b_2 b_3$....Dans ce cas, le développement de Ψ suivant ce nouveau système complet de fonctions propres

$$\Psi(x_1, x_2) = \sum_{n=1}^{\infty} \varphi_n(x_2) v_n(x_1)$$

Si la mesure sur l'observable B donne la valeur b_k d'après le postulat de la mesure de la mécanique quantique, le système I devrait se trouvé dans l'état défini par $v_k(x_1)$ et par conséquent le deuxième système est laissé en l'état données par $\varphi_k(x_2)$ puisque par réduction du paquet d'onde la série précédente sera réduite au terme $\varphi_k(x_2)v_k(x_1)$. La base des fonctions $v_n(x_1)$ détermine le choix sur l'observable B.

Par conséquent, deux différentes mesures sur le système I laisse le système II dans deux états différents. En plus, pendant le temps de la mesure les deux systèmes n'interagissent plus et aucun changement n'affectera le système II suite à l'action sur le système I. Donc, il est possible d'affecter au système II, deux différentes fonctions d'onde d'une même réalité physique du système II.

L'étape suivante des auteurs, c'est de mettre à défaut le formalisme de la mécanique quantique en choisissant deux états incompatibles suivant le principe d'incertitude d'Heisenberg. L'exemple de l'observable position et l'observable impulsion du système II sert adéquatement bénéfiquement la stratégie de la contradiction. Dans ce but, nous chosissons pour les bases $\psi_n(x_2)$ et $\varphi_n(x_2)$ correspondantes aux quantités physiques P et Q.

Dans un premier temps, on fait le choix

$$\Psi(x_1, x_2) = \int_{-\infty}^{+\infty} \exp(\frac{i}{\hbar} p(x_1 - x_2 + x_0))dp$$

x_0 est une certaine constante. Soit A l'impulsion du premier système alors les $u_n(x_1) \rightarrow u_p(x_1) = \exp(\frac{i}{\hbar} p x_1)$ dont la valeur propre est p. On déduit alors les coefficients $\psi_n(x_2) \rightarrow \exp(\frac{-i}{\hbar} p(x_2 - x_0))$ qui correspondent à la valeur propre $(-p)$ de l'impulsion P du systéme II.

Dans le second cas, on choisit $u_n(x_1) \rightarrow u_x(x_1) = \delta(x_1 - x)$ donc l'observable B est l'opérateur position du système I dont la valeur propre est x et par suite $\psi_n(x_2) \rightarrow v_x(x_2) = \int_{-\infty}^{+\infty} \exp(\frac{i}{\hbar} p(x - x_2 + x_0))dp = 2\pi\hbar\delta(x - x_2 + x_0)$ qui est la fonction propre de l'opérateur position Q du système II dont la valeur propre est $x + x_0$. Comme

$$PQ - QP = \frac{\hbar}{i}$$

les auteurs déclarent alors que suivant les régles de la mécanique quantique, ils ont pu montrer en adoptant leur critère de réalité physique que P et Q doivent correspondre à des éléments de réalité simultanée ; ce qui contredit la relation de commutation précédente et son contenu d'indétermination. Ils concluent alors que le contenu physique de la fonction d'onde de la mécanique quantique est incomplet. Les auteurs croient qu'une théorie plus complète devrait exister.

La complémentarité comme réponse à ce paradoxe : (réponse de Niels Bohr)

Niels Bohr reconnait la lucidité et le caractère incontestable en apparence des arguments proposés dans l'article EPR. Le caractère subtil de l'argumentation indique combien la physique atomique dépasse le domaine accessible aux images intuitives. Le problème soulevé est de même type que celui qui se relève dans la description des fentes de Young quand on essaye de contrôler la mesure sur la position et l'impulsion de l'électron. La complémentarité et donc le principe d'indétermination de Heisenberg surgit pour nous éviter l'incohérence des représentations intuitives et complémentaires. Sans tarder, exposons les arguments de Bohr en faveur de cette complémentarité en physique quantique. Bohr écrivait : " Une telle argumentation, cependant, ne semble guère apte à remettre en question la validité de la description par la mécanique quantique, car celle-ci est fondée sur un formalisme mathématique cohérent qui prend en compte automatiquement tout procédé de mesure tel que ceux en question. La contradiction apparente révèle seulement que le point de vue habituel de la philosophie naturelle est essentiellement inadéquat pour représenter rationnellement les phénomènes physiques du type que nous rencontrons en mécanique quantique. L'interaction finie entre l'objet et les instruments de mesure, conséquence immédiate de l'existence du quantum d'action, entraîne parce qu'il est impossible de entraîne parce qu'il est impossible de contrôler la réaction de l'objet sur les appareils- la nécessité de renoncer définitivement à l'idéal classique de causalité et de modifier de fond en comble notre attitude à l'égard du problème de la réalité physique. En fait, comme nous le verrons, un critère de réalité, tel que celui des auteurs, contient quelque prudent que puisse paraître son énoncé- une ambiguïté essentielle lorsqu'il est appliqué aux problèmes actuels qui nous intéressent ici". Bohr montra ensuite que, dans la représentation de l'état de deux objets atomiques en interaction mutuelle, les conséquences du formalisme correspondaient aux arguments simples invoqués dans le cas des fentes de Young, lors de la discussion des montages expérimentaux adaptés à l'étude des phénomènes complémentaires. En effet, bien que toute paire P et Q de variables conjuguées obéisse à la régle de commutation et ne puisse par conséquent être fixée qu'avec des incertitudes réciproques, la différence $(Q_1 - Q_2)$ et la somme $(P_1 + P_2)$ se rapportant aux deux constituants du système, commutent et peuvent ainsi être fixées de façon aussi précise par un montage expérimental. Nous pouvons par suite prédire Q_1

ou P_1 si Q_2 ou P_2 ont été respectivement déterminés par une mesure directe. Le point essentiel ici et que des mesures de genre exigent des dispositifs expérimentaux qui s'excluent mutuellement. Bohr réécrivait encore en résumé : " De notre point de vue, nous voyons maintenant que l'énoncé du critère de réalité physique proposé par Einstein, Podolsky et Rosen contient une ambiguïté relative au sens de l'expression " sans perturber le système en aucune façon" ; évidemment, il n'est pas question dans un tel cas d'une perturbation mécanique du système étudié pendant le dernier stade critique du processus de mesure. Mais, même à ce stade, la question essentielle est celle d'une influence sur les conditions mêmes qui définissent les types possibles de prédictions relatives au comportement futur du système. Comme ces conditions constituent un élément inhérent à la description de tout phénomène auquel le terme "réalité physique" peut être attaché à juste titre, nous voyons que l'argumentation des auteurs ne leur donne pas le droit de conclure que la description par la mécanique quantique est essentiellement incomplète. Au contraire, cette description, comme il ressort de la discussion précédente, peut être caractérisée comme une utilisation rationnelle de toutes les possibilités d'une interprétation non ambigüe des mesures qui soit compatible en théorie quantique avec l'interaction finie et incontrôlable entre objets et instruments de mesure. En fait, c'est seulement parce que deux dispositifs expérimentaux quelconques, permettant de définir sans ambiguïté des grandeurs physiques complémentaires, s'excluent mutuellement, qu'il y a place pour des nouvelles lois physiques dont la coexistence pourrait à première vue paraître inconciliable avec les principes fondamentaux de la science. C'est justement cette situation entièrement nouvelle dans la description des phénomènes physiques que la notion de complémentarité cherche à préciser".

La localité "rigide", la non séparabilté des états quantiques

Comme on l'a déjà vu, le paradoxe EPR laissait entendre suivant le critère de réalité que la mécanique quantique est incomplète et qu'il faudrait la compléter par une théorie qui contiendrait des variables dites variables cachées dont la mécanique quantique n'a pas tenu compte et que ses calcules statistiques, sont une certaine moyenne sur ces variables calculées cette théorie a été choisit de manière à faire ressortir les prédictions de la mécanique quantique. On appelle ces tentatives théories à variables supplémentaires. Ces variables cachées pourraient être des variables dynamique évaluent dans le système physique. En continuité et conformité

avec l'esprit de la causalité classique qui induit avec elle une localité des phénomènes physique : Ces variables cachées est un caractère locale. Cette propriété de localité permis à J.S.Bell de déduire des inégalités de Bell. La théorie de Bell stipule que :

- Une théorie à variables supplémentaires locales est contrainte par des inégalités de Bell.

- Certaines prédictions de la mécanique quantique viole ces inégalités et par conséquent la mécanique quantique et incompatible avec les théories à variables supplémentaires locales.

Dans ce que suit repensons à nouveau le paradoxe EPR dans sa version simplifiée par Bell

Schema d'experience de pensée du paradoxe EPR

Une source S émet une paire de photons de différentes fréquences, ν_1 et ν_2 se propageant dans des directions opposées le long de l'axe z.

Supposons que la polarisation de la paire de photons est décrite par l'état

$$|\psi\left(\nu_1,\nu_2\right)\rangle = \frac{1}{\sqrt{2}}\left(|x,x\rangle + |y,y\rangle\right)$$

Où $|x\rangle$ et $|y\rangle$ sont les états de polarisation linéaires. Cet état, dit état de Bell, est remarquable puisqu'il ne peut être factorisé en un produit des états de chacun des états de photons. Dans ce cas on ne peut attribuer un état bien défini à chaque photon. Il est dit état intriqué vu cette impossibilité de factorisation (en anglais Entangled state).

Nous effectuons des mesures de polarisation sur les deux photons avec des analyseur I et II (voir fig 1)

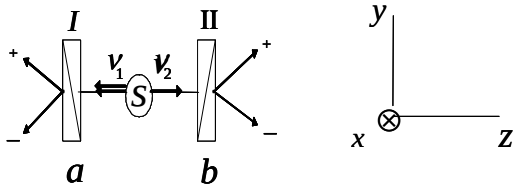


figure 1

L'analyseur$I$ est orienté dans la direction $\vec{a}$ est suivi par deux detecteurs donnant les resultats + et − suivant que la polarisation du premier photon est soit parallèle ou orthogonale à $\vec{a}$. L'analyseur II agit de la même sorte suivant la direction $\vec{b}$.

Qeulles sont les prédictions de la mécanique quantique pour ces mesures de polarisations effectuées soit sur 1 seul photon ou en coïncidence ?

Soient $P_{\pm}(\vec{a})$ et $P_{\pm}\left(\vec{b}\right)$ respectivement probabilités d'avoir $\pm$ suivant $\vec{a}$ pour le photon ν_1 et d'avoir $\pm$ suivant $\vec{b}$ pour le photon ν_2.

Les prédictions de la mécanique quantique sont

$$\begin{aligned} P_{+}(\vec{a}) &= P_{-}(\vec{a}) = \frac{1}{2} \\ P_{+}\left(\vec{b}\right) &= P_{-}\left(\vec{b}\right) = \frac{1}{2} \end{aligned}$$

Soient $P_{\pm\pm}\left(\vec{a},\vec{b}\right)$ les différentes probabilités d'avoir différents résultats suivant $\vec{a}$ et $\vec{b}$ sur les deux photons $\nu_1$et ν_2 en coïncidence. Les prédictions de la mécanique quantique sont

$$\begin{aligned} P_{++}\left(\vec{a},\vec{b}\right) &= P_{--}\left(\vec{a},\vec{b}\right) = \frac{1}{2}\cos^2\left(\vec{a},\vec{b}\right) \\ P_{+-}\left(\vec{a},\vec{b}\right) &= P_{-+}\left(\vec{a},\vec{b}\right) = \frac{1}{2}\sin^2\left(\vec{a},\vec{b}\right) \end{aligned}$$

Il n'est pas difficile de s'assurer que les différents résultat de mesure sont corrélés.

En effet considérons le cas où les analyseurs sont parallèle $\left(\vec{a},\vec{b}\right) = 0$. Les prédictions de la mécanique quantique donnent

$$\begin{aligned} P_{++}(\vec{a},\vec{a}) &= P_{--}(\vec{a},\vec{a}) = \frac{1}{2} \\ P_{+-}(\vec{a},\vec{a}) &= P_{-+}(\vec{a},\vec{a}) = 0 \end{aligned}$$

C'est à dire que si la polarisation du photon $\nu_1$est mesurée dans la direction $\vec{a}$ la polarisation du photon ν_2 est certainement dans la direction $\vec{a}$ et le même pour le résultat $-$.

Donc pour de polariseurs parallèles il y a une corrélation totale entre les résultats aléatoires des mesures de polarisations sur chacun des photons. Définissons alors une fonction de corrélation donnée par :

$$E\left(\vec{a},\vec{b}\right) = P_{++}\left(\vec{a},\vec{b}\right) + P_{--}\left(\vec{a},\vec{b}\right) - P_{+-}\left(\vec{a},\vec{b}\right) + P_{-+}\left(\vec{a},\vec{b}\right)$$

Les prédictions de la mécanique quantique donnent

$$E_{QM}\left(\vec{a},\vec{b}\right)=\cos 2\left(\vec{a},\vec{b}\right)$$

En particulier

$$\text{si } \left(\vec{a},\vec{b}\right)=0 \text{ alors } E_{QM}\left(\vec{a},\vec{b}\right)=1$$

donc une totale corélation.

