

Mines ParisTech

CRYPTOGRAPHIE,  
THÉORIE DES NOMBRES  
ET INFORMATION QUANTIQUE

Pierre Rouchon

Enseignement spécialisé

Décembre 2012

# Table des matières

<b>1</b>	<b>Cryptographie classique</b>	<b>5</b>
1.1	Fonctions à sens unique	5
1.2	Stockage des mots de passe	6
1.3	Exponentielle modulaire	7
1.3.1	Définition	7
1.3.2	Le protocole de Diffie-Hellman	8
1.3.3	Système d'El Gamal	8
1.3.4	Signature et DSS	9
1.4	Le système RSA	10
1.5	Grands nombres premiers	11
1.5.1	Répartition	12
1.5.2	Algorithme AKS	12
1.5.3	Tests probabilistes	13
1.5.4	Fabrication de grands nombres premiers	17
1.5.5	Conclusion	17
1.6	Complexité	18
1.6.1	Introduction	18
1.6.2	Classe <b>P</b>	19
1.6.3	Classe <b>NP</b>	20
1.6.4	Classe <b>RP</b>	22
1.6.5	Fonctions à sens unique et la conjecture <b>P</b> $\neq$ <b>NP</b>	23
<b>2</b>	<b>Théorie des nombres</b>	<b>25</b>
2.1	PGCD	25
2.1.1	$\mathbb{Z}_n$ et $\mathbb{Z}_n^*$	25
2.1.2	Algorithme d'Euclide	26
2.1.3	Complexité de l'algorithme d'Euclide	27
2.2	La fonction d'Euler $\varphi(n)$	28
2.2.1	Fermat et Euler	28
2.2.2	Théorème chinois	29
2.2.3	Déchiffrement RSA	30

2.2.4	Eléments primitifs . . . . .	31
2.2.5	Théorème de Lucas . . . . .	32
2.3	Fonctions génératrices . . . . .	32
2.4	La fonction zêta . . . . .	35
2.4.1	Répartition des nombres premiers . . . . .	37
2.4.2	Le théorème de la progression arithmétique . . . . .	39
<b>3</b>	<b>Information et calculs quantiques</b>	<b>45</b>
3.1	Mécanique quantique . . . . .	45
3.1.1	Bra, Ket, états purs et états mixtes . . . . .	45
3.1.2	Opérateurs hermitiens, unitaires et équation différentielle de Schrödinger . . . . .	48
3.1.3	Mesures et réduction du paquet d'ondes . . . . .	50
3.1.4	Systèmes composites et produit tensoriel . . . . .	52
3.2	Qubit et $n$ -qubit . . . . .	53
3.2.1	Qubit : système à deux niveaux . . . . .	53
3.2.2	Matrices de Pauli . . . . .	54
3.2.3	$n$ -qubit . . . . .	55
3.2.4	Complément : manipulation d'un qubit . . . . .	56
3.3	Oscillateur harmonique . . . . .	61
3.4	Mesures généralisées et trajectoires quantiques . . . . .	64
3.4.1	La boîte à photons du LKB . . . . .	64
3.4.2	Physique et modélisation simplifiées . . . . .	66
3.4.3	Réduction progressive du paquet d'ondes et mesure quantique non destructive . . . . .	68
3.4.4	POVM et trajectoires quantiques . . . . .	71
3.5	Impossibilité du clonage . . . . .	73
3.6	Intrication . . . . .	75
3.6.1	Intrication et non-localité . . . . .	75
3.6.2	Inégalités de Bell et paradoxe EPR . . . . .	76
3.6.3	Téléportation quantique . . . . .	80
3.7	Cryptographie quantique . . . . .	83
3.7.1	Distribution de clés secrètes par BB84 . . . . .	83
3.7.2	Clés secrètes par partage d'états intriqués . . . . .	85
3.8	Introduction au calcul quantique . . . . .	86
3.8.1	Portes et circuits logiques classiques . . . . .	86
3.8.2	Portes et circuits logiques quantiques . . . . .	87
3.8.3	Algorithme de Deutsch-Josza (1992) . . . . .	89
3.8.4	Algorithme de recherche de Grover (1996) . . . . .	90
	<b>Bibliographie</b>	<b>96</b>

<i>TABLE DES MATIÈRES</i>	3
---------------------------	---

<b>A Système oscillant et moyennisation</b>	<b>97</b>
---	-----------



# Chapitre 1

## Cryptographie classique

Ce chapitre est une courte introduction à quelques aspects de la cryptographie. Pour un exposé plus détaillé nous renvoyons à l'excellent cours de Gilles Zémor de l'ENST [29].

La cryptographie moderne fondée sur les fonctions à sens unique commence en 1976 avec [14] où Diffie et Hellman proposent une solution à un problème considéré alors comme insoluble : Alice et Bob ne disposent pour communiquer que d'une ligne de transmission écoutée en permanence par le méchant Oscar ; ils souhaitent cependant tous les deux communiquer de manière confidentielle. Ainsi ils doivent publiquement (c'est à dire en présence du méchant Oscar) se mettre d'accord sur un protocole de communication garantissant la confidentialité. Diffie et Hellman proposent une solution à ce problème en utilisant le fait qu'Oscar n'a qu'une puissance finie de calcul. Ainsi cette solution n'est pas valable que si Oscar dispose de moyen de calcul très puissant ou si Oscar a tout son temps.<sup>1</sup>

### 1.1 Fonctions à sens unique

Voici une définition assez imprécise de fonction à sens unique (on parle aussi de fonction di-symétrique). Cela n'a pas beaucoup d'importance pour l'instant car nous allons voir des exemples par la suite qui permettront de mieux comprendre cette pseudo-définition. De plus, nous ne savons pas actuellement s'il existe réellement des fonctions à sens unique. Nous verrons plus loin qu'une telle existence entraînerait que  $\mathbf{P} \neq \mathbf{NP}$ , conformément à ce que pense l'immense majorité des spécialistes.

---

1. Nous supposons implicitement que Oscar ne peut pas se faire passer pour Alice auprès de Bob. Cela pose le problème de l'authentification des échanges, authentification que l'on peut aussi résoudre par des fonctions à sens unique (cf. signature).

Soit  $A_n$  et  $B_n$  deux ensembles finies indexés par  $n$ , avec  $\#A_n = n$  et  $f_n$  une fonction de  $A_n$  dans  $B_n$ . On peut toujours supposer que  $A_n$  et  $B_n$  correspondent à des parties finies  $\mathbb{N}$  et que  $A_n$  s'identifie aux entiers entre 1 et  $n$ . La notion de fonction à sens unique n'a de sens que lorsque  $n$  tend vers l'infini. Nous dirons que  $f_n$  est à sens unique, si et seulement si, pour  $n$  devenant très grand

1. Il est facile de calculer  $f_n(x)$  pour importe quel  $x \in A_n$  ;
2. Il est difficile pour  $y \in f_n(A_n)$  de trouver un  $x$  tel que  $f_n(x) = y$ .

Le point-1 veut dire qu'il existe un algorithme "rapide" pour calculer  $f_n(x)$ , par rapide on veut dire nécessitant une quantité polynômiale de calculs en fonction du nombre de bits nécessaires pour coder  $x \in A_n$ , à savoir  $\log_2(n)$ . Si on note  $C_n(x)$  le nombre d'opérations élémentaires nécessaires au calcul de  $f_n(x)$ , cela veut dire qu'il existe  $M, \alpha > 0$  tels que pour tout  $n \in \mathbb{N}$ , et pour tout  $x \in A_n$ ,  $C_n(x) \leq M(\log n)^\alpha$ .

Le point-2 veut simplement dire que l'on ne connaît pas d'algorithme rapide qui permette de résoudre  $f_n(x) = y$ . Pour  $n$  grand, il est illusoire pour trouver un tel  $x$  d'utiliser la méthode "brutale" en testant tous les  $x$  de  $A_n$  via le calcul "rapide" de  $f_n$ . En effet, le nombre d'opérations élémentaires est alors de l'ordre de  $Mn(\log n)^\alpha$  c'est à dire exponentiel en fonction de l'espace mémoire nécessaire à l'écriture des données,  $\log_2(n)$ . Pour les fonctions à sens unique usuelles,  $n$  est pris assez grand pour que le calcul de  $f_n^{-1}$  soit impossible avec les moyens actuels. Typiquement,  $\log_2(n) > 1000$ , i.e.,  $n$  est un chiffre de quelques milliers de bits.

Il est important de faire cette estimation une fois dans sa vie pour comprendre ce que signifie une complexité exponentielle. Prenons  $n = 2^{128}$  et supposons que l'évaluation de  $f_n(x)$  prenne 1 seconde. Alors  $n$  évaluations de  $f_n$  nécessiteront environ  $10^{31}$  années de calcul.

## 1.2 Stockage des mots de passe

Supposons que nous ayons à notre disposition une telle fonction  $f_n$  et que nous ayons à stocker les mots de passe pour accéder à un ordinateur. L'ensemble des mots de passe en clair (celui que l'on tape dans le "login") constitue une partie de  $A_n$  avec  $n$  bien plus grand que le nombre des utilisateurs disponibles. Au lieu de stocker les mots de passe en clair sur un fichier même protégé du compte "system", il suffit de stocker dans un fichier l'image des mots de passe via la fonction  $f_n$ . Lorsque l'on se connecte avec son mot de passe, disons  $\pi$ , la machine calcule  $f_n(\pi)$  et vérifie s'il est bien dans la liste qu'elle a sur son disque dur. Nous voyons qu'il est difficile même connaissant  $n$ ,  $f_n$  et la liste des images par  $f_n$  des mots de passe, de remonter à ceux-ci.

## 1.3 Exponentielle modulaire

Il s'agit de l'exemple le plus simple et aussi très utilisé de fonction à sens unique. On l'appelle aussi exponentielle modulo un nombre premier  $p$  ou encore exponentielle discrète. Son caractère di-symétrique vient du fait que l'on ne connaît pas d'algorithme rapide pour calculer le logarithme discret.

### 1.3.1 Définition

Soit  $p$  un nombre premier, a priori grand. L'ensemble  $\mathbb{Z}_p^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ , les entiers définis modulo  $p$  et différents de zéro, forme un groupe pour la multiplication. Tout entier  $x$  entre 1 et  $p-1$  est premier avec  $p$ . L'algorithme d'Euclide calcule le pgcd et fournit en même temps les entiers  $u$  et  $v$  tels que  $ux + vp = 1$  (identité de Bezout). Ainsi l'inverse de  $x$  dans  $\mathbb{Z}_p^*$  est  $u$  car  $ux = 1 \pmod{p}$  et le calcul de  $x^{-1}$  dans  $\mathbb{Z}_p^*$  est facile. De plus  $\mathbb{Z}_p^*$  est un groupe cyclique : il est engendré par les puissances de certains de ses éléments, dits éléments primitifs. Supposons donc que l'on connaisse l'un d'entre eux, noté  $\alpha$ . Alors les gens s'accordent pour dire que la fonction

$$\begin{array}{ccc} \mathbb{Z}_p^* & \rightarrow & \mathbb{Z}_p^* \\ x & \mapsto & f(x) = \alpha^x \end{array}$$

est à sens unique sans pour autant en avoir une preuve (cf. la définition en 1.1 avec  $n$  parcourant les nombres premiers). Pour calculer  $f(x)$ , on écrit  $x$  en base 2 :  $x = \sum_{i=0}^m a_i 2^i$  avec  $a_i \in \{0, 1\}$  ce qui donne un algorithme avec au plus  $E(2(1 + \log_2(p)))$  multiplications modulo  $p$  ( $E$  est la partie entière). Détaillons un peu cet algorithme d'exponentiation rapide. Tout d'abord les  $\beta_i = \alpha^{2^i}$  s'obtiennent par  $m$  multiplications :

$$\beta_0 = \alpha, \quad \beta_1 = (\beta_0)^2, \quad \beta_2 = (\beta_1)^2, \quad \dots, \quad \beta_m = (\beta_{m-1})^2.$$

Avec au plus  $m$  multiplications supplémentaires on obtient  $\alpha^x$  car

$$\alpha^x = \prod_{i \mid a_i=1} \beta_i.$$

Il faut après chaque multiplication réduire son résultat modulo- $p$ , si l'on ne veut pas saturer la mémoire de l'ordinateur. Nous avons en tout au plus  $2m$  multiplications modulo- $p$  et  $m \leq \log_2(p)$ .

Tous les algorithmes connus pour inverser cette fonction (le logarithme discret) nécessitent un temps de calcul non polynômial en  $\log(p)$  et sont impraticables dès que  $p$  est un nombre de quelques centaines de bits.



Pourquoi donc prendre un nombre premier  $p$  et un élément primitif modulo- $p$ . Tout d'abord,  $p$  premier implique que tout entier non nul plus petit que  $p$  est inversible. Ensuite  $\alpha$  primitif implique que l'application  $f$  est bijective. Nous verrons plus loin comment fabriquer à la fois des grands nombres premiers  $p$  et un élément primitif  $\alpha$  modulo- $p$ .

Nous avons maintenant tous les éléments pour comprendre le protocole de Diffie et Hellman, protocole permettant de partager un secret via un canal public (cf. le problème évoqué au tout début du chapitre).

### 1.3.2 Le protocole de Diffie-Hellman

Pour communiquer de façon confidentielle, Alice et Bob vont se mettre d'accord sur un nombre secret  $S$  qui leur servira de clé à un système classique de chiffrement. Voici comment, en utilisant uniquement le canal public, ils vont procéder pour s'échanger la clé secrète  $S$ .

Alice et Bob se mettent d'accord publiquement et en face du méchant Oscar sur un nombre premier  $p$  et un élément primitif  $\alpha$  modulo- $p$ . Ensuite, chacun dans son coin, de façon aléatoire et secrète, choisit un nombre entre 1 et  $p$ . Le nombre choisi par Alice est noté  $a$  et celui choisi par Bob,  $b$ . Alice et Bob calculent chacun une exponentielle (facile),  $A = \alpha^a \pmod{p}$  pour Alice et  $B = \alpha^b \pmod{p}$  pour Bob. Ce calcul fait, ils échangent publiquement et toujours devant le grand méchant Oscar  $A$  et  $B$ . Enfin leur secret sera  $S = \alpha^{ab} \pmod{p}$ . En effet, Alice peut calculer  $S = B^a \pmod{p}$  avec les informations dont elle dispose. Bob fait de même avec  $S = A^b \pmod{p}$ . Maintenant Oscar ne connaît que  $p$ ,  $\alpha$ ,  $A$  et  $B$ . Il ne connaît pas  $a$  et  $b$  car ces données n'ont pas été transmises sur le canal. On ne voit pas comment, il pourrait calculer  $S$  sans calculer un logarithme modulo- $p$ . Nous voyons que l'exponentielle est utilisée pour les deux propriétés suivantes : elle est facile à calculer et  $(\alpha^a)^b = (\alpha^b)^a$ .

### 1.3.3 Système d'El Gamal

Il s'agit d'introduire une di-symétrie dans le chiffrement et le déchiffrement. On considère toujours l'exponentielle modulaire associée à un nombre premier  $p$  et un nombre primitif modulo- $p$ ,  $\alpha$ .

Le destinataire Bob dispose de deux clés : la clé secrète (un nombre  $s$ ) avec laquelle il calcule  $P = \alpha^s \pmod{p}$ ; la clé publique  $(p, \alpha, P)$ .

Alice souhaite envoyer le message  $M$  (représenté par un entier  $M$  défini mod  $(p)$ ) à Bob. Elle dispose de la clé  $(p, \alpha, P)$  que Bob lui a envoyée en clair et publiquement. Alice choisit alors un nombre  $k$  aléatoirement et calcule les

deux exponentielles suivantes :

$$A = \alpha^k \pmod{p}, \quad B = MP^k \pmod{p}.$$

Alice envoie alors à Bob  $A$  et  $B$  :  $(A, B)$  forme le message chiffré. Pour le décodage, Bob connaissant  $s$ , calcule  $A^s \pmod{p}$  qui n'est autre que  $P^k \pmod{p}$  (commutation des exponentiations). Ainsi Bob obtient le message en clair d'Alice par le calcul suivant :  $M = B/A^s \pmod{p}$ . On suppose maintenant que le méchant Oscar souhaite décoder le message  $(A, B)$  d'Alice. Il ne dispose que de la clé publique  $(p, \alpha, P)$ . On ne voit pas comment il pourrait faire sans passer par un calcul de logarithme.

Un des avantages de cette méthode est que le même message  $M$  codé deux fois ne donne pas le même message codé  $(A, B)$  à cause de l'aléa pour  $k$ . De plus, pour faire tous ces calculs, on n'a pas besoin d'avoir  $p$  premier et  $\alpha$  primitif. Le seul point bloquant est le fait de pouvoir diviser par  $A^s$ , c'est à dire il faut s'assurer que pour tout  $k$  et  $s$ , l'élément  $\alpha^{ks}$  soit inversible modulo- $p$ . Ce qui est le cas car  $\alpha$  est primitif modulo  $p$  et donc inversible modulo  $p$ .

De façon plus générale : pour faire ces calculs, il suffit uniquement que  $\alpha$  et  $p$  soient premiers entre eux ( $p$  premier et  $\alpha$  primitif modulo  $p$  sont des hypothèses très fortes). Cependant il faut choisir  $\alpha$  et  $p$  pour que le logarithme soit difficile à calculer, ce qui n'est pas encore prouvé.

### 1.3.4 Signature et DSS

La version optimisée de ce qui suit est à la base de la norme américaine DSS (Digital Signature Standard) qui date de 1994.

On ne souhaite plus que le message  $M$  qu'envoie Alice à Bob soit confidentiel mais Bob souhaite avoir la garantie lorsqu'il reçoit le message  $M$  que c'est bien Alice qui le lui a envoyé et pas une autre personne. Pour cela Alice dispose d'un nombre premier  $p$  et de  $\alpha$  primitif modulo- $p$ . Elle choisie un nombre  $s$  au hasard et une fois pour toute. Elle communique de façon officielle sa signature par le triplet rendu public et dont Bob sait qu'il a été construit par Alice  $(p, \alpha, P = \alpha^s)$ . Connaissant la signature l'Alice, Bob reçoit un jour un message contenant  $M$  et il veut être bien sûr que c'est Alice qui lui a envoyé ce message. Pour cela Alice rajoute à  $M$  deux nombres  $S = (u, v)$  qui authentifient le message et en forment une signature très difficile à imiter et en plus liée au contenu du message  $M$ . Ces nombres sont construits de la façon suivante : Alice choisit au hasard un nombre  $k$  premier avec  $p - 1$ . Elle calcule ensuite  $u = \alpha^k \pmod{p}$  et alors  $v$  est l'unique solution de  $M = us + kv \pmod{p - 1}$  ( $k$  est inversible modulo- $(p - 1)$ ).

Ainsi Bob recevant  $M$  avec la signature  $S = (u, v)$  connaissant  $(p, \alpha, \alpha^s)$  vérifie par une simple exponentiation que seule Alice peut avoir envoyé ce message. En effet, le calcul de  $\alpha^M$  donne

$$\alpha^M = \alpha^{us+kv+r(p-1)} = (\alpha^s)^u (\alpha^k)^v \pmod{p}$$

où  $r$  est un certain entier et utilisant le petit théorème de Fermat qui assure que  $\alpha^{p-1} = 1 \pmod{p}$  dès que  $p$  est premier et  $\alpha$  entre 1 et  $p-1$ . Comme  $(\alpha^s)^u = P^u$  et  $(\alpha^k)^v = u^v$ , Bob peut calculer  $P^u$  et  $u^v$  et s'assurer que leur produit donne bien  $\alpha^M$  modulo- $p$ . Pour signer le message  $M$  sans connaître  $s$  on est face à un problème difficile trouver  $u$  et  $v$  vérifiant

$$\alpha^M = P^u u^v \pmod{p}$$

problème qui nécessite a priori le calcul d'un logarithme.

Comme la signature  $S = (u, v)$  dépend de  $M$ , il est très difficile pour le grand méchant Oscar qui a intercepté le message d'Alice avant qu'il n'arrive à Bob, de changer son contenu, i.e., de le falsifier. De plus, même envoyé plusieurs fois, le même message  $M$  n'aura pas la même signature  $S$  à cause du choix aléatoire de  $k$ .

En conclusion, tout le monde sait authentifier le message d'Alice mais seule Alice peut authentifier ses messages. Pour cela Alice utilise astucieusement l'exponentielle modulaire et le petit théorème de Fermat.

**Exercice** Imaginer un protocole à base d'exponentielles modulaires pour jouer à pile ou face sur internet, garantissant le fait qu'aucun des deux joueurs ne pourra tricher sans que l'autre ne le sache.

## 1.4 Le système RSA

Les systèmes précédents utilisent le fait que le calcul d'une exponentielle est facile alors que l'opération inverse est difficile. Le protocole d'El Gamal de clé publique n'est pas historiquement le premier. Il s'agit du système RSA inventé par Rivest, Shamir et Adleman en 1977 [26]. Ce système s'appuie sur la difficulté de factoriser un grand nombre (d'au moins 1024 bits) qui est le produit de deux grands nombres premiers.

On reprend le problème résolu par le protocole di-symétrique d'El Gamal. La clé secrète que garde précieusement Bob est formée de deux grands nombres premiers  $p$  et  $q$  de plusieurs centaines de bits. La clé rendue publique par Bob est le produit  $n = pq$  ainsi qu'un entier  $e$  qui a la propriété particulière d'être inversible modulo  $(p-1)(q-1)$ , i.e., d'être premier avec

$(p-1)(q-1)$ . En fait  $(p-1)(q-1)$  est la valeur de la fonction indicatrice d'Euler  $\varphi$  en  $n$  ( $\varphi(n)$  est par définition le nombre d'entiers premiers avec  $n$  et plus petits que  $n$ ). Le chiffrement d'un message représenté par un entier  $M \pmod{n}$  se fait par la transformation suivante :

$$M \mapsto M^e \pmod{n}.$$

Ainsi Bob reçoit via un canal public  $A = M^e$ . Pour déchiffrer, il lui suffit d'élever  $A$  à la puissance  $d$  où  $d$  est l'inverse de  $e$  modulo  $\varphi(n) = (p-1)(q-1)$ . On sait en utilisant un raffinement du théorème d'Euler-Fermat avec le théorème chinois (voir page 30) que

$$M^{ed} = M \pmod{n}$$

et donc que

$$A^d = (M^e)^d = M^{ed} = M \pmod{n}.$$

Remarquons maintenant que le grand méchant Oscar doit trouver  $M$

$$A = M^e \pmod{n}$$

connaissant  $A$ ,  $e$  et  $n$ . On ne sait pas comment faire un tel calcul en temps polynômial sans connaître  $\varphi(n)$ . Comme,  $\varphi(n) = (p-1)(q-1)$  et  $n = pq$  cela revient à connaître  $p$  et  $q$ .

En mode signature, il suffit de permuter le rôle de  $e$  et  $d$ . Ainsi, Alice choisit  $p$  et  $q$  deux grands nombres premiers et communique sa signature officielle sous la forme de  $(n = pq, e)$  où  $e$  est inversible par rapport à  $\varphi(n)$ . Alice garde bien-sûr sa clé secrète  $d$  qui est l'inverse de  $e$  modulo  $\varphi(n)$ . Pour signer son message Alice envoie à Bob  $M$  et sa signature  $M^d$ . Alors Bob authentifie le message comme provenant d'Alice en vérifiant que  $(M^d)^e = M \pmod{n}$  qui signifie implicitement que l'expéditeur connaît un inverse de  $e$  modulo  $\varphi(n)$  et donc la factorisation de  $n$ . Ce ne peut donc être qu'Alice.

**Exercice** Imaginer un système de monnaie électronique anonyme utilisant la fonction puissance de RSA.

## 1.5 Grands nombres premiers

Les grands nombres premiers jouent un rôle important en cryptographie. L'un des premiers problèmes pratiques est d'en construire. Nous montrons ici comment des résultats en théorie des nombres permettent de répondre à cette préoccupation.

### 1.5.1 Répartition

On note  $\mathbb{P}$  l'ensemble de nombres premiers. Euclide avait démontré l'existence d'une infinité de nombres premiers. Pour caractériser leur répartition, on introduit la fonction de comptage  $\pi(x)$  suivante :

$$\pi(x) := \#\{p \in \mathbb{P} \mid p \leq x\}$$

Gauss et Legendre avaient déjà suggéré au cours des dernières années du *XVIII<sup>e</sup>* siècle que  $\pi(x) \sim x/\log(x)$  pour  $x$  grand. Ce n'est qu'en 1896 que Hadamard et de la Vallée-Poussin ont montré ce résultat en utilisant une fonction de la variable complexe "qui code les nombres premiers", la fonction  $\zeta$  de Riemann définie par la série de Diriclet

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \tag{1.1}$$

absolument convergente pour  $\Re(s) > 1$ .

Il s'en suit que le moyen le plus simple pour obtenir un grand nombre premier est de prendre au hasard un grand entier et de tester s'il est premier. En effet, nous le verrons plus loin, on dispose, avec par exemple le test de Miller-Rabin, d'un algorithme très efficace qui garantie la primalité, avec une probabilité aussi petite que l'on souhaite. Si l'on tire au hasard un nombre de 1024 bits, on sait, en utilisant  $\pi(x) \equiv x/\log(x)$ , que l'on a une chance sur  $\log(2^{1024}) \approx 710$  de tomber sur un nombre premier. Une telle méthode est tout à fait praticable si l'on dispose de tests rapides de primalité.

Une autre façon de voir la répartition  $\pi(x) \sim x/\log(x)$  est la suivante. Supposons que nous ayons classé les nombres premiers par ordre croissant  $p_n$  avec  $n \in \mathbb{N}^*$ ,  $p_n < p_{n+1}$ . Alors dire  $\pi(x) \sim x/\log(x)$  pour  $x$  grand, équivaut à dire que  $p_n \sim n \log(n)$  pour  $n$  grand. En effet  $\pi(p_n) = n$  par construction. Donc, si  $\pi(x) \sim x/\log(x)$  alors  $p_n/\log(p_n) \sim n$  et donc  $p_n \sim n \log(n)$ . Réciproquement si  $p_n \sim n \log(n)$  alors, par définition  $\pi(x) = n$  où  $n$  est l'unique entier tel que  $p_n \leq x < p_{n+1}$ . En remplaçant  $p_n$  par  $n \log(n)$  dans cette inégalité on voit que,  $n \log(n) \sim x$  soit donc  $\pi(x) = n \sim x/\log(x)$ .

### 1.5.2 Algorithme AKS

Depuis de nombreuses années, les spécialistes pensaient qu'il existait un algorithme en temps polynomial pour tester la primalité d'un nombre  $n$ . Cette conjecture est effectivement vraie car en 2002, Manindra Agrawal de l'Indian Institute of Technology à Kanpur et deux de ses étudiants Neeraj Kayal et Nitin Saxena ont trouvé un algorithme simple et polynômial en  $0(\log^{12}(n))$  qui teste la primalité de  $n$ .

Leur algorithme s'appuie de façon ingénieuse sur le petit théorème de Fermat qui dit que pour tout entier premier  $n$  et tout entier  $a \not\equiv 0 \pmod{n}$  (i.e.  $a$  premier avec  $n$ ) alors  $a^{n-1} \equiv 1 \pmod{n}$ . Nous ne décrivons pas ici cet algorithme. Nous renvoyons le lecteur à "google" avec comme mots clés "AKS" et "Prime" pour avoir les informations les plus récentes sur cet algorithme.

Enfin, l'algorithme AKS répond par "oui" ou "non" à la question : "  $n$ , est-il premier?". Si la réponse est "non", l'algorithme ne donne pas de diviseur non trivial de  $n$ . Ainsi, la difficulté de la factorisation, difficulté sur laquelle repose le système RSA reste entière. Mais il reste possible que des étudiants brillants trouvent un algorithme efficace de factorisation. Cependant, les spécialistes pensent qu'un tel algorithme n'existe pas alors que pour la primalité, l'ensemble de la communauté s'accordait à penser avant l'été 2002 qu'être premier est dans **P** .

### 1.5.3 Tests probabilistes

Le test de Miller-Rabin est le prototype d'algorithme **RP** (c'est à dire qui comporte un part d'aléatoire et donc assure la primalité avec une probabilité aussi proche de 1 que l'on veut). Cet algorithme est nettement plus efficace en pratique que la version actuelle d'AKS. Cela peut changer mais pour l'instant ce n'est pas le cas. Pour comprendre ce test, il faut revenir au test de Fermat.

#### Test de Fermat et nombres de Carmichael

Rappelons le petit théorème de Fermat : si  $n$  est premier alors pour tout  $a \not\equiv 0 \pmod{n}$ ,  $a^{n-1} \equiv 1 \pmod{n}$ .

Ainsi, si après avoir tiré au hasard un nombre  $n$ , on trouve un  $1 \leq a < n$  tel que  $a^{n-1} \not\equiv 1 \pmod{n}$ , on sait que  $n$  n'est pas premier. Aussi, il est tentant de faire le dépistage heuristique suivant appelé test de Fermat : prendre  $a < n$  au hasard et calculer  $a^{n-1} \pmod{n}$ . Si  $a^{n-1} \equiv 1 \pmod{n}$  on dit que  $n$  est premier en base  $a$ .

Etudier l'efficacité de ce test revient à étudier la densité des nombres composés et premiers en base  $a$  par rapport celle des nombres premiers : on parle alors d'entiers pseudo-premiers en base  $a$ . Si on note  $\pi_a(x)$  le nombre d'entiers  $n$  composés, premiers en base  $a$  et  $\leq x$ , alors on sait que  $\pi_a(x)/\pi(x)$  tend vers zéros quand  $x$  tend vers l'infini. Par exemple, pour  $a = 2$ , Pomerance (1981) a montré que

$$\exp(\log(x)^{5/14}) \leq \pi_2(x) \leq x \exp\left(-\frac{\log(x) \log \log \log(x)}{2 \log \log(x)}\right)$$

Ainsi pour  $x = 2^{512}$  on a

$$\pi_2(x)/\pi(x) \leq 5,3 \cdot 10^{-32}.$$

On peut dire que pour  $n$  grand choisi au hasard, il faut être très malchanceux pour que  $n$  soit pseudo-premier en base  $a$  pour un grand nombre de  $a$ . Cependant, cela ne veut pas dire qu'il n'existe pas de nombre  $n$  qui soit pseudo-premier pour toutes bases  $a$  entre 2 et  $n-1$  avec  $a$  premier avec  $n$ . En fait, il en existe une infinité. Ce sont les nombres de Carmichael qui sont la plaie du test de Fermat. On a montré en 1994 que pour  $x$  assez grand il existe au moins  $x^{2/7}$  nombres de Carmichael inférieurs à  $x$  (pour plus d'information voir [29][pages 101–103]).

### Algorithme de Miller-Rabin

Nous allons simplement décrire l'algorithme sans en justifier tous les points. On peut voir cet algorithme comme une version étendue du test de Fermat qui évite la plaie associée aux nombres de Carmichael. Nous ne parlerons pas ici du test de Soloway-Strassen qui est historiquement le premier du genre. En fait, le test de Miller-Rabin est une réelle amélioration de ce dernier tout en étant plus simple à expliquer (pas de symbole de Jacobi).

Pour  $n$  premier et  $2 \leq a \leq n-1$ , on sait que  $a^{n-1} = 1 \pmod{n}$ . Mais  $n-1$  est pair donc  $b = a^{\frac{n-1}{2}}$  vérifie  $b^2 = 1 \pmod{n}$ . Donc  $b$  est racine du polynôme  $y^2 - 1 = 0$  dans  $\mathbb{Z}/n\mathbb{Z}$  qui est un corps pour l'addition et la multiplication modulo- $n$  car  $n$  est premier. Dans un corps, le nombre de racines d'un polynôme est au plus égal à son degré. Donc on a nécessairement  $b = 1 \pmod{n}$  ou  $b = -1 \pmod{n}$ , car 1 et  $-1$  sont deux racines distinctes de  $y^2 - 1$ . Ainsi, si  $n$  est premier,  $a^{\frac{n-1}{2}} = \pm 1 \pmod{n}$  pour tout  $0 < a < n$ . Si  $(n-1)/2$  est encore pair et si  $a^{\frac{n-1}{2}} = 1 \pmod{n}$ , alors un raisonnement identique montre que nécessairement  $a^{\frac{n-1}{4}} = \pm 1 \pmod{n}$ . En continuant jusqu'à l'entier  $s$  pour lequel  $\frac{n-1}{2^s}$  soit impair on obtient le test très astucieux suivant.

**Test de Miller-Rabin** Pour un entier impair  $n$  que l'on écrit  $n = 1 + 2^s t$  avec  $s \geq 1$  et  $t$  impair : on prend au hasard  $a$  entier entre 2 et  $n-1$  et on calcule les nombres  $r_i = a^{2^i t} \pmod{n}$ . L'entier  $n$  passe le test dans les deux cas suivants : soit  $r_0 = r_1 = \dots = r_s = 1$  ; soit il existe  $i$  entre 0 et  $s-1$  tel que  $r_i = -1$ .

Un nombre  $n$  qui passe le test de Miller-Rabin pour un certain  $a$  est dit fortement premier en base  $a$ .

**Exercice** Donner une version optimisée sur le plan algorithmique du test de Miller-Rabin et en donner sa complexité en terme de multiplication modulo  $n$ .

Cependant, la situation est très différente du test de Fermat, car il n'existe pas pour ce test ci l'analogie des nombres de Carmichael qui passeraient le test pour tout entier  $a < n$  bien que  $n$  soit composé. En effet, on peut montrer par des raisonnements arithmétiques assez élémentaires que, si  $n$  est composé,  $n$  est fortement premier en base  $a$  pour au plus  $1/4$  des entiers  $a$  entre 2 et  $n - 1$ .

Ainsi une utilisation probabiliste du test de Miller-Rabin pour un entier  $n$  impair est la suivante. On prend  $k$  entier grand. On choisit  $a_1$  entre 2 et  $n - 1$  au hasard. Si  $n$  n'est pas fortement premier en base  $a_1$ ,  $n$  n'est pas premier on s'arrête. Sinon, on choisit toujours au hasard un nouveau  $a_2$  différent de  $a_1$  entre 2 et  $n - 1$ . Si  $n$  est fortement premier en base  $a_2$ , on choisit un troisième nombre  $a_3$  différent des deux précédents. Et ainsi de suite jusqu'à avoir choisi au plus  $k$  nombres différents  $a_i$  entre 2 et  $n - 1$ . Bien sûr, on s'arrête avant si pour un certain  $a_i$ ,  $n$  n'est pas fortement premier en base  $a_i$ .

Supposons maintenant que le nombre  $n$  soit fortement premier pour toutes les bases  $a_1$  à  $a_k$  de la procédure précédente. Un simple comptage montre que, la proportion des  $k$ -uples  $(a_1, \dots, a_k) \in \{2, \dots, n - 1\}^k$  tels que  $n$  soit fortement premier pour chaque  $a_i$  est plus petite que  $\frac{1}{4^k}$ . Ainsi on peut dire qu'un tel  $n$  est premier avec une probabilité de  $1 - \frac{1}{4^k}$ .

Cependant, il faut faire attention à l'utilisation de ce type de probabilité. En effet, on pourrait en conclure des estimations probabilistes fausses concernant la méthode suivante de génération de grands nombres premiers.

Tirons au hasard un nombre  $n$  parmi tous les nombres au plus égaux à  $N$  avec  $N$  grand. La probabilité que  $n$  soit premier est de  $1/\log(N)$ . Supposons que pour un entier  $k$  assez grand,  $n$  ait passé avec succès  $k$  tests de Miller-Rabin. Un raisonnement un peu rapide nous dirait que  $n$  est premier avec une probabilité de  $1 - 1/4^k$ . Cela est faux, car il faut aussi considérer le fait que  $n$  est pris au hasard parmi les nombres plus petits que  $N$ , avec une probabilité de  $1/\log(N)$  de tomber lors de ce premier tirage sur un nombre premier. Alors on peut montrer mais ce n'est pas si facile (cf. exercice ci-dessous) que la probabilité pour que  $n$ , tiré au hasard (loi uniforme) dans  $[0, N]$  avec  $N$  grand, soit composé et que  $n$  passe le test  $k$  fois, vérifie l'estimation

$$\text{Prob}(n \text{ composé} \mid \text{test passé } k \text{ fois}) < \log(N)/4^k \quad (1.2)$$

dès que  $k$  est assez grand pour que  $4^k \gg \log(N)$ . Ainsi, si l'on se fixe maintenant  $\varepsilon \ll 1$  et le nombre de bits  $B$  pour  $n$  ( $N = 2^{B+1}$ ), on en déduit le



nombre minimal  $k$  de tests à faire par la formule

$$k = \frac{\log(\log(N)/\varepsilon)}{\log(4)}.$$

Par exemple, pour un nombre de 512-bits pris au hasard, il faut prendre  $k = 26$  (resp.  $k = 42$ ) si on veut avoir une probabilité d'erreur de moins de  $10^{-5}$  (resp.  $10^{-10}$ ) de se tromper après  $k$  tests de Miller-Rabin positifs.

**Exercice (sur la formule de Bayes)** Montrer que la probabilité qu'un nombre  $n$  pris au hasard parmi les nombres plus petits que  $N$  ( $N$  grand) passe  $k$  tests de Miller-Rabin et soit composé, est donnée par

$$\frac{p_k(1 - 1/\log(N))}{p_k(1 - 1/\log(N)) + 1/\log(N)}$$

où  $p_k$  est la probabilité de passer le test  $k$  fois sachant le nombre  $n$  composé. Utiliser le fait que  $p_k \leq 1/4^k$  pour en déduire la formule (1.2).

### Algorithme de Miller-Bach

Il s'agit d'un algorithme déterministe et polynômial qui repose sur une conjecture plausible en théorie des nombres : l'hypothèse de Riemann généralisée. Pour donner une idée de cette conjecture, voici l'hypothèse de Riemann pour la fonction  $\zeta(s)$ . Bien que la série (1.1) ne semble définir  $\zeta(s)$  que pour  $\Re(s) > 1$ , on peut prolonger  $\zeta$  sur tout le plan complexe sauf en  $s = 1$  qui est un pôle simple. Plus directement  $\zeta(s) - 1/(s-1)$  est une fonction holomorphe définie sur tout le plan complexe : c'est donc une fonction entière comme le sont les fonctions  $\cos s$  ou  $\sin s/s$  par exemple<sup>2</sup>. L'hypothèse de Riemann porte alors sur la localisation des zéros de  $\zeta$ . On sait depuis longtemps que  $\zeta(-2n) = 0$  pour  $n$  entier  $> 0$ . On sait aussi depuis longtemps que les autres zéros, appelés zéros non triviaux, sont dans la bande verticale  $0 < \Re(s) < 1$ . Dans son fameux article de 1859, Riemann émet l'hypothèse que les zéros non triviaux de  $\zeta$  sont sur la droite verticale  $\Re(s) = 1/2$ . Cette hypothèse, corroborée par des calculs numériques très poussés n'a pas encore été démontrée et constitue la grande conjecture de la théorie analytique des nombres. Maintenant, l'hypothèse de Riemann généralisée porte sur des fonctions similaires à  $\zeta$  du type

$$\sum_{n \geq 1} \frac{\chi(n)}{n^s}$$

---

2. Une fonction entière de  $s \in \mathbb{C}$  est caractérisée par le fait que son développement en séries en  $s = 0$  admet un rayon infini de convergence.

où la fonction  $\chi : \mathbb{N} \mapsto \mathbb{C}$  est une fonction périodique et multiplicative ( $\chi(n_1 n_2) = \chi(n_1) \chi(n_2)$ ) particulière dite caractère de Dirichlet modulo- $N$ ,  $N$  étant la période de  $\chi$ . L'hypothèse est alors que les zéros non triviaux de ces fonctions sont tous sur la droite  $\Re(s) = 1/2$ .

En 1985, Miller et Bach ont prouvé, en supposant vraie l'hypothèse de Riemann généralisée, que si l'entier impair  $n$  est fortement premier pour toute base  $a$  entre 2 et  $2 \log^2(n)$  alors il est premier.

Ainsi comme le test de Miller-Rabin est polynômial, il est facile de voir que les  $E(2 \log^2(n)) - 1$  tests qui constituent l'algorithme de Miller-Bach impliquent une complexité polynômiale.

### 1.5.4 Fabrication de grands nombres premiers

On s'appuie sur un théorème classique en théorie des nombres, le théorème de Lucas que nous rappelons maintenant : le nombre  $n$  est premier, si et seulement si, il existe  $2 \leq \alpha \leq n - 1$ , tel que  $\alpha^{n-1} = 1 \pmod{(n)}$  et  $\alpha^{\frac{n-1}{p}} \neq 1 \pmod{(n)}$  pour tout diviseur premier  $p$  de  $n - 1$ .

Si on connaît la décomposition en facteur premier de  $n - 1$ , i.e., si on sait que  $n = 1 + p_1^{\nu_1} \dots p_k^{\nu_k}$ , il est facile d'avoir un test qui garantit la primalité de  $n$  : on choisit un  $\alpha$  au hasard et on calcule

$$\alpha^{n-1} \pmod{(n)}, \quad \alpha^{\frac{n-1}{p_1}} \pmod{(n)} \quad \dots \quad \alpha^{\frac{n-1}{p_k}} \pmod{(n)}$$

Si le test est positif on est sûr que  $n$  est premier, s'il est négatif alors on change de  $\alpha$ . Si au bout de plusieurs essais avec des  $\alpha$  différents les tests sont toujours négatifs, on a de fortes craintes que  $n$  ne soit pas premier et on change de  $n$  en jouant sur les exposants  $\nu_i$ .

L'idée pour obtenir un grand nombre premier  $p$  avec un élément primitif  $\alpha$  consiste à construire récursivement des nombres premiers de plus en plus grands par cette méthode en posant  $n = 1 + p_1^{\nu_1} \dots p_k^{\nu_k}$  où l'on sait que les  $p_i$  sont premiers. Une fois que l'on a trouvé des exposants  $\nu_i$  tels que  $n$  soit premier alors on rajoute  $n$  dans la liste des  $p_i$  et on continue l'opération avec  $k + 1$  nombres premiers cette fois.

### 1.5.5 Conclusion

Pour obtenir des grands entiers RSA  $n = pq$ , il vaut mieux générer les nombres premiers  $p$  et  $q$  au hasard, car ces derniers constituent la clé secrète. Une construction via le théorème de Lucas est à déconseiller. Ainsi les tests probabilistes sont adaptés. Puisque le test de Miller Rabin n'est

guère plus compliqué que celui de Fermat et qu'il conduit à des probabilités d'erreur arbitrairement faibles en le répétant suffisamment de fois, il est systématiquement utilisé.

Si l'on souhaite utiliser une exponentielle modulaire, il faut disposer d'un nombre premier  $p$  et d'un élément primitif  $\alpha$  modulo- $p$ . Comme  $p$  et  $\alpha$  sont publics, la fabrication par le théorème de Lucas est possible puisqu'elle donne en même temps de grands nombres premiers avec éléments primitifs.

Enfin, s'il s'agit de tester la primalité d'un nombre dont on ne maîtrise pas l'origine, il vaut mieux ne pas utiliser le test de Fermat. On pourrait avoir affaire à un nombre de Carmichael. Il faut utiliser le test de l'algorithme de Miller-Rabin.

## 1.6 Complexité

### 1.6.1 Introduction

L'un des buts de cette section est de comprendre pourquoi la preuve formelle de l'existence de fonctions à sens unique impliquerait  $\mathbf{P} \neq \mathbf{NP}$ , la célèbre conjecture en théorie de la complexité. De plus les liens entre cryptographie et complexité sont étroits et souvent à l'origine de nouvelles classes de complexité comme la classe  $\mathbf{RP}$  issue de l'algorithme de Miller-Rabin. Nous allons donner maintenant une description très informelle mais que nous espérons suggestive de diverses classes de complexité. Mais avant cela, prenons trois types de problèmes représentatifs des difficultés rencontrées. Les deux problèmes peuvent se traiter par des algorithmes, le dernier ne peut pas se traiter par un algorithme.

**Satisfaisabilité des formules booléennes** La donnée (on parle aussi d'instance) est un entier  $n$  et  $F$  une fonction booléenne de  $n$  variables booléennes ( $x_i \in \{0, 1\}$ ,  $i = 1, \dots, n$ )

$$(x_1, \dots, x_n) \mapsto F(x_1, \dots, x_n) \in \{0, 1\}.$$

où  $F$  est construite avec des expressions faisant intervenir les opérateurs logiques usuels (et, ou et négation). La question est : existe-t-il un  $(x_1, \dots, x_n)$  tel que  $F(x_1, \dots, x_n) = 1$ .

**Véracité des formules booléennes quantifiées** La donnée est un entier  $n$ ,  $F$  une fonction booléenne de  $n$  variables booléennes ( $x_i \in \{0, 1\}$ ,  $i = 1, \dots, n$ ) et la formule avec quantificateurs

$$\forall x_i, \exists x_j, \dots \quad F(x_1, \dots, x_n).$$

La question est alors : cette formule est-elle vraie ?

**Dixième problème de Hilbert** La donnée est un entier  $n$  et un polynôme à coefficients entiers de  $n$  variables  $P(x_1, \dots, x_n)$ . La question est alors : l'équation dite diophantienne  $P(x_1, \dots, x_n) = 0$  admet-elle une solution entière  $(x_1, \dots, x_n) \in \mathbb{Z}^n$ .

En 1971, Matjacevic a montré qu'il n'existe pas d'algorithme (dans toutes les définitions actuelles de cette notion) qui décide si une équation diophantienne admet une solution entière. Cela veut dire que ce problème est inaccessible à l'algorithmique.

En revanche les deux autres problèmes sont accessibles à l'algorithmique. Pour résoudre le premier problème, il suffit de calculer  $F$  pour tous les  $n$ -uplets possibles  $(x_1, \dots, x_n)$ . Si  $F$  est identiquement nulle la réponse est non et oui sinon. Pour résoudre le second, il suffit aussi de faire l'inventaire de toutes les possibilités. Nous voyons bien que, pour le troisième problème, il n'est pas possible d'explorer toutes les possibilités car l'ensemble des entiers étant infini, nous avons une infinité de cas à traiter.

Le premier problème est représentatif de la classe des problèmes dits de complexité **NP** car c'est un problème de difficulté maximale dans cette classe (problème dit **NP**-complet). Un problème est dit **NP** si l'on peut certifier ces instances positives en temps polynômial en  $\log(n)$  par un oracle. Nous verrons plus loin à quoi correspond un oracle.

Le second problème est représentatif de la classe des problèmes dits de complexité PSPACE car c'est un problème de difficulté maximale dans cette classe. Nous n'aborderons pas cette classe de problèmes qui admettent un algorithme nécessitant un espace mémoire polynômial en  $\log(n)$ .

Nous allons maintenant considérer les problèmes de décision, i.e. dont la réponse est oui ou non, en connexion directe avec les algorithmes que nous avons vus précédemment. Nous noterons formellement  $x$  les données d'un problème  $\mathcal{P}$ . Nous ne parlerons pas de machine de Turing. Aussi, les définitions qui suivent ne sont pas rigoureuses. Nous y avons remplacé la notion de Machine de Turing et de calculabilité par un autre terme que nous n'avons pas défini, celui d'algorithme, terme qui correspond plus à l'intuition. Pour un exposé rigoureux, nous renvoyons le lecteur à [4, 18].

### 1.6.2 Classe P

Le problème  $\mathcal{P}$  sera dit de classe **P** s'il existe un algorithme polynômial en temps qui le résout. Par polynômial, nous entendons polynômial par rapport à l'espace nécessaire pour coder les données  $x$ . Pour se faire une idée plus précise, prenons trois exemples.

Le premier problème est : les entiers  $m$  et  $n$  sont-ils premiers entre eux ?

Nous savons par l'algorithme d'Euclide calculer le pgcd. Ce calcul nécessite au plus  $E\left(\frac{\log(n)}{\log\left(\frac{1+\sqrt{5}}{2}\right)}\right)$  divisions pour  $m \leq n$  (voir le chapitre suivant).

Le second problème est plus instructif. Il montre l'équivalence entre le calcul en temps polynômial d'une famille de fonctions  $(f_n)_{n \in \mathbb{N}}$  de  $\{1, \dots, n\}$  dans lui-même et le problème de décision suivant. Les données sont l'entier  $n$  et deux autres entiers  $x$  et  $t$  plus petits que  $n$ . La question est : A-t-on  $f_n(x) \leq t$  ?

En effet si  $f_n(x)$  se calcule en temps polynômial par rapport à  $\log(n)$ , ce problème est de façon évidente dans  $\mathbf{P}$ . Supposons maintenant que ce problème est dans  $\mathbf{P}$ . Prenons  $n$  et  $x$  entiers avec  $1 \leq x \leq n$ , voyons comment calculer  $f_n(x)$  en temps polynômial. Pour cela, nous pouvons savoir en temps polynômial si  $f_n(x) \in [1, n/2]$  ou  $f_n(x) \in [n/2, n]$ . Si  $f_n(x) \in [1, n/2]$  on peut savoir en temps polynômial si  $f_n(x) \in [1, n/4]$  ou  $f_n(x) \in [n/4, n/2]$ . Si  $f_n(x) \in [n/2, n]$  on peut savoir en temps polynômial si  $f_n(x) \in [n/2, 3n/4]$  ou  $f_n(x) \in [3n/4, n]$ . On voit bien qu'avec de telles dichotomies, on sait en faisant appel  $s$ -fois à l'algorithme polynômial si  $f_n(x)$  est dans un intervalle de longueur au plus  $n/2^s$ . Il suffit maintenant de prendre  $s = 1 + E(\log_2(n))$  pour avoir la valeur exacte de  $f_n(x)$  puisque c'est un entier. On aura obtenu ainsi la valeur de  $f_n(x)$  en résolvant un nombre polynômial de problèmes polynômiaux. Donc le calcul de  $f_n(x)$  est polynômial en  $\log(n)$ .

Le troisième problème est :  $n$  est-il un nombre premier ? L'algorithme AKS répond à la question avec un temps en  $O(\log^{12}(n))$ .

### 1.6.3 Classe NP

Le problème de décision  $\mathcal{P}$  est dit calculable par un algorithme non déterministe et polynômial en temps, si et seulement si, il existe un algorithme ayant comme données de départ  $x$  et aussi  $y$  (fini et correspondant à l'oracle évoqué dans l'introduction de cette section), tel que pour toute instance  $x$  vérifiant  $\mathcal{P}(x)$  vrai alors il existe un certificat  $y(x)$  tel que cet algorithme ayant  $x$  et  $y(x)$  comme données calcule  $\mathcal{P}(x)$  vrai en temps polynômial par rapport à  $x$ .

Cette définition peut paraître obscure. Elle ne dit rien du comportement de cet algorithme quand on le lance avec un  $x$  et  $y$  arbitraire. Il peut très bien ne pas s'arrêter ou s'arrêter mais après un temps gigantesque. Tout ce que nous demandons est que si l'on part d'une instance positive  $x$  et si l'on choisit bien le complément  $y(x)$  des données de départ, l'algorithme montre que  $\mathcal{P}(x)$  est vrai en temps polynômial. Le temps est polynômial par rapport aux données brutes  $x$ , celles que l'on connaît en excluant les autres données  $y(x)$  dont nous connaissons l'existence mais que nous sommes a priori bien in-

capables de calculer. C'est pourquoi on parle d'algorithme non-déterministe car le bon certificat  $y(x)$  associé l'instance positive  $x$  du problème n'en fait pas partie. La classe **NP** est l'ensemble des problèmes de décision calculables par un algorithme non-déterministe polynômial en temps. A cause de la disymétrie entre  $\mathcal{P}(x)$  vraie et  $\mathcal{P}(x)$  faux, on définit **coNP** l'ensemble des problèmes  $\mathcal{P}$  donc le complémentaire est dans **NP** (on remplace instances positives par instances négatives dans la définition). Nous allons maintenant prendre deux exemples qui montrent bien que cette définition un peu obscure provient en fait de problèmes algorithmiques concrets.

Montrons que le problème de la factorisation est dans **NP**. Pour cela nous le traduisons en un problème de décision : les données sont deux entiers  $n$  et  $M < n$ . La question est : existe-t-il un diviseur de  $n$  plus petit que  $M$  et  $> 1$ .

Par dichotomie successive, on voit que si l'on sait résoudre ce problème en temps polynômial, disons en  $p(\log(n))$  avec  $p$  polynôme, on sait trouver un diviseur de  $n$  en temps polynômial. On part de  $M = E(n/2)$ , un premier calcul donne la position du diviseur éventuel soit dans  $[2, E(n/2)[$  ou  $[E(n/2), n]$ , i.e. dans un intervalle de longueur au plus  $n/2$ . Un second calcul va le localiser dans un intervalle de longueur au plus  $n/4$ . Après  $s$  calculs on a localisé le diviseur dans un intervalle de longueur au plus  $n/2^s$ . Ainsi avec  $s = 1 + E(\log_2(n))$  on aura localisé le diviseur dans un intervalle de longueur au plus de 1, i.e. on aura donc le diviseur au bout du temps  $p(\log(n)) \log_2(n)$ .

Montrons que notre problème de décision est dans **NP**. En effet, il suffit pour les instances  $x = (n, M)$  positives (i.e., telles qu'il existe un diviseur de  $n$  plus petit que  $M$ ) de prendre un diviseur de  $n$  plus petit que  $M$  que nous noterons  $y(n, M)$ . L'algorithme de vérification consiste simplement à diviser  $n$  par  $y(n, M)$  et ainsi on vérifie que  $n$  a bien un diviseur non trivial plus petit que  $M$ . Montrons aussi que ce problème est dans **coNP**. C'est un peu plus compliqué car on s'intéresse à  $x = (n, M)$  tel qu'il n'existe pas de diviseur de  $n$  plus petit que  $M$ . Pour cela, la structure de  $y$  est plus lourde. En effet, il faut que  $y$  comporte les données suivantes : la décomposition de  $n$  en facteurs premiers  $n = \prod_{i=1}^k p_i^{\nu_i}$ . Avec ces données supplémentaires  $y = (p_i, \nu_i)_{i=1, \dots, k}$  nous pouvons proposer l'algorithme suivant : vérification via AKS que les  $k$  nombres  $p_i$  sont bien des nombres premiers; vérification que chaque  $p_i$  est bien plus grand que  $M$ . On laisse au lecteur le soin de montrer que notre algorithme est en temps polynômial par rapport à  $\log(n)$ .

On peut utiliser la même démarche pour montrer que le logarithme discret est dans **NP** et aussi dans **coNP**. Pour  $p$  premier,  $\alpha$  primitif modulo- $p$  et

$n < p$  on définit la fonction  $\log$  ainsi

$$(p, \alpha, n) \mapsto \log(p, \alpha, n) = \begin{cases} m & \text{si } p \text{ est premier, } \alpha \text{ primitif modulo-}p \\ & \text{et } m \text{ l'unique entier tel que} \\ & 0 < m < p \text{ et } \alpha^m = n \pmod{p} \\ 0 & \text{sinon.} \end{cases}$$

et le problème de décision suivant : les données sont  $p$  et les nombres  $\alpha, n$  et  $t$  plus petits que  $p$ ; la question est " A-t-on  $\log(p, \alpha, n) < t$  ? "

### 1.6.4 Classe **RP**

Il s'agit de problèmes pouvant être résolus par des algorithmes probabilistes polynômiaux (ne pas confondre probabiliste avec non-déterministe, ici). Un problème  $\mathcal{P}$  est dans **RP**, si et seulement si, il existe des polynômes  $p(n)$  et  $q(n)$  où  $n$  la taille des données<sup>3</sup>  $x$  et un algorithme ayant comme données de départ  $x$  et  $y$  (certificat) telles que

- les instances  $x$  négatives de  $\mathcal{P}$  ( $\mathcal{P}(x)$  faux) sont caractérisées par le fait que pour tout  $y$  de taille plus petite que  $p(n)$ , l'algorithme partant de  $x$  et  $y$  donne en un temps plus petit que  $q(n)$  la réponse  $\mathcal{P}(x)$  faux.
- si  $x$  est une instance positive de  $\mathcal{P}$  ( $\mathcal{P}(x)$  vrai) alors pour au moins la moitié des certificats  $y$  de taille plus petite que  $p(n)$ , l'algorithme fournit la réponse vraie en un temps inférieur à  $q(n)$ .

Notons d'abord que **RP** est contenu dans **NP**. Ensuite, cette définition est faite sur mesure pour le test de Miller-Rabin de primalité.

Détaillons un peu ce problème. La question est : l'entier  $x$  est-il composé? Les variables  $y$  correspondent ici à un entier entre 2 et  $x$ , donc le polynôme  $p(n)$  où  $n = \log(x)$  n'est autre que l'identité : on ne fait que doubler au plus la taille des données en rajoutant le certificat  $y$ . Le fait que  $x$  ne soit pas composé, c'est à dire que  $x$  soit premier, est équivalent au fait que  $x$  soit fortement premier pour toutes les bases  $y$  entre 2 et  $x - 1$ . De plus, l'algorithme qui teste si  $x$  est fortement premier en base  $y$  n'est autre que le test de Miller-Rabin, il est de complexité polynômiale en la taille de  $x$ , le polynôme  $q$  correspond donc à la complexité du test de Miller-Rabin. Ainsi le premier point de la définition est vérifié. Le second point découle du fait que si  $x$  est composé alors pour au moins les 3/4 des  $y$  entre 2 et  $x - 1$ ,  $x$  n'est pas fortement premier en base  $y$ .

---

3. Si  $x$  est entier,  $n$  correspond donc à  $\log(x)$ .

### 1.6.5 Fonctions à sens unique et la conjecture $\mathbf{P} \neq \mathbf{NP}$

L'existence de fonctions à sens unique est une conjecture aussi difficile que  $\mathbf{P} \neq \mathbf{NP}$ . En effet reprenons la définition de la section 1.1 où nous supposons que chaque  $f_n$  est une bijection de  $A_n = \{1, \dots, n\}$  dans  $B_n = \{1, \dots, n\}$ . On considère alors la famille  $(f_n)_{n \in \mathbb{N}}$ . Le fait que les  $f_n$  soient faciles à calculer se formalise alors via le problème noté  $\mathcal{F}$  suivant : les données sont un entier  $n$  et deux autres entiers  $x$  et  $t$  entre 1 et  $n$ . La question est : A-t-on  $f_n(x) \leq t$ ? Si pour chaque  $n$  le calcul de  $f_n(x)$  est polynômial, le problème  $\mathcal{F}$  est trivialement dans  $\mathbf{P}$ . Supposons donc  $\mathcal{F}$  dans  $\mathbf{P}$ .

De même, le calcul de l'inverse des  $f_n$  est associé au problème de décision suivant noté  $\mathcal{F}^{-1}$  : les données sont un entier  $n$  et deux autres entiers  $x$  et  $t$  entre 1 et  $n$ ; la question est : a-t-on  $f_n^{-1}(x) \leq t$ ?

Clairement,  $\mathcal{F}^{-1}$  est dans  $\mathbf{NP}$ . En effet, il suffit de prendre comme certificat  $y = f_n^{-1}(x)$ . Le fait que le problème  $\mathcal{F}^{-1}$  soit difficile, i.e., que les  $f_n$  soient à sens unique, se traduit donc par le fait que  $\mathcal{F}^{-1}$  n'est pas dans  $\mathbf{P}$  (car sinon le calcul de  $f_n^{-1}$  serait polynômial, voir le second problème de la section 1.6.2). Comme  $\mathcal{F}^{-1}$  est nécessairement dans  $\mathbf{NP}$ , on voit que l'existence d'une fonction à sens unique implique  $\mathbf{P} \neq \mathbf{NP}$ .





# Chapitre 2

## Théorie des nombres

Nous reprenons ici certains résultats qui interviennent dans le chapitre sur la cryptographie. Les deux premières sections s'appuient en partie sur le premier chapitre de [29]. Les autres sections abordent la théorie analytique des nombres et la distribution des nombres premiers. Pour le rédiger nous nous sommes souvent inspirés des cours de Jean-Benoît Bost sur les séries de Dirichlet et les nombres premiers [8, 9].

En complément le “Que sais-je” sur les nombres premiers [28] donne en dernière partie un éclairage probabiliste ainsi qu’une preuve élémentaire mais assez difficile du théorème des nombres premiers. Nous recommandons aussi l’excellent livre de vulgarisation de Jean-Paul Delahaye sur les nombres premiers [13] qui inclut un chapitre entier sur la cryptographie. On pourra aussi consulter l’Encyclopaedia Universalis qui comportent d’excellents articles sur des sujets connexes. Enfin un lecteur voulant vraiment approfondir le sujet pourra consulter le livre classique dû à Hardy et Wright [20].

### 2.1 PGCD

#### 2.1.1 $\mathbb{Z}_n$ et $\mathbb{Z}_n^*$

Deux entiers  $a$  et  $b$  sont congrus modulo un entier  $n$ , si et seulement si, leur différence  $a - b$  est un multiple de  $n$ . On note alors :  $a = b \pmod{n}$ . La relation de congruence modulo  $n$  est une relation d’équivalence. On note  $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$  l’ensemble des classes modulo  $n$ . Il y en a  $n$  ( $\#\mathbb{Z}_n = n$ ) et on identifie  $\mathbb{Z}_n$  à l’ensemble  $\{0, 1, \dots, n-1\}$ .  $\mathbb{Z}_n$  est muni d’une structure naturelle d’anneau pour l’addition et la multiplication. En particulier  $\mathbb{Z}_n$  muni de l’addition  $+$  est un groupe commutatif (on dit aussi abélien). En revanche  $\mathbb{Z}_n$  n’est pas en général un groupe pour la multiplication (le produit de 3 par

2 dans  $\mathbb{Z}_6$  donne 0). On note  $\mathbb{Z}_n^*$  l'ensemble des éléments inversibles de  $\mathbb{Z}_n$  pour la multiplication. Nous allons voir que, si  $n$  est premier,  $\mathbb{Z}_n^* = \mathbb{Z}_n/\{0\}$  et  $\mathbb{Z}_n$  est un corps.

Soit  $k$  inversible modulo  $n$ , i.e.,  $k \in \mathbb{Z}_n^*$ . Supposons que  $k$  et  $n$  admettent un diviseur non trivial  $a > 1$ . On pose  $k = pa$  et  $n = qa$  avec  $p$  et  $q$  entier. Alors,  $kq = paq = pn = 0 \pmod{n}$ . Ce qui n'est pas possible car  $k$  est inversible et donc nécessairement  $q = 0 \pmod{n}$ . Ainsi, tout élément de  $\mathbb{Z}_n^*$  est un entier premier avec  $n$  (un entier n'ayant pas de diviseur commun avec  $n$ , ou encore un entier dont le pgcd avec  $n$  est 1). La réciproque est vraie :  $\mathbb{Z}_n^*$  correspond exactement à l'ensemble des entiers entre 1 et  $n - 1$  premiers avec  $n$ , i.e., qui n'admettent pas de diviseur commun avec  $n$  autre que 1. La preuve de ce résultat repose sur l'algorithme d'Euclide et l'identité de Bezout.

### 2.1.2 Algorithme d'Euclide

L'algorithme d'Euclide permet de calculer efficacement les inverses modulo  $n$  via la relation de Bezout. Soient donc deux entiers strictement positifs  $k < n$ . L'algorithme de division d'Euclide est composé des divisions successives suivantes :

$$\begin{aligned} n &= kq_0 + r_0, & r_0 < k \\ k &= r_0q_1 + r_1, & r_1 < r_0 \\ r_0 &= r_1q_2 + r_2, & r_2 < r_1 \\ &\vdots \\ r_{m-2} &= r_{m-1}q_m + r_m, & r_m < r_{m-1} \\ r_{m-1} &= r_mq_{m+1} + r_{m+1}, & 0 = r_{m+1} < r_m \end{aligned}$$

où la suite  $(n, k, r_0, r_1, \dots, r_m, r_{m+1})$  est strictement décroissante et arrive à zéro avec  $r_{m+1} = 0$  (ce qui définit l'indice  $m$ ). Il est facile de voir que le pgcd est  $r_m$ . En effet si  $p$  divise  $n$  et  $k$  alors il divise  $r_0$  (première division), mais aussi  $r_1$  (seconde division), ..., et enfin  $r_m$  (avant dernière division). Comme  $r_m$  divise  $r_{m-1}$  (dernière division),  $r_m$  divise aussi  $r_{m-2}$  (avant dernière division), ..., en enfin  $k$  (seconde division) et  $n$  (première division). L'algorithme d'Euclide calcule donc le pgcd.

Il donne aussi l'inverse de  $k$  modulo  $n$ . Il donne même plus avec l'identité de Bezout : pour tout  $1 < k < n$ , il existe  $u$  et  $v$  dans  $\mathbb{Z}$  tels que

$$un + vk = \text{pgcd}(n, k).$$

Il suffit de résoudre le système formé par les  $m + 1$  premières divisions par rapport aux  $m + 1$  restes  $r_i$ ,  $i = 0, \dots, m$ . Il s'agit d'un système linéaire de la forme

$$A \begin{pmatrix} r_0 \\ r_1 \\ r_2 \\ \vdots \\ r_m \end{pmatrix} = \begin{pmatrix} n - kq_0 \\ k \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

où la matrice  $A$  est à coefficients entiers, triangulaire inférieure et avec 1 sur la diagonale. Donc son inverse est aussi une matrice à coefficients entiers (on appelle ce type de matrices, des matrices uni-modulaires, on les retrouve très souvent et elles jouent un rôle fort important dans de nombreux domaines, ...). Donc chaque  $r_i$  est combinaison linéaire à coefficients dans  $\mathbb{Z}$  de  $k$  et de  $n$  et en particulier  $r_m = \text{pgcd}(n, k) = un + vk$  avec  $u$  et  $v$  dans  $\mathbb{Z}$ .

Si  $n$  et  $k$  sont premiers entre eux, alors il existe  $u$  et  $v$  dans  $\mathbb{Z}$  tels que  $un + vk = 1$ , ce qui s'écrit aussi  $vk = 1 \pmod{(n)}$  donc  $v$  est l'inverse de  $k$  pour la multiplication dans  $\mathbb{Z}_n$ , et donc  $k \in \mathbb{Z}_n^*$ .

### 2.1.3 Complexité de l'algorithme d'Euclide

Evaluons le nombre  $D$  de divisions de l'algorithme d'Euclide en fonction de la taille de  $n$ . L'algorithme sera le plus long lorsque chaque quotient  $q_i$  vaut 1 avec  $r_m = 1$  et  $r_{m+1} = 0$ . Ainsi, on a

$$r_i = r_{i+1} + r_{i+2}, \quad i = 0, \dots, m - 2$$

et

$$k = r_0 + r_1, \quad n = k + r_0$$

En prenant la récurrence précédente en sens rétrograde avec les  $i$  décroissants, on voit que  $n$  correspond au  $(m + 4)$ -ième nombre de la suite

$$F_j = F_{j-1} + F_{j-2}$$

avec comme départ de la récurrence,  $F_0 = 0$  et  $F_1 = 1$ . Il s'agit de la suite de Fibonacci où apparaît le nombre d'or  $\phi = (1 + \sqrt{5})/2$ . En effet, on sait (faire une transformée en  $Z$ , classique en contrôle linéaire) que la solution générale d'une récurrence linéaire est obtenue par combinaison linéaire des puissances des racines de l'équation caractéristique

$$Z^2 = Z + 1.$$

Les racines sont le nombre d'or  $\phi$  et  $\psi = 1 - \phi$ . Aussi  $F_j = a\phi^j + b\psi^j$  où  $a$  et  $b$  sont déterminés par les conditions initiales  $F_0$  et  $F_1$ . Ainsi

$$F_j = (\phi^j - \psi^j)/\sqrt{5}.$$

Comme  $F_{m+4} = n$  dans le cas le plus défavorable, le nombre  $D = m + 2$  de divisions effectives est relié à  $n$  via l'inéquation

$$n \geq F_{D+2} = (\phi^{D+2} - \psi^{D+2})/\sqrt{5}$$

Un petit calcul montre que  $D \leq \log_\phi(n)$ . Ainsi, l'algorithme d'Euclide est polynômial. L'estimation précédente est due à Lamé (1845).

## 2.2 La fonction d'Euler $\varphi(n)$

Pour tout entier  $n > 1$ , on note  $\varphi(n)$  le nombre d'entiers entre 1 et  $n - 1$  premiers avec  $n$ . Ainsi, par définition,

$$\varphi(n) = \#\mathbb{Z}_n^*.$$

Nous voyons que “ $n$  premier” est équivalent à “ $\varphi(n) = n - 1$ ”. Nous allons voir que  $\varphi$  est une fonction multiplicative, au sens où, si  $n$  et  $m$  sont premiers entre eux,  $\varphi(mn) = \varphi(n)\varphi(m)$ . Ce type de fonctions joue un grand rôle en arithmétique et dans les séries de Dirichlet (cf. la fin de ce chapitre avec les produits eulériens).

### 2.2.1 Fermat et Euler

**Théorème 1** (Fermat-Euler). *Si  $a$  est premier avec  $n$  alors  $a^{\varphi(n)} = 1 \pmod{n}$ .*

La preuve est très simple. L'hypothèse sur  $a$  se traduit par  $a \in \mathbb{Z}_n^*$ . Donc l'application  $x \mapsto ax$  de  $\mathbb{Z}_n^*$  dans lui-même est une bijection. Il s'agit d'un simple changement d'indexation des éléments de  $\mathbb{Z}_n^*$  via le changement de variable  $y = ax$  :

$$\prod_{x \in \mathbb{Z}_n^*} x = \prod_{x \in \mathbb{Z}_n^*} ax \pmod{n}$$

Mais  $\prod_{x \in \mathbb{Z}_n^*} ax = a^{\varphi(n)} \prod_{x \in \mathbb{Z}_n^*} x$ . D'où nécessairement  $a^{\varphi(n)} = 1 \pmod{n}$ .

Lorsque  $n$  est premier  $\varphi(n) = n - 1$  et tout  $a$  entre 1 et  $n - 1$  est premier avec  $n$ . On a donc le corollaire suivant :

**Théorème 2** (petit théorème de Fermat). *Si  $n$  est premier et si  $a$  entier entre 1 et  $n - 1$ , alors  $a^{n-1} = 1 \pmod{n}$ .*

Ainsi l'inverse de  $a$  dans  $\mathbb{Z}_n^*$  est  $a^{n-2}$ . On a aussi un dernier résultat (| veut dire "divise")

**Théorème 3** (Euler).

$$\sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d) = n$$

La somme porte sur tous les diviseurs de  $n$  entre 1 et  $n$ . Lorsque  $n$  est premier cette somme est réduite à  $d = 1$  et  $d = n$  ( $\varphi(1) = 1$  et  $\varphi(n) = n - 1$ ).

La preuve de ce théorème est la suivante : Pour  $1 \leq d \leq n$ , on pose ( $\#$  veut dire cardinal)

$$\psi(d, n) = \#\{x \in \mathbb{Z}_n \mid \text{pgcd}(x, n) = d\}.$$

Si  $d$  divise  $n$  alors  $\psi(d, n) \neq 0$  sinon  $\psi(d, n) = 0$ . Donc  $n = \sum_{d=1}^n \psi(d, n) = \sum_{d|n} \psi(d, n)$ . Mais,  $\psi(d, n) = \varphi(n/d)$  si  $d$  divise  $n$ . En effet, il suffit de diviser par  $d$ , pour mettre en bijection les nombres  $x$  tels que  $\text{pgcd}(x, n) = d$  et les nombres  $y$  tels que  $\text{pgcd}(y, n/d) = 1$ . Ainsi on a

$$n = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d).$$

### 2.2.2 Théorème chinois

**Théorème 4** (théorème chinois). *Soient deux entiers  $p$  et  $q \geq 1$  et premiers entre eux. Alors les anneaux  $\mathbb{Z}_p \times \mathbb{Z}_q$  et  $\mathbb{Z}_{pq}$  sont isomorphes.*

Considérons l'application  $\pi : \mathbb{Z} \mapsto \mathbb{Z}_p \times \mathbb{Z}_q$  qui à  $x \in \mathbb{Z}$  associe  $(x \bmod p, x \bmod q)$ . C'est un homomorphisme d'anneau :  $\pi(x+y) = \pi(x) + \pi(y)$  et  $\pi(xy) = \pi(x)\pi(y)$ . Le noyau de  $\pi$ , i.e., l'ensemble des  $x \in \mathbb{Z}$  tels que  $\pi(x) = 0$ , i.e., tels que  $x = 0 \bmod p$  et  $x = 0 \bmod q$  n'est autre que l'ensemble des multiples de  $pq$  car  $p$  et  $q$  sont premiers entre eux. De plus,  $\pi$  est surjectif, car  $(1, 0)$  et  $(0, 1)$  sont dans  $\pi(\mathbb{Z})$  : comme  $p$  et  $q$  sont premiers entre eux, il existe  $u$  et  $v$  dans  $\mathbb{Z}$  tel que  $up + vq = 1$ . Donc  $\pi(vq) = (1, 0)$  et  $\pi(up) = (0, 1)$ ; si  $(n, m) \in \mathbb{Z}_p \times \mathbb{Z}_q$  ( $n \in \{0, \dots, p-1\}$  et  $m \in \{0, \dots, q-1\}$ ) on a

$$\begin{aligned} \pi(nvq + mup) &= \pi(nvq) + \pi(mup) \\ &= n\pi(vq) + m\pi(up) = n(1, 0) + m(0, 1) = (n, m). \end{aligned}$$

Ainsi,  $\mathbb{Z}/pq\mathbb{Z} = \mathbb{Z}_{pq}$  et  $\mathbb{Z}_p \times \mathbb{Z}_q$  sont isomorphes.

En particulier, ils ont le même nombre d'éléments inversibles pour la multiplication. Or  $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_q$  inversible, si et seulement si,  $x$  l'est dans  $\mathbb{Z}_p$  et  $y$  dans  $\mathbb{Z}_q$ . Ainsi,  $\mathbb{Z}_{pq}^*$  est isomorphe à  $\mathbb{Z}_p^* \times \mathbb{Z}_q^*$ . Donc  $\varphi(pq) = \varphi(p)\varphi(q)$ . On a prouvé le corollaire suivant.

**Corollaire 1.** *Si  $p$  et  $q$  sont premiers entre eux, alors  $\varphi(pq) = \varphi(p)\varphi(q)$*

Comme pour  $p$  premier et pour tout entier  $\alpha > 0$ ,  $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ . On en déduit directement l'autre corollaire suivant.

**Corollaire 2.** *Si  $n$  admet comme décomposition en facteurs premiers  $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$  alors*

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k-1})$$

### 2.2.3 Déchiffrement RSA

On a admis au chapitre précédent l'identité qui est à la base du déchiffrement RSA via la clé secrète  $d$  du message chiffré  $M^e$ . :

$$\forall M \in \{0, 1, \dots, n-1\}, \quad M^{ed} = M \pmod{(n)}$$

dès que

- $n = pq$  où  $p$  et  $q$  sont deux nombres premiers
- $e \in \{1, \dots, \varphi(n-1)\}$  inversible modulo  $\varphi(n)$  et d'inverse  $d$  appartenant à  $\{1, \dots, \varphi(n-1)\}$ . On rappelle que  $ed = 1 + k\varphi(n)$  pour un certain entier positif  $k$ .

Voici une preuve de cette identité. Si  $M$  et  $n$  sont premiers entre eux, alors par le théorème d'Euler-Fermat  $M^{\varphi(n)} = 1 \pmod{(n)}$ . Ainsi

$$M^{ed} = M^{1+k\varphi(n)} = M \pmod{(n)}.$$

Supposons maintenant que  $M$  et  $n$  ne soient pas premiers entre eux. Quitte à échanger les rôles de  $p$  et  $q$ , on a  $M = kp$  avec  $k \in \{1, \dots, q-1\}$ . Donc  $M$  est premier avec  $q$ . Ainsi, toujours via le théorème d'Euler-Fermat,  $M^{\varphi(q)} = 1 \pmod{(q)}$ . Comme  $\varphi(n) = \varphi(p)\varphi(q)$  ( $p$  et  $q$  sont 1er entre eux), on en déduit que  $M^{\varphi(n)} = M^{\varphi(p)\varphi(q)} = 1 \pmod{(q)}$ . Donc  $M^{ed} = M^{1+k\varphi(n)} = M \pmod{(q)}$ . Par ailleurs, on a  $M = 0 \pmod{(p)}$ , donc  $M^{ed} = 0 \pmod{(p)}$ . Ainsi l'image par l'homomorphisme d'anneau  $\pi : \mathbb{Z} \mapsto \mathbb{Z}_p \times \mathbb{Z}_q$  de  $M$  et  $M^{ed}$  sont les mêmes :  $\pi(M) = \pi(M^{ed}) = (0, M)$ . Puisque  $\pi(M^{ed} - M) = 0$ ,  $M^{ed} - M$  appartient au noyau de  $\pi$  qui n'est autre que l'ensemble des multiples de  $n = pq$ . Ainsi  $M^{ed} = M \pmod{(n)}$ .

### 2.2.4 Éléments primitifs

**Théorème 5** (élément primitif). *Si  $p$  est premier alors, le groupe  $(\mathbb{Z}_p^*, \times)$  est cyclique, i.e., il est de la forme*

$$\mathbb{Z}_p^* = \{1, a, a^2, \dots, a^{p-2}\}$$

où  $a \in \mathbb{Z}_p^*$  est appelé élément primitif (non nécessairement unique).

Comme l'anneau  $(\mathbb{Z}_p, +, \times)$  est un corps commutatif, un polynôme de degré  $q$  à coefficients dans  $\mathbb{Z}_p$  admet aux plus  $q$  racines distinctes dans  $\mathbb{Z}_p$  (il peut en avoir moins). Soit  $x \in \mathbb{Z}_p^*$ . On note  $d$  son ordre, i.e., le plus petit entier  $d > 0$  tel que  $x^d = 1 \pmod{p}$ . Le petit théorème de Fermat implique que  $d$  est bien défini et  $d \leq p-1$ . On a même plus. Puisque  $x^{p-1} = 1 \pmod{p}$ , on a, pour tout entier  $n$ ,  $x^{p-1-nd} = 1 \pmod{p}$ . Donc nécessairement  $d$  divise  $p-1$  (sinon, le reste  $r < d$  non nul de la division euclidienne de  $p-1$  par  $d$  donnerait  $x^r = 1 \pmod{p}$ , ce qui est impossible par définition de  $d$ ). On sait aussi, que les  $d$  éléments

$$\{1, x, x^2, \dots, x^{d-1}\}$$

sont distincts (sinon,  $x^{d_1} = x^{d_2}$  avec  $1 \leq d_1 < d_2 \leq d-1$  impliquerait que  $x^{d_2-d_1} = 1 \pmod{p}$  avec  $0 < d_2 - d_1 < d$ , en contradiction avec la définition de  $d$ ). Les  $x^i$  ( $i = 0, \dots, d-1$ ) constituent les  $d$  racines distinctes du polynôme  $X^d - 1$  dans  $\mathbb{Z}_p$ . De plus tout élément  $y \in \mathbb{Z}_p^*$  d'ordre  $d$  est racine de  $X^d - 1$  donc s'écrit sous la forme d'une puissance de  $x$ ,  $y = x^s$  avec un certain exposant  $s$ . Il est alors clair, puisque  $d$  est l'ordre de  $y$  que  $y^d = x^{sd} = 1 \pmod{p}$  implique que  $s$  et  $d$  sont premiers entre eux. Ainsi, lorsque l'ensemble des éléments d'ordre  $d$  est non vide, il contient au plus  $\varphi(d)$  éléments, le nombre d'entiers  $s$  plus petits que  $d$  et premiers avec lui. Notons maintenant  $N_d$  le nombre des éléments d'ordre  $d$ . Puisque tout élément de  $\mathbb{Z}_p^*$  est d'ordre au plus  $p-1$ , on a

$$\sum_{d=1}^{p-1} N_d = p-1.$$

Maintenant comme  $N_d = 0$  si  $d$  ne divise pas  $p-1$ , on a

$$\sum_{d|(p-1)} N_d = p-1.$$

Mais on a vu que soit  $N_d \leq \varphi(d)$ . Donc

$$p-1 = \sum_{d|(p-1)} N_d \leq \sum_{d|(p-1)} \varphi(d)$$



avec une inégalité stricte si l'un des  $N_d$  vaut 0. Par le théorème d'Euler on sait que

$$\sum_{d|p-1} \varphi(d) = p - 1$$

Donc nécessairement pour tout diviseur  $d$  de  $p - 1$  on a  $N_d = \varphi(d)$ . En particulier,  $N_{p-1} = \varphi(p - 1) \geq 1$ . Il existe donc au moins un élément de  $\mathbb{Z}_p^*$  d'ordre  $p - 1$ .

Noter qu'une bonne partie des raisonnements précédents sur les ordres ne font pas intervenir le fait que  $p$  soit premier.

### 2.2.5 Théorème de Lucas

Ce théorème permet de certifier la primalité d'un nombre  $n$  dès que l'on connaît la décomposition en facteurs premiers de  $n - 1$ .

**Théorème 6** (Lucas). *Le nombre  $n$  est premier, si et seulement si, il existe  $\alpha \in \mathbb{Z}_n^*$  tel que  $\alpha^{n-1} = 1 \pmod{n}$  et  $\alpha^{\frac{n-1}{p}} \neq 1 \pmod{n}$  pour tout diviseur premier de  $n - 1$ .*

Si  $n$  est premier alors il suffit de prendre pour  $\alpha$  un élément primitif modulo  $n$ . Inversement, si un tel élément  $\alpha$  existe alors il est forcément d'ordre  $n - 1$  dans  $\mathbb{Z}_n^*$ . Ainsi  $\#\{1, \alpha, \dots, \alpha^{n-2}\} = n - 1$  et  $\{1, \alpha, \dots, \alpha^{n-2}\} \subset \mathbb{Z}_n^*$ . Or dans tous les cas  $\#\mathbb{Z}_n^* \leq n - 1$ , donc ici  $\#\mathbb{Z}_n^* = n - 1$ , soit  $\varphi(n) = n - 1$ . Cela signifie  $n$  premier (cf. corollaire 2).

## 2.3 Fonctions génératrices

Voici ce qu'écrit Jean Dieudonné dans son article sur la théorie analytique des nombres de l'Encyclopaedia Universalis :

“ Ce qu'on appelle la théorie analytique des nombres ne peut pas être considéré comme une théorie mathématique au sens usuel qu'on donne à ces mots, c'est-à-dire un système organisé de définitions et de théorèmes généraux accompagné d'applications à des exemples importants. Il s'agit au contraire ici presque exclusivement de problèmes particuliers qui se posent en arithmétique et qui, pour la plupart, consistent à étudier l'allure à l'infini de certaines fonctions définies par des conditions de nature arithmétique : par exemple le nombre  $\pi(x)$  de nombres premiers  $p \leq x$  ou le nombre  $U(n)$  des solutions de l'équation  $(x_1)^2 + (x_2)^2 = n$  en nombres entiers  $(x_1, x_2)$ . Depuis 1830, on a imaginé, pour résoudre ces questions, des méthodes d'une extraordinaire ingéniosité qui consistent

à associer aux fonctions arithmétiques étudiées des fonctions analytiques auxquelles on peut appliquer la théorie de Cauchy ou l'analyse harmonique ; mais, malgré les succès spectaculaires obtenus par ces méthodes, on ne peut dire que l'on en comprenne vraiment les raisons profondes. ”

Cependant, quelques exemples permettent de saisir tout l'intérêt de la méthode et pourquoi les fonctions de variables complexes apparaissent naturellement. La méthode consiste à associer à une suite d'entiers  $a_n$  (définis par une construction arithmétique (nombre de solutions d'une équation dépendant de  $n$ , cardinal d'un certain ensemble d'entiers plus petits que  $n$ , ...)) une série formelle. Le plus simple est de considérer la série

$$S(X) = \sum_{n \geq 0} a_n X^n$$

mais il faut être souvent plus malin comme nous le verrons avec les nombres premiers  $p_n$ . Suite à des manipulations astucieuses on propose une autre écriture de cette série que l'on manipule alors avec les règles usuelles de calcul sur les fonctions de la variable complexe (dérivée, résidu, intégrale de Cauchy, ...). Le but est très souvent d'avoir des informations sur les  $a_n$ , pour des grands indices  $n$ , informations souvent reliées aux singularités de la fonction analytique attachée à la série  $S$ .

Prenons maintenant un exemple simple mais déjà non trivial. Supposons que  $a_n$  soit le nombre de solutions en entiers  $\geq 0$  de l'équation diophantienne à trois variables  $x + 2y + 3z = n$ . Alors nous allons voir que

$$\sum_{n \geq 0} a_n X^n = \frac{1}{(1-X)(1-X^2)(1-X^3)}.$$

En effet, pour  $|X| \leq 1$ , On a

$$\frac{1}{1-X} = 1 + X + X^2 + X^3 + \dots$$

Donc

$$\frac{1}{(1-X)(1-X^2)(1-X^3)} = \left( \sum_{i_1 \geq 0} X^{i_1} \right) \left( \sum_{i_2 \geq 0} X^{2i_2} \right) \left( \sum_{i_3 \geq 0} X^{3i_3} \right).$$

En développement ce triple produit on voit que le terme  $X^n$  apparaît autant de fois que le nombre de triplets  $(i_1, i_2, i_3)$  tels que  $i_1 + 2i_2 + 3i_3 = n$ , i.e.,  $a_n$ .

Maintenant pour calculer  $a_n$ , il vaut mieux passer par la décomposition en éléments simples de  $\frac{1}{(1-X)(1-X^2)(1-X^3)}$ . Ainsi les nombres complexes apparaissent naturellement car les racines de  $X^3 = 1$  sont  $1, j = \exp(2i\pi/3)$  et

$j^2 = \exp(-2i\pi/3)$ . Faisons ce petit calcul (avec l'aide de Maple ou Mathematica) :

$$\frac{1}{(1-X)(1-X^2)(1-X^3)} = \frac{1}{6(1-X)^3} + \frac{1}{4(1-X)^2} + \frac{17}{72(1-X)} \\ + \frac{1}{8(1+X)} + \frac{1}{9(1-jX)} + \frac{1}{9(1-j^2X)}.$$

Il suffit maintenant d'utiliser la formule  $a_n = \frac{d^n S}{dX^n}(0)/(n!)$  et de calculer cette dérivée  $n$ -ième sur la décomposition en éléments simples. En utilisant l'identité

$$\frac{d^n}{dX^n} \left( \frac{1}{(1-\beta X)^\alpha} \right)_{X=0} = \beta^n \alpha(\alpha+1)\dots(\alpha+n-1)$$

on obtient

$$a_n = \frac{(n+1)(n+2)}{12} + \frac{n+1}{4} + \frac{17}{72} + \frac{(-1)^n}{8} + \frac{j^n + j^{2n}}{9}.$$

Remarquons maintenant que si nous nous intéressons à une estimation de  $a_n$  pour  $n$  grand, il suffit de considérer le pôle de degré le plus élevé  $X = 1$ , les autres donnant des contributions en  $n$  au plus. Ainsi, la structure des singularités de  $S(X)$ , i.e., de ces pôles, donnent les asymptotiques de  $a_n$  pour  $n$  grand. Ce phénomène est très général comme le montre l'exercice suivant.

**Exercice** Soient  $r$  entiers  $> 0$ ,  $q_1, \dots, q_r$ , sans diviseurs communs autre que 1. Notons  $a_n$  le nombre de solutions en entiers  $\geq 0$  ( $x_1, \dots, x_r$ ) de l'équation diophantienne

$$q_1 x_1 + \dots + q_r x_r = n$$

Montrer que  $a_n \sim \frac{n^{r-1}}{q_1 \dots q_r (r-1)!}$ . On utilisera le fait que la série génératrice  $\frac{1}{(1-X^{q_1}) \dots (1-X^{q_r})}$  a en  $X = 1$  son pôle de plus haut degré.

Voici un autre exemple donné par Jacobi à l'aide de sa théorie des fonctions elliptiques. Le problème consiste à chercher le nombre de solutions  $a_n$  en nombres entiers (positifs ou négatifs) d'une équation à  $r$  inconnues :

$$x_1^2 + \dots + x_r^2 = n$$

Ce nombre  $a_n$  est le coefficient de  $X^n$  dans la série de  $(F(X))^r$  où

$$F(X) = \sum_{m \in \mathbb{Z}} X^{m^2}.$$

Cette série converge pour  $X \in \mathbb{C}$  de module plus petit que 1.

Enfin un dernier exemple où  $a_n = p(n)$  est la fonction de partition. Le nombre de partitions  $p(n)$  d'un entier  $n \geq 0$  est par définition le nombre de solutions en entiers  $x_i \geq 0$  de

$$x_1 + 2x_2 + \dots + mx_m + \dots = n$$

où le nombre d'inconnues  $m$  n'est pas limité (pour un  $n$  donné, il est clair que  $x_m = 0$  dès que  $m > n$ ).  $p(n)$  se définit aussi comme le nombre des classes d'équivalence des partitions d'un ensemble de  $n$  éléments, lorsque l'on range dans une même classe deux partitions qui se déduisent l'une de l'autre par une permutation des  $n$  éléments. La série génératrice, convergente pour  $|X| < 1$ , est donnée par :

$$S(X) = \sum_{n=0}^{\infty} p(n)X^n = \prod_{m=1}^{\infty} (1 - X^m)^{-1}.$$

Pour s'en convaincre, il suffit d'écrire chaque  $1/(1 - X^m)$  comme la série  $1 + X^m + X^{2m} + \dots$  et de développer le produit. L'idée est alors d'exprimer le coefficient  $p(n)$  à l'aide de la formule de Cauchy

$$p(n) = \frac{1}{2i\pi} \oint_{\mathcal{C}} \frac{S(z)}{z^{n+1}} dz$$

où  $\mathcal{C}$  est un cercle de centre  $O$  et de rayon  $R$  inférieur à 1. Le problème est d'évaluer cette intégrale lorsque  $R$  tend vers 1. Cela permet d'obtenir l'asymptotique suivante (résultat dû à Hardy et Ramanujan)

$$p(n) \sim \frac{1}{4\sqrt{3n}} \exp\left(\pi\sqrt{\frac{2n}{3}}\right)$$

pour  $n$  tendant vers l'infini.

## 2.4 La fonction zêta

Le reste du chapitre est maintenant consacré à l'ensemble  $\mathbb{P}$  des nombres premiers. On note  $(p_n)_{n \geq 1}$  les nombres premiers rangés par ordre croissant :

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 7, \dots$$

Pour abrégé, on note souvent  $\sum_{p \in \mathbb{P}} h(p)$  la somme suivante  $\sum_{n \geq 1} h(p_n)$  où  $h(p)$  est une fonction donnée de  $p$ . De même pour les produits :  $\prod_{p \in \mathbb{P}} h(p) = \prod_{n \geq 1} h(p_n)$ .

Voyons comment Euler a “codé” la suite des  $p_n$  dans une fonction de la variable complexe  $s$ . Pour  $\Re(s) > 1$ , il est facile de voir que la série suivante est absolument convergente et définit la fonction  $\zeta$  de Riemann :

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}.$$

Le lien entre  $\zeta$  et les nombres premiers vient du calcul suivant dû à Euler :

$$\prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}} = \prod_{p \in \mathbb{P}} \left( 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \dots \right).$$

En développant ce produit infini, nous voyons qu’il fait intervenir tous les produits d’un nombre fini de puissances de  $\frac{1}{p^s}$  de la forme

$$\frac{1}{p_1^{\alpha_1 s}} \cdots \frac{1}{p_k^{\alpha_k s}}$$

pour  $k$  entier et  $\alpha_i$  entier et  $p_i$  premier. Chacun de ces produits finis correspond à  $1/n^s$  où  $n$  est l’unique entier dont la décomposition en facteurs premiers est  $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ . Ainsi, on voit que

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}}.$$

C’est maintenant en jouant sur les deux formes de  $\zeta$ , la série de Dirichlet  $\sum 1/n^s$  et le produit eulérien  $\prod 1/(1-1/p^s)$ , que l’on obtient des informations sur les grands nombres premiers.

En y regardant de plus près, il est facile de voir que les manipulations formelles ci-dessus sont parfaitement justifiées dès que  $\Re(s) > 1$ , car alors toutes les séries et produits infinis sont absolument convergents. Dans un premier temps, il suffit pour s’en convaincre facilement de prendre  $s$  réel  $> 1$ .

Dès 1737, Euler avait utilisé  $\zeta$  comme fonction de la variable réelle  $s$  pour étudier la suite  $p_n$ . L’équivalent  $\pi(x) \sim x/\log(x)$ , le nombre de  $p_n$  plus petits que l’entier  $x$ , avait été conjecturé par Gauss et Legendre à la fin du XVIIIème siècle. Il a fallu cependant attendre le milieu du XIXème siècle pour que Tschebyschef établisse par des moyens arithmétiques élémentaires qu’il existe deux constantes  $A$  et  $B$ ,  $0 < A < 1 < B$  telles que, pour  $x$  assez grand

$$A \frac{x}{\log(x)} < \pi(x) < B \frac{x}{\log(x)}.$$

Ce n’est qu’en 1896 que Hadamard et de la Vallée-Poussin démontrèrent indépendamment le théorème sur des nombres premiers, i.e., le fait que

$\pi(x) \sim x/\log(x)$  lorsque  $x \mapsto +\infty$ . Pour cela, ils se sont fortement appuyés sur le célèbre article de Riemann [15] qui montrait que  $\zeta$  admettait un prolongement méromorphe pour  $s \in \mathbb{C}$  et aussi qui mettait en évidence de façon largement conjecturale le lien entre la distribution des zéros de  $\zeta$  et celle des nombres premiers.

Rappelons enfin la relation entre la fonction  $\zeta$  et la fonction entière  $\xi$  qui code les zéros non triviaux  $\rho_n$  de  $\zeta$  et dont on pense (hypothèse de Riemann) qu'ils sont sur l'axe  $\Re = 1/2$  ( $\Re(\rho_n) = 1/2$ , pour tout  $n$ ) :

$$\xi(s) = \Pi(s/2)(s-1)\pi^{-s/2}\zeta(s)$$

avec  $\Pi(s) = \Gamma(s+1) = \int_0^{+\infty} \exp(-x)x^s dx$  et

$$\xi(s) = \xi(0) \prod_1^{\infty} \left(1 - \frac{s}{\rho_n}\right).$$

### 2.4.1 Répartition des nombres premiers

**Théorème 7** (théorème des nombres premiers). *On note  $\pi(x)$ , le nombre des entiers premiers et plus petits que  $x > 0$ . Alors, lorsque  $x$  tend vers  $+\infty$ ,  $\pi(x) \sim x/\log(x)$ . Ceci est équivalent à dire que  $p_n \sim n \log(n)$  lorsque  $n$  tend vers  $+\infty$ .*

Nous n'allons pas donner ici de démonstration rigoureuse de ce théorème car elle déborde largement du cadre de ce cours (voir, e.g., [20, 28, 9]). Cependant, nous allons donner un argument heuristique emprunté à [9], c'est-à-dire, non rigoureux mais suggestif en utilisant la fonction  $\zeta(s)$  comme produit eulérien

$$\sum_{n \geq 1} 1/n^s = \zeta(s) = \prod_{n \geq 1} (1 - 1/p_n^s)^{-1}$$

pour  $s > 1$  réel tendant vers 1.

En prenant le log on a :

$$\log(\zeta(s)) = - \sum_{n \geq 1} \log(1 - 1/p_n^s)$$

Mais

$$\forall y \in [0, 1/2], \quad y \leq -\log(1 - y) \leq y + y^2.$$

Donc

$$\sum_{n \geq 1} \frac{1}{p_n^s} \leq \log(\zeta(s)) \leq \sum_{n \geq 1} \frac{1}{p_n^s} + \sum_{n \geq 1} \frac{1}{p_n^{2s}}.$$

Ainsi,

$$0 \leq \log(\zeta(s)) - \sum_{n \geq 1} \frac{1}{p_n^s} \leq \sum_{n \geq 1} \frac{1}{p_n^{2s}}.$$

Mais, pour  $s \geq 1$ ,  $\sum_{n \geq 1} \frac{1}{p_n^{2s}} \leq \sum_{n \geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$ . Donc, quand  $s \mapsto 1^+$ ,  $\log(\zeta(s)) - \sum_{n \geq 1} \frac{1}{p_n^s}$  reste borné. Comme  $\lim_{s \rightarrow 1^+} \zeta(s) = +\infty$  (la série  $\sum 1/n$  diverge) on voit que nécessairement la série,  $\sum 1/p_n$  est aussi divergente. Ainsi, nous voyons sans beaucoup d'effort qu'il n'existe pas de constantes  $A$  et  $\epsilon > 0$  telles que  $p_n \geq An^{1+\epsilon}$  pour tout  $n$ .

Comme chacun des termes du produit est plus grand que 1, on a pour tout entier  $N$ ,

$$\zeta(s) \geq \prod_{p_n \leq N} (1 - 1/p_n^s)^{-1}.$$

Avec  $(1 - 1/p_n^s)^{-1} = \sum_{k \geq 0} 1/p_n^{ks}$  on voit que

$$\prod_{p_n \leq N} (1 - 1/p_n^s)^{-1} = \sum_{n \in E_N} 1/n^s$$

où  $E_N$  est l'ensemble des entiers dont les diviseurs premiers sont tous inférieurs à  $N$ . Il est clair que  $E_N$  contient au moins  $\{1, \dots, N\}$ . Cela suggère que  $\sum_{1 \leq n \leq N} 1/n$  et  $\prod_{p_n \leq N} (1 - 1/p_n)^{-1}$  sont similaires pour  $N$  grand. Comme

$$\log \left( \sum_{1 \leq n \leq N} 1/n \right) = \log(\log(N)) + O(1)$$

et (utiliser  $y \leq -\log(1 - y) \leq y + y^2$  pour  $0 \leq y \leq 1/2$ ),

$$\log \left( \prod_{p_n \leq N} (1 - 1/p_n)^{-1} \right) = \sum_{p_n \leq N} 1/p_n + O(1)$$

cela nous suggère que

$$\sum_{p_n \leq N} 1/p_n \sim \log(\log(N)) \quad (N \mapsto +\infty).$$

Si  $n$  est premier alors  $\pi(n) - \pi(n - 1) = 1$ , sinon  $\pi(n) - \pi(n - 1) = 0$ . Donc

$$\sum_{p_n \leq N} 1/p_n = \sum_{1 \leq n \leq N} (\pi(n + 1) - \pi(n))/n$$

En réorganisant cette somme et comme  $\pi(N + 1) \leq N$ , on voit que

$$\sum_{p_n \leq N} 1/p_n = \sum_{1 \leq n \leq N-1} \pi(n)/(n(n + 1)) + O(1).$$

Mais aussi on a (comparer avec  $\int_2^N dx/(x \log(x))$ )

$$\log(\log(N)) = \sum_{2 \leq n \leq N-1} 1/(n \log(n)) + O(1).$$

Ainsi il est tentant de conjecturer que

$$\pi(n)/(n(n+1)) \sim 1/(n \log(n))$$

soit  $\pi(n) \sim n/\log(n)$ .

Dans ce qui précède, le seul résultat rigoureusement prouvé est la divergence de la série  $\sum 1/p_n$ . Nous allons voir que des arguments similaires sont à la base du théorème de la progression arithmétique.

### 2.4.2 Le théorème de la progression arithmétique

Le résultat suivant est dû à Dirichlet.

**Théorème 8** (progression arithmétique). *Soient  $a$  et  $m$  des entiers strictement positifs et premiers entre eux. Il existe une infinité de nombres premiers de la forme  $a + km$  avec  $k$  entier positif.*

Remarquons d'abord que, si  $a$  et  $m$  ne sont pas premiers entre eux, tous les nombres de la forme  $a + km$  sont composés. En fait ce théorème admet une formulation nettement plus précise : les nombres premiers se distribuent uniformément parmi les  $\varphi(m)$  classes associées aux nombres  $a$  plus petits que  $m$  et premiers avec lui. Autrement dit, si on note  $\pi_a(x)$  le nombre d'entiers premiers plus petits que  $x$  et de la forme  $a + km$ , alors on a l'asymptotique suivante pour  $x \mapsto +\infty$  :

$$\pi_a(x) \sim \frac{1}{\varphi(m)} \pi(x) = \frac{x}{\varphi(m) \log(x)}.$$

Ainsi, on comprend mieux à travers ce résultat la philosophie générale sous-jacente à de nombreuses conjectures sur les nombres premiers : tout ce qui n'est pas trivialement interdit est en fait réalisé. Citons pour mémoire les conjectures suivantes :

- nombres premiers jumeaux : il existe une infinité de nombres premiers  $p$  tels que  $p + 2$  soit aussi premier.
- nombres premiers cousins : il existe une infinité de nombres premiers  $p$  tels que  $p + 4$  et  $p + 6$  soient aussi premiers.
- C. Goldbach, un contemporain d'Euler, avait émis en 1742 la conjecture que tout entier pair est somme de deux nombres premiers et tout entier impair somme de trois nombres premiers.



**Exercice** Pourquoi dans la conjecture des nombres cousins on ne prend pas  $p$ ,  $p + 2$  et  $p + 4$  ?

Revenons au théorème de la progression arithmétique et supposons pour simplifier que  $m = 4$ . Alors, nous n'avons que deux valeurs possibles pour  $a$  : 1 ou 3. Soient les deux fonctions  $\chi_0$  et  $\chi_2$  de  $\mathbb{N}$  vers  $\{-1, 0, 1\}$  définies par

$$\chi_0(n) = \begin{cases} 1 & \text{si } n = 1 \text{ ou } 3 \pmod{4} \\ 0 & \text{sinon} \end{cases}, \quad \chi_1(n) = \begin{cases} 1 & \text{si } n = 1 \pmod{4} \\ -1 & \text{si } n = 3 \pmod{4} \\ 0 & \text{sinon} \end{cases}$$

Ainsi  $\chi_0$  et  $\chi_1$  sont périodiques (période 4) et multiplicatives, i.e.,  $\chi_0(nm) = \chi_0(n)\chi_0(m)$  et  $\chi_1(nm) = \chi_1(n)\chi_1(m)$  pour tout couple d'entiers  $(n, m)$ . Cette propriété est essentielle pour associer à chacune de ces fonctions multiplicatives une série de Dirichlet qui s'exprime sous la forme d'un produit eulérien. On pose

$$\zeta_0(s) = \sum_{n \geq 1} \frac{\chi_0(n)}{n^s}, \quad \zeta_1(s) = \sum_{n \geq 1} \frac{\chi_1(n)}{n^s}, \quad .$$

Considérons maintenant les produits suivants :

$$\prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\chi_0(p)}{p^s}}, \quad \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\chi_1(p)}{p^s}}.$$

Comme (on utilise le fait que  $(\chi_0(p))^k = \chi_0(p^k)$ )

$$\frac{1}{1 - \frac{\chi_0(p)}{p^s}} = 1 + \frac{\chi_0(p)}{p^s} + \frac{\chi_0(p^2)}{p^{2s}} + \frac{\chi_0(p^3)}{p^{3s}}$$

et idem pour  $\chi_1$ , on voit en développant ces produits que

$$\zeta_0(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\chi_0(p)}{p^s}}, \quad \zeta_1(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{\chi_1(p)}{p^s}}.$$

Tous ces calculs portent sur des séries absolument convergentes lorsque  $\Re(s) > 1$ . Ainsi, pour  $\Re(s) > 1$ ,  $\zeta_0$  et  $\zeta_1$  ne peuvent pas s'annuler (prendre le produit). On peut donc en prendre le log. Alors on a les relations suivantes

$$\log(\zeta_0) = \sum_{p \in \mathbb{P}} \frac{\chi_0(p)}{p^s} + h_0(s), \quad \log(\zeta_1) = \sum_{p \in \mathbb{P}} \frac{\chi_1(p)}{p^s} + h_1(s)$$

où les fonctions  $h_0$  et  $h_1$  sont des fonctions régulières de  $s$  définies autour de  $s = 1$ . En effet  $-\log(1 - y)$  s'écrit toujours sous la forme de  $y + w(y)y^2$  pour

$y$  de module inférieur à  $1/2$  et où  $w(y)$  est une fonction analytique de  $y$  et bornée sur le disque de rayon  $1/2$ . Donc

$$-\sum_{p \in \mathbb{P}} \log \left( 1 - \frac{\chi_0(p)}{p^s} \right) = \sum_{p \in \mathbb{P}} \frac{\chi_0(p)}{p^s} + \sum_{p \in \mathbb{P}} w \left( \frac{\chi_0(p)}{p^s} \right) \frac{\chi_0(p^2)}{p^{2s}}$$

la seconde somme définissant  $h_0(s)$  étant absolument convergente dès que  $s > 1/2$  (idem pour  $\chi_1(s)$  avec  $h_1(s)$ ).

Regardons maintenant de plus près l'allure des fonctions  $\zeta_0$  et  $\zeta_1$ . On a

$$\zeta_0(s) = \sum_{k \geq 0} \left( \frac{1}{(4k+1)^s} + \frac{1}{(4k+3)^s} \right).$$

Ainsi, lorsque  $s$  est réel et tend vers 1 par valeur supérieur,  $\zeta_0(s)$  tend vers  $+\infty$ . Par contre  $\zeta_1$  reste borné autour de  $s = 1$  car

$$\zeta_1(s) = \sum_{k \geq 0} \left( \frac{1}{(4k+1)^s} - \frac{1}{(4k+3)^s} \right)$$

où  $\frac{1}{(4k+1)^s} - \frac{1}{(4k+3)^s}$  est équivalent lorsque  $k$  tend vers l'infini à  $\frac{s}{2^{2s+1}k^{s+1}}$ . De plus chaque terme est strictement positif, donc  $\zeta_1(1) = \sum_{k \geq 0} \frac{2}{(4k+1)(4k+3)} > 0$ . Notons maintenant

$$P_1(s) = \sum_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod{4}}} \frac{1}{p^s}, \quad P_3(s) = \sum_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod{4}}} \frac{1}{p^s}.$$

Ainsi

$$\begin{aligned} \log(\zeta_0(s)) &= P_1(s) + P_3(s) + h_0(s) \\ \log(\zeta_1(s)) &= P_1(s) - P_3(s) + h_1(s) \end{aligned}$$

Comme,  $\zeta_1(s)$ ,  $h_0$  et  $h_1$  sont régulières en  $s = 1$ ,  $\zeta_1(1) > 0$  et  $\lim_{s \rightarrow 1^+} \zeta_0(s) = +\infty$  on en déduit nécessairement que  $\lim_{s \rightarrow 1^+} P_1(s) = +\infty$  et  $\lim_{s \rightarrow 1^+} P_3(s) = +\infty$ . Ainsi, chacune des deux séries

$$\sum_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod{4}}} \frac{1}{p}, \quad \sum_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod{4}}} \frac{1}{p}.$$

diverge et donc comporte un nombre infini de termes. Nous avons ainsi montré le théorème de la progression arithmétique pour  $a = 1, 3$  et  $m = 4$ .

La méthode que nous avons utilisée est en fait général. Donnons en une brève esquisse. Pour un entier  $m > 2$  on a en fait  $\varphi(m)$  choix possibles pour  $a$ , soit  $a \in \mathbb{Z}_m^*$ . Sur le groupe multiplicatif  $\mathbb{Z}_m^*$  on définit l'analogie des fonctions  $\chi_0$  et  $\chi_1$ , en fait  $\varphi(m)$  fonctions  $\chi_0, \dots, \chi_{\varphi(m)-1}$  fonctions multiplicatives distinctes mais à valeurs dans le cercle unité (les nombres complexes de module 1) : ce sont les caractères de Dirichlet. On note toujours le caractère trivial égal à 1 sur  $\mathbb{Z}_m^*$  par  $\chi_0$ . Les autres caractères  $\chi_k, k = 1, \dots, \varphi(m) - 1$  se distinguent de  $\chi_0$  par le fait que

$$\sum_{a \in \mathbb{Z}_m^*} \chi_k(a) = 0$$

Ainsi, les séries de Dirichlet

$$\zeta_k(t) = \sum_{n \geq 1} \frac{\chi_k(n)}{n^s}$$

sont très différentes autour de  $s = 1$  de la série  $\zeta_0$  associée à  $\chi_0$ . Contrairement à  $\zeta_0$  qui diverge en  $s = 1$ , ces séries  $\zeta_k$  sont des "séries alternées" (utiliser le critère d'Abel) et ainsi convergent en  $s = 1$ . Maintenant, chaque  $\zeta_j$  s'exprime comme un produit eulérien. Ainsi, après des manipulations (utilisant  $-\log(1 - y) = y + w(y)y^2$ ), on obtient les  $\varphi(m)$  formules suivantes

$$\log(\zeta_j) = \sum_{p \in \mathbb{P}} \frac{\chi_j(p)}{p^s} + h_j(s),$$

où  $h_j$  est une fonction régulière de  $s$  définie autour de  $s = 1$ . Maintenant, on pose, pour  $a \in \mathbb{Z}_m^*$ ,

$$P_a(s) = \sum_{\substack{p \in \mathbb{P} \\ p = a \pmod{m}}} \frac{1}{p^s}.$$

Alors on a

$$\log(\zeta_j(s)) = h_j(s) + \sum_{a \in \mathbb{Z}_m^*} \chi_j(a) P_a(s).$$

Des calculs simples sur les caractères montrent que la matrice  $\varphi(m) \times \varphi(m)$  d'éléments  $(\chi_j(a))$  pour  $0 \leq j \leq \varphi(m) - 1$  et  $a \in \mathbb{Z}_m^*$  est inversible, d'inverse sa conjuguée (hermitienne) divisée par  $\varphi(m)$ . Ainsi on voit que les  $P_a(s)$  s'expriment comme des combinaisons linéaires à coefficients non nuls des  $\log(\zeta_j)$  et des  $h_j$ . Maintenant, la partie dure de la preuve est de montrer qu'aucune des valeurs prises en  $s = 1$  par les  $\zeta_k$  ( $k \in \{1, \dots, \varphi(m) - 1\}$ ) n'est

nulle. Comme  $\zeta_0(s)$  est la seule à diverger en  $s = 1$ , on en déduit alors que chacun des  $P_a(s)$  diverge en  $s = 1$ . Et donc  $\{p \in \mathbb{P} \mid p = a \pmod{m}\}$  est infini pour tout  $a \in \mathbb{Z}_m^*$ .

On comprend un peu mieux pourquoi la localisation des zéros des fonctions de Dirichlet  $\zeta_j$  est si importante. La conjecture de Riemann généralisée affirme que les zéros (à partie réelle positive) des  $\zeta_j$  se situent tous sur la droite parallèle à l'axe imaginaire  $\Re(s) = 1/2$ .



# Chapitre 3

## Information et calculs quantiques

Pour rédiger ce chapitre, nous avons utilisé les références suivantes :

- [24], un livre très pédagogique sur l’informatique quantique.
- [5], un cours très actuel et bien adapté à des élèves passés par les classes préparatoires.
- [21], un excellent livre, accessible à partir de [12, 5], sur des expériences récentes réalisant diverses manipulations et opérations sur des systèmes quantiques simples et fondamentaux de type spin/ressort (“spin/spring systems”).
- Les notes de cours de Serge Haroche au Collège de France et en particulier celles de l’année 2001-2002 sur l’introduction au calcul quantique : <http://www.cqed.org/college/collegeparis.html>

### 3.1 Mécanique quantique

#### 3.1.1 Bra, Ket, états purs et états mixtes

Nous rappelons ici quelques notions de base de mécanique quantique. Nous renvoyons vers [5, 11] où toutes ces notions sont expliquées en détail. Bra  $\langle \bullet |$  et Ket  $|\bullet\rangle$  sont des co-vecteurs et des vecteurs. *L’état pur* d’un système quantique est décrit par un vecteur unitaire  $|\psi\rangle$  appartenant à un espace vectoriel hilbertien de dimension finie ou infinie  $\mathcal{H}$ . On appelle aussi  $|\psi\rangle$  *fonction d’onde*. Considérons pour simplifier que  $\mathcal{H}$  est de dimension finie  $d > 0$ . Soit  $(|n\rangle)_{1 \leq n \leq d}$  une base hilbertienne de  $\mathcal{H}$ . Il s’agit simplement d’une

base orthonormée. Soient deux fonctions d'onde  $|\psi\rangle$  et  $|\phi\rangle$

$$|\psi\rangle = \sum_{n=1}^d \psi_n |n\rangle, \quad |\phi\rangle = \sum_{n=1}^d \phi_n |n\rangle$$

où  $\psi_n, \phi_n \in \mathbb{C}$ . Comme  $|\psi\rangle$  et  $|\phi\rangle$  sont de longueur 1, on a

$$1 = \sum_n |\psi_n|^2, \quad 1 = \sum_n |\phi_n|^2.$$

Ainsi  $|\psi\rangle$  et  $|\phi\rangle$  sont représentées dans la base  $(|n\rangle)$  par deux matrices  $d \times 1$  :

$$|\psi\rangle \equiv \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_d \end{pmatrix}, \quad |\phi\rangle \equiv \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_d \end{pmatrix}.$$

Le symbole  $\dagger$  correspond à la *transposition hermitienne*. Comme  $\langle\psi| = |\psi\rangle^\dagger$  et  $\langle\phi| = |\phi\rangle^\dagger$  sont des co-vecteurs (éléments du dual de  $\mathcal{H}$ ), ils sont représentés par des matrices  $1 \times d$  :

$$\langle\psi| \equiv (\psi_1^*, \dots, \psi_d^*), \quad \langle\phi| \equiv (\phi_1^*, \dots, \phi_d^*).$$

où  $*$  est la conjugaison complexe que l'on peut aussi noter  $\dagger$ . Ainsi

$$\langle\psi|\psi\rangle = \langle\psi| \cdot |\psi\rangle = (\psi_1^*, \dots, \psi_d^*) \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_d \end{pmatrix} = \sum_n |\psi_n|^2 = 1$$

de même pour  $|\phi\rangle$ . Le produit hermitien est caractérisé par

$$\langle\psi|\phi\rangle = \langle\psi| \cdot |\phi\rangle = (\psi_1^*, \dots, \psi_d^*) \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_d \end{pmatrix} = \sum_n \psi_n^* \phi_n.$$

Noter que  $\langle\psi|\phi\rangle^* = \langle\phi|\psi\rangle$ .

L'intérêt des notations de Dirac vient en outre du calcul suivant : le projecteur orthogonal  $P$  sur le sous espace vectoriel de base orthonormée les  $p$  vecteurs  $(|\psi_1\rangle, \dots, |\psi_p\rangle)$  s'écrit

$$P = \sum_k |\psi_k\rangle\langle\psi_k|.$$

En effet  $P|\phi\rangle = \sum_k \langle\psi_k|\phi\rangle |\psi_k\rangle$ . Il est instructif de vérifier que  $P^2 = P$  découle simplement du fait que  $\langle\psi_k|\psi_{k'}\rangle = \delta_{k,k'}$ .

Lorsque l'on considère des états quantiques qui sont des mélanges statistiques d'états quantiques purs, il convient de les décrire par l'opérateur densité (*matrice densité*). Il n'est pas possible de faire simplement des moyennes avec des vecteurs sur la sphère unité de  $\mathcal{H}$ .

Pour s'en convaincre, il suffit de prendre  $\mathcal{H} = \mathbb{C}^2$  et les trois fonctions d'ondes  $|\psi_k\rangle = \cos(2k\pi/3)|1\rangle + \sin(2k\pi/3)|2\rangle$ ,  $k = 0, 1, 2$  chacune équiprobable de probabilité  $1/3$ . Comme  $\sum_k |\psi_k\rangle = 0$ , une simple moyenne ne permet pas d'attribuer une fonction d'onde à ce mélange statistique. Pour représenter un tel mélange statistique, il convient de faire des moyennes sur les projecteurs orthogonaux  $|\psi_k\rangle\langle\psi_k|$  associés aux états quantiques  $|\psi_k\rangle$ . Ainsi on considère l'opérateur hermitien  $\rho$  ( $\rho^\dagger = \rho$ ) défini par

$$\rho = \frac{1}{3} (|\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2| + |\psi_3\rangle\langle\psi_3|).$$

Il s'agit de l'opérateur densité. C'est l'analogie quantique d'une mesure de probabilité. Un simple calcul montre qu'ici  $\rho = \mathbb{I}/3$  où  $\mathbb{I} = |1\rangle\langle 1| + |2\rangle\langle 2|$  est l'opérateur identité :  $\mathbb{I}|\psi\rangle \equiv |\psi\rangle$ .

Plus généralement, un état quantique mixte est décrit par  $\rho$ , l'opérateur densité : il s'agit d'un opérateur hermitien de  $\mathcal{H}$  dans  $\mathcal{H}$ ,  $\rho^\dagger = \rho$ , semi-défini positif  $\rho \geq 0$  ( $\forall |\psi\rangle, \langle\psi|\rho|\psi\rangle \geq 0$ ) et de trace 1. On note généralement par  $\mathcal{D}$  l'ensemble de tous les opérateurs densité possibles :

$$\mathcal{D} = \{ \rho \in L(\mathcal{H}, \mathcal{H}) \mid \rho^\dagger = \rho, \rho \geq 0, \text{Tr}(\rho) = 1 \}$$

( $L(\mathcal{H}, \mathcal{H})$  désigne l'ensemble des applications linéaires de  $\mathcal{H}$  dans  $\mathcal{H}$ ). Ainsi  $\rho$  est diagonalisable en base orthonormée. Ses valeurs propres  $p_n$  sont dans  $[0, 1]$ . Supposons les  $p_n$  toutes distinctes : on dit que le spectre de  $\rho$  est non dégénéré. Notons  $|\psi_n\rangle$  un vecteur propre associé à  $p_n$  et de longueur 1. Alors on a

$$\rho = \sum_n p_n |\psi_n\rangle\langle\psi_n|, \quad \text{Tr}(\rho) = 1 = \sum_n p_n.$$

Ainsi chaque  $p_n$  peut être vu comme la probabilité pour que l'état du système soit  $|\psi_n\rangle$ . Noter que chaque  $|\psi_n\rangle$  est défini à une phase globale près :  $|\psi_n\rangle$  et  $|\tilde{\psi}_n\rangle = e^{i\theta_n} |\psi_n\rangle$ ,  $\theta_n \in \mathbb{R}$  arbitraire, correspondent au même état quantique, i.e. au même  $\rho$  :

$$\sum_n p_n |\psi_n\rangle\langle\psi_n| = \rho = \sum_n p_n |\tilde{\psi}_n\rangle\langle\tilde{\psi}_n|.$$

Si le spectre de  $\rho$  est dégénéré alors la somme sur  $n$  se réduit aux  $p_n$  distincts. Chaque projecteur  $|\psi_n\rangle\langle\psi_n|$  de rang 1 est remplacé par le projecteur



orthogonal  $P_n$  sur l'espace propre associé à la valeur propre  $p_n$ . Si  $p_n$  est de multiplicité  $s_n$  alors l'espace propre associé est de dimension  $s_n$ , le rang du projecteur  $P_n$ .

Un calcul élémentaire montre que  $\text{Tr}(\rho^2) \leq 1$ . Si  $\text{Tr}(\rho^2) = 1$  alors  $\rho$  est de rang 1 :  $\rho$  est dans ce cas un état pur  $|\phi\rangle\langle\phi|$  où  $|\phi\rangle$  est la fonction d'onde de cet état pur.

### 3.1.2 Opérateurs hermitiens, unitaires et équation différentielle de Schrödinger

Un opérateur hermitien  $H$  est un opérateur auto-adjoint pour le produit scalaire hermitien. L'opérateur densité  $\rho$  est donc hermitien. Pour un système à  $d$  états,  $\dim \mathcal{H} = d$ , avec une base orthonormée,  $(|n\rangle)_{n=1,\dots,d}$ , est associé à l'opérateur  $H$  la matrice hermitienne  $(H_{n,n'})_{1 \leq n,n' \leq d}$  avec  $H_{n,n'} = \langle n|H|n'\rangle \in \mathbb{C}$  :

$$H = \sum_{n,n'} H_{n,n'} |n\rangle\langle n'|, H^\dagger = H \text{ signifie que } \forall n, n', H_{n,n'}^* = H_{n',n}$$

où  $*$  est la conjugaison complexe. Comme  $H$  est diagonalisable en base orthonormée, on a

$$H = V\Delta V^\dagger$$

où  $V$  est une *matrice unitaire*  $VV^\dagger = V^\dagger V = \mathbb{I}$  et  $\Delta = \text{diag}(h_1, \dots, h_d)$  une matrice diagonale formée avec les valeurs propres réelles  $h_1, \dots, h_d$  de  $H$ , comptées avec leur multiplicités éventuelles.

Pour toutes fonctions  $\mathbb{R} \ni x \mapsto f(x) \in \mathbb{R}$ , on définit l'opérateur hermitien  $f(H)$  par la formule

$$f(H) = Vf(\Delta)V^\dagger$$

où  $f(\Delta) = \text{diag}(f(h_1), \dots, f(h_d))$ . Lorsque  $f(x) = \sum_k f_k x^k$  est un polynôme ou une fonction entière comme  $\cos(x)$ ,  $e^x$ , on retrouve le calcul usuel  $f(H) = \sum_k f_k H^k$  avec une somme absolument convergente.

L'évolution au cours du temps d'un état quantique  $|\psi\rangle$  est donnée par l'équation différentielle de Schrödinger ( $\hbar$  constante de Planck)  $\frac{d}{dt}|\psi\rangle = -i\frac{H}{\hbar}|\psi\rangle$  équation entièrement caractérisée par l'opérateur auto-adjoint  $H$  dit hamiltonien du système ( $H = H^\dagger$ ). Ce dernier peut dépendre du temps. Dans toute la suite  $\hbar$  est pris égale à l'unité et les éléments de  $H$  seront homogènes à des pulsations. Ainsi l'évolution du système d'état pur  $|\psi\rangle_t$  sera décrite par ( $i = \sqrt{-1} \in \mathbb{C}$ ) :

$$\frac{d}{dt}|\psi\rangle_t = -iH(t)|\psi\rangle_t \text{ avec la condition initiale } |\psi\rangle_{t=0} \in \mathcal{H}.$$

Lorsque  $H$  ne dépend pas du temps, la résolution de l'équation de Schrödinger se ramène à la diagonalisation de  $H$ . On note  $|n\rangle$ ,  $n = 1, \dots, d$ , une base orthonormée de vecteurs propres de  $H$  associés aux valeurs propres,  $h_n$ ,  $n = 1, \dots, d$ . Avec  $|\psi\rangle_t = \sum_n \psi_n(t) |n\rangle$  où  $\psi_n \in \mathbb{C}$  et  $\sum_n |\psi_n|^2 = 1$ , la solution de  $\frac{d}{dt} |\psi\rangle = -\imath H |\psi\rangle$  s'écrit

$$|\psi\rangle_t = \sum_n \psi_n(0) e^{-\imath h_n t} |n\rangle.$$

Lorsque  $H$  dépend du temps, il n'est plus possible de faire ainsi. On utilise en général des développements asymptotiques pour calculer des solutions approchées (cf. la sous-section 3.2.4 sur la manipulation d'un qubit et les oscillations de Rabi). On utilise aussi des simulations numériques.

Cependant, il est important de remarquer que l'évolution, selon l'équation de Schrödinger, préserve le produit hermitien. En effet, soient  $|\psi\rangle$  et  $|\phi\rangle$  deux solutions de la même équation de Schrödinger :

$$\frac{d}{dt} |\psi\rangle = -\imath H |\psi\rangle, \quad \frac{d}{dt} |\phi\rangle = -\imath H |\phi\rangle$$

alors

$$\begin{aligned} \frac{d}{dt} \langle \psi | \phi \rangle &= \frac{d}{dt} (|\psi\rangle)^\dagger |\phi\rangle + \langle \psi | \frac{d}{dt} (|\phi\rangle) \\ &= (-\imath H |\psi\rangle)^\dagger |\phi\rangle + \langle \psi | (-\imath H |\phi\rangle) \\ &= (\imath \langle \psi | H) |\phi\rangle - \imath \langle \psi | (H |\phi\rangle) = 0. \end{aligned}$$

Ce calcul est valable même si  $H$  dépend du temps. Ainsi  $\langle \psi | \phi \rangle_0 = \langle \psi | \phi \rangle_t$  pour tout  $t > 0$ . Donc l'évolution selon l'équation de Schrödinger préserve le produit hermitien. Il s'agit d'une évolution unitaire.

Cette évolution unitaire se traduit par l'équation du propagateur  $U(t)$ , opérateur linéaire de  $\mathcal{H}$  dans  $\mathcal{H}$ , solution de l'équation différentielle matricielle suivante

$$\frac{d}{dt} U(t) = -\imath H(t) U(t), \quad U(0) = \mathbb{I}$$

où  $\mathbb{I}$  est la matrice identité. Comme  $\frac{d}{dt} (UU^\dagger) = \frac{d}{dt} (U^\dagger U) = 0$ ,  $U(t)$  est une matrice inversible dont l'inverse est sa conjuguée hermitienne  $UU^\dagger = U^\dagger U = \mathbb{I}$  : c'est un opérateur unitaire. On note  $\mathcal{U}(d)$  le groupe des matrices unitaires  $d \times d$ . La solution de

$$\frac{d}{dt} |\psi\rangle_t = -\imath H(t) |\psi\rangle_t, \quad |\psi\rangle_{t=0} = |\psi\rangle_0$$

est alors  $|\psi\rangle_t = U(t) |\psi\rangle_0$ . Ainsi  $U$  est le propagateur associé à l'équation de Schrödinger. C'est une application linéaire qui préserve le produit hermitien.

Lorsque  $H$  est indépendant du temps, on a  $U(t) = e^{-iHt}$ . On retrouve alors le fait que l'exponentielle d'une matrice anti-hermitienne  $(iH)^\dagger = -iH$  est une matrice unitaire. Lorsque la trace de  $H(t)$  est nulle à chaque instant, alors  $\det U(t) \equiv 1$  car la formule de Liouville donne

$$\frac{d}{dt} \det U = -i \operatorname{Tr}(H(t)) \det U = 0$$

et donc  $U \in SU(d)$ , le sous-groupe des matrices unitaires  $d \times d$  et de déterminant 1.

L'équation de Schrödinger  $\frac{d}{dt} |\psi\rangle_t = -iH(t) |\psi\rangle_t$  donne l'évolution du système fermé d'état pur initial  $|\psi\rangle_{t=0} = |\phi\rangle$ . En terme de matrice densité  $\rho(t) = |\psi\rangle\langle\psi|_t$  on voit que

$$\rho(0) = |\phi\rangle\langle\phi|, \quad \rho(t) = U(t)\rho(0)U^\dagger(t), \quad \frac{d}{dt}\rho(t) = -i[H(t), \rho(t)]$$

où  $[H, \rho] = H\rho - \rho H$  est le commutateur de  $H$  avec  $\rho$ . Si la condition initiale est un mélange statistique  $\rho_0 = \sum_k p_k |\phi_k\rangle\langle\phi_k|$  où  $\sum_k p_k = 1$  et chaque  $|\phi_k\rangle$  de longueur 1 avec

$$\frac{d}{dt} |\psi_k\rangle_t = -iH(t) |\psi_k\rangle_t, \quad |\psi_k\rangle_{t=0} = |\phi_k\rangle$$

alors  $\rho(t) = \sum_k p_k |\psi_k\rangle\langle\psi_k|_t$  est la solution de l'équation différentielle matricielle (équation de Liouville) pour l'opérateur densité

$$\frac{d}{dt}\rho = -i[H(t), \rho(t)], \quad \rho(0) \in \mathcal{D}.$$

Il est alors direct de montrer que  $\rho(t) \in \mathcal{D}$  pour tout  $t > 0$  et que son spectre reste constant. En effet,  $\rho(t)$  et  $\rho(0)$  sont deux opérateurs semblables :  $\rho(t)U(t) = U(t)\rho(0)$  avec  $U^{-1}(t) = U^\dagger(t)$ .

### 3.1.3 Mesures et réduction du paquet d'ondes

A chaque mesure est attachée un opérateur auto-adjoint  $M$ . On parle aussi de l'observable  $M$ . Nous supposons toujours que l'espace de Hilbert est de dimension finie  $d$ . On considère la décomposition spectrale de  $M$  :

$$M = \sum_{n'=1}^{d'} m_{n'} P_{n'}$$

où le spectre de  $M$  est donné par les  $d'$  ( $\leq d$ ) valeurs réelles distinctes  $m_{n'}$  et où  $P_{n'}$  est le projecteur orthogonal sur l'espace propre associé à  $m_{n'}$ .

Lorsque  $d' = d$ , toutes les valeurs propres de  $M$  sont distinctes. On parle de spectre non dégénéré et alors  $M = \sum_{n=1}^d m_n |n\rangle\langle n|$  où  $|n\rangle$  est le vecteur propre unitaire associé à  $m_n$ .  $|n\rangle$  est défini à un complexe de module 1 près, i.e., à une phase près.

On suppose ici que le processus de mesure est instantané. La mesure individuelle de l'état  $|\psi\rangle$  donne alors  $m_{n'}$  avec la probabilité  $\langle\psi|P_{n'}|\psi\rangle = \text{Tr}(P_{n'}\rho)$  avec  $\rho = |\psi\rangle\langle\psi|$ . Si le résultat observé est  $m_{n'}$ , alors, juste après la mesure, l'état quantique n'est plus  $|\psi\rangle$  mais devient (réduction du paquet d'ondes)

$$|\psi\rangle_+ = \frac{P_{n'}|\psi\rangle}{\sqrt{\langle\psi|P_{n'}|\psi\rangle}}.$$

On notera que  $\langle\psi|P_{n'}|\psi\rangle$  ne peut pas être nul puisque le résultat observé est  $m_{n'}$ . Pour l'opérateur densité  $\rho$  cette réduction du paquet d'ondes associée au résultat  $m_{n'}$  s'écrit

$$\rho_+ = \frac{P_{n'}\rho P_{n'}}{\text{Tr}(P_{n'}\rho)}.$$

On remarque que cette formule s'étend pour tout  $\rho \in \mathcal{D}$  et que  $\rho_+$  reste bien dans  $\mathcal{D}$  : cette formule est aussi valable pour un mélange statique, i.e., lorsque le rang de  $\rho$  excède 1.

La mesure répétée un grand nombre de fois du même état quantique pur  $|\psi\rangle$  ou mixte  $\rho$  donne comme moyenne

$$\langle M \rangle = \text{Tr}(M\rho) = \sum_{n'=1}^d m_{n'} \text{Tr}(P_{n'}\rho) = \sum_{n'=1}^d p_{n'}(\rho) m_{n'}$$

où  $p_{n'}(\rho) = \text{Tr}(P_{n'}\rho)$  est la probabilité d'obtenir la mesure  $m_{n'}$ . Comme  $\sum_{n'} P_{n'} = \mathbb{I}$ , on a

$$\text{Tr}(\rho) = \text{Tr}\left(\rho \sum_{n'} P_{n'}\right) = \sum_{n'} \text{Tr}(P_{n'}\rho) = \sum_{n'} p_{n'}(\rho) = 1.$$

En résumé, chaque mesure individuelle de l'état quantique, donne un nombre qui est l'une des valeurs propres de  $M$ . Après chaque mesure individuelle, l'état quantique est projeté orthogonalement (et renormalisé) sur l'espace propre associé à la valeur propre correspondante à la mesure obtenue. Ainsi toute mesure secoue violemment le système. On parle alors de réduction du paquet d'ondes : après la mesure ayant donnée comme résultat la valeur propre  $m_{n'}$  de  $M$ , les composantes de la fonction d'onde selon les vecteurs propres associées aux  $m_{n''}$  avec  $n'' \neq n'$  sont mises à zéro. Si, juste après avoir obtenu  $m_{n'}$ , on mesure à nouveau  $M$  on obtient nécessairement de même résultat  $m_{n'}$ . En effet, l'état quantique  $\rho_+$  n'a pas le temps d'évoluer,  $p_{n'}(\rho_+) = 1$  et  $|\psi\rangle_{++} = |\psi\rangle_+$  et  $\rho_{++} = \rho_+$ .

### 3.1.4 Systèmes composites et produit tensoriel

Un système composite est formé à partir de plusieurs sous-systèmes. Son espace d'états n'est pas le produit cartésien des espaces d'états de ses sous-systèmes mais le produit tensoriel. C'est une différence essentielle par rapport au cas classique.

Soit donc un système composite formée de deux sous-systèmes (système bipartite) : l'espace de Hilbert du premier sous-système est noté  $\mathcal{A}$  et celui du second  $\mathcal{B}$ . L'espace d'état du système complet est  $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$ , le produit tensoriel de  $\mathcal{A}$  et  $\mathcal{B}$ . On construit la structure hilbertienne sur  $\mathcal{H}$  à partir de celles sur  $\mathcal{A}$  et  $\mathcal{B}$ . Pour cela on prend une base hilbertienne  $(|n_a\rangle)_{1 \leq n_a \leq d_a}$  sur  $\mathcal{A}$  et  $(|n_b\rangle)_{1 \leq n_b \leq d_b}$  sur  $\mathcal{B}$  ( $d_a, d_b$  entiers  $> 0$ ). Alors  $\mathcal{H}$  est de dimension  $d_a d_b$  (et non  $d_a + d_b$  comme cela serait le cas si  $\mathcal{H}$  était le produit cartésien de  $\mathcal{A}$  et  $\mathcal{B}$ ) avec comme base hilbertienne  $(|n_a\rangle \otimes |n_b\rangle)$ . On note souvent  $|n_a\rangle \otimes |n_b\rangle$  par  $|n_a, n_b\rangle$  ou par  $|n_a n_b\rangle$ . Toute fonction d'onde  $|\psi\rangle \in \mathcal{H}$  s'écrit

$$|\psi\rangle = \sum_{n_a, n_b} \psi_{n_a, n_b} |n_a\rangle \otimes |n_b\rangle = \sum_{n_a, n_b} \psi_{n_a, n_b} |n_a n_b\rangle, \quad \psi_{n_a, n_b} \in \mathbb{C}.$$

Le produit hermitien de  $|\psi\rangle$  avec  $|\phi\rangle = \sum_{n_a, n_b} \phi_{n_a, n_b} |n_a n_b\rangle$  est défini par

$$\langle \psi | \phi \rangle = \sum_{n_a, n_b} \psi_{n_a, n_b}^* \phi_{n_a, n_b}.$$

Cette définition est indépendante des bases orthonormées choisies sur  $\mathcal{A}$  et  $\mathcal{B}$ . Il est instructif de le montrer en utilisant des matrices unitaires quelconque  $U_a \in \mathcal{U}(d_a)$  et  $U_b \in \mathcal{U}(d_b)$  associées à tous les changements de bases orthonormées sur  $\mathcal{A}$  et  $\mathcal{B}$ .

Un état  $|\psi\rangle \in \mathcal{A} \otimes \mathcal{B}$  est dit *intriqué entre A et B* si, seulement si, il n'existe pas de  $|\psi_a\rangle \in \mathcal{A}$  et de  $|\psi_b\rangle \in \mathcal{B}$  tels que  $|\psi\rangle = |\psi_a\rangle \otimes |\psi_b\rangle$ . Pour un tel  $|\psi\rangle$ , il n'est pas possible de définir un état partiel et pur ni pour le sous-système  $A$ , ni pour le sous-système  $B$ . On parle aussi d'état  $|\psi\rangle$  non séparable entre  $A$  et  $B$ . C'est un peu comme une fonction scalaire de deux variables  $f(x_a, x_b)$  qui n'est pas à variables séparables, i.e. de la forme  $f(x_a, x_b) = f_a(x_a) f_b(x_b)$ . En général, une fonction scalaire de deux variables  $x_a$  et  $x_b$  n'est pas la multiplication d'une fonction scalaire de  $x_a$  seul par une autre fonction scalaire de  $x_b$  seul.

Prenons maintenant un opérateur  $H_a$  sur  $\mathcal{A}$  et un opérateur  $H_b$  sur  $\mathcal{B}$ . Alors  $H_a$  et  $H_b$  se prolongent en opérateur sur  $\mathcal{H}$  avec  $H_a \otimes \mathbb{I}_b$  et  $\mathbb{I}_a \otimes H_b$  ( $\mathbb{I}_a$

et  $\mathbb{I}_b$  sont les opérateurs identité sur  $\mathcal{A}$  et  $\mathcal{B}$  :

$$(H_a \otimes \mathbb{I}_b) |\psi\rangle = \sum_{n_a, n_b} \psi_{n_a, n_b} H_a |n_a\rangle \otimes |n_b\rangle,$$

$$(\mathbb{I}_a \otimes H_b) |\psi\rangle = \sum_{n_a, n_b} \psi_{n_a, n_b} |n_a\rangle \otimes H_b |n_b\rangle.$$

Par abus de notations et quand il n'y a pas de confusion possible, on ne rappelle pas le produit tensoriel avec les opérateurs identités :

$$H_a \equiv H_a \otimes \mathbb{I}_b, \quad H_b \equiv \mathbb{I}_a \otimes H_b.$$

On peut aussi former l'opérateur  $H_a \otimes H_b$  défini par

$$(H_a \otimes H_b) |\psi\rangle = \sum_{n_a, n_b} \psi_{n_a, n_b} H_a |n_a\rangle \otimes H_b |n_b\rangle.$$

## 3.2 Qubit et $n$ -qubit

### 3.2.1 Qubit : système à deux niveaux

Pour un système à deux états,  $|\psi\rangle \in \mathcal{H} = \mathbb{C}^2$  s'écrit  $|\psi\rangle = \psi_g |g\rangle + \psi_e |e\rangle$  avec  $\psi_g, \psi_e \in \mathbb{C}$  et

$$|g\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |e\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Les composantes de  $|\psi\rangle$  sont des amplitudes complexes de probabilité et donc on a  $|\psi_g|^2 + |\psi_e|^2 = 1$ . Il est usuel de noter par  $|g\rangle$  l'état quantique dont l'énergie est la plus basse ( $g$  pour "ground state") et par  $|e\rangle$  celui dont l'énergie est la plus haute ( $e$  pour "excited state").

Un système de spin  $\frac{1}{2}$  est un système à deux états. On parle aussi de *qubit* pour désigner un système à deux états, i.e., un système quantique décrit par un vecteur (un Ket) de dimension deux. Un qubit est donc représenté par  $|\psi\rangle = \psi_g |g\rangle + \psi_e |e\rangle$ . Par convention, on note, en *informatique quantique*,  $|1\rangle = |g\rangle$  et  $|0\rangle = |e\rangle$ .

Le conjugué hermitien d'un Ket est un Bra :  $\langle\psi| = |\psi\rangle^\dagger = \psi_g^* \langle g| + \psi_e^* \langle e|$ . Le produit scalaire hermitien permet d'assigner un nombre complexe à un Bra et un Ket : si  $|\psi\rangle = \psi_g |g\rangle + \psi_e |e\rangle$  et si  $|\phi\rangle = \phi_g |g\rangle + \phi_e |e\rangle$ , alors

$$\langle\psi|\phi\rangle = \psi_g^* \phi_g + \psi_e^* \phi_e.$$

### 3.2.2 Matrices de Pauli

Les matrices de Pauli sont des matrices hermitiennes  $2 \times 2$  définies par

$$\sigma_x = |e\rangle \langle g| + |g\rangle \langle e|, \quad \sigma_y = -i|e\rangle \langle g| + i|g\rangle \langle e|, \quad \sigma_z = |e\rangle \langle e| - |g\rangle \langle g|$$

où  $|g\rangle$  et  $|e\rangle$  sont deux états quantiques orthogonaux ( $\langle g|g\rangle = \langle e|e\rangle = 1$  et  $\langle g|e\rangle = \langle e|g\rangle = 0$ ). Elles anti-commutent deux à deux

$$\sigma_x \sigma_y = -\sigma_y \sigma_x, \quad \sigma_y \sigma_z = -\sigma_z \sigma_y, \quad \sigma_z \sigma_x = -\sigma_x \sigma_z,$$

et vérifient les identités suivantes

$$\sigma_x^2 = \mathbb{I}, \quad \sigma_y^2 = \mathbb{I}, \quad \sigma_z^2 = \mathbb{I}, \quad \sigma_x \sigma_y = i\sigma_z, \quad \sigma_y \sigma_z = i\sigma_x, \quad \sigma_z \sigma_x = i\sigma_y.$$

où  $\mathbb{I}$  désigne la matrice identité :  $\mathbb{I} = |g\rangle \langle g| + |e\rangle \langle e|$ . Pour tout angle  $\theta \in \mathbb{R}$  on a

$$e^{i\theta\sigma_\xi} = \cos \theta \mathbb{I} + i \sin \theta \sigma_\xi, \quad \text{pour } \xi = x, y, z.$$

Lorsqu'il n'y a pas d'ambiguïté, on note aussi  $\mathbb{I}$  par 1 et  $\cos \theta \mathbb{I}$  est remplacé par  $\cos \theta$ , ce qui donne la formule plus compacte :

$$e^{i\theta\sigma_\xi} = \cos \theta + i \sin \theta \sigma_\xi, \quad \text{pour } \xi = x, y, z.$$

Nous utiliserons souvent cette notation raccourcie par la suite.

Ainsi la solution de l'équation de Schrödinger ( $\Omega \in \mathbb{R}$ ,  $H = \frac{\Omega}{2}\sigma_\xi$ ,  $\xi = x, y, z$ )

$$\frac{d}{dt} |\psi\rangle = -i\frac{\Omega}{2}\sigma_\xi |\psi\rangle$$

est

$$|\psi\rangle_t = e^{-\frac{i\Omega t}{2}\sigma_\xi} |\psi\rangle_0 = \left( \cos\left(\frac{\Omega t}{2}\right) - i \sin\left(\frac{\Omega t}{2}\right) \sigma_\xi \right) |\psi\rangle_0.$$

Pour  $\alpha, \beta = x, y, z$ ,  $\alpha \neq \beta$  on a les relations très utiles suivantes :

$$\sigma_\alpha e^{i\theta\sigma_\beta} = e^{-i\theta\sigma_\beta} \sigma_\alpha, \quad (e^{i\theta\sigma_\alpha})^{-1} = (e^{i\theta\sigma_\alpha})^\dagger = e^{-i\theta\sigma_\alpha}$$

et aussi, à cause de l'anti-commutation  $\sigma_\alpha \sigma_\beta = -\sigma_\beta \sigma_\alpha$ ,

$$e^{-\frac{i\theta}{2}\sigma_\alpha} \sigma_\beta e^{\frac{i\theta}{2}\sigma_\alpha} = e^{-i\theta\sigma_\alpha} \sigma_\beta = \sigma_\beta e^{i\theta\sigma_\alpha}$$

A chaque mesure est attachée un opérateur hermitien, dit aussi observable. Prenons un système à deux états  $|g\rangle$  et  $|e\rangle$  d'énergies définies et distinctes. Supposons que l'on mesure l'énergie  $H = H_g |g\rangle \langle g| + H_e |e\rangle \langle e|$  où  $H_g < H_e$  et que l'on dispose d'un grand nombre  $N$  de systèmes ayant le même état quantique  $|\psi\rangle = \psi_g |g\rangle + \psi_e |e\rangle$ . Pour chaque système pris individuellement on mesure  $H$  et on obtient soit

1.  $H_g$  et alors, juste après la mesure, le système est dans l'état  $|g\rangle$  ;
2.  $H_e$  et alors, juste après la mesure, le système est dans l'état  $|e\rangle$ .

On note  $N_g$  (resp.  $N_e$ ) le nombre de fois où l'on a obtenu  $H_g$  (resp.  $H_e$ ). Alors, pour  $N$  grand, on a

$$\frac{N_g}{N} \approx |\psi_g|^2, \quad \frac{N_e}{N} \approx |\psi_e|^2$$

(cohérent avec  $N = N_g + N_e$  et  $|\psi_g|^2 + |\psi_e|^2 = 1$ ). La valeur moyenne de ces  $N$  mesures est donc  $|\psi_g|^2 H_g + |\psi_e|^2 H_e$ . C'est pour cela que l'on interprète les composantes de  $|\psi\rangle$  comme des amplitudes de probabilités.

### 3.2.3 $n$ -qubit

Un  $n$ -qubit est un système composé de  $n$  fois le même qubit élémentaire.

Son état appartient donc à  $\mathcal{H} = \overbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \dots \otimes \mathbb{C}^2}^{n \text{ fois}}$ , isomorphe à  $\mathbb{C}^{2^n}$ . C'est très différent du produit cartésien qui donnerait alors  $\mathbb{C}^{2n}$ .

La base d'un 2-qubit est ( $|g\rangle$  et  $|e\rangle$  désignent les deux états de base du qubit élémentaire)

$$|g\rangle \otimes |g\rangle = |gg\rangle, \quad |g\rangle \otimes |e\rangle = |ge\rangle, \quad |e\rangle \otimes |g\rangle = |eg\rangle, \quad |e\rangle \otimes |e\rangle = |ee\rangle.$$

La base d'un 3-qubit est

$$|ggg\rangle, \quad |gge\rangle, \quad |geg\rangle, \quad |gee\rangle, \quad |egg\rangle, \quad |ege\rangle, \quad |eeg\rangle, \quad |eee\rangle.$$

La mesure de  $\sigma_z = -|g\rangle\langle g| + |e\rangle\langle e|$  sur le premier qubit d'un 2-qubit correspond à l'opérateur  $M = \sigma_z \otimes \mathbb{I}$ . Sur le 2-qubit

$$|\psi\rangle = \psi_{gg} |gg\rangle + \psi_{ge} |ge\rangle + \psi_{eg} |eg\rangle + \psi_{ee} |ee\rangle$$

la mesure de  $\sigma_z$  sur le 1er qubit donne en moyenne

$$\langle \psi | M | \psi \rangle = -(|\psi_{gg}|^2 + |\psi_{ge}|^2) + (|\psi_{eg}|^2 + |\psi_{ee}|^2)$$

i.e., donne soit  $-1$  avec une probabilité  $|\psi_{gg}|^2 + |\psi_{ge}|^2$ , soit  $+1$  avec une probabilité  $|\psi_{eg}|^2 + |\psi_{ee}|^2$ . Si, juste avant la mesure de  $\sigma_z$  sur le premier qubit, l'état quantique est  $|\psi\rangle = \psi_{gg} |gg\rangle + \psi_{ge} |ge\rangle + \psi_{eg} |eg\rangle + \psi_{ee} |ee\rangle$ , alors juste après la mesure (ici idéalisée comme une opération instantanée) l'état quantique est

$$- \text{ soit } \frac{\psi_{gg}|gg\rangle + \psi_{ge}|ge\rangle}{\sqrt{|\psi_{gg}|^2 + |\psi_{ge}|^2}} = |g\rangle \otimes \left( \frac{\psi_{gg}|g\rangle + \psi_{ge}|e\rangle}{\sqrt{|\psi_{gg}|^2 + |\psi_{ge}|^2}} \right) \text{ si la mesure est } -1,$$



– soit  $\frac{\psi_{eg}|eg\rangle + \psi_{ee}|ee\rangle}{\sqrt{|\psi_{eg}|^2 + |\psi_{ee}|^2}} = |e\rangle \otimes \left( \frac{\psi_{eg}|g\rangle + \psi_{ee}|e\rangle}{\sqrt{|\psi_{eg}|^2 + |\psi_{ee}|^2}} \right)$  si la mesure est +1

Ce type de mesure illustre la réduction ("collapse" en anglais) du paquet d'ondes, réduction associée au processus de mesure et sur laquelle repose l'interprétation de Copenhague de la fonction d'onde.

### 3.2.4 Complément : manipulation d'un qubit

#### Physique simplifiée du système

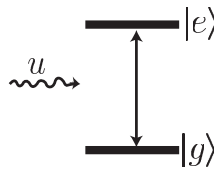


FIGURE 3.1 – Un système à deux états

Soit le système à deux états de la figure 3.1. Typiquement, il s'agit d'un électron autour d'un atome. Cet électron est soit dans l'état fondamental  $|g\rangle$  d'énergie  $H_g$ , soit dans l'état excité  $|e\rangle$  d'énergie  $H_e$  ( $H_g < H_e$ ). On ne regarde pas les autres niveaux d'énergie possible. C'est un peu comme pour les systèmes mécaniques flexibles où l'on ne considère que deux modes de vibration : au lieu de considérer l'équation aux dérivées partielles de Schrödinger qui décrit l'évolution de la fonction d'onde de l'électron, on ne considère que ses composantes selon deux états propres, un état dit fondamental et un état dit excité. Comme nous verrons que les contrôles sont des contrôles proches de la résonance, une telle approximation est très naturelle (au moins pour un physicien).

Ainsi, l'état quantique est décrit par  $|\psi\rangle \in \mathbb{C}^2$  de longueur 1,  $\langle\psi|\psi\rangle = 1$ , qui est une superposition linéaire de l'état fondamental  $|g\rangle$  et de l'état excité  $|e\rangle$ , deux états orthogonaux,  $\langle g|e\rangle = 0$  et de longueur 1,  $\langle g|g\rangle = \langle e|e\rangle = 1$  :

$$|\psi\rangle = \psi_g |g\rangle + \psi_e |e\rangle$$

avec  $\psi_g, \psi_e \in \mathbb{C}$  les deux amplitudes complexes de probabilité.

L'état  $|\psi\rangle$  dépend du temps. Pour ce système à deux niveaux, l'équation de Schrödinger est alors une équation différentielle ordinaire

$$\frac{d}{dt} |\psi\rangle = -iH |\psi\rangle = -i \left( H_g |g\rangle \langle g| + H_e |e\rangle \langle e| \right) |\psi\rangle$$

entièrement déterminée par  $H$ , l'opérateur hamiltonien.

Comme l'énergie est définie à une constante près, les hamiltoniens  $H$  et  $H + \omega_0(t)$  (avec  $\omega_0(t) \in \mathbb{R}$  arbitraire et où  $\omega_0$  correspond à  $\omega_0 \mathbb{I}$ ,  $\mathbb{I}$  la matrice identité) décrivent le même système physique. Si  $|\psi\rangle$  vérifie  $\frac{d}{dt} |\psi\rangle = -iH |\psi\rangle$  alors  $|\chi\rangle = e^{-i\theta_0(t)} |\psi\rangle$  avec  $\frac{d}{dt} \theta_0 = \omega_0$  vérifie  $\frac{d}{dt} |\chi\rangle = -i(H + \omega_0) |\chi\rangle$ . Ainsi pour tout  $\theta_0$ ,  $|\psi\rangle$  et  $e^{-i\theta_0} |\psi\rangle$  représentent le même système physique. La phase globale de l'état quantique  $|\psi\rangle$  peut être choisie arbitraire. Tout se passe comme si l'on pouvait rajouter un contrôle  $\omega_0$  de la phase globale, ce contrôle étant choisi comme on le souhaite (degré de liberté de jauge associé au choix d'origine pour l'énergie). Ainsi, la famille à un paramètre d'hamiltoniens

$$\left( (H_g + \omega_0) |g\rangle \langle g| + (H_e + \omega_0) |e\rangle \langle e| \right)_{\omega_0 \in \mathbb{R}}$$

décrit le même système à deux niveaux. Il est alors naturel de prendre  $\omega_0 = -\frac{H_g + H_e}{2}$  et de poser  $\Omega = H_e - H_g$ , la pulsation des photons qui interviennent dans le passage entre l'état fondamental et l'état excité. C'est la fréquence de la lumière émise par l'électron lors de son passage de l'état  $|e\rangle$  à l'état  $|g\rangle$  (lumière observée en spectroscopie, qui est une signature de la différence d'énergie et donc de l'atome considéré).

En résumé, pour le système isolé, la dynamique de  $|\psi\rangle$  s'écrit :

$$\frac{d}{dt} |\psi\rangle = -i\frac{\Omega}{2} (|e\rangle \langle e| - |g\rangle \langle g|) |\psi\rangle.$$

Ainsi

$$|\psi\rangle_t = \psi_{g0} e^{\frac{i\Omega t}{2}} |g\rangle + \psi_{e0} e^{-\frac{i\Omega t}{2}} |e\rangle.$$

Il est usuel d'utiliser les matrices de Pauli et en particulier

$$\sigma_z = |e\rangle \langle e| - |g\rangle \langle g|.$$

Comme  $\sigma_z^2 = 1$ , on a  $e^{i\theta\sigma_z} = \cos \theta + i \sin \theta \sigma_z$  ( $\theta \in \mathbb{R}$ ) et une autre écriture de l'évolution temporelle de  $|\psi\rangle$  :

$$|\psi\rangle_t = e^{-\frac{i\Omega t}{2} \sigma_z} |\psi\rangle_0 = \cos\left(\frac{\Omega t}{2}\right) |\psi\rangle_0 - i \sin\left(\frac{\Omega t}{2}\right) \sigma_z |\psi\rangle_0.$$

Supposons maintenant, le système en interaction avec un champ électromagnétique variable, décrit de façon classique par  $u(t) \in \mathbb{R}$  (typiquement un laser éclairant l'atome). Alors, l'évolution de  $|\psi\rangle$  est toujours donnée par une équation de Schrödinger mais avec un hamiltonien qui dépend du temps via le contrôle  $u(t)$ . Très souvent, cet hamiltonien contrôlé admet la forme suivante (approximation dipolaire et grande longueur d'onde par rapport à l'espace occupé par l'électron) :

$$H(t) = \frac{\Omega}{2} (|e\rangle \langle e| - |g\rangle \langle g|) + \frac{u(t)}{2} (|e\rangle \langle g| + |g\rangle \langle e|)$$

où  $u$  est homogène à une fréquence. L'équation de Schrödinger  $\frac{d}{dt}|\psi\rangle = -iH|\psi\rangle$  s'écrit alors simplement

$$i\frac{d}{dt}\begin{pmatrix}\psi_e \\ \psi_g\end{pmatrix} = -\frac{i\Omega}{2}\begin{pmatrix}1 & 0 \\ 0 & -1\end{pmatrix}\begin{pmatrix}\psi_e \\ \psi_g\end{pmatrix} + \frac{iu(t)}{2}\begin{pmatrix}0 & 1 \\ 1 & 0\end{pmatrix}\begin{pmatrix}\psi_e \\ \psi_g\end{pmatrix}.$$

A ce niveau il est très commode de faire intervenir les trois matrices de Pauli

$$\sigma_x = |e\rangle\langle g| + |g\rangle\langle e|, \quad \sigma_y = -i|e\rangle\langle g| + i|g\rangle\langle e|, \quad \sigma_z = |e\rangle\langle e| - |g\rangle\langle g|.$$

Ainsi l'hamiltonien contrôlé s'écrit

$$H = \frac{\Omega}{2}\sigma_z + \frac{u(t)}{2}\sigma_x.$$

Du fait que  $\sigma_z$  et  $\sigma_x$  ne commutent pas, on ne dispose pas de formule simple pour la solution au problème de Cauchy,  $\frac{d}{dt}|\psi\rangle = -iH(t)|\psi\rangle$ , lorsque  $u(t)$  dépend effectivement du temps.

### Contrôle résonant et oscillations de Rabi

Dans l'équation de Schrödinger,  $\frac{d}{dt}|\psi\rangle = -i\left(\frac{\Omega}{2}\sigma_z + \frac{u}{2}\sigma_x\right)|\psi\rangle$ , il est souvent impossible<sup>1</sup> d'avoir  $u$  et  $\Omega$  du même ordre de grandeur. Le contrôle est généralement très petit :  $|u| \ll \Omega$ . Dans ce cas, la seule façon de procéder consiste à rentrer en résonance avec le système en boucle ouverte, i.e., à choisir  $u$  oscillant avec une pulsation  $\Omega^L$  proche de  $\Omega$ , un peu comme des enfants lorsqu'ils apprennent à faire de la balançoire en donnant de très légères impulsions en phase avec les oscillations.

On commence par faire un changement de variables,  $|\psi\rangle = e^{-\frac{i\Omega t}{2}\sigma_z}|\phi\rangle$ , que les physiciens interprètent comme le passage dans le repère d'interaction. Le but est d'éliminer le terme en  $\frac{\Omega}{2}\sigma_z$  dans l'hamiltonien (élimination du "drift"). La dynamique de  $|\phi\rangle$  est :

$$\frac{d}{dt}|\phi\rangle = -\frac{iu}{2}e^{\frac{i\Omega t}{2}\sigma_z}\sigma_x e^{-\frac{i\Omega t}{2}\sigma_z}|\phi\rangle = H_{\text{int}}|\phi\rangle$$

avec

$$H_{\text{int}} = \frac{u}{2}e^{i\Omega t}\sigma_+ + \frac{u}{2}e^{-i\Omega t}\sigma_-$$

l'hamiltonien dans le repère d'interaction et où

$$\sigma_+ = |e\rangle\langle g| = \frac{\sigma_x + i\sigma_y}{2}, \quad \sigma_- = |g\rangle\langle e| = \frac{\sigma_x - i\sigma_y}{2}.$$

---

1. Sauf à utiliser des champs très intenses mais alors d'autres phénomènes doivent être pris en compte.

Les opérateurs (non hermitiens)  $\sigma_+$  et  $\sigma_-$  correspondent aux sauts quantiques de  $|g\rangle$  vers  $|e\rangle$  et de  $|e\rangle$  vers  $|g\rangle$ , respectivement. Il est alors logique de prendre un contrôle résonant de pulsation  $\Omega$

$$u = \mathbf{u}e^{i\Omega t} + \mathbf{u}^*e^{-i\Omega t}$$

avec  $\mathbf{u}$  amplitude complexe lentement variable et petite en module :

$$\left| \frac{d}{dt} \mathbf{u} \right| \ll \Omega |\mathbf{u}|, \quad |\mathbf{u}| \ll \Omega.$$

Ainsi

$$i \frac{d}{dt} |\phi\rangle = \left( \left( \frac{\mathbf{u}e^{2i\Omega t} + \mathbf{u}^*}{2} \right) \sigma_+ + \left( \frac{\mathbf{u} + \mathbf{u}^*e^{-2i\Omega t}}{2} \right) \sigma_- \right) |\phi\rangle$$

On voit donc que ce système est sous la forme standard du théorème de moyennisation, rappelé dans l'appendice A avec comme petit paramètre  $\epsilon = \frac{|\mathbf{u}|}{\Omega}$ . L'approximation du premier ordre est appelée approximation du champ tournant. Elle consiste simplement à négliger les termes oscillant à la pulsation  $2\Omega$  et de moyenne nulle. Ainsi  $|\phi\rangle$  vérifie, à des petits termes oscillant à la pulsation  $2\Omega$ , l'équation moyenne :

$$i \frac{d}{dt} |\phi\rangle = \left( \frac{\mathbf{u}}{2} \sigma_- + \frac{\mathbf{u}^*}{2} \sigma_+ \right) |\phi\rangle.$$

C'est encore une équation de type Schrödinger mais avec l'hamiltonien dit effectif

$$H_{eff} = \frac{\mathbf{u}}{2} \sigma_- + \frac{\mathbf{u}^*}{2} \sigma_+.$$

On suppose jusqu'à la fin de cette sous-section  $\mathbf{u} = \omega_r e^{i\theta}$  avec  $\omega_r > 0$  et  $\theta$  réels et constants. Alors

$$\frac{\mathbf{u}^* \sigma_+ + \mathbf{u} \sigma_-}{2} = \frac{\omega_r}{2} (\cos \theta \sigma_x + \sin \theta \sigma_y)$$

et le système oscille entre  $|e\rangle$  et  $|g\rangle$  avec la pulsation de Rabi  $\frac{\omega_r}{2}$ . En effet  $(\cos \theta \sigma_x + \sin \theta \sigma_y)^2 = \mathbb{I}$ , donc

$$e^{-i \frac{\omega_r t}{2} (\cos \theta \sigma_x + \sin \theta \sigma_y)} = \cos \left( \frac{\omega_r t}{2} \right) - i \sin \left( \frac{\omega_r t}{2} \right) (\cos \theta \sigma_x + \sin \theta \sigma_y),$$

et la solution de  $\frac{d}{dt} |\phi\rangle = \frac{-i\omega_r}{2} (\cos \theta \sigma_x + \sin \theta \sigma_y) |\phi\rangle$  est

$$|\phi\rangle_t = \cos \left( \frac{\omega_r t}{2} \right) |g\rangle - i \sin \left( \frac{\omega_r t}{2} \right) e^{-i\theta} |e\rangle, \quad \text{quand } |\phi\rangle_0 = |g\rangle,$$

$$|\phi\rangle_t = \cos \left( \frac{\omega_r t}{2} \right) |e\rangle - i \sin \left( \frac{\omega_r t}{2} \right) e^{i\theta} |g\rangle, \quad \text{quand } |\phi\rangle_0 = |e\rangle,$$

On part souvent de l'état fondamental  $|\phi\rangle_0 = |g\rangle$  et on prend une amplitude  $\mathbf{u} = -i\omega_r$  complexe constante sur  $[0, T]$  (pulse de durée  $T$ ). Comme

$$|\phi\rangle_T = \cos \left( \frac{\omega_r T}{2} \right) |g\rangle + \sin \left( \frac{\omega_r T}{2} \right) |e\rangle,$$

on voit que

- si  $\omega_r T = \pi$  alors  $|\phi\rangle_T = |e\rangle$  et donc on bascule sur l'état excité par absorption stimulée d'un photon. Si on mesure l'énergie dans cet état on trouve toujours  $H_e$ . C'est un pulse  $\pi$ .
- si  $\omega_r T = \pi/2$  alors  $|\phi\rangle_T = (|g\rangle + |e\rangle)/\sqrt{2}$  et le système est dans une superposition cohérente de  $|g\rangle$  et  $|e\rangle$ . Si on mesure l'énergie dans cet état, on trouve  $H_g$  ou  $H_e$  avec une probabilité de  $1/2$  pour  $H_g$  et  $H_e$ . C'est un pulse  $\pi/2$ .

Comme  $|\psi\rangle = e^{-\frac{i\Omega t}{2}\sigma_z} |\phi\rangle$ , on voit qu'un pulse  $\pi$  transfère  $|\psi\rangle$  de  $|g\rangle$  en  $t = 0$  vers  $e^{i\alpha}|e\rangle$  en  $t = T = \frac{\pi}{\omega_r}$  où la phase  $\alpha \approx \frac{\Omega}{\omega_r}\pi$  est très grande car  $\omega_r \ll \Omega$ . De façon similaire, une pulse  $\pi/2$ , transfère  $|\psi\rangle$  de  $|g\rangle$  en  $t = 0$  à  $\frac{e^{-i\alpha}|g\rangle + e^{i\alpha}|e\rangle}{\sqrt{2}}$  en  $t = T = \frac{\pi}{2\omega_r}$  avec une demie-phase relative  $\alpha \approx \frac{\Omega}{2\omega_r}\pi$  très grande. Ainsi, ce type de pulse est bien adapté lorsque les états initiaux  $|\psi\rangle_0$  et finaux  $|\psi\rangle_T$  sont caractérisés par  $|\langle\psi|g\rangle|^2$  et  $|\langle\psi|e\rangle|^2$  où ces termes de phase disparaissent. On parle alors de populations puisque  $|\langle\psi|g\rangle|^2$  (resp.  $|\langle\psi|e\rangle|^2$ ) est la probabilité de trouver  $H_g$  (resp.  $H_e$ ) lorsque l'on mesure l'énergie du système isolé  $H_0 = H_g |g\rangle\langle g| + H_e |e\rangle\langle e|$ .

### Opérateur densité et sphère de Bloch

On part de  $|\psi\rangle$  qui vérifie  $\frac{d}{dt}|\psi\rangle = -iH|\psi\rangle$ . On considère le projecteur orthogonal  $\rho = |\psi\rangle\langle\psi|$ , dit opérateur densité. Alors  $\rho$  est un opérateur auto-adjoint  $\geq 0$ , vérifie  $\text{Tr}(\rho) = 1$ ,  $\rho^2 = \rho$  et obéit à l'équation :

$$\frac{d}{dt}\rho = -i[H, \rho]$$

où  $[\cdot, \cdot]$  est le commutateur :  $[H, \rho] = H\rho - \rho H$ . Dans le passage de  $|\psi\rangle$  au projecteur  $\rho$  on perd la phase globale, qui, on l'a vu ci-dessus, n'a pas de sens physique. En effet, pour toute phase  $\theta$ ,  $|\psi\rangle$  et  $e^{i\theta}|\psi\rangle$  donnent le même projecteur  $\rho$ .

Pour un système à deux niveaux  $|\psi\rangle = \psi_g |g\rangle + \psi_e |e\rangle$  et on a

$$|\psi\rangle\langle\psi| = |\psi_g|^2 |g\rangle\langle g| + \psi_g \psi_e^* |g\rangle\langle e| + \psi_g^* \psi_e |e\rangle\langle g| + |\psi_e|^2 |e\rangle\langle e|.$$

En posant

$$x = 2\Re(\psi_g \psi_e^*), \quad y = 2\Im(\psi_g \psi_e^*), \quad z = |\psi_e|^2 - |\psi_g|^2$$

on obtient l'écriture suivante

$$\rho = \frac{I + x\sigma_x + y\sigma_y + z\sigma_z}{2}.$$

Ainsi  $(x, y, z) \in \mathbb{R}^3$  s'interprète comme les coordonnées dans une base orthonormée  $(\vec{i}, \vec{j}, \vec{k})$  d'un vecteur  $\vec{M}$  de  $\mathbb{R}^3$ , dit vecteur de Bloch :

$$\vec{M} = x\vec{i} + y\vec{j} + z\vec{k}.$$

Comme  $\text{Tr}(\rho^2) = x^2 + y^2 + z^2 = 1$ ,  $\vec{M}$  est de longueur unité. Il évolue sur la sphère unité, dite sphère de Bloch, selon

$$\frac{d}{dt}\vec{M} = (u\vec{i} + \Omega\vec{k}) \times \vec{M},$$

une autre écriture de  $\frac{d}{dt}\rho = -i \left[ \frac{\Omega}{2}\sigma_z + \frac{u}{2}\sigma_x, \rho \right]$ . Ainsi  $u\vec{i} + \Omega\vec{k}$  est la vitesse instantanée de rotation. Cette interprétation géométrique de la dynamique de  $|\psi\rangle$  sur la sphère de Bloch est très utilisée en résonance magnétique où le système à deux niveaux est alors un spin  $\frac{1}{2}$ . La connaissance de  $\vec{M}$  est équivalente à celle de  $|\psi\rangle$  à une phase globale près.

Lorsque l'état quantique n'est pas pur, alors  $x^2 + y^2 + z^2 = \text{Tr}(\rho^2) \leq 1$  et alors le vecteur  $\vec{M}$  est à l'intérieur de la sphère de Bloch. L'équation de Schrödinger redonne la même équation différentielle pour  $\vec{M}$ .

### 3.3 Oscillateur harmonique

On trouvera dans [11] un exposé bien plus didactique. La formulation hamiltonienne d'un oscillateur harmonique de pulsation  $\omega$ ,  $\frac{d^2}{dt^2}x = -\omega^2x$ , est la suivante :

$$\frac{d}{dt}x = \omega p = \frac{\partial \mathbf{H}}{\partial p}, \quad \frac{d}{dt}p = -\omega x = -\frac{\partial \mathbf{H}}{\partial x}$$

avec l'hamiltonien classique  $\mathbf{H}(x, p) = \frac{\omega}{2}(p^2 + x^2)$ . Le principe de correspondance donne directement la quantification suivante. l'hamiltonien classique devient un opérateur,  $H$ , qui opère sur les fonctions de  $x \in \mathbb{R}$  à valeurs complexes. L'état classique  $(x, p)$  est alors remplacé par la fonction d'onde  $|\psi\rangle$ . C'est une fonction de  $x$  et  $t$  :  $\psi(x, t) \in \mathbb{C}$ . A chaque instant  $t$ ,  $\mathbb{R} \ni x \mapsto \psi(x, t)$  est mesurable et de carré sommable :  $\int_{\mathbb{R}} |\psi(x, t)|^2 dx = 1$ . Ainsi pour tout  $t$ ,  $|\psi\rangle_t \in L^2(\mathbb{R}, \mathbb{C})$ .

L'opérateur hamiltonien  $H$  est obtenu en remplaçant dans l'hamiltonien classique  $\mathbf{H}$ ,  $x$  par l'opérateur  $X$ , la multiplication par  $\frac{x}{\sqrt{2}}$  et  $p$  par  $P = -\frac{i}{\sqrt{2}}\frac{\partial}{\partial x}$ , l'opérateur de dérivation partielle par rapport à  $x$  à  $t$  fixé. Ainsi on a

$$H = \omega(P^2 + X^2) = -\frac{\omega}{2}\frac{\partial^2}{\partial x^2} + \frac{\omega}{2}x^2.$$

L'équation de Schrödinger

$$\frac{d}{dt} |\psi\rangle = -\imath H |\psi\rangle$$

est alors une équation aux dérivées partielles qui définit  $\psi(x, t)$  en fonction de la condition initiale  $(\psi(x, 0))_{x \in \mathbb{R}}$  :

$$\imath \frac{\partial \psi}{\partial t}(x, t) = -\frac{\omega}{2} \frac{\partial^2 \psi}{\partial x^2}(x, t) + \frac{\omega}{2} x^2 \psi(x, t), \quad x \in \mathbb{R}.$$

La position moyenne est donc

$$\langle X \rangle_t = \langle \psi | X | \psi \rangle = \frac{1}{\sqrt{2}} \int_{-\infty}^{+\infty} x |\psi|^2 dx,$$

et l'impulsion moyenne

$$\langle P \rangle_t = \langle \psi | P | \psi \rangle = -\frac{\imath}{\sqrt{2}} \int_{-\infty}^{+\infty} \psi^* \frac{\partial \psi}{\partial x} dx.$$

Une simple intégration par partie montre que  $\langle P \rangle_t$  est bien réel.

Il est très utile de considérer les opérateurs d'annihilation et de création de photons  $a$  et  $a^\dagger$  :

$$a = X + \imath P = \frac{1}{\sqrt{2}} \left( x + \frac{\partial}{\partial x} \right), \quad a^\dagger = X - \imath P = \frac{1}{\sqrt{2}} \left( x - \frac{\partial}{\partial x} \right). \quad (3.1)$$

On a

$$[X, P] = \frac{\imath}{2} \mathbb{I}, \quad [a, a^\dagger] = \mathbb{I}, \quad H = \omega(P^2 + X^2) = \omega \left( a^\dagger a + \frac{1}{2} \mathbb{I} \right)$$

où  $\mathbb{I}$  est l'opérateur identité. Usuellement on note aussi  $\mathbb{I}$  par 1. Cela donne les expressions compactes :

$$[X, P] = \frac{\imath}{2}, \quad [a, a^\dagger] = 1, \quad H = \omega(P^2 + X^2) = \omega \left( a^\dagger a + \frac{1}{2} \right)$$

Comme  $[a, a^\dagger] = 1$ , la décomposition spectrale de  $a^\dagger a$  est simple et justifie la dénomination de  $a$  et de  $a^\dagger$ . L'opérateur hermitien  $a^\dagger a$  admet  $\mathbb{N}$  comme spectre non dégénéré. Le vecteur propre unitaire associé à la valeur propre  $n \in \mathbb{N}$  est noté  $|n\rangle$  : on l'appelle état de Fock avec  $n$  quanta (des photons pour les ondes électro-magnétiques, des phonons pour des vibrations mécaniques). On a pour tout  $n > 0$ ,

$$a|n\rangle = \sqrt{n} |n-1\rangle, \quad a^\dagger|n\rangle = \sqrt{n+1} |n+1\rangle.$$

L'état fondamental  $|0\rangle$  est caractérisé par  $a|0\rangle = 0$ . Il correspond à la fonction gaussienne :

$$\psi_0(x) = \frac{1}{\pi^{1/4}} \exp(-x^2/2).$$

$a$  (resp.  $a^\dagger$ ) correspond à l'opérateur d'annihilation (resp. de création) car il envoie  $|n\rangle$  sur  $|n-1\rangle$  (resp.  $|n+1\rangle$ ) et donc diminue (resp. augmente) le nombre de quanta d'une unité.

On note  $N = a^\dagger a$  l'opérateur nombre de quanta car  $N|n\rangle = n|n\rangle$  et donc  $N = \sum_n n |n\rangle\langle n|$ . On peut montrer que pour toute fonction  $f$  on a les relations de commutation suivante :

$$af(N) = f(N + \mathbb{I})a, \quad a^\dagger f(N) = f(N - \mathbb{I})a^\dagger.$$

Ainsi  $e^{i\theta N} a e^{-i\theta N} = e^{-i\theta} a$  et  $e^{i\theta N} a^\dagger e^{-i\theta N} = e^{i\theta} a^\dagger$ .

Pour chaque amplitude complexe  $\alpha \in \mathbb{C}$ , on considère l'opérateur unitaire  $D_\alpha$  défini par

$$D_\alpha = e^{\alpha a^\dagger - \alpha^* a} \quad (3.2)$$

appelé opérateur de déplacement de Glauber. On remarque que  $D_\alpha^{-1} = D_\alpha^\dagger = D_{-\alpha}$ . Une formule très utile est la suivante (formule de Glauber) : si deux opérateurs  $A$  et  $B$  commutent avec leur commutateur, i.e., si  $[A, [A, B]] = [B, [A, B]] = 0$ , alors on a

$$e^{A+B} = e^A e^B e^{-\frac{1}{2}[A,B]} \quad (3.3)$$

Comme c'est le cas pour  $A = \alpha a^\dagger$  et  $B = -\alpha^* a$ , on a une autre expression de  $D_\alpha$

$$D_\alpha = e^{-\frac{|\alpha|^2}{2}} e^{\alpha a^\dagger} e^{-\alpha^* a} = e^{+\frac{|\alpha|^2}{2}} e^{-\alpha^* a} e^{\alpha a^\dagger}. \quad (3.4)$$

Le terme déplacement vient de la propriété suivante, valable pour tout complexe  $\alpha$  :

$$D_{-\alpha} a D_\alpha = a + \alpha \quad \text{and} \quad D_{-\alpha} a^\dagger D_\alpha = a^\dagger + \alpha^*. \quad (3.5)$$

Un état cohérent d'amplitude  $\alpha$ , usuellement noté  $|\alpha\rangle$ , est défini par  $D_\alpha$  :

$$|\alpha\rangle = D_\alpha |0\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{+\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \quad (3.6)$$

La probabilité  $p_n$  d'obtenir  $n \in \mathbb{N}$  lors d'une mesure de  $N$  sur  $|\alpha\rangle$  suit une loi de Poisson  $p_n = e^{-|\alpha|^2} |\alpha|^{2n} / n!$ . L'énergie moyenne de  $|\alpha\rangle$  est donnée par

$$\langle \alpha | N | \alpha \rangle = |\alpha|^2.$$



Il faut faire un peu attention avec ces notations très utilisées en optique quantique : pour  $\alpha = n$  entier positive, l'état cohérent d'amplitude  $\alpha$  et l'état de Fock avec  $n$  photons, notés tous les deux  $|\alpha\rangle$  et  $|n\rangle$  ne se correspondent que pour l'état du vide quantique  $\alpha = n = 0$ .

L'état cohérent d'amplitude  $\alpha \in \mathbb{C}$  est le vecteur propre unitaire de  $a$  de valeur propre complexe  $\alpha$  :

$$a|\alpha\rangle = \alpha|\alpha\rangle.$$

Il est aussi facile de voir que, comme  $H = \omega(N + \frac{1}{2})$ , la solution de  $\frac{d}{dt}|\psi\rangle = -iH|\psi\rangle$ , de condition initiale l'état cohérent d'amplitude  $\alpha_0 \in \mathbb{C}$ ,  $|\psi\rangle_{t=0} = |\alpha_0\rangle$ , reste un état cohérent d'amplitude  $\alpha_t = e^{-i\omega t}\alpha_0$  :

$$|\psi\rangle_t = e^{-i\omega t/2}|\alpha_t\rangle.$$

Ces états cohérents sont les états quantiques correspondant aux solutions de l'équation de l'oscillateur harmonique. En effet, comme  $\frac{d}{dt}\alpha_t = -i\omega\alpha_t$ , on voit qu'en posant  $\alpha_t = x + ip$ , avec  $(x, p) \in \mathbb{R}^2$  on retrouve les deux équations classiques sous forme hamiltonienne de l'oscillateur harmonique :  $\frac{d}{dt}x = \omega p$ ,  $\frac{d}{dt}p = -\omega x$ .

## 3.4 Mesures généralisées et trajectoires quantiques

### 3.4.1 La boîte à photons du LKB

Serge Haroche a obtenu le prix Nobel de physique 2012 pour toute une série d'expériences sur l'observation et la manipulation de photons. Dans son livre écrit avec Jean-Michel Raimond [21], il présente des expériences, conduites au laboratoire Kastler-Brossel (LKB) de l'école normale supérieure de Paris, où des photons micro-ondes sont observés et manipulés sans les détruire. Nous décrivons ici très schématiquement l'une de ces expériences. Le but est d'illustrer pour mieux les comprendre, trois ingrédients spécifiques au monde quantique :

1. l'équation différentielle linéaire de Schrödinger qui gouverne l'évolution unitaire de la fonction d'onde ;
2. l'intrication due au fait que l'espace de Hilbert d'un système composite est le produit tensoriel des espaces de Hilbert attachés aux sous-systèmes qui le composent ;
3. la réduction du paquet d'ondes liée au processus de mesure.

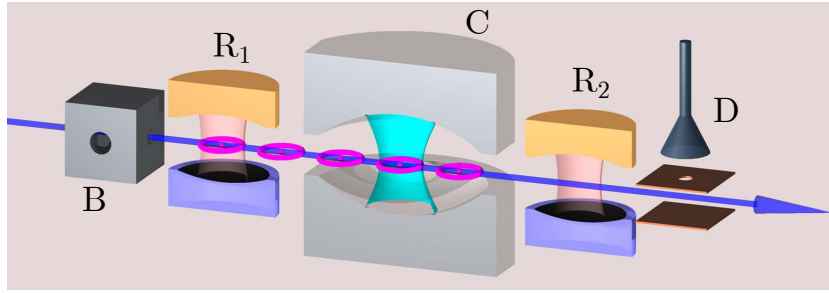


FIGURE 3.2 – Schéma de l'expérience du LKB qui observe des photons sans les détruire. Les photons piégés entre les deux miroirs de la cavité  $C$  sont mesurés avec des atomes (les petits anneaux couleur rose foncé) sortant de  $B$ . Les atomes traversent l'un après l'autre la cavité  $C$ . Ils sont manipulés individuellement avant et après leur passage dans la cavité dans  $R_1$  et  $R_2$ . Ils sont mesurés par le détecteur  $D$  soit dans un état de basse énergie  $|g\rangle$  soit dans un état de forte énergie  $|e\rangle$ .

Usuellement, un photo-détecteur est un capteur qui compte des photons tout en les détruisant. Les expériences du LKB ont montré qu'il était possible de compter des photons un par un et sans les détruire. Nous allons ici décrire succinctement les principales étapes pour réaliser ce type de comptage non destructif.

Ces photons correspondent aux états quantiques d'un oscillateur harmonique. Cet oscillateur harmonique est obtenu après quantification d'un mode du champ micro-onde piégé entre les deux miroirs supra-conducteurs de la cavité  $C$ , la zone en bleu clair et de dimension centimétrique sur la figure 3.2. La fonction d'onde de ces photons piégés dans  $C$  est notée  $|\psi\rangle$  et  $\mathcal{H}_S = l^2(\mathbb{C})$  correspond aux suites complexes de carré sommable :

$$\mathcal{H}_S = \left\{ |\psi\rangle = \sum_{n=0}^{\infty} \psi_n |n\rangle \mid (\psi_n)_{n=0}^{\infty} \in l^2(\mathbb{C}) \right\},$$

où  $|n\rangle$  représente un état quantique d'énergie parfaitement déterminée avec exactement  $n$  photons (état de Fock). Les  $|n\rangle$  pour  $n \in \mathbb{N}$  forment une base hilbertienne de  $\mathcal{H}_S$  :  $\langle n|n'\rangle = \delta_{n,n'}$ . La mesure porte uniquement sur les atomes qui traversent l'un après l'autre la cavité  $C$ . Ils sont mesurés en  $D$ .

Pour analyser l'effet de la mesure d'un atome ayant traversé la cavité sur les photons dans la cavité, il est suffisant de le décrire par un système à deux niveaux, un niveau bas  $|g\rangle$  et un niveau haut  $|e\rangle$ . Ainsi l'espace de Hilbert associé à un atome est simplement  $\mathcal{H}_M = \mathbb{C}^2$  avec comme base orthonormée  $(|g\rangle, |e\rangle)$ . Quand un atome sort de  $B$  (cf. figure 3.2) il est toujours dans l'état  $|g\rangle$ . Les atomes se succèdent au rythme d'un atome par

période d'échantillonnage  $\tau$ . Nous allons considérer ce qu'il se passe durant une période de  $t = 0^+$  à  $t = \tau^-$  : à  $t = 0^+$ , un atome sort de  $B$  dans l'état  $|g\rangle \in \mathcal{H}_M$  pour traverser ensuite  $R_1$ ,  $C$ ,  $R_2$  et enfin arriver à  $D$  au temps  $t = \tau^-$  où l'on mesure son énergie. Nous donnons ci-dessous une description des diverses transformations que subissent l'atome et la cavité entre 0 et  $\tau$ . Cette description est simplifiée pour que les calculs soient élémentaires. Elle n'en reste pas moins très représentative de descriptions plus élaborées.

### 3.4.2 Physique et modélisation simplifiées

Sur  $]0, \tau[$ , nous avons un système composite dont la fonction d'onde  $|\Psi\rangle$  évolue avec  $t$  et appartient à  $\mathcal{H}_S \otimes \mathcal{H}_M$ . Comme à  $t = 0^+$  l'atome sortant de  $B$  et les photons dans  $C$  n'ont rien à voir entre eux, l'état quantique en  $t = 0^+$  est séparable :

$$|\Psi\rangle_{0^+} = |\psi\rangle_{0^+} \otimes |g\rangle$$

où  $|\psi\rangle_{0^+} \in \mathcal{H}_S$  est l'état dans la cavité supposé pur.

En  $\tau_1 < \tau$ , l'atome est entre  $R_1$  et  $C$  : il a subi une transformation unitaire dans  $R_1$  correspondant à un hamiltonien agissant sur  $|\Psi\rangle$  de la forme  $H(t) = \mathbb{I} \otimes u_1(t)(|e\rangle\langle g| - |g\rangle\langle e|)$  valable entre les instants  $t = 0^+$  et  $t = \tau_1$  ( $u_1(t) \in \mathbb{R}$  est un contrôle classique correspondant à une impulsion micro-onde très similaire à celles utilisées dans les téléphones portables). Le propagateur  $U$  solution de

$$\frac{d}{dt}U = -iH(t)U(t), \quad U(0^+) = \mathbb{I}$$

est de la forme  $U(\tau_1) = \mathbb{I} \otimes U_{R_1}$  où  $u_1(t)$  est ajusté pour que

$$U(\tau_1) = \mathbb{I} \otimes U_{R_1} \equiv \frac{1}{\sqrt{2}}(|g\rangle\langle g| + |e\rangle\langle g| - |g\rangle\langle e| + |e\rangle\langle e|).$$

Dans cette dernière égalité nous n'avons pas rappelé le produit tensoriel avec l'identité sur  $\mathcal{H}_S$ . Ainsi en  $t = \tau_1$ , on a

$$|\Psi\rangle_{\tau_1} = U(\tau_1) |\Psi\rangle_{0^+} = |\psi\rangle_{0^+} \otimes \left( \frac{|g\rangle + |e\rangle}{\sqrt{2}} \right) = \frac{1}{\sqrt{2}} |\psi\rangle_{0^+} \otimes |g\rangle + \frac{1}{\sqrt{2}} |\psi\rangle_{0^+} \otimes |e\rangle.$$

$|\Psi\rangle_{\tau_1}$  reste un état séparable. L'atome et la cavité ne sont pas encore intriqués. On peut encore parler de l'état de l'atome atomique,  $\frac{|g\rangle + |e\rangle}{\sqrt{2}}$  et de celui de la cavité  $|\psi\rangle_{0^+}$ .

En  $\tau_c \in ]\tau_1, \tau[$ , l'atome est entre  $C$  et  $R_2$  : l'état  $|\Psi\rangle$  a évolué entre  $t \in [\tau_1, \tau_c]$  selon un hamiltonien de la forme  $H(t) = \frac{\Omega(t)}{2} N \otimes (|e\rangle\langle e| - |g\rangle\langle g|)$  où  $\Omega(t) > 0$  est un paramètre réglable (interaction dispersive atome/cavité, voir [21]).  $N$  est ici l'opérateur nombre de photons :  $N = \sum_n n |n\rangle\langle n|$  et donc

### 3.4. MESURES GÉNÉRALISÉES ET TRAJECTOIRES QUANTIQUES 67

pour tout entier  $n$ ,  $N|n\rangle = n|n\rangle$ . Un calcul direct montre que le propagateur entre  $\tau_1$  et  $\tau_1 + \tau_c$ , solution de

$$\frac{d}{dt}U = -i \left( \frac{\Omega(t)}{2} N \otimes (|e\rangle\langle e| - |g\rangle\langle g|) \right) U(t), \quad U(\tau_1) = \mathbb{I}$$

est de la forme

$$U(\tau_c) = \exp(-i\frac{\theta}{2}N) \otimes |e\rangle\langle e| + \exp(i\frac{\theta}{2}N) \otimes |g\rangle\langle g|$$

où  $\theta = \int_{\tau_1}^{\tau_c} \Omega(t)dt$ . Ainsi on a

$$|\Psi\rangle_{\tau_c} = U(\tau_c) |\Psi\rangle_{\tau_1} = \frac{1}{\sqrt{2}} \exp(i\frac{\theta}{2}N) |\psi\rangle_{0+} \otimes |g\rangle + \frac{1}{\sqrt{2}} \exp(-i\frac{\theta}{2}N) |\psi\rangle_{0+} \otimes |e\rangle.$$

Cet état n'est plus séparable en général (sauf si  $|\psi\rangle_{0+} = |n\rangle$  pour un certain  $n \in \mathbb{N}$ ). On ne peut plus définir la fonction d'onde de la cavité et celle de l'atome séparément : en  $t = \tau_c$  l'atome et la cavité sont intriqués. Cette intrication va durer jusqu'à la mesure de l'atome en  $t = \tau^-$ .

En  $\tau_2 \in ]\tau_c, \tau[$  l'atome est entre  $R_2$  et le détecteur  $D$  : on s'arrange pour que le système subisse la même évolution qu'entre  $t = 0^+$  et  $t = \tau_1$ , évolution donnée par le propagateur  $\frac{1}{\sqrt{2}}(|g\rangle\langle g| + |e\rangle\langle g| - |g\rangle\langle e| + |e\rangle\langle e|)$ . Un calcul simple montre que

$$|\Psi\rangle_{\tau_2} = i \sin\left(\frac{\theta}{2}N\right) |\psi\rangle_{0+} \otimes |g\rangle + \cos\left(\frac{\theta}{2}N\right) |\psi\rangle_{0+} \otimes |e\rangle.$$

Entre  $\tau_2$  et  $\tau^-$ , il ne se passe rien et donc  $|\Psi\rangle_{\tau^-} = |\Psi\rangle_{\tau_2}$ .

En  $t = \tau^-$  on mesure l'énergie de l'atome. L'opérateur de mesure est donc  $M = |e\rangle\langle e| - |g\rangle\langle g|$ . La valeur propre  $+1$  est associée au projecteur  $P_e$  sur l'espace propre  $\mathcal{H}_S \otimes |e\rangle$ ,  $P_e = \mathbb{I} \otimes |e\rangle\langle e| \equiv |e\rangle\langle e|$ . La valeur propre  $-1$  est associée au projecteur  $P_g$  sur l'espace propre  $\mathcal{H}_S \otimes |g\rangle$ ,  $P_g = \mathbb{I} \otimes |g\rangle\langle g| \equiv |g\rangle\langle g|$ . Selon la théorie de la mesure, on mesure  $+1$  avec la probabilité  $\langle \Psi | P_e | \Psi \rangle_{\tau^-}$  et  $-1$  avec  $\langle \Psi | P_g | \Psi \rangle_{\tau^-}$ . Avec les opérateurs de Kraus  $M_g = i \sin\left(\frac{\theta}{2}N\right)$  et  $M_e = \cos\left(\frac{\theta}{2}N\right)$  on a

$$|\Psi\rangle_{\tau^-} = (M_g |\psi\rangle_{0+}) \otimes |g\rangle + (M_e |\psi\rangle_{0+}) \otimes |e\rangle.$$

Comme la transformation de  $|\Psi\rangle_{0+}$  vers  $|\Psi\rangle_{\tau^-}$  est unitaire (composition des trois transformations unitaires résultant des passages dans  $R_1$ ,  $C$  et  $R_2$  de l'atome), on voit que nécessairement,  $M_g^\dagger M_g + M_e^\dagger M_e = \mathbb{I}$ . Ici cette identité est évidente car  $\cos^2 + \sin^2 = 1$ .

Si on détecte  $+1$  (resp.  $-1$ ), il y a réduction du paquet d'ondes  $|\Psi\rangle_{\tau^-}$  sur  $(M_e |\psi\rangle_{0+}) \otimes |e\rangle$  (resp.  $(M_g |\psi\rangle_{0+}) \otimes |g\rangle$ ). Après la mesure, le nouvel état noté  $|\Psi\rangle_{\tau^+}$  est redevenu séparable : l'atome et la cavité ne sont plus intriqués.

Aussi on résume le passage de  $t = 0^+$  à  $t = \tau^+$  par le processus stochastique suivant :

$$|\psi\rangle_{\tau^+} = \begin{cases} \frac{M_g|\psi\rangle_{0^+}}{\sqrt{p_g}}, & \text{avec la probabilité } p_g = \langle\psi|M_g^\dagger M_g|\psi\rangle_{0^+}; \\ \frac{M_e|\psi\rangle_{0^+}}{\sqrt{p_e}}, & \text{avec la probabilité } p_e = \langle\psi|M_e^\dagger M_e|\psi\rangle_{0^+}. \end{cases}$$

Il s'agit d'une chaîne de Markov d'état  $|\psi\rangle \in \mathcal{H}_S$ . On oublie ici l'atome qui a permis de mesurer indirectement et sans trop les perturber les photons piégés dans  $C$ .

Dans le langage de la matrice densité, il suffit de se souvenir que pour un état pur  $\rho = |\psi\rangle\langle\psi|$ . Alors on obtient la chaîne de Markov pour des états mixtes :

$$\rho(\tau^+) = \begin{cases} \frac{M_g\rho(0^+)M_g^\dagger}{\text{Tr}(M_g\rho(0^+)M_g^\dagger)}, & \text{avec la probabilité } p_g = \text{Tr}(M_g\rho(0^+)M_g^\dagger); \\ \frac{M_e\rho(0^+)M_e^\dagger}{\text{Tr}(M_e\rho(0^+)M_e^\dagger)}, & \text{avec la probabilité } p_e = \text{Tr}(M_e\rho(0^+)M_e^\dagger). \end{cases}$$

### 3.4.3 Réduction progressive du paquet d'ondes et mesure quantique non destructive

Pour  $k \in \mathbb{N}$ , on note  $\rho(k\tau^+)$  par  $\rho_k$ . On a donc

$$\rho_{k+1} = \begin{cases} \frac{M_g\rho_k M_g^\dagger}{\text{Tr}(M_g\rho_k M_g^\dagger)}, & \text{avec la probabilité } p_{g,k} = \text{Tr}(M_g\rho_k M_g^\dagger); \\ \frac{M_e\rho_k M_e^\dagger}{\text{Tr}(M_e\rho_k M_e^\dagger)}, & \text{avec la probabilité } p_{e,k} = \text{Tr}(M_e\rho_k M_e^\dagger); \end{cases} \quad (3.7)$$

avec  $M_g = \sin\left(\frac{\theta}{2}N\right)$  et  $M_e = \cos\left(\frac{\theta}{2}N\right)$ . Comme  $N = \sum_n n|n\rangle\langle n|$ , les opérateurs  $M_g$  et  $M_e$  sont diagonaux dans la base de Fock  $(|n\rangle)_n$  :  $M_g = \sum_n \sin\left(\frac{n\theta}{2}\right)|n\rangle\langle n|$  et  $M_e = \sum_n \cos\left(\frac{n\theta}{2}\right)|n\rangle\langle n|$ .

Nous allons maintenant étudier les propriétés de cette chaîne de Markov d'état  $\rho \in \mathcal{D}$ . Partant d'une même condition initiale  $\rho_0$ , chaque réalisation donne lieu à une trajectoire  $k \mapsto \rho_k$  différente, *une trajectoire quantique* (en temps discret). Cependant, nous allons voir que chacune de ces trajectoires converge vers un état pur  $|n\rangle\langle n|$ , un état de Fock.

Pour éviter les complications mathématiques liées au fait que  $\mathcal{H}_S$  est de dimension finie, nous allons considérer dans toute la suite que l'on tronque  $\mathcal{H}_S$  à un nombre fini de photon  $n_{max} > 0$  qui peut être aussi grand que l'on veut :

$$\bar{\mathcal{H}}_S = \left\{ |\psi\rangle = \sum_{n=0}^{n_{max}} \psi_n |n\rangle \mid \psi_n \in \mathbb{C} \right\}.$$

Cette troncature aux nombres de photons plus petits que  $n_{max}$  ne pose pas de problème puisque  $M_g$  et  $M_e$  sont des opérateurs diagonaux dans la base hilbertienne des états de Fock  $(|n\rangle\langle n|)_{n \in \mathbb{N}}$ .

Il est facile de voir que si  $\rho_0 \in \mathcal{D}$  alors pour tout  $k \geq 0$ ,  $\rho_k \in \mathcal{D}$ . Si  $\rho_0 = |n\rangle\langle n|$  pour un entier  $n$  (état de Fock) alors  $\rho_1 = \rho_0$  et donc  $\rho_k \equiv |n\rangle\langle n|$  pour tout  $k \geq 0$ . Cela découle directement du fait que  $|n\rangle$  est un vecteur propre à la fois de  $M_g$  et  $M_e$  :  $M_g |n\rangle = \sin\left(\frac{n\theta}{2}\right) |n\rangle$  et  $M_e |n\rangle = \cos\left(\frac{n\theta}{2}\right) |n\rangle$ . Ainsi tous les états purs  $|n\rangle\langle n|$  sont des états stationnaires de cette chaîne de Markov.

Pour deux variables aléatoires  $X$  et  $Y$ , on note  $\mathbb{E}(X \setminus Y)$  l'espérance conditionnelle de la variable aléatoire  $X$  sachant  $Y$ . Pour chaque entier  $k \geq 0$ , calculons l'espérance conditionnelle de  $X = \text{Tr}(|n\rangle\langle n| \rho_{k+1}) = \langle n | \rho_{k+1} | n \rangle$  sachant  $Y = \rho_k$ . On a grâce à (3.7)

$$\begin{aligned} \mathbb{E}(\langle n | \rho_{k+1} | n \rangle \setminus \rho_k) &= p_{g,k} \left\langle n \left| \frac{M_g \rho_k M_g^\dagger}{\text{Tr}(M_g \rho_k M_g^\dagger)} \right| n \right\rangle + p_{e,k} \left\langle n \left| \frac{M_e \rho_k M_e^\dagger}{\text{Tr}(M_e \rho_k M_e^\dagger)} \right| n \right\rangle \\ &= \langle n | M_g \rho_k M_g^\dagger + M_e \rho_k M_e^\dagger | n \rangle = \langle n | \mathcal{K}(\rho_k) | n \rangle \end{aligned}$$

où  $\mathcal{K}$  est un super-opérateur, dit opérateur de Kraus, défini par

$$\mathcal{K}(\rho) = M_g \rho M_g^\dagger + M_e \rho M_e^\dagger. \quad (3.8)$$

Comme  $M_g^\dagger M_g + M_e^\dagger M_e = \mathbb{I}$ , on voit que si  $\rho \in \mathcal{D}$  alors  $\mathcal{K}(\rho) \in \mathcal{D}$ . On note  $\mathcal{K}^*$  l'opérateur adjoint défini par

$$\mathcal{K}^*(A) = M_g^\dagger A M_g + M_e^\dagger A M_e$$

et caractérisé par :

$$\forall A, B \in L(\mathcal{H}, \mathcal{H}), \text{Tr}(A \mathcal{K}(B)) = \text{Tr}(\mathcal{K}^*(A) B).$$

On a donc  $\mathbb{E}(\text{Tr}(|n\rangle\langle n| \rho_{k+1}) \setminus \rho_k) = \text{Tr}(\mathcal{K}^*(|n\rangle\langle n|) \rho_k)$ . Comme  $\mathcal{K}^*(|n\rangle\langle n|) = |n\rangle\langle n|$ , on voit que la variable aléatoire  $\text{Tr}(|n\rangle\langle n| \rho) = \langle n | \rho | n \rangle$  est *une martingale* car son espérance reste constante au cours des itérations sur  $k$  :

$$\mathbb{E}(\langle n | \rho_{k+1} | n \rangle \setminus \rho_k) = \langle n | \rho_k | n \rangle$$

et donc  $\mathbb{E}(\langle n | \rho_{k+1} | n \rangle \setminus \rho_0) = \langle n | \rho_0 | n \rangle$  ne dépend que de la valeur initiale de  $\rho$ .

Plus généralement on voit que l'énergie  $\langle N \rangle = \text{Tr}(N \rho)$  est aussi une martingale car  $N = \sum_n n |n\rangle\langle n|$  :  $\langle N \rangle_k = \langle N \rangle_0$ . Ce processus de mesure préserve donc l'énergie : il observe les photons sans les détruire.

Considérons maintenant

$$V(\rho) = 1 - \sum_n \langle n|\rho|n \rangle^2.$$

Comme  $V(\rho)$  est une combinaison concave de martingales,  $V(\rho)$  est une *super-martingale* : son espérance décroît avec  $k$ . En effet, on part de l'identité scalaire

$$\forall x, y, p \in \mathbb{R}, \quad px^2 + (1-p)y^2 = (px + (1-p)y)^2 + p(1-p)(x-y)^2$$

avec

- $p = p_{g,k} = \sum_n \sin^2(n\theta/2) \langle n|\rho_k|n \rangle$  et  $1-p = p_{e,k} = \sum_n \cos^2(n\theta/2) \langle n|\rho_k|n \rangle$ ,
- pour chaque  $n$  entier

$$x = \sin^2(n\theta/2) \langle n|\rho_k|n \rangle / p_{g,k}, \quad y = \cos^2(n\theta/2) \langle n|\rho_k|n \rangle / (1-p_{g,k}).$$

On obtient après quelques calculs

$$\begin{aligned} \mathbb{E}(V(\rho_{k+1}) | \rho_k) - V(\rho_k) = \\ - p_{g,k}(1-p_{g,k}) \left( \sum_n \left( \frac{\sin^2(n\theta/2)}{p_{g,k}} - \frac{\cos^2(n\theta/2)}{1-p_{g,k}} \right)^2 \langle n|\rho_k|n \rangle^2 \right). \end{aligned}$$

On a donc

$$\mathbb{E}(V(\rho_{k+1})) = \mathbb{E}(V(\rho_k)) - \mathbb{E}(Q(\rho_k))$$

où

$$Q(\rho) = p_g(1-p_g) \left( \sum_n \left( \frac{\sin^2(n\theta/2)}{p_g} - \frac{\cos^2(n\theta/2)}{1-p_g} \right)^2 \langle n|\rho|n \rangle^2 \right)$$

avec  $p_g = \sum_n \sin^2(n\theta/2) \langle n|\rho|n \rangle$ . La suite  $\mathbb{E}(V(\rho_k))$  étant décroissante et positive,  $\mathbb{E}(V(\rho_{k+1})) - \mathbb{E}(V(\rho_k))$  converge vers 0. Ainsi on sait que  $\mathbb{E}(Q(\rho_k))$  converge vers 0 quand  $k$  tend vers  $+\infty$  : or  $Q \geq 0$  donc, pour presque toutes les réalisations,  $Q(\rho_k)$  converge vers 0.

Supposons  $\theta/\pi$  irrationnel et cherchons les  $\rho \in \mathcal{D}$  tels que  $Q(\rho) = 0$ . On a trois possibilités :  $p_g = 0, 1$  et  $\sum_n \left( \frac{\sin^2(n\theta/2)}{p_g} - \frac{\cos^2(n\theta/2)}{1-p_g} \right)^2 \langle n|\rho|n \rangle^2 = 0$  :

1. si  $p_g = 0$  alors, comme  $\langle n|\rho|n \rangle \geq 0$  et  $\text{Tr}(\rho) = \sum_n \langle n|\rho|n \rangle = 1$ , la seule possibilité est que  $\langle n|\rho|n \rangle = 0$  pour  $n \geq 1$  car  $\sin^2(n\theta/2) > 0$  dès que  $n \geq 1$  ; ainsi  $\rho = |0\rangle\langle 0|$ .
2. si  $p_g = 1$ , alors  $p_e = 1 - p_g = \sum_n \cos^2(n\theta/2) \langle n|\rho_k|n \rangle = 0$ . C'est impossible car  $\cos^2(n\theta/2) > 0$  pour tout  $n \geq 0$ ,  $\langle n|\rho_k|n \rangle \geq 0$  et  $\sum_n \langle n|\rho|n \rangle = 1$ .

3. si  $\left( \sum_n \left( \frac{\sin^2(n\theta/2)}{p_g} - \frac{\cos^2(n\theta/2)}{1-p_g} \right)^2 \langle n|\rho|n \rangle^2 \right) = 0$  avec  $p_g \in ]0, 1[$ , alors il existe  $n > 0$  tel que  $\rho = |n\rangle\langle n|$ . En effet, sinon, il existe  $n_1 > n_2 > 0$  tels que  $\langle n_1|\rho_k|n_1 \rangle, \langle n_2|\rho_k|n_2 \rangle > 0$ . Alors  $\frac{\sin^2(n_1\theta/2)}{p_g} - \frac{\cos^2(n_1\theta/2)}{1-p_g} = \frac{\sin^2(n_2\theta/2)}{p_g} - \frac{\cos^2(n_2\theta/2)}{1-p_g} = 0$ . Donc  $\tan^2(n_1\theta/2) = \tan^2(n_2\theta/2) = \frac{1-p_g}{p_g}$ . Mais alors nécessairement  $\cos(n_1\theta) = \cos(n_2\theta) = 2p_g - 1$  et donc  $n_1\theta = \pm n_2\theta \pmod{\pi}$ . Ce qui est aussi impossible car  $\theta/\pi$  est irrationnel et  $n_1 > n_2 > 0$ .

On voit donc que pour  $\theta/\pi$  irrationnel  $Q(\rho) = 0$  si et seulement si  $\rho = |n\rangle\langle n|$  pour un certain  $n$  entier.

Ainsi quelque soit la condition initiale  $\rho_0$ ,  $\rho_k$  converge presque sûrement vers un état de Fock  $|n\rangle\langle n|$ . Comme  $\langle n|\rho|n \rangle$  est une martingale (espérance constante), la probabilité de converger vers  $|n\rangle\langle n|$  à partir de  $\rho_0$  est simplement donnée par  $\langle n|\rho_0|n \rangle$ . Pour des  $k$  grands, tout se passe comme si on mesurait directement le nombre de photons associé à l'observable  $N$ . La probabilité d'obtenir exactement  $n$  photons est donné par  $\langle n|\rho_0|n \rangle$ . La réduction du paquet d'ondes correspond à la limite  $\rho_\infty = |n\rangle\langle n|$  de  $\rho_k$  pour  $k$  très grand. Ce processus de mesure progressive de  $N$  est donc un processus de mesure non destructive dit QND pour "Quantum Non Demolition" : il laisse intacte les états initiaux  $\rho_0 = |n\rangle\langle n|$  qui sont déjà des états ayant un nombre de photons  $n$  bien déterminé. Tout cela est en parfait accord avec la théorie de la mesure résumée dans une sous section précédente. Les expériences conduites au LKB ont confirmé cette analyse de la convergence de  $\rho_0$  vers  $|n\rangle\langle n|$  avec la probabilité  $\langle n|\rho_0|n \rangle$ .

On remarquera enfin l'analogie de cette analyse de convergence avec celle que l'on peut faire pour les solutions  $x(t)$  d'un système différentiel ordinaire  $\frac{d}{dt}x = f(x)$  vers un état stationnaire  $\bar{x}$  caractérisé par  $f(\bar{x}) = 0$  : l'évolution stochastique (3.7) remplace  $\frac{d}{dt}x = f(x)$  ; les états stationnaires  $|n\rangle\langle n|$  de (3.7) correspondent à  $\bar{x}$  ; le rôle joué ici par la super-martingale  $V(\rho)$  correspond à celui d'une fonction de Lyapunov  $V(x)$  qui décroît le long des trajectoires  $\frac{d}{dt}V = Q(x) \leq 0$  ; l'ensemble limite pour  $x(t)$  (valeur d'adhérence en  $t = +\infty$ ) est alors directement lié aux solutions de  $Q(x) = 0$ . On pourra se référer à [25] pour des énoncés mathématiquement précis dans le cadre déterministe en temps continu et aussi en temps discret. Pour le cadre stochastique voir [22].

### 3.4.4 POVM et trajectoires quantiques

La modélisation de l'expérience du LKB se généralise sans difficulté à un système quantique ouvert quelconque en temps-discret avec la notion générale de POVM, abréviation de "Positive Operator Valued Measurement".



Le système  $S$  interagit avec le système mètre  $M$ . Le système mètre est ensuite mesuré selon une observable  $O_M$ . On considère l'espace de Hilbert du système composite  $(S, M) : \mathcal{H}_S \otimes \mathcal{H}_M$  où  $\mathcal{H}_S$  et  $\mathcal{H}_M$  sont les espaces de Hilbert associés à  $S$  et  $M$ . On distingue trois étapes ;

1. Initialement l'état du système composite est séparable

$$\mathcal{H}_S \otimes \mathcal{H}_M \ni |\Psi\rangle = |\psi_S\rangle \otimes |\theta_M\rangle$$

avec un état initial  $|\theta_M\rangle$  bien défini pour  $M$ .

2. Pendant un intervalle de temps donné,  $|\Psi\rangle$  évolue selon une équation de Schrödinger. Son propagateur  $U_{S,M}$  agissant sur  $|\psi_S\rangle \otimes |\theta_M\rangle$  donne l'état quantique à la fin de cet intervalle. En général,  $U_{S,M}(|\psi_S\rangle \otimes |\theta_M\rangle)$  n'est plus un état séparable entre  $S$  et  $M$  :  $U_{S,M}$  produit de l'intrication entre  $S$  et  $M$ .
3. On mesure alors  $M$ . Cela revient à considérer une observable qui ne porte que sur  $M$  et donc de la forme  $O_M = \mathbb{I}_S \otimes (\sum_\mu \lambda_\mu |\lambda_\mu\rangle \langle \lambda_\mu|)$ . Les valeurs propres  $\lambda_\mu$  sont toutes de multiplicité 1 et  $|\lambda_\mu\rangle \in \mathcal{H}_M$  est le vecteur propre unitaire associé à  $\lambda_\mu$  :  $(|\lambda_\mu\rangle)_\mu$  est donc une base hilbertienne de  $\mathcal{H}_M$ .

On définit les opérateurs de mesure  $M_\mu$  par linéarité de  $U_{S,M}$  :

$$\forall |\psi_S\rangle \in \mathcal{H}_S, \quad U_{S,M}(|\psi_S\rangle \otimes |\theta_M\rangle) = \sum_\mu (M_\mu |\psi_S\rangle) \otimes |\lambda_\mu\rangle.$$

Comme  $\forall |\psi_S\rangle \in \mathcal{H}_S$ , la norme de  $U_{S,M}(|\psi_S\rangle \otimes |\theta_M\rangle)$  est égal à 1 ( $U_{S,M}$  unitaire), on voit que nécessairement

$$\sum_\mu M_\mu^\dagger M_\mu = \mathbb{I}_S.$$

L'ensemble  $\{M_\mu\}$  définit alors un POVM pour "Positive Operator Valued Measurement".

Dans  $\mathcal{H}_S \otimes \mathcal{H}_M$ , la mesure projective associée à  $O_M = \mathbb{I}_S \otimes (\sum_\mu \lambda_\mu P_\mu)$  de la fonction d'onde  $U_{S,M}(|\psi_S\rangle \otimes |\theta_M\rangle)$  se caractérise par les deux propriétés suivantes :

1. La probabilité d'obtenir  $\lambda_\mu$  est donnée par  $p_\mu = \langle \psi_S | M_\mu^\dagger M_\mu | \psi_S \rangle$
2. Après la mesure, la nouvelle fonction d'onde devient séparable

$$|\Psi\rangle_+ = |\psi_S\rangle_+ \otimes |\lambda_\mu\rangle, \quad |\psi_S\rangle_+ = \frac{M_\mu |\psi_S\rangle}{\sqrt{p_\mu}}$$

si on a obtenu comme résultat de mesure  $\lambda_\mu$ .

Pour un état général de  $S$  décrit par la matrice densité  $\rho$  on voit que

$$p_\mu = \text{Tr} (M_\mu \rho M_\mu^\dagger) \text{ avec } \rho_+ = \frac{M_\mu \rho M_\mu^\dagger}{\text{Tr} (M_\mu \rho M_\mu^\dagger)}.$$

Le POVM  $(M_\mu)$  sur  $\mathcal{H}_S$  définit ainsi une chaîne de Markov d'état la matrice densité  $\rho$  :

$$\rho_{k+1} = \frac{M_\mu \rho_k M_\mu^\dagger}{\text{Tr} (M_\mu \rho_k M_\mu^\dagger)} \text{ avec la probabilité } p_{\mu,k} = \text{Tr} (M_\mu \rho_k M_\mu^\dagger).$$

Pour toute observable  $A$  sur  $\mathcal{H}_S$ , l'espérance conditionnelle de sa valeur moyenne  $\langle A \rangle = \text{Tr} (A \rho)$  à l'étape  $k + 1$  est uniquement fonction de l'état  $\rho$  à l'instant  $k$  :

$$\mathbb{E} (\text{Tr} (A \rho_{k+1}) \mid \rho_k) = \text{Tr} (A \mathcal{K}(\rho_k))$$

où  $\mathcal{K}$  est l'application de Kraus  $\rho \mapsto \mathcal{K}(\rho) = \sum_\mu M_\mu \rho M_\mu^\dagger$ . L'application de Kraus  $\mathcal{K}$  caractérise un canal quantique (quantum channel) :  $\mathbb{E} (\rho_{k+1} \mid \rho_k) = \mathcal{K}(\rho_k)$ .

Si l'opérateur  $\bar{A}$  est un point fixe  $\mathcal{K}^*$  ( $\mathcal{K}^*(\bar{A}) = \bar{A}$ ), l'application adjointe de  $\mathcal{K}$  (pour toute observable  $A$ ,  $\mathcal{K}^*(A) = \sum_\mu M_\mu^\dagger A M_\mu$ ), alors  $\text{Tr} (\bar{A} \rho)$  est une martingale :

$$\mathbb{E} (\text{Tr} (\bar{A} \rho_{k+1}) \mid \rho_k) = \text{Tr} (\bar{A} \mathcal{K}(\rho_k)) = \text{Tr} (\rho_k \mathcal{K}^*(\bar{A})) = \text{Tr} (\bar{A} \rho_k).$$

### 3.5 Impossibilité du clonage

Supposons que nous disposons d'un état quantique  $|\psi\rangle$  dans un espace de Hilbert de dimension arbitraire. Est-il possible de faire une copie de  $|\psi\rangle$  sur un autre système sans détruire  $|\psi\rangle$ ? Il s'agit du problème de clonage. Nous allons voir que cela n'est pas possible. L'obstruction vient du fait que l'évolution du système composite formé par le système à cloner, le système sur lequel on souhaite recopier  $|\psi\rangle$  et la machine sensée faire le clonage, obéit à une équation de Schrödinger globale dont l'évolution préserve le produit hermitien. Cette invariance du produit hermitien au cours du temps empêche le clonage.

Supposons pour simplifier l'exposé que  $|\psi\rangle$  soit dans  $\mathbb{C}^2$  et que nous disposons d'une machine quantique à cloner. Ainsi  $|\psi\rangle = \psi_g |g\rangle + \psi_e |e\rangle$  avec  $\psi_g, \psi_e \in \mathbb{C}$  arbitraires vérifiant  $|\psi_g|^2 + |\psi_e|^2 = 1$ . L'état dans lequel la machine copie  $|\psi\rangle$  appartient à un autre espace  $\mathbb{C}^2$ . On note  $|g_c\rangle$  et  $|e_c\rangle$  la base

de l'espace  $\mathbb{C}^2$  correspondant au clone. On note enfin par  $|\Xi\rangle$  l'état quantique de la machine qui vit dans un espace de Hilbert  $\mathcal{H}$  de dimension arbitraire. On note par  $|\Psi\rangle$ , l'état du système composite, état à copier, clone et machine. Cet état global appartient au produit tensoriel  $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathcal{H}$ .

Supposons que l'opération de clonage commence à partir de  $t = 0$  et qu'elle se termine à  $t = T > 0$ . Pour  $t = 0$ ,  $|\Psi\rangle_0$  est un produit tensoriel :

$$|\Psi\rangle_0 = |\psi\rangle \otimes |\Lambda\rangle_0$$

où  $|\Lambda\rangle_0 \in \mathbb{C}^2 \otimes \mathcal{H}$  est l'état du système formé par la future copie et la machine. Cet état quantique est toujours le même et ne dépend pas de  $|\psi\rangle$ , l'état à cloner. Le fait que  $|\Psi\rangle_0$  soit un tel produit tensoriel vient du fait que pour  $t < 0$ , les deux systèmes formés par l'état  $|\psi\rangle$  et la machine avec sa copie blanche  $|\Lambda\rangle_0$  sont indépendants.

A  $t = T$ ,  $|\Psi\rangle_T$  est un produit tensoriel :

$$|\Psi\rangle_T = |\psi\rangle \otimes |\psi\rangle^c \otimes |\Xi\rangle_{\psi_g, \psi_e}$$

avec  $|\psi\rangle^c = \psi_g |g_c\rangle + \psi_e |e_c\rangle$  et où  $|\Xi\rangle_{\psi_g, \psi_e}$  est l'état final de la machine, état qui dépend a priori de  $|\psi\rangle$ , l'état qu'elle vient de cloner. Le fait que l'état quantique de la machine avec la copie  $|\Lambda\rangle_T = |\psi\rangle^c \otimes |\Xi\rangle_{\psi_g, \psi_e}$  soit un produit tensoriel (alors que nous n'avons pas supposé que  $|\Lambda\rangle_0$  l'était), signifie qu'après l'opération de clonage, la copie  $|\psi\rangle^c$  admet un état quantique parfaitement défini et elle n'a plus de relation avec la machine. La copie est déconnectée de l'original et de la machine : c'est un véritable clone qui peut être manipulé indépendamment.

La difficulté vient du fait que pour passer de  $|\Psi\rangle_0$  à  $|\Psi\rangle_T$ , le système complet obéit à une équation de Schrödinger, équation que nous n'écrirons pas mais qui peut être aussi complexe que l'on peut imaginer. Ainsi  $|\Psi\rangle_T = U_T |\Psi\rangle_0$  où  $U_T$  est le propagateur associé, une transformation unitaire  $U_T^{-1} = U_T^\dagger$ . On doit donc avoir, pour la même transformation unitaire  $U_T$  (elle ne peut pas dépendre de  $|\psi\rangle$ )

$$\begin{aligned} |g\rangle \otimes |g_c\rangle \otimes |\Xi\rangle_{1,0} &= U_T (|g\rangle \otimes |\Lambda\rangle_0) \\ \left( \frac{|g\rangle + |e\rangle}{\sqrt{2}} \right) \otimes \left( \frac{|g_c\rangle + |e_c\rangle}{\sqrt{2}} \right) \otimes |\Xi\rangle_{\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}} &= U_T \left( \left( \frac{|g\rangle + |e\rangle}{\sqrt{2}} \right) \otimes |\Lambda\rangle_0 \right) \end{aligned}$$

Mais le produit hermitien de  $|g\rangle \otimes |\Lambda\rangle_0$  avec  $\left( \frac{|g\rangle + |e\rangle}{\sqrt{2}} \right) \otimes |\Lambda\rangle_0$  vaut  $1/\sqrt{2}$ . Alors que celui des images par  $U_T$  vaut  $\langle \Xi_{1,0} | \Xi_{\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}} \rangle / 2 \leq 1/2$ . Or ces deux produits hermitiens doivent être égaux car  $U_T$  préserve le produit hermitien. Aussi, le processus de clonage ne peut obéir à une équation de Schrödinger

entre  $t = 0$  et  $t = T$ . Ce qui est problématique. Remarquons enfin que ces arguments montrent qu'il est impossible de cloner une famille de  $|\psi\rangle$  non orthogonaux, même si cette famille est réduite à deux types de qubit.

## 3.6 Intrication

### 3.6.1 Intrication et non-localité

Avec le théorème de non-clonage ci-dessus, nous avons entrevu les liens entre état quantique factorisable et indépendance entre sous-systèmes. En fait, on ne peut parler d'état quantique bien défini pour un sous-système que lorsque l'état du système complet est factorisable par rapport à ce sous-système.

Considérons le système composite  $(A, B)$  ( $A$  pour Alice et  $B$  pour Bob) dont la fonction d'onde  $|\psi\rangle$  vit dans le produit tensoriel  $\mathbb{C}^2 \otimes \mathbb{C}^2$ . Ainsi  $|\psi\rangle$  est un 2-qubit :

$$|\psi\rangle = \psi_{gg} |gg\rangle + \psi_{ge} |ge\rangle + \psi_{eg} |eg\rangle + \psi_{ee} |ee\rangle$$

Le premier qubit est celui dont dispose Alice et le second est celui dont dispose Bob : ces deux qubits sont donc à des positions spatiales distinctes. En général,  $|\psi\rangle$  n'est pas factorisable, i.e., il n'existe pas 4 nombres complexes  $\psi_g^a, \psi_e^a, \psi_g^b$  et  $\psi_e^b$ , tels que

$$|\psi\rangle = (\psi_g^a |g\rangle + \psi_e^a |e\rangle) \otimes (\psi_g^b |g\rangle + \psi_e^b |e\rangle).$$

En effet on doit avoir par identification

$$\psi_g^a \psi_g^b = \psi_{gg}, \quad \psi_g^a \psi_e^b = \psi_{ge}, \quad \psi_e^a \psi_g^b = \psi_{eg}, \quad \psi_e^a \psi_e^b = \psi_{ee}$$

et donc nécessairement  $\psi_{gg}\psi_{ee} = \psi_{eg}\psi_{ge}$ . Réciproquement, si  $\psi_{gg}\psi_{ee} = \psi_{eg}\psi_{ge}$  alors les deux vecteurs  $(\psi_{gg}, \psi_{ge})$  et  $(\psi_{eg}, \psi_{ee})$  sont colinéaires, donc il existe, un vecteur non nul de module 1,  $(\psi_g^b, \psi_e^b)$ ,  $|\psi_g^b|^2 + |\psi_e^b|^2 = 1$  tel que  $(\psi_{gg}, \psi_{ge}) = \psi_g^a(\psi_g^b, \psi_e^b)$  et  $(\psi_{eg}, \psi_{ee}) = \psi_e^a(\psi_g^b, \psi_e^b)$  avec  $\psi_g^a, \psi_e^a \in \mathbb{C}$ . Comme  $|\psi\rangle$  est de longueur 1, on voit que  $|\psi_g^a|^2 + |\psi_e^a|^2 = 1$  et on a  $|\psi\rangle = (\psi_g^a |g\rangle + \psi_e^a |e\rangle) \otimes (\psi_g^b |g\rangle + \psi_e^b |e\rangle)$ .

Ainsi pour les états quantiques du 2-qubit  $|\psi\rangle$  tels que  $\psi_{gg}\psi_{ee} \neq \psi_{eg}\psi_{ge}$ , il n'est pas possible de donner séparément un sens à l'état quantique du qubit d'Alice et à celui de Bob. On ne peut considérer que l'état quantique global  $|\psi\rangle$  bien que physiquement les deux qubits puissent être très éloignés l'un de l'autre.

Alice ne peut agir que sur le premier qubit et Bob sur le second. Cela veut dire par exemple qu'Alice peut

- faire un impulsion  $\pi$  selon  $\sigma_x^a$  (l'indice  $A$  rappelle qu'il s'agit du qubit d'Alice), cette impulsion envoie  $|g\rangle$  sur  $|e\rangle$  et  $|e\rangle$  sur  $-|g\rangle$ . Elle correspond au propagateur  $e^{-i\frac{\pi}{2}\sigma_x^a} = (|e\rangle\langle g| - \langle g|e\rangle) \otimes \mathbb{I}^b$  où  $\mathbb{I}^b$  est l'opérateur unité sur  $B$ . Ainsi l'état quantique  $|\psi\rangle$  devient avec cette impulsion  $\pi$  :

$$\psi_{gg} |eg\rangle + \psi_{ge} |ee\rangle - \psi_{eg} |gg\rangle - \psi_{ee} |ge\rangle$$

S'il n'était pas séparable avant l'impulsion, il ne l'est toujours pas après celle ci.

- ou faire la mesure de  $\sigma_z^a$  sur le premier qubit, i.e. à prendre comme observable  $(\langle e|e\rangle - \langle g|g\rangle) \otimes \mathbb{I}^b$  :
  1. avec la probabilité  $|\psi_{gg}|^2 + |\psi_{ge}|^2$  Alice obtient  $-1$ , juste après cette mesure de  $-1$  le qubit d'Alice est dans l'état quantique  $|g\rangle$ ,  $|\psi\rangle$  est alors factorisé :

$$|g\rangle \otimes \left( \frac{\psi_{gg} |g\rangle + \psi_{ge} |e\rangle}{\sqrt{|\psi_{gg}|^2 + |\psi_{ge}|^2}} \right)$$

2. avec la probabilité  $|\psi_{eg}|^2 + |\psi_{ee}|^2$  Alice obtient  $+1$ ; juste après cette mesure de  $+1$  le qubit d'Alice est dans l'état quantique  $|e\rangle$ ,  $|\psi\rangle$  est alors factorisé :

$$|e\rangle \otimes \left( \frac{\psi_{eg} |g\rangle + \psi_{ee} |e\rangle}{\sqrt{|\psi_{eg}|^2 + |\psi_{ee}|^2}} \right).$$

Ainsi avant la mesure d'Alice, le qubit de Bob n'avait pas d'état quantique bien défini lorsque  $|\psi\rangle$  n'est pas factorisable. Après la mesure d'Alice, le qubit de Bob admet un état quantique bien défini qui dépend du résultat de la mesure d'Alice. Ce phénomène est caractéristique de la non-localité de la fonction d'onde  $|\psi\rangle$ .

Lorsque  $|\psi\rangle$  n'est pas factorisable, on dit que les qubits d'Alice et Bob sont *intriqués*. Les exemples typiques d'états intriqués sont les états de Bell (intrication dite maximale) :

$$|\phi^\pm\rangle = \frac{|gg\rangle \pm |ee\rangle}{\sqrt{2}}, \quad |\psi^\pm\rangle = \frac{|ge\rangle \pm |eg\rangle}{\sqrt{2}}.$$

### 3.6.2 Inégalités de Bell et paradoxe EPR

Nous reprenons une forme simplifiée (proposée dans [10]) des inégalités que Bell a établies en 1964 [6].

On suppose qu'Alice et Bob disposent d'un grand nombre  $N$  de 2-qubits dans le même état quantique intriqué  $|\psi^-\rangle_k = \frac{|g_a e_b\rangle - |e_a g_b\rangle}{\sqrt{2}}$ . Ces 2-qubits sont numérotés par  $k$  entre 1 à  $N$ . Par rapport à la sous-section précédente, nous avons rajouté les indices  $a$  et  $b$  aux états  $|g\rangle$  et  $|e\rangle$  pour bien insister sur le fait qu'Alice dispose physiquement de  $N$  premiers qubits ( $|g_a\rangle, |e_a\rangle$ ) et que Bob dispose des  $N$  seconds ( $|g_b\rangle, |e_b\rangle$ ). Alice et Bob sont suffisamment éloignés pour que, chacun de son côté, ils puissent faire les  $N$  mesures décrites ci-dessous dans un temps plus court que celui du trajet de la lumière entre eux.

Les  $N$  mesures d'Alice consistent simplement à choisir aléatoirement, pour chaque  $k \in \{1, \dots, N\}$ , la mesure  $M_k^a$  entre  $\sigma_z^a = |e_a\rangle\langle e_a| - |g_a\rangle\langle g_a|$  et  $\sigma_x^a = |e_a\rangle\langle g_a| + |g_a\rangle\langle e_a|$  et à noter le résultat de la mesure  $m_k^a \in \{-1, +1\}$ . Bob fait de même mais il choisit la mesure  $M_k^b$  entre  $-\frac{\sigma_z^b + \sigma_x^b}{\sqrt{2}}$  et  $\frac{\sigma_z^b - \sigma_x^b}{\sqrt{2}}$  et note le résultat  $m_k^b \in \{-1, +1\}$ . Les choix qu'effectuent Alice et Bob pour chaque  $k$  sont indépendants. On note

$$Q = \sigma_z^a \otimes \mathbb{I}^b, \quad R = \sigma_x^a \otimes \mathbb{I}^b, \quad S = \mathbb{I}^a \otimes \left( -\frac{\sigma_z^b + \sigma_x^b}{\sqrt{2}} \right), \quad T = \mathbb{I}^a \otimes \left( \frac{\sigma_z^b - \sigma_x^b}{\sqrt{2}} \right).$$

A la fin des  $N$  mesures, Alice et Bob rentrent en contact et mettent en commun leur résultats. Ils commencent par faire 4 paquets disjoints d'indices  $k$  selon le tri suivant

1.  $I_{QS} = \{k \mid M_k^a = \sigma_z^a, M_k^b = -(\sigma_z^b + \sigma_x^b)/\sqrt{2}\}$
2.  $I_{RS} = \{k \mid M_k^a = \sigma_x^a, M_k^b = -(\sigma_z^b + \sigma_x^b)/\sqrt{2}\}$
3.  $I_{RT} = \{k \mid M_k^a = \sigma_x^a, M_k^b = (\sigma_z^b - \sigma_x^b)/\sqrt{2}\}$
4.  $I_{QT} = \{k \mid M_k^a = \sigma_z^a, M_k^b = (\sigma_z^b - \sigma_x^b)/\sqrt{2}\}$

Ensuite, ils calculent 4 moyennes selon les 4 paquets :

$$m_\Upsilon = \frac{\sum_{k \in I_\Upsilon} m_k^a m_k^b}{\#I_\Upsilon} \quad \text{pour } \Upsilon = QS, RS, RT, QT.$$

Ils calculent enfin

$$m = m_{QS} + m_{RS} + m_{RT} - m_{QT}$$

On voit que  $m_{QS}$  est la valeur moyenne de l'opérateur  $QS$  sur le 2-qubit  $|\psi^-\rangle = \frac{|g_a e_b\rangle - |e_a g_b\rangle}{\sqrt{2}}$ . On remarquera que,  $QS = SQ$  (les opérateurs commutent) et donc l'ordre dans lequel on fait la mesure de  $Q$  pour Alice et  $S$  pour Bob n'a pas d'importance : cela ne change en rien la valeur moyenne  $\langle \psi^- | QS | \psi^- \rangle$ . Ainsi on a ( $\#I_{QS}$  grand) :

$$\langle \psi^- | QS | \psi^- \rangle \approx m_{QS}$$

Pour des raisons similaires on a aussi

$$\langle \psi^- | RS | \psi^- \rangle \approx m_{RS}, \quad \langle \psi^- | RT | \psi^- \rangle \approx m_{RT}, \quad \langle \psi^- | QT | \psi^- \rangle \approx m_{QT}.$$

Ainsi on a

$$m \approx \langle \psi^- | QS + RS + RT - QT | \psi^- \rangle.$$

Or un calcul direct montre que

$$\begin{aligned} QS + RS + RT - QT = \\ \sigma_z^a \otimes \left( -\frac{\sigma_z^b + \sigma_x^b}{\sqrt{2}} \right) + \sigma_x^a \otimes \left( -\frac{\sigma_z^b + \sigma_x^b}{\sqrt{2}} \right) + \sigma_x^a \otimes \left( \frac{\sigma_z^b - \sigma_x^b}{\sqrt{2}} \right) - \sigma_z^a \otimes \left( \frac{\sigma_z^b - \sigma_x^b}{\sqrt{2}} \right) = \\ -\sqrt{2} (\sigma_x^a \otimes \sigma_x^b + \sigma_z^a \otimes \sigma_z^b) \end{aligned}$$

Ainsi on a  $\langle \psi^- | QS + RS + RT - QT | \psi^- \rangle = 2\sqrt{2}$ . Alice et Bob doivent trouver une valeur proche de celle-ci et donc strictement supérieure à 2. Alain Aspect et ses collaborateurs ont fait en 1982 la première expérience de ce type avec des photons polarisés : ils ont trouvé effectivement une valeur supérieure à 2 [3, 2].

Pourquoi le fait de trouver expérimentalement  $m > 2$  est crucial ? Parce que cette expérience contredit les réserves faites par Einstein, Podolsky et Rosen en 1935 [16] sur une possible incomplétude de la mécanique quantique. Pour faire court, les arguments développés dans [16] (argument dit EPR) conduisent à la conclusion suivante : la description de la réalité physique par la fonction d'onde  $|\psi\rangle$  est incomplète ; elle nécessite donc une super-théorie avec l'introduction de variables supplémentaires, variables dites cachées. Pour être compatible avec la relativité restreinte, cette super-théorie doit introduire des variables cachées locales en espace et les couplages entre ces variables supplémentaires ne peuvent aller plus vite que la lumière. Suite à ces réserves, plusieurs physiciens ont développé des super-théories à variables cachées locales. Grâce aux inégalités de Bell [6], ces théories peuvent être testées expérimentalement sans rentrer dans le détail des variables cachées qu'elles introduisent. Les inégalités de Bell sont une conséquence des deux seules propriétés suivantes : la localité spatiale et la compatibilité avec la relativité restreinte. Pour l'expérience d'Alice et Bob, ces inégalités impliquent que, si de telles super-théories existent, alors nécessairement  $m$  doit être entre  $-2$  et  $+2$ .

Pour comprendre, revenons dans un premier temps à un simple qubit dans un état fixé une fois pour toute  $|\psi\rangle = \psi_g |g\rangle + \psi_e |e\rangle$ ,  $|\psi_g|^2 + |\psi_e|^2 = 1$ . Une théorie à variables cachées introduit alors (en plus de  $\psi_g$  et  $\psi_e$ ) des variables supplémentaires notées symboliquement par  $\xi$  appartenant à l'ensemble  $\Xi$ .

Ainsi, le qubit est décrit par les paramètres connus  $(\psi_g, \psi_e)$  et aussi les paramètres cachés  $\xi$  : derrière  $|\psi\rangle$  se trouve en fait toute une famille d'états physiques distincts  $(\psi_g, \psi_e, \xi)$  où les variables  $\xi$  échappent à la théorie quantique actuelle<sup>2</sup>. A tout opérateur de mesure  $M$  ayant le spectre  $(\lambda_M^+, \lambda_M^-)$  est attaché une partition de  $\Xi$  en deux sous-ensembles  $\Xi_M^+$  et  $\Xi_M^-$  telle que si  $\xi \in \Xi_M^+$ , alors la mesure de  $M$  donne  $\lambda_M^+$  et si  $\xi \in \Xi_M^-$ , elle donne  $\lambda_M^-$ . Ainsi, toute théorie à variables cachées présuppose l'existence de toute grandeur physique attachée à un opérateur  $M$  avant même d'avoir effectué sa mesure. C'est le principe –quasiment philosophique– de réalité de toute grandeur physique : pour Einstein, une grandeur physique existe indépendamment de sa mesure.

Pour le 2-qubit  $|\psi^-\rangle = \frac{|g_a e_b\rangle - |e_a g_b\rangle}{\sqrt{2}}$ , Alice dispose de deux mesures locales au premier qubit  $Q = \sigma_z^a \otimes \mathbb{I}^b$  et  $R = \sigma_x^a \otimes \mathbb{I}^b$  alors que Bob dispose de deux autres mesures locales au second qubit  $S = \mathbb{I}^a \otimes \left(-\frac{\sigma_z^b + \sigma_x^b}{\sqrt{2}}\right)$  et  $T = \mathbb{I}^a \otimes \left(\frac{\sigma_z^b - \sigma_x^b}{\sqrt{2}}\right)$ . Reprenons la super-théorie, à variables cachées locales, évoquée ci-dessus. Nous rajoutons donc pour représenter le 2-qubit  $|\psi^-\rangle$ , les variables cachées  $\xi$  dans l'ensemble  $\Xi$ . Pour la mesure de  $W \in \{Q, R, S, T\}$ , on a alors la partition  $\Xi = \Xi_W^+ \sqcup \Xi_W^-$  telle que, pour le 2-qubit de fonction d'onde  $|\psi^-\rangle$  et de variables cachées  $\xi \in \Xi$ , on ait

1. si  $\xi \in \Xi_W^+$  alors la mesure de  $W$  donne  $m_W^\xi = +1$ .
2. si  $\xi \in \Xi_W^-$  alors la mesure de  $W$  donne  $m_W^\xi = -1$ .

Au 2-qubit numéro  $k$  est attaché les variables cachées  $\xi_k$ . A priori  $\xi_k \neq \xi_{k'}$  pour  $k \neq k'$ . Comme pendant les  $2N$  mesures faites par Alice et Bob, il ne peut y avoir échanges d'informations (même au sein des variables cachées) entre ce qui se passe du côté d'Alice et ce qui se passe du côté de Bob, on a pour tout  $k \in I_{QS}$ ,  $m_k^a = m_Q^{\xi_k}$  et  $m_k^b = m_S^{\xi_k}$ . Plus précisément, cela résulte des deux points suivants :

- les choix pour le 2-qubit no  $k$  entre  $Q$  et  $R$  pour Alice et entre  $S$  et  $T$  pour Bob sont indépendants et aléatoires.
- Alice et Bob sont assez loin l'un de l'autre pour que les mesures de Bob et d'Alice ne puissent pas se perturber mutuellement pendant toute la durée où elles sont effectuées (compatibilité avec la relativité restreinte).

Ainsi on voit que

$$\forall U \in \{Q, R\}, \quