Introduction à l'information quantique

Y. Leroyer et G. Sénizergues [1] ENSEIRB-MATMECA

Year 2016-2017 [2]

1. YL a créé cette UE en 2007 et ce document en 2007-10 ; GS y a ajouté les parties 5 et 9 en 2012.
2. last update : 27 avril 2017

Table des matières

Introduction

L'information quantique est un domaine récent des Sciences et Technologies de l'Information et de la Communication (STIC) qui est en plein développement. La plupart des grands centres de recherche publics et privés ont créé, ces dernières années, des équipes voire des laboratoires sur ce thème.

L'essor de l'information quantique est venu de la conjonction de plusieurs avancées :

— la découverte par Peter Shor en 1994 d'un algorithme basé sur les principes de la mécanique quantique qui permet de factoriser un grand nombre entier en facteurs premiers dans un temps " raisonnable ". Comme la plupart des codes de cryptage dits "à clé publique " actuellement utilisés sont basés sur l'impossibilité de réaliser cette factorisation (dans un délai raisonnable) l'émoi a été grand dans la communauté des spécialistes de cryptographie et aussi parmi tous les acteurs économiques qui utilisent ces codes pour protéger leurs données (banques, industries high-tech, militaires). Il faut dire que pour l'instant si l'algorithme existe bel et bien l'ordinateur qui le mettra en œ uvre n'est pas encore construit. D'autres découvertes algorithmiques (Grover, cryptographie) ont également contribué à ce développement.

— les progrés considérables de la nanophysique, qui permettent la réalisation de la cryptographie quantique et laissent envisager un futur possible pour l'ordinateur quantique

La mécanique quantique, développée dans les années 1920-1940, est la théorie fondamentale de toute description microscopique de la matière. Les composants électroniques des ordinateurs actuels n'ont pu être développés que grâce à la compréhension quantique des phénomènes atomiques. Le fonctionnement du transistor découvert en 1947 par Bardeen, Brattain et Schockley repose sur cette compréhension. Mais ce sont ces mêmes lois de la mécanique quantique qui imposent une limitation à ce développement : la dimension caractéristique des composants est actuellement d'environ 50 nm ; certains effets gênants apparaissent déjà (comme par exemple le " quantum leakage " dû à un effet quantique appelé " effet tunnel ") ; par ailleurs en extrapolant la célèbre loi de Moore pendant encore une quinzaine d'années la taille des composants atteindra l'ordre du nanomètre, échelle à laquelle l'ordinateur " classique " cessera de fonctionner.

Le tableau ci-dessous synthétise cette idée :

Processus informatique	Mise en oeuvre physique	Informatique classique	Informatique quantique
Stockage de l'information	Etat de la matière	Charge d'un condensateur, aimantation d'un volume	Etat quantique d'un atome, d'un photon
Calcul	Evolution physique de l'état	Physique classique/quantique	Physique quantique

Les champs d'application de l'information quantique concernent essentiellement deux secteurs :

— Le calcul quantique : les algorithmes quantiques exploitent des caractéristiques des états quantiques - le principe de superposition des états, le phénomène d'*enchevètrement* d'états, le principe de la mesure projective - qui conduisent pour certains problèmes à une réduction drastique de la complexité (voir l'algorithme de Shor). La réalisation physique des ordinateurs quantiques est un sujet en pleine activité.

— La communication de l'information : par exemple la sécurisation de l'échange de clés secrètes de codage (cryptographie quantique) mais aussi le transfert de l'information (téléportation quantique).

Nous passerons en revue ces différents aspects de l'information quantique.

Chapitre 1

Le B-A-BA Quantique

1.1 Qu'est-ce qu'un qubit ?

1.1.1 Bit classique et bit quantique

La brique élémentaire d'information classique [1] est le bit (binary digit originellement) qui prend deux valeurs 0 ou 1. La mise en œuvre physique du calcul, réalisée par l'ordinateur, repose alors sur des systèmes à deux états : aimantation " up/down ", interrupteur " on/off ", condensateurs "chargés-déchargés" dans les RAM... Même si le fonctionnement des composants électroniques qui créent, stockent et manipulent les bits repose sur les principes de la mécanique quantique, les états du système qui définissent les bits sont décrits par la physique classique, essentiellement parce qu'ils mettent en jeu un grand nombre de particules (courants électriques).

Le bit quantique ou *qubit* peut lui aussi se trouver dans deux états 0/1 mais qui sont maintenant les états d'un système *quantique* ; pour les distinguer des états classiques, on les note $|0\rangle$ ou $|1\rangle$ suivant la convention introduite par le physicien P.A.M. Dirac dans les années 30. La différence essentielle avec l'état classique 0/1 est que le qubit peut se trouver dans d'autres états (une infinité) que les états $|0\rangle$ ou $|1\rangle$. En fait tout état de la forme

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

où α et β sont deux nombres complexes, est accessible au qubit ; autrement dit l'état du qubit est un vecteur d'un espace vectoriel complexe de dimension 2 dans lequel les éléments $|0\rangle$ et $|1\rangle$ forment une base dite *base de calcul*.

Que trouve-t-on si on cherche à lire le contenu du qubit, si on le *mesure* ? On trouvera 0 s'il est dans l'état $|0\rangle$ et 1 s'il est dans l'état $|1\rangle$. Ceci n'est pas très inattendu et ne change pas du bit classique ! Et s'il est dans l'état $|\psi\rangle$? Et bien là aussi on trouvera 0 ou 1 mais de façon aléatoire. En fait on aura 0 avec la probabilité [2] $|\alpha|^2$ ou 1 avec la probabilité $|\beta|^2$. On ne peut donc pas observer directement l'état de superposition $|\psi\rangle$ du qubit ! De plus, une fois qu'il a été mesuré, l'état du qubit est projeté dans l'état correspondant au résultat de la mesure : par exemple si le qubit, originellement dans l'état $|\psi\rangle$ est mesuré et que le résultat est 1, le qubit se trouvera alors projeté dans l'état $|1\rangle$ et toute nouvelle mesure donnera immanquablement le résultat 1. Ces "règles de vie" du monde quantique concernant la description de l'état et à sa mesure constituent ce qu'on appelle les *premiers postulats de la mé canique quantique* que l'on développera dans la suite. Ce que permettent ces règles et qui constitue la base du *calcul quantique* c'est de modifier l'état du

1. Dans la suite le mot *classique* sera antinomique du mot *quantique*

2. Evidemment on doit avoir $|\alpha|^2 + |\beta|^2 = 1$ ce qui traduit le fait que l'état $|\psi\rangle$ est un vecteur unité dans un espace vectoriel complexe de dimension 2.

qubit, en lui appliquant des portes logiques ou en l'associant à un ou plusieurs autres qubit, sans le mesurer, c'est à dire sans le projeter sur les états $|0\rangle$ | ou $|1\rangle$. C'est seulement à la fin du calcul que le qubit est lu et si l'algorithme est bien choisi le processus de projection que réalise la mesure finale du qubit permet d'extraire l'information recherchée.

Avant d'entrer dans le détail de ces processus de calcul donnons une illustration de la façon de réaliser concrètement un qubit.

1.1.2 Réalisation physique d'un qubit

Etats internes d'un atome

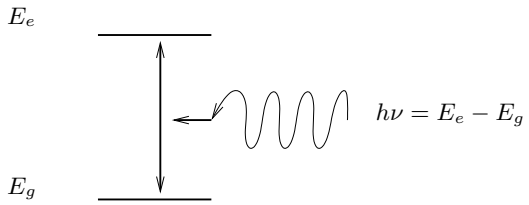


FIGURE 1.1 – Atome à deux niveaux

Par exemple dans le diagramme ci-contre on considère deux niveaux de l'atome :
— le niveau fondamental : c'est celui de plus basse énergie ; l'état quantique de l'atome est noté $|g\rangle$ (ground state) et son énergie E_g.
— le premier niveau excité ; l'état atomique est noté $|e\rangle$ et son énergie E_e.

Si on envoit sur l'atome dans son état fondamental un photon d'énergie exactement $E_e - E_g$ le photon est absorbé par l'atome qui passe dans le niveau excité : $|g\rangle \to |e\rangle$. Les énergies mises en jeu à l'échelle atomique sont de l'ordre de l'électron-volt (1.6×10^{-19} J) ; le rayonnement lumineux associé au photon a une longueur d'onde $\lambda = \frac{c}{\nu} = \frac{hc}{E_e - E_g}$ où c est la vitesse de la lumière (3×10^8 ms^{-1}) et h la constante de Planck (6.6×10^{-34} Js) ; l'ordre de grandeur des longueurs d'onde correspondant aux énergies atomiques de l'ordre d'un eV est entre 0.4 et 1 μm ; c'est le domaine de la lumière visible.

L'atome revient dans son état fondamental au bout d'un temps moyen appel é durée de vie du niveau excité, en émettant un photon de même énergie $E_e - E_g$ (émission spontanée). La durée de vie d'un niveau atomique varie de quelques nanosecondes à la seconde.

Si on envoit un photon d'énergie $E_e - E_g$ sur l'atome quand il est encore dans l'état excité l'atome va se désexciter en émettant un photon à la même énergie (émission induite)

Supposons qu'on éclaire continuement l'atome avec cette radiation lumineuse composée de photons d'énergie $E_e - E_g$ (radiation résonante), l'atome va osciller entre l'état $|g\rangle$ à l'état $|e\rangle$. A l'instant t il sera dans un état de superposition

$$|\psi\rangle = \cos(\omega t/2)\,|g\rangle + \sin(\omega t/2)e^{i\phi}\,|e\rangle \tag{1.1}$$

On voit que si on associe à l'état $|g\rangle$ le qubit $|0\rangle$ et à l'état $|e\rangle$ le qubit $|1\rangle$ on peut, en jouant sur le temps d'éclairement, mettre l'atome dans n'importe quel état de superposition $\alpha\,|0\rangle + \beta\,|1\rangle$.

Pour mesurer l'état de l'atome à un moment donné on envoie sur celui-ci une impulsion laser "accordée" sur une transition $|g\rangle \to |a\rangle$ qui n'a pas d'équivalent à partir de l'état $|e\rangle$. Si le photon est absorbé c'est que le système est dans l'état $|g\rangle$ sinon il est dans l'état $|e\rangle$.

Polarisation d'un photon

Une onde électromagnétique, la lumière par exemple, peut être représentée mathématiquement par un champs vectoriel transverse, i.e. orthogonal à la direction de propagation. Dans un référentiel $(O, \hat{e_x}, \hat{e_y}, \hat{e_z})$, de coordonnés (x, y, z), choisi tel que l'onde se propage selon l'axe des z , le champ électrique est décrit par

$$\overline{E}(t, z) = \overline{E}_0 e^{i(\omega t - kz)}$$

où $\overline{E}_0 = E_{0x}\hat{e_x} + E_{0y}\hat{e_y}$. Le vecteur $\overline{E}_0$, vu comme un nombre complexe, définit la *polarisation* de l'onde. L'intensité de l'onde est proportionnelle au module au carré de $\overline{E}_0$: $\|\overline{E}_0\|^2$. La pola-

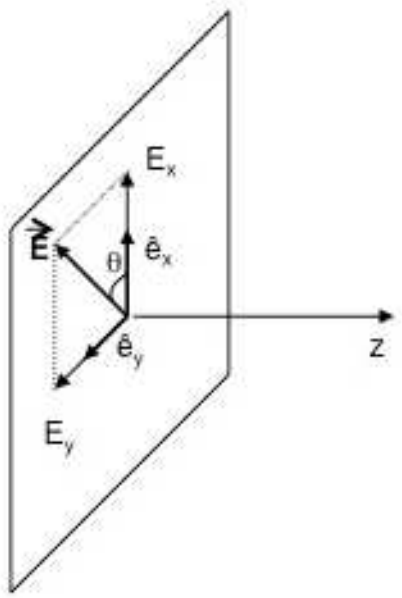


FIGURE 1.2 – Onde polarisée.

risation peut être mise en évidence à l'aide de cristaux ayant une propriété optique particulière : la biréfringence. Si nous envoyons sur une lame biréfringente un faisceau d'intensité I, polarisé linéairement suivant une direction qui fait un angle θ avec l'axe ordinaire du cristal qu'on prend comme axe Ox : le faisceau est séparé en un faisceau polarisé suivant Ox d'intensité $I\cos^2\theta$ et un autre faisceau polarisé suivant Oy d'intensité $I\sin^2\theta$.

Planck et Einstein ont suggéré au début du XXème siècle que la lumière puisse aussi être décrite en termes de flot de *photons*. Les sources de lumière "classiques" émettent des grandes quantités de photons même pour des faibles intensités (plusieurs milliards de milliards de photon à la seconde pour une lampe de 1W) ce qui fait que l'aspect "corpusculaire" de la lumière est difficile à mettre en évidence. L'avènement récent de l'optique quantique et des nanotechnologies a permis de développer des sources qui émettent des photons "un par un", c'est à dire séparés par des intervalles de temps mesurables avec la technologie actuelle (nanoseconde).

Comment interpréter l'expérience du dédoublement du faisceau lumineux dans une lame biréfringente si on considère le faisceau comme un flot discret de photons ? Quand un photon arrive à l'entrée de la lame, quel chemin va-t-il choisir ? Comment se fait-il qu'une fraction $\cos^2\theta$ va passer d'un côté et qu'une fraction $\sin^2\theta$ va passer de l'autre ?

La réponse est donnée par la mécanique quantique : le photon est un "objet quantique" ; on associe un état quantique à chaque vecteur de base de polarisation de l'onde : $|x\rangle$ pour l'état de polarisation suivant l'axe Ox et $|y\rangle$ pour l'état de polarisation suivant l'axe Oy. A l'orientation θ de la polarisation on associe l'état

$$|\theta\rangle = \cos\theta\ |x\rangle + \sin\theta\ |y\rangle \tag{1.2}$$

Quelle trajectoire va suivre le photon qui se trouve dans cet état ? La réponse de la mécanique quantique est qu'*on ne peut pas le savoir*. Mais ce qu'on peut connaitre (postulat de la mesure) c'est la probabilité que le photon sorte polarisé suivant x et qui est donnée par $\cos^2\theta$ et la probabilité complémentaire qu'il sorte polarisé suivant y, donnée par $\sin^2\theta$. Donc, en moyenne, si N est le nombre total de photons qui traversent la lame, on en trouvera $N\cos^2\theta$ sortant avec la polarisation Ox et $N\sin^2\theta$ sortant avec la polarisation Oy. Les coefficients $\cos\theta$ et $\sin\theta$ sont en fait des *amplitudes de probabilité* de trouver le photon dans l'état $|x\rangle$ ou $|y\rangle$ respectivement.

On peut associer un qubit à chacun des deux états de polarisation du photon, par exemple

$$\begin{aligned} |x\rangle &\rightarrow |0\rangle \\ |y\rangle &\rightarrow |1\rangle \end{aligned}$$

En jouant sur l'orientation du polariseur et sur le type de polarisation (linéaire, circulaire, elliptique) on peut construire là aussi un état quelconque de superposition $\alpha|0\rangle + \beta|1\rangle$.

1.2 Qubits et postulats quantiques

Il est temps maintenant de préciser les premiers postulats de la mécanique quantique.

1.2.1 Postulat de l'état d'un système quantique

Les états d'un système quantique sont décrits comme étant des éléments d'un espace vectoriel, appelé espace des états noté $\mathcal{E}$. La dimension de cet espace peut être finie ou infinie selon le système considéré. Dans cet espace on peut définir une base dénombrable et un produit scalaire (espace de Hilbert).

Les états du systéme quantique associé à un qubit sont les éléments d'un espace à deux dimensions, engendrés par les états de la base $|0\rangle$ et $|1\rangle$ (on verra comment le troisième postulat permet de choisir cette base). Tout état sera donc de la forme

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.3}$$

On retrouve donc là la spécificité des qubits de pouvoir se trouver dans un état de superposition.

Nous verrons plus loin avec le postulat de la mesure que les coefficients α et β sont en fait des amplitudes de probabilités et doivent satisfaire $|\alpha|^2 + |\beta|^2 = 1$.

La notation abstraite de Dirac pour l'état $|\psi\rangle$ peut conduire à différentes repésentations mathématiques : l'état peut être repésenté par une fonction $\psi(\mathbf{r}, t)$ (formalisme des fonctions d'ondes et de la mécanique ondulatoire), ou par une matrice (notament dans le cas d'espaces de dimensions finies), ou par les deux (matrice de fonctions). Dans notre espace à deux dimensions on peut utiliser une représentation matricielle :

$$|0\rangle \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad ; \quad |1\rangle \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.4}$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{1.5}$$

Rappelons les quelques de base d'algèbre linéaire exprimées dans la notation de Dirac.

— le *produit scalaire hermitien* de deux vecteurs $|\psi\rangle$ et $|\phi\rangle$ est noté $\langle\psi\,|\phi\rangle$ et il satisfait $\langle\psi\,|\phi\rangle = \overline{\langle\phi\,|\psi\rangle}$ et $\langle\psi\,|\lambda_1\phi_1+\lambda_2\phi_2\rangle = \lambda_1\langle\psi\,|\phi_1\rangle + \lambda_2\langle\psi\,|\phi_2\rangle$; les états $\langle 0|$, $\langle 1|$ et $\langle\psi|$ duaux de$|0\rangle$, $|1\rangle$ et $|\psi\rangle$, sont représentés par les matrices-ligne

$$\langle 0| \to (1\ 0) \quad ; \quad \langle 1| \to (0\ 1) \quad ; \quad \langle\psi| \to \left(\overline{\alpha}\ \overline{\beta}\right)$$

— la *norme* du vecteur $|\psi\rangle$ est notée $\|\psi\|^2 = \langle\psi\,|\psi\rangle$; les états de base sont *orthonormés* ce qui équivaut à

$$\begin{aligned}\langle 0\,|1\rangle &= 0\\ \langle 0\,|0\rangle &= \langle 1\,|1\rangle = 1\end{aligned}$$

Si $|\psi\rangle = \alpha\,|0\rangle+\beta\,|1\rangle$ et $|\phi\rangle = \gamma\,|0\rangle+\delta\,|1\rangle$ alors $\langle\psi\,|\phi\rangle = \overline{\alpha}\gamma+\overline{\beta}\delta$ et $\|\psi\|^2 = |\alpha|^2+|\beta|^2$, $\|\phi\|^2 = |\gamma|^2+|\delta|^2$; La représentation matricielle des états conduit à

$$|\phi\rangle \to \begin{pmatrix}\gamma\\ \delta\end{pmatrix} \quad ; \quad \langle\psi| \to (\overline{\alpha}\ \overline{\beta}) \Rightarrow \langle\psi\,|\phi\rangle = (\overline{\alpha}\ \overline{\beta})\begin{pmatrix}\gamma\\ \delta\end{pmatrix} = \overline{\alpha}\gamma+\overline{\beta}\delta$$

1.2.2 Postulat sur les grandeurs observables

A toute grandeur observable est associé un opérateur liné aire (hermitique) agissant dans l'espace des états $\mathcal{E}$.

Par exemple à l'énergie totale du système est associée l'opérateur hamiltonien H ; à la polarisation du photon est associé l'opérateur de polarisation P.

Dans les situations que nous considérerons ces opérateurs auront un ensemble discret de valeurs propres et d'états propres ; par exemple pour un observable $\mathcal{A}$ auquel est associé un opérateur A

$$\exists\, a_n \in \mathbb{C} \text{ et } |\phi_n\rangle \in \mathcal{E}, \text{ tels que } A\,|\phi_n\rangle = a_n\,|\phi_n\rangle \quad \text{pour } n = 1..N = \dim(\mathcal{E})$$

Les états $|\phi_n\rangle$ sont orthonormés et *constituent une base dans $\mathcal{E}$* :

$$\begin{aligned}\langle\phi_n\,|\phi_m\rangle &= \delta_{nm}\\ \forall\,|\psi\rangle \in \mathcal{E} \quad |\psi\rangle &= \sum_n \alpha_n\,|\phi_m\rangle \text{ avec } \alpha_n = \langle\phi_n\,|\psi\rangle\end{aligned}$$

Dans la première équation δ_{nm} est le symbole de Kronecker défini par $\delta_{nm} = 1$ si $n = m$ et 0 sinon.

Dans notre exemple du qubit les états $|0\rangle$ et $|1\rangle$ sont les états propres d'une grandeur observable. Si le système physique est un atome l'observable est l'énergie de l'atome et les états $|0\rangle$ et $|1\rangle$ correspondent aux états $|g\rangle$ et $|e\rangle$ (état fondamental et premier état excité) de l'atome. Dans le cas où le système quantique est le photon l'observable est la polarisation qui peut prendre les deux état $|x\rangle$ et $|y\rangle$. Comme ces états forment une base dans l'espace des états du qubit, on a $\forall\,|\psi\rangle \in \mathcal{E} \quad |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.

— Exemple : les *opérateurs de projection (ou projecteurs)* sur les états de base :

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

sont tels que

$$P_0\,|\psi\rangle = |0\rangle\langle 0|\,|\psi\rangle = \alpha\,|0\rangle \text{ et } P_1\,|\psi\rangle = |1\rangle\langle 1|\,|\psi\rangle = \beta\,|1\rangle$$

En représentation matricielle

$$P_0 = \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} \text{ et } P_1 = \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$$

1.2.3 Postulat de la mesure

Soit un observable $\mathcal{A}$ auquel est associé l'opérateur A de valeurs propres $\{a_n\}$ et d'états propres $\{\phi_n\}$. Quand un système initialement dans un état $|\psi\rangle$ est soumis à la mesure de l'observable $\mathcal{A}$

- *les seuls résultats possibles sont les $\{a_n\}$, valeurs propres de A*
- *la probabilité d'obtenir la valeur a_n est donnée par $\mathcal{P}(a_n) = |\langle\phi_n\,|\psi\rangle|^2$*
- *après la mesure si le résultat est a_n le système se trouve projeté dans l'état $|\phi_n\rangle$.*
- *Si le système est déjà dans un état propre $|\phi_n\rangle$ de A, c'est-à -dire si $|\psi\rangle = |\phi_n\rangle$ la mesure de $\mathcal{A}$ donnera a_n avec certitude.*

C'est donc le système de mesure qui va fixer la base des états dans $\mathcal{E}$: les états de base sont les états propres de l'observable mesuré.

Appliquons ce postulat à notre système physique porteur de qubit.

- Dans le cas de l'atome la "lecture" s'effectue en envoyant sur l'atome une impulsion laser accordée sur une transition qui permet de distinguer l'état fondamental $|g\rangle$ de l'état excité $|e\rangle$. Ces deux états sont "états propres" de la mesure, les valeurs propres correspondantes sont l'énergie de ces états E_g ou E_e.
- Dans le cas du photon c'est l'analyseur qui est l'appareil de mesure et l'état résultant ne peut être que $|x\rangle$ ou $|y\rangle$.

Nous allons nous abstraire du système physique et du dispositif de mesure en notant de façon générique $|0\rangle$ et $|1\rangle$ les deux états possibles du système de mesure, qui serviront de base dans l'espace des états du qubit. On appelle cette base générique la *base de calcul*. Par exemple si le système est dans l'état $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ le résultat de la mesure sera obtenu avec une certaine probabilité dont *l'amplitude* est définie par

$$\begin{aligned} \alpha &= \langle 0\,|\psi\rangle \quad \text{amplitude de probabilité d'obtenir l'état } |0\rangle \\ \beta &= \langle 1\,|\psi\rangle \quad \text{amplitude de probabilité d'obtenir l'état } |1\rangle \end{aligned}$$

1.3 Une première application : la cryptographie quantique

1.3.1 Quelques mots sur la cryptographie

Le problème de la transmission de messages secrets est vieux comme le monde. Le problème est résolu si on sait coder le message de façon à ce qu'un espion qui ne connait pas la clé de décodage ne puisse pas le déchiffrer, et que le destinataire du message qui possède la clé de décodage puisse facilement déchiffrer. Dans le folklore anglo-saxon standard en matière de cryptographie, on appelle Alice et Bob les personnes qui échangent le message et Eve (comme eavesdropper, celui ou celle qui écoute aux portes) l'espion(ne).

Il y a à ce jour essentiellement deux types de codage :

- les codages à clé privée : Alice et Bob possèdent tous les deux la clé qui sert à la fois à coder et à décoder (clé symétrique). Il existe des algorithmes de codage qui sont incassables si on ne possède pas la clé. La faiblesse dans ces protocoles se situe dans la capacité pour Alice et Bob de se transmettre la clé de codage de façon fiable.
- les codages à clé publique, dont le plus connu est le RSA (Rivest, Shamir, Adelman, 1977). Alice fabrique la clé de codage et la clé de décodage (codage asymétrique). Elle transmet (publiquement) à Bob la clé de codage. Il est en principe impossible, étant donnée la connaissance humaine du moment, d'obtenir la clé de décodage à partir de la clé de codage ; par exemple il est impossible d'obtenir les facteurs premiers (= clé de décodage) d'un très grand nombre entier (= clé de codage). Bob ne pourra donc que coder. Ce qu'il fait, puis

il transmet le message à Alice qui pourra décoder. La faiblesse du protocole réside dans le fait que la connaissance humaine peut évoluer ; un espion particulièrement ingénieux peut trouver le moyen d'obtenir la clé de décodage à partir de la clé de codage, par exemple dans RSA, trouver dans un temps raisonnable les facteurs premiers d'un grand nombre entier. L'algorithme quantique découvert par Peter Shor en 1995 permet effectivement de réaliser rapidement cette opération. Il ne reste qu' à construire l'ordinateur quantique qui le mettra en oeuvre !

1.3.2 Transmission sécurisée de clès secrètes de codage

On se place dans le cadre des protocoles à clé privée.

Nous allons voir que les principes de la mécanique quantique nous permettront d'avoir la (quasi)certitude qu'une information transmise entre deux points A et B (Alice et Bob pour les anglo-saxons) a été ou non interceptée par un espion. Si elle n'a pas été interceptée, elle constituera alors de façon sûre la clé de codage d'un protocole à clé privée.

L'information va être véhiculée par des photons dont la polarisation sert de support au codage de l'information. Au lieu de $|x\rangle$ et $|y\rangle$ désignons par $|\uparrow\rangle$ et $|\longrightarrow\rangle$ les deux états de base de polarisation du photon. A chacun des ces états on peut associer la valeur d'un bit :

$$\begin{aligned} |\uparrow\rangle &\rightarrow 1 \\ |\longrightarrow\rangle &\rightarrow 0 \end{aligned}$$

Pour coder son message, Alice dispose d'une source de photons "un par un" qu'elle envoie sur un polariseur ; elle oriente le polariseur horizontalement ou verticalement selon qu'elle veuille produire un 0 ou un 1. Bob reçoit les photons dans un analyseur qui détermine leur polarisation. Si on en restait là, un espion qui intercepte le message peut procéder exactement comme Bob , lire le message, et le re-transmettre tel quel à Bob sans que celui-ci ne s'aperçoive de rien.

Quelle solution la mécanique quantique propose-t-elle qui permette d' éliminer cette difficulté ? La réponse a été trouvée par C. H. Bennett et G. Brassard en 1984 dans un protocole nommé depuis BB84.

Ils proposent de rajouter une autre base de polarisation dans laquelle les polariseurs sont inclinés à 45° par rapport à la verticale (horizontale). Les états du photon seront (d'après l'éq.(1.2) avec $\theta = 45°$

$$\begin{aligned} |\nearrow\rangle &= \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\longrightarrow\rangle\right) \\ |\searrow\rangle &= \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\longrightarrow\rangle\right) \end{aligned}$$

On décide arbitrairement (mais définitivement) d'associer

$$\begin{aligned} |\nearrow\rangle &\rightarrow 1 \\ |\searrow\rangle &\rightarrow 0 \end{aligned}$$

Donc le bit 1 pourra être codé de deux façons différentes, par la polarisation $|\uparrow\rangle$ ou par la polarisation $|\nearrow\rangle$. On va désigner par $\oplus$ la base de polarisation horizontale-verticale et par $\otimes$ la base orientée à 45°.

En vertu du postulat de la mesure, si un photon polarisé dans l'état $|\nearrow\rangle$ est envoyé sur un analyseur orienté dans la base $\oplus$ (en d'autres termes si on *mesure* la polarisation dans la base $\oplus$)

le résultat sera $|\uparrow\rangle$ ou $|\longrightarrow\rangle$ avec une égale probabilité de 1/2. En revanche le même photon analysé dans la base $\otimes$ donnera $|\nearrow\rangle$, c'est à dire 1, avec certitude.

Comment Alice et Bob procèdent-ils pour se transmettre l'information ?

Alice va coder son message en binaire *en choisissant aléatoirement, pour chaque bit, la base de polarisation*, $\oplus$ ou $\otimes$, mais en notant la succession de choix de bases. Lors de la réception des photons Bob de son côté procède de même avec l'orientation de son analyseur et conserve lui aussi les différents choix qu'il a fait *et communique publiquement cette liste à Alice* (c'est à dire par une voie non sécurisée). Alice compare cette liste à la sienne et transmet à Bob, toujours publiquement, *l'intersection des deux listes* c'est à dire quelles sont les *positions* des bits dans la séquence qui auront bien la même valeur pour Alice et Bob puisque pour ces bits là ils auront tous les deux utilisés le même choix de codage. Exemple :

Alice	bits à transmettre	0	0	1	1	0	0
Alice	choix de base de codage	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$
Alice	polarisation envoyée	$\|\longrightarrow\rangle$	$\|\longrightarrow\rangle$	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\longrightarrow\rangle$	$\|\searrow\rangle$
Bob	choix de base de codage	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$
Bob	polarisation mesurée	$\|\longrightarrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\searrow\rangle$	$\|\longrightarrow\rangle$
Bob	bits lus	0	1	1	1	0	0
Alice et Bob	bits acceptés	oui	non	oui	oui	non	non
Alice et Bob	message secret	0		1	1		

Cet ensemble de bits constituera le message secret (une clé de codage par exemple).

Comment s'assurer que ce message n'a pas été intercepté par un espion ? Si un espion intercepte un photon, il va lire la polarisation dans l'une des deux bases qu'il choisira, lui-aussi aléatoirement. Ce faisant il va projeter la polarisation du photon intercepté sur l'état qu'il lit. Par exemple supposons qu'Alice ait envoyé un photon $|\longrightarrow\rangle$ (un 0 donc) et que l'espion utilise la base $\otimes$; il va trouver avec une chance sur deux $|\searrow\rangle$ par exemple, et lire dans ce cas la bonne valeur, 0. Le photon est maintenant projeté dans l'état $|\searrow\rangle$ et parvient à Bob ; supposons que Bob ait fait le même choix de base qu'Alice, $\oplus$ en l'occurence, il a une chance sur deux de lire $|\uparrow\rangle$, c'est à dire une valeur différente de celle du bit émis. Donc l'interception du photon par un espion peut modifier la valeur du bit, avec une probabilité de 25% (50%×50%).

Pour s'assurer que le canal de transmission n'est pas "écouté" il suffit donc à Alice et Bob de prendre au hasard un échantillon des bits acceptés, de se les communiquer publiquement et de les comparer : *ils doivent être tous identiques*. Une seule différence signe la présence d'un intrus sur la ligne [3]. Si le nombre de bits échangés est suffisament grand, le fait qu'ils soient tous identiques correspond à la certitude de n'avoir pas été écouté car la possibilité résiduelle que l'espion les ait tous écoutés et n'en ait modifié aucun a une probabilité négligeable : par exemple pour un échantillon de 1000 bits échangés elle est de $0.75^{1000} \simeq 10^{-180}$.

1.4 Manipulations d'un qubit

Nous avons vu que la mesure altère en général l'état d'un qubit puisqu'il en sort nécessairement dans un état propre de l'observable mesuré. Par contre l'environnement peut agir sur le qubit pour faire évoluer son état tant qu'aucune mesure (aucune "prise d'information") n'est réalisée. L'évolution de l'état quantique entre deux mesures est gouvernée par un nouveau postulat.

3. ou d'une erreur de transmission. L'intrusion n'est avérée que si le taux de bits qui diffèrent dans le processus de reconnaissance est sup érieur au taux d'erreur de transmission.

1.4.1 Postulat d'évolution

Entre deux mesures le système quantique évolue avec le temps. Cette évolution de l'état résulte de l'application d'un opérateur linéaire, l'opérateur d'évolution

$$|\psi(t_0)\rangle \rightarrow |\psi(t)\rangle = U(t,t_0)\,|\psi(t_0)\rangle$$

L'opérateur jouit d'une propriété particulière qui résulte de la conservation de la norme de l'état quantique au cours du temps. En effet on doit avoir

$$\begin{aligned}\langle\psi(t_0)\,|\psi(t_0)\rangle &= 1 = \langle\psi(t)\,|\psi(t)\rangle \\ &= \langle\psi(t_0)\,U^\dagger U\,|\psi(t_0)\rangle \text{ où } U^\dagger = \overline{(U^t)} \\ &\Rightarrow U^\dagger U = UU^\dagger = I\end{aligned}$$

L'opérateur est *unitaire*.

Rappel de quelques définitions sur les opérateurs et les matrices

A est un opérateur agissant dans un espace $\mathcal{E}$; $|i\rangle, i = 1...\dim\mathcal{E}$ une base orthonormée dans $\mathcal{E}$;on appelle *éléments de matrice* de l'opérateur

$$A_{ij} = \langle i|\,A\,|j\rangle$$

— Opérateur adjoint ou conjugué hermitique, $A^\dagger$ d'un opérateur A : $\left(A^\dagger\right)_{ij} = \overline{A_{ji}} \Leftrightarrow \langle i|\,A^\dagger\,|j\rangle = \overline{\langle j|\,A\,|i\rangle}$

L'action de l'opérateur adjoint se situe dans l'espace dual :

$$A\,|\phi\rangle = |\psi\rangle \Leftrightarrow \langle\phi|\,A^\dagger = \langle\psi|$$

— Opérateur hermitique : $A^\dagger = A$

— Opérateur unitaire $A^\dagger A = AA^\dagger = I \Rightarrow A^\dagger = A^{-1}$. Un opérateur ayant cette propriété *conserve la norme*. En effet

$$\begin{aligned}A\,|\phi\rangle &= |\psi\rangle \Leftrightarrow \langle\phi|\,A^\dagger = \langle\psi| \\ \langle\psi\,|\psi\rangle &= \langle\phi|\,A^\dagger A\,|\phi\rangle = \langle\phi\,|\phi\rangle\end{aligned}$$

La question est de savoir quel est cet opérateur unitaire. En fait l' évolution temporelle de l'état est gouvernée par la célèbre équation de Shrödinger

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

où $\mathcal{H}$ est l'opérateur hamiltonien, c'est-à-dire l'opérateur quantique associé à l'observable "énergie totale du système". La solution formelle de cette équation est

$$|\psi(t)\rangle = \exp(-i\frac{t-t_0}{\hbar}\mathcal{H})\,|\psi(t_0)\rangle$$

de laquelle on déduit

$$U(t,t_0) = \exp(-i\frac{t-t_0}{\hbar}\mathcal{H})$$

On peut "ajuster" physiquement l'opérateur hamiltonien par un choix approprié d'interactions du système avec son environnement ce qui nous permettra donc de *piloter* l'évolution de son état quantique.

1.4.2 Espace des valeurs d'un qubit

Valeurs discernables En fait, deux qbits de valeurs $w \in \mathbb{S}^3$ et $w' \in \mathbb{S}^3$ telles que

$$\exists \lambda \in \mathbb{C}, |\lambda| = 1 \text{ et } w' = \lambda w \tag{1.6}$$

sont indiscernables par des mesures physiques. Soit A un opérateur hermitien sur $\mathbb{C}^2$, et $|w_1\rangle, |w_2\rangle$ une base orthonormée de vecteurs propres de A tels que $A|w_1\rangle = \lambda_1 |w_1\rangle, A|w_2\rangle = \lambda_2 |w_2\rangle$.

$$w = \alpha_1 |w_1\rangle + \alpha_2 |w_2\rangle$$

et

$$w' = \lambda\alpha_1 |w_1\rangle + \lambda\alpha_2 |w_2\rangle .$$

La distribution de probabilité des résultats d'une mesure (correspondant à A) est la même pour w et w' . Donc aucune suite de mesures appliquées à w, w' ne parviendra à les distinguer. Notons $\sim$ l'équivalence définie par (1.6). On peut considérer que "l'espace des valeurs d'un qubit" est l'ensemble des classes de $\mathbb{S}^3$ pour cette équivalence :

$$\mathbb{S}^3/\sim .$$

(Cet ensemble est l'espace projectif complexe de dimension 1, noté $\mathbb{P}^1(\mathbb{C})$) Nous allons voir, ci-dessous, qu'il est homéomorphe à la sphère $\mathbb{S}^2$ i.e. le sous-espace de $\mathbb{R}^3$:

$$\{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}.$$

Application de $\mathbb{S}^3$ dans $\mathbb{S}^2$: fibration de Hopf
Soit

$$(u, v) \in \mathbb{C}^2 \text{ tel que } |u|^2 + |v|^2 = 1.$$

Il existe des nombres réels $r \geq 0, \rho \geq 0, \alpha \in [0, 2\pi[, \beta \in [0, 2\pi[$ tels que

$$u = re^{i\alpha}, \quad v = \rho e^{i\beta}.$$

Donc (u, v) est équivalent, modulo $\sim$, au couple

$$(r, \rho e^{i(\beta-\alpha)}). \tag{1.7}$$

et comme $r \in \mathbb{R}$, ce couple peut être vu comme un point de $\mathbb{S}^2$; sur la figure 1.3, nous représentons un point $(x, u) \in \mathbb{R} \times \mathbb{C}$ comme le point de la sphère $\mathbb{S}^2$ dont la projection sur l'axe vertical (nord-sud) est x et la projection horizontale (dans le plan équatorial) est u.
N.B.mais ce point $(r, \rho e^{i(\alpha-\beta)})$ est nécessairement dans l'hémisphère "nord", donc on ne peut espérer obtenir une surjection de $\mathbb{S}^3$ sur $\mathbb{S}^2$ par la formule 1.7.
Définissons

$$\theta := 2\arctan(\rho/r) \text{ si } r \neq 0, \quad \theta := \pi \text{ si } r = 0, \quad \varphi := \beta - \alpha.$$

On obtient

$$(r, \rho e^{i(\beta-\alpha)}) = (\cos(\theta/2), \sin(\theta/2)e^{i\varphi})$$

Et on définit

$$\mathrm{FH(u, v)} := (\cos(\theta), \sin(\theta)\mathrm{e}^{\mathrm{i}\varphi}). \tag{1.8}$$

(voir la figure 1.3). Remarquons que la formule (1.8) définit bien une application :
- si $u \neq 0, v \neq 0$ alors les nombres $r \geq 0, \rho \geq 0, \alpha \in [0, 2\pi[, \beta$ sont entièrement déterminés par u, v

et donc le membre droit de (1.8) est bien défini ;
- si $u = 0$ alors $r = 0$, donc $\theta = \pi$, de facon que le membre droit de (1.8) vaut $(-1, 0)$ (indépendamment du choix de α) ;
- si $v = 0$ alors $\rho = 0$, donc $\theta = 0$, de facon que le membre droit de (1.8) vaut $(1, 0)$ (indépendamment du choix de β) ;
De plus $|\cos(\theta)|^2 + |\sin(\theta)e^{i\varphi}|^2 = 1$ donc

$$\mathrm{FH} : \mathbb{S}^3 \to \mathbb{S}^2$$

Montrons que cette application FH (la "fibration de Hopf") est continue.

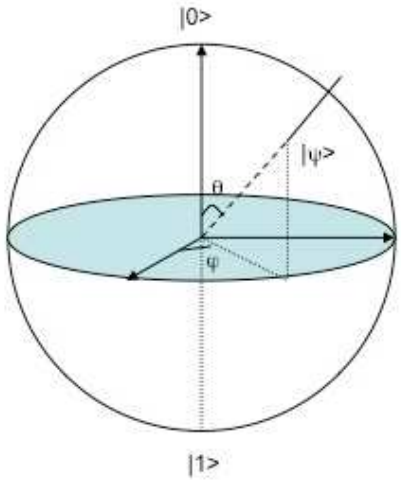


FIGURE 1.3 – Sphère de Bloch

N.B. comme la relation binaire $(u, v) \mapsto (r, \rho, \alpha, \beta)$ n'est ni une application, ni continue en les points de $(\mathbb{R} \setminus \{0\}) \times (\mathbb{R} \setminus \{0\})$, un peu de soin est nécessaire.
Vérifions que, pour tous $(u, v) \in \mathbb{S}^3$

$$\mathrm{FH(u, v)} := (|\mathrm{u}|^2 - |\mathrm{v}|^2, 2\bar{\mathrm{u}}\mathrm{v}) \tag{1.9}$$

Si $u \neq 0$, et $v \neq 0$, alors

$$\cos(\theta/2) = r = |u|, \;\; \sin(\theta/2) = \rho = |v|, \;\; e^{i\varphi} = \frac{v}{|v|} \cdot (\frac{u}{|u|})^{-1}$$

En utilisant les identités $\cos(\theta) = \cos^2(\theta/2) - \sin(^2\theta/2)$ et $\sin(\theta) = 2\cos(\theta/2)\sin(\theta/2)$ on obtient

$$\cos(\theta) = |u|^2 - |v|^2, \sin(\theta) = 2|u||v|$$

donc

$$\mathrm{FH(u, v)} = (|\mathrm{u}|^2 - |\mathrm{v}|^2, 2|\mathrm{u}||\mathrm{v}|\frac{\mathrm{v}}{|\mathrm{v}|} \cdot (\frac{\mathrm{u}}{|\mathrm{u}|})^{-1})$$

ce qui se simplifie en l'égalité (1.9).
Si $u = 0$ alors $\mathrm{FH(u, v)} = (-1, 0)$ ce qui est bien la valeur donnée par (1.9).

Si $v = 0$ alors $\mathrm{FH(u, v)} = (1, 0)$ ce qui est bien la valeur donnée par (1.9).
On voit clairement sur les formules (1.9) que FH est composée de fonctions continues, donc FH est continue.

Application de $\mathbb{S}^3/\sim$ dans $\mathbb{S}^2$ On remarque que $(u, v) \sim (u', v') \Rightarrow \mathrm{FH(u, v)} = \mathrm{FH(u', v')}$. On peut donc définir une application

$$\tilde{\mathrm{FH}} : \mathbb{S}^3/\sim \ \to \ \mathbb{S}^2$$

par

$$\tilde{\mathrm{FH}}([u, v]_\sim) := \mathrm{FH(u, v)}.$$

Nous allons voir que $\tilde{\mathrm{FH}}$ est une bijection et que, pour la topologie quotient sur $\mathbb{S}^3/\sim$ c'est un homéomorphisme.

Fait 1 *L'application* $\tilde{\mathrm{FH}}$ *est surjective.*

Soit $(r, w) \in \mathbb{R} \times \mathbb{C} \mid r^2 + |w|^2 = 1$.
Il existe $\theta \in \mathbb{R}$.

$$r = \cos(\theta), |w| = \sin(\theta).$$

Comme w et $\sin(\theta)$ ont le même module, il existe $\varphi \in \mathbb{R}$ tel que

$$w = \sin(\theta) e^{i\varphi}.$$

Alors

$$w = \mathrm{FH}(\cos(\theta/2), \sin(\theta/2)\mathrm{e}^{\mathrm{i}\varphi}).$$

(qed)

Fait 2 *L'application* $\tilde{\mathrm{FH}}$ *est injective.*

Supposons que $\tilde{\mathrm{FH}}([u, v]_\sim) = \tilde{\mathrm{FH}}([u', v']_\sim)$, i.e.

$$\mathrm{FH(u, v)} = \mathrm{FH(u', v')}$$

où $|u|^2 + |v|^2 = 1$ et $|u'|^2 + |v'|^2 = 1$.
Cas 1 : $u = 0$.
Alors $|v| = 1$. Donc $|u|^2 - |v|^2 = -1$, ce qui entraine que $|u'|^2 - |v'|^2 = -1$. Mais $|v^2| \leq 1$, donc $|u'|^2 = 0$ i.e. $u' = 0$. Dans ce cas

$$(u, v) \sim (u', v').$$

Cas 2 : $u \neq 0$.
Alors $|u|^2 - |v|^2 > -1$, d'où $|u'|^2 - |v'|^2 > -1$, donc $u' \neq 0$.
Nous connaissons les trois relations

$$|u|^2 - |v|^2 = |u'|^2 - |v'|^2 \quad (1.10)$$
$$2\bar{u}v = 2\bar{u'}v' \quad (1.11)$$
$$|u|^2 + |v|^2 = |u'|^2 + |v'|^2 \quad (1.12)$$

En additionnant (1.10) et (1.12) on trouve que $|u|^2 = |u'|^2$, donc $|u| = |u'|$,
En additionnant (1.10) et l'opposée de (1.12) on trouve que $|v|^2 = |v'|^2$, donc $|v| = |v'|$,
En multipliant (1.11) par $\frac{1}{|u|^2}$, on trouve que $\frac{v}{u} = \frac{v'}{u'}$, ce qui entraine que

$$(u, v) \sim (u', v').$$

(qed)
Notons $p : \mathbb{S}^3 \to \mathbb{S}^3/\sim$ la projection canonique :

$$p(u, v) := [(u, v)]_\sim.$$

Rappelons la définition de la topologie de $\mathbb{S}^3/\sim$ obtenue à partir de la topologie habituelle sur $\mathbb{S}^3$

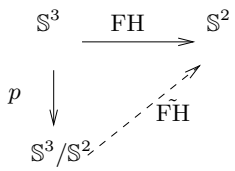


FIGURE 1.4 – La fibration de Hopf

(définie, par exemple , par la restriction à $\mathbb{S}^3$ de la distance euclidienne sur $\mathbb{R}^4$) et de l'opération de quotient par $\sim$: un sous-ensemble $U \subseteq \mathbb{S}^3/\sim$ est dit *ouvert* ssi

$$p^{-1}(U) \text{ est ouvert dans } \mathbb{S}^3.$$

Fait 3 *L'application* $\tilde{\text{FH}}$ *est continue.*

Soit Ω un ouvert de $\mathbb{S}^2$. Comme FH est continue

$$\text{FH}^{-1}(\Omega) \text{ est ouvert dans } \mathbb{S}^3.$$

Comme $\text{FH} = \tilde{\text{FH}} \circ \text{p}$

$$\text{FH}^{-1}(\Omega) = \text{p}^{-1} \circ \tilde{\text{FH}}^{-1}(\Omega)$$

ce qui prouve que $p^{-1} \circ \tilde{\text{FH}}^{-1}(\Omega)$ est ouvert, i.e. (par la définition de la topologie quotient) que

$$\tilde{\text{FH}}^{-1}(\Omega) \text{ est ouvert dans } \mathbb{S}^3/\sim$$

(qed)
Le fait suivant nous aidera à démontrer que $\tilde{\text{FH}}^{-1}$ est continue.

Fait 4 *L'espace topologique* $\mathbb{S}^3/\sim$ *est séparé.*

On remarque que, pour tous $(u, v), (u', v') \in \mathbb{S}^3$

$$(u, u') \sim (u', v') \Leftrightarrow \det((u, v), (u', v')) = 0.$$

L'application $\det : \mathbb{C}^4 \to \mathbb{C}$ est continue (c'est une fonction polynomiale). Considérons deux points

$$[(u, v)] \neq [(u', v')]$$

de $\mathbb{S}^3/\sim$ (nous omettons les indices $\sim$ dans la notation $[(u,v)]_\sim$). Montrons que ces points possèdent des voisinages disjoints dans $\mathbb{S}^3/\sim$.
Posons

$$\det((u,v),(u',v')) = \delta \in \mathbb{C}\setminus\{0\}.$$

Puisque det est continue, il existe $\varepsilon > 0$ tel que

$$\forall w \in \mathbb{C}^2, \forall w' \in \mathbb{C}^2, \mathrm{d}((u,v,u',v'),(w,w')) < \varepsilon \Rightarrow |\det(w,w') - \det((u,v),(u',v'))| < |\delta|/2$$

donc

$$\forall w \in \mathbb{C}^2, \forall w' \in \mathbb{C}^2, \mathrm{d}((u,v,u',v'),(w,w')) < \varepsilon \Rightarrow |\det(w,w')| > |\delta|/2. \tag{1.13}$$

Notons $\mathrm{B}(u,v,\varepsilon/2)$ (resp. $\mathrm{B}(u',v',\varepsilon/2)$) les boules ouvertes de centre (u,v) (resp. (u',v')) et de rayon $\varepsilon/2$ dans $\mathbb{S}^3$. Vérifions que

$$[\mathrm{B}(u,v,\varepsilon/2)] \cap [\mathrm{B}(u',v',\varepsilon/2)] = \emptyset \tag{1.14}$$

(Pour toute partie $Q \subseteq \mathbb{S}^3$, on note $[Q] := \{w \in \mathbb{S}^3, \exists q \in Q, w \sim q\}$).
Soient $(h,k) \in [\mathrm{B}(u,v,\varepsilon/2)], (h',k') \in [\mathrm{B}(u,v,\varepsilon/2)]$. Il existe des couples $w \in \mathrm{B}(u,v,\varepsilon/2), w' \in \mathrm{B}(u',v',\varepsilon/2)$ tels que $(h,k) \sim w$ et $(h',k') \sim w'$. on a alors

$$|\det((h,k),(h',k'))| = |\det(w,w')| \tag{1.15}$$

car (h,k) et w ne diffèrent que par un facteur de module 1 et de même pour (h',k') et w'. Par l'inégalité triangulaire $\mathrm{d}((u,v,u',v'),(w,w')) < \varepsilon$, donc par (1.13) $|\det(w,w')| > |\delta|/2$ et par (1.15)

$$\det((h,k),(h',k')) > |\delta|/2.$$

ce qui prouve bien l'affirmation (1.14) : les classes $[\mathrm{B}(u,v,\varepsilon/2)], [\mathrm{B}(u,v,\varepsilon/2)]$ sont disjointes. Donc les parties $p(\mathrm{B}(u,v,\varepsilon/2)), p(\mathrm{B}(u,v,\varepsilon/2))$ sont aussi disjointes. De plus

$$p^{-1}(p(\mathrm{B}(u,v,\varepsilon/2))) = [\mathrm{B}(u,v,\varepsilon/2)]$$

ce qui prouve que $p(\mathrm{B}(u,v,\varepsilon/2)$ est un ouvert de $\mathbb{S}^3/\sim$ et de même pour $p(\mathrm{B}(u',v',\varepsilon/2)$. Finalement $p(\mathrm{B}(u,v,\varepsilon/2)), p(\mathrm{B}(u',v',\varepsilon/2))$ sont des ouverts disjoints qui séparent $[u,v]$ de $[u',v']$.(qed)

Fait 5 *L'application* $\tilde{\mathrm{FH}}^{-1}$ *est continue.*

Il s'agit de montrer que l'image réciproque de tout ouvert de $\mathbb{S}^3/\sim$ par $\tilde{\mathrm{FH}}^{-1}$ est ouverte. Cela revient à prouver que l'image réciproque de tout fermé de $\mathbb{S}^3/\sim$ par $\tilde{\mathrm{FH}}^{-1}$ est fermée i.e. que l'image directe , par $\tilde{\mathrm{FH}}$, de tout fermé de $\mathbb{S}^3/\sim$ est fermé.
Comme l'application p est continue et l'espace $\mathbb{S}^3/\sim$ est séparé, $\mathrm{Im}(p)$ est un sous-espace compact de $\mathbb{S}^3/\sim$; et comme p est surjective, $\mathbb{S}^3/\sim$ est un espace compact.
Soit F une partie fermée de $\mathbb{S}^3/\sim$; c'est donc une partie compacte (puisque $\mathbb{S}^3/\sim$ est compact) ; donc $\tilde{\mathrm{FH}}(F)$ est compact, donc fermé (qed).
Nous avons finalement démontré que $\tilde{\mathrm{FH}}$ est un *homéomorphisme* de $\mathbb{S}^3/\sim$ dans $\mathbb{S}^2$.

1.4.3 Opérations logiques sur un qubit

Nous allons associer à l'évolution de l'état du qubit les opérations logiques nécessaires à la mise en oeuvre d'algorithmes. Par exemple les portes logiques classiques agissant sur un bit sont résumées dans le tableau ci-dessous

Porte logique$\backslash b_{in}$	0	1
EFFACE	0	0
IDENTITE	0	1
NON	1	0
SET	1	1

Une première difficulté apparaît : les "portes logiques" quantiques correspondent à des opérateurs unitaires, donc *réversibles.* Dans la table ci-dessus la porte EFFACE qui n'est pas réversible ne pourra pas être simulée par l'évolution d'un qubit. Ce point sera discuté au chapitre 2 (§2.2) où nous verrons que tout algorithme classique peut s'exprimer en termes de portes réversibles.

La seule opération réversible non triviale qu'on puisse réaliser sur un bit classique est le *NON* logique :

$$\begin{aligned} 0 &\rightarrow 1 \\ 1 &\rightarrow 0 \end{aligned}$$

Peut-on transposer cette opération au qubit, c'est -à-dire existe-t-il une opération unitaire qui réalise l'évolution

$$\begin{aligned} |0\rangle &\rightarrow |1\rangle \\ |1\rangle &\rightarrow |0\rangle \end{aligned}$$

Si on utilise la représentation matricielle des états, (équations (1.4,1.5)) alors (exercice) l'opérateur *NON* est représenté par la matrice carrée

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

On peut vérifier que cette matrice est bien unitaire.

La réalisation physique de cette opération est en général assez aisée. Par exemple pour l'atome irradié décrit par l'état (1.1) il suffit d'exposer l'atome initialement dans l'état $|0\rangle$ à l'éclairage laser pendant un temps t tel que $\omega t/2 = \pi/2$ (impulsion π) pour qu'il passe dans l'état $|1\rangle$ et vice-versa.

Si on applique une impulsion π (l'opérateur X) à un état quelconque, on obtient

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \overset{NON}{\rightarrow} |\psi\rangle_N = \alpha\,|1\rangle + \beta\,|0\rangle$$

ce qui revient simplement à échanger les "coordonnées" α et β.

Peut-on trouver d'autres matrices, autre que X ci-dessus, qui représent une opération sur un qubit ? Nous avons vu au paragraphe précedent que la réponse est oui et que toute matrice unitaire est susceptible de représenter une porte logique à un qubit. Donc, à la différence des bits classiques pour lesquels il n'existe qu'une seule opération non triviale, le *NON* logique, pour les qubit il existe une famille *continue* de transformations qui sont représentées par les matrices unitaires. Parmi celles qui sont particulièrement utilisées citons

— la porte Y définie par la matrice $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ dont la table de vérité est

$$\begin{aligned} |0\rangle &\rightarrow i\,|1\rangle \\ |1\rangle &\rightarrow -i\,|0\rangle \end{aligned}$$

— la porte Z définie par la matrice $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ou opérateur de *flip* dont la table de vérité est

$$\begin{aligned} |0\rangle &\rightarrow |0\rangle \\ |1\rangle &\rightarrow -|1\rangle \end{aligned}$$

— La porte de *Hadamard* définie par la matrice $H = \frac{1}{\sqrt{2}}(X + Z) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ dont la table de vérité est

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

— La porte $\pi/8$ définie par la matrice $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

On vérifie que ces matrices sont bien unitaires.

1.5 EXERCICES

Exercice 1 *Bases de polarisation*

Un photon polarisé suivant un angle α avec Ox est envoyé sur un analyseur qui fait un angle θ avec Ox.

1. Exprimer l'état $|\theta\rangle$ et l'état orthogonal $|\theta_\perp\rangle$ dans la base ($|x\rangle$,$|y\rangle$) ; Exprimer l'état $|\alpha\rangle$ toujours dans la base ($|x\rangle$,$|y\rangle$).
2. Etablir que
$$|\alpha\rangle = \cos(\alpha-\theta)\,|\theta\rangle + \sin(\alpha-\theta)\,|\theta_\perp\rangle$$
3. En déduire que la probabilité pour que le photon traverse l'analyseur est
$$p(\theta \to \alpha) = \cos^2(\alpha-\theta)$$

Exercice 2 *Mesure ; projecteurs*

1. Les états $|0\rangle$ et $|1\rangle$ sont états propres d'un observable Z avec les valeurs propres +1 et -1 respectivement :
$$\begin{aligned} Z\,|0\rangle &= |0\rangle \\ Z\,|1\rangle &= -\,|1\rangle \end{aligned}$$
Si on utilise la représentation matricielle des états $|0\rangle$ et $|1\rangle$ l'opérateur Z sera représenté par une matrice 2x2. Construire cette matrice.
2. On construit les opérateurs $P_0 = |0\rangle\langle 0|$ et $P_1 = |1\rangle\langle 1|$;
   (a) Donner leur représentation matricielle
   (b) Quelle est leur action sur l'état $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$? Evaluer $\langle\psi|\,P_i\,|\psi\rangle$.
   (c) Vérifier que ces opérateurs satisfont $P_i^2 = P_i, i = 0, 1$. On appelle projecteur un opérateur jouissant de cette propriété.
   (d) Exprimer Z comme une combinaison linéaire de P_0 et P_1 ; montrer que $P_0 + P_1 = I$
   (e) En déduire l'interprétation que l'on peut donner au nombre $\langle\psi|\,Z\,|\psi\rangle$

Exercice 3 *Phase globale ; phase relative*

On considère les états $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $|\psi_G\rangle = e^{i\varphi}\,|\psi\rangle = \frac{e^{i\varphi}}{\sqrt{2}}(|0\rangle + |1\rangle)$ où φ est une nombre réel.

1. Montrer que, dans n'importe quelle base, les deux états sont physiquement indiscernables.
2. Montrer qu'au contraire les deux états $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $|\psi_R\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ sont discernables (appliquer sur ces deux états l'opérateur de Hadamard).

La conclusion est que les états sont définis à *une phase globale près*. En revanche deux états qui diffèrent par *une phase relative* sont distincts.

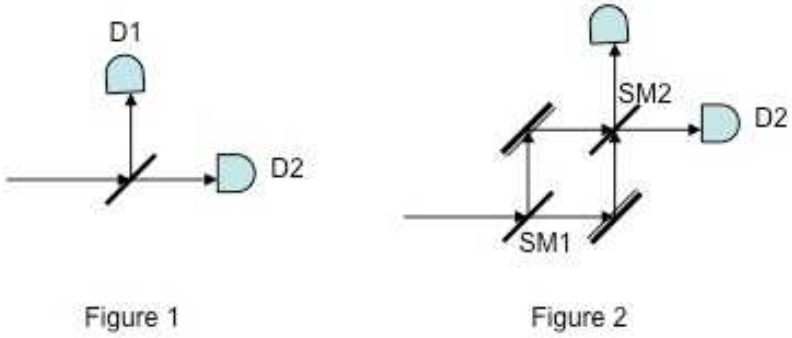


FIGURE 1.5 – interferometre de Mach-Zehnder

Exercice 4 *Interféromètre de Mach-Zehnder*

Si on envoie un faisceau lumineux sur une lame semi réfléchissante, on observe un rayon transmis et un rayon réfléchi chacun d'intensité moitié de celle du rayon incident. L'interféromètre de Mach-Zehnder (figure 2) est une succession de deux lames semi-réfléchissantes séparées par des miroirs. Le problème est de déterminer la quantité de lumière arrivant dans les detecteurs D_1 et D_2.

1. *Interprétation classique.* La lumière est une onde électromagnétique.
   - A chaque réflexion l'amplitude de l'onde est multipliée par un facteur i
   - Sur la lame semi réfléchissante l'amplitude de chaque faisceau émergent est multipliée par $\frac{1}{\sqrt{2}}$
   - Pendant la propagation la phase évolue avec un facteur $e^{i\overrightarrow{k}.\overrightarrow{r}}$ où $\overrightarrow{k} = k\overrightarrow{e_x}$ ou $k\overrightarrow{e_y}$ et $\overrightarrow{r} = x\overrightarrow{e_x}$ ou $y\overrightarrow{e_y}$ selon la direction de propagation
   En déduire l'intensité de la lumière arrivant dans chaque détecteur D_1 et D_2.
2. *Interprétation quantique.* La lumière est constituée de photons. On associe à la direction de propagation du photon suivant Ox un état quantique $|x\rangle$ et un état quantique $|y\rangle$ à la direction de propagation du photon suivant Oy ; l'action d'une lame semi réfléchissante sur l' état du photon est de le projeter dans un état de superposition

$$\begin{aligned} |x\rangle &\rightarrow \frac{1}{\sqrt{2}}\left[|x\rangle + i\,|y\rangle\right] \\ |y\rangle &\rightarrow \frac{1}{\sqrt{2}}\left[|y\rangle + i\,|x\rangle\right] \end{aligned}$$

   tandis que l'action d'un miroir est

$$\begin{aligned} |x\rangle &\rightarrow i\,|y\rangle \\ |y\rangle &\rightarrow i\,|x\rangle \end{aligned}$$

   En déduire l'intensité de la lumière arrivant dans chaque détecteur D_1 et D_2.

Exercice 5 *Protocole BB84*

1. Dans l'expérience de cryptographie Alice veut transmettre un bit 0 en polarisant un photon avec un polariseur orienté au hasard $\oplus$ ou $\otimes$; le photon est intercepté par un espion qui en mesure la polarisation.
   (a) Il utilise un analyseur $\oplus$. Quelle est la probabilité qu'il obtienne 0 ?
   (b) Il utilise un analyseur qui fait un angle θ avec Ox. Montrer que la probabilité d'obtenir $|0\rangle$ est maintenant $p(\theta) = \frac{1}{4}(2 + \cos(2\theta) + \sin(2\theta))$
   (c) En déduire qu'il peut améliorer son taux de réussite par un choix optimal de l'angle θ.
2. Supposons que Alice et Bob aient leur polariseur orienté dans la même direction mais que le photon, émis intialement par Alice dans l'état $|0\rangle$, soit intercepté par l'espion ; celui-ci mesure la polarisation avec un choix aléatoire d'orientation $\oplus$ ou $\otimes$;
   Quelle est la probabilité que Bob reçoive le photon dans l'état $|1\rangle$?
3. Dans l'expérience décrite dans la section (1.3.2), 700 bits sont prélevés pour être comparés entre Alice et Bob .
   (a) Quelle est la probabilité que si un espion mesure tous les qubits transmis, aucun des 700 bits ne soit modifié par cette interception.
   (b) La ligne a un taux d'erreur physique de 3%. Quel pourcentage de qubit un espion peut-il intercepter pour que le taux d'erreurs dû à l'interception ne soit pas supérieur au taux physique.

Exercice 6 *Protocole B92 (C. Bennett, 1992)*

Ce protocole repose sur un codage à deux états seulement à la différence du protocole BB84 qui repose sur un codage à quatre états. Alice adopte le codage suivant (voir BB84 pour les notations) pour le bit x à transmettre

$$\begin{aligned} |\uparrow\rangle &\rightarrow x = 0 \\ |\nearrow\rangle &= \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\longrightarrow\rangle) \rightarrow x = 1 \end{aligned}$$

Bob associe au *tirage aléatoire de la base* de mesure un bit y de la façon suivante :

$$\begin{aligned} y &= 0 \rightarrow \text{ base } \oplus \\ y &= 1 \rightarrow \text{ base } \otimes \end{aligned}$$

de plus il associe au *résultat* de la mesure un bit b de la façon suivante

$$\begin{aligned} b &= 0 \rightarrow \text{ si le résultat est } |\uparrow\rangle \text{ ou } |\nearrow\rangle \\ b &= 1 \rightarrow \text{ si le résultat est } |\longrightarrow\rangle \text{ ou } |\searrow\rangle \end{aligned}$$

1. Montrer que le résultat $b = 1$ ne peut être obtenu que si les bits x et y sont différents.
2. En déduire comment Alice et Bob peuvent constituer un clé secrète connue d'eux seuls.
3. Si n est le nombre de bits transmis quelle est (en moyenne) le nombre de bits de la clé ?

Exercice 7 *Racine carrée de NOT.*

1. Trouver la porte logique quantique à un qubit notée $\sqrt{NOT}$ telle que si on l'applique deux fois successivement le résultat est celui de la porte NOT ; (indication : rechercher la matrice unitaire R telle que $RR = X$)
2. existe-t-il une porte logique classique, à un bit notée $\sqrt{NOT}$ telle que si on l'applique deux fois successivement le résultat est celui de la porte NOT ?

Exercice 8 *Portes à un qubit*

On définit, pour tout nombre réel δ les opérateurs :

$$S(\delta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\delta} \end{pmatrix} \quad R(\delta) = \begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{-i\delta} \end{pmatrix}$$

1. Quelle est l'action de l'opérateur $S(\delta)$ sur les états de base $|0\rangle$ et $|1\rangle$?
2. Vérifier que n'importe quel vecteur $(u, v) \in \mathbb{C}^2$, tel que $|u|^2 + |v|^2 = 1$ peut être engendré (à une phase globale près) à partir de l'état $|0\rangle$ par la succession d'opérations

$$S\left(\varphi + \frac{\pi}{2}\right) HS(\theta) H |0\rangle$$

où H est l'opérateur de Hadamard et θ, φ sont des nombres réels bien choisis.

3. Quelle conclusion peut-on tirer ?
4. Soit $U \in \mathsf{SU}(2)$. Montrer qu'il existe des nombres $\delta_1, \delta_2, \delta_3 \in \mathbb{R}$ tels que

$$U = R(\delta_1)HR(\delta_2)HR(\delta_3).$$

5. Montrer que $\{iH\} \cup \{R(\delta) \mid \delta \in \mathbb{R}\}$ est une partie génératrice du groupe $\mathsf{SU}(2)$.

Exercice 9 *Opérateurs de Hadamard et de Pauli.*

On rappelle l'expression des matrices de Pauli, notées désormais X, Y, Z et de la matrice de Hadamard, H :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

1. Quelles sont les valeurs propres et vecteurs propres (normalisés) des matrices de Pauli ?
2. Calculer $X^2, Y^2, Z^2, XY, YZ, ZX$
3. Calculer HZH, HXH

Exercice 10 *Groupe* $\mathsf{SU}(2)$ *et algèbre de Lie* $\mathsf{su}(2)$.

On note $\mathsf{SU}(2)$ le groupe formé des matrices de dimension 2×2, à coefficients complexes, unitaires, de déterminant 1. On note $\mathsf{su}(2)$ l'ensemble des matrices de dimension 2×2, à coefficients complexes, anti-hermitiennes, de trace 0.

1. Vérifier que $\mathsf{SU}(2)$ est un groupe pour le produit de matrices.

2. Vérifier que $\mathsf{su}(2)$ est un sous-espace vectoriel (sur $\mathbb{R}$) de l'espace des matrices de dimension 2×2, à coefficients complexes. Montrer que les matrices iX, iY, iZ (où X, Y, Z sont les matrices de Pauli) forment une base de $su(2)$.

3. Pour toutes matrices carrées A, B on note

$$[A, B] := A \cdot B - B \cdot A$$

Cette opération s'appelle le "crochet de Lie". Montrer que $\mathsf{su}(2)$ est clos par crochet de Lie.

4. Montrer que si $M \in \mathsf{su}(2)$ alors $\exp(M) \in \mathsf{SU}(2)$.
5. Montrer que, si $\forall n \in \mathbb{N} \setminus \{0\}, \exp(\frac{1}{n}M) \in \mathsf{SU}(2)$, alors $M \in \mathsf{su}(2)$.

Exercice 11 *Quaternions.*

On définit trois nouvelles matrices $\overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k}$ par :

$$\overrightarrow{i} := iY, \quad \overrightarrow{j} := iX, \overrightarrow{k} := iZ$$

où X, Y, Z sont les matrices de Pauli. On appelle *quaternion* toute matrice de la forme

$$a\mathrm{I} + b\overrightarrow{i} + c\overrightarrow{j} + d\overrightarrow{k}$$

avec $a, b, c, d \in \mathbb{R}$. On note $\mathbb{H}$ l'ensemble des quaternions.

Partie 1 : structure de corps

1. Vérifier que $\mathbb{H}$ est un sous-espace vectoriel (sur $\mathbb{R}$) de dimension 4 de $\mathbb{M}_{2,2}(\mathbb{C})$.
2. Montrer que $(\mathbb{H}, +, \cdot, \cdot, \mathrm{I})$ est une algèbre associative, unitaire sur $\mathbb{R}$ (le deuxième symbole $\cdot$ dénote le produit externe d'un réel avec une matrice).
3. Vérifier la "table de multiplication" des vecteurs $\mathrm{I}, \overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k}$:

	I	$\overrightarrow{i}$	$\overrightarrow{j}$	k
I	I	$\overrightarrow{i}$	$\overrightarrow{j}$	k
$\overrightarrow{i}$	$\overrightarrow{i}$	$-\mathrm{I}$	k	$-\overrightarrow{j}$
$\overrightarrow{j}$	$\overrightarrow{j}$	$-k$	$-\mathrm{I}$	$\overrightarrow{i}$
k	k	$-\overrightarrow{j}$	$-\overrightarrow{i}$	$-\mathrm{I}$

4. Etant donné $q = a\mathrm{I} + b\overrightarrow{i} + c\overrightarrow{j} + d\overrightarrow{k}$ on note $\mathcal{R}(q) = a\mathrm{I}$, $\mathcal{I}(q) = b\overrightarrow{i} + c\overrightarrow{j} + d\overrightarrow{k}$. On dit qu'un quaternion q est *réel* (resp. *imaginaire pur*) si $q = \mathcal{R}(q)$ (resp. $q = \mathcal{I}(q)$). On identifie $\mathbb{R}$ à l'ensemble des quaternions réels. On note $\mathbb{H}_3$ l'ensemble des quaternions imaginaires purs.
Vérifier que $q \in \mathbb{R} \Leftrightarrow q \cdot q \in \mathbb{R}_+$ et $q \in \mathbb{H}_3 \Leftrightarrow q \cdot q \in \mathbb{R}_-$.

5. On définit le quaternion conjugué du quaternion q par : $\bar{q} := \mathcal{R}(q) - \mathcal{I}(q)$.
Montrer que $q \cdot \bar{q} \in \mathbb{R}_+$.

6. On note $\mathsf{N}(q) = \sqrt{q \cdot \bar{q}}$.
Vérifier que $\mathsf{N}(q) = 0 \Leftrightarrow q = 0_{\mathbb{H}}$.

7. Montrer que $\overline{q \cdot r} = \bar{r} \cdot \bar{q}$.

8. Montrer que $\mathsf{N}(q \cdot r) = \mathsf{N}(q) \cdot \mathsf{N}(r)$.

9. Montrer que, si $q \neq 0_{\mathbb{H}}$, $\bar{q} \cdot (1/\mathsf{N}^2(q))$ est un inverse de q pour le produit.

Partie 2 : représentation des rotations

1. Vérifier que, pour $q, r \in \mathbb{H}_3$, $q \cdot r = -(q \mid r) + q \wedge r$.

2. Soit $s \in \mathbb{H} - \{0\}$. On définit l'application $\rho_s : \mathbb{H} \to \mathbb{H}$ par

$$\rho_s(q) = s \cdot q \cdot s^{-1}.$$

- Montrer que $\mathbb{H}_3$ est globalement invariant par ρ_s.
- Montrer que la restriction ρ'_s de ρ_s à $\mathbb{H}_3$ est une rotation.

3. Vérifier que $s \mapsto \rho_s$ est un homomorphisme du groupe $(\mathbb{H} - \{0\}, \cdot)$ dans $SO(3)$, le groupe des rotations (vectorielles) de $\mathbb{R}^3$.

4. Quel est le noyau de l'homomorphisme de la question précédente ?

5. Montrer que toute symétrie orthogonale (sur $\mathbb{H}_3$) est de la forme $q \mapsto -(sqs^{-1})$ pour un quaternion $s \in \mathbb{H} - \{0\}$.

6. En déduire que toute rotation de $\mathbb{H}_3$ est de la forme ρ'_s pour au moins un quaternion $s \in \mathbb{H} - \{0\}$ tel que $\mathsf{N}(q) = 1$.

Exercice 12 $\mathsf{SU}(2)$ *et quaternions.*

Le but de l'exercice est de démontrer que $\mathsf{SU}(2)$ coincide avec l'ensemble des quaternions de norme 1.

1. Montrer que $\{q \in Q \mid \mathsf{N}(q) = 1\} \subseteq \mathsf{SU}(2)$.
2. On définit une action de $\mathsf{SU}(2)$ sur le sous-espace vectoriel $\mathbb{H}_3 := \langle \overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k} \rangle$ par : pour tout $u \in \mathbb{H}_3$

$$M \odot u = M \cdot u \cdot M^{-1}.$$

Vérifier qu'il s'agit bien d'une action (à gauche) de groupe i.e. $\forall u \in \mathbb{H}_3, \forall M, N \in \mathsf{SU}(2)$,

$$\mathrm{I} \odot u = u, \;\; (M \cdot N) \odot u = M \odot (N \odot u).$$

3. Montrer que , pour tout $M \in \mathsf{SU}(2)$, l'application

$$u \mapsto M \odot u$$

est une rotation de $\mathbb{H}_3$.

4. On appelle noyau de l'action $\odot$ l'ensemble

$$K_{\odot} := \{M \in \mathsf{SU}(2) \mid \forall u, M \odot u = u\}.$$

Que vaut $K_{\odot}$?

5. Soit $M \in \mathsf{SU}(2)$. On sait, d'après la question 3, que l'action de M sur $\mathbb{H}_3$ est une rotation. Soit q un quaternion de norme 1 qui induit la même rotation (voir l'exercice précédent) :

$$\forall u \in \mathbb{H}_3, q \odot u = M \odot u.$$

   Montrer que $M \in \{q, -q\}$.
6. Montrer que $\{q \in Q \mid \mathsf{N}(q) = 1\} = \mathsf{SU}(2)$.

Chapitre 2

Plus subtil : l'intrication quantique

2.1 Etats à deux qubits

Définition d'un état à deux qubits

C'est ici que se situe le caractère le plus subtil et paradoxal de la mécanique quantique, qui a engendré des débats épistémologiques célèbres [1] et qui est à la base du développement de l'information quantique

Nous allons définir les états du *système* de deux qubits A et B ; pour cela on part des états d'un qubit, $|0_A\rangle$ et $|1_A\rangle$ pour le qubit A et $|0_B\rangle$ et $|1_B\rangle$ pour le qubit B. Le système AB peut donc se trouver dans l'un des états $|0_A\rangle\,|0_B\rangle$, $|0_A\rangle\,|1_B\rangle$, $|1_A\rangle\,|0_B\rangle$, $|1_A\rangle\,|1_B\rangle$. Supposons maintenant que chaque qubit se trouve dans un état de superposition

$$\begin{aligned} \text{qubit } A \quad &: \quad |\psi_A\rangle = \alpha\,|0_A\rangle + \beta\,|1_A\rangle \\ \text{qubit } B \quad &: \quad |\psi_B\rangle = \gamma\,|0_B\rangle + \delta\,|1_B\rangle \\ \text{système } (A,\ B) \quad &: \quad |\psi_A\rangle\,|\psi_B\rangle = \alpha\gamma\,|0_A\rangle\,|0_B\rangle + \alpha\delta\,|0_A\rangle\,|1_B\rangle + \beta\gamma\,|1_A\rangle\,|0_B\rangle + \beta\delta\,|1_A\rangle\,|1_B\rangle \end{aligned} \tag{2.1}$$

Les quatre états à deux qubits $|0_A\rangle\,|0_B\rangle$, $|0_A\rangle\,|1_B\rangle$, ... constituent en fait une base dans l'espace des états à deux qubits qui est de dimension 4. On va simplifier les notations et désigner ces états par $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. *Tout état à deux qubits se décompose donc sur cette base* (voir le premier postulat)

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle \tag{2.2}$$

avec

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \tag{2.3}$$

C'est le cas pour l'état factorisé de l'équation (2.1). Bien évidemment il existe des états *qui ne peuvent pas se factoriser* en un produit d'états à un qubit. On les nomme *états intriqués* (ou états enchevétrés, "entangled states" en anglais). Ces états sont spécifiques de la description quantique. Ils engendrent entre les particules des corrélations fortes qui sont à la base des différents protocoles et algorithmes de l'information quantique. Il est important de comprendre que dans ces états intriqués l'état individuel d'un qubit n'est pas défini (il n'y a pas de *réalité* sous-jacente pour chaque qubit) ; c'est le *système* qui est dans un état défini, qui d'ailleurs évolue globalement au cours du temps selon une opération unitaire. Ce n'est que lors d'une mesure sur un des qubits que son état se révèle,

1. Dont la célèbre polémique soulevée en 1935 par A. Einstein, B. Podolsky et N. Rosen (EPR) et qui n'a trouvé son dénouement qu'avec les travaux théoriques de J.S. Bell en 1964 confirmés par les expériences d'Alain Aspect *et al* en 1982.

avec une (amplitude de) probabilité donnée par les coefficients de l'état intriqué. L'intrication fait qu'une fois que l'état d'un qubit est mesuré, l'état de l'autre qubit s'en déduit le plus souvent (corrélation).

Un exemple particulièrement utilisé d'état intriqué est le premier *état de Bell* défini par

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \tag{2.4}$$

Tant qu'aucune mesure n'est effectuée sur le système l'état de chaque qubit n'est pas défini. Supposons que nous mesurions le premier qubit et que nous trouvions l'état $|0\rangle$. Cela signifie que l'état $|\beta_{00}\rangle$ est projeté sur l'état $|00\rangle$ ce qui entraîne que le deuxième qubit est forcément lui aussi dans l'état $|0\rangle$.

Mesure d'un état à deux qubits

D'après le postulat de la mesure si on mesure l'état des deux qubits le système est projeté dans l'un des états de base $|00\rangle$, $|01\rangle$, $|10\rangle$ ou $|11\rangle$ avec une probabilité$|\alpha_{ij}|^2$ où les α_{ij} sont les coefficients des états de base dans la décomposition de l'équation (2.2).

On peut 'effectuer une *mesure partielle* c'est à dire uniquement sur l'un des deux qubits. La mesure va fixer l'état du qubit mesuré ; l'état du système sera une superposition des états de base compatible avec l'état initial et dans laquelle le qubit mesuré aura une valeur fixée. Par exemple si on mesure le premier qubit pour un système dans l'état (2.2) et qu'on trouve $|0\rangle$ le système est projeté dans l'état

$$\left|\widetilde{\psi}\right\rangle = \frac{\alpha_{00}}{|\alpha_{00}|^2 + |\alpha_{01}|^2}|00\rangle + \frac{\alpha_{01}}{|\alpha_{00}|^2 + |\alpha_{01}|^2}|01\rangle$$

Si maintenant l'état initial du système est l'état de Bell $|\beta_{00}\rangle$ (éq. 2.4) et que la mesure du premier bit donne $|0\rangle$ alors le système est projeté dans l'état $|00\rangle$

Théorème de non-clonage quantique

Revenons maintenant sur ce théorème (Wooters & Zurek, Nature 299, 802 (1982)) que nous avons vu au chapitre précédent et qui assurait le fonctionnement des protocoles de distribution sécurisée de clés secrètes. Ce théorème stipule

Il n'existe pas de "photocopieuse" quantique.

c'est-à-dire qu'il est impossible de dupliquer un état quantique.

Une photocopieuse est (schématiquement) une machine avec un bac pour l'original dans lequel on met le document à reproduire et un bac pour la copie, qui contient initialement une feuille blanche et dans lequel on récupère la copie. Imaginons une photocopieuse quantique qui aurait deux qubits (deux "bacs"), un pour l'"original" et un pour la "copie". On note $|\psi\rangle$ l'état à "photocopier" et $|b\rangle$ (avec b comme le *blanc* de la feuille vierge du photocopieur) l'état initial du qubit de copie.

Le processus de copie consiste à faire passer l'état de la machine de $|\psi\rangle|b\rangle \overset{\text{Xcopy}}{\rightarrow} |\psi\rangle|\psi\rangle$. Selon les postulats du paragraphe précédent cette évolution est décrite par un opérateur unitaire U caractéristique de la machine c'est-à-dire qui ne dépend pas de l'état à dupliquer. On a donc $|\psi\rangle|\psi\rangle = U|\psi\rangle|b\rangle$. Pour un autre état à dupliquer $|\phi\rangle \neq |\psi\rangle$; on doit avoir aussi $|\phi\rangle|\phi\rangle = U|\phi\rangle|b\rangle$ avec le même U.

Evaluons le produit scalaire de ces deux expressions

$$\begin{aligned} \langle\phi|\langle\phi|\psi\rangle|\psi\rangle &= \langle b|\langle\phi|U^\dagger U|\psi\rangle|b\rangle \\ (\langle\phi\psi\rangle)^2 &= \langle bb\rangle\langle\phi\psi\rangle = \langle\phi\psi\rangle \end{aligned}$$

La seule solution de cette dernière équation est $\langle\phi\psi\rangle = 0$ (ou $\langle\phi\psi\rangle = 1 \rightarrow |\phi\rangle = |\psi\rangle$ ce qui est exclu par hypothèse) c'est à dire que les deux états doivent être orthogonaux. Cette machine ne serait donc pas universelle puisqu'elle ne pourrait cloner que deux états, mais pas, par exemple,une superposition de ces deux états. D'où le théorème.

Remarques :

— Si on restreignait le protocole de distribution de clé de codage aux seuls deux états orthogonaux de polarisation $|\uparrow\rangle$ et $|\longrightarrow\rangle$ le théorème de non-clonage ne pourrait pas être invoqué.

— On peut fabrique une machine qui copie seulement les états de base $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ qui sont orthogonaux. On retrouve l'analogue classique de la porte COPIE. Cette machine ne pourra pas copier les états *quantiques* de superposition des états de base.

2.2 Manipulations d'états à deux qubits

Nous avons vu au paragraphe précédent que les opérations sur un (ou plusieurs) qubit(s) correspondent à l'action d'opérateurs unitaires c'est à dire à des évolutions *réversibles*. Ceci constitue une différence fondamentale avec le fonctionnement des ordinateurs classiques qui lui est *irréversible*. En effet un théorème de logique dit que toute porte logique peut être construite à partir de l'opération NAND, qui est irréversible, et de l'opération COPY de copie. En raison du caractère réversible des opérations quantiques d'une part et du théorème de non clonage d'autre part, ni l'une ni l'autre de ces portes classiques (universelles), n'est directement transposable à l'information quantique.

Il est cependant possible de transformer les algorithmes classiques irréversibles en algorithmes réversibles [2]. Le prix à payer est une augmentation du volume d'information traitée et l'introduction d'une nouvelle porte logique à trois bits, la *porte de Toffoli*, notée TOF, qui réalise $(x, y, z) \rightarrow (x, y, z \oplus xy)$. On utilisera aussi la porte SWAP qui réalise $(x, y) \rightarrow (y, x)$. On dit que $f : \mathbb{B}^n \rightarrow \mathbb{B}^n$ est calculable, "avec variables auxiliaires", sur l'ensemble de portes (réversibles) $\mathcal{G}$ ssi il existe un circuit C à $n + m$ entrées (et sorties) tel que : pour tout $\overrightarrow{x} \in \mathbb{B}^n$

$$C(\overrightarrow{x}, 0^m) = (f(\overrightarrow{x}), 0^m)$$

Autrement dit, le circuit C se sert des m dernières places pour calculer, mais ne prend aucune donnée, ni ne retourne aucun résultat, dans ces m places "auxiliaires". Étant donnée $f : \mathbb{B}^n \rightarrow \mathbb{B}$ on notera $f_\oplus : \mathbb{B}^{n+1} \rightarrow \mathbb{B}^{n+1}$ l' application définie par :

$$f_\oplus(\overrightarrow{x}, y) := (\overrightarrow{x}, y \oplus f(\overrightarrow{x})).$$

On peut montrer que tout circuit irréversible calculant une fonction f, peut être transformé en circuit réversible, avec variables auxiliaires, calculant la bijection $f_\oplus$ (qui plus est sans changer sa classe de complexité). On pourra, à travers cette équivalence, associer un algorithme quantique (réversible) à tout algorithme classique (irréversible).

Théorème 6 (Bennet-Landauer-Toffoli) *Soit $N \geq 2$. Toute application booléenne inversible $f : \mathbb{B}^N \rightarrow \mathbb{B}^N$ est calculable par un circuit (avec var. auxiliaires) sur l'ensemble de portes* {NOT, SWAP, TOF}.

2. voir le DM de 2011/12

Dans ce théorème, la porte NOT peut être remplacée apr la porte *controlled NOT* ou *cNOT*, (*NON contrôlé* en français) qui fonctionne de la façon suivante :

Etat d'entrée	Etat de sortie
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

La valeur du deuxième bit (bit *cible*) est inchangée si le premier bit (dit bit de *contrôle*) vaut zéro et il est inversé si le bit de contrôle vaut un. Le bit cible vaut à la sortie la somme binaire (modulo 2) des deux bits d'entrée tandis que le bit de contrôle reste inchangé : $(x, y) \to (x, x \oplus y)$.

$$cNOT : \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

La traduction quantique cNÔT de cette porte réversible est représentée par une matrice dans la base $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ ou par un circuit quantique : Une généralisation de cette notion de

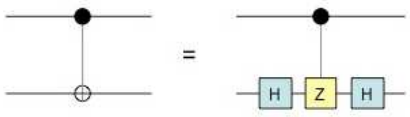


FIGURE 2.1 – circuit c-NOT

contrôle est la suivante : pour tout opérateur unitaire U sur $\mathcal{B}^{\otimes n}$, l'opérateur $\Lambda(U)$ sur $\mathcal{B}^{\otimes(n+1)}$ est défini par :

$$\begin{aligned} \Lambda(U)\,|x_1, \ldots, x_n\rangle = &\quad |x_1\rangle \otimes |x_2, \ldots, x_{n+1}\rangle \qquad \text{si } x_1 = 0 \\ = &\quad |x_1\rangle \otimes U\,|x_2, \ldots, x_{n+1}\rangle \qquad \text{si } x_1 = 1 \end{aligned}$$

On peut alors démontrer le

Théorème 7 (Kitaev-Shen-Vialyi) *Soit $n \geq 2, N := 2^n$. Toute matrice unitaire $U_N \in \mathsf{U}(N)$, vue comme une porte à n q-bits, est calculée par un circuit sur l'ensemble de portes :*

$$\{\text{NÔT}, \text{SWÂP}, \text{TÔF}\} \cup \{\Lambda(U) \mid U \in \mathsf{U}(2)\}$$

Autrement dit : les portes réversibles de base (traduites en transformations unitaires) ainsi que toutes les portes à 1 qbits, contrôlés par un autre qbit, suffisent pour calculer n'importe quelle transformation unitaire sur N qbits. D'un point de vue matriciel, une porte à p qbits est une matrice de la forme

$$\mathrm{I}_{2^k} \otimes U_p \otimes \mathrm{I}_{2^{n-k-p}}$$

où $U_p \in \mathsf{U}(2^p)$. Précisions :
- le *nombre* de portes utilisées dans la décomposition de U_N est au plus polynomial par rapport à N (donc, au plus exponentiel par rapport à n)
- il existe un algorithme (classique, déterministe, polynomial en N) permettant de calculer à partir de U_N la décomposition annoncée (dans le cas général, cet algorithme utilise comme un "oracle" les opérations arithmétiques sur $\mathbb{C}$; dans le cas particulier où les coefficients de U_N sont algébriques, on peut le traduire en algorithme au sens usuel).

Nous avons vu qu'il y a un continuum de portes à un qubit. L'ensemble universel ne doit comporter qu'un nombre *fini* de portes pour être opérationnel.Le théorème 7 répond presque au problème : il suffit de le compléter en démontrant qu'un opérateur unitaire à deux dimensions U peut être *approché avec une précision arbitraire* par le produit d'opérateurs unitaires pris dans un ensemble *fini*. On montre que cet ensemble fini peut être constitué seulement de la porte de Hadamard (noté H) et de la porte $\pi/8$ (notée T) :

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Autrement dit : le sous-groupe de $\mathsf{U}(2)$ engendré par $\{H, T\}$ est *dense* dans $\mathsf{U}(2)$.

2.3 Application : la téléportation quantique

Ce nom accrocheur décrit une application amusante et surprenante des états intriqués. En langage courant le problème peut se formuler ainsi :

— *Un agent secret remet à Anne une enveloppe qui contient un message très important destiné à un autre agent, Benoît situé à quelques kilomètres de là. L'agent demande à Anne de ne pas prendre connaissance du message et, n'ayant pas confiance dans les services postaux, de ne pas envoyer l'enveloppe à Benoît. Dans ces conditions comment Anne parviendra-t-elle à transmettre le message à Benoît ?*

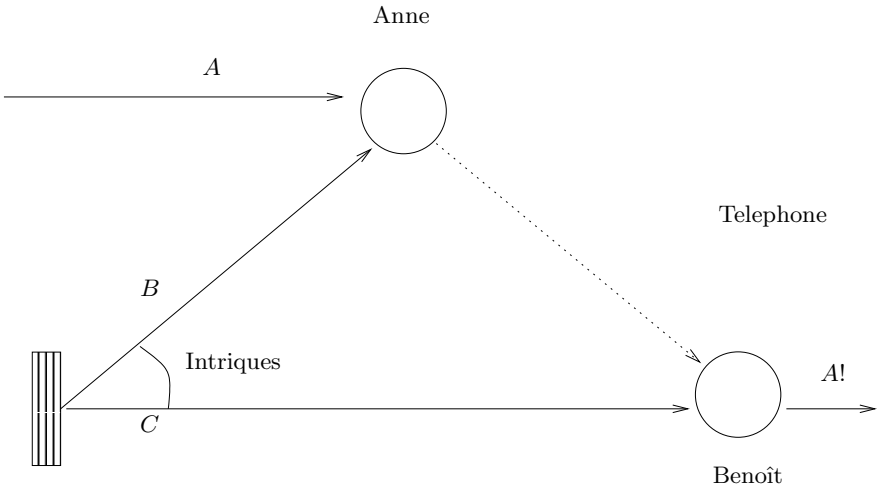


FIGURE 2.2 – Comment communiquer le qbit A ?

En langage quantique cela devient : comment transmettre d'un point A (Anne) à un point B (Benoît) le contenu inconnu d'un qubit, sans transporter le système physique porteur du qubit ?

Anne veut transmettre à Benoît le contenu d'un qubit dans un état $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ que Anne ne connait pas. Anne et Benoît se sont rencontrés à une époque antérieure, plus ou moins lointaine, au cours de laquelle ils se sont mutuellement offerts un des deux qubits d'un état intriqué de Bell (eq. 2.4). Nous avons donc un système à trois qubits dont l'état est décrit par

$$\begin{aligned} |\psi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}\left\{(\alpha\,|0\rangle + \beta\,|1\rangle)\,(|00\rangle + |11\rangle)\right\} \\ &= \frac{1}{\sqrt{2}}\left\{\alpha\,(|000\rangle + |011\rangle) + \beta\,(|100\rangle + |111\rangle)\right\} \end{aligned}$$

où l'ordre des qubits est :

1. le qubit inconnu (noté A) à transmettre, détenu par Anne,
2. le premier qubit de la paire intriquée (noté B), détenu par Anne,
3. le second qubit de la paire intriquée (noté C), détenu par Benoît.

Anne réalise les opérations suivantes :

1. Elle réalise un *cNOT* sur la paire *(A,B)* ; elle obtient

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left\{\alpha\,(|000\rangle + |011\rangle) + \beta\,(|110\rangle + |101\rangle)\right\}$$

2. Elle envoie le premier qubit sur une porte de Hadamard ; l'état du système devient

$$|\psi_2\rangle = \frac{1}{2}\left\{\alpha\,(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \beta\,(|010\rangle - |110\rangle + |001\rangle - |101\rangle)\right\}$$

qui peut être reécrit en utilisant $|000\rangle = |00\rangle\,|0\rangle$ ...

$$\begin{aligned} |\psi_2\rangle = \frac{1}{2} \quad & \{\ |00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) \\ & + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) \\ & + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) \\ & + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)\ \} \end{aligned}$$

Nous sommes au coeur de la *téléportation* : l'état du qbit C est complétement déterminé par celui de la paire (AB) ; c'est l'effet de corrélation quantique due à l'intrication de la paire (BC).

3. Anne lit maintenant la paire (AB) (mesure) et transmet le résultat à Benoît par sa ligne téléphonique [3]
4. Benoît reçoit le résultat d'Anne, $|b_1 b_2\rangle$; vérifier que si Benoît réalise sur son qubit C l'opération :$Z^{b_1}\,X^{b_2}$ où X et Z sont les portes à un qubit définies au § 1.4.3 l'état résultant du qubit C est l'état $|\psi\rangle$.

3. C'est cette étape qui assure que la téléportation du qubit $|\psi\rangle$ ne viole pas le principe de ralativité qui dit qu'aucune information ne peut être transmise plus vite que la lumière.

Quantum teleportation across the Danube

A real-world experiment marks a step towards worldwide quantum communication.

Efficient long-distance quantum teleportation[1] is crucial for quantum communication and quantum networking schemes[2]. Here we describe the high-fidelity teleportation of photons over a distance of 600 metres across the River Danube in Vienna, with the optimal efficiency that can be achieved using linear optics. Our result is a step towards the implementation of a quantum repeater[3], which will enable pure entanglement to be shared between distant parties in a public environment and eventually on a worldwide scale.

Quantum teleportation is based on a quantum channel, here established through a pair of polarization-entangled photons shared between Alice and Bob (Fig. 1). We have implemented this by using an 800-metre-long optical fibre installed in a public sewer system located in a tunnel underneath the River Danube, where it is exposed to temperature fluctuations and other environmental factors.

For Alice to be able to transfer the unknown polarization state of an input photon $|\chi\rangle_b$, she has to perform a joint Bell-state measurement on the input photon *b* and her member, *c*, of the shared entangled photon pair (*c* and *d*). Our scheme allows her to identify two of the four Bell states, the optimum achievable with only linear optics[4,5].

As a result of this Bell-state measurement, Bob's 'receiver' photon *d* will be projected into a well defined state that already contains full information on the original input photon *b*, except for a rotation that depends on the specific Bell state that Alice observed. Our teleportation scheme therefore also includes active feed-forward of Alice's measurement results, which is achieved by means of a classical microwave channel together with a fast electro-optical modulator (EOM). It enables Bob to perform the unitary transformation on photon *d* to obtain an exact replica of Alice's input photon *b*.

Specifically, if Alice observes the $|\psi^-\rangle_{bc}$ Bell state, which is the same as the initial entangled state of photons *c* and *d*, then Bob already possesses the original input state. But if Alice observes the $|\psi^+\rangle_{bc}$ state, he introduces a π-phase shift between the horizontal and vertical polarization components of photon *d* by applying a voltage pulse of 3.7 kV on the EOM. For successful operation, Bob has to set the EOM correctly before photon *d* arrives. Because of the reduced velocity of light within the fibre-based quantum channel (two-thirds of that *in vacuo*), the classical signal arrives about 1.5 microseconds before the photon.

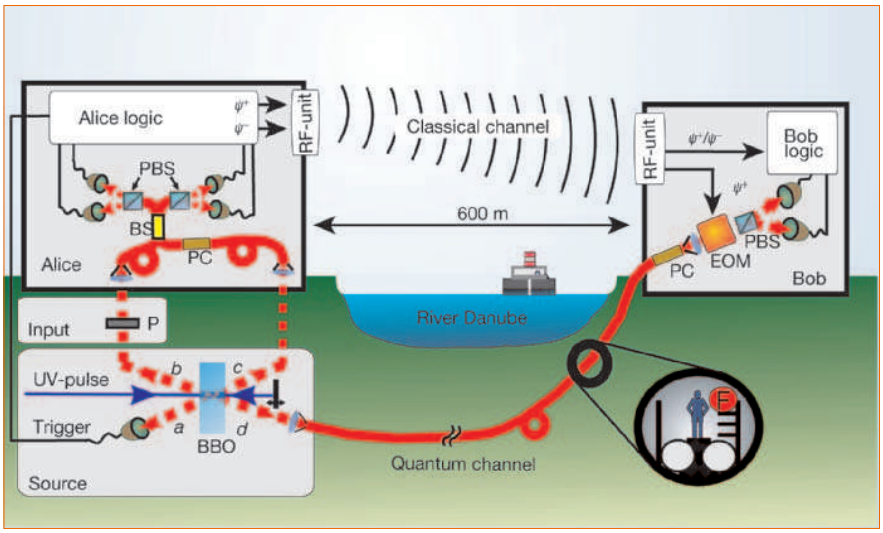


Figure 1 Long-distance quantum teleportation across the River Danube. The quantum channel (fibre F) rests in a sewage-pipe tunnel below the river in Vienna, while the classical microwave channel passes above it. A pulsed laser (wavelength, 394 nm; rate, 76 MHz) is used to pump a β-barium borate (BBO) crystal that generates the entangled photon pair *c* and *d* and photons *a* and *b* (wavelength, 788 nm) by spontaneous parametric down-conversion. The state of photon *b* after passage through polarizer P is the teleportation input; *a* serves as the trigger. Photons *b* and *c* are guided into a single-mode optical-fibre beam splitter (BS) connected to polarizing beam splitters (PBS) for Bell-state measurement. Polarization rotation in the fibres is corrected by polarization controllers (PC) before each run of measurements. The logic electronics identify the Bell state as either $|\psi^-\rangle_{bc}$ or $|\psi^+\rangle_{bc}$ and convey the result through the microwave channel (RF unit) to Bob's electro-optic modulator (EOM) to transform photon *d* into the input state of photon *b*.

We demonstrated the teleportation of three distinct polarization states: linear at 45°, left-handed circular or horizontal. The teleportation fidelity achieved was 0.84, 0.86 or 0.90 for the 45°, for each of these input states, respectively. These fidelities comfortably surpass the classical limit of 0.66 (ref. 6) and prove that our teleportation system is operating correctly. Without operation of the EOM, however, Bob observes a completely mixed polarization for the 45° and circular polarization input states, causing the observed fidelity for these states to drop to 0.54 and 0.59, respectively, in the absence of active unitary transformation. The deviation from the random fidelity of 0.5 is due to statistical fluctuations in the observed counts.

Each measurement run lasted for 28 h and the rate of successful teleportation events was 0.04 per second. Polarization stability proved to be better than 10° on the fibre between Alice's and Bob's labs, corresponding to an ideal teleportation fidelity of 0.97 over a full measurement run. Hence, despite the exposure of our system to the environment, high-fidelity teleportation was still achievable without permanent readjustments.

We have demonstrated quantum teleportation over a long distance and with high fidelity under real-world conditions outside a laboratory. Our system combines for the first time, to our knowledge, an improved Bell-state analyser with active unitary transformation, enabling a doubling of the efficiency of teleportation compared with earlier experiments based on independent photons[7,8]. Our experiment demonstrates feed-forward of measurement results, which will be essential for linear-optics quantum computing[9–11], and constitutes a step towards the full-scale implementation of a quantum repeater.

Rupert Ursin*, Thomas Jennewein*†, Markus Aspelmeyer*, Rainer Kaltenbaek*, Michael Lindenthal*, Philip Walther*, Anton Zeilinger*†

**Institute for Experimental Physics, University of Vienna, 1090 Vienna, Austria*
e-mail: rupert.ursin@univie.ac.at
†Austrian Academy of Science, 1090 Vienna, Austria

1. Bennett, C. H. *et al. Phys. Rev. Lett.* **70,** 1895–1899 (1993).
2. Bose, S., Vedral, V. & Knight, P. L. *Phys. Rev. A* **57,** 822–829 (1998).
3. Briegel, H. J., Dür, W., Cirac, J. I. & Zoller, P. *Phys Rev. Lett.* **81,** 5932–5935 (1998).
4. Lütkenhaus, N., Calsamiglia, J. & Suominen, K.-A. *Phys. Rev. A* **59,** 3295–3300 (1999).
5. Kim, Y.-H. *et al. Phys. Rev. Lett.* **86,** 1370–1373 (2001).
6. Popescu, S. *Phys. Rev. Lett.* **72,** 797–799 (1994).
7. Bouwmeester, D. *et al. Nature* **390,** 575–579 (1997).
8. Marcikic, I., de Riedmatten, H., Tittel, W., Zbinden, H. & Gisin, N. *Nature* **421,** 509–513 (2003).
9. Riebe, M. *et al. Nature* **429,** 734–737 (2004).
10. Barrett, M. D. *et al. Nature* **429,** 737–739 (2004).
11. Gottesmann, D. & Chuang, I. L. *Nature* **402,** 390–393 (1999).

Competing financial interests: declared none.

2.4 EXERCICES

Exercice 13 *Théorème de non clonage*

1. Montrer que la porte C-Not permet de réaliser l'opération de copie (clonage) $(x, b) \to (x, x)$ si $x = |0\rangle$ ou $|1\rangle$ et b le bit "page blanche", initialement dans un état à définir.
2. Montrer que le même processus ne fonctionne plus si le qubit x est une superposition quelconque $\alpha |0\rangle + \beta |1\rangle$.
   Ceci est une manifestation du fait qu'on peut effectuer une copie d'un bit classique (l'analogue des qubits de la base de calcul) mais pas d'un qubit en général (théorème de non clonage quantique).

Exercice 14 *Portes réversibles.*

On considère l'ensemble de portes $\mathcal{G} = \{\mathsf{NOT}, \mathsf{SWAP}, \mathsf{TOF}\}$. Construire des circuits (avec variables auxiliaires) sur $\mathcal{G}$, pour les fonctions booléennes (bijectives) :
$\mathsf{cNOT}, \mathsf{NOT}_{\oplus}, \mathsf{OR}_{\oplus}, \mathsf{NAND}_{\oplus}$.

Exercice 15 *Porte de Toffoli*

1- Donner explicitement une matrice unitaire R telle que $R^2 = \hat{\mathsf{NOT}}$,
On choisit maintenant une telle matrice unitaire R.
On définit, pour $1 \leq k \leq n$ et tout opérateur unitaire U sur $\mathcal{B}$, l'opérateur $\Lambda^k(U)$ sur $\mathcal{B}^{\otimes(k+1)}$ par :

$$\begin{aligned} \Lambda^k(U) |x_1, \ldots, x_k, x_{k+1}\rangle = &\quad |x_1, \ldots, x_k\rangle \otimes |x_{k+1}\rangle \quad \text{si } x_1 x_2 \cdots x_k = 0 \\ = &\quad |x_1, \ldots, x_k\rangle \otimes U |x_{k+1}\rangle \quad \text{si } x_1 x_2 \cdots x_k = 1 \end{aligned}$$

2- Vérifier que l'opérateur de Toffoli est égal à l'opérateur $\Lambda^2(\hat{\mathsf{NOT}})$.
3- On définit le circuit T sur 3 qbits par la figure 2.3.
Montrer que ce circuit T calcule l'opérateur de Toffoli.

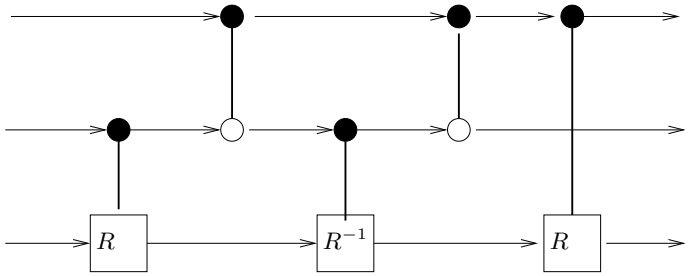


FIGURE 2.3 – Le circuit T

Indication : on pourra distinguer les quatre cas de figure $(x_1, x_2) = (0, 0)$, $(x_1, x_2) = (0, 1)$, $(x_1, x_2) = (1, 0)$, $(x_1, x_2) = (1, 1)$ et vérifier que, dans chaque cas, $T |x_1, x_2, x_3\rangle = \hat{\mathsf{TOF}} |x_1, x_2, x_3\rangle$.
4- Donner un ensemble de portes unitaires $\mathcal{G}_2$, sur 2 qubits, qui engendre *toutes* les applications unitaires (de dimension finie quelconque $d \geq 2$) i.e. tout $U \in \mathsf{U}(d)$ est calculée par un circuit sur $\mathcal{G}_2$.

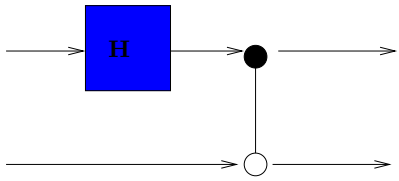


FIGURE 2.4 – Une porte créant des états de Bell.

Exercice 16 *Etats de Bell*

1. Déterminer les états obtenus (états de Bell) en injectant dans la porte logique ci-dessus les quatre états de la base de calcul à deux qubits :$|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ (on notera $\beta_{00}, \beta_{01}, \beta_{10}, \beta_{11}$ les états de Bell correspondants).
2. Montrer que ces états sont orthogonaux
3. Prenons l'état β_{01} ; on effectue une mesure sur le premier qubit. Quelle est la probabilité d'obtenir 0 ? On obtient effectivement 0 et on mesure maintenant le deuxième bit. Quelle est la probabilité d'obtenir 0 ?

   Répondre aux mêmes questions en partant de l'état $|\varphi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
4. Dans les expériences de téléportation ou de super dense coding (exercice ci-dessous) deux personnes distantes possèdent chacune un des deux qubits d'une paire dans un état de Bell. La mesure de son qubit par l'une des deux personnes fixe automatiquement la valeur du qubit détenu par l'autre personne. Comment expliquer que cette corrélation qui semble instantanée ne viole pas le principe de la relativité restreinte qui dit qu'aucune information ne peut se propager plus vite que la vitesse de la lumière ?

Exercice 17 *Super dense coding*

Anne dispose de deux bits (classiques) d'information à transmettre à Benoît ; comment peut-elle faire en sorte que Benoît ait connaissance de la valeur de ces deux bits en ne lui envoyant qu'*un seul qubit* ? (Anne et Benoît disposent chacun d'un qubit d'un état de Bell $|\beta_{00}\rangle$)

1. Selon la valeur de la paire de bits classiques Anne agit sur son qubit de la façon suivante

Bits classiques	Action sur le qubit
00	I
01	X
10	Z
11	ZX

   Dans chaque cas quel est l'état des deux qubits résultant de l'action sur le qubit de Anne ?
2. Anne transmet à Benoît le qubit transformé. Benoît fait agir sur l'état des deux qubits maintenant en sa possession l'inverse de la porte de l'exercice précédent : d'abord C-Not puis Hadamard sur le premier qubit. Quel état obtient-il (pour chaque éventualité) ?
3. En déduire qu'en mesurant l'état obtenu dans la base de calcul le résultat est, avec une probabilité de 100% la paire de bit classiques détenue par Anne.

Chapitre 3

Nettement plus compliqué : le calcul quantique

3.1 Ordinateur classique *vs* ordinateur quantique

On peut schématiser un ordinateur classique (machine de Turing) à l'aide de trois composants
- des registres qui contiennent les données à traiter
- une unité de calcul qui transforme les données suivant un algorithme défini en actionnant des portes logiques
- une unité d'entrées/sorties qui initialise les registres au début du traitement et lit les résultats à la fin.

Quel peut être l'analogue quantique ?

3.1.1 Les registres

Un registre classique est un ensemble de n bits permettant de stocker les $N = 2^n$ entiers compris entre 0 à $2^n - 1$. On définit un *registre quantique* en associant à chaque bit un *qu*bit. Un registre quantique est donc un *système quantique* de n qubits dont les états seront éléments de l'espace des états de dimension $N = 2^n$. On définit dans cet espace la *base de calcul* :

$$|j_1 j_2 \cdots j_n\rangle := |j_1\rangle\,|j_2\rangle \cdots |j_n\rangle \quad ; \quad j_1, j_2, \cdots j_n \in \{0, 1\}$$

On utilisera selon le contexte deux notations complétements équivalentes pour désigner ces états de base :
- Soit par la liste des états de chaque qubit, éléments de $Z_2 = \{0, 1\}$; par exemple $|j_1 j_2 \cdots j_n\rangle$
- Soit par le nombre entier $j \in [0, 2^n - 1]$ dont l'ensemble $(j_1, j_2, \cdots, j_n)$ constitue la décomposition binaire
$$j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_k 2^{n-k} + ...j_n 2^0$$

Si on note Z_N l'ensemble des entiers modulo N on a donc une équivalence dans la notation

$$j \in Z_N \leftrightarrow (j_1, j_2, \cdots, j_n) \in Z_2^n \quad ; \quad N = 2^n$$

On utilisera parfois la notation

$$\begin{aligned} & j = j_1 2^{n-1} + j_2 2^{n-2} + ...j_n 2^0 \qquad k = k_1 2^{n-1} + k_2 2^{n-2} + ...k_n 2^0 \\ \Rightarrow j \cdot k &= j_1 k_1 + j_2 k_2 + ... + j_n k_n \bmod 2 \\ &= j_1 k_1 \oplus j_2 k_2 \oplus ... \oplus j_n k_n \end{aligned}$$

où $\oplus$ désigne l'addition binaire sans retenue ou encore l'opération logique XOR : $0 \oplus 0 = 1 \oplus 1 = 0 \quad 0 \oplus 1 = 1 \oplus 0 = 1$.

Ainsi les N états de la base de calcul seront désormais notés $|x\rangle$ avec $x \in Z_N$ (compris dans $[0, 2^n - 1]$).

$$\begin{array}{rcll} \overbrace{|000...00\rangle}^{n \text{ qubits}} & \leftrightarrow & |0\rangle & \\ |000...01\rangle & \leftrightarrow & |1\rangle & \\ |x_1\, x_2 ... x_n\rangle & \leftrightarrow & |x\rangle & \text{où} \quad x = x_1 2^{n-1} + x_2 2^{n-2} + ... + x_k 2^{n-k} + ... x_n 2^0 \end{array}$$

La spécificité des registres quantiques réside dans le fait qu'ils peuvent se trouver non seulement dans un des états de la base de calcul (équivalent du registre classique) mais aussi dans un état quelconque de superposition

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle$$

Nous verrons plus loin que les algorithmes quantiques peuvent être représentés par l'évolution d'un ou plusieurs registres sous l'effet de l'application d'opérateurs unitaires. Le système quantique représentant l'état de l'ordinateur peut comprendre plusieurs registres (le plus souvent deux) par exemple : un registre à n qubits dont les états sont notés $|x\rangle$ avec $x \in Z_{2^n}$ et un registre à m qubits dont les états sont notés $|y\rangle$ avec $y \in Z_{2^m}$; dans ce cas l'état quantique total est noté $|x\rangle\,|y\rangle$ ou $|xy\rangle$ indifféremment et est élément d'un espace des états à 2^{n+m} dimensions.

3.1.2 Les portes logiques

On a vu au chapitre précédent qu'un état quantique ne peut évoluer que selon une transformation unitaire ce qui induit une logique réversible. Nous avons vu également que cela n'est pas pénalisant puisque tout algorithme irréversible peut être transformé en algorithme réversible à l'aide d'un ensemble universel fini de portes, sans changer la classe de complexité de l'algorithme. L'ensemble universel que nous utiliserons est constitué

— des deux portes à un qubit,

	$\|0\rangle$	$\|1\rangle$
Hadamard	$\frac{1}{\sqrt{2}}[\|0\rangle + \|1\rangle]$	$\frac{1}{\sqrt{2}}[\|0\rangle - \|1\rangle]$
$S(\frac{\pi}{4})$	$\|0\rangle$	$e^{i\frac{\pi}{4}}\|1\rangle$

On peut écrire l'action de ces portes de façon plus condensée :

$$\begin{array}{rcl} H\,|j\rangle & = & \dfrac{1}{\sqrt{2}}\left[|0\rangle + (-1)^j\,|1\rangle\right] \\ & = & \dfrac{1}{\sqrt{2}}\sum_{k=0}^{1}(-1)^{jk}\;|k\rangle \quad \text{où} \quad j \in Z_2 \\ S(\dfrac{\pi}{4})\,|j\rangle & = & e^{i\frac{\pi}{4}j}\,|j\rangle \quad \text{où} \quad j \in Z_2 \end{array}$$

— de la porte à deux qubits *C-NOT* : $|j_1\ j_2\rangle \to |j_1\ j_1 \oplus j_2\rangle$

Exercice : On appelle *transformation de Hadamard* d'un état à n qubits l'action simultanée d'une porte de Hadamard sur chacun des qubits. Soit $|x\rangle$ où $x \in Z_N$, $(N = 2^n)$, montrer que

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{N-1} (-1)^{x \cdot z} |z\rangle$$

Quel état résulte de $H^{\otimes n} |0\rangle$?

3.1.3 Evaluation d'une fonction - Parallélisme quantique

Les calculs nécessitent le plus souvent l'évaluation de fonctions $f : Z_2^n \to Z_2^m$ qui ne sont en général pas bi-univoques (inversibles, bijectives). On ne peut donc pas les représenter par un opérateur *unitaire*. La solution pour associer un opérateur unitaire à l'évaluation d'une fonction est d'introduire des qubits auxiliaires : on définit

— un *registre de données* $|x\rangle$ à n qubits, avec $x \in Z_{2^n}$ qui contiendra la valeur de la variable
— un *registre de résultats* $|y\rangle$ à m qubits, avec $y \in Z_{2^m}$ qui contiendra le résultat
— un *opérateur unitaire* agissant dans un espace des états à 2^{m+n} dimensions

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$

où l'opération $\oplus$ désigne l'addition binaire (sans retenue). On montre que cet opérateur est unitaire (on vérifie facilement que $U_f^2 = I$ puisque $x \oplus x = 0\ \forall x$).

Exemple : L'opérateur AND

	0	1
0	0	0
1	0	1

L'opérateur AND n'est pas inversible $(x, y) \to f(x, y) = x \wedge y = xy$ dont la table de vérité est ci-contre. On peut le mettre en oeuvre de façon réversible par la procédure ci-dessus. cela donne $(x, y, z) \to (x, y, z \oplus xy)$ qui n'est autre que la porte de Toffoli.

Exercice : Donner la représentation matricielle de l'opérateur unitaire U_f correspondant à cette porte dans l'espace des états à $2^{2+1} = 8$ dimensions

Le parallélisme est un trait caractéristique de beaucoup d'algorithmes quantiques dans lesquels une fonction $f(x)$ peut être évaluée simultanément pour plusieurs valeurs de x, comme conséquence de la propriété de superpositions d'états d'un qubit. Nous verrons au paragraphe suivant l'exemple standard, un peu académique mais historiquement fondateur [1], de l'algorithme de Deutsch.

Prenons l'exemple d'un registre de donnée et d'un registre de résultats à un seul qubit. Prenons comme valeur initiale de chaque registre la valeur $|0\rangle$ et effectuons la succession d'opérations ci-contre

où $|\psi_i\rangle$ désigne l'état du système des deux registres le long du circuit.

$$\begin{aligned} |\psi_0\rangle &= |00\rangle \\ |\psi_1\rangle &= \frac{1}{\sqrt{2}} [|00\rangle + |10\rangle] \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}} [|0, f(0)\rangle + |1, f(1)\rangle] \end{aligned}$$

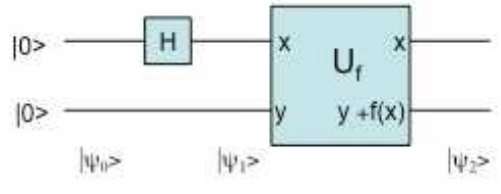


FIGURE 3.1 – Circuit pour 1 qubit

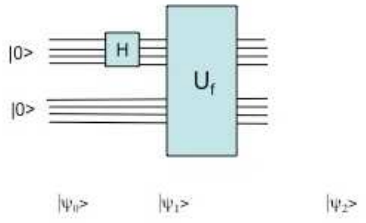


FIGURE 3.2 – Circuit pour n qubits

L'état de sortie, $|\psi_2\rangle$, est remarquable car il contient à la fois $f(0)$ et $f(1)$ obtenus par *une seule application* de la porte U_f. Cette procédure peut être généralisée à un nombre quelconque de bits d'entrée.

Soit un registre de données à n qubits. La transformation de Hadamard (H sur chaque qubit) donne pour le registre de données $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$. Cet état en entrée de la porte U_f engendre en sortie (si l'autre entrée est initialisée avec l'état $|0\rangle^{\otimes m}$) l'état intriqué

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\,|f(x)\rangle \tag{3.1}$$

qui fait apparaître de nouveau *toutes* les valeurs de f en une seule opération. C'est cela qu'on désigne par *parallélisme quantique*.

Cependant cette propriété n'est pas directement exploitable puisqu'au moment de "lire" le qubit on ne récupére aléatoirement qu'un des états $|x, f(x)\rangle$. Nous allons voir qu'en étant astucieux on peut quand même obtenir plus d'information qu'une seule valeur de f.

3.1.4 Les entrées/sorties

L'équivalent quantique de l'unité d'entrée/sortie est là aussi très spécifique.

L'*entrée* correspond à mettre le système quantique que constitue le(s) registre(s) dans un état initial ; on dit qu'on *prépare* le système. Le plus souvent les différents registres sont initialement dans l'état $|0\rangle$ et la préparation consiste à faire agir différents opérateurs (par exemple la transformation de hadamard).

1. David Deutsch de l'Université d'Oxford (UK) proposa cet algorithme en 1985 à l'appui de sa thèse sur la version quantique de la machine de Turing

La *sortie* correspond à la lecture d'un registre ce qui pour nous correspond à une *mesure* de l'état quantique final du registre. D'après le postulat de la mesure cet opération *modifie* en général [2], et de façon irréversible, l'état du registre puisqu'il le projette sur un des états de la base de calcul. Les algorithmes quantiques tirent partie de cette transformation le plus souvent en utilisant des mesures partielles de l'état final, c'est à dire en ne mesurant qu'un des registres, voire même seulement que quelques qubits d'un registre.

3.2 Algorithme de Deutsch

Le problème se formule de la façon suivante : soit f une fonction de $Z_2 \to Z_2$; une telle fonction est soit constante (fonctions f_0 et f_3 de l'exercice 18), soit *équilibrée*, c'est à dire qu'elle vaut 0 dans la moitié des cas et 1 dans l'autre moitié (fonctions f_1 et f_2 de l'exercice 18). Pour déterminer si une fonction prise au hasard fait partie de l'une ou l'autre de ces catégories, il est clair qu'il faut calculer la fonction pour (au moins) deux valeurs différentes de la variable. Deutsh a montré (1985) qu'en exploitant le parallélisme quantique on peut répondre au problème en une seule évaluation.

Réalisons le circuit suivant où $|\psi_i\rangle$ désigne l'état du système des deux registres au fil du circuit :

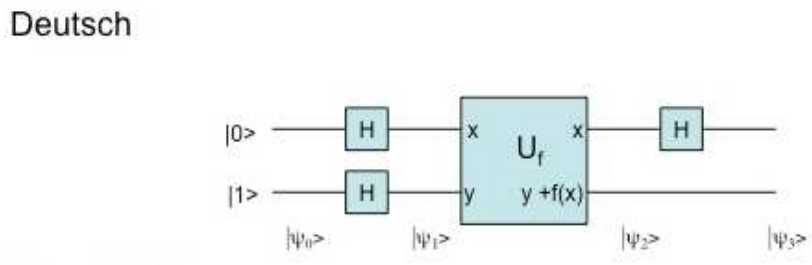


FIGURE 3.3 – algorithme de Deutsch

— $|\psi_0\rangle = |01\rangle$
— $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}\left[\sum_{x=0,1}|x\rangle\right](|0\rangle - |1\rangle) = \frac{1}{2}\sum_{x=0,1}[|x,0\rangle - |x,1\rangle]$
— $|\psi_2\rangle = \frac{1}{2}\sum_{x=0,1}[|x,0\oplus f(x)\rangle - |x,1\oplus f(x)\rangle]$; pour déterminer cette expression remarquons que $y \oplus f(x) = y$ si $f(x) = 0$, et $\overline{y}$ (complément) sinon ; donc

$$\begin{aligned} |x,0\oplus f(x)\rangle - |x,1\oplus f(x)\rangle &= |x,0\rangle - |x,1\rangle \text{ si } f(x)=0 \\ &= |x,1\rangle - |x,0\rangle \text{ si } f(x)=1 \end{aligned}$$

En résumé $(|x,0\oplus f(x)\rangle - |x,1\oplus f(x)\rangle = (-1)^{f(x)}[|x,0\rangle - |x,1\rangle]$.
Donc $|\psi_2\rangle = \frac{1}{2}\sum_{x=0,1}(-1)^{f(x)}[|x,0\rangle - |x,1\rangle] = \left\{\frac{1}{2}\sum_{x=0,1}(-1)^{f(x)}|x\rangle\right\}\{|0\rangle - |1\rangle\}$
— On envoie le premier qubit sur une porte de Hadamard ; l'état résultant de *ce qubit* sera

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{2\sqrt{2}}(-1)^{f(0)}(|0\rangle + |1\rangle) + \frac{1}{2\sqrt{2}}(-1)^{f(1)}(|0\rangle - |1\rangle) \\ &= \frac{1}{2\sqrt{2}}\left[(-1)^{f(0)} + (-1)^{f(1)}\right]|0\rangle + \frac{1}{2\sqrt{2}}\left[(-1)^{f(0)} - (-1)^{f(1)}\right]|1\rangle \end{aligned}$$

Si la fonction f est constante, alors $f(0) = f(1)$ et le qubit vaut $\pm|0\rangle$; si la fonction est *équilibrée* (balanced) c'est-à-dire $f(0) \neq f(1)$ alors le qubit vaut $\pm|1\rangle$.

2. sauf si l'état du registre est déjà un des états de la base de calcul

Par conséquent une mesure du qubit donnera à coup sûr :
— $|0\rangle$ si la fonction f est constante
— $|1\rangle$ si la fonction f est équilibrée.

On a donc pu déterminer en une seule action de la porte U_f cette propriété globale de la fonction, qui nécessite en principe plusieurs évaluations de f (exactement deux dans ce cas simple). Le gain du parallélisme quantique n'est pas spectaculaire dans cet exemple très académique. Il l'est un peu plus si on généralise le problème à un registre de données à n qubits ($n \geq 2$). On peut alors montrer (exercice 19) qu'il suffit de nouveau d'une seule action de la porte unitaire U_f pour déterminer si la fonction f est équilibrée ou constante alors qu'il faut en moyenne $2^{n-1}+1$ évaluations de f pour obtenir la même information classiquement.

3.3 Algorithme de Grover

Cet algorithme permet de trouver de façon efficace un (ou plusieurs) élément(s) particuliers dans une base de donnée non structurée.

La base de données comprend N éléments non triés, non liés, numérotés de 0 à $N-1$. L'objectif est de trouver dans cette liste l'élément (de numéro x_0) ayant une caractéristique particulière [3]. Un argument simple de probabilité montre qu'il faut en moyenne $N/2$ tirages (exhaustifs) dans la liste pour trouver le bon élément. Nous allons voir qu'avec un algorithme quantique qui porte son nom Lov Grover a montré qu'il suffisait d'environ $\sqrt{N}$ tirages.

On prendra $N = 2^n$ de sorte que la représentation binaire du numéro x de chaque élément fasse intervenir n bits. Tout d'abord définissons une fonction de reconnaissance $f : \mathbb{B}^n \to \mathbb{B}$ telle que $f(x) = 0$ si $x \neq x_0$ et $f(x) = 1$ si $x = x_0$. Cette fonction va être mise en oeuvre au moyen d'un opérateur unitaire appelé *oracle* qui agit sur un registre de donnée à n qubits contenant $|x\rangle$ et un registre de résultat à un qubit, q :

$$|x\rangle\,|q\rangle \xrightarrow{O} |x\rangle\,|q \oplus f(x)\rangle$$

Si le qubit q est initialisé avec $H\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ on obtient (voir paragraphe précédent)

$$|x\rangle\,\frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{O} (-1)^{f(x)}\,|x\rangle\,\frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Notons que le qubit q de l'oracle demeure inchangé ; on s'intéressera surtout à l'évolution du registre de donnée. Celui-ci sera initialisé avec l'état de superposition *uniforme* $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x\in\mathbb{B}^n}|x\rangle$ obtenu en faisant agir une porte H sur chaque qubit du registre de donnée initialement dans l'état $|0\rangle$ (transformation de Hadamard). Si on fait agir l'oracle sur l'état $|\psi\rangle$ le résultat est $|\psi\rangle \xrightarrow{O} \frac{1}{\sqrt{N}}\sum_{x\in\mathbb{B}^n}(-1)^{f(x)}\,|x\rangle$ c'est à dire que l'élément $|x_0\rangle$ est "taggé" dans la superposition par un signe "moins".

Il est important d'insister sur l'étape qui vient d'être décrite parce qu'elle différencie fondamentalement un algorithme quantique des algorithmes classiques. L'application de l'oracle sur l'état d'entrée est l'analogue dans le cas de l'algorithme classique de vérifier si l'élément qui vient d'être tiré au hasard (l'état d'entrée) a le bon numéro ou non. Si non, on tire un nouvel élément (on reprépare un nouvel état d'entrée). Il faut répéter en moyenne $N/2$ fois cette étape pour obtenir l'élément recherché.

3. l'algorithme se généralise facilement au cas où la liste comprend $M(>1)$ éléments ayant la caractéristique recherchée.

L'avantage de l'algorithme quantique est que l'état d'entrée n'est pas un élément unique de la liste, mais la *superposition de tous les éléments* (les états de la base de calcul). L'application de l'oracle se fait donc simultanément sur *tous* les éléments. L'état résultant contient l'information recherchée c'est-à-dire que le numéro de l'élément recherchéa été "signé". Il ne reste plus qu'à manipuler cet état astucieusement pour extraire cette information. Cette dernière étape n'est pas tout à fait triviale comme on va le voir mais on montrera qu'elle ne nécessite que $\sqrt{N}$ opérations à comparer aux $N/2$ de l'algorithme classique. Cette étape consiste à appliquer répétitivement la *porte de Grover* que l'on va maintenant définir.

Définissons au préalable l'opérateur S_ψ :

— soit S_0 l'opération qui change de signe tous les états sauf l'état $|0\rangle$:

$$\begin{aligned} S_0 : |0\rangle &\rightarrow |0\rangle \\ |x\rangle &\rightarrow -|x\rangle \quad \text{pour } |x\rangle \neq |0\rangle \end{aligned}$$

Cet opérateur (unitaire) peut s'écrire[4] $S_0 = 2|0\rangle\langle 0| - I$ (voir exercice)

— On applique à droite et à gauche de cet opérateur la transformation de Hadamard c'est à dire qu'on fait agir l'opérateur H sur chaque qubit d'entrée et de sortie.

$$S_\psi = H^{\otimes n} S_0 H^{\otimes n}$$

Comme $H^{\otimes n}|0\rangle = |\psi\rangle$ et que $H^2 = I$ on en déduit $S_\psi = 2|\psi\rangle\langle\psi| - I$

La porte de Grover G consiste à appliquer successivement l'oracle puis l'opérateur S_ψ :

$$G = S_\psi O$$

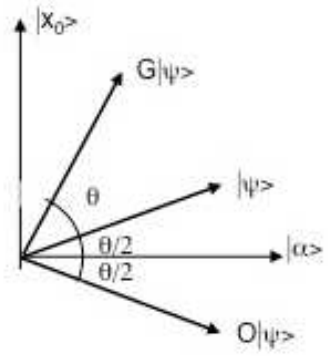


FIGURE 3.4 – Itérations de Grover

Pour avoir une intuition de l'action de cet opérateur nous utilisons une représentation géométrique simple. Soient les deux vecteurs orthogonaux $|x_0\rangle$ et

$$|\alpha\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \in \mathbb{B}^n, x \neq x_0} |x\rangle$$

4. On rappelle que les états de la base de calcul sont orthonormés : $\langle x|\ y\rangle = \delta_{xy}$

Dans la base orthonormée définie par ces deux vecteurs, le vecteur $|\psi\rangle$ est représenté par

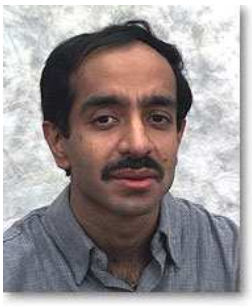
$$\begin{aligned} |\psi\rangle &= \sqrt{\frac{N-1}{N}}\,|\alpha\rangle + \frac{1}{\sqrt{N}}\,|x_0\rangle \\ &= \cos\frac{\theta}{2}\,|\alpha\rangle + \sin\frac{\theta}{2}\,|x_0\rangle \end{aligned}$$

où l'angle θ est défini par $\sin\frac{\theta}{2} = \frac{1}{\sqrt{N}}$ et qui est donc très petit (contrairement à ce que la figure ci-dessus laisse penser) puisqu'en général $N \gg 1$ et $\theta \simeq \frac{2}{\sqrt{N}}$. L'application de l'oracle sur l'état $|\psi\rangle$ change de signe la "composante" $|x_0\rangle$ ce qui dans ce diagramme réalise une symétrie par rapport à l'axe $|\alpha\rangle$. L'action de l'opérateur S_ψ réalise une symétrie par rapport au vecteur $|\psi\rangle$ (exercice 20). Le bilan net de l'action de la porte $G = S_\psi O$ sur le vecteur $|\psi\rangle$ est donc une rotation d'un angle θ dans ce diagramme. Le nouvel état s'est "rapproché" de l'axe $|x_0\rangle$; en répétant cette procédure l'état du système évolue en se rapprochant de l'état $|x_0\rangle$ qui est l'objectif à atteindre. Combien faut-il d'itérations pour y parvenir ? On a

$$\begin{aligned} G\,|\psi\rangle &= \cos\frac{3\theta}{2}\,|\alpha\rangle + \sin\frac{3\theta}{2}\,|x_0\rangle \\ G^k\,|\psi\rangle &= \cos\left[(2k+1)\frac{\theta}{2}\right]\,|\alpha\rangle + \sin\left[(2k+1)\frac{\theta}{2}\right]\,|x_0\rangle \end{aligned}$$

et nous voulons trouver k tel que $\cos(2k+1)\frac{\theta}{2} = 0$ soit $(2k+1)\frac{\theta}{2} = \frac{\pi}{2}$ donc $k \simeq \frac{\pi}{2\theta} \simeq \frac{\pi}{4}\sqrt{N} = O(\sqrt{N})$.Remarquons qu'à l'issue du processus l'état du système n'est pas *exactement* $|x_0\rangle$; si on fait une mesure dans la base de calcul la probabilité d'obtenir un état autre que $|x_0\rangle$ est de l'ordre de $1/N$ ce qui représente le taux d'erreur (voir exercice).

Pour estimer le "coût" total de l'algorithme il faut prendre en compte l' évaluation de l'opérateur S_ψ à chaque itération qui nécéssite essentiellement $2n$ portes de Hadamard ainsi que le coût de l'opération S_0 , qui est en $O(n)$. Ce coût total est donc en fait d'ordre $O(\sqrt{N}\ln N)$.



Lov Grover était chercheur aux Bell Labs quand il découvrit l'algorithme auquel il donna son nom.

3.4 EXERCICES

Exercice 18 *Fonctions de* $\{0,1\}$ *dans* $\{0,1\}$

x	0	1
$f_0(x)$	0	0
$f_1(x)$	0	1
$f_2(x)$	1	0
$f_3(x)$	1	1

Il existe 4 fonctions de $\{0,1\}$dans $\{0,1\}$ listées ci-contre : f_0 et f_3 sont les fonctions constantes et f_1 et f_2 sont respectivement la fonction identité et la fonction NOT ; ces deux dernières sont des fonctions équilibrées.

1. Pour chacune de ces fonctions construire la matrice unitaire U_f qui implémente $(x,y) \stackrel{U_f}{\rightarrow} (x, y \oplus f(x))$
2. Trouver l'état résultant de l'application de la transformation U_{f_2} (NOT) à l'état $(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|00\rangle + \beta|10\rangle$ puis à l' état $(\alpha|0\rangle + \beta|1\rangle)|1\rangle = \alpha|01\rangle + \beta|11\rangle$; on pourra utiliser soit la représentation matricielle soit la définition ci-dessus.

Exercice 19 *Algorithme de Jozsa-Deutsch*

Il s'agit de l'extension de l'algorithme de Deutsch au cas de fonctions de $\{0,1\}^n \rightarrow \{0,1\}$ qui sont soit constantes soit équilibrées. On pose $N = 2^n$.

1. Par les méthodes classiques :
   (a) Combien faut-il d'évaluations de la fonction pour déterminer si elle est constante ou équilibrée.
   (b) Supposons que l'on tire aléatoirement (et exhaustivement) les valeurs de x en lesquelles on évalue la fonction. Avec quelle probabilité peut-on conclure que la fonction est constante ou équilibrée après $k \leq N/2$ évaluations *aléatoires* de f.
2. On complète le registre de donnée $|x\rangle$ (où $x \in \{0,1\}^n$), par un registre de résultat à un qubit $|y\rangle$ (où $y \in \{0,1\}$). La fonction f est mise en oeuvre par la porte logique

$$U_f : |x\rangle|y\rangle \stackrel{U_f}{\rightarrow} |x\rangle|y \oplus f(x)\rangle .$$

   On initialise les registres à $|\psi_0\rangle = |00...0\rangle|1\rangle \equiv |0\rangle|1\rangle$.
   (a) Chacun des qubits de l'état initial passe dans une porte de Hadamard.Établir que l'état résultant est de la forme

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \left[\sum_{x \in \mathbb{B}^n} |x\rangle \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

   (b) L'état $|\psi_1\rangle$ est envoyé dans la porte U_f ; montrer qu'il en sort l'état

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \left[\sum_{x \in \mathbb{B}^n} (-1)^{f(x)} |x\rangle \right] \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

(c) On fait de nouveau subir à l'état $|\psi_2\rangle$ une transformation de Hadamard (porte de Hadamard sur chaque qubit sauf sur le bit de résultat). Montrer qu'on obtient

$$|\psi_3\rangle = \left[\sum_{z\in\mathbb{B}^n} A(z)\,|z\rangle\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

où l'amplitude $A(z)$ est donnée par $A(z) = \frac{1}{2^n}\sum_{x\in\mathbb{B}^n}(-1)^{x\cdot z+f(x)}$. Dans cette expression $x\cdot z = x_1z_1 + x_2z_2 + \cdots x_nz_n \bmod 2$.

3. Evaluer l'amplitude $A(z)$ dans les deux cas d'une fonction constante et d'une fonction équilibrée (dans ce cas on calculera $A(0)$). En déduire la méthode de discrimination entre les deux cas.

Exercice 20 *Algorithme de Grover*

1. Montrer que l'opérateur $S_\psi = 2\,|\psi\rangle\,\langle\psi| - I$ réalise dans le plan $(|\alpha\rangle\,,\,|x_0\rangle)$ une symétrie par rapport à la direction de l'état $|\psi\rangle$; *Indication : introduire un vecteur* $|\Phi\rangle$ *du plan* $(|\alpha\rangle\,,\,|x_0\rangle)$ *qui soit orthogonal à* $|\psi\rangle$.
2. *Probabilité d'erreur dans l'algorithme de Grover*
   (a) Quel est le nombre optimal d'itérations.
   (b) Quand on réalise la mesure à ce moment là quelle est la probabilité de ne pas trouver $|x_0\rangle$?
3. On va mettre en oeuvre l'algorithme de Grover dans le cas d'une liste de 4 éléments : on a donc $N = 4$ et $n = 2$; le registre comportera donc deux qubits.
   (a) Montrer que dans le cas où $x_0 = 3$ le circuit associé à la porte de Toffoli fait fonction d'oracle $|x\rangle\,|q\rangle \xrightarrow{O} |x\rangle\,|q\oplus f(x)\rangle$ c'est-à-dire que $f(3) = 1$ et $f(x) = 0$ sinon.
   (b) Quel serait le circuit dans le cas $x_0 = 1$?
   (c) Montrer que le circuit ci-dessous permet de trouver x_0 en exactement une itération (on prendra $x_0 = 3$).

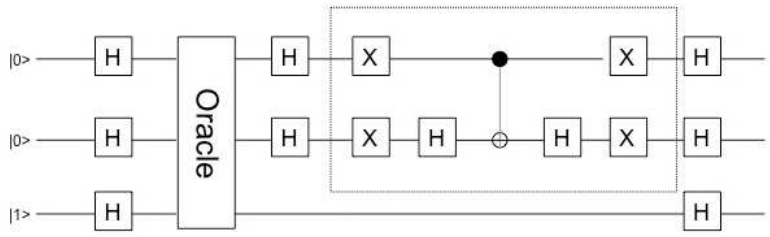


FIGURE 3.5 – Circuit Grover

Exercice 21 *Algorithme de Grover : la porte* S_0

Le but de l'exercice est de construire un circuit, sur un nombre de portes fini, qui réalise la transformation unitaire S_0 utilisée dans l'algorithme de Grover.
On rappelle que, pour tout opérateur unitaire U sur $\mathcal{B}$, l'opérateur $\Lambda^1(U)$ sur $\mathcal{B}^{\otimes 2}$ est défini par :

$$\begin{aligned}\Lambda^1(U)\,|x_1,x_2\rangle &= \quad |x_1\rangle \otimes |x_2\rangle \qquad \text{si } x_1 = 0\\ &= \quad |x_1\rangle \otimes U\,|x_2\rangle \qquad \text{si } x_1 = 1\end{aligned}$$

1- Construire un circuit sur les portes $\{\hat{\mathsf{SWAP}}, \Lambda^1(-\mathrm{Id})\}$ qui calcule la transformation $T_n : \mathcal{B}^{\otimes n+1} \to \mathcal{B}^{\otimes n+1}$ définie par :

$$\begin{aligned}T_n\,|x_1,\ldots,x_n,y\rangle &= \quad |x_1,\ldots,x_n,y\rangle \qquad \text{si } y = 0\\ &= \quad -\,|x_1,\ldots,x_n,y\rangle \qquad \text{si } y = 1\end{aligned}$$

(T_n est une transformation $-\mathrm{Id}_{2^n}$ contrôlée par le $(n+1)$-ième qbit).
2- Construire un circuit, avec variables auxiliaires, sur le jeu de portes $\{\hat{\mathsf{OR}}_{\oplus}, \hat{\mathsf{SWAP}}\}$ qui calcule la transformation $\hat{\mathsf{OR}}_{n,\oplus}$ définie par :

$$|x_1,\ldots,x_n,y\rangle \mapsto \left|x_1,\ldots,x_n,y\oplus\bigvee_{i=1}^{n} x_i\right\rangle$$

3- Vérifier que, pour tout $\varepsilon \in \{+1,-1\}$,

$$\hat{\mathsf{OR}}_{n,\oplus}\;\varepsilon\left|x_1,x_2,\ldots,x_n,y\oplus\bigvee_{i=1}^{n} x_i\right\rangle = \varepsilon\,|x_1,x_2,\ldots,x_n,y\rangle$$

4- Construire un circuit S_0 sur le jeu de portes $\{\hat{\mathsf{OR}}_{\oplus}, \hat{\mathsf{SWAP}}, \Lambda^1(-\mathrm{Id})\}$ qui calcule la symétrie s_0 :

$$\begin{aligned}|x_1,x_2,\ldots,x_n\rangle &\mapsto \quad |x_1,x_2,\ldots,x_n\rangle \qquad \text{si } x_1,x_2,\ldots,x_n = 0^n\\ &\mapsto \quad -\,|x_1,x_2,\ldots,x_n\rangle \qquad \text{si } x_1,x_2,\ldots,x_n \neq 0^n.\end{aligned}$$

Exercice 22 *Algorithme de Grover : la mesure finale.*

Soient $\mathcal{M},\mathcal{M}'$ deux observables définies sur un même système physique, dont l'espace des états est $\mathcal{H}$, un espace de Hilbert de dimension finie. Soient $M, M' : \mathcal{H} \to \mathcal{H}$ les deux opérateurs hermitiens qui représentent ces observables. Pour tout nombre réel λ on note $\mathrm{pr}_\lambda : \mathcal{H} \to \mathcal{H}$ la projection orthogonale sur le sous-espace propre de M associée à la valeur propre λ (cette projection est nulle si λ n'est pas valeur propre). On note $\mathrm{pr}'_{\lambda'}$ la projection sur le sous-espace propre de M' associée à la valeur propre λ'. On note

$$(\mathcal{M}' = \lambda', \mathcal{M} = \lambda)$$

l'événement suivant :
une mesure de l'observable $\mathcal{M}$ donne la valeur λ, puis une mesure de l'observable $\mathcal{M}'$ sur le système résultant donne la valeur λ'.
1- Montrer que, si le système est dans l'état $|u\rangle \in \mathcal{H}$,

$$\Pr(\mathcal{M}' = \lambda', \mathcal{M} = \lambda) = \|\mathrm{pr}'_{\lambda'} \circ \mathrm{pr}_\lambda\,|u\rangle\,\|^2.$$

2- Dans le cas de l'algorithme de Grover, $\mathcal{H} = \mathcal{B}^{\otimes n}$ (on oublie la $(n+1)$ième composante $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$).
On note $\mathcal{M}_i$ l'observable "$i$ème composante de l'état" (c'est un nombre 0 ou 1, bien défini dans

chacun des 2^n états de base).
2.1 Pour un vecteur $|\varphi\rangle$ quelconque de $\mathcal{H}$, et des bits $b_1, \ldots, b_n \in \{0,1\}$ exprimer la probabilité

$$\Pr(\mathcal{M}_n = b_n, \ldots, \mathcal{M}_1 = b_1)$$

à partir des projecteurs pr_b^i pour $b \in \{0,1\}$ et $1 \leq i \leq n$: pr_b^i est la projection orthogonale sur le sous-espace engendré par

$$\{|\vec{x}\rangle \mid x_i = b\}.$$

2.2 Soit $|u\rangle$ l'etat du registre de n qbits à la fin de l'exécution de l'algorithme de Grover et $\vec{x}_0 = (b_1, b_2, \ldots, b_n)$ le vecteur booléen recherché. Montrer que

$$\Pr(\mathcal{M}_n = b_n, \ldots, \mathcal{M}_1 = b_1) \geq 1 - \frac{4}{2^n}.$$

Chapitre 4

L'algorithme de factorisation de Shor

Peter Shor, né en 1959, est professeur au M.I.T. Il était chercheur aux Bell Labs quand il a découvert en 1994 l'algorithme qui porte son nom.

Cet algorithme ainsi que plusieurs autres reposent sur la mise en oeuvre efficace de la transformation de Fourier sur un circuit quantique. En fait l'algorithme classique de transformée de Fourier rapide (FFT) né cessite $O(n2^n)$ opérations pour transformer un nombre de n bits. Nous allons voir que la TF quantique ne nécessite que $O(n^2)$ opérations : le gain est ici *exponentiel*.

4.1 Transformée de Fourier quantique

La transformée de Fourier discrète est une opération (classique) qui associe à un vecteur complexe X de N éléments : $(x_0, x_1, ..., x_{N-1})$ un autre vecteur complexe Y de N éléments : $(y_0, y_1, ..., y_{N-1})$

$$Y = \mathcal{F}(X) \Leftrightarrow y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{\frac{2i\pi}{N} kj} x_j \tag{4.1}$$

La *transformée de Fourier quantique* transforme les états de la base de calcul $|0\rangle, |1\rangle, ... |N-1\rangle$

$$|j\rangle \xrightarrow{\mathcal{F}} U_{\mathcal{F}} |j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2i\pi}{N} kj} |k\rangle \tag{4.2}$$

De façon équivalente l'action sur un état arbitraire peut être écrite :

$$|x\rangle = \sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{\mathcal{F}} |\widetilde{x}\rangle = U_{\mathcal{F}} |x\rangle = \sum_{k=0}^{N-1} y_k |k\rangle \tag{4.3}$$

où les amplitudes y_k sont les transformées de Fourier discrètes des amplitudes x_j (équation 4.1).

Cette opération est unitaire - on le montre (exercice 23) à partir de l'identité $\frac{1}{N}\sum_{j=0}^{N-1} e^{\frac{2i\pi}{N}jk} = \delta_{k0}$ - et peut donc définir une porte quantique.

L'opération de TF classique (équation 4.1) nécessite N multiplications pour chaque composante (les noyaux $e^{\frac{2i\pi}{N}jk}$ peuvent être calculés une fois pour toute et tabulés ; on ne compte pas leur calcul dans la complexité de l'algorithme). Il faut donc en tout N^2 opérations qui peuvent être ramenées à $N \ln N$ grâce à l'algorithme de FFT. Nous allons montrer que l'évaluation de l'opérateur unitaire $U_{\mathcal{F}}$ ne nécessite que $(\ln N)^2$ opérations.

Comme dans le paragraphe précédent on prendra $N = 2^n$ de sorte que les états $|0\rangle, |1\rangle, ... |N-1\rangle$ correspondent aux états à n qubits de la base de calcul

$$\begin{aligned} |0\rangle &\rightarrow \overbrace{|000...0\rangle}^{n \text{ qubits}} \\ |1\rangle &\rightarrow |000...01\rangle \\ |j\rangle &\rightarrow |j_1\, j_2 ... j_n\rangle \end{aligned}$$

où

$$j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_k 2^{n-k} + ... j_n 2^0. \tag{4.4}$$

Dans la suite on utilisera aussi la représentation *fractionnaire* binaire : $0.j_1 j_2 ... j_n = j_1/2 + j_2/2^2 + ... + j_n/2^n$.

Nous allons établir (exercice 23) que la transformée de Fourier quantique peut se factoriser de la façon suivante :

$$|j_1\, j_2 ... j_n\rangle \xrightarrow{\mathcal{F}} \frac{1}{2^{n/2}} \left(|0\rangle + e^{2i\pi\, 0.j_n} |1\rangle\right) . \left(|0\rangle + e^{2i\pi\, 0.j_{n-1}j_n} |1\rangle\right) ... \left(|0\rangle + e^{2i\pi\, 0.j_1 j_2 ... j_n} |1\rangle\right) \tag{4.5}$$

Cette expression de la transformée de Fourier d'un état de base nous permet de comprendre pourquoi un algorithme *quantique* sera ici plus efficace qu'un algorithme classique : la TF se traduit par une rotation de chaque qubit qui ne nécessite donc l'action que de seulement $n = \ln N$ opérateurs à un qubit. L'état résultant (un état de superposition pour chaque qubit) n'a pas d'équivalent classique.

Cette décomposition peut être représentée par une succession d'applications de portes quantiques [1] que nous allons définir.

Définissons d'abord la porte à un qubit, R_k, $(k = 1, 2, ...n)$ qui, dans la base de calcul, est représentée par la matrice

$$R_k := \begin{pmatrix} 1 & 0 \\ 0 & e^{2i\pi/2^k} \end{pmatrix}$$

Remarquons que $R_0 = I$, $R_1 = Z$, $R_2 = S$, $R_3 = T$ (voir § 2.1.5). On associe à cet opérateur la porte "contrôlée" à deux qubits, $c - R_k$ dont l'action est la suivante (en prenant pour bit de contrôle le second bit x_2).

$$\begin{aligned} & & |x_1 x_2\rangle &\xrightarrow{c-R_k} |x_1' x_2\rangle \\ \text{si } |x_2\rangle &= & |0\rangle \rightarrow |x_1'\rangle &= |x_1\rangle \\ \text{si } |x_2\rangle &= & |1\rangle \rightarrow |x_1'\rangle &= R_k |x_1\rangle = e^{2i\pi x_1/2^k} |x_1\rangle \end{aligned}$$

1. Coppersmith D. (1994), Deutsch D. (1994)

Le circuit quantique QFT ("Quantum Fourier Transform") qui réalise la transformation de l'équation (4.5) est schématisée sur la figure ci-dessous et explicité dans les exercices.

Circuit réalisant la transformation de Fourier quantique :

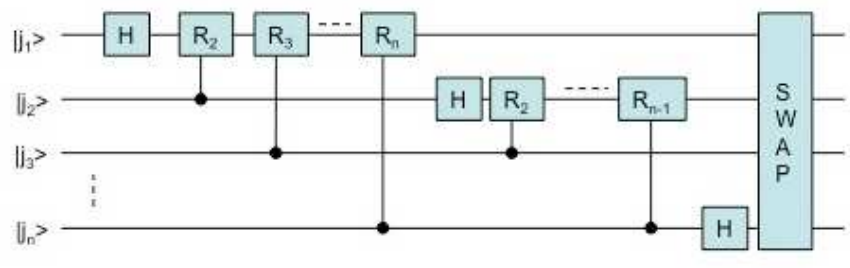


FIGURE 4.1 – Circuit QFT.

La porte SWAP, d'ordre n , "retourne" la suite de q-bits i.e. envoie chaque vecteur de base $|i_1 i_2 \dots i_n\rangle$ sur le vecteur $|i_n \dots i_2 i_1\rangle$.

Le nombre d'opérations (d'applications de portes) dans ce circuit est le suivant :

— sur la ligne j_1 : 1 Hadamard + n-1 R_k soient n opérations

— $n-1$ opérations sur la ligne j_2

— ...

Soient en tout $n + (n-1) + ... + 1 = \frac{n(n+1)}{2} = O(n^2)$ opérations.

4.2 Recherche de la période d'une fonction

L'algorithme de Shor repose sur la possibilité de trouver "rapidement" la période d'une fonction. Dans ce paragraphe nous allons voir comment l'algorithme de transformée de Fourier quantique permet de résoudre ce problème.

Soit f une fonction définie sur Z_N (les entiers modulo N, i.e. $x = 0, 1, 2, ..., N-1$) avec N quelconque (pas forcément une puissance de 2). Cette fonction est périodique de période $r < N$, c'est-à-dire qu'elle satisfait : $\forall x \in [0, N-r-1]$

$$f(x+r) = f(x);$$

nous supposerons de plus que *dans une même période* f ne prend jamais deux fois la même valeur [2]. Classiquement pour trouver la période inconnue on évalue la fonction pour des valeurs successives jusqu'à trouver une répétition. Cela requiert typiquement $O(r) \approx O(N)$ évaluations de f. L'algorithme quantique que nous allons présenter permet de réduire le nombre de calculs de f à $O((\log N)^3)$ ce qui représente une accélération exponentielle.

Dans la suite nous prendrons $x \in [0, 2^n - 1]$ avec $2^n > N$ [3] afin de mettre facilement en oeuvre l'algorithme de transformation de Fourier quantique. Les entiers x seront donc représentés par un registre à n qubits.

2. C'est le cas de la fonction a^x mod N où $1 < a < N$ et a premier avec N

3. En fait pour pouvoir traiter le cas le plus général il faut que n soit tel que $2^n > N^2$.

Commençons par préparer un état "parallélisé" au moyen de la porte U_f associée à la fonction f (voir paragraphe 3.2.1, equation (3.1))

$$|\psi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\,|f(x)\rangle \tag{4.6}$$

Nous effectuons une mesure sur le registre de résultats, et nous obtenons comme résultat y_0. Du fait de l'intrication de l'état (eq. 4.6), le registre de données se trouve projeté dans un état qui est la superposition de tous les états $|x\rangle$ tels que $f(x) = y_0$. Si x_0 est la plus petite de ces valeurs de x ($0 \leq x_0 \leq r-1$) alors les numéros des états qui contribuent sont $x_0, x_0+r, x_0+2r...x_0+(K-1)r$ où $K = \lceil \frac{2^n}{r} \rceil$. La figure ci-dessous représente les paramètres N, r et n dans différentes situations :
(a) cas où $K = \frac{N}{r}$ (entier).
(b) cas où $K = \lceil \frac{N}{r} \rceil, r \not| N$ et $x_0 \leq N-1-(K-1)r$
(c) cas où $K = \lceil \frac{N}{r} \rceil, r \not| N$ et $x_0 > N-1-(K-1)r$
Le *registre de données* sera dont dans l'état :

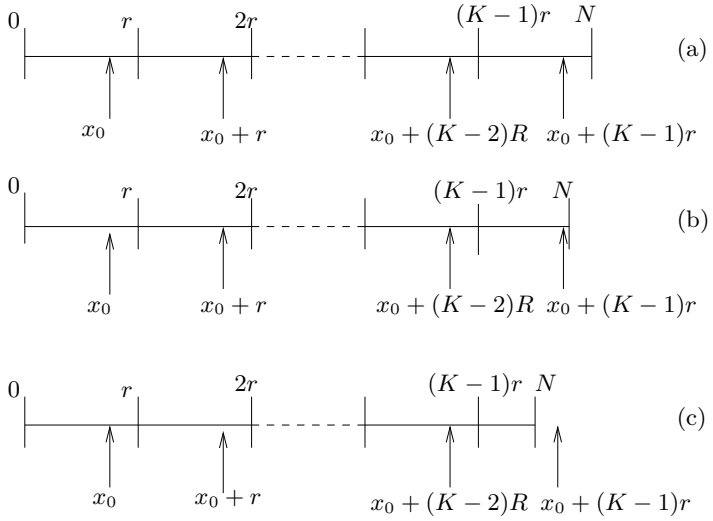


FIGURE 4.2 – K et N : 3 cas de figure

$$|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + kr\rangle \tag{4.7}$$

Nous allons maintenant faire l'hypothèse que r divise exactement 2^n c'est à dire $K = \frac{2^n}{r}$ (c'est-à-dire encore que $r = 2^m$). Si ce n'est pas le cas la procédure nécessite quelques traitements supplémentaires qui ne changent que marginalement sa complexité (voir exercice 26).

Comme x_0 n'est pas connu, l'état ci-dessus ne nous apprend rien sur r pour l'instant. Nous allons maintenant utiliser la transformée de Fourier.

Si on représente $|\psi\rangle$ et $\mathcal{F}\,|\psi\rangle$ dans la base de calcul alors (voir équations (4.1) et (4.3))

$$|\psi\rangle = \sum_{x=0}^{2^n-1} \varphi(x)\,|x\rangle \quad \rightarrow \quad \mathcal{F}\,|\psi\rangle = \sum_{y=0}^{2^n-1} \widetilde{\varphi}(y)\,|y\rangle$$

$$\widetilde{\varphi}(y) \quad = \quad \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \varphi(x)\, e^{\frac{2i\pi}{2^n}xy}$$

D'après l'équation (4.7) on a :

$$\begin{aligned}\varphi(x) &= \frac{1}{\sqrt{K}} \text{ si } x = x_0 + kr \\ &= 0 \text{ sinon}\end{aligned}$$

Par conséquent

$$\widetilde{\varphi}(y) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{K-1} \frac{1}{\sqrt{K}} e^{\frac{2i\pi}{2^n} y(x_0+kr)} = \frac{1}{\sqrt{2^n K}} e^{\frac{2i\pi}{2^n} y x_0} \sum_{k=0}^{K-1} e^{\frac{2i\pi}{K} yk}$$

où dans la dernière somme on a remplacé 2^n par Kr. La somme sur k dans cette dernière expression vaut 0 sauf si $y = 0 \pmod K$ auquel cas elle vaut K. Finalement

$$\begin{aligned}\widetilde{\varphi}(y) &= \frac{1}{\sqrt{r}} e^{\frac{2i\pi}{2^n} y x_0} \text{ si } y \text{ est un multiple de } K = \frac{2^n}{r} \\ &= 0 \text{ sinon}\end{aligned}$$

Donc en prenant $y = jK$ avec $j \in [0, r-1]$

$$\mathcal{F} |\psi\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{\frac{2i\pi}{r} j x_0} \left| j \frac{2^n}{r} \right\rangle \tag{4.8}$$

Remarquons que x_0 n'apparait pas dans la définition des états superposés, seulement dans les coefficients de la superposition. Si nous effectuons de nouveau une mesure dans la base de calcul nous allons trouver un état $|z\rangle$ où z est un multiple de $\frac{2^n}{r} : z = j\frac{2^n}{r}$ $(0 \leq j \leq r-1) \rightarrow \frac{z}{2^n} = \frac{j}{r}$. Dans cette dernière équation z et 2^n sont connus mais j ne l'est pas ; on ne peut donc pas encore en déduire r. Sauf que ... si j et r sont premiers entre eux, il suffit de réduire le rapport $\frac{z}{2^n}$ pour en déduire j et r. Remarquons que comme dans l'expression (4.8) tous les états ont la même probabilité d'être obtenus lors d'une mesure (puisque $\left| e^{\frac{2i\pi}{r} j x_0} \right|^2 = 1$) ; le nombre j est donc aléatoirement uniforme dans $[0, r-1]$. La probabilité que ce nombre soit premier avec r est donnée par un théorème de théorie des nombres et est au moins d'ordre $\frac{1}{\log r}$ qui est plus grand que $\frac{1}{\log 2^n} = \frac{1}{n}$; donc en répétant la mesure (le tirage de z) n fois on peut obtenir r avec une probabilité aussi proche de 1 que l'on veut. Comme la transformée de Fourier ne requiert que $O(n^2)$ opérations, globalement l'algorithme aura comme degré de complexité $O(n^3) \simeq O(\log N)^3$.

4.3 Factorisation

Il nous reste la dernière étape qui est de relier le problème de la décomposition d'un nombre N en facteurs premiers (factorisation), à celui de la recherche de la période d'une fonction.

Pour factoriser un nombre N l'algorithme le plus simple consiste à le diviser par tous les nombres premiers plus petits que $\sqrt{N}$ ce qui requiert $\sqrt{N} = \exp(\frac{1}{2} \log N)$ opérations. Les algorithmes actuels les plus sophistiqués permettent de réaliser la factorisation en $\exp((\log N)^{1/3} (\log \log N)^{2/3})$.

Examinons l'algorithme de Shor : Nous cherchons un facteur de N.

1. On tire au hasard un entier $a < N$. Le plus probable pour des grands nombres est que a soit premier avec N. Sinon on a trouvé un facteur de N (on utilise l'algorithme d'Euclide pour chercher un PGCD éventuel, ce qui coûte de l'ordre de $\log N$ opérations).

2. Si a et N sont premiers entre eux, d'après un théorème dû à Euler il existe un entier r tel que $a^r = 1 \pmod N$. Le plus petit entier r qui satisfait cette relation est appelé *l'ordre* de a modulo N. L'équation peut se reécrire $a^r - 1 = 0 \pmod N$. Supposons de surcroît que r soit *pair*. Alors
$$(a^{r/2} - 1)(a^{r/2} + 1) = 0 \pmod N$$
Soit $\alpha = a^{r/2} - 1$ et $\beta = a^{r/2} + 1$. Alors N divise exactement le produit $\alpha\beta$; α ne peut pas être multiple de N car cela signifierait que $r/2 < r$ serait l'ordre de $a \pmod N$ or on a supposé que c'était r. Donc soit β est multiple de N, soit α et β contiennent chacun un facteur de$N$ de telle sorte que $\alpha\beta$ soit multiple de N ; en cherchant le PGCD de N avec α et β on obtient des facteurs de N.
En fait le théorème 23 (section 9.2) nous dit que le plus probable est que r soit pair et que β ne soit pas multiple de N. Donc la situation qui permet d'arriver à la conclusion a une probabilité non nulle ; il suffit donc de répéter les différentes étapes pour aboutir avec une probabilité arbitrairement petite .
3. Le problème se ramène à la détermination de r. Soit la fonction $f(x) = a^x \pmod N$. Alors la définition de r entraine que r est période de $f(x)$ (exercice : montrer que $(ab) \pmod N = ((a \pmod N)(b \pmod N)) \pmod N$) et on est ramené au problème précédent. CQFD.

L'algorithme de Shor peut se synthétiser de la façon suivante :

Entrée	Un entier N non premier
Sortie	un facteur de N
Durée	$O\left((\log N)^3\right)$ opérations ; probabilité de succés $= O(1)$
Procédure	
1.	Si N est pair retourner 2 ; *fin*
2.	Si N est de la forme m^k (pour $2 \leq m$, $2 \leq k \leq \log_2(N)$), retourner m ; *fin*
3.	Tirer au hasard $a \in [1, N-1]$; si PGCD$(a, N) = d > 1$ retourner d ; *fin*
4.	Utiliser l'algorithme de recherche de la période pour trouver l'ordre r de a modulo N
5.	Si r est pair et $a^{r/2} \neq -1 \bmod N$ calculer PGCD$(a^{r/2}+1, N)$ et PGCD$(a^{r/2}-1, N)$. L'un au moins de ces deux nombres est un facteur de N. - *fin* *Sinon aller à 2*

Pour mesurer l'efficacité de l'algorithme voici quelques estimations de temps de calcul (tirés de Gruska) pour factoriser un nombre de 1024 bits.

— temps de factorisation sur un ordinateur classique (en 2006) : 100 000 ans
— temps de factorisation sur un ordinateur quantique avec un registre de 5100 qubits et environ un milliard de portes quantiques : 5mn.

Cet algorithme a été implémenté sur un ordinateur quantique à 7 qubits et a permis de factoriser le nombre $N = 15$ (Vandersypen L.M.K., Steffen M., Breyta G., Yannoni C.S., Sherwood M.H., Chuang I.L : *Experimental realisation of Shor's quantum factoring algorithm using nuclear magnetc resonance,* Nature, **414**, 883.

4.4 Appendice

4.4.1 Le protocole de cryptage RSA (Rivest R., Shamir A., Adleman L, 1977)

Le principe du cryptage à clé publique est le suivant : Anne veut envoyer à Benoît un message codé. Benoît envoie à Anne publiquement une clé de codage et il garde pour lui une clé de décodage

(clé privée). Anne code le message avec la clé publique - il devient alors indéchiffrable puisque seul Benoît possède la clé de décodage - et l'envoie à Benoît qui le décode. Remarquons que Anne peut coder mais ne peut pas décoder : le protocole n'est pas symétrique. La mise en oeuvre dans le cas du protocole RSA se fait de la façon suivante.

Benoît choisit deux nombres premiers p et q et constitue le nombre $N = pq$. Il choisit par ailleurs un nombre c, premier avec le produit $(p-1)(q-1)$. Il calcule le nombre d tel que $cd = 1 \pmod{(p-1)(q-1)}$ c'est-à-dire inverse de c pour la multiplication $\pmod{(p-1)(q-1)}$

La clé publique est constituée des deux nombres (N, c) ; la clé privée est le nombre d. La procédure est la suivante

- Transmission de la clé publique (N, c) à Anne ;
- Codage ; Le message à coder est représenté par un entier $M < N$; Anne calcule $m \equiv M^c \pmod{N}$ qui constitue le message codé ;
- Transmission de m à Benoît
- Décodage : Benoît calcule $m^d \pmod{N} = M$ qui est le message originel d'Anne ; cette dernière égalité résulte de la théorie des nombres.

Si un espion peut trouver les facteurs de N il aura accés à la clé de décodage, puisque connaissant c qui est public et p et q qu'il aura trouvés, il saura, comme Benoît, calculer d tel que $cd = 1 \pmod{(p-1)(q-1)}$.

4.4.2 Quelques éléments d'arithmétique

1 -Théorème sur les nombres premiers

Notons $\pi(N)$ le nombre de nombres premiers plus petits ou égaux à N. Le théorème des nombres premiers dit que

$$\lim_{N\to\infty} \frac{\pi(N)}{N/\ln N} = 1$$

On traduit "librement" ce théorème en disant que pour N suffisament grand $\pi(N) \simeq N/\ln N$. Comme $\phi(N) \geq \pi(N)$ on en déduit

$$\phi(N) \geq \frac{N}{\ln N}$$

La probabilité qu'un entier a $(< N)$ soit premier avec N est $\frac{\phi(N)}{N}$ donc $\geq \frac{1}{\ln N}$, ce que l'on a utilisé ci-dessus. Cette borne est très faible. Dans l'exemple $N = 15$, sur les quatorze nombres plus petits que N il y en a huit (soit 57%) qui sont premiers avec N. Par ailleurs en tirant aléatoirement deux nombres entre 1 et N la probabilité qu'ils soient premiers entre eux est $\frac{6}{\pi^2} > 60\%$ quand $N \to \infty$.

2 -Arithmétique et RSA

p et q sont premiers et $N = pq$ donc $\phi(N) = (p-1)(q-1)$. Benoît choisit un nombre c premier avec $(p-1)(q-1)$ donc avec $\phi(N)$. D'après le théorème de Bachet de Méziriac ce nombre a donc un inverse modulo $\phi(N)$: $\exists d \quad cd = 1 \bmod \phi(N)$.

Le message qu'Anne veut envoyer est M et le message codé est $m = M^c \bmod N$; pour décoder Benoît fait $m^d = M^{cd} \bmod N$; mais $cd = 1 + k\phi(N)$; donc $m^d = M\left[M^{\phi(N)}\right]^k \bmod N$.

Supposons maintenant *que M est premier avec N* (ce qui nest pas obligatoire). Alors (voir la formule 9.19) $M^{\phi(N)} = 1 \bmod N$ et $m^d = M$.
(Ici $\phi(N)$, est l'indicatrice d'Euler de N, rappelée dans la section 9.2, equation (9.19)).

Si M n'est pas premier avec N on arrive quand même au résultat mais c'est plus dur à démontrer.

4.5 Autres applications de la transformation de Fourier quantique

— Estimation de Phase (voir exercice 27)

Problème : Trouver la valeur propre $e^{2i\pi\phi}$ associée à l'un des vecteurs propres $|u\rangle$ d'un opérateur unitaire U

Entrée. : Une boite noire qui réalise l'application de U et l'état propre $|u\rangle$ de U duquel on cherche la valeur propre

Sortie : La phase ϕ

— Problème du logarithme discret

Problème : Etant donnés deux entiers a et b premiers avec N ($N > b \geq a$) tels qu'il existe un entier s satisfaisant $a^s = b \bmod N$; trouver s (remarque : si r est l'ordre de $a \bmod N$, $s \leq r - 1$)

Entrée. : Une boite noire qui réalise l'opération $U_f |x_1\rangle |x_2\rangle |y\rangle = |x_1\rangle |x_2\rangle |y \oplus f(x_1, x_2)\rangle$ où $f(x_1, x_2) = b^{x_1} a^{x_2}$

Sortie : Le plus petit entier s tel que $a^s = b \bmod N$

— Compter les solutions du problème de recherche dans une liste de N items (voir exercice 28).

Problème : On cherche à déterminer combien d' éléments d'une liste de N satisfont un critère prédéfini.

Entrée. : La fonction de reconnaissance (oracle) de la solution et l'opérateur de Grover associé.

Sortie : Le nombre M de solutions

4.6 EXERCICES

Exercice 23 *Transformation de Fourier quantique*

1. Montrer que $\frac{1}{N}\sum_{j=0}^{N-1} e^{\frac{2i\pi}{N}jk} = \delta_{k0}$
2. Quels sont les coefficients de la matrice la transformation de Fourier (dans la base de calcul) (voir l'équation (4.2)) ; en déduire que la transformation de Fourier est unitaire.
3. *Factorisation de la transformation de Fourier :* Reprenons l'équation (4.2)

$$|j\rangle \overset{\mathcal{F}}{\to} \mathcal{F}\,|j\rangle = \widetilde{|j\rangle} = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{\frac{2i\pi}{N}jk}\,|k\rangle$$

   (a) En remplaçant l'état $|k\rangle$ par sa représentation binaire :$|k\rangle \to |k_1k_2...k_n\rangle$ où $k = k_1 2^{n-1} + k_2 2^{n-2} + ...k_n 2^0$ montrer que :

$$\widetilde{|j\rangle} = \frac{1}{\sqrt{2^n}}\prod_{l=1}^{n}\left(|0\rangle + e^{2i\pi\frac{j}{2^l}}\,|1\rangle\right)$$

   Dans cette expression $|0\rangle$ et $|1\rangle$ réfèrent aux deux états du qubit $|k_l\rangle$

   (b) Soit $j = \left(j_1 2^{n-1} + j_2 2^{n-2} + ...j_n 2^0\right)$ la représentation binaire de j ; pour $p \in [1,n]$ on note $0.j_1j_2...j_p = j_1/2 + j_2/2^2 + ... + j_p/2^p$ Montrer que :

$$\begin{aligned} e^{2i\pi\frac{j}{2^l}} &= e^{2i\pi 0.j_n} \quad \text{pour } l=1 \\ &= e^{2i\pi 0.j_{n-1}j_n} \quad \text{pour } l=2 \\ &= \cdots \\ &= e^{2i\pi\,0.j_1j_2...j_n} \quad \text{pour } l=n \end{aligned}$$

   (c) En déduire l'equation (4.5)

4. *Construction du circuit QFT*

   (a) Montrer que l'action de la porte de Hadamard sur le premier qubit peut s'écrire

$$|j_1\rangle \overset{H}{\to} \frac{1}{\sqrt{2}}\left[|0\rangle + e^{2i\pi 0.j_1}\,|1\rangle\right]$$

   (b) Montrer que l'action de la porte cR_2 (c'est le qubit $|j_2\rangle$ qui contrôle)sur le résultat a pour effet

$$|j_1\rangle\,|j_2\rangle \overset{H}{\to} \left(|0\rangle + e^{2i\pi 0.j_1}\,|1\rangle\right)|j_2\rangle \overset{cR_2}{\to} \left(|0\rangle + e^{2i\pi 0.j_1j_2}\,|1\rangle\right)|j_2\rangle$$

   (c) En déduire que l'application successive des portes $cR_3...cR_n$ conduit à

$$|j_1\rangle\,|j_2\rangle\,|j_3\rangle\,...\,|j_n\rangle \to \left(|0\rangle + e^{2i\pi\,0.j_1j_2...j_n}\,|1\rangle\right)|j_2\rangle\,|j_3\rangle\,...\,|j_n\rangle$$

   qui est le dernier terme de l'expression (4.5).

   (d) Que donne la succession de portes agissant sur le deuxième qubit $|j_2\rangle$?

   (e) Une fois que tous le qubits ont été traités l'état obtenu coïncide-t-il avec celui de l'équation (4.5) ? Quelle opération faut-il réaliser pour obtenir le bon résultat ?

Exercice 24 Algorithme d'Euclide

Il s'agit de trouver le PGCD de deux entiers positifs a et b ($a > b$), c'est à dire le plus grand entier k tel que $a = kq_a$ et $b = kq_b$ o ù q_a et q_b sont deux entiers. L'algorithme fonctionne de la fa çon suivante : divise a par b, quotient q_1,reste k_2 ; puis divise b par k_2, quotient q_2,reste k_3 , et ainsi de suite.

$$\begin{aligned} k_n &= q_{n+1} \times k_{n+1} + k_{n+2} \\ k_0 &= a \quad k_1 = b \end{aligned}$$

On résume dans le tableau

Etape	Dividende	Diviseur	Quotient	Reste
0	$a = k_0$	$b = k_1$	q_1	k_2
1	k_1	k_2	q_2	k_3
2	k_2	k_3	q_3	k_4
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$m-1$	k_{m-1}	k_m	q_m	k_{m+1}
m	k_m	k_{m+1}	q_{m+1}	0

On a alors $PGCD(a, b) = k_{m+1}$.

1. Calculer PGCD(6825,1430) puis PGCD(105,22). Dans chaque cas combien d' étapes sont nécessaires ?
2. Montrer qu'en général $k_{i+2} \leq \frac{1}{2} k_i$; en déduire que le nombre d'étapes est au plus $2 \times [\ln a]$.

Exercice 25 Factorisation de 91

1. Dans la liste des entiers premiers avec N (et $< N$) on choisit $a = 4$. Calculer r, l'ordre de a modulo N.
2. Vérifier que r satisfait : r pair et $a^{r/2} \neq -1 \bmod N$.
3. Calculer le PGCD($a^{r/2}+1 \bmod N$, N) et PGCD($a^{r/2}-1 \bmod N$, N). En déduire les facteurs de 91.
4. Montrer que pour le choix $a = 9$ la méthode ne fonctionne pas.

Exercice 26 *r ne divise pas exactement 2^n*

Reprenons l'algorithme de Shor au niveau de l'équation (4.7)

$$|\psi\rangle = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + kr\rangle$$

et supposons maintenant que r ne divise pas exactement 2^n c'est-à -dire que $K \neq \frac{2^n}{r}$. Comme dans le cas précédent la transformation de Fourier sur cet état donne

$$\mathcal{F}\,|\psi\rangle = \sum_{y=0}^{2^n-1} \widetilde{\varphi}(y)\,|y\rangle \;\text{ avec }\; \widetilde{\varphi}(y) = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{K-1} \frac{1}{\sqrt{K}}\, e^{\frac{2i\pi}{2^n} y(x_0+kr)}$$

1. Montrer que la probabilité d'obtenir l'état $|y\rangle$ est donnée par
$$P(y) = |\widetilde{\varphi}(y)|^2 = \frac{1}{2^n K} \frac{\sin^2(\pi y K r/2^n)}{\sin^2(\pi y r/2^n)}$$
2. Retrouver à partir de cette expression le résultat du cours dans le cas où $K = \frac{2^n}{r}$
3. Faire un plot (Maple ou autre logiciel) de $P(y)$ pour $y \in [0, 50]$, en posant $K - \frac{2^n}{r} = \delta$ avec $K = 10$ et $\delta = 0.1$.
4. On s'aperçoit donc que la fonction $P(y)$ est très "piquée" pour $y \simeq jK$. Pour étudier le comportement de $P(y)$ au voisinage d'un de ces pics on pose $y = jK + \delta$ où j est un entier $0 \leq j \leq r-1$. En utilisant l'inégalité $\frac{2}{\pi}x \leq \sin x \leq x$ valable pour $0 \leq x \leq \frac{\pi}{2}$ montrer que
$$P(y) \geq \frac{4}{\pi^2}\frac{1}{r} \text{ pour } j\frac{2^n}{r} - \frac{1}{2} \leq y \leq j\frac{2^n}{r} + \frac{1}{2}$$
où on a supposé $\frac{2^n}{r} \simeq K$. En déduire que la probabilité que y se trouve dans le voisinage de l'un des multiples de $\frac{2^n}{r}$ est supérieure à 40%.
5. *Fin de l'histoire :* Ce résultat signifie que si y n'est pas exactement un multiple $\frac{2^n}{r}$ il a une forte probabilité d'en être proche. Une mesure projetera probablement l'état $\mathcal{F}|\psi\rangle$ sur un état $|y\rangle$ tel que $\left|y - j\frac{2^n}{r}\right| \leq \frac{1}{2}$. On connait n et y (le résultat de la mesure) il faut en déduire j et r..
   (a) L'inégalité précédente s'écrit aussi $\left|\frac{y}{2^n} - \frac{j}{r}\right| \leq \frac{1}{2^{n+1}}$; on a pris au départ $2^n > N^2 > r^2$; Donc $\left|\frac{y}{2^n} - \frac{j}{r}\right| < \frac{1}{2r^2}$.
   (b) Un théorème (Hardy et Wright, 1965) dit qu'étant donné le nombre rationnel x il existe une unique fraction $\frac{p}{q}$ qui satisfait $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$. Cette fraction s'obtient sous forme irréductible $\frac{p_0}{q_0}$ à partir d'une technique (développement de x en fraction continue) qui coûte $O(n^3)$ opérations. On applique ce théorême avec $x = \frac{y}{2^n}$; on en déduit j et r s'ils sont premiers entre eux. La probabilité que cette éventualité survienne est d'environ 60% (voir appendice arithmétique). Sinon on peut essayer $r = 2r_0$, $r = 3r_0, ...$ On a globalement $0.4 \times 0.6 = 0.24$ chance que ça marche. Sinon on recommence.

Exercice 27 *Estimation de phase*

1. Montrer que les valeurs propres d'un opérateur unitaire sont de la forme $e^{i\theta}$
2. Soit U un opérateur unitaire dans l'espace des états à n qubits, $|u\rangle$ un de ses vecteurs propres et $e^{2i\pi\phi}$ la valeur propre associé. Le problème de l'estimation de phase est de déterminer $\phi \in [0, 1]$
   On définit la porte logique quantique c-U (U controlé) de la façon suivante
$$|q\rangle|\psi\rangle \overset{c-U}{\rightarrow} \begin{array}{ll} |q\rangle|\psi\rangle & \text{si } q = 0 \\ |q\rangle U|\psi\rangle & \text{si } q = 1 \end{array}$$
   où $|q\rangle$ est le qubit de contrôle et $|\psi\rangle$ un état quelconque à n qubits.
   On représente cette porte logique par le diagramme ci dessus
   Montrer que si $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ et $|\psi\rangle = |u\rangle$ alors l'action de c-U équivaut à
$$[\alpha|0\rangle + \beta|1\rangle]\ |u\rangle \overset{c-U}{\rightarrow} \left[\alpha|0\rangle + \beta e^{2i\pi\phi}|1\rangle\right]\ |u\rangle$$

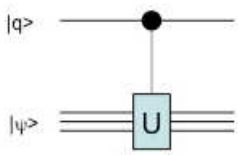
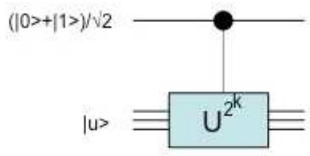


FIGURE 4.3 – Porte c-U.

3. Supposons que ϕ ait une représentation binaire exacte sur t bits :

$$\phi = \phi_1/2 + \phi_2/2^2 + \cdots \phi_t/2^t = 0.\phi_1\phi_2\cdots\phi_t$$

(a) Montrer que $e^{2i\pi\, 2^k\phi} = e^{2i\pi\, 0.\phi_{k+1}\phi_{k+2}\cdots\phi_t}$ pour $k = 0, ..., t-1$



(b) En déduire que la sortie de la porte logique ci-contre est de la forme

$$\frac{1}{\sqrt{2}}\left[|0\rangle + e^{2i\pi\, 0.\phi_{k+1}\phi_{k+2}\cdots\phi_t}\,|1\rangle\right]\,|u\rangle$$

4. Donner l'expression de l'état de sortie $|\Psi\rangle$ associé au circuit ci-dessous
Premières étapes du circuit d'estimation de phase

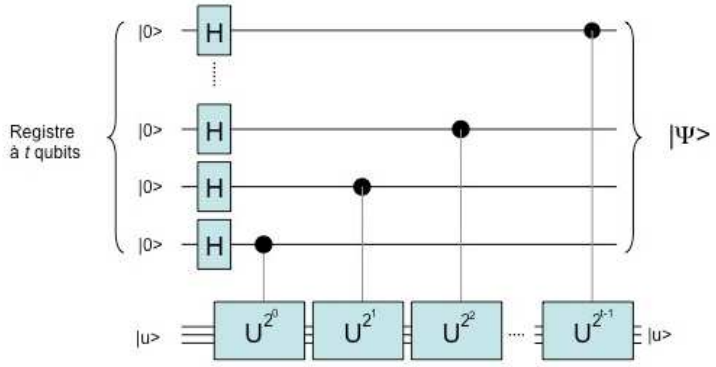


FIGURE 4.4 – Premières étapes du circuit d'estimation de phase.

5. On note QFT le circuit qui réalise la transformation de Fourier quantique et QFT^{-1} le même circuit mais pris "de droite à gauche". On applique QFT^{-1} sur l'état $|\Psi\rangle$. Quel est l'état résultant ? Comment en déduire une détermination de ϕ ?

6. *Fin de l'histoire* : si ϕ n'a pas une repré sentation binaire exacte sur t bits, alors la méthode engendre une erreur statistique et une erreur systématique. On peut montrer que si on veut une approximation de ϕ à moins de $1/2^p$ (erreur syst ématique) avec une probabilité supérieure à $1-\epsilon$ (l'erreur statistique est alors de ϵ) alors le nombre t de bits dans le registre de donnée doit être

$$t = p + \left\lceil \ln(2 + \frac{1}{2\epsilon}) \right\rceil$$

où la notation $\lceil x \rceil$ désigne l'entier le plus proche de x plus grand que x.

Exercice 28 *Le comptage quantique*

L'algorithme de Grover permet de trouver un ou plusieurs éléments dans une liste non structurée à condition que le nombre de solutions soit connu. Si ce n'est pas le cas nous allons voir que la méthode d'estimation de phase permet de déterminer ce nombre de solutions.

Supposons que parmi les N éléments de la liste il y en ait $M \geq 1$ qui satisfassent le critère c'est à dire que pour ces éléments $f(x) = 1$ où f est l'oracle. Désignons par $\mathcal{B}$ (comme "bon") l'ensemble de ces états et par $\mathcal{M}$ (comme "mauvais") l'ensemble des $N - M$ autres états. L'état $|\psi\rangle$ de superposition uniforme peut être alors décomposé,

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \sqrt{\frac{N-M}{N}} \frac{1}{\sqrt{N-M}} \sum_{x\in\mathcal{M}} |x\rangle + \sqrt{\frac{M}{N}} \frac{1}{\sqrt{M}} \sum_{x\in\mathcal{B}} |x\rangle \\ &= \cos(\frac{\theta}{2}) |\alpha\rangle + \sin(\frac{\theta}{2}) |\beta\rangle \qquad \text{avec} \\ |\alpha\rangle &= \frac{1}{\sqrt{N-M}} \sum_{x\in\mathcal{M}} |x\rangle \quad ; \quad |\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x\in\mathcal{B}} |x\rangle \qquad \sin(\frac{\theta}{2}) = \sqrt{\frac{M}{N}} \end{aligned}$$

1. On veut exprimer l'opérateur de Grover G dans la base $\{|\alpha\rangle, |\beta\rangle\}$

   (a) Montrer que dans cette base, G est représenté par la matrice unitaire

   $$\widetilde{G} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

   (b) Quelles sont les vecteurs propres et les valeurs propres de cette matrice.

   (c) On désigne par $|u\rangle$ et $|v\rangle$ les états propres de l'opérateur G correspondant aux vecteurs propres ci-dessus. Exprimer ces états en fonction des états $|\alpha\rangle$ et $|\beta\rangle$; en déduire que l'état $|\psi\rangle$ de superposition uniforme peut s'écrire

   $$|\psi\rangle = c_u |u\rangle + c_v |v\rangle$$

   où l'on précisera la valeur des coefficients c_u et c_v.

2. On va mettre en oeuvre l'algorithme d'estimation de phase pour trouver la phase des valeurs propres associées aux états propres $|u\rangle$ et $|v\rangle$. Au lieu d'initaliser le registre du bas du circuit de la figure 1 avec l'un des états propres $|u\rangle$ ou $|v\rangle$ qu'on ne connait pas on l'initialise avec l'état de superposition uniforme $|\psi\rangle$.

(a) Quel est l'état de sortie du système des deux registres après application de QFT^{-1} sur le registre de données ? (on suppose que la phase - divisée par 2π - de chacune des deux valeurs propres a une représentation binaire exacte sur t bit.)

(b) Comment en déduire le nombre M de solutions ?

Exercice 29 *Le problème de Simon (1994)*

Il constitue le prémisse du problème de recherche d'une période. Soit $f : \{0,1\}^n \to \{0,1\}^n$ ayant la propriété (périodique)

$$\exists\, s \in \{0,1\}^n \text{ tel que pour } x \neq y \quad f(x) = f(y) \Leftrightarrow y = x \oplus s$$

Combien faut-il d'évaluation de f pour trouver s ? Réponse :

— algorithme classique : $O(2^{n/3})$

— algorithme quantique de Simon : $O(n)$

1. Montrer (de nouveau) que

$$\text{pour } x \in \{0,1\}^n \text{ alors } H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle$$

où $x \cdot z = x_0 z_0 + x_1 z_1 + \cdots + x_{n-1} z_{n-1} \pmod 2$

2. On dispose d'une boite noire U_f qui réalise $|x\rangle |b\rangle \overset{U_f}{\to} |x\rangle |b \oplus f(x)\rangle$ où $x \in \{0,1\}^n$ et $f(x) \in \{0,1\}^n$. On réalise le circuit suivant

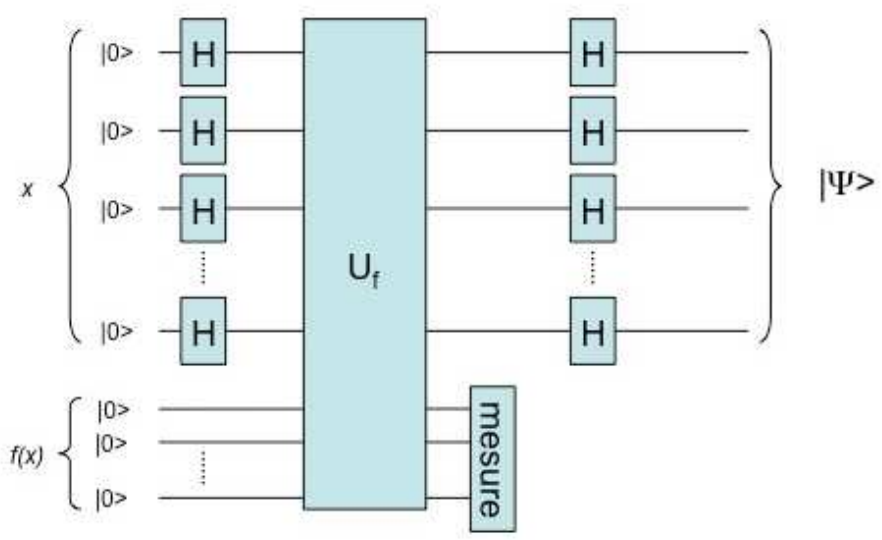


FIGURE 4.5 – Le circuit.

(a) Montrer qu'avant la mesure l'état du système est

$$\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

(b) Le résultat de la mesure du second registre est w. On définit $x_0 : f(x_0) = w$. Exprimer l'état du premier registre après la mesure du second.

(c) Quel est l'état du premier registre après la (deuxième) transformation de Hadamard ?

(d) En conclure que les seuls états de base qui contribuent à l' état final $|\psi\rangle$ sont orthogonaux à s.

3. On réalise alors une mesure du premier registre et on note le résultat z_1 ; On réinitialise le système et on reparcourt tout le circuit, puis on effectue une mesure du premier registre et on note le résultat z_2 ; on répète cette opération $n-1$ fois pour obtenir un ensemble de mesures $\{z_1, z_2, ...z_{n-1}\}$. La probabilité que ces $n-1$ éléments de $\{0,1\}^n$ soient indépendants est supérieure à $1/4$. On supposera donc qu'ils le sont (sinon on recommence tout le processus). Tous ces éléments sont tels que

$$z_i \cdot s = 0 \quad i = 1, 2, ..., n-1$$

En déduire s. Combien d'évaluations de f a-t-il fallu ?

4. Exemple avec $n = 4$; on a trouvé $z_1 = (0111),\ z_2 = (1011),\ z_3 = (1101)$. Trouver s.

Chapitre 5

Jeux quantiques

Nous étudions dans ce chapitre un jeu coopératif à deux joueurs, que nous nommerons "jeu de Bell" [1] car les espérances des joueurs suivant que l'on se trouve dans un monde quantique ou, au contraire, déterministe (ou même stochastique) avec des variables cachées, violent ou, au contraire, vérifient les *inégalités de Bell*. Historiquement ces inégalités forment un théorème, prouvé par le physicien J. Bell dans les années 60, qui s'applique à certains dispositifs physiques.
Dans une seconde partie nous décrivons le principe de l'expérience de A. Aspect et alii (1982) qui réalise expérimentalement un dispositif satisfaisant les hypothèses du théorème de Bell. Nous l'interpréterons aussi comme une réalisation pratique du jeu de Bell. Cette expérience célèbre a permis de trancher entre la mécanique quantique et la possibilité d'une description à la fois *locale* et *déterministe* du monde physique.

5.1 Le jeu de Bell

John Bell(1928-1990), physicien d'origine Irlandaise, a travaillé au CERN (Genève). Il a formulé en 1964 l' "inégalité de Bell".

Le jeu Une équipe de deux joueurs Anne (A) et Benoit (B), est opposée à un arbitre R. Chaque partie se déroule comme suit :
0- A et B communiquent librement : ils se mettent d'accord sur un vecteur $\vec{\lambda}$;
1- R choisit un couple de deux questions $(r, s) \in \{(0,0),(0,1),(1,0),(1,1)\}$

1. en suivant les idées de [Wat06] lecture 20

R envoie la question r à Anne et la question s à Benoit (Chaque joueur ne connaît que la question qu'il reçoit de R).
2- Anne répond par un nombre $a \in \{-1, 1\}$ et Benoit répond par un nombre $b \in \{-1, 1\}$.
3- L'équipe AB reçoit un gain de $(-1)^{r \wedge s} \cdot a \cdot b$.
La table suivante résume les cas où AB "gagne la partie" i.e. gagne $+1$; dans tout autre cas, AB gagne -1.

r	s	$a \cdot b$	gain
0	0	1	1
0	1	1	1
1	0	1	1
1	1	-1	1

Dans tous les scénarios examinés ci-dessous, A et B ne sont pas autorisés à communiquer l'un avec l'autre au cours des phases 1,2,3 du jeu. Dans le cas déterministe, ils peuvent utiliser le vecteur $\vec{\lambda}$

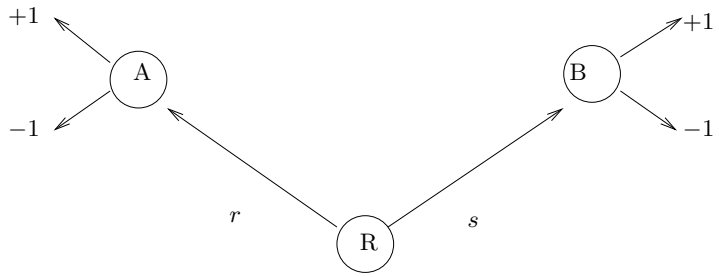


FIGURE 5.1 – Le jeu de Bell

(ainsi que leurs données personnelles) dans des calculs arbitrairement complexes mais *déterministes*.
Dans le cas probabiliste, ils peuvent utiliser le vecteur $\vec{\lambda}$ (ainsi que leurs données personnelles) dans des calculs arbitrairement complexes et *probabilistes* (i.e. connaissant la question , ils peuvent, chacun de leur côté, tirer des bits au hasard).
Dans le cas quantique, ils peuvent partager un vecteur de paramètres $|\psi\rangle$ dans le produit tensoriel de leurs espaces personnels, et l'utiliser, ainsi que des données personnelles dans des calculs *quantiques*.
Dans ce qui suit nous supposons que l'arbitre choisit (r, s) au hasard, selon une loi de probabilité uniforme.

Stratégies déterministes A et B peuvent librement discuter pour élaborer une stratégie commune. Supposons que la stratégie consiste en ce que A (resp. B) réponde : A_0 (resp. B_0) à la question 0 et A_1 (resp. B_1) à la question 1.
Remarquons tout d'abord que, pour que cette stratégie gagne toutes les parties il faudrait que :

$$A_0 \cdot B_0 = 1, \;\; A_0 \cdot B_1 = 1, \;\; A_1 \cdot B_0 = 1, \;\; A_1 \cdot B_1 = -1$$

Or le produit des trois premières égalités fournit : $A_1 \cdot B_1 = 1$. Donc cette stratégie ne peut être gagnante sur toutes les parties. On en déduit l'analyse suivante.
Cas 1 : $A_0 = B_0 = B_1 = A_1$.
AB gagne 1 si $rs \in \{00, 01, 10\}$ et gagne -1 si $rs = 11$. Donc $E(S) = \frac{1}{2}$.
Cas 2 : $A_0 \neq B_0$ ou $A_0 \neq B_1$ ou $A_1 \neq B_0$.

Alors AB gagne -1 pour au moins l'un des couples $rs \in \{00, 01, 10\}$. Donc $E(S) \leq \frac{1}{2}$.
La stratégie du cas 1 maximise donc le gain moyen de AB, qui vaut $\frac{1}{2}$.

Stratégies probabilistes Dans ce cas on note A_i (resp. B_i) la variable aléatoire qui représente le choix de réponse d'Anne (resp. Benoit) à la question i.

Le gain moyen de AB est alors :

$$G_p := \frac{1}{4}[\mathbb{E}(A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1)].$$

A et B partagent leurs paramètres $\vec{\lambda}$ mais ils tirent leurs bits aléatoires *indépendamment* l'un de l'autre. La modélisation (mathématique) des stratégies A_i, B_j traduit cette hypothèse (physique) par le fait que, pour tout $(i, j) \in \{0, 1\}^2$, les variables A_i, B_j sont indépendantes (au sens probabiliste du terme). Donc

$$G_p = \frac{1}{4}[\mathbb{E}(A_0)\mathbb{E}(B_0) + \mathbb{E}(A_0)\mathbb{E}(B_1) + \mathbb{E}(A_1)\mathbb{E}(B_0) - \mathbb{E}(A_1)\mathbb{E}(B_1)].$$

Lemme 8 *Soient a_0, a_1, b_0, b_1 quatre nombres réels dans $[-1, +1]$. Alors*

$$a_0b_0 + a_0b_1 + a_1b_0 - a_1b_1 \leq 2.$$

Preuve. Notons $f : [-1, +1]^4 \to \mathbb{R}$ l'application définie par

$$f(a_0, a_1, b_0, b_1) := a_0b_0 + a_0b_1 + a_1b_0 - a_1b_1$$

Elle est continue, elle atteint donc son maximum max sur un point du compact $[-1, +1]^4$. Ce maximum est > 0 (vu que $f(1, 1, 1, 1) = 2$). Supposons que

$$\max = f(a_0, a_1, b_0, b_1),$$

et montrons que max est atteint en un point de $\{-1, +1\}^4$ (l'ensemble des sommets de $[-1, +1]^4$).
Etape 1 : Supposons que $-1 < a_0 < 1$.
$f(a_0, a_1, b_0, b_1) := a_0(b_0 + b_1) + a_1b_0 - a_1b_1$ Si $b_0 + b_1 \neq 0$ alors il existe un point $(a_0 \pm \varepsilon, a_1, b_0, b_1)$ qui a une image par f $>$ max, ce qui est impossible. Donc $b_0 + b_1 = 0$. Donc $f(1, a_1, b_0, b_1) = \max$.
On peut donc se ramener au cas où $a_0 \in \{-1, +1\}$.
Etape 2 : Supposons que $a_0 \in \{-1, 1\}, -1 < a_1 < 1$
Comme $f(a_0, a_1, b_0, b_1) := a_0b_0 + a_0b_1 + a_1(b_0 - b_1)$, on obtient que $(b_0 - b_1) = 0$, ce qui entraine que $f(a_0, 1, b_0, b_1) = \max$.
En raisonnant de façon analogue sur b_0 puis b_1 on prouve finalement que :

$$\exists (a_0, a_1, b_0, b_1) \in \{-1, +1\}^4, f(a_0, a_1, b_0, b_1) = \max .$$

Mais l'analyse des stratégies déterministes nous a montré que,

$$\forall (a_0, a_1, b_0, b_1) \in \{-1, +1\}^4, f(a_0, a_1, b_0, b_1) \leq 2.$$

■

Revenons à G_p. Il résulte du lemme que, pour toute stratégie probabiliste,

$$G_p \leq \frac{1}{2}$$

et comme la stratégie déterministe $A_0 = A_1 = B_0 = B_1 = 1$ atteint ce gain moyen, c'est le gain moyen maximal que peut réaliser AB.

Stratégie quantique A et B partagent un vecteur

$$\psi := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{5.1}$$

(A peut agir sur le premier qbit et B peut agir sur le second qbit). Leur stratégie est la suivante :
- pour tout $r \in \{0,1\}$, A mesure son qbit avec l'observable A_r, puis répond à R le résultat a de cette mesure
- pour tout $s \in \{0,1\}$, B mesure son qbit avec l'observable B_s, puis répond à R le résultat b de cette mesure.

Les observables (i.e. opérateurs hermitiens) utilisées sont :

$$A_0 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} (= s_0); \quad A_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} (= s_{\pi/4});$$

$$B_0 := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} (= s_{\pi/8}); \quad B_1 := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} (= s_{-\pi/8}).$$

On a vu aux chapitres 1,2, que l'espérance d'une observable $\mathcal{M}$ sur un état $|\varphi\rangle$ vaut

$$\langle\varphi| M |\varphi\rangle .$$

La réponse a, b renvoyée par AB à R est obtenue, par une mesure de A suivie d'une mesure de B, ou bien une mesure de B suivie d'une mesure de A. Comme les opérateurs $A_i \otimes \mathrm{Id}$ et $\mathrm{Id} \otimes B_j$ commutent, en fait l'ordre des mesures ne change pas la loi de probabilité de la variable aléatoire $\omega \mapsto (a, b)$ (où a est une valeur propre de $A_i \otimes \mathrm{Id}$, b est une valeur propre de $\mathrm{Id} \otimes B_j$). La loi de probabilité de $\omega \mapsto ab$ est en fait celle correspondant à l'opérateur produit $A_i \otimes \mathrm{Id} \cdot \mathrm{Id} \otimes B_j = A_i \otimes B_j$. Donc, l'espérance de la variable aléatoire $\omega \mapsto ab$, conditionnée par la valeur de la question (r, s) est :

$$\langle\psi| A_r \otimes B_s |\psi\rangle . \tag{5.2}$$

et l'espérance de gain de AB est finalement :

$$G = \frac{1}{4}[\langle\psi| A_0 \otimes B_0 |\psi\rangle + \langle\psi| A_0 \otimes B_1 |\psi\rangle + \langle\psi| A_1 \otimes B_0 |\psi\rangle - \langle\psi| A_1 \otimes B_1 |\psi\rangle].$$

Un calcul soigneux montre que,

$$\text{si } (r,s) \in \{(0,0),(0,1),(1,0)\}, \text{ alors} \quad \langle\psi| A_r \otimes B_s |\psi\rangle = \frac{1}{\sqrt{2}}$$
$$\text{et} \quad \langle\psi| A_1 \otimes B_1 |\psi\rangle = -\frac{1}{\sqrt{2}}.$$

Donc

$$G_{QM} = \frac{\sqrt{2}}{2} \tag{5.3}$$

Comparaison Il s'avère que les gains (moyens) maximaux des stratégies déterministes, probabilistes et quantiques sont :

$$G_d = \frac{1}{2}, \quad G_p = \frac{1}{2}, \quad G_{QM} = \frac{\sqrt{2}}{2}$$

Or $\frac{\sqrt{2}}{2} > \frac{1}{2}$. On en conclut que :
1- le partage de qbits intriqués et des moyens de calcul quantiques fournissent des possibilités de

calcul plus puissantes que le partage de bits déterministes ou aléatoires et des moyens de calcul déterministes ou aléatoires ;
2- il n'est pas possible de simuler les phénomènes de calcul prédits par la mécanique quantique, par des calculs déterministes ou stochastiques, sous réserve que ces calculs vérifient les hypothèses que nous avons inclues dans la règle du jeu i.e. que A et B ne peuvent plus communiquer après que R leur a posé sa question (hypothèse de *localité*).

5.2 Expérience d'Aspect et alii

Alain Aspect, physicien Français, est professeur à l'institut supérieur d'optique, à Orsay.

De fait, ce que nous avons appelé "jeu de Bell", est une version imagée de l'expérience *réalisée* par A. Aspect et alii (1982) en vue de trancher entre la mécanique quantique et d'autres théories (hypothétiques) [Asp02].

Dispositif expérimental
Une source S de paires de photons intriqués ν_A, ν_B dans l'état de Bell (5.1) envoie le photon ν_A

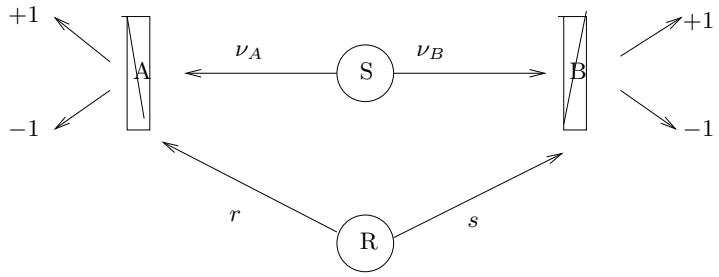


FIGURE 5.2 – L'expérience de [Aspect et alii, 1982]

vers un analyseur A et le photon ν_B vers un analyseur B de polarisation linéaire. Dans la position 0 (resp. 1) l'analyseur A mesure la polarisation selon la base des vecteurs propres de la matrice A_0 (resp. A_1), ce qui revient à dire qu'il applique l'observable A_0 (resp. A_1). l'analyseur B, lui-aussi, dans la position i, applique l'observable B_i. Le réglage des analyseurs (sur la position 0 ou 1) est défini "pendant le vol du photon", suffisamment longtemps après l'émission des photons, ce qui garantit que, aucune interaction se propageant à une vitesse $\leq c$ ne peut aller de l'analyseur A ou

de ν_A (resp. B ou de ν_B) jusqu'à la particule ν_B (resp. ν_A) avant son passage dans l'analyseur.
L'expérience est répétée un grand nombre N de fois ; la $k$ieme expérience fournit un choix (aléatoire, suivant une loi uniforme) de valeurs (r_k, s_k) et les résultats a_k, b_k des analyseurs.
On calcule finalement

$$\frac{1}{N}\sum_{k=1}^{N}(-1)^{r_k \wedge s_k} \cdot a_k \cdot b_k. \tag{5.4}$$

L'expérience fournit un résultat proche de $\frac{\sqrt{2}}{2}$ (qui est prédit par la mécanique quantique). L'analyse de la précision des mesures montre que la déviation par rapport à $\frac{1}{2}$ ne peut être imputée à des défauts du dispositif.

Analyse .
Le jeu de Bell est donc la métaphore suivante :
- l'expérimentateur est vu comme l'arbitre R
- le couple de réglages des analyseurs est vu comme une question (r, s) adressée au système physique AB
- le mécanisme (inconnu) par lequel les photons "déterminent le résultat de leurs interactions avec les analyseurs" est vu comme la stratégie de AB.
Comme N est grand et comme les (r, s) sont tirés uniformément, le nombre (5.4) est proche de l'espérance de la stratégie de AB.

Nous avons vu que des mécanismes déterministes (ou stochastiques) aboutissent à une espérance $\leq \frac{1}{2}$ (c'est l' "inégalité de Bell"). Or la nature dispose d'une stratégie d'espérance proche de $\frac{\sqrt{2}}{2}$. On en conclut que la nature *n'utilise pas* les mécanismes envisagés dans nos deux premières analyses (stratégies déterministes ou stochastiques, mais avec indépendance entre A et B, sachant la valeur de (r, s)).

Plus généralement, toute théorie qui décrirait cette expérience par :
- des paramètre cachés $\vec{\lambda}$, inconnus de l'expérimentateur et portés par les photons ν_A, ν_B,
- des mécanismes déterministes, locaux (pas d'action de l'analyseur A ni de ν_A sur ν_B, après le choix de r, ni de B ni de ν_B sur ν_A, après le choix de s),
est *réfutée*.

Épilogue .
Quoique cette expérience ait eu un grand retentissement, A. Aspect explique dans [Asp02] que certains détails du dispositifs n'étaient pas encore parfaits et pouvaient laisser une brèche ouverte aux théories à variables cachées : en particulier la qualité "d'aléatoirité" des réglages (r, s) pouvait faire l'objet de critiques. Des expériences plus récentes, en particulier par le groupe de A. Zeilinger, ont encore amélioré ce point et ont confirmé les prédictions de la mécanique quantique (en violant nettement les inégalités de Bell).

5.3 EXERCICES

Exercice 30 *Soient M, N deux opérateurs hermitiens sur un espace de Hilbert $\mathcal{H}$ de dimension finie d.*
1- Montrer que $M \cdot N = N \cdot M$ ssi ils sont diagonalisables dans une même base orthonormée.
2- On suppose que M, N sont les opérateurs hermitiens qui traduisent des observables $\mathcal{M}, \mathcal{N}$ et qu'ils ont des valeurs propres $(\lambda_1, \ldots, \lambda_m), (\mu_1, \ldots, \mu_n)$ dans la base de vecteurs propres $(|u\rangle_1, \ldots, |u\rangle_d)$. On applique à l'état $|u\rangle$ du système physique d'abord l'observable $\mathcal{M}$ puis l'observable $\mathcal{N}$. Quelle est la probabilité d'obtenir le résultat λ_i puis le résultat μ_j ?
3- On note $\mathcal{N} \cdot \mathcal{M}$ l'observable définie par le protocole de mesure suivant :
- mesurer l'observable $\mathcal{M}$, recueillir le résultat λ ;
- mesurer ensuite l'observable $\mathcal{N}$, recueillir le résultat μ ;
- donner comme résultat le produit $\lambda \cdot \mu$.
Montrer que l'opérateur NM (ou MN) représente correctement l'observable $\mathcal{N} \cdot \mathcal{M}$.
4- Vérifier que l'espérance de l'observable $\mathcal{N} \cdot \mathcal{M}$ sur l'état $|\varphi\rangle$ vaut

$$\langle\varphi| NM |\varphi\rangle .$$

(ce qui justifie l'equation (5.2) du cours).

Exercice 31 (Jeu de GHZ) *Une équipe de trois joueurs Anne (A), Benoit (B) et Charles (C), est opposée à un arbitre R. Chaque partie se déroule comme suit :*
0- A ,B ,C communiquent librement : ils se mettent d'accord sur une stratégie et éventuellement un vecteur $\vec{\lambda}$ qu'il peuvent utiliser dans leur stratégie.
1- R choisit un triplet de questions $(r, s, t) \in \{(0,0,0), (0,1,1), (1,0,1), (1,1,0)\}$
R envoie la question r à Anne, la question s à Benoit et la question t à Charles (Chaque joueur ne connait que la question qu'il reçoit de R).
2- Anne répond par un booléen $a \in \{0,1\}$, Benoit par $b \in \{0,1\}$ et Charles par $c \in \{0,1\}$.
3- L'équipe ABC reçoit un gain de 1 dans les cas suivants

r	s	t	$a \oplus b \oplus c$	*gain*
0	*0*	*0*	0	1
0	*1*	*1*	1	1
1	*0*	*1*	1	1
1	*1*	*0*	1	1

et perd i.e. gagne -1, dans tout autre cas. Dans tous les scénarios examinés ci-dessous, A,B,C ne sont pas autorisés à communiquer entre eux au cours des phases 1,2,3 du jeu ;
1- Montrer que ABC n'ont pas de stratégie déterministe qui gagne sur toute question de R.
2- On suppose que R tire ses questions de façon aléatoire, uniforme. Quelle est l'espérance de gain maximale de ABC, avec une stratégie déterministe ?
avec une stratégie probabiliste ?
3- Supposons maintenant que ABC partagent trois qbits intriqués, dans l'état

$$|\psi\rangle := \frac{1}{2}|000\rangle - \frac{1}{2}|011\rangle - \frac{1}{2}|101\rangle - \frac{1}{2}|110\rangle .$$

Ils choisissent la stratégie (quantique) suivante :
- sur la question $q = 1$ ($q = 0$), le joueur applique H (resp. Id*) à son qbit.*

- chaque joueur "mesure son qbit dans la base standard" et renvoie à R le résultat de cette mesure.
3.1 Quel est le gain de ABC sur la question 000 *?*
3.2 Quel est le gain de ABC sur la question 011 *?*
3.3 Quel est le gain moyen de ABC (avec cette stratégie) ?
Note : GHZ sont les initiales des physiciens Greenberger-Horne-Zeilinger qui ont réalisé une expérience que ce jeu décrit métaphoriquement.

Chapitre 6

Corrections d'erreurs

6.1 Décohérence

C'est le principal "ennemi" du calcul quantique car elle induit des "erreurs", elle limite le "temps de calcul" et la "taille" des ordinateurs quantiques (le nombre de qubits susceptibles d'interagir). Ce phénomè ne physique résulte simplement du couplage du système quantique (le ou les qubits) avec son environnement, ce qui a pour conséquence de transférer progressivement l'information contenue dans le système quantique vers l'environnement, et ce faisant de perdre cette information. Une autre conséquence est de transformer l'évolution réversible d'un système quantique isolé (cohérent) en une évolution irr éversible quand il est couplé à l'environnement.

Prenons l'exemple du qubit réalisé par les deux plus bas niveaux d' énergie d'un atome ; en fait ces niveaux peuvent être démultipli és par des phénomènes parasites plus ou moins difficilement contr ôlables, comme les vibrations de l'atome, les fluctuations des champs externes - par exemple ceux du laser qui induit les transitions - etc ...Le sysème quantique réel est plus complexe qu'un simple système à deux niveaux : on peut le modéliser comme un système à deux niveaux décrit par l'état $|q\rangle = |0\rangle$ ou $|1\rangle$ couplé au "reste" des autres degrés de liberté, l'environnement, dont les é tats sont décrits par $|E\rangle$.

$$\text{système quantique complet} \quad \rightarrow |q\rangle\,|E\rangle$$

L'état de l'environnement est susceptible d'évoluer avec le temps selon des paramètres non (ou peu) contrôlables et qui dépendent de l'état du qubit $|q\rangle$. L'évolution du syst ème total se fait donc selon un opérateur unitaire $U(t)$ global de la façon suivante

$$\begin{aligned} \text{Etat initial} \quad &: \qquad |0\rangle\,|E\rangle \overset{U(t)}{\rightarrow} a_1\,|0\rangle\,|E_1(t)\rangle + a_2\,|1\rangle\,|E_2(t)\rangle \\ \text{Etat initial} \quad &: \qquad |1\rangle\,|E\rangle \overset{U(t)}{\rightarrow} a_3\,|0\rangle\,|E_3(t)\rangle + a_4\,|1\rangle\,|E_4(t)\rangle \end{aligned}$$

Supposons maintenant que l'état initial du qubit soit une superposition :

$$\text{Etat initial} \quad : \quad [\alpha\,|0\rangle + \beta\,|1\rangle]\,|E\rangle \overset{U(t)}{\rightarrow} \alpha\,[a_1\,|0\rangle\,|E_1(t)\rangle + a_2\,|1\rangle\,|E_2(t)\rangle] + \beta\,[a_3\,|0\rangle\,|E_3(t)\rangle + a_4\,|1\rangle\,|E_4(t)\rangle]$$

L'état résultant est intriqué entre le qubit et l'environnement. Il peut être ré-écrit :

$$\begin{aligned}\text{Etat final} \quad : \quad & \frac{1}{2}\left[\alpha\left|0\right\rangle + \beta\left|1\right\rangle\right]\left[a_1\left|E_1(t)\right\rangle + a_3\left|E_3(t)\right\rangle\right] \\ + \quad & \frac{1}{2}\left[\alpha\left|0\right\rangle - \beta\left|1\right\rangle\right]\left[a_1\left|E_1(t)\right\rangle - a_3\left|E_3(t)\right\rangle\right] \\ + \quad & \frac{1}{2}\left[\alpha\left|1\right\rangle - \beta\left|0\right\rangle\right]\left[a_2\left|E_2(t)\right\rangle - a_4\left|E_4(t)\right\rangle\right] \\ + \quad & \frac{1}{2}\left[\alpha\left|1\right\rangle + \beta\left|0\right\rangle\right]\left[a_2\left|E_2(t)\right\rangle + a_4\left|E_4(t)\right\rangle\right]\end{aligned}$$

Si on note $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ on voit que le couplage avec l'environnement fait apparaître un mélange de l'état initial du qubit $\left|\psi\right\rangle$ et des états "erronés" $X\left|\psi\right\rangle$, $Z\left|\psi\right\rangle$, et $XZ\left|\psi\right\rangle$.

$$\left|\psi\right\rangle\left|E\right\rangle \rightarrow \left|e_0\right\rangle\left|\psi\right\rangle + \left|e_1\right\rangle X\left|\psi\right\rangle + \left|e_2\right\rangle Y\left|\psi\right\rangle + \left|e_3\right\rangle Z\left|\psi\right\rangle \tag{6.1}$$

Nous verrons dans les paragraphes suivants comment détecter et ré parer ces erreurs.

De plus la phase relative entre les états $\left|0\right\rangle$ et $\left|1\right\rangle$ de l'état initial du qubit est perdue puisque l'état final fait apparaitre une superposition de plusieurs é tats de phase différente ; c'est la *décohérence* (on peut quantifier cet effet en mesurant l'opérateur d'état du système).

A ce processus de décohérence est associé un temps caracté ristique de mise en oeuvre qui dépend du système physique et qui limite donc son temps de fonctionnement. Celui-ci varie de la microseconde (quantum dots) à la seconde (ions piégés) mais doit être mis en regard du temps élémentaire de calcul de ces systèmes (nanoseconde pour les QD, 10^{-14}s pour les ions piégés). Né anmoins même si ces temps laissent la place pour beaucoup d'opé rations, nous avons vu ci-dessus qu'un des effets de la décohérence est d'induire des erreurs. Il est donc crucial en calcul quantique, plus encore qu'en calcul classique de mettre en oeuvre les codes de correction d'erreur.

6.2 Codes de correction d'erreurs quantiques

6.2.1 Code classique à trois bits

Dans un circuit logique les fils de transmission et les portes logiques sont susceptibles d'engendrer des erreurs sur les données. Ces erreurs se manifestent par l'inversion de la valeur d'un bit : $0 \overset{erreur}{\rightarrow} 1$, et $1 \overset{erreur}{\rightarrow} 0$ avec une certaine probabilité p. Il existe de nombreuses méthodes pour s'en pré munir, qui consistent à rajouter de l'information redondante (*codage*) permettant de tester si le message codé a été perturbé et, le cas échéant, de corriger les erreurs. Parmi ces codes, le plus simple (de loin pas le plus performant) est le codage à trois bits. Il consiste à tripliquer chaque bit d'information : $0 \rightarrow 000$, $1 \rightarrow 111$. On suppose que la probabilité d'erreur (de flip d'un bit) est suffisament faible pour que la probabilité que deux erreurs surviennent simultanément est négligeable. Donc après avoir traversé un canal susceptible de créer une erreur le triplet de bits peut se retrouver avec au plus un bit inversé. La détection de l'erreur se fait en testant si tous les bits sont égaux ou non ; si non on utilise la règle de la majorité pour rétablir la bonne valeur logique associée au triplet. C'est ce qu'on appelle le *d écodage*. Alternativement si le bit codé doit traverser d'autres canaux erronés on peut ne pas le décoder mais le restaurer en effectuant une correction d'erreur. Par exemple si un des trois bits (b_1, b_2, b_3) du bit codé a été flippé, on peut savoir lequel (exercice) en effectuant $XOR(\ b_1, b_2)$ et $XOR(\ b_1, b_3)$ et effectuer la correction.

Ce genre de codage ne supprime pas totalement le risque d'erreur ; celui-ci reste lié à la probabilité de flipper plus qu'un bit qui est de $3p^2(1-p)$ (deux bit-flips) $+p^3$ (trois bit-flips) $= 3p^2 - 2p^3$ qui est plus petite que p - la probabilité d'un bit flip - si celle ci est $< \frac{1}{2}$.

6.2.2 Code de correction d'erreurs quantiques

La transposition au cas quantique de ce code simple n'est pas immédiate pour plusieurs raisons :
— la triplication d'un qubit est interdite par le théorème de non clonage ;
— la perturbation apportée à un qubit est plus complexe que le simple bit-flip, qui correspond à l'action de l'opérateur X, puisque d'après l'équation (6.1) il peut aussi y avoir des erreurs de type Y ou de type Z (phase-flip) ;
— la correction d'erreur semble nécessiter une mesure du qubit cod é ce qui va en modifier la valeur.
On peut néanmoins passer outre ces difficultés [1].

La première peut être évitée en utilisant un codage sur n bits qui ne nécessite pas de dupliquer l'état $|\psi\rangle$. En fait on associe à l'état $|\psi\rangle$ un *mot codé* à n bits

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \rightarrow |\psi\rangle_C = \alpha\,|00\cdots0\rangle + \beta\,|11\cdots1\rangle$$

Le nombre n minimal de qubits nécessaires au codage doit être tel que les états perturbés doivent être tous différents (donc orthogonaux) pour pouvoir ensuite être identifiés et corrigés. Par exemple pour $n = 2$ les deux mots codés de base sont $|00\rangle$ et $|11\rangle$. L'action de l'opé rateur X donne

$$\begin{aligned} |00\rangle &\rightarrow |10\rangle \text{ et } |01\rangle \\ |11\rangle &\rightarrow |01\rangle \text{ et } |10\rangle \end{aligned}$$

qui sont les mêmes états. Le codage ne permet pas dans ce cas de distinguer les états perturbés et donc est inopérant.

Supposons que la seule erreur possible soit de type X, équivalent au bit-flip classique. Celui-ci peut agir sur n'importe lequel des qubits des deux mots codés de base,$|00\cdots0\rangle$ et $|11\cdots1\rangle$, engendrant ainsi $2n$ états perturb és plus 2 états non perturbés, soient $2\,(n+1)$ é tats qui doivent tous être différents. Le nombre d'états orthogonaux engendrés par un mot à n qubits est 2^n. On doit donc avoir

$$2^n \geq 2\,(n+1)$$

La plus petite valeur de n qui satisfait cette inégalité est $n = 3$. Le code à 3 qubits est donc le code minimal pour réparer les erreurs de type X [2]. Ce code sera étudié au prochain paragraphe.

Si maintenant on prend en compte les trois types d'erreur, X, Y, Z, toujours en supposant qu'un même qubit ne peut pas subir deux erreurs successives, le nombre d'états perturbés est $2 \times 3n$ auxquels s'ajoutent les deux états non perturbés et l'inégalité pr écédente devient

$$2^n \geq 2\,(3n+1)$$

La valeur minimale de n compatible avec cette inégalité est maintenant $n = 5$. Le code minimal *quantique* pour réparer tous les types d'erreurs est donc le code à 5 qubits qui sera étudié plus loin.

Pour répondre à la denière difficulté mise en avant dans le d ébut du paragraphe, notons que même dans les protocoles classiques, le décodage - qui correspondrait à la mesure dans le protocole quantique et qui détruirait l'état du qubit - n'est pas né cessaire pour réparer l'erreur. Il faudra donc mettre en oeuvre dans le protocole quantique l'équivalent du mécanisme classique de dé tection-correction décrit dans le paragraphe précédent.

1. Nous supposerons que la probabilité qu'une erreur survienne est suffisament faible pour négliger l'occurence des doubles erreurs

2. On retrouve les 3 bits nécessaires à la mise en oeuvre de la rè gle classique de la majorité.

6.3 Codes de correction d'erreurs à 3 qubits

En premier lieu nous effectuons le *codage* en rajoutant des qubits redondants

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \rightarrow |\psi\rangle\,|00\rangle = \alpha\,|0\rangle\,|00\rangle + \beta\,|1\rangle\,|00\rangle \stackrel{codage}{\rightarrow} |\psi\rangle_C = \alpha\,|000\rangle + \beta\,|111\rangle$$

Le *qubit* $|\psi\rangle$ est remplacé par le *mot codé* $|\psi\rangle_C$. Le circuit qui réalise le codage est le suivant `Figure ici, KZUIW100.wmf`
Supposons maintenant que le seul type d'erreur qui affecte le qubit $|\psi\rangle_C$ soit un bit-flip (réalisée par l'action de l'opérateur X) ; il y a trois possibilités

$$\begin{aligned} X_1\left[\alpha\,|000\rangle + \beta\,|111\rangle\right] &= \alpha\,|100\rangle + \beta\,|011\rangle \\ X_2\left[\alpha\,|000\rangle + \beta\,|111\rangle\right] &= \alpha\,|010\rangle + \beta\,|101\rangle \\ X_3\left[\alpha\,|000\rangle + \beta\,|111\rangle\right] &= \alpha\,|001\rangle + \beta\,|110\rangle \end{aligned}$$

où la notation X_i signifie "action de l'opérateur X sur le $i^{ème}$ bit".

La détection de l'erreur se fait par une méthode inspirée de la m éthode classique décrite au paragraphe précédent et né cessitant que deux qubits auxiliaires. Le shéma apparaît ci-dessous :

`Figure ici, JFVHTO00.wmf`

Vérifier (exercice) que le nombre binaire yx est le numéro du qubit erroné. La correction d'erreur consiste donc simplement à redresser le bit en question. Concrétement cela peut être réalisé en mesurant les bits auxiliaires pour obtenir les valeurs de x et de y, puis de faire agir un opérateur X sur le qubit erroné. Remarquons qu'à aucun moment nous n'avons besoin de connaître l'état pour le corriger.

Une autre façon de procéder dont l'avantage est qu'elle peut être généralisable à la correction d'autres types d'erreurs est la suivante :

- on définit des opérateurs de *syndrome* qui ont la particularité d'avoir comme états propres les états erronés ainsi que l'état non perturbé.
- on *mesure* ces opérateurs ; les états, erronés ou non, ne sont pas modifiés puisqu'ils sont états propres et le ré sultat de la mesure (les valeurs propres) signent la position de l'erreur. Il suffit alors d'apporter la correction.

Dans le cas du codage à trois qubits ces opérateurs de syndrome sont : $S_1 = Z_1Z_2$ et $S_2 = Z_2Z_3$; on vérifie que les états perturbés et l'état non perturbé sont états propres de ces deux opérateurs. De plus le couple de valeurs propres signe sans ambiguité la position de l'erreur. Le tableau ci-dessous indique les valeurs propres du couple (S_1, S_2) pour chacun des états

$$\begin{aligned} |\psi_0\rangle = |\psi\rangle = \alpha\,|000\rangle + \beta\,|111\rangle &\rightarrow (+1,+1) \\ |\psi_1\rangle = X_1\,|\psi\rangle = \alpha\,|100\rangle + \beta\,|011\rangle &\rightarrow (-1,+1) \\ |\psi_2\rangle = X_2\,|\psi\rangle = \alpha\,|010\rangle + \beta\,|101\rangle &\rightarrow (-1,-1) \\ |\psi_3\rangle = X_3\,|\psi\rangle = \alpha\,|001\rangle + \beta\,|110\rangle &\rightarrow (+1,-1) \end{aligned}$$

La mesure du syndrome peut être mise en oeuvre dans le cicuit ci-dessous qui fait apparaître deux qubits auxiliaires associés à chacun des opérateurs de syndrome.

`Figure ici, KZVXL500.wmf`

La mesure des opérateurs de syndrome s'effectue sur le qubit auxiliaire qui leur est associé. Le résultat de la mesure permet alors la correction d'erreur. Nous allons analyser ce circuit et en extraire une généralisation.

Désignons par $|\psi_k\rangle$ l'état erroné ($k = 1, 2, 3$) ou non ($k = 0$) qui entre dans le cicuit sur le registre du haut. L'action contrôlée du premier syndrome donne

$$\begin{aligned}(I \otimes H)\,[C\text{-}S_1]\,(I \otimes H)\,|\psi_k\rangle\,|0\rangle &= \frac{1}{\sqrt{2}}\,(I \otimes H)\,[C\text{-}S_1]\,|\psi_k\rangle\,(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2}}\,(I \otimes H)\,(|\psi_k\rangle\,|0\rangle + S_1\,|\psi_k\rangle\,|1\rangle) \\ &= \frac{1}{2}\,[|\psi_k\rangle\,(|0\rangle + |1\rangle) + S_1\,|\psi_k\rangle\,(|0\rangle + |1\rangle)] \\ &= \frac{1}{2}\,(1 + S_1)\,|\psi_k\rangle\,|0\rangle + \frac{1}{2}\,(1 - S_1)\,|\psi_k\rangle\,|1\rangle\end{aligned}$$

Selon la valeur propre de S_1 associée à $|\psi_k\rangle$ l'état du qubit auxiliaire sera projeté vers $|0\rangle$, pour $k = 0$ et 3 ou vers $|1\rangle$ pour $k = 1$ et 2. On recommence avec le syndrome S_2 contrôlé par le deuxième qubit auxiliaire. Finalement la mesure des deux qubits auxiliaires $|x\rangle$ et $|y\rangle$ donnera

x	y	k
0	0	0
0	1	3
1	0	1
1	1	2

On vérifie que quelque soit la valeur de k la correction est apportée sur chaque qubit par l'application de l'opérateur

$X^{x\overline{y}}$ sur le qubit 1 (fil du haut)
X^{xy} sur le qubit 2 (fil du milieu)
$X^{\overline{x}y}$ sur le qubit 3 (fil du bas)

6.4 Codes de correction d'erreurs à 5 qubits

Essayons d'abstraire la méthode de l'exemple du paragraphe précé dent pour la généraliser.

On définit des mots codés de base à 5 qubits $\left|\overline{0}\right\rangle$ et $\left|\overline{1}\right\rangle$ tels que $|\psi\rangle = \alpha\left|\overline{0}\right\rangle + \beta\left|\overline{1}\right\rangle$ ainsi que les 15 états erronés de la forme

$$X_i\,|\psi\rangle\,,\ Y_i\,|\psi\rangle\,,\ Z_i\,|\psi\rangle\,,\ i = 1...5 \tag{6.2}$$

soient états propres des opérateurs de syndrome, $S_1,\ S_2,\ S_3,\ S_4$ avec valeurs propres ± 1. Il suffit de 4 opérateurs puisqu'on peut former $2^4 = 16$ ensembles distincts de 4 nombres prenant leurs valeurs dans $(-1, +1)$ permettant d'identifier les 16 états erronés ou non. Ces opérateurs sont

$$\begin{aligned}S_1 &= Z_2X_3X_4Z_5 \\ S_2 &= Z_3X_4X_5Z_1 \\ S_3 &= Z_4X_5X_1Z_2 \\ S_4 &= Z_5X_1X_2Z_3\end{aligned}$$

Ils satifont $S_i^2 = 1$, ils commutent entre eux et commutent ou anticommutent avec les opérateurs $X_i,\ Y_i,\ Z_i$. Nous allons construire les mots codés de base par application des projecteurs associ és

$$\begin{aligned}\left|\overline{0}\right\rangle &= \frac{1}{4}\,(1 + S_1)\,(1 + S_2)\,(1 + S_3)\,(1 + S_4)\,|00000\rangle \\ \left|\overline{1}\right\rangle &= \frac{1}{4}\,(1 + S_1)\,(1 + S_2)\,(1 + S_3)\,(1 + S_4)\,|11111\rangle\end{aligned}$$

Ces états sont états propres des syndromes puisque $[S_i, S_j] = 0$ et $S_i\,(1 + S_i) = (1 + S_i)$. Si maintenant on fait agir les opérateurs de syndrome sur les é tats erronés équation (6.2) où $|\psi\rangle = \alpha\,|\overline{0}\rangle + \beta\,|\overline{1}\rangle$

$$S_k X_i\,|\psi\rangle = \pm X_i S_k\,|\psi\rangle = \pm X_i\,|\psi\rangle\,...$$

on vérifie bien que ces états sont états propres avec les v.p. ± 1. Dans le tableau ci-dessous chaque colonne donne la liste de 4 valeurs propres correspondant à un des 16 états, non perturbé (colonne 1) et perturbés (les autres colonnes)

	1	X_1	Y_1	Z_1	X_2	Y_2	Z_2	X_3	Y_3	Z_3	X_4	Y_4	Z_4	X_5	Y_5	Z_5
$S_1 = Z_2X_3X_4Z_5$	+	+	+	+	−	−	+	+	−	−	+	−	−	−	−	+
$S_2 = Z_3X_4X_5Z_1$	+	−	−	+	+	+	+	−	−	+	+	−	−	+	−	−
$S_3 = Z_4X_5X_1Z_2$	+	+	−	−	−	−	+	+	+	+	−	−	+	+	−	−
$S_4 = Z_5X_1X_2Z_3$	+	+	−	−	+	−	−	−	−	+	+	+	+	−	−	+

Il suffit donc de mesurer ces opérateurs dans un circuit analogue à celui que nous avons construit dans le paragraphe précédent mais avec 4 qubits auxiliaires.

6.5 Le code de Shor

Le code à 3 qubit permet de corriger les erreurs bit-flip (type X). Les erreurs de type Z : $Z\,|0\rangle = |0\rangle$ et $Z\,|1\rangle = -\,|1\rangle$ sont appel ées *phase-flip.* Définissons une nouvelle base

$$\begin{aligned} |+\rangle &= H\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle \\ |-\rangle &= H\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle \end{aligned}$$

Alors

$$Z\,|+\rangle = |-\rangle \text{ et } Z\,|-\rangle = |+\rangle$$

l'opérateur Z agit comme un opérateur de bit-flip dans cette base. Pour corriger l'erreur phase flip il suffit donc de tripliquer l'est états $|+\rangle$ et $|-\rangle$. Shor a exploité ce mécanisme pour construire un code à 9 bits - 3 pour corriger le bit-flip $\times$ 3 pour corriger le phase-flip à l'aide des mots codés

$$\begin{aligned} |0\rangle &\rightarrow |0\rangle_C = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \\ &= \frac{1}{2\sqrt{2}}(|000000000\rangle + |000000111\rangle + |000111000\rangle + \cdots) \\ |1\rangle &\rightarrow |1\rangle_C = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) \\ &= \frac{1}{2\sqrt{2}}(|000000000\rangle - |000000111\rangle - |000111000\rangle + |000111111\rangle + \cdots) \end{aligned}$$

Le circuit ci-dessous réalise le codage de Shor.

`Figure ici, L01I6Y00.wmf`

Si un bit flip affecte le mot codé il peut être détecté en faisant agir les syndromes Z_1Z_2 et Z_2Z_3 sur chaque triplet ; les opérateurs de syndrome pour le bit-flip sont donc $B_1 = Z_1Z_2$ et $B_2 = Z_2Z_3$, $B_3 = Z_4Z_5$ et $B_4 = Z_5Z_6$, $B_5 = Z_7Z_8$ et $B_6 = Z_8Z_9$ De même si un phase flip affecte le mot codé

(ce qui changera l'un des signes dans l'expression) les syndromes sont $P_1 = X_1X_2X_3X_4X_5X_6$ et $P_1 = X_4X_5X_6X_7X_8X_9$.

Vérifier que ces opérateurs laissent l'état $|\psi\rangle = \alpha\left|\overline{0}\right\rangle + \beta\left|\overline{1}\right\rangle$ invariant et que les états erronés sont état propre, y compris les états erronés de type $Y_k|\psi\rangle$ ce qui établit que ce code corrige tout type d'erreur.

6.5.1 Calculs tolérants les fautes

Dans un circuit quantique chaque étape est source d'erreur : les "fils" de transmission aussi bien que les portes logiques. Le principe de codage du paragraphe précédent n'exclut pas qu'une erreur s'introduise dans l'opération de décodage. Le principe du calcul tolérant aux fautes (*fault tolerant* en anglais) est de mettre au point des portes logiques qui travaillent directement sur les mots codés et qui ne produisent que des erreurs corrigibles. On peut préciser quantitativement cette phrase de la façon suivante :

Si une porte logique élémentaire (à un ou deux qubits) a une probabilité d'erreur p on dira que la porte associée agissant sur un mot codé est tolérante aux fautes si la probabilité qu'elle induise sur le mot codé une erreur incorrigible (par exemple qui affecte plusieurs qubits) est bornée par cp^2 où c est une constante qui dépend de la porte et qui induit une *condition de seuil* é vidente $cp^2 \leq p \Rightarrow p \leq \frac{1}{c}$.

Prenons un exemple simple dans le cas du code à trois bits et de la porte c-Not :

porte c-Not non codée	code à trois qubits
$\|0\rangle\|0\rangle \overset{cNot}{\rightarrow} \|0\rangle\|0\rangle$	$\|000\rangle\|000\rangle \overset{cNot}{\rightarrow} \|000\rangle\|000\rangle$
$\|0\rangle\|1\rangle \overset{cNot}{\rightarrow} \|0\rangle\|1\rangle$	$\|000\rangle\|111\rangle \overset{cNot}{\rightarrow} \|000\rangle\|111\rangle$
$\|1\rangle\|0\rangle \overset{cNot}{\rightarrow} \|1\rangle\|1\rangle$	$\|111\rangle\|000\rangle \overset{cNot}{\rightarrow} \|111\rangle\|111\rangle$
$\|1\rangle\|1\rangle \overset{cNot}{\rightarrow} \|1\rangle\|0\rangle$	$\|111\rangle\|111\rangle \overset{cNot}{\rightarrow} \|111\rangle\|000\rangle$

`Figure ici, KZW0WA01.wmf`

Exercice : vérifier que les circuits ci-dessus correspondent effectivement à la porte c-Not agissant sur les mots codés à trois qubits sans erreur mais qu'en cas d'erreur sur le premier qubit le premier cicuit (a) est non tolérant aux fautes alors que le second (b) est tolérant aux fautes.

Chapitre 7

Réalisations physiques

7.1 Introduction

Les progrés des nanotechnologies ont largement contribué au rapide développement de l'information quantique [1]. Pour être le support d'un qubit un système quantique doit satisfaire certaines conditions ; la première d'entre elle est d'avoir un système à deux états le plus "pur" possible, c'est-à dire tel que le nombre d'états accessibles soit exactement deux. C'est le cas des systèmes de spin 1/2 qui constitueront donc un terrain de choix. La contrainte paradoxale que doit résoudre le bon système est d'être à la fois peu sensible à l'environnement pour résister à la décohérence mais en même temps de pouvoir rester accessible à la mesure et aux interactions avec les autres qubits pour permettre les opérations quantiques. De façon générale les exigences que doit satisfaire le système quantique sont les suivantes :

- les deux états de base doivent être suffisament stable pour minimiser les transitions spontanées qui engendreraient une erreur bit-flip,
- le temps de décohérence doit être suffisament long en regard du temps moyen d'une opération,
- le système pouvoir facilement être initialisé dans l'état $|0\rangle$,
- le système doit posséder un ensemble universel de portes quantiques qui puissent être controlées efficacement,
- un procédure efficace de mesure de l'état du système (lecture du qubit) doit pouvoir être mise en oeuvre,
- le système doit pouvoir être extrapolable (*scalable*) à un grand nombre de qubits.

Pour l'instant aucun système ne répond complètement à toutes ces exigences, surtout la dernière (scalability). Différentes pistes sont explorées, parmi lesquelles :

- les systèmes optiques : le qubit est soit l'état de polarisation du photon, soit le nombre de photons (0 ou 1) dans une cavité,
- la résonance magnétique nucléaire,
- les ions piégés,
- les systèmes en phase solide : nanocircuits supraconducteurs, puits quantiques,...

7.2 La résonance magnétique nucléaire

Cette technique, sur laquelle est basée l'imagerie par résonance magn étique (IRM), a été l'une des premières utilisée pour le calcul quantique et est toujours détentrice du record (7 qubits). Le qubit est un noyau atomique de spin 1/2 et le registre est constitué des (jusqu'à 7) noyaux atomiques

1. *Quantum Information Processing* (QIP) en anglais, est maintenant le nom couramment adopté.

de spin 1/2 d'une même molécule. Par exemple dans la molécule de trichlorétylène enrichi il y a deux atomes de carbone 13 et un d'hydrogène dont le noyau a spin 1/2. En fait, à la différence des autres systèmes listés ci-dessus, le qubit n'est pas constitué d'un noyau unique mais de l'ensemble des noyaux des molécules en phase liquide qui réagissent comme un *ensemble* statistique ce qui a pour effet de rendre les signaux détectables. Mais on peut raisonner comme si chaque noyau était unique.

L'observable sera donc ici le spin représenté par l'opérateur $\overrightarrow{\sigma} = (\frac{1}{2}X, \frac{1}{2}Y, \frac{1}{2}Z)$; les états propres de Z constitueront les états de la base de calcul $|0\rangle$ et $|1\rangle$. L'évolution d'un qubit se fait en plaçant le système dans un champ magnétique

$$\overrightarrow{B} = B_0 \overrightarrow{e}_z + B_1(\cos\omega t \, \overrightarrow{e}_x - \sin\omega t \, \overrightarrow{e}_y)$$

avec lequel le spin interagit selon l'opérateur hamiltonien

$$\mathcal{H} = -\frac{\hbar}{2}\gamma \overrightarrow{\sigma} \cdot \overrightarrow{B}$$

où γ est une constante mesurable qui dépend de l'atome. La pulsation ω est un paramètre ajustable.

Si on note $\omega_0 = \gamma B_0$ et $\omega_1 = \gamma B_1$ l'op érateur hamiltonien se met sous la forme (exercice)

$$\mathcal{H} = -\frac{\hbar}{2}\begin{pmatrix} \omega_0 & \omega_1 e^{i\omega t} \\ \omega_1 e^{-i\omega t} & -\omega_0 \end{pmatrix}$$

L'évolution d'un système quantique se fait selon l'équation de Shrödinger

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = \mathcal{H}|\psi(t)\rangle$$

qui est équivalente (exercice) à $|\psi(t)\rangle = U(t,0)|\psi(0)\rangle$ avec $U(t,0) = e^{-i\mathcal{H}t/\hbar}$

Si $|\psi(0)\rangle = \alpha|0\rangle + \beta|1\rangle$ alors $|\psi(t)\rangle = \alpha(t)|0\rangle + \beta(t)|1\rangle$ où $\alpha(t)$ et $\beta(t)$ satisfont les équations diffé rentielles (exercice) :

$$\begin{aligned} i\frac{d\alpha(t)}{dt} &= -\frac{\omega_0}{2}\alpha(t) - \frac{\omega_1 e^{i\omega t}}{2}\beta(t) \\ i\frac{d\beta(t)}{dt} &= -\frac{\omega_1 e^{-i\omega t}}{2}\alpha(t) + \frac{\omega_0}{2}\beta(t) \end{aligned}$$

Ces équations se résolvent facilement, par exemple en posant $\alpha(t) = \widetilde{\alpha}(t)e^{i\omega_0 t/2}$ et $\beta(t) = \widetilde{\beta}(t)e^{-i\omega_0 t/2}$. Si on prend comme condition initiale $|\psi(0)\rangle = |0\rangle$ c'est-à-dire $\alpha = 1$ et $\beta = 0$ on obtient

$$|\beta(t)|^2 = P_{0\to 1} = \left(\frac{\omega_1}{\Omega}\right)^2 \sin^2\frac{\Omega t}{2} \quad \text{avec} \quad \Omega = \sqrt{(\omega-\omega_0)^2 + \omega_1^2}$$

Si la fréquence ω du champ $\overrightarrow{B}_1$ est ajust ée à $\omega \simeq \omega_0$ (résonance) alors l'état $|\psi(t)\rangle$ oscillera entre $|0\rangle$ et $|1\rangle$ au cours du temps avec une période $2\pi/\omega_1$. La pulsation ω_0 dépend de l'intensité du champ magnétique statique B_0. Pour une intensit é typique en RMN de 15 Teslas cette fréquence est de l'ordre de 500 MHz, ; c'est le domaine des radio-fréquences (RF). La durée d'application du champ B_1 (du pulse RF) permettra de manipuler l'é tat de spin c'est-à-dire de réaliser des opérations à un qubit.

Une fois la phase d'évolution terminée l'état de spin final induit dans l'échantillon une aimantation qui est mesurée : c'est la phase de lecture.

La réalisation de portes à deux qubits se fait au moyen de l'interaction entre le spin de deux noyaux voisins. Le hamiltonien de cette interaction est de la forme

$$\mathcal{H}_I = JZ_1Z_2$$

où les indices 1 et 2 réfèrent aux noyaux. Le facteur de couplage $J/\hbar$ représente une fréquence de quelques centaines de Hz si bien que ce terme de couplage n'a d'effet qu'en l'absence de champ RF (évolution libre) ou si l'intensité B_1 est faible de telle sorte que $J/\hbar \lesssim \omega_1$; il induit donc un opérateur unitaire d'évolution $U_I = \exp(-\frac{i}{\hbar}tJZ_1Z_2)$. La r éalisation d'une porte C-NOT peut s'obtenir par la séquence d'impulsions associée aux opérateurs suivants (exercice : le vé rifier)

$$M_{CNOT} = e^{i\frac{\pi}{4}} R_z^{(2)}(-\frac{\pi}{2})\, R_x^{(2)}(\frac{\pi}{2}) \exp(-iZ^{(1)}Z^{(2)}\frac{\pi}{4})\, R_y^{(2)}(\frac{\pi}{2})\, R_z^{(1)}(\frac{\pi}{2})$$

L'opérateur d'interaction est ici appliqué pendant un temps $\Delta t = \frac{\pi}{4}\frac{\hbar}{J}$ qui est donc de l'ordre de la milliseconde compte tenu de la valeur de J.

Le temps de décohérence résulte des effets thermodynamiques : l'action des impulsions RF est de modifier la population statistique des états $|0\rangle$ et $|1\rangle$ qui au contraire est ramenée vers l'équilibre thermodynamique au bout d'un temps de relaxation qui est de l'ordre de la seconde.

Cette technique a été implémentée par Chuang *et al* sur une molécule de fluorine qui comporte 7 atomes dont le noyau est de spin 1/2 (5 de fluor et 2 de carbone réalisant les 7 qubits) et a permis la mise en oeuvre de l'algorithme de Shor pour factoriser le nombre 15 ce qui est un véritable tour de force expérimental.

Le principal inconvénient est la préparation de l'état initial du système qui doit en principe être un état pur de la forme $|000..0\rangle$. Ici le système est en fait un ensemble de molécules indépendantes et la probabilité (à temp érature non nulle) qu'elle soient toutes dans le même état $|000..0\rangle$ varie comme $1/2^n$ où n est le nombre de qubits dans la molécule. En conséquence deux de nos crit ères sont irrémédiablement perdus : la préparation du syst ème et la "scalability", ce qui fait qu'en dépit de ses succés cette méthode n'a pas vraiment d'avenir.

7.3 Les ions piégés

`Figure ici, KEJL1308.bmp`
Dans l'expérience de Schmidt-Kaler *et al* (*Nature* **422** (2003), p 408) on aligne 8 ions de $^{40}Ca^+$ dans un piège de Paul (potentiel quadrupolaire électrique). Les ions centraux sont distants de 5.3 μm et peuvent être éclairés individuellement par un laser dont la tâche focale est de 2.5 μm. Chaque ion peut se trouver dans un des deux états internes $|g\rangle$ ou $|e\rangle$ séparés par une énergie $\hbar\omega_0$ (avec $\omega_0 = 3 \times 10^{15}\ rad/s$) correspondant à une longueur d'onde de $\lambda = 729\ nm$.

Le piège de Paul peut être assimilé pour chaque ion à un potentiel harmonique dans lequel il va vibrer. Le mouvement d'un ion influence celui de ses voisins si bien que les vibrations de la chaîne d'ions sont corrélées en modes collectifs qui sont quantifiés et désignés par $|n\rangle$. Les deux états de plus basse énergie, $|n = 0\rangle$ et $|n = 1\rangle$ correspondent respectivement au mouvement de translation du centre de masse de l'ensemble des ions et au mouvement en accordéon (dit de "respiration").

L'énergie $\hbar\omega_z$ entre les deux niveaux correspond à une fréquence (pulsation) $\omega_z \simeq 10\ MHz$ et donc à une température $T = \frac{\hbar\omega_z}{k_B} \simeq 0.1\ mK$ à laquelle le dispositif devra être refroidi par des techniques sophistiquées.

L'état quantique de chaque ion est donc caractérisé par son é tat interne et par l'état collectif de vibration $|\alpha, n\rangle$ où $\alpha = g$ ou e et où $n = 0$ ou 1.

`Figure ici, KEJFXV03.wmf`

A chacun de ces états on peut associer des états à 2 qubits :

$$\begin{aligned} |g, n=0\rangle &\rightarrow \quad |00\rangle \\ |g, n=1\rangle &\rightarrow \quad |01\rangle \\ |e, n=0\rangle &\rightarrow \quad |10\rangle \\ |e, n=1\rangle &\rightarrow \quad |11\rangle \end{aligned}$$

On peut réaliser des portes logiques qui permettent de passer d'un de ces états à un autre en éclairant l'ion par une impulsion laser de longueur d'onde et de durée appropriées.

`Figure ici, KEJRKM0B.wmf`

Impulsion de résonance	ω_0 ou	$\|00\rangle \longleftrightarrow \|10\rangle$ $\|01\rangle \longleftrightarrow \|11\rangle$
Impulsion rouge	$\omega_0 - \omega_z$	$\|01\rangle \longleftrightarrow \|10\rangle$
Impulsion bleue	$\omega_0 + \omega_z$	$\|00\rangle \longleftrightarrow \|11\rangle$

On voit que l'impulsion rouge réalise l'opération d'échange (SWAP) des deux états, interne et vibration : $|01\rangle \longleftrightarrow |10\rangle$.

La porte logique cZ est définie par

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

et peut être implémentée au moyen d'un niveau interne auxiliaire noté $|a\rangle = |2\rangle$ dont l'é nergie se situe entre celle des deux états $|g\rangle = |0\rangle$ et $|e\rangle = |1\rangle$.

`Figure ici, KEURPS00.wmf`

Soit $\hbar\omega_a$ l'écart d'énergie entre $|2\rangle$ et $|1\rangle$. Si on éclaire l'ion avec un laser de fréquence $\omega_a + \omega_z$, seule la transition $|20\rangle \longleftrightarrow |11\rangle$ va être excitée. Donc si l'ion se trouve initialement dans l'un des états $|00\rangle$, $|01\rangle$, $|10\rangle$ rien ne sepassera. Si en revanche il se trouve dans l'état $|11\rangle$ et que la durée de l'impulsion est 2π l'ion se rerouvera dans l'état $-|11\rangle$. On aura ainsi réalisé l'action de la porte cZ.

Nous allons maintenant construire la porte cNOT selon la procédure dé finie par Cirac et Zoller [2].-Les qubits concernés sont les états internes de deux ions adjacents, les états de vibration

2. Phys. Rev. Lett. **74**, 4091 (1995) et "New frontiers in quatum information with atoms and ions", *Physics Today*, **57**, 38 (2004).

n'intervenant que pour le couplage entre les ions. Préparons deux ions voisins dans un état (interne) arbitraire

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

l'état collectif de vibration étant le mode $|0\rangle$. L'état initial global du système des deux ions est donc

$$\begin{aligned} |\psi_T\rangle &= \{\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle\} \otimes |0\rangle \\ &= \alpha\,|00,0\rangle + \beta\,|01,0\rangle + \gamma\,|10,0\rangle + \delta\,|11,0\rangle \end{aligned}$$

Nous allons effectuer la succession d'opérations qui couplent état interne et état de vibration d'un ion (l'indice indique l'ion sur lequel agit l'opérateur)

$$\begin{aligned} SWAP_2 \text{ (impulsion rouge sur l'ion 2)} &\rightarrow \alpha\,|00,0\rangle + \beta\,|00,1\rangle + \gamma\,|10,0\rangle + \delta\,|10,1\rangle \\ cZ_1 \text{ (impulsion auxilliaire sur l'ion 1)} &\rightarrow \alpha\,|00,0\rangle + \beta\,|00,1\rangle + \gamma\,|10,0\rangle - \delta\,|10,1\rangle \\ SWAP_2 \text{ (impulsion rouge sur l'ion 2)} &\rightarrow \alpha\,|00,0\rangle + \beta\,|01,0\rangle + \gamma\,|10,0\rangle - \delta\,|11,0\rangle \end{aligned}$$

Au bilan nous avons réalisé une porte cZ entre les deux qubits (états internes des deux ions). Pour passer au $cNOT$ on utilise l'identité (exercice)

`Figure ici, KEUUA301.wmf`

La porte de Hadamard est obtenue par une impulsion $\frac{\pi}{2}$ à la fréquence ω_0.

La dernière étape est la lecture du résultat. Elle se fait à l'aide d'un autre niveau auxilliaire appelé "niveau étagère" (shelving level) noté $|r\rangle$: on éclaire l'ion avec une impulsion laser dont la longueur d'onde est accordée sur la différence d'énergie entre les niveaux $|g\rangle$ et $|r\rangle$. Si l'ion se trouve dans l'état $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha\,|g\rangle + \beta\,|e\rangle$ l'interaction avec le laser va le projeter vers l'état $|g\rangle$ avec probabilité $|\alpha|^2$ ou vers $|e\rangle$ avec probabilité $|\beta|^2 = 1 - |\alpha|^2$. Dans le premier cas l'ion va transiter vers l'état $|r\rangle$ et redescendre dans le fondamental en emettant un photon de fluorescence. En éclairant suffisament longtemps, le cycle $|g\rangle \longleftrightarrow |r\rangle$ va se répéter de nombreuses fois et la fluorescence est observable (à l'oeil nu). Si l'ion est projeté dans l'état $|e\rangle$ alors il n'y a pas de transition vers l'état étagère et pas de fluorescence. En répétant l'expérience un grand nombre de fois (une centaine en pratique) on peut avoir une estimation de $|\alpha|^2$.

La situation actuelle et les perspectives : Deux équipes, une autichienne à Innsbruck (Rainer Blatt) et une américaine au NIST dans le Colorado (Denis Wineland) tiennent le haut du pavé. Ces é quipes ont réussi à créer des états intriqués à 8 qubits. Actuellement le développement des ions piégés sur circuit conduit à des dispositifs très petit (qques cm) pouvant pi éger jusqu'à 12 ions. Cette technique semble prometteuse mais souffre d'inconvénients comme par exemple le chauffage des ions par des champs parasites qui augmente quand le volume dévolu à chaque ion diminue c'est à dire quand la taille totale du piège diminue et/ou quand le nombre d'ions dans le piège augmente.

7.3.1 Qubits en phase solide

7.4 EXERCICES

Exercice 32 *Evolution d'un qubit en RMN*

La plupart des particules portent un moment magnétique lié à une grandeur intrinsèque d'origine purement quantique appelée *spin* . Le moment magnétique quantique est un opérateur agissant dans un espace des états à deux dimensions et s'exprime (dans la repré sentation matricielle)

$$\overrightarrow{\mu} = \frac{\hbar}{2}\gamma\overrightarrow{\sigma}$$

où $\overrightarrow{\sigma} = (X, Y, Z)$ représente le triplet des matrices de Pauli.

Si la particule porteur du moment magnétique est plongée dans un champ magnétique $\overrightarrow{B}$ elle ressentira une énergie potentielle

$$\mathcal{H} = -\overrightarrow{\mu} \cdot \overrightarrow{B}$$

qui pourra faire évoluer son état selon l'opérateur d'é volution $U(t, t_0)$ solution de

$$i\frac{d}{dt}U(t, t_0) = \mathcal{H}U(t, t_0)$$

En Résonance Magnétique Nucléaire (RMN) le champ magnétique $\overrightarrow{B}$ est la superposition d'un fort champ statique le long de la direction z et d'un champ transverse oscillant à la fré quence ajustable ω.

$$\overrightarrow{B} = B_0\widehat{e}_z + B_1\left[\widehat{e}_x\cos(\omega t) + \widehat{e}_y\sin(\omega t)\right]$$

1. Donner l'expression matricielle du hamiltonien $\mathcal{H}$ avec les notations : $\omega_0 = \gamma B_0 \quad ; \quad \omega_1 = \gamma B_1$
2. Le système est intialement dans l'état $|\psi(0)\rangle = |0\rangle$. On suppose qu'à l'instant t il est dans l'état

$$\begin{aligned} |\psi(t)\rangle &= U(t,0)\,|\psi(0)\rangle \\ &= \alpha(t)\,|0\rangle + \beta(t)\,|1\rangle \end{aligned}$$

où $\alpha(t)$ et $\beta(t)$ sont des fonctions inconnués du temps que l'on va déterminer.

(a) A partir de l'équation de Schrödinger

$$i\frac{d}{dt}\,|\psi(t)\rangle = \mathcal{H}\,|\psi(t)\rangle$$

obtenir les équations différentielles couplées que satisfont $\alpha(t)$ et $\beta(t)$.

(b) On pose $\alpha(t) = \widehat{\alpha}(t)e^{i\omega_0 t}$ et $\beta(t) = \widehat{\beta}(t)e^{-i\omega_0 t}$; on se place *à la r ésonance* : $\omega = \omega_0$. Trouver la solution des équations.

(c) En déduire que

$$|\psi(t)\rangle = \cos\left(\frac{\omega_1 t}{2}\right)|0\rangle + i\sin\left(\frac{\omega_1 t}{2}\right)e^{i\omega_0 t}\,|1\rangle$$

à une phase globale près.

Exercice 33 *cNOT en RMN*

1. Rappeler l'action des portes $R_x(\theta)$, $R_y(\theta)$, $R_z(\theta)$ sur les états de base $|0\rangle, |1\rangle$.
2. Quelle est l'action de $U = \exp(-iZ^{(1)}Z^{(2)}\frac{\theta}{2})$ sur les états de base à 2 qubits $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ (dans l'exponentielle l'opérateur $Z^{(1)}$ agit sur le qubit 1 et $Z^{(2)}$ sur le qubit 2) ?
3. Montrer que

$$U_{cNOT} = e^{i\frac{\pi}{4}}R_z^{(2)}(-\frac{\pi}{2})\,R_x^{(2)}(\frac{\pi}{2})\exp(-iZ^{(1)}Z^{(2)}\frac{\pi}{4})\,R_y^{(2)}(\frac{\pi}{2})\,R_z^{(1)}(\frac{\pi}{2})$$

où l'exposant $^{(k)}$ $k = 1, 2$ indique le qubit sur lequel agit l'opérateur.

Exercice 34 *cNOT vs cZ*

Montrer que $cNOT = H^{(2)}\ cZ\ H^{(2)}$ où $H^{(2)}$ désigne la porte de Hadamard agissant sur le second qubit.

Exercice 35 *Algorithme de Deutsch avec des ions piègés*

L'algorithme de Deutsch permet d'identifier si une fonction $f : \{0,1\} \to \{0,1\}$ est *équilibrée* ou *constante* en une seule évaluation de la fonction. (voir § 3.2). On va implémenter cet algorithme à l'aide de la technique des ions piég és (Gulde S. *et al, Nature* **421**, 48 (2003)).

1. On note $f_0,\ f_1,\ f_2,\ f_3$ les quatre fonctions de $\{0,1\} \to \{0,1\}$ définies dans l'exercice 15. Expliciter pour chaque fonction la *porte logique* qui réalise l'opération unitaire $|x,y\rangle \to |x,y+f(x)\rangle$. On pourra utiliser les portes NOT, $cNOT$ et $\overline{c}NOT$ qui est l'analogue de la porte $cNOT$ mais où le bit cible bascule si le bit de contrôle vaut 0 au lieu de 1.

Chapitre 8

Bibliographie

Ouvrages destinés au grand public ("vulgarisation scientifique") : [Sca06, Bit08, Ell12]
Ouvrages d'enseignement de la mécanique quantique :[BD11]
Sources d'inspiration du cours :[Wat06, Bel05, KSV02, Asp02]
Autres ouvrages :[BCS04, Gru99, Mer07, NC03, Pre]

Bibliographie

[Asp02] A. Aspect. Bell's theorem : the naive view of an experimentalist. *Quantum [Un]speakables-From Bell to Quantum information*, 2002. Conference in memory of John Bell, Vienne, December 2000.

[BCS04] G. Benenti, G. Casati, and G. Strini. *Principles of quantum computation and information.* World Scientific, 2004.

[BD11] J.L. Basdevant and J. Dalibard. *Mécanique quantique.* Editions de l'école polytechnique, 2011.

[Bel05] M. Le Bellac. *Introduction à l'information quantique.* Belin, 2005.

[Bit08] M. Bitbol. Mécanique quantique : l'erreur d'Einstein. *La Recherche*, 418 :31–35, 2008.

[Ell12] G. Ellis. Le multivers existe-t-il ? *Pour la science*, Février, no 412 :50–56, 2012.

[Gru99] Jozef Gruska. *Quantum computing.* Advanced Topics in Computer Science Series. McGraw-Hill International (UK) Limited, London, 1999.

[KSV02] A.Yu. Kitaev, A.H. Shen, and M.N. Vyalyi. *Classical and quantum computation.* American Mathematical Society, 2002.

[Mer07] D.N. Mermin. *Quantum computer science.* Cambridge University Press, 2007.

[NC03] M.A. Nielsen and I.L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, 2003.

[Pre] J. Preskill. *Cours en ligne.* Disponible à l'adresse :`http://www.theory.caltech.edu/people/preskill/ph229/`.

[Sca06] V. Scarani. *Initiation à la physique quantique.* Vuibert, 2006.

[Wat06] J. Watrous. *Introduction to Quantum Computing (notes from Winter 2006).* 2006. `https://cs.uwaterloo.ca/~watrous/LectureNotes.html`.

Chapitre 9

Annexes

9.1 Espaces de Hilbert

9.1.1 Espaces pré-Hilbertiens

Soit $\mathcal{H}$ un espace vectoriel sur le corps des nombres complexes $\mathbb{C}$. On appelle "produit scalaire" sur $\mathcal{H}$ toute application de $\mathcal{H} \times \mathcal{H}$ dans $\mathbb{C}$, notée :

$$(u, v) \mapsto (u|v)$$

qui vérifie les propriétés suivantes :
linéarité à droite :pour tous $u, v_1, v_2 \in \mathcal{H}, \lambda_1, \lambda_2 \in \mathbb{C}$

$$(u|\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 (u|v_1) + \lambda_2 (u|v_2) \tag{9.1}$$

anti-linéarité à gauche :pour tous $u_1, u_2, v \in \mathcal{H}, \lambda_1, \lambda_2 \in \mathbb{C}$

$$(\lambda_1 u_1 + \lambda_2 u_2|v) = \overline{\lambda_1}(u_1|v) + \overline{\lambda_2}(u_2|v) \tag{9.2}$$

symétrie hermitienne :pour tous $u, v \in \mathcal{H}$

$$(u|v) = \overline{(v|u)} \tag{9.3}$$

Remarquons que :
(9.1) et (9.3) entrainent (9.2) ; (9.3) entraine que $(u|u)$ est un nombre réel.
positivité :pour tout $u \in \mathcal{H}$

$$(u|u) \geq 0 \tag{9.4}$$

non-dégénérescence :pour tout $u \in \mathcal{H}$

$$\forall v \in \mathcal{H}, (u|v) = 0 \Rightarrow u = 0 \tag{9.5}$$

Cette dernière propriété, sachant que $(*|*)$ est positif, revient à énoncer que

$$\forall u \in \mathcal{H}, (u|u) = 0 \Rightarrow u = 0. \tag{9.6}$$

On appelle *espace pré-hilbertien* tout espace vectoriel $\mathcal{H}$ sur $\mathbb{C}$ muni d'un produit scalaire $(*|*)$ vérifiant les propriétés ci-dessus. Lorsque $\mathcal{H}$ est de dimension finie, il s'agit d'un espace *de Hilbert* (cette notion est en fait plus générale : un espace de Hilbert est, par définition, un espace pré-Hilbertien, qui est complet et qui admet une partie dénombrable dense). On fixe, dans ce qui suit,

un espace de Hilbert de dimension finie $\mathcal{H}$. On rappelle que le dual de $\mathcal{H}$, noté $\mathcal{H}^*$ est l'espace des formes linéaires sur $\mathcal{H}$: $\mathcal{H}^* := \mathcal{L}(\mathcal{H}, \mathbb{C})$.
$\mathcal{H}$ admet au moins une base orthonormée i.e. une famille de vecteurs $e_1, e_2, \ldots, e_n$ qui est une base et telle que

$$\forall i, j \in [1, n], (e_i | e_j) = \delta_i^j$$

où δ_i^j, le symbole de Kronecker signifie 1 si $i = j$ et 0 si $i \neq j$. Fixons une base orthonormée de $\mathcal{H}$. Si les vecteurs u, v ont pour coordonnées respectives $X, Y \in \mathbb{M}_{n,1}(\mathbb{C})$ dans cette base, alors leur produit scalaire vaut

$$(u, v) = X^\dagger \cdot Y.$$

(dans le membre droit, $\cdot$ dénote le produit matriciel). Autrement écrit : si

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_k \\ \vdots \\ x_n \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ \vdots \\ y_k \\ \vdots \\ k_n \end{pmatrix}$$

alors

$$X^\dagger = \begin{pmatrix} \bar{x}_1 & \ldots & \bar{x}_k & \ldots & \bar{x}_n \end{pmatrix}$$

$$(u, v) = \sum_{k=1}^{n} \bar{x}_k \cdot y_k.$$

Considérons une application linéaire $L : \mathcal{H} \to \mathcal{H}$. L'application adjointe, L^* est définie par :

$$\forall u, v \in \mathcal{H}, (u, Lv) = (L^* u, v). \tag{9.7}$$

On vérifie que si M est la matrice de L dans une bases orthonormée $\mathcal{E}$, alors la matrice de L^* dans la même base est $M^\dagger$ définie par

$$M = (m_{i,j})_{i,j \in [1,n]}, \quad M^\dagger := (\bar{m}_{j,i})_{i,j \in [1,n]}.$$

Les propriétés suivantes des applications linéaires sont souvent utilisées en mécanique quantique :
L est *hermitien* ssi

$$\forall u, v \in \mathcal{H}, (u, Lv) = (Lu, v)$$

ce qui revient à $L = L^*$ ou encore au fait que sa matrice M (dans une base orthonormée) vérifie $M = M^\dagger$.
L est *unitaire* ssi

$$\forall u, v \in \mathcal{H}, (Lu, Lv) = (u, v)$$

ce qui revient à $L^* L = \mathrm{Id}_{\mathcal{H}}$, ou encore au fait que sa matrice M (dans une base orthonormée) vérifie $M \cdot M^\dagger = \mathrm{I}_n$.
La propriété de non-dégénérescence du produit scalaire entraine que l'application :

$$G : \mathcal{H} \to \mathcal{H}^*$$

definie par

$$G(u) : v \mapsto (u|v) \tag{9.8}$$

est semi-linéaire et injective (puisque son noyau est réduit à $\{0\}$). Comme $\mathcal{H}$ est de dimension finie, $\mathcal{H}$ et $\mathcal{H}^*$ ont même dimension, ce qui entraîne que G est un isomorphisme anti-linéaire.

9.1.2 Notation de Dirac

Nous introduisons ici une notation pour les objets déjà décrits dans la sous-section 9.1.1. Comme elle fut inventée par Paul Dirac, elle se dénomme "notation de Dirac". Signalons enfin qu'elle est universellement utilisée dans les ouvrages de physique quantique.

Cette notation s'appuie sur la remarque suivante : pour tous vecteurs $u, v \in \mathcal{H}$

$$(u|v) = G(u)(v) \tag{9.9}$$

i.e. le produit scalaire du vecteur u par le vecteur v est égal à la valeur de la forme linéaire $G(u)$ appliquée à l'argument v. Donc si nous introduisons une notation commode pour G, alors la notation $(*|*)$ ne sera plus nécessaire, puisque nous utiliserons le membre droit de (9.9) pour le désigner. En d'autres termes, la donnée d'un e.v. $\mathcal{H}$ sur $\mathbb{C}$ et d'un produit scalaire est équivalente à la donnée d'un e.v. $\mathcal{H}$ sur $\mathbb{C}$ et d'un isomorphisme anti-linéaire $G : \mathcal{H} \to \mathcal{H}^*$.

Décidons de noter

$$|u\rangle, |v\rangle, |w\rangle, |0\rangle, |1\rangle, \dots$$

les vecteurs de $\mathcal{H}$, puis de noter

$$\langle u|, \langle v|, \langle w|, \langle 0|, \langle 1|, \dots$$

leurs images par G.
Autrement dit, nous utilisons maintenant un alphabet *typé* où chaque lettre de la forme $|\dots\rangle$ est un élément de $\mathcal{H}$ et chaque lettre de la forme $\langle \dots|$ est un élément de $\mathcal{H}^*$ et enfin les deux alphabets sont liés par une bijection $|u\rangle \mapsto \langle u|$. [1]

L'équation (9.9) devient alors

$$(u|v) = G(u)(v) = \langle u|\,|v\rangle \tag{9.10}$$

Décidons maintenant de ne retenir qu'une barre verticale dans le membre droit de (9.10), on obtient alors

$$(u|v) = G(u)(v) = \langle u|v\rangle$$

Nous pouvons ainsi oublier $(*|*)$ ainsi que G (on n'oublie pas que ces *notations*, on peut, en principe, oublier les *concepts* eux-mêmes, puiqu'ils sont exprimables à partir des formes et de leur évaluation). Soit $L \in \mathcal{L}(\mathcal{H}, \mathcal{H})$, La notation

$$\langle u|\,L\,|v\rangle \tag{9.11}$$

signifie : la forme $\langle u|$ appliquée à l'argument $L(|v\rangle)$ Mais si nous déplaçons les parenthèses d'un cran vers la gauche, la notation devient

$$(\langle u|\,L)\,|v\rangle$$

qui signifie : la forme $\langle u|\,L$ appliquée à l'argument $|v\rangle$; mmmh, mais qui est cette forme $\langle u|\,L$? Là il faut comprendre qu'il s'agit de $G(L^*\,|u\rangle)$, ce qui, selon la définition (9.7) de l'adjoint, donne un résultat identique à celui du premier parenthésage. Retenons donc que, en notation de Dirac :

$$\langle u|\,L, L^*\,|u\rangle$$

1. Une telle convention d'ecriture est aussi coutumière en théorie des groupes où des symboles x et x^{-1} se correspondent, quelle que soit la nature du symbole x. On peut toutefois écrire $(x^{-1}y)^{-1}$ ou même $(x^{-1})^{-1}$ et cela reste une notation pourvue de sens. Ici $|\langle u|\rangle$ ou $|\lambda\,\langle u| + \mu\,\langle v|\rangle$ ne semblent pas idiomatiques, on préférera $|u\rangle$ ou $\lambda\,|u\rangle + \mu\,|v\rangle$,i.e. les propriétés de la bijection sont inclues dans son usage

sont reliés par la bijection entre les vecteurs et les formes [2] Remarquons enfin que, la traduction sous forme matricielle du produit $\langle u| L |v\rangle$ donne

$$X^\dagger \cdot M \cdot Y$$

que l'on utilise le premier ou le second parenthésage (car la matrice de L^* est $M^\dagger$ ce qui fait que $(M^\dagger X)^\dagger = X^\dagger \cdot M$). Moyennant quoi, l'oubli de parenthèses dans les expressions à trois arguments $\langle u| L |v\rangle$ n'induit pas d'ambiguité (i.e. cette notation ne désigne bien qu'un seul nombre complexe). Une notation de prime abord plus étrange est la suivante :

$$|v\rangle \langle u| \tag{9.12}$$

Quel objet mathématique peut-elle désigner ? un vecteur ? une forme ? un nombre ? Non, rien de tout cela ! elle désigne l'application linéaire :

$$|w\rangle \mapsto |v\rangle \langle u| |w\rangle = |v\rangle (\langle u|w\rangle)$$

L'expression entre parenthèses est un nombre ; on ferme les yeux sur le fait qu'il est situé à droite du vecteur $|v\rangle$ et on estime donc que (9.12) désigne l'application linéaire :

$$|w\rangle \mapsto \langle u|w\rangle |v\rangle$$

N.B. Cette adjonction d'une action à droite des scalaires sur les vecteurs, identique à leur action à gauche, est inoffensive tant que l'espace n'est pas équipé d'une autre action à droite.
Une fois adoptée cette écriture, on peut l'utiliser pour exprimer la décomposition diagonale d'une application linéaire L : si $|u_1\rangle, \ldots, |u_k\rangle, \ldots, |u_n\rangle$ est une base orthonormée de vecteurs propres de L (avec $L |u_k\rangle = \lambda_k |u_k\rangle$) alors

$$L = \sum_{k=1}^{n} \lambda_k |u_k\rangle \langle u_k| \tag{9.13}$$

9.1.3 Produit tensoriel

Cas général Soient E, F deux espaces vectoriels de dimension finie sur un corps commutatif K. Soit $\mathcal{B}$ (resp. $\mathcal{C}$) une base de E (resp. de F). Considérons l'ensemble

$$T := K^{\mathcal{B}\times\mathcal{C}}$$

muni des opérations suivantes :
addition :

$$\varphi + \psi : (b, c) \mapsto \varphi(b, c) + \psi(b, c)$$

produit par un scalaire :

$$k \cdot \varphi : (b, c) \mapsto k \cdot \varphi(b, c)$$

On vérifie que T, muni de ces deux opérations, est un espace vectoriel sur K. Définissons, pour tout $b \in \mathcal{B}$ et tout $c \in \mathcal{C}$, l'élément suivant de T, que nous noterons $b \otimes c$:

$$b \otimes c : (b, c) \mapsto 1, (b', c') \mapsto 0(\text{ pour tout } (b', c') \neq (b, c)$$

2. mais on n'a plus de notation pour le dire ! sauf si on autorise : $\langle u| L = \langle L^* |u\rangle|$.

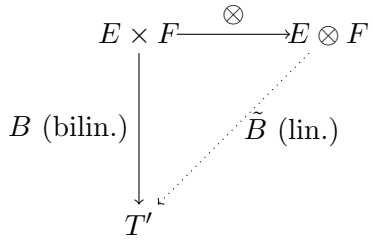


FIGURE 9.1 – La propriété universelle du produit tensoriel.

On vérifie alors que tout élément φ de T s'écrit sous la forme :

$$\varphi = \sum_{b \in \mathcal{B}, c \in \mathcal{C}} \varphi(b,c) \cdot b \otimes c$$

et que, d'autre part, si

$$\varphi = \sum_{b \in \mathcal{B}, c \in \mathcal{C}} k_{b,c} \cdot b \otimes c$$

pour une famille $(k_{b,c})_{(b,c) \in \mathcal{B} \times \mathcal{C}}$, alors

$$\forall b \in \mathcal{B}, \forall c \in \mathcal{C}, k_{b,c} = \varphi(b,c).$$

Donc $\{b \otimes c \mid b \in \mathcal{B}, c \in \mathcal{C}\}$ est une base de T. L'application $(b,c) \mapsto b \otimes c$ peut être étendue, par bilinéarité, à l'espace produit :

$$(\sum_{b \in \mathcal{B}} \lambda_b b) \otimes (\sum_{c \in \mathcal{C}} \mu_c c) := \sum_{b \in \mathcal{B}, c \in \mathcal{C}} \lambda_b \mu_c \cdot (b \otimes c).$$

Cette application bilinéaire $\otimes : E \times F \to T$ est, en quelque sorte, l'application bilinéaire la plus générale que l'on puisse définir depuis $E \times F$ vers n'importe quel autre e.v. sur K. Précisons cette affirmation :

Proposition 9 *Soit B une application bilinéaire de $E \times F$ dans un espace vectoriel T' sur K. Alors, il existe une unique application linéaire $\tilde{B} : T \to T'$ telle que :*

$$B = \tilde{B} \circ \otimes.$$

L'espace T est appelé *produit tensoriel* de E par F. La proposition 9 énonce la *propriété universelle* du produit tensoriel :
- elle est universelle, en ce qu'elle parle de *toutes* les applications bilinéaires
- elle est importante car, en fait elle *caractérise* l'espace T, à isomorphisme près (à démontrer, en guise d'exercice) ; en particulier, cela implique qu'une construction qui partirait de bases $\mathcal{B}', \mathcal{C}'$ différentes, aboutirait certes à un ensemble T' différent de T, mais qui, en tant qu'espace vectoriel, serait isomorphe à l'espace T que nous avons construit, par un isomorphisme compatible avec les applications $\otimes : E \times F \to T$ et $\otimes : E \times F \to T'$.

Cas des espaces de Hilbert Considérons maintenant le cas où E, F sont des espaces de Hilbert de dimension finie.

Produit scalaire

Supposons que $\mathcal{B} = \{b_1, \ldots, b_i, \ldots, b_n\}$ est une base orthonormée de E et $\mathcal{C} = \{c_1, \ldots, c_j, \ldots, c_m\}$ est une base orthonormée de F.

Considérons la forme sesqui-linéaire S (i.e. semi-linéaire à gauche, linéaire à droite) définie sur la base $\{b_i \otimes c_j | i \in [1, n], j \in [1, m]\}$ par

$$S(b_i \otimes c_j, b_k \otimes c_\ell) := (b_i|b_k) \cdot (c_j|c_\ell). \tag{9.14}$$

Elle est (par définition) sesqui-linéaire. La matrice de S, dans la base $\{b_i \otimes c_j | i \in [1, n], j \in [1, m]\}$ est :

$$\mathrm{I}_{nm}.$$

Donc S est "hermitienne, définie-positive". L'espace $E \otimes F$, muni de la forme S, est donc un espace de Hilbert. La forme S sera noté $(*|*)$ (comme dans E et F). On aura donc, par définition de S, puis de cette notation : pour tous $u, u' \in E, v, v' \in F$

$$(u \otimes v | u' \otimes v') = (u|u')(v|v'). \tag{9.15}$$

Produit d'applications linéaires

Soient E, E, F, F' des espaces vectoriels de dimension finie sur un corps commutatif K. Nous définissons ci-dessous , pour toutes applications linéaires

$$\varphi \in \mathcal{L}(E, E'), \psi \in \mathcal{L}(F, F')$$

une application linéaire

$$\varphi \hat{\otimes} \psi \in \mathcal{L}(E \otimes F, E' \otimes F')$$

de la façon suivante : supposons que $\mathcal{B}$ (resp. $\mathcal{C}$) est une base de E (resp. de F). On pose

$$\varphi \hat{\otimes} \psi (\sum_{(b,c) \in \mathcal{B} \times \mathcal{C}} \lambda_{b,c} b \otimes c) := \sum_{(b,c) \in \mathcal{B} \times \mathcal{C}} \lambda_{b,c} \varphi(b) \otimes \psi(c). \tag{9.16}$$

Une définition alternative, ne faisant pas appel à des bases particulières, consiste à utiliser la propriété universelle du produit tensoriel : l'application $(u, v) \mapsto \varphi(u) \otimes \psi(v)$ est une application bilinéaire de $E \times F$ dans $E' \otimes F'$, donc il existe une unique application linéaire

$$\Phi : E \otimes F \to E' \otimes F'$$

qui fait commuter le diagramme 9.1.3 ci-dessous. On définit alors :

$$\varphi \hat{\otimes} \psi := \Phi. \tag{9.17}$$

L'application $\varphi \hat{\otimes} \psi$ ne dépend donc *que* des applications φ, ψ et *ne* dépend *pas* des bases $\mathcal{B}, \mathcal{C}$ invoquées dans la première définition (formule (9.16)). Comme l'application définie par la formule (9.16) fait commuter le diagramme 9.1.3, nous sommes certains que les définitions (9.16) et (9.17) sont équivalentes (pour n'importe quelles bases) [3]. Considérons maintenant l'application :

$$\hat{\otimes} : \mathcal{L}(E, E') \times \mathcal{L}(F, F') \to \mathcal{L}(E \otimes F, E' \otimes F')$$

$$(\varphi, \psi) \mapsto (\varphi \hat{\otimes} \psi)$$

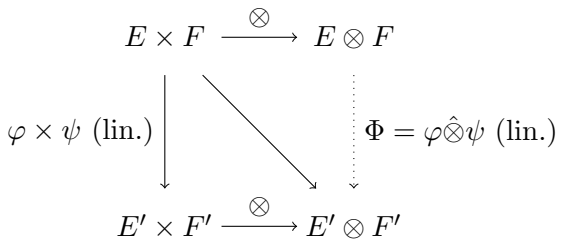


FIGURE 9.2 – Produit tensoriel d'applications linéaires.

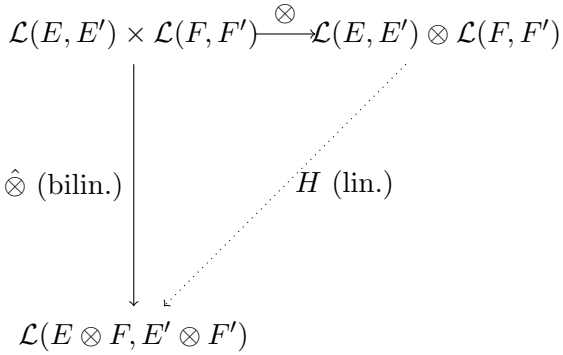


FIGURE 9.3 – L'isomorphisme H.

Cette application est bilinéaire. Par la propriété universelle, il existe une unique application linéaire

$$H : \mathcal{L}(E,E') \otimes \mathcal{L}(F,F') \to \mathcal{L}(E \otimes F, E' \otimes F')$$

faisant commuter le diagramme 9.1.3, i.e. vérifiant que, pour tous $\varphi \in \mathcal{L}(E,E'), \psi \in \mathcal{L}(F,F')$,

$$H(\varphi \otimes \psi) = \varphi \hat{\otimes} \psi.$$

Théorème 10 *L'application H est isomorphisme de $\mathcal{L}(E,E') \otimes \mathcal{L}(F,F')$ dans $\mathcal{L}(E \otimes F, E' \otimes F')$.*

une preuve
Cet isomorphisme entraîne que nous pourrons identifier l'objet $\varphi \otimes \psi$ avec son image par H i.e. $\varphi \hat{\otimes} \psi$ (autrement dit : nous nous autoriserons cet abus de notation).
Le cas particulier de ce théorème où $E' = F' = K$ fournit le

Corollaire 11 *L'application H est isomorphisme de $E^* \otimes F^*$ dans $(E \otimes F)^*$.*

Notation de Dirac
La notation de Diract est fondée sur l'anti-isomorphisme G défini en (9.8). Cet anti-isomorphisme est-il "compatible" avec le produit tensoriel ?
Soient E, F des espaces de Hilbert (de dimension finie). L'équation (9.8) définit 3 anti-isomorphismes :

$$G_E : E \to E^*, \;\; G_F : F \to F^*, \;\; G_{E \otimes F} : E \otimes F \to (E \otimes F)^* \approx_{H^{-1}} E^* \otimes F^*.$$

3. la formule (9.16) peut donc être utilisée sans scrupule

(l'isomorphisme H est donné dans le corollaire 11). Nous utiliserons G en omettant les indices pour alléger les notations. Remarquons aussi que $(K \otimes K) \approx K$ pour l'isomorphisme défini par $(k \otimes k') \mapsto (k \cdot k')$.
Soient $u \in E, v \in F$. Examinons l'effet de $G(u \otimes v)$ sur un argument $u' \otimes v'$ (où $u' \in E, v' \in F$) :

$$\begin{aligned} G(u \otimes v)(u' \otimes v') &= (u \otimes v, u' \otimes v') && \text{def. de } G_{E\otimes F} \\ &= (u, u') \cdot (v, v') && \text{d'après (9.15)} \\ &= G(u)(u') \cdot G(v)(v') && \text{def. de } G_E, G_F \\ &= G(u)(u') \otimes G(v)(v') && \text{produit tensoriel dans } K \\ &= (G(u)\hat{\otimes}G(v))(u' \otimes v') && \text{def. de } \hat{\otimes} \end{aligned}$$

Comme cette égalité est valable pour tout argument $u' \otimes v'$, on a

$$G(u \otimes v) = G(u)\hat{\otimes}G(v))$$

i.e. du point de vue de la notation de Dirac,

$$\text{la forme associée au vecteur } |u\rangle \otimes |v\rangle \text{ est } \langle u| \hat{\otimes} \langle v|$$

ou encore, avec un abus de notation supplémentaire (mais assez naturel)

$$\langle u \otimes v| = \langle u| \hat{\otimes} \langle v|$$

puis, sachant que $\langle u| \hat{\otimes} \langle v|$ et $\langle u| \otimes \langle v|$ se correspondent dans l'isomorphisme H

$$\langle u \otimes v| = \langle u| \otimes \langle v| . \tag{9.18}$$

9.2 Groupes abéliens

Nous rassemblons dans cette section les résultats concernant la structure de l'anneau $(\mathbb{Z}/N\mathbb{Z}, +, \cdot)$ qui sont utiles pour comprendre l'algorithme de Shor (étudié au chapitre 4). On s'intéresse, en particulier, à la probabilité qu'une classe d'entier $x \pmod N$, qui est supposée inversible, possède un ordre pair ω (dans le groupe multiplicatif des classes inversible) et que $x^{\omega/2} \not\equiv -1 \pmod N$.

9.2.1 Généralités sur les groupes abéliens

Soit $(G, \cdot)$ un groupe abélien. Notons 1 son élément neutre. On appelle *ordre* d'un élément $x \in G$ le plus petit entier $n > 0$ tel que

$$x^n = 1$$

On notera $\text{ord}(x)$ l'ordre de x. Cela revient à la caractérisation :

$$\forall m \in \mathbb{N}, x^m = 1 \Leftrightarrow \text{ord}(x)|m.$$

Soit $(G, \cdot)$ un groupe abélien *fini*. L' *exposant* du groupe G est le plus petit entier $e > 0$ tel que

$$\forall x \in G, x^e = 1.$$

Comme pour tout $x \in G$, $x^{|G|} = 1$, l' existence de l'exposant est assurée, et il divise $|G|$. On notera $\exp(G)$ l'exposant de G.

Proposition 12 *Soit $(G,\cdot)$ un groupe abélien. Si* $\mathrm{ord}(x)$ *et* $\mathrm{ord}(y)$ *sont premiers entre eux, alors* $\mathrm{ord}(x\cdot y)=\mathrm{ord}(x)\cdot\mathrm{ord}(y)$,

Preuve. Soient $x,y\in G$. Supposons que $\mathrm{ord}(x)$ et $\mathrm{ord}(y)$ sont premiers entre eux,
Soit $m>0$ tel que $(xy)^m=1$.
Posons $z:=x^m=y^{-m}$. Comme $z^{\mathrm{ord}(x)}=1$, $\mathrm{ord}(z)|\mathrm{ord}(x)$.
De même, $\mathrm{ord}(z)|\mathrm{ord}(y)$.
Mais comme $\mathrm{ord}(x)$ et $\mathrm{ord}(y)$ sont premiers entre eux, cela entraîne que $\mathrm{ord}(z)=1$, i.e. que $z=1$.
Comme $x^m=1$, $\mathrm{ord}(x)|m$ et comme $y^m=1$, $\mathrm{ord}(y)|m$, ce qui entraîne que $\mathrm{ord}(x)\cdot\mathrm{ord}(y)|m$.
Réciproquement, $(xy)^{\mathrm{ord}(x)\cdot\mathrm{ord}(y)}=1$.
On a établi que : $\mathrm{ord}(xy)=\mathrm{ord}(x)\cdot\mathrm{ord}(y)$. ■

Proposition 13 *Soit $(G,\cdot)$ un groupe abélien et $x,y\in G$. Alors il existe un élément $z\in G$ tel que*

$$\mathrm{ord}(z)=\mathrm{ppcm}(\mathrm{ord}(x),\mathrm{ord}(y))$$

Preuve. Soient $x,y\in G$. Supposons que $\mathrm{ord}(x)=\prod_{i\in I}p_i^{\alpha_i}$ et $\mathrm{ord}(y)=\prod_{i\in I}p_i^{\beta_i}$, où les entiers p_i sont premiers et distincts deux à deux.
Soit

$$J:=\{i\in I\mid \alpha_i>\beta_i\}, K:=\{i\in I\mid \alpha_i\leq\beta_i\}$$

Posons

$$r:=\prod_{i\in J}p_i^{\alpha_i},\quad s:=\prod_{i\in K}p_i^{\beta_i}$$

et enfin

$$x':=x^{\mathrm{ord}(x)/r},\quad y':=y^{\mathrm{ord}(y)/s}$$

Alors $\mathrm{ord}(x')=r$ et $\mathrm{ord}(y')=s$. Comme les facteurs premiers de r et s sont disjoints, r et s sont premiers entre eux.
Par la prop. 12, $\mathrm{ord}(x'y')=rs$, mais $rs=\mathrm{ppcm}(\mathrm{ord}(x),\mathrm{ord}(y))$. L'élément $z:=x'y'$ vérifie la propriété annoncée. ■

Proposition 14 *Soit $(G,\cdot)$ un groupe abélien fini. L'exposant de G est le plus grand ordre des éléments de G, pour l'ordre de divisibilité.*

Preuve. 1- Soit $x\in G$. Comme $x^{\exp(G)}=1$, $\mathrm{ord}(x)|\exp(G)$. Donc $\exp(G)$ est un majorant commun, pour la divisibilité, de tous les ordres. Autrement dit, $\mathrm{ppcm}(\{\mathrm{ord}(x)\mid x\in G\})|\exp(G)$.
2- Montrons que $\exp(G)$ est un ordre.
Soient $x_1,\ldots,x_n$ les éléments de G.
En utilisant la prop. 13, on montre par récurrence sur k que :

$$\exists x\in G,\mathrm{ord}(x)=\mathrm{ppcm}(x_1,\ldots,x_k)$$

Donc

$$\exists\hat{x}\in G,\mathrm{ord}(\hat{x})=\mathrm{ppcm}(\{\mathrm{ord}(x)\mid x\in G\}).$$

Comme $\hat{x}^{\exp(G)}=1,\mathrm{ord}(\hat{x})|\exp(G)$. Combiné avec point 1, cela entraine que : $\mathrm{ord}(\hat{x})=\exp(G)$. ■

9.2.2 L' anneau $\mathbb{Z}/N\mathbb{Z}$

La structure de l'anneau $(\mathbb{Z}/N\mathbb{Z}, +, \cdot)$, pour un entier N quelconque, se ramène à la structure des anneaux $\mathbb{Z}/p^\alpha\mathbb{Z}$ avec p premier, via le "théorème chinois", énoncé ci-dessous.

Théorème 15 (Théorème chinois) *Soient n, m deux entiers, non nuls, premiers entre eux. Alors*

$$\mathbb{Z}/(nm)\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Un isomorphisme d'anneaux est donné par :

$$\dot{x} \mapsto (\dot{x} \pmod{n}, \dot{x} \pmod{m}).$$

La preuve repose, essentiellement, sur le théorème de Bezout.

Corollaire 16 (Décomposition de $\mathbb{Z}/N\mathbb{Z}$) *Soit N un entier dont la décomposition en facteurs premiers est*

$$N = \prod_{i=1}^{\ell} p_i^{\alpha_i}$$

(pour tout $i \in [1, \ell]$, p_i premier, $1 \leq \alpha_i$). Alors

$$\mathbb{Z}/N\mathbb{Z} \simeq \prod_{i=1}^{\ell} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}.$$

Pour tout $N \geq 1$, nous notons $\mathrm{U}(\mathbb{Z}/N\mathbb{Z})$ le groupe des unités (i.e. des éléments inversibles) du monoide multiplicatif $(\mathbb{Z}/N\mathbb{Z}, \cdot, 1)$. Le cardinal de $\mathrm{U}(\mathbb{Z}/N\mathbb{Z})$ est exactement le nombre d'entiers $x \in [1, N]$ qui sont premiers avec N, que l'on note classiquement $\varphi(N)$ (φ est l'*indicatrice d'Euler*). On rappelle que φ est faiblement multiplicative i.e. si m, n sont premiers entre eux, alors

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

(cela résulte aisément du théorème chinois).
On en déduit que le *cardinal* du groupe $\mathrm{U}(\mathbb{Z}/N\mathbb{Z})$ est

$$\varphi(N) = N \prod_{i=1}^{\ell} (1 - \frac{1}{p_i}). \tag{9.19}$$

La *structure* du groupe $\mathrm{U}(\mathbb{Z}/N\mathbb{Z})$ est décrite par le théorème chinois combiné avec le

Théorème 17 (Structure des unités de $\mathbb{Z}/N\mathbb{Z}$, pour N primaire)
1- pour $p \geq 3$, p premier, $\alpha \geq 1$,

$$(\mathrm{U}(\mathbb{Z}/p^\alpha\mathbb{Z}), \cdot) \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +) \times (\mathbb{Z}/p^{\alpha-1}\mathbb{Z}, +).$$

2- pour $\alpha \geq 2$,

$$(\mathrm{U}(\mathbb{Z}/2^\alpha\mathbb{Z}), \cdot) \simeq (\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z}, +).$$

Preuve. 1.1- Cas où $p \geq 3, \alpha = 1$ i.e. on s' intéresse à $\mathrm{U}(\mathbb{Z}/p\mathbb{Z})$.
Rappelons que, comme p est premier, $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ est un corps.
Soit e l' exposant du groupe $\mathrm{U}(\mathbb{Z}/p\mathbb{Z})$.
Par définition de l'exposant :

$$\forall x \in \mathrm{U}(\mathbb{Z}/p\mathbb{Z}), x^e = 1$$

donc le polynôme $X^e - 1$ possède $p-1$ racines distinctes. Son degré est donc $\geq p-1$ i.e.

$$e \geq p-1$$

Comme par ailleurs e divise $p-1$, on en conclut que $e = p-1$, et par la prop. 14, il existe un élément $\omega \in \mathrm{U}(\mathbb{Z}/p\mathbb{Z})$ d' ordre $p-1$.
1.2- Cas où $p \geq 3, \alpha \geq 2$.
Montrons que $1 + \dot{p}$ est d'ordre $p^{\alpha-1}$ dans $\mathrm{U}(\mathbb{Z}/p^\alpha\mathbb{Z})$.
Il suffit de montrer par récurrence sur k que

$$(1+p)^{p^k} = 1 + \lambda p^{k+1}$$

avec $\mathrm{pgcd}(\lambda, p) = 1$. (Utiliser le fait que C_p^j est divible par p lorsque $1 \leq j \leq p-1$).
Il existe un élément d'ordre $p-1$ dans $\mathrm{U}(\mathbb{Z}/p^\alpha\mathbb{Z})$:
soit $x \in \mathbb{N}$ tel que sa classe est d'ordre $p-1$ dans $\mathrm{U}(\mathbb{Z}/p\mathbb{Z})$ (voir point 1.1). Notons m l'ordre de la classe de x modulo p^α.
Comme $x^m \equiv 1 \pmod{p^\alpha}$, on a aussi $x^m \equiv 1 \pmod{p}$ donc $p-1 | m$. Donc $\dot{x}^{m/(p-1)}$ est d'ordre $p-1$ dans $\mathrm{U}(\mathbb{Z}/p^\alpha\mathbb{Z})$.
En appliquant la prop. 12, on est sûr que $(1+\dot{p})\cdot \dot{x}^{m/(p-1)}$ est d'ordre $(p-1)p^{\alpha-1}$.
2- Cas où $p = 2, \alpha \geq 2$.
Montrons que l'ordre de la classe de $5 \pmod{p^\alpha}$ est $p^{\alpha-2}$. Il suffit de montrer par récurrence sur k que

$$5^{p^k} = 1 + \lambda 2^{k+2}$$

avec $\mathrm{pgcd}(\lambda, 2) = 1$. L'ordre de la classe de $-1 \pmod{p^\alpha}$ est 2.
On remarque que tout nombre 5^k $(k \geq 0)$ est congru à 1 modulo 4, donc

$$\forall k \geq 0, 5^k \not\equiv -1 \pmod{2^\alpha}.$$

Les deux sous-groupes $\langle \dot{-1} \rangle$ et $\langle \dot{5} \rangle$ de $\mathrm{U}(\mathbb{Z}/2^\alpha\mathbb{Z})$ ont donc une intersection triviale. Leur produit dans $\mathrm{U}(\mathbb{Z}/2^\alpha\mathbb{Z})$ est donc isomorphe à leur produit direct, qui est de cardinal $2^{\alpha-1}$. Donc

$$\mathrm{U}(\mathbb{Z}/2^\alpha\mathbb{Z}) \simeq \langle \dot{-1} \rangle \times \langle \dot{5} \rangle \simeq (\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2^{\alpha-2}\mathbb{Z}, +).$$

■
On remarquera que l'image de la classe de -1 , par l'isomorphisme donné au point (1), est le couple $(\dot{p-1}/2, \dot{0})$: en effet , les deux solutions de l'équation $2x = 0$ dans $(\mathbb{Z}/(p-1)\mathbb{Z}, +) \times (\mathbb{Z}/p^{\alpha-1}\mathbb{Z}, +)$ sont $(\dot{0}, \dot{0})$ et $(\dot{p-1}/2, \dot{0})$.
Nous sommes maintenant à pieds d'oeuvre pour évaluer le cardinal de l'ensemble suivant :

$$F_N := \{v \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \mid \mathrm{ord}(v) \equiv 0 \pmod 2 \wedge v^{\frac{\mathrm{ord}(v)}{2}} \not\equiv -1 \pmod N\}. \tag{9.20}$$

La notation ord(v) désigne l'ordre de v dans le groupe $\mathrm{U}(\mathbb{Z}/N\mathbb{Z})$. La lettre F évoque l'épithète "favorable" ; en effet, si u appartient à cet ensemble, alors la décomposition de 0 dans $\mathbb{Z}/N\mathbb{Z}$

$$(u^{\frac{\mathrm{ord}(u)}{2}}+1)(u^{\frac{\mathrm{ord}(u)}{2}}-1)\equiv 0 \pmod N$$

fournit un facteur non-trivial de N. Nous voulons établir que ce cas *favorable* est aussi, en fait, *probable*.
Remarquons que v appartient à F_N ssi, la classe $u := v^{\frac{\mathrm{ord}(v)}{2}}$ est une racine carrée de 1 qui est ni 1 ni -1. Nous allons donc étudier de près ces racines carrées de 1 et voir que, contrairement à ce qui se passe lorsque $\ell = 1$ (où ces racines n'existent pas), lorsque $\ell \geq 2$ et N est impair, ces racines sont au contraire ... typiques.

Fait 18 *Si p est un nombre premier et $\alpha \geq 1$, alors la proportion des éléments d'ordre pair, dans $\mathrm{U}(\mathbb{Z}/p^\alpha\mathbb{Z})$, est supérieure ou égale à $\frac{1}{2}$.*

Preuve. On utilise le théorème 17.
Dans le cas où $p = 2$ tout élément a un ordre qui divise $2^{\alpha-1}$, donc est d'ordre pair.
Supposons maintenant que $p \geq 3$ et considérons l'ordre d'un couple (x, y) dans le groupe $(\mathbb{Z}/(p-1)\mathbb{Z}, +) \times (\mathbb{Z}/p^{\alpha-1}\mathbb{Z}, +)$.
Si x est impair, alors l'ordre d de $(\dot{x}, \dot{y})$ vérifie $d \cdot (\dot{x}, \dot{y}) = (\dot{dx}, \dot{dy}) = 0$. Donc $(p-1)$ divise dx, donc dx est pair alors que x est impair, donc d est pair. Donc tous les éléments de la forme $(2\dot{z}+1, \dot{y})$ sont d'ordre pair. ■

Lemme 19 *Soit N est un nombre dont la décomposition en nombres premiers est*

$$N = \prod_{i=1}^{\ell} p_i^{\alpha_i}.$$

Alors la proportion des éléments d'ordre pair, dans $\mathrm{U}(\mathbb{Z}/N\mathbb{Z})$, est supérieure ou égale à $1 - \frac{1}{2^\ell}$.

Preuve. En utilisant le Corollaire 16, on obtient que

$$\mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_{i=1}^{\ell} \mathrm{U}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}).$$

Soit $x := (x_1, \ldots, x_i, \ldots, x_\ell) \in \prod_{i=1}^{\ell} \mathrm{U}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$.
L'ordre de x est le ppcm des ordres des x_i dans leur facteur $\mathrm{U}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$. Donc ord$(x)$ est pair ssi l'un, au moins, des x_i a un ordre pair. La proportion des éléments x d'ordre impair est donc $\leq (\frac{1}{2})^\ell$ (vu le fait 18). ■

Fait 20 *Soit $p \geq 3$ un nombre premier et $\alpha \geq 1$. Alors 1 a exactement 2 racines carrées dans $\mathrm{U}(\mathbb{Z}/p^\alpha\mathbb{Z})$.*

Preuve. On utilise le Théorème 17.
Considérons un couple $(\dot{x}, \dot{y})$ dans le groupe $(\mathbb{Z}/(p-1)\mathbb{Z}, +) \times (\mathbb{Z}/p^{\alpha-1}\mathbb{Z}, +)$.
Il est racine carrée (additive) de 0 ssi $(2\dot{x}, 2\dot{y}) = (\dot{0}, \dot{0})$ i.e.

$$\begin{aligned} & 2x \equiv 0 \pmod{p-1} \wedge y \equiv 0 \pmod{p^{\alpha-1}} \\ \Leftrightarrow \quad & (x \equiv 0 \vee x \equiv \tfrac{p-1}{2}) \wedge y \equiv 0 \end{aligned}$$

Donc il y a exactement deux "racines carrées" (additives) de 0 : $(\dot{0}, \dot{0})$ et $(\dot{\frac{p-1}{2}}, \dot{0})$. ■

Fait 21 *Soit N est un nombre entier, $N = \prod_{i=1}^{\ell} p_i^{\alpha_i}$, avec $p_i \geq 3$.*
Alors 1 a exactement 2^ℓ racines carrées dans $\mathrm{U}(\mathbb{Z}/N\mathbb{Z})$.

Preuve. On part de

$$\mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_{i=1}^{\ell} \mathrm{U}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}).$$

Dans chaque facteur $\mathrm{U}(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$ il y a exactement 2 racines carrées. Or un élément $x := (x_1, \ldots, x_i, \ldots, x_\ell)$ est racine carré de 1 ssi tous les x_i sont des racines carrées de 1 (dans leur facteur). ■
Notons $R_2 := \{u \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \mid u^2 = 1\}$.

Fait 22 *Soit N est un nombre entier, $N = \prod_{i=1}^{\ell} p_i^{\alpha_i}$ (avec $\ell \geq 1, p_i \geq 3, \alpha_i \geq 1$) et soit $\omega \geq 1$ un entier. Alors*

$$\frac{\mathrm{Card}\{x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \mid x^\omega \in R_2 \setminus \{1, -1\}\}}{\mathrm{Card}\{x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \mid x^\omega \in R_2 \setminus \{1\}\}} \geq \frac{2^\ell - 2}{2^\ell - 1}.$$

Preuve. On sait que $\mathrm{Card}(R_2) = 2^\ell$.
Cas 1 : $\forall x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}), x^\omega \neq \dot{-1}$
On a alors

$$\mathrm{Card}\{x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \mid x^\omega \in R_2 \setminus \{1, -1\}\} = \mathrm{Card}\{x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \mid x^\omega \in R_2 \setminus \{1\}\}$$

et l'énoncé est clairement vrai.
Cas 2 : $\exists x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \mid x^\omega = \dot{-1}$
Par le Théorème chinois combiné avec le Théorème 17 (structure des unités), on peut voir $\mathrm{U}(\mathbb{Z}/N\mathbb{Z})$ comme le groupe additif

$$(\mathbb{Z}/(p_1 - 1)\mathbb{Z}) \times (\mathbb{Z}/p_1^{\alpha_1 - 1}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/(p_i - 1)\mathbb{Z}) \times (\mathbb{Z}/p_1^{\alpha_i - 1}\mathbb{Z}) \times \ldots \times (\mathbb{Z}/(p_\ell - 1)\mathbb{Z}) \times (\mathbb{Z}/p_\ell^{\alpha_\ell - 1}\mathbb{Z})$$

L'image de la classe de -1, par isomorphisme avec ce produit est

$$(\frac{\dot{p_1 - 1}}{2}, \dot{0}), \ldots, \frac{\dot{p_i - 1}}{2}, \dot{0}), \ldots, (\frac{\dot{p_\ell - 1}}{2}, \dot{0}) \tag{9.21}$$

Les éléments de R_2 sont les éléments de la forme

$$(\dot{r_1}, \dot{0}), \ldots, (\dot{r_i}, \dot{0}), \ldots, (\dot{r_\ell}, \dot{0})$$

tels que $\forall i \in [1, \ell], r_i = \frac{p_i - 1}{2}$ ou $r_i = 0$. On sait que : il existe des classes $\dot{x_1}, \ldots, \dot{x_i}, \ldots, \dot{x_\ell}$ telles que

$$(\omega \dot{x_1}, \dot{0}), \ldots, (\omega \dot{x_i}, \dot{0}), \ldots, (\omega \dot{x_\ell}, \dot{0})$$

est l'élément décrit par la formule (9.21). On voit donc que, en remplaçant chaque x_i par l'un des nombres 0 ou x_i on obtient 2^ℓ vecteurs de classes qui ont pour multiples par ω tous les éléments de R_2 :

$$\forall u \in R_2, \exists x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}), x^\omega = u.$$

Posons

$$S := \{x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}), x^\omega = 1\}.$$

On voit aisément que, pour tout $u \in R_2$:

$$\mathrm{Card}\{x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}), x^\omega = u\} = \mathrm{Card}(S)$$

Donc :

$$\mathrm{Card}\{x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}), x^\omega \in R_2 \setminus \{1, -1\}\} = (2^\ell - 2) \cdot \mathrm{Card}(S)$$

et

$$\mathrm{Card}\{x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \mid x^\omega \in R_2 \setminus \{1\}\} = (2^\ell - 1) \cdot \mathrm{Card}(S).$$

ce qui prouve l'énoncé. ■

Théorème 23 *Soit N est un nombre impair dont la décomposition en nombres premiers est*

$$N = \prod_{i=1}^{\ell} p_i^{\alpha_i}$$

avec $\ell \geq 2, p_i \geq 3, \alpha_i \geq 1$. Alors

$$\frac{\mathrm{Card}(F_N)}{\mathrm{Card}(\mathrm{U}(\mathbb{Z}/N\mathbb{Z}))} \geq \frac{1}{2}.$$

Preuve. Soit N satisfaisant les hypothèses du théorème. Notons $\mathrm{PU}(\mathbb{Z}/N\mathbb{Z})$ l'ensemble des éléments d'ordre pair dans $\mathrm{U}(\mathbb{Z}/N\mathbb{Z})$. Par le Lemme 19,

$$\frac{\mathrm{Card}(\mathrm{PU}(\mathbb{Z}/N\mathbb{Z}))}{\mathrm{Card}(\mathrm{U}(\mathbb{Z}/N\mathbb{Z})} \geq 1 - \frac{1}{2^\ell} \geq \frac{3}{4} \tag{9.22}$$

Remarquons les décompositions en unions disjointes :

$$\mathrm{PU}(\mathbb{Z}/N\mathbb{Z}) = \bigcup_{1 \leq \omega \leq N} \{x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}), x^\omega \neq 1, x^{2\omega} = 1\}$$

$$F_N = \bigcup_{1 \leq \omega \leq N} \{x \in \mathrm{U}(\mathbb{Z}/N\mathbb{Z}) \mid x^\omega \in R_2 \setminus \{1, -1\}\}$$

En utilisant le Fait 22, pour chaque entier $\omega \geq 1$, on conclut que

$$\frac{\mathrm{Card}(F_N)}{\mathrm{Card}(\mathrm{PU}(\mathbb{Z}/N\mathbb{Z}))} \geq \frac{2^\ell - 2}{2^\ell - 1} \geq \frac{2}{3} \tag{9.23}$$

En multipliant les deux inégalités (9.22)(9.23), on obtient que

$$\frac{\mathrm{Card}(F_N)}{\mathrm{Card}(\mathrm{U}(\mathbb{Z}/N\mathbb{Z}))} \geq \frac{3}{4} \cdot \frac{2}{3} = \frac{1}{2}.$$

■