En conclusion, la mécanique quantique suggère que malgré que les résultas de mesures individuelles sont aléatoires ces résultats aléatoires sont corrélés.

Quelle est la difficulté ? !

Essayons de penser cette expérience autrement. Au lieu d'imaginer une mesure simultannée dans les polariseurs I et II, supposons qu'on ait effectué d'abord celle du photon $\nu_1$et que le résultat de la mesure est $+$. Ce résultat à une probabilité $P_+(\vec{a})=\frac{1}{2}$.Utilisons maintenant le postulat de réduction du paquet d'ondes. Donc juste aprés la mesure :

$$\begin{aligned}|\psi(\nu_1,\nu_2)\rangle \quad &\rightarrow \quad \left|\dot{\psi}(\nu_1,\nu_2)\right\rangle \\ &\qquad |\psi(\nu_1)\rangle \overset{\text{projection}}{\rightarrow} \quad |\vec{a}\rangle\end{aligned}$$

On trouve

$$\left|\dot{\psi}(\nu_1,\nu_2)\right\rangle=|\vec{a},\vec{a}\rangle$$

Ce qui veut dire qu'immédiatement après la mesure le photon $\nu_1$est dans l'état $|\vec{a}\rangle$ ce qui est trés clair puisqu'on a effectué une mesure sur lui.

La surprise est que le photon qui n'est pas encore en interaction avec le polariseur II est déjà dans l'état $|\vec{a}\rangle$. Ce résultat surprenant donne suivant la loi de Malus lors de la mesure de la polarisation du photon ν_2 dans la direction $\vec{b}$.

$$P_{++}\left(\vec{a},\vec{b}\right)=\frac{1}{2}\cos^2\left(\vec{a},\vec{b}\right)$$

Ce qui est la prédiction de la mécanique quantique. Mais pose une difficulté ? !

Comment se fait-il que l'état du photon ν_2 est projecté suivant $\vec{a}$ d'une manière instantanée quelque soit les distances entre les photons ν_1,ν_2 au moment de la mesure faite sur ν_1.

Cette image parait contredire la causalité relativiste. Ce qui se passe dans une région spatio-temporelle ne peut influencer les regions spatio-temporelles séparées par des intervalles

relativistes genre espace. Un exemple de cette violation de localité "rigide" est donnée par l'exemple de la téléportation quantique (voir ci dessous).

2.1.6 Inégalités de Bell

Ces corrélations entre des mesures effectuées sur deux systèmes distants qu'étaient auparavant en interaction existent aussi dans le monde classique. Prenons l'exemple d'un objet qui avait une impulsion nulle puis se sépare en deux parties suite à une quelconque répulsion intérieure ; ses deux parties gardent leurs impulsions égales et opposées en évolution libre.Ces impulsions restent corrélées puisque sa valeur à chaque instant dépend de sa valeur initiale.

La théorie à variables cachées ou paramètres supplémentaires tente de rapprocher le paradoxe EPR de cette situation classique en injectant via le "critère de réalité" EPR ces paramètres en plus.

Le fait d'avoir + pour le photon υ_1 nous donne la certitude d'avoir + pour le photon υ_2 ou de même pour $(-,\upsilon_1)$ et $(-,\upsilon_2)$ invite d'après ce "critère de réalité" à ajouter une telle propriété dont la mécanique quantique ne dit aucun mot.

Ces théories prétendent alors expliquer ces corrélations suivant ce schéma classique en rajoutant ces paramètres et les résultats statistiques de la mécanique quantique seraient alors retrouvés quand on moyenne sur ces variables supplémentaires. Cette manière de voir les prédictions statistiques ne contredire pas de la mécanique quantique et conforte dans l'explication de paradoxe EPR. Malheureusement, comme on va le voir de telles théories à variables supplémentaires locales obéissent à des inégalités de Bell auxquelles ma mécanique quantique n'obéit pas. Le conflit reste installé et c'est l'expérience qui touchera (Expérience d'Alain Aspect).

Inégalités de Bell

Ces théories introduisent leurs variables supplémentaires comme un ensemble λ et leur confèrent une distribution de probabilité

$$\rho(\lambda) \geq 0 \qquad \int d\lambda \rho(\lambda) = 1$$

Ces variables entrent en jeu dans les résultats de l'expérimentation

$A(\lambda, a) = \pm 1$ pour l'analyseur I(dans l'orientation a).

$B(\lambda, a) = \pm 1$ pour l'analyseur II (dans l'orientation b).

La théorie à variables supplémentaires est complètement déterminée par la donnée $\rho(\lambda)$, $A(\lambda, a)$, $B(\lambda, b)$ .Les prédictions de la mécanique quantique s'écrivent par exemple

$$\begin{aligned} P_+(a) &= \int d\lambda \rho(\lambda) \left[\frac{A(\lambda, a)+1}{2}\right] \\ P_{+-}(a,b) &= \int d\lambda \rho(\lambda) \left[\frac{A(\lambda, a)+1}{2}\right] \left[1 - \frac{B(\lambda, b)}{2}\right] \\ E(a,b) &= \int d\lambda \rho(\lambda) A(\lambda, a) B(\lambda, b) \end{aligned}$$

Soit les quantités

$$\begin{aligned} S &= A(\lambda, a) B(\lambda, b) - A(\lambda, a) B\left(\lambda, \grave{b}\right) + A(\lambda, \grave{a}) B(\lambda, b) + A(\lambda, \grave{a}) B\left(\lambda, \grave{b}\right) \\ &= A(\lambda, a)\left[B(\lambda, b) - B\left(\lambda, \grave{b}\right)\right] + A(\lambda, \grave{a})\left[B(\lambda, b) + B\left(\lambda, \grave{b}\right)\right] \\ S\left(\lambda, a, \grave{a}, b, \grave{b}\right) &= \pm 2 \end{aligned}$$

Alors

$$-2 \leq \int d\lambda \rho(\lambda) S\left(\lambda, a, \grave{a}, b, \grave{b}\right) \leq 2$$

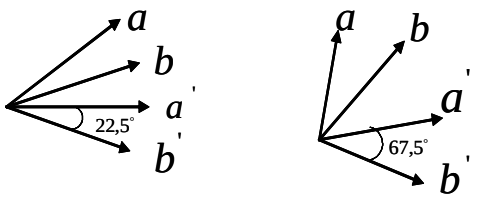
On aura l'inégalité de Bell suivant

$$-2 \leq S\left(\lambda, a, \grave{a}, b, \grave{b}\right) \leq 2$$

Où

$$S\left(a, \grave{a}, b, \grave{b}\right) = E(a, b) - E\left(a, \grave{b}\right) + E(\grave{a}, b) + E\left(\grave{a}, \grave{b}\right)$$

La mécanique quantique viole ces inégaités, par exemple pour



$$S_{QM} = 2\sqrt{2}$$

Le conflit entre la mécanique quantique et les théories à variables supplémentaires locales émergent surtout de :

- les systèmes physique separés (sans interaction) ont des réalités physiques sépareés.
- les paramètres qui définissent la théorie $\{A, B, \rho\}$ sont locales.

Chapitre 3

De l'information classique à l'information quantique

Le vingtième siècle a connu d'énormes développements scientifiques et technologiques. On a assisté à deux grandes découvertes scientifiques qui sont la relativité et la mécanique quantique et en parallèle nous avons eu deux principaux développements : la télécommunication de l'information et l'informatique. Toutes les deux ont des bases physiques, i.e., véhiculer ou effectuer sur des composants physiques. Ces composants sont en général considérés du point de vue de l'information comme des systèmes physiques obéissant aux règles de la physique classique et de ce fait une question naïve s'impose : que deviennent ces processus d'information si on les véhicule ou on les effectue sur des systèmes quantiques ? La réponse à cette question a germé lentement à travers les dernières décennies et elle a été tributaire de multiples domaines de la recherche scientifique telles :

- La mécanique quantique en comprenant de plus en plus les bases de la mécanique quantique par ses effets étranges du principe de superposition en exploitant à outrance la non séparabilité des états quantiques tels les états de Bell qui reflètent une intrication quantique inouïe. Ces états très prisés ont immergés lors des grandes discussions et controverses des esprits éclairés de la physique moderne sur la complétude du formalisme quantique (paradoxe EPR, Chat de Schrödinger, etc.).

- L'information quantique : élaboration et développements des algorithmes quantiques s'effectuant sur ces machines quantiques.

- Théorie de l'information quantique : développements de la communication par une mathématisation et physicalisation des concepts selon le schéma quantique et en conséquence développement des techniques de codage et décodage des messages véhiculés sur ces supports quantiques.

Dans ce qui suit nous allons introduire quelques concepts de ce qui est l'information classique et le calcul classique puis de les revoir dans leur contexte quantique en remplaçant le bit d'information, qui est l'élément fondamental de leurs processus, par un bit quantique qu'on appellera qubit et ce qu'on appellera aujourd'hui calcul quantique et information quantique.

3.1 Du calcul classique au calcul quantique

3.1.1 Calcul classique

L'information est le support formel d'un message susceptible d'être représenté par un codage afin d'être conservé, traité ou communiqué. L'informatique est la science de traitement de cette information dans les domaines scientifiques, techniques, économiques et sociaux. Une donnée est la représentation de cette information sous forme codée destinée à faciliter le traitement. En informatique, il est possible de définir et de décrire les données d'entrée et les résultats de sortie. Le passage des données en résultats est décomposé e une suite d'opérations élémentaires dont chacune peut être exécutée sur une machine. Le calcul proportionnel naïf est basée sur les valeurs de vérité des propositions logique muni des opérations simples sont le "et", "ou", "non", et "=", qu'on appelle les connecteurs logiques. A partir de ces opérations on peut construire des règles de déduction. Ces outils permettent une construction raisonnée des programmes informatiques. La logique interne des ordinateurs actuels est basée sur la logique booléenne.

Algèbre de Boole

On appelle algèbre de Boole tout ensemble E muni de deux opérations internes $\bullet$ et $\oplus$ et une application involutive dite complémentaire $(x \to \overline{x})$. Chacune des opérations est associative et commutative et chacune est distributive par rapport à l'autre. Chacune des opérations a

un élément neutre. Chacun élément de E est idempotent pour ces opérations internes.Ces opérations vérifient les axiomes de complémentarité et les lois de Morgan.

Exemple de l'algèbre des circuits électroniques : $E = \{0, 1\}$ muni de l'opération . et + et on a

$$\begin{aligned} x+1 &= 1, x+0 = x, x+x = x, x+\overline{x} = 1, \overline{x+y} = \overline{x}.\overline{y}, \overline{0} = 1 \\ x.1 &= x, x.0 = 0, x.x = x, x.\overline{x} = 0, \overline{x.y} = \overline{x} + \overline{y}, \overline{1} = 0 \end{aligned}$$

La table de vérité de cette algèbre est la suivante

x	y	$\overline{x}$	$x \cdot y$	$x+y$
1	1	0	1	1
1	0	0	0	1
0	1	1	0	1
0	0	1	0	0

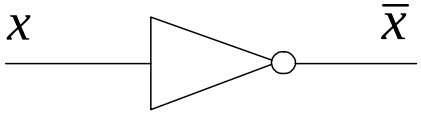
Cette algèbre est utile pour décrire les schémas électroniques et elle sert alors l'informatique puisque les ordinateurs sont construits à base d'électronique. On affecte à $x = 0$ quand le courant ne passe pas et $x = 1$ quand le courant passe. Cette manière permet de visualiser cet état physique du courant sous forme de bit d'information $(0, 1)$. Les principaux circuits sont :

Operation NON

C'est une opération à une seule variable et elle est notée $NONx$

$$NONx = \overline{x}$$

Elle est représentée par un symbole graphique



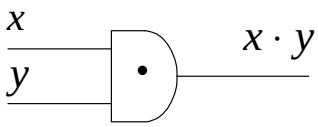
porte logique NON

Opération ET

C'est une opération à deux variables et elle est notée $xETy$

$$xETy = x \cdot y$$

Elle est représentée par le symbole graphique



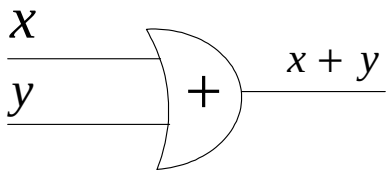
porte logique ET : AND

Opération OU

C'est une opération à deux variables, et elle est notée $xOU\ y$

$$xOUy = x + y$$

Elle est représentée par le symbole graphique



porte logique OU : OR

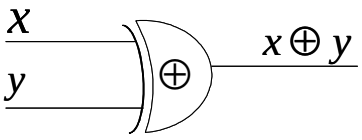
On construit d'autres circuits classiques à partir des précédents.

Opération XOR

L'opération XOR notée $\oplus$ définie par

$$x \oplus y = \overline{x}.y + x.\overline{y}$$

Elle est représentée par le symbole graphique

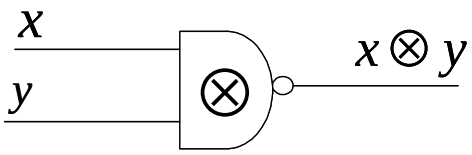


Opération NAND

L'opération $NAND$ notée $\otimes$ définie par

$$x \otimes y = \overline{x} + \overline{y}$$

Elle est représentée par le symbole graphique

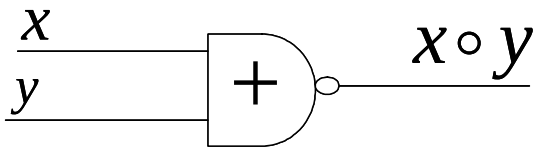


Opération NOR

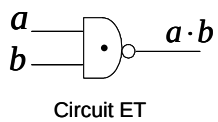
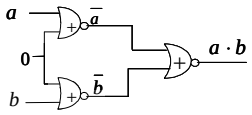
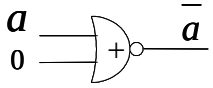
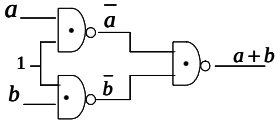
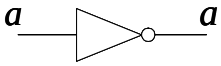
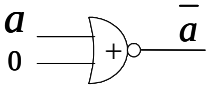
L'opération NOR notée $\odot$ définie par

$$x \odot y = \overline{x}.\overline{y}$$

Elle est représentée par le symbole graphique

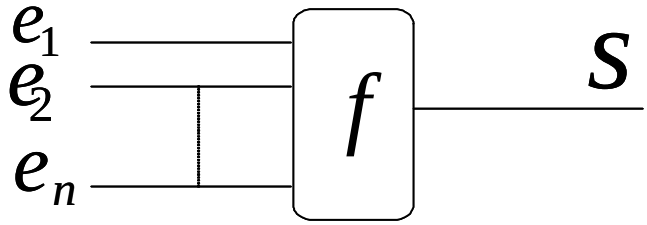


On montre que $NAND$ et NOR génèrent les trois opérations de base de l'algèbre de Boole et en plus, ils sont simplement réalisables avec un minimum de composants électroniques de type transistor et diode. En effet

Opérateur de base	Réalisation de l'opérateur en NAND ou en NOR
 Circuit ET	
 Circuit OU	
 Circuit NON	

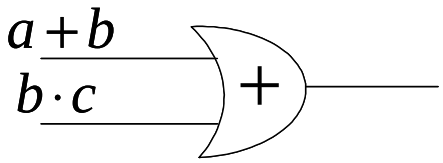
Circuit logique

Un circuit logique est un système de logique séquentielle où la valeur de sortie dépend des valeurs d'entrée.



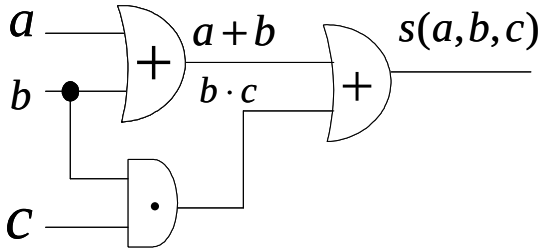
Pour calculer sa valeur de sortie à partir d'un schéma de circuits logiques, il suffit d'indiquer à la sortie de chaque opération (circuit de base) la valeur booléenne en cours. Nous obtenons à la fin une valeur booléenne que l'on simplifie à l'aide des axiomes ou des théorèmes de l'algèbre de Boole.

Exemple : $S(a, b, c) = (a + b) + (b.c)$



A l'inverse, la création de circuits logiques à partir d'une sortie à n entrées est aussi simple. Dans la fonction de sortie, on exprime graphiquement chaque opération par un circuit, les entrées étant les opérandes de l'opération. En répétant l'action sur tous les opérateurs, on construit un graphique de circuit logique associé à la fonction de sortie.

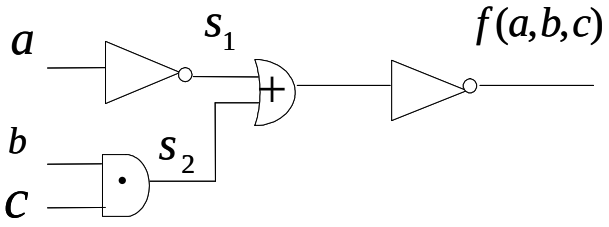
Exemple : pour $S(a, b, c) = (a + b) + (b.c)$ on a



On a deux types de circuits :

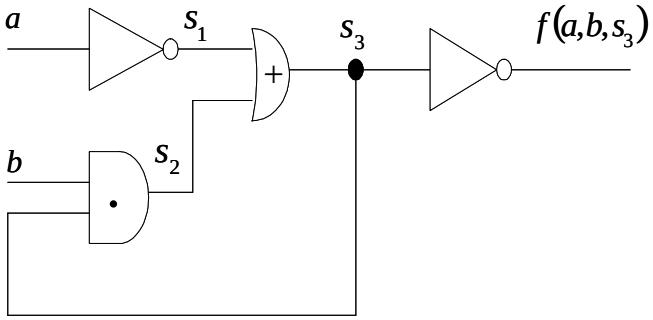
Le circuit combinatoire : est un circuit logique à n entrées dont la sortie ne dépend uniquement que des entrées

Exemple



Le circuit à mémoire : est un circuit logique à n entrées dont la sortie dépend à la fois des entrées et des états antérieurs déjà mémorisés.

Exemple :



Parmi on trouve :

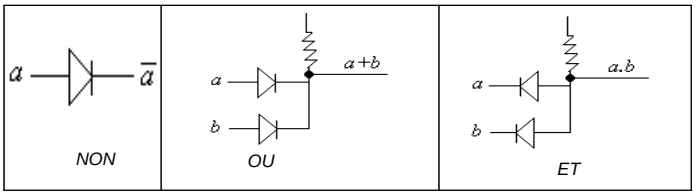
Circuit combinatoire : additionneur, multiplexeur, décodeur, décaleur, comparateur.

Circuit à mémoire : bascules logiques, registres.

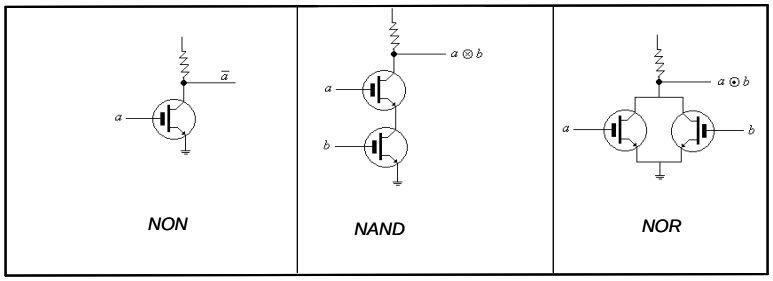
Quelques réalisations électroniques de circuits logiques

Voici quelques exemples de schémas électroniques de base des réalisation physiques possibles de différentes opérations de Boole.

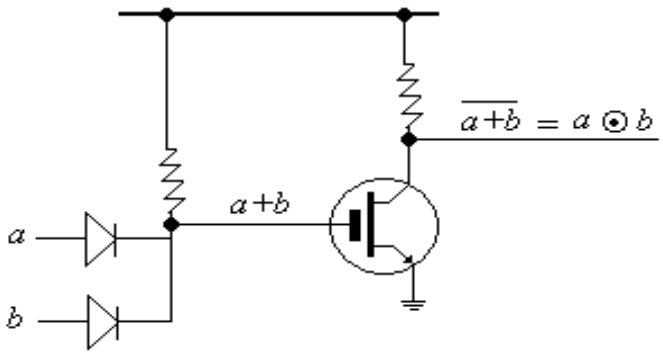
Circuits (ET, OU , NON) élaborés à partir de diodes :



Circuits (NOR, NAND , NON) élaborés à partir de transistor MOS :



Circuit NOR à partir de transistor et de diodes :



3.1.2 Calcul quantique

La physique quantique insiste sur le phénomène de superposition et décrit les systèmes physiques quantiques se trouvant dans une superposition d'états. Lors d'une mesure de l'état du système, chaque état possible est observé avec une certaine probabilité, fonction de son amplitude. L'objet du calcul quantique est de profiter de cette superposition d'états pour construire de nouveaux algorithmes dits algorithmes quantiques. Les ordinateurs quantiques n'existent pas à cause des difficultés de réalisations sur lesquelles butent encore les expérimentateurs de la nanotechnologie. Bien que d'âpres débats fassent les discussions des physiciens de tous bords, l'étude théorique du calcul quantique est intrinsèquement intéressante. On exposera les principes et les algorithmes les plus connus. L'informatique quantique est un exemple pertinent de l'utilisation des spécificités des modèles théoriques de la physique quantique pour le traitement et la transmission de l'information.

La grande nouveauté, depuis le début des années 1980, est la possibilité pour les physiciens de manipuler et d'observer des objets quantiques élémentaires individuels : photons, atomes, ions, etc. C'est cette possibilité de manipuler et d'observer des objets quantiques élémentaires qui est à l'origine de l'information quantique, où ces objets quantiques élémentaires permettront de construire physiquement le qubit élément fondamental de l'information quantique. Ce concept fondamental nouveau n'a pas été introduit depuis les années 1930, mais les fondateurs de la physique quantique (Bohr, Heisenberg, Schrödinger, Dirac, Planck, Einstein,...), ne seraient pas surpris par l'informatique quantique, bien que maintenant on réussisse à réaliser

qualifiées à l'époque d'expériences imaginaires. La miniaturisation croissante de l'électronique va trouver ses limites en raison des effets quantiques, qui vont devenir sûrement incontournables en dessous du nanomètre.

Dans les années 70 et 80, les premiers ordinateurs quantiques ont vu le jour par l'imagination des physiciens tels que Richard Feynman, Paul Benioff, David Deutsch ou Charles Bennett. L'idée de Feynman était d'utiliser ces phénomènes quantiques pour faire un calcul plus puissant que nos ordinateurs actuels ne puissent faire.

La mémoire d'un ordinateur classique est faite donc de bits . Chaque bit porte soit un 0 soit un 1 . La machine calcule en manipulant ces bits. Un calculateur quantique travaille par qubit. Un qubit peut porter soit un 0, soit un1, soit une superposition de 0 et 1(ou, plus exactement, il porte une distribution de phase). Le calculateur quantique calcule en manipulant ces distributions comme nous le verrons plus loin.

Un calculateur quantique pourrait être simulé à partir de toute particule pouvant avoir deux états. Ils peuvent être construit à partir de photons, ou à partir de n'importe qu'elle particule quantique ou à partir de ses propriétés tel un spin.

Le calcul quantique est un nouveau modèle théorique des procédés de calcul basés sur la notion de qubit jouissant des propriétés de superposition quantique. Il ouvre des nouvelles perspectives pour mettre au point des algorithmes efficaces pour réaliser des tâches qui étaient classiquement presque impossibles. L'exposé portera sur quelques bases du calcul quantique et décrira l'algorithme quantique de Shor pour la factorisation des grands entiers.

Définition du qubit

Un bit quantique ou "qubit" est un système physique dans une superposition de deux états, sur lequel on peut faire une mesure qui donne un des deux états, de manière probabiliste. Ce qubit se compose en fait d'une superposition de deux états de base, notés $|0>$ et $|1>$.

Description mathématique de qubit

On représente un qubit par un vecteur $|\psi\rangle$ de C^2 et de norme 1

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

où a et b sont des nombres complexes tels que

$$|\alpha|^2 + |\beta|^2 = 1$$

Le qubit est un vecteur dans un espace vectoriel à deux dimensions :

- Soientt les vecteurs $|0\rangle$, $|1\rangle$, qui forment une base

avec

$$|0\rangle = \binom{1}{0}, \qquad |1\rangle = \binom{0}{1}$$

La sphère de Bloch

Le qubit $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ peut être représenté comme point (θ, ϕ)d'une sphère unité appelée la sphère de Bloch. Définir les angles de θ et ϕ en posant $a = \cos(\theta/2)$ et $b = e^{i\phi}\sin(\theta/2)$. Ici, a est pris pour réel, ou qui peut toujours être rendu réel en multipliant $|\psi\rangle$ par un facteur global de phase. Alors $|\psi\rangle$ est le represente par le vecteur unité $(\cos(\phi)\sin(\theta),\ \sin(\phi)\sin(\theta),\ \cos(\theta))$ appelé le vecteur de Bloch.

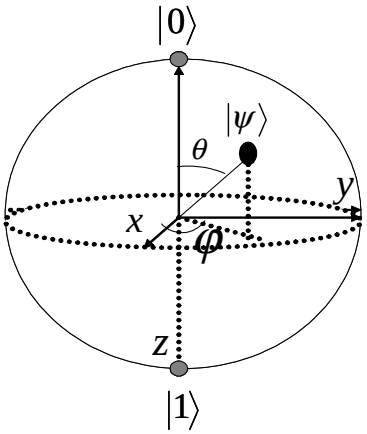
Alors on peut écrire le qubit $|\psi\rangle$ comme suit

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\right)$$

Où θ, ϕ et γ sont les nombres réels. les nombres $0 \leq \theta \leq \pi$ et $0 \leq \phi \leq 2\pi$ définissent un point sur une sphère de trois dimention.

Les états de qubit avec des valeurs arbitraires de γ sont représentés par le même point sur le sphère de Bloch parce que le facteur $e^{i\gamma}$ n'a aucun effet sur l'observable, et nous pouvons donc écrire

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle$$



La sphère de Bloch

Description physique de qubit

Un qubit est un système physique dans une supperposition de deux états. Alors le qubit est une unité d'information quantique, celle-ci est décrite par un vécteur d'état dans un système mécanique quantique à 2 niveaux.

Exemple

- Un photon dont on mesure la polorisation : elle est soit verticale soit horizontal

- Un éléctron dont on mesure le spin : il est soit "up" soit "down".

- $\{|0\rangle, |1\rangle\}$est une base orthogonale dans l'espace de Hilbert C^2. L'opération NOT est définie par

$$|0\rangle \to |1\rangle, \qquad |1\rangle \to |0\rangle$$

Trouvons l'opérateur unitaire U_{NOT} qui met en application NOT en ce qui concerne la base $\{|0\rangle, |1\rangle\}$.

(1) On définira :

$$|0\rangle = \binom{1}{0}, \qquad |1\rangle = \binom{0}{1} \ .$$

Trouvons la representation matricielle de U_{NOT} pour cette base évidemment,

$$U_{NOT} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

avec

$\langle 0|\,0\rangle = \langle 1|\,1\rangle = 1$ et $\langle 0|\,1\rangle = \langle 1|\,0\rangle = 0$. Pour la base standard nous trouvons

$$U_{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

(2) On définira la base de Hadamard par

$$|0\rangle = \frac{1}{\sqrt{2}}\binom{1}{1}, \qquad |1\rangle = \frac{1}{\sqrt{2}}\binom{1}{-1}.$$

Trouvons la representation matricielle de U_{NOT} pour cette base

$$U_{NOT} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Ainsi nous voyons que les représentations respectives de matrice pour les deux bases sont différentes.

- La transformation de Hadamard est une opération de 1-qubit dénotée par H, et exécute le suivant transforment

$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Trouver l'opérateur unitaire U_H qui met en application H en ce qui concerne la base $\{|0\rangle, |1\rangle\}$ .Evidemm

$$\begin{aligned} U_H &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1| \\ &= \frac{1}{\sqrt{2}}|0\rangle(\langle 0| + \langle 1|) + \frac{1}{\sqrt{2}}|1\rangle(\langle 0| - \langle 1|) \end{aligned}$$

L'opérateurU_H est unitaire et l'inverse est donné par

$$U_H^{-1} = U_H^* = U_H,$$

Pour la base standard nous trouvons

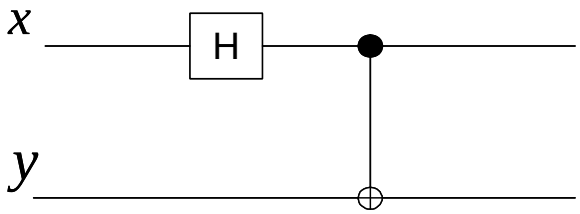
$$U_H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Pour la base de Hadamard nous trouvons

$$U_H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

3.1.3 Les états de Bell

Soit le circuit suivant :



Si

$$x \begin{cases} x = |0\rangle \\ y = |0\rangle \end{cases} \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$
$$\xrightarrow{CNOT} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

Si

$$x \begin{cases} x = |0\rangle \\ y = |1\rangle \end{cases} \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$
$$\xrightarrow{CNOT} \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$$

Si

$$x \begin{cases} x = |1\rangle \\ y = |0\rangle \end{cases} \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$
$$\xrightarrow{CNOT} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

Si

$$x \begin{cases} x = |1\rangle \\ y = |1\rangle \end{cases} \overset{H}{\rightarrow} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
$$\overset{CNOT}{\rightarrow} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

On les appelle les états de Bell( ) états EPR. On les écrit alors comme

$$|B_{xy}\rangle = \frac{|0, y\rangle + (-1)^x \left|1, \bar{y}\right\rangle}{\sqrt{2}}$$

Où $\bar{y} \equiv$ negation de y.

3.1.4 Les registres quantiques

Un registre quantique se compose de réseaux de qubits. C'est un système ayant ainsi les propriétés de l'informatique quantique. Ceux-ci pourrait être fabriqués en laboratoire. Une forme possible des registres quantique est de se servir d'une molécule dont chaque atome constitue un qubit.

De façon plus scientifique, un registre quantique est définit comme étant un vecteur normalisé dans H_n (avec n facteurs, n étant le nombre de qbits constituant le registre). Un registre peut donc être représenter par une combinaison linéaire des vecteurs de base $\{|x>: x \in \{0,1\}^n\}$.

$$\begin{aligned} |v\rangle &= \sum \alpha_x |x\rangle \\ x &\in \{0,1\}^n \end{aligned}$$

Où

$$\sum_x |\alpha_x|^2 = 1$$

Le registre quantique de deux qubits

L'état d'un registre de 2 qubits est un vecteur dans un espace à 4 dimention, la base de ce registre est représenée par 4 états

$$\{|00\rangle\,,\ |01\rangle\,,\ |10\rangle\,,\ |11\rangle\}\,.$$

Alors l'état de ce registre est décrit par

$$|\psi\rangle = \alpha\,|00\rangle + \ \beta\,|01\rangle + \gamma\,|10\rangle + \delta\ \ |11\rangle\,.$$

Avec

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

On remarque que l'état d'un registre est une superposition d'états de base de cette registre.

Le registre quantique de n qubits

On représente le registre de n qubits par un vecteur dans un espace de 2^n dimension ; la base de ce registre est une collection de 2^n états ;

$$\{|00...0\rangle\,,\ |00...1\rangle\,,\ |00...10\rangle\,,...,\ |11...11\rangle\}$$

Et on présente aussi cette base par :

$$\{|0\rangle\,,\ |1\rangle\,,\ |2\rangle\,,...,\ |2^n-1\rangle\}$$

Alors :

$$|\psi\rangle = \alpha_0\,|0\rangle + \alpha_1\,|1\rangle + \alpha_2\,|2\rangle + ... + \alpha_{2^n-1}\,|2^n-1\rangle\,.$$

Avec

$$\left|\alpha_0^2\right| + |\alpha_1|^2 + |\alpha_2|^2 + ... + \left|\alpha_{_{2^n-1}}\right|^2 = 1.$$

3.1.5 La mesure sur les qubits

La mesure sur un qubit

On a :

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

Pour mesurer la valeur 0, on projecte l'état qui correspond à cett valeur sur l'état quantique $|\psi\rangle$

$$\begin{aligned} \langle 0 \mid \psi \rangle &= \alpha \langle 0 \mid 0 \rangle + \beta \langle 0 \mid 1 \rangle \\ &= \alpha \end{aligned}$$

Avec $\langle 0 \mid 0 \rangle = 1$ et $\langle 0 \mid 1 \rangle = 0$

Alors la probabilitée de trouvée cette valeur est :

$$P = |\langle 0 \mid \psi \rangle|^2 = \langle \psi \mid 0 \rangle \langle 0 \mid \psi \rangle = \alpha^* \alpha = |\alpha|^2$$

La mesure sur deux qubits

On a :

$$|\psi\rangle = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle$$

Pour mesurer l'état $|00\rangle$, on projecte cette état sur $|\psi\rangle$

$$\begin{aligned} \langle 00 \mid \psi \rangle &= \alpha \langle 00 \mid 00 \rangle + \beta \langle 00 \mid 01 \rangle + \gamma \langle 00 \mid 10 \rangle + \delta \langle 00 \mid 11 \rangle \\ &= \alpha \end{aligned}$$

Avec : $\langle 00 \mid 00 \rangle = 1$, et $\langle 00 \mid 01 \rangle = \langle 00 \mid 10 \rangle = \langle 00 \mid 11 \rangle = 0$

Alors la probabilitée est :

$$P = |\langle 00 \mid \psi \rangle|^2 = \langle \psi \mid 00 \rangle \langle 00 \mid \psi \rangle = \alpha^* \alpha = |\alpha|^2$$

3.1.6 Opérations sur les qubits et les portes quantiques

Pour décrire une opération sur un qubit, il est possible de passer par une matrice unitaire 2×2. Il est alors possible de développer cette opération sur la base constituée des matrices de Pauli. Ces opération sont les suivantes :

Opération unitaire I

On a une matrice unitaire I

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

La représentation de cette opération sur un qubit est représentée par la tronsformation suivante

$$|0\rangle \rightarrow |0\rangle\,, \qquad |0\rangle \rightarrow |0\rangle$$

Opération X

On a une matrice de Pauli X

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

La projection de cette matrice sur un qubit est décrite par la transformation suivante

$$|0\rangle \rightarrow |1\rangle\,, \qquad |1\rangle \rightarrow |0\rangle$$

Opération Y

On a une matrice de Pauli Y

$$Y = \begin{pmatrix} 0 & -i \\ i & 1 \end{pmatrix}$$

La projection de cette matrice sur un qubit est décrite par la transformation suivante

$$|0\rangle \rightarrow -i\,|1\rangle\,, \qquad |1\rangle \rightarrow i\,|0\rangle$$

Opération Z

On a une matrice de Pauli Z

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

La projection de cette matrice sur un qubit est décrite par la transformation suivante

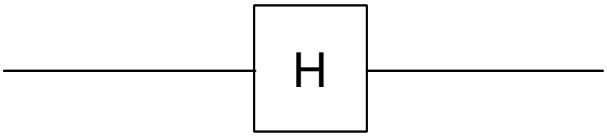
$$|0\rangle \rightarrow |0\rangle\,, \qquad |1\rangle \rightarrow -\,|1\rangle$$

La porte de Hadamard

On représente la matrice de Hadamard par

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Et



La porte de Hadamard

Le principe de fonctionnement de cette porte est de combiner les états initiaux à partir d'une transformation (voir intrication des états). Cette transformation est la suivante :

$$|0\rangle \ \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |1\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Cette transformation, permet, d'effectuer une superposition d'états pondérés de façon égale,à partir d'un état avec |0>. Celle-ci se justifie par l'utilisation des matrices définies précédemment, de la manière suivante :

$$H = \frac{(X+Y)}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

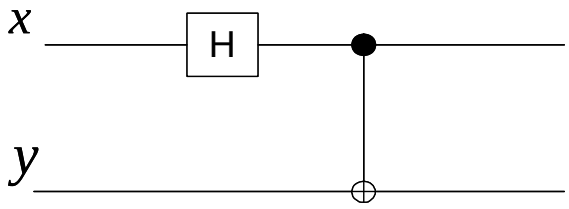
La porte NOT Contrôlée

C'est une porte agissant sur deux qubit, qubit "cible" et qubit "contrôle",

Alors l'opération NOT contrôlée est représentée par la transformation suivante

$$\begin{aligned} |11\rangle &\rightarrow |10\rangle, \quad |00\rangle \rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle, \quad |10\rangle \rightarrow |11\rangle \end{aligned}$$

Et



La porte de C_NOT

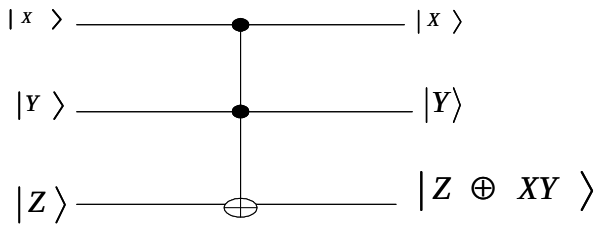
Le principe de fonctionnement de cette porte est d'échanger les états |0> et |1> du qubit de destination si le qubit de contrôle est dans l'état |1>.

La porte de Toffoli

C'est une porte NOT doublement contrôlée, elle est représentée par la transformation suivante

$$|110\rangle \rightarrow |111\rangle\,, \quad |111\rangle \rightarrow |110\rangle$$
$$\text{et } |abc\rangle \rightarrow |abc\rangle \text{ si } ab \neq 11$$

Et



La porte de Toffoli

Cette porte logique n' a d'effet que si les deux qubits de contrôle sont à l'état |1>.

Les régles des circuits quantiques

Les circuits quantiques présentent en général des propriétés differentes du cas classique, leurs régles sont les suivantes :

1- pas de boucles ou dit que : les circuits quantiques sont acyclique

2- on ne peut pas joindre deux fils pour obtenir un seul fil on dit : on n'a pas de FANIN.

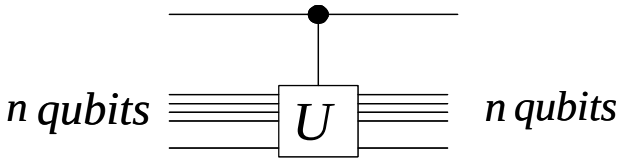
3- l'opération inverse Fanout (qui permet de faire plusieurs copies) n'est pas possible.

On introduit autant de portes quantiques qu'on veut, par exemple, on peut définir une porte U agissant sur plusieurs qubits, n qubits (U est donc une matrice unitaire). Nous pouvons en plus contrôler U par un qubit nous obtenons alors une porte quantique dite controlled-U qui fonctionne comme suit

Si le qubit contrôle est $|0\rangle$ rien ne se passe

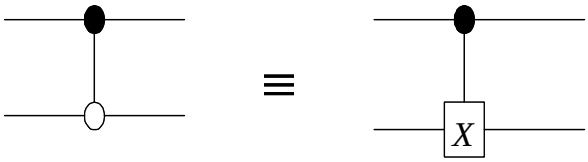
Si le qubit contrôle est $|1\rangle$ alors U sera appliqueé au n qubits cibles.

Nous dessinons alors



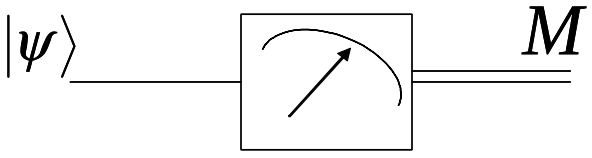
Controlled $-$ U

Exemple $CNOT$ devient



$CNOT$

Il existe aussi une opération importante qui est la mesure qu'on représentera par un symbole qui convertit le qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ en un bit classique probabiliste M noté $\underline{\underline{\mathrm{M}}}$ qui est 0 avec une probabilité $= |\alpha|^2$ et 1 avec une probabilité $= |\beta|^2$



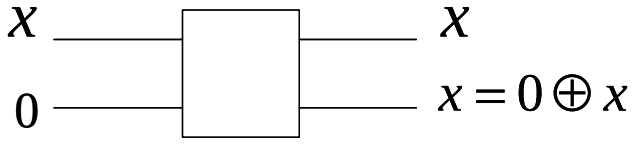
Ci*rcuit quantique pour une mesure*

Théorème de non clonage quantique

Existe-t-il un circuit copiant un qubit ?

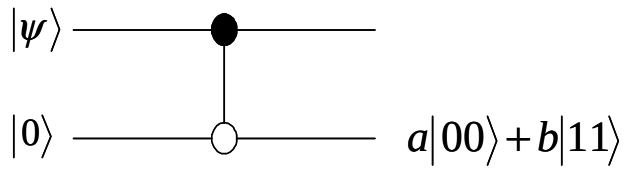
Classiquement on copie un bit comme suit :

Soit le CNOT classique (x état quelconque)



En quantique que devient cette procedure

$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ état quelconque



$$\begin{aligned} |\psi\rangle\,|0\rangle &= |\psi,0\rangle \overset{CNOT}{\rightarrow} \alpha\,|00\rangle + \beta\,|11\rangle \\ |\psi,0\rangle &= \alpha\,|00\rangle + \beta\,|11\rangle \\ \overset{CNOT}{\rightarrow} \alpha\,|00\rangle + \beta\,|11\rangle &\neq |\psi\rangle \end{aligned}$$

Cette propriété de ne pas pouvoir copie un qubit est connue sous le nom de " no-cloning theorem"

Exemple de la téléportation quantique

L'ideé de la téléportation quantique et de déplacer un état quantique sans utiliser de lien entre l' émetteur et le recepteur. Elle utilise la corrélation des états de Bell (Entanglement de la paire).

Exemple :

Soit un état inconnu

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

Et $|\beta_{00}\rangle$ la paire de Bell

L'état input est donné par

$$\begin{aligned} |\psi_0\rangle &= |\psi\rangle |\beta_{00}\rangle \\ &= \frac{1}{\sqrt{2}} (\alpha |0\rangle + \beta |0\rangle) (|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}} (\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle)) \end{aligned}$$

On sous-entend que dans $|\beta_{00}\rangle$ un 2-qubits, le premier est celui de l'envoyeur (Alice) et le deuxième est celui du recepteur (Bob).

Alice envoie son qubit à travers un CNOT controlé par $|\psi\rangle$ .Alors

$$\begin{aligned} |\psi_0\rangle &\overset{CNOT}{\rightarrow} |\psi_1\rangle \\ |\psi_1\rangle &= \frac{1}{\sqrt{2}} (\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|10\rangle + |01\rangle)) \end{aligned}$$

puis elle fait passer le qubit du contrôle par une porte de Hadamard

$$\begin{aligned} |\psi_1\rangle &\overset{H}{\rightarrow} |\psi_2\rangle \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}} (\alpha(|0\rangle + |1\rangle) (|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle) (|10\rangle + |01\rangle)) \end{aligned}$$

Qu'on écrira comme

$$|\psi_2\rangle = \frac{1}{2} [|00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle)]$$

Juste aprés Alice effectue une double mesure sur ces 2 qubits :

Si la double mesure donne 00 alors celui de Bob est

$$|\psi_{00}\rangle = \alpha |0\rangle + \beta |1\rangle = |\psi\rangle$$

Si elle donne 01, celui de Bob

$$|\psi_{01}\rangle = \alpha |0\rangle + \beta |1\rangle$$

Si elle donne 10, celui de Bob est

$$|\psi_{10}\rangle = \alpha |0\rangle - \beta |1\rangle$$

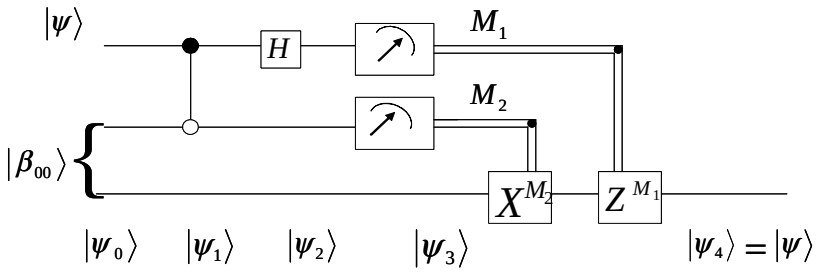
Si elle donne 11, celui de Bob est

$$|\psi_{11}\rangle = \alpha\,|1\rangle - \beta\,|0\rangle$$

Le qubit de Bob dépend de résultat de la double mesure de Alice. Alice communique alors son résultat de mesure et Bob s'arrange alors à retrouver dans tous les cas l'état inconnu $|\psi\rangle$; en rejoutant deux autre portes :

$$X^{M_2} \text{ puis } Z^{M_1}$$

M_1, M_2 résultat de la mesure et on a alors



Dans cette exemple de la téléportation juste avant qu'Alice effectue la mesure

$$|\psi_2\rangle = \frac{1}{2}\left[|00\rangle\left(\alpha\,|0\rangle + \beta\,|1\rangle\right) + |01\rangle\left(\alpha\,|1\rangle + \beta\,|0\rangle\right) + |10\rangle\left(\alpha\,|0\rangle - \beta\,|1\rangle\right) + |11\rangle\left(\alpha\,|1\rangle - \beta\,|0\rangle\right)\right]$$

Qui est une combinaison de quatre possibilités, la probabilité de chacune 1/4. Nous pouvons alors décrire l'ensemble par une matrice densité

$$\rho = \frac{1}{4}\begin{bmatrix} |00\rangle\langle 00|\left(\alpha\,|0\rangle + \beta\,|1\rangle\right)\left(\alpha^*\langle 0| + \beta^*\langle 1|\right) + |01\rangle\langle 01|\left(\alpha\,|1\rangle + \beta\,|0\rangle\right)\left(\alpha^*\langle 1| + \beta^*\langle 0|\right) \\ + |10\rangle\langle 10|\left(\alpha\,|0\rangle - \beta\,|1\rangle\right)\left(\alpha^*\langle 0| - \beta^*\langle 1|\right) + |11\rangle\langle 11|\left(\alpha\,|1\rangle - \beta\,|0\rangle\right)\left(\alpha^*\langle 1| - \beta^*\langle 0|\right) \end{bmatrix}$$

La matrice réduite de Bob est

$$\rho^B = Tr_A(\rho) = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{1}{2}$$

Alors après la mesure d'Alice et avant la mesure de Bob, On a 1/2 (mélange de ket $|0\rangle$ et ket $|1\rangle$ avec la probabilité 1/2,1/2)

Cet état mélange est indépendant de l'état à téléporter, Aucune information sur cet état $|\psi\rangle$, Bob ne peut rien déduire et il doit attendre les information de Alice, (pas d'information⟩c).

3.1.7 Algorithmes

La première définition du mot algorithme, dans son sens actuel, a été donnée par le mathématicien russe Markov : « Tout ensemble de règles précises qui définit un procédé de calcul destiné à obtenir un résultat déterminé à partir de certaines données initiales .» Les algorithmes sont constitués par un ensemble de règles précises et compréhensibles par tous. Ils s'appliquent à des données qui peuvent changer et élaborent les résultats en fonction des données initiales.

Algorithme informatique

Procédé de calcul mis en œuvre sur un ordinateur, et qui, répété autant de fois qu'il est nécessaire, permet d'obtenir le résultat cherché.

Algorithme mathématiques

Méthode de résolution d'un problème suivant un enchaînement déterminé de règles opératoires. Le mot « algorithme » est dérivé du nom du mathématicien persan al-Khuwarizmi à qui l'on doit un traité d'algèbre (1825). Dans le domaine des mathématiques, les algorithmes furent utilisés dès l'Antiquité pour traiter des problèmes d'arithmétique ou de géométrie. Plus tard, les algorithmes intervinrent dans les méthodes de résolution d'équations algébriques (algorithme de Newton, méthode d'élimination de Gauss) et d'équations différentielles.

Algorithme génétique

Méthode de programmation qui repose sur le principe de l'évolution pour effectuer la recherche d'une solution à un problème.

Algorithme quantique

Le calcul quantique permet de calculer exactement les mêmes fonctions qu'un ordinateur classique. Donc tous les algorithmes classiques peuvent exister en quantique. Ce qui se passe, c'est qu'il y a certains problèmes que l'on sait résoudre plus rapidement grâce au calcul quantique, et il y en a aussi pour lesquels le calcul quantique n'améliore pas même avec la rapidité.

3.1.8 Transformation quantique de Fourier

Transformation de Fourier discrète classique

On considère un vecteur X de N nombres complexes$x_0, x_1, ...x_{N-1}$,avec$N = 2^n$. On définit la transformée de Fourier classique de X comme étant le vecteur Y=$(y_0, y_1, ..., y_{N-1})$ dont les coordonnées sont définies par

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=o}^{N-1} x_j e^{2\pi ijk/N}$$

La transformée de Fourier inverse est définie par la relation suivant :

$$x_j = \frac{1}{\sqrt{N}} \sum_{k=o}^{N-1} y_k e^{-2\pi ijk/N}$$

Transformée de Fourier quantique

On se place maintenant dans un espace de Hilbert de dimension$N$, muni d'une base orthonormée $|j\rangle$, $j = 0, ...N-1$.On appelle transformée de Fourier quantique, l'application linéaire qui transforme la base $|j\rangle$ en la base $\left|\tilde{j}\right\rangle$ suivant la relation :

$$\left|\tilde{j}\right\rangle = U_{TF} |j\rangle = \frac{1}{\sqrt{N}} \sum_{k=o}^{N-1} e^{2\pi ijk/N} |k\rangle$$

U_{TF} est unitaire

$$U_{TF} \cdot U_{TF}^{-1} = 1$$

Transformée de Fourier discrète quantique

Considérer l'opération unitaire U_{TF} qui agit sur un registre

$$U_{DTF} |x\rangle = \frac{1}{2^L} \sum_{y}^{2^{2L}-1} \exp(2\pi i \frac{xy}{2^{2L}}) |y\rangle$$

Où 2L est la taille du registre. La raison d'appeler cette transformation unitaire particulière, la transformée de Fourier discrète devient évidente quand nous remarquons que

$$U_{DTF} \sum_{x=0}^{2^{2L}-1} c_x |x\rangle = \sum_y c_y |y\rangle$$

Les coefficients c_y sont la transformée de Fourier discrète du c_x, i.e.

$$c_y = \frac{1}{2^L} \sum_{x=0}^{2^{2L}-1} \exp(2\pi i \frac{xy}{2^{2L}}) c_x.$$

Décomposition de la transfotmée de Fourier quantique en portes élémentaires à 1et 2 qubits

Puisque l'on a $N = 2^n$ on peut décomposer l'espace de Hilbert comme le produit tensoriel de n espaces de Hilbert de dimension 2, i.e il nous faut n qubits comme ressource pour effectuer notre calcul. On choisit comme base de calcul la base usuelle :

$$|j\rangle = |j_1, j_2, ..., j_n\rangle = \otimes_{l=1}^{n} |j_l\rangle$$

Où le qubit $|j_l\rangle$ se trouve dans l'état $|0\rangle_l$où $|1\rangle_l$ suivant la relation

$$j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_n 2^0$$

On définit la *fraction binaire*, notée $0.j_l j_{l+1....j_m}$, par la relation :

$$0.j_l j_{l+1....j_m} = \frac{j_l}{2} - \frac{j_{l-1}}{4} + ... + \frac{j_m}{2^{m-l+1}}$$

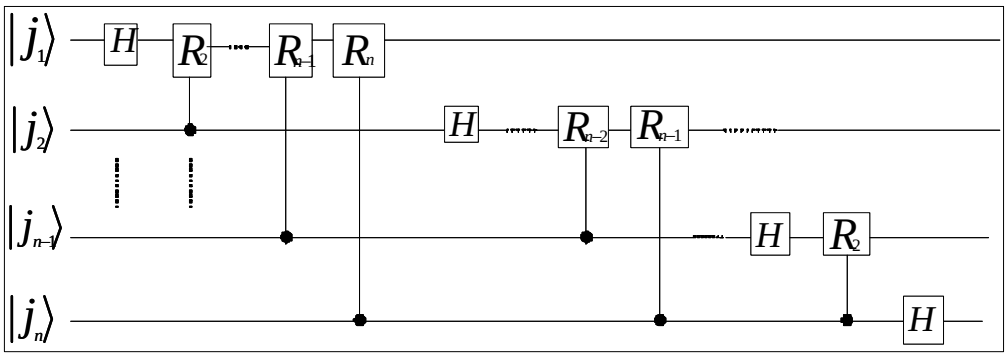
Dans le cadre de la représentation tensorielle U_{TF} peut être définie par

$$|j_1, j_2, ..., j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i 0.j_n} |1\rangle) \otimes (|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle) \otimes ..... \otimes (|0\rangle + e^{2\pi i 0.j_1 j_2 ....j_n} |1\rangle)}{2^{n/2}}$$

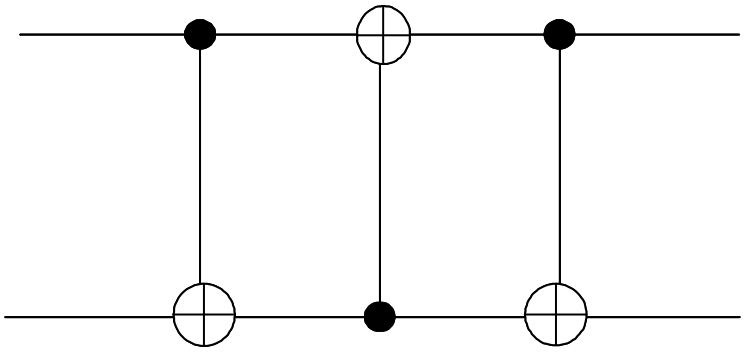
On définit l'opération unitaire R_K dans l'espace de Hilbert d'un qubit :

$$R_K = \begin{pmatrix} 1 & 0 \\ 0 & 2^{2\pi i/2^k} \end{pmatrix}.$$

On peut montrer que le circuit suivant permet de calculer U_{TF} si on lui rajoute un ensemble d'opérations de permutation "SWAP" entre 2 qubits,

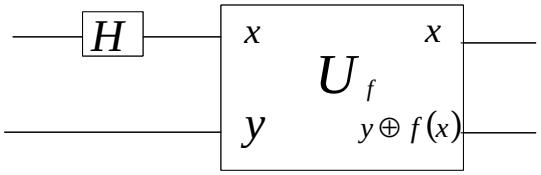


L'operation "SWAP" peut être réalisée par le circuit suivant :



L'opération SWAP

3.1.9 Les fonctions parallèles



Ci*rcuit*

calculant en parallèle toutes les valeurs possibles d'une fonction f

Le circuit à deux qubit présenté sur la figure représente symboliquement le circuit qui calcule en parallèle toutes les valeurs possibles d'une fonction $f(x)$ dans le cas le plus simple

d'une fonction binaire d'une variable x. La boite U_f est la transformation unitaire à deux qubits définie par :

$$|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$$

Où $\oplus$ désigne l'addition modulo 2. En tenant compte de la porte Hadamard appliquée au qubit $|x\rangle$,le circuit représenté sur la figure réalise la transformation :

$$|0, 0\rangle \rightarrow \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

L'état final du registre quantique contient virtuellement une information sur la fonction f évaluée pour toutes les valeurs possibles de la variable x. On a ici calculé en parallèle deux valeurs de $f(x)$ en une seule opération de U_f . Ce circuit se généralise à toute fonction logique $f(x)$ d'une variable x à n bits à valeurs dans un espace à p bits. On obtient ainsi en une seule action de U_f un état quantique contenant virtuellement toutes les valeurs de $f(x)$ correspondant aux 2^nvaleurs possibles de x.Classiquement, on doit évaluer f 2^n fois pour obtenir cette information.C'est là l'origine de l'accélération exponentielle d'un calcul quantique pour la résolution de certains problèmes.

3.1.10 Algorithme de Deutsch

Le problème de Deutsch est un algorithme quantique simple qui illustre certains des éléments du calcul quantique.

Considérer toutes les fonctions f

$$f : \{0, 1\} \rightarrow \{0, 1\}$$

Alors il y a seulement quatre possibilités, à savoir

$$\begin{aligned} f_1(0) &= f_1(1) = 0 \\ f_2(0) &= f_2(1) = 1 \\ f_3(0) &= 0 \; et \; f_3(1) = 1 \\ f_4(0) &= 1 \; et \; f_4(1) = 0. \end{aligned}$$

Soit donné une fonction inconnue f parmi les quatre possibilités, le probleme consiste à determiner si la fonction est ($f_1$ou f_2)constant ou le ($f_3$ou f_4) équilibré. Intuitivement, la meilleure stratégie classique est clairement d'évaluer f sur l'entrée 0 et 1, et comparer les résultats.

La méthode de l'algorithme de Deutsch est la suivante

- les premiers qubits est placés dans l'état initial $|0\rangle$ et les deuxièmes qubits dans l'état $|1\rangle$. L'état général est dans $|01\rangle$.

- La première étape consiste en appliquant sur chaque qubit la porte U_A, ceci laisse les deux qubits dans l'état

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right).$$

- Après on calcule la fonction f sur cette superposition et ceci est fait par une porteU_f , qui est complètement définie par son action sur les vecteurs de base :

$$|i, j\rangle \rightarrow |i, j \oplus f\left(i\right)\rangle .$$

avec $i, j = 0, 1$ et $\oplus$ dénote l'addition modulo de2.

- la dernière opération consiste en appliquant une fois de plus la porte U_A sur chaque qubit.

On peut facilement vérifier que l'état final des deux qubits est

$$\begin{aligned} |01\rangle \quad & \text{si } f = f_1 \\ -|01\rangle \quad & \text{si } f = f_2 \\ |11\rangle \quad & \text{si } f = f_3 \\ -|11\rangle \quad & \text{si } f = f_4 \end{aligned}$$

Donc une mesure finale sur le premier qubit indiquera si la fonction est la constante 0 ou 1 équilibré.

On peut faire plusieurs remarques au sujet de cet algorithme. D'abord, l'algorithme quantique permet la classification de la fonction inconnue f avec une évaluation simple, tandis que classiquement deux évaluations sont nécessaires.

3.1.11 Algorithme de Schor

L'algorithme de Shor est un algorithme quantique pour factoriser un nombre N en temps $O((logN)3)$ et en espace $O(logN)$, Comme tous les algorithmes pour calculateur quantique, l'algorithme de Shor est probabiliste : il donne la réponse correcte avec une haute probabilité, et la probabilité d'échec peut être diminuée en répétant l'algorithme. L'algorithme de Shor fut utilisé en 2001 par un groupe d'IBM, qui factorisa 15 en 3 et 5, en utilisant un calculateur quantique de 7 qubits.

L'algorithme quantique de Shor nécessite d'effectuer des exponentielles modulaires et des transformations de Fourier. Ces opérations, longues en général, peuvent être traitées en un temps polynomial par l'algorithme quantique. La réalisation quantique de cet algorithme depuis sa démonstration au milieu des années 90 a été tentée mais sans réussite.

Cette réalisation est un pas en avant dans la technologie des ordinateurs quantiques à photon et des supercalculateurs.

Dans le monde quantique, on peut résoudre un problème analogue où la consultation des cartes est une opération quantique qui permet de les consulter simultanément.

Choisissons un a $\langle N$; si $a$divise N on a fini. Sinon il existe un r tel que

$$\alpha^r \equiv 1 \bmod N \qquad \text{Euler-Fermat}$$

Soit la fonction

$$f(x) = \alpha^x \bmod N$$

Elle est périodique, de période r.

On sait déterminer r comme suit :

Supposont que r soit paire

$$\alpha^r - 1 = \left(\alpha^{\frac{r}{2}} - 1\right)\left(\alpha^{\frac{r}{2}} + 1\right) \equiv 0 \bmod N$$

Il suffit de déterminer le plus grand facteur commun a $\left(\alpha^{\frac{r}{2}} - 1\right)$ et N pour obtenir une factorisation de N.

Si r n'est pas paire on choist un autre a.

L'algorithme de Shor est composé de deux parties. La première transforme le problème de factorisation en un problème de recherche de la périodicité d'une fonction mathématique, ce qui peut être réalisé de manière « classique ». La seconde partie trouve la période à l'aide d'une opération appelée « transformée de Fourier quantique ». L'intérêt de cette transformation pour les problèmes de périodicité venait d'être mis récemment en évidence.

3.2 Quelques exemples physiques des qubits

3.2.1 Résonance magnétique nucléaire

Un spin 1/2 nucléaire dans un champ magnétique peut être simuler une réalisationréalise d'un qubit. Il est couplé à l'envirenement et on manipule son état par résonance magnétique, combinant un champ statique et un champ oscillant.

Dans une molécule, les fréquences de résonance de noyaux identiques à des états quantiques différents. Ces états chimiques permettent d'orienter individuellement les spins en choisissant la fréquence du champ oscillant. Deux spins voisins sont également couplés entre eux : la fréquance de transition d'un spin dépend de l'état quantique du voisin. Ces couplages sont les ingrédients de portes logique quantiques.

On a pu adapter les spectromètres RMN au calcul quantique : portes logique variées, intrication de deux et de trois qubits, jusqu'à une remarquable démonstration de l'algorithmede Shor dans le cas "15=3×5".

3.2.2 Ions piégés

Les pièges à ions sont des dispositifs expérimentaux permettant de stocker des particules chargées pendant une longue durée dans le but de mesurer leurs propriétés physiques.

Les pièges de Paul et de Penning ont en commun l'utilisation d'un champ électrique quadripolaire, à haute fréquence dans le piège de Paul, et constant dans le piège de Penning, où il est combiné à un champ magnétique intense. La mise en œuvre des ces pièges à ions dans le domaine de la spectroscopie atomique de précision est devenu possible et a valu à Hans Dehmelt (avec le piège de Penning) et à Wolfgang Paul (avec le piège portant son nom) le prix Nobel

de physique en 1989, partagé avec Norman Foster Ramsey pour ses travaux sur les horloges atomiques.

On arrive à piéger un ou quelques ions dans une configuration particulière et adaquate de champs électriques. La fluorescence d'un ion unique, induite par un laser résonnant sur une transition forte entre un deux niveaux exités, permet de lire l'état final du qubit ionique individuel. C'est un avantage de la méthode par rapport au cas de RMN. Le mouvement quantifié de l'ion dans le piège fournit un autre qubit. Des transitions optiques couplant des états internes et de vibration permettent de réaliser la porte logique $CNOT$.

Les expériences sont trés délicates. Le groupe de D.Wineland a réalisé la première porte logique quantique entre les niveaux internes et de vibration d'un ion unique.

3.2.3 Ordinateur quantique

Un ordinateur quantique possède plusieurs avantages complètement différentes de n'importe quel ordinateur classique pour mener à bien les calculs qui n'ont pas pu se faire par le biais des ordinateurs classiques.

Un ordinateur classique manipule un bit à valeurs 0 ou 1 et effectue les calculs mais il existe des problèmes difficiles telle la factorisation qui est presque impossible.

Ordinateur quantique manipule des systèmes quantiques représenée par un qubit à valeurs quantiques $|0\rangle$ ou $|1\rangle$. Il obéit au principe de superposition. Les qubits peuvent avoir les valeur 0et 1 à la fois.

Un ordinateur quantique peut effectuer simultanément tous les calculs possibles etfacilite des problèmes difficiles telle la factorisation.

Il y a aussi d'autres raisons qui nous invitent à étudier l'ordinateur quantique notamment qu'il est difficile d'analyser un grand nombre d'ordinateurs. Pour accélérer ce processus les ordinateurs ont besoin d'un processeur plus rapide. La mécanique quantique nous permet d'accéder à niveau dit ordinateur quantique.

Cette nouvelle vision récente concerne la réalisation d'ordinateurs quantiques et le traitement quantique de l'information.

3.3 Information quantique

3.3.1 Information classique

La théorie de l'information est une théorie mathématique de la transmission et de la manupilation de l'information.Cette théorie s'intéresse à la mesure de la quantité d'information, à la représentation de cette information, encore appelée codage, ainsi qu'aux systèmes de communication qui la transmettent et la traitent. Ce codage peut ainsi se référer à la conversion de sons et d'images en signaux électromagnétiques, mais également au chiffrage de messages confidentiels grâce aux techniques de la cryptographie. Outre les télécommunications, l'électronique et l'informatique, la théorie de l'information s'applique à divers domaines.

L'information classique donne une réponse à deux questions fondamentales (théorèmes de Shannon-1948) :

1) quelle est la manière maximale de compresser un message

2) quel est le taux maximal de communication par un canal

La réponse à ces deux questions fondamentales sont respectivement l'entropie de Shannon et la capacité du canal

L'entropie de Shanon

L'information contenue dans un message est une quantité mathématiquement mesurable, liée à la probabilité que ce message soit choisi parmi un ensemble de messages possibles. Plus le message est probable, plus la quantité d'information qu'il transporte est faible. Par conséquent, un message attendu avec certitude possède une quantité d'information nulle. l'entropie de Shanon se définit par

$$H_{Sh}(X) = -\sum_{x=0}^{k} p(x)) \log_2(p(x))$$

Dans ce cas on a k lettres $a(x)$ et X est la distribution de probabilité des $a(x)$ dont la probabilité est $p(x)$.

On montre rigoureusement qu'un code optimal comprime chaque lettre en $H_{Sh}(X)$ bits (premier théorème de Shanon)

Capacité du canal

Si on envoie un message, on a aussi de l'information à partir de cette entropie de Shanon. Si on suppose que quand en envoie $a(x)$ on a une probabilité $p(x \mid y)$ pour que $a(y)$ soit lue alors on peut calucler

$$H_{Sh}(X \mid Y) = -\sum_{x=0}^{k} p(x \mid y)) \log_2(p(x \mid y)) = H_{Sh}(X, Y) - H_{Sh}(Y)$$

et l'information mutuelle (le gain en information) est définie par

$$I(X \mid Y) = H_{Sh}(X) - H_{Sh}(X \mid Y)$$

c'est le nombre de bits par lettre $a(x)$qu'on peut acquérir en lisant $a(y)$. la capacité du canal est définit comme un maximum sur cette entropie mutuelle

$$C = \max_{p(x)} I(X \mid Y)$$

Le contenu du deuxième théorème de Shanon est : une transmission sans erreur est possible si le taux de transmission du canal est inférieur à C.

3.3.2 Mesures en présence d'environnement

Nous avons rencontré au paravant au moins différents types d'opérations quantiques : des transformations unitaires et des mesures quantiques.

Lors de ces opérations nous avons vu que l'état du système ρ se transforme comme

$$\rho \rightarrow \rho\prime = U\rho U^{+}$$

qui est une transformation unitaire et

$$\rho \rightarrow \rho\prime = M_n \rho M_n^{+}$$

qui est une mesure quantique

D'une façon générale définissons une opération quantique par une application ζ qui transforme l'état du système ρ comme

$$\rho \rightarrow \rho\prime = \zeta(\rho)$$

Il existe plusieurs façons de descriptions de ces opérations quantiques qui sont en général équivalentes mais dont chacune jouit d'un avantage particulier.

1- La première décrit la dynamique comme résultat de l'interaction entre le système et l'environnement elle est plus physique et moins mathématique. Elle permet une projection immédiate sur le monde réel (système couplé à l'environnement).

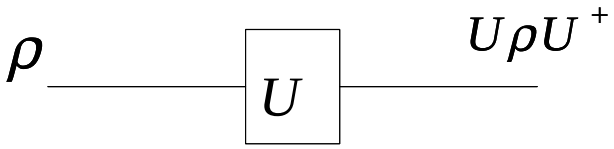
2- La deuxième exactement équivalente à la première mais elle nous permet de dépasser l'inconvénient mathématique de la première on l'appelle représentation somme d'opérateurs (opérateur sum representation)

3- La troisième équivalente aux précédentes mais plus axiomatique. Son grand avantage est quel convient à toutes les situations.

Elle est moins calculatoire et plus abstraite. Ces trois approches ensemble permettent de cerner efficacement la dynamique des systèmes ouverts et en particulier le bruit quantique.

3.3.3 Opérateurs quantiques et environnement

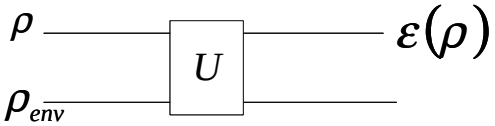
L'évolution d'un système fermé est décrite pas des transformations unitaires qu'on décrira par le schéma suivant



Donc comme une boite ayant un input ρ et un output $U\rho U^{+}$.

En général U n'est pas spécifié, il peut être généré par des circuits quantiques, des Hamiltoniens ou bien autre chose.

La dynamique des systèmes ouverts est décrite par l'interaction entre système principal et l'environnement. L'ensemble constitue un système fermé.



Entre ρ et $\varepsilon(\rho)$ on suppose que l'environnement intervient via U, ie, initialement on a Input

$\rho \otimes \rho_{env}$ système totale fermé séparé et après U le système n'intéragit plus avec l'environnement et l'état du système principal est décrit par la trace partielle de l'évolution de l'ensemble

Output

$$\varepsilon(\rho) = Tr_{env}\left(U\left(\rho \otimes \rho_{env}\right)U^{+}\right)$$

Si dans U le système n'interagit pas avec l'environnement alors on peut écrire

$$U = U_{\rho} \otimes U_{env}$$

et on a

$$\begin{aligned}
\varepsilon(\rho) &= Tr_{env}\left(U_{\rho} \otimes U_{env}\right)\left(\rho \otimes \rho_{env}\right)\left(U_{\rho} \otimes U_{env}\right)^{+} \\
&= \left(U_{\rho}\rho U_{\rho}^{+}\right) Tr_{env}\left(U_{\rho}\rho_{env}U_{env}^{+}\right) \\
&= U_{\rho}\rho U_{\rho}^{+}
\end{aligned}$$

On retrouve l'évolution fermé du système.

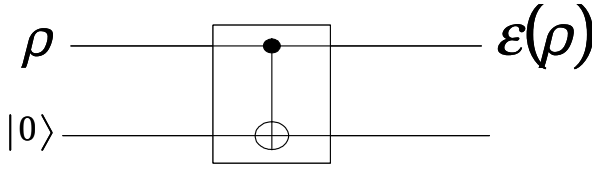
Exemple :

Soit deux qubits, l'un constitue le système principal décrit par ρ et l'autre l'environnement qui initialement était

$$\rho_{env} = |0\rangle\langle 0|$$

U étant la porte $C-NOT$ contrôlée par le système principal, on a alors

$$\varepsilon(\rho) = Tr_{env}\left(U\left(\rho \otimes \rho_{env}\right)U^{+}\right)$$



$$\begin{aligned}
\varepsilon(\rho) &= Tr_{env}\left(U_{C-NOT}\left(\rho \otimes |0\rangle\langle 0|\right)U_{C-NOT}^{+}\right) \\
&= P_0\rho P_0 + P_1\rho P_1
\end{aligned}$$

Avec

$$P_0 = |0\rangle\langle 0|, \qquad P_1 = |1\rangle\langle 1|$$

Représentation en somme d'opérateurs

Dans cette approche, on exprime $\varepsilon(\rho)$ comme somme d'opérateurs agissant sur l'espace du système principal. Pour ce faire, on définit un certain espace de dimension finie pour l'environnement avec $\{|e_k\rangle\}$ comme base. Initialement, on a

$$\rho_{env} = |e_0\rangle \langle e_0|$$

S'il n' y a pas d'états purs on le purifie et on aura

$$\varepsilon(\rho) = \sum_k \langle e_k| U(\rho \otimes |e_0\rangle \langle e_0|)U^+ |e_k\rangle$$

Ainsi

$$\varepsilon(\rho) = \sum_k E_k \rho E_k^+$$

avec $E_k = \langle e_k| U |e_0\rangle$ un opérateur agissant sur le système principal.

Cette écriture est dite représentation en somme d'opérateurs et $\{E_k\}$ sont dits éléments d'opération. On vérifie

$$1 = Tr(\varepsilon(\rho)) = Tr(\sum_k E_k E_k^+ \rho)$$

Comme ρ est quelconque alors nous aurons soit

$$\sum_k E_k E_k^+ = I$$

Et cette égalité est satisfaite pour les opérations qui préservent la trace

$$1 = Tr(\varepsilon(\rho)) = Tr(\rho)$$

Soit

$$\sum_k E_k E_k^+ \leq I$$

Cette représentation jouit de multiples avantages en plus de son pouvoir de calcul. Elle évite de connaitre les propriètés de l'environnement puisque les E_k agissent sur le système principal. différents environnements peuvent conduire à une même dynamique.

Approche axiomatique aux opérations quantiques

D'une manière plus abstraite, nous définissons une opération quantique comme une application qui transforme $\rho \rightarrow \rho\prime = \zeta(\rho)$ vérifiant trois axiomes principaux :

1- $Tr\ (\varepsilon(\rho))$ est la probabilité pour que le processus représenté par ε se passe quand ρ est l'état initial. Alors

$$0 \leq Tr(\varepsilon Tr(\rho) \leq 1$$

2- ε est une application linéaire convexe, ie,

$$\varepsilon\left(\sum_i P_i\rho_i\right) = \sum_i P_i\varepsilon(\rho_i)$$

pour$\{Pi\}$ des probabilités.

3- ε est une application complètement positive, ie, $\varepsilon(A)$ doit être positif pour tout A positif.

Entropie de Von Neuman

L'entropie de Von Neuman pour un état $\rho = \sum_i \lambda_i |\psi_i\rangle \langle\psi_i|$ est définie comme

$$S(\rho) = -tr(\rho \log_2 \rho) = -\sum_i \lambda_i \log_2 \lambda_i$$

Quelques propriètés de l'entropie de Von Neumann :

- $S(\rho) \geq 0$.
- $S\left(\frac{I}{d}\right) = \log d$.
- Si ρ^{AB} est un système à deux parties. alors $S\left(\rho^A\right) = S\left(\rho^B\right)$.
- Soit $\{p_i\}$un ensemble de probabilités et un ensemble d'état $\{\rho_i\}$, alors

$$S\left(\sum_I p_i\rho_i\right) \leq H_{Sh}(p_i) + \sum_I p_i\ S\ (\rho_i).$$

avec égalité si et seulement si les sous-espaces définis par les $\{\rho_i\}$ sont orthogonaux

- Entropie conjointe(théorème) : Soient $\{p_i\}$un ensemble de probabilités et $\{|i\rangle\}$, des vecteurs orthogonaux, alors

$$S\left(\sum_i p_i\ |i\rangle\langle i| \otimes \rho_i\right) = H_{Sh}(p_i) + \sum_I p_i\ S\ (\rho_i).$$

l'entropie de Shanon est toujours supérieure à celle de Von Neumann

$$H_{Sh} \geq S$$

L'entropie de Von Neumann permet alors de généraliser les théorèmes de Shanon dans le cas de l'information quantique en remplçant la notion de séquence de lettres typiques par celles des sous espaces quantiques typiques et l'entropie de Shanon par celle de Von Neumann

3.4 Cryptographie

La cryptographie est la science qui utilise les mathématiques pour coder ou décoder des messages. La cryptographie nous permet de stocker des informations ou de les transmettre à travers des réseaux. Par conséquent, on s'intéresse dans la cryptographie à la sécurisation des ces données. La cryptographie classique est une combinaison de raisonnement analytique, d'application d'outils mathématiques, de découverte de redondances, et de détermination.

3.4.1 Cryptographie quantique :

Prenons l'exemple de l'expérience D'Alice et Bob de l'expérience de la téléportation quantique. La cryptographie quantique va permettre à Alice et Bob de convenir d'une clé dont le secret soit garanti. Ils pourront ensuite crypter et décrypter classiquement un message en utilisant cette clé.

Il existe deux principaux types de protocoles :

- 1^{er}type de protocole, basé sur l'envoi de photons polarisés ou modulés en phase, la sécurité de ce type repose sur la possibilité de bénificier d'une vraie source de photons uniques.

- $2^{ème}$type de protocole est basée sur la production de paire de photones intriquées.

La cryptographie est une manipulation de chiffres, de codes ou de messages cachés. Ces derniers, "invisibles" ou dissimulés dans des textes apparemment quelconques, n'ont d'intérêt que s'ils restent insoupçonnés :s'ils sont découverts, il n'est pas difficile de décoder le message. Les codes, dans lesquels les mots, les phrases ou les messages complets sont représentés par des expressions ou symboles prédéfinis, sont impossibles à lire les clés des codes, mais il faut transmettre cet annuaire de codes de façon secrètes. Enfin, le codage consiste à transformer

les symboles d'un texte en cryptogramme au moyen d'un calculateur ou d'une machine, le décryptage ou décodages s'obtient par la transformation inverse.

3.4.2 Le cryptage RSA

En 1978, trois mathématiciens, Rivest, Shamir et Adleman, ont mis au point une méthode de cryptage à clé publique, procédé aujourd'hui largement utilisé pour assurer la sécurité des données sur Internet.

La méthode RSA permet à chacun de coder un message à partir d'une clé publique mais n'autorise pas le décodage qui est conditionné par la connaissance d'une clé privée.

La sécurité de ce système de cryptage repose sur le fait qu'il est très facile de calculer, à l'aide d'un ordinateur ou d'une calculatrice symbolique, de très grands nombres premiers mais que la factorisation d'un très grand nombre prend un temps considérable sur les machines actuelles pour peu que les nombres premiers qui le compose soient suffisamment grands.

Un utilisateur, Bob, choisit premierement deux grands nombres p et q et $N = pq$.Il choisit alors aléatoirement la clé de codage tels que e et $(p-1)(q-1)$ n'ont aucun facteur commun. Après, il calcule la clef unique de décodage, d, telle que

$$ed = 1\,[\mathrm{mod}(p-1)(q-1)]$$

Ce calcul peut être fait efficacement par l'algorithme Euclidien. Maintenant e et N sont f publiqueset ils peuvent être édités dans un annuaire principal public de la même manière qu'un annuaire de téléphone. La clé de décodage, d, doit être maintenue secrète. Pendant que p et q ne sont nécessaires plus, ils peuvent être jetés, mais ne jamais être indiqués. Supposer une personne qu'Alice, avant qui ne puisse pas avoir rencontré Bob, voudrait envoyer à Bob un message $m(modN)$. Elle peut faire ainsi en le soulevant à la puissance$e$, i.e.,

$$c = m^e (\mathrm{mod}\, N)$$

et l'envoi de c à Bob peut récupérer le message m en soulevant c à la puissance d. La théorie élémentaire de nombre, $m^{(p-1)(q-1)=1}$ $(modN)$ pour n'importe quel $m(modN)$ donne en conséquence,

$$c^d = m^{ed} = m^{k(p-1)(q-1)} \times m = m \qquad \text{tous} \quad (modN).$$

Pour un long message, Alice peut, par exemple, l'augmenter dans la puissance de N et coder chaque entrée dans l'expansion de N-ième individuellement.

Celui qui ne sait pas d ni la factorisation de N aura généralement un moment difficile en déduisant m seul de c, de e et de N. D'autre part, si le facteur N dans p chronomètre q, alors elle peut trivialement trouver la clé d de décodage en employant l'algorithme euclidien avec d et $(p-1)(q-1)$ comme entrées.

Chapitre 4

Conclusion

En conclusion, ce mémoire donne une introduction pédagogique à un domaine très florissant de la physique qui est celui de l'information quantique. Certes pour pouvoir maîtriser cette matière il nous faut beaucoup de connaissance et de polyvalence dans les domaines variés de la physique, surtout celui de la mécanique quantique, de ses réalisations expérimentales en nanotechnologie et de ses applications actuelles en cryptographie et algorithmique. Nous avons fait de notre mieux pour exposer les fondements de la mécanique quantique, de préciser ses points puissant dans l'explication et la prédiction des phénomènes microscopique surtout en l'appliquant sur la notion de qubit. Bien sûr sans oublier d'évoquer les tentatives des physiciens à vouloir montrer son incomplétude comme théorie finale. Sans départager les vais on a essayé de montrer la richesse apportée par ses critiques a développement de cette mécanique quantique. Une introduction au calcul quantique a été présentée vue l'effervescence de ce domaine d'actualité. Nous avons alors présenté les registres quantiques, les portes quantiques, la transformée de Fourier. Les algorithmes les plus connus ceux de Deutch et de Schor sont exposés. Quelques réalisations de qubit sont présentées tels que la résonance nucléaire magnétique et le piège à ions. On a présenté une introduction à l'information quantique en présentant quelques notions sur l'entropie des applications à la téléportation, la cryptographie quantique.

Nous souhaitons que ce mémoire sera d'une assistance agréable et bénéfique pour celui qui veut s'initier d'une manière débutante à ce domaine très difficile et très riche de la physique moderne de l'actualité en cours.

Bibliographie

[1] Michel A. Nielsen & Isaac L. Chang. Quantum Computation and Quantum Information.(2000).

[2] Denis Crottet, L'Ordinateur Quantique,EPFL, Physique, 8ème sem.Ecublens, le 29 mars 2000.

[3] Dheera Venkatraman. Methods and implementation of quantum cryptography. (27 avril 2004).

[4] P.Navez[1]et G. Van Assche [1,2]. Une transmission sécurisée : la cryptograpie quantique. Avril 2002.

[5] Hervé Zwirin. Mécanique quantique et connaissance du réel.

[6] Michel Bitbol. Mécanique quantique, Une Introduction Philosophique. (1996)

[7] R.Jackiw. A.Shimony. The Depth and Breadth of John Bell's Physics. Physics/ 0105046. 16 May 2001.

[8] D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, Proc. R. Soc. London Ser. A 400, 97-117
(1985).

[9] J.B. Bell, speakable ans unspeakable in quantum mechanics, Cambridge University Press (1989)

[10] C.H. Bennett, D.P. Divincenzo, Quantum information and computation, Nature 404, 247-255 (2000).

[11] R. A. Bertlmann. A. Zeilinger. Quantum [Un] speakables. (2002).

[12] Niels Bohr, Physique atomique et connaissance humaine, Editions Gallimard (1991).

[13] Alain Aspect, Philippe Grangier. Optique quantique 2 : Photons. Tome 1. (2006).

[14] Julia Kempe, Sophie Laplante et Frédéric Magniez. L'ordinateur quantique. Juin 2006.

[15] Dirk Bouwmeester. Artur Ekert. Anton Zeilinger. The Physics of Quantum Information.(2000).

[16] Alain Aspect, Jean Dalibard, and Gérard Roger, Exprimental Test of Bell's Inequalities Using Time-Varying Analtzers , Institut d'optique

Théorique et Appliquée, F-91406 Orsay Cédex, France (Received 27 September 1982).

[17] G.Alber. T.Beth. M.Horodecki. P.Horodecki. R.Horodecki. M.Rôtteler. H.Weinfuter. R.Werner. A.Zéelinger.Quntum Information. An

Introduction to basic Théoretical concepts and Experiments.

[18] Hoi-Kwong Lo. Sandu Popescu. Tim Spiller. Intrduction to Quantum Computation and Information (1998).

[19] Willi-Hans Steeb. Yorick Hardy. Problems & Solutions. Quantum Computing & Quantum Information. Rand Afrikens University, South

Africa.

[20] Gilles Nogues. Transformée de Fourier quantique. 7 avril 2006.

[21] Michael Keyl. Fundamentals of Quantum Information Théory.Physics Reports 369 (2002) 431-548.

[22] M.A.B. Whitaker. Theory and Experiment in the Foundations of Quantum Theory. Progress in Quantum Electronics 24 (2000)1_106 .

[23] Raquel Fernandez Delicado*, David Bellever Cabello, Ivan Lioro Boada. The quantum cryptograpy : Communication and Computation 57

(2005)384_355 .

[24] Thierry Masson. La physique quantique, 100 ans de questions. 10mars2004.

[25] N. Canosa*, R. Rossignoli. General non-additive entropic forms and the inference of quantum density operators. 348 (2005)121_130 .

[26] Isabelle Zaquine TSI. Réalisations physiques pour l'information quantique. 9 décembre 2004.

[27] Serge Haroche. Atomes et photons en cavité : tests fondamentaux et application à l'information quantique. 17 Juin 2004

[28] Romain Alléaume. Cryptography quantique : des concepts aux applications. Département Informatique et Réseaux. 17 Avril 2007.

[29] C. Longumare. Limites classiques de la mécanique quantique. 3 Juiliet 2007.

[30] Grégoire Ribordy et Olivier Guinnard. Nicolas Gisin et Hugo Zbinden. Un Saut Quantique en Cryotpgraphie. Septembre 2004.

[31] David Papoular. Intrication quantique, paradoxe EPR et théorème de Bell. 27 Octobre 2005.

[32] Alain Aspect, Philippe Grangier, and Gérard Roger, Exprimental Test of Realistic Local Theorie via Bell's Theorem , Institut d'optique
Théorique et Appliquée, F-91406 Orsay , France (Received 30 March 1981)

[33] Matthieu Deconinck. Dirk Lange. Olivier Marfaing. Matthieu Rambaud. Jimena Royo-Letelier. Logique fondements, applications,
perspectives (2005).

[34] Sylvain Guilley. Des qubits aux algorithmes quantiques. 21octobre2004.

[35] Frédéric Magniez. Vérification approchée–Calcul quantique. Université de Paris Sud (2007).

[36] Gilles Noguès. Différence entre information quantique et information classique. 9 mars 2006.

[37] Ian Glendinning. The Bloch Sphere. February 16,2005.

[38] Charles H. Bennett. Quantum Information Processing. 15 Feb 2005.

[39] Sébastien Giraud. Une Introduction au Calcul Quantique : L'algorithme de Shor. 22 mai 2007.

[40] E. Farhi, J. Goldstone, S. Gutman, M. Sipser, Limit on the speed of quantum computa-tion in determining parity, Phys. Rev. Lett. 81,
5442-5444 (1998).

[41] Azhar Iqbal. Investigations in quantum games using EPR-type set-ups. BSc (Hons), U niversity of Sheffield, UK, 1995 (2006).

[42] Hervé Zwirn. Formalisme quantique et préférences indéterminées en théorie de la décision. Décembre 2006.

[43] Ben Taieb Souhaib.L'algorithmique quantique. Département d'Informatique. 19 - 25 mars 2007.

[44] Étienne Klein. Réflexions sur la mesure, et Petit voyage dans le monde des quanta, Champs, Flammarion, 2004.. Direction des sciences de la matière, CEA centre de Saclay.

[45] Marco Testi. Intrication sujet-objet dans la mesure de l'information. Mémoire de recherche (2002-2003).

[46] M.X.He [a,*], P.E. Ricci [b]. Information entropy of orthogonal polynomials 128 (2002).

[47] Armin Uhlmann. Quantum Information Transfer From One System to Another One. 21(2005)

[48] E.Jeandel. Universalité en calcul quantique. Laboratoire d'Informatique Fondamentale de Marseille. CNRS&Université de Provence.

[49] Jean-Michel Raimond. Rapport d'Activité L'Université Pierre et Marie Curie. 2001-2006

[50] V. Scarani, Quantum Computing, Am. J. Phys. 66, 956-960 (1998).

[51] A. Barenco, C.H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter, Elementary gates for quantum computation, Phys. Rev. A 52, 3457-3467 (1995).

[52] A. Peres, Quantum Theory Concepts and Methods, Kluwer Academic Publishers (1995)

[53] A. Heidmann. Mesures à la limite quantique. La boratoire Kastler Brossel. Septembre 2007.

[54] Armond Duwell. Quntum Information Does Not Exist 34 (2003) 479_499

[55] A.M. Steane. A quantum computer only needs one universe 34 (2003) 469 478.

[56] Vander Sypen. Information quantique : une clef universelle (2003).

[57] Emmanuel Jeande. Techniques algébriques En calcul quantique (2005).

[58] Gilles Noguès. Détection sans Destruction d'un seul photon. Une Expérience d'électrodynamique quantique en cavité (1999).

[59] Niels Bohr, Physique atomique et connaissance humaine, Editions Gallimard (1991).

[60] Robert Michel Di Scala. Informatique & programmation. L'ouvrage papier de 1372 page édité en Novembre 2004 par les éditions Bertià Alger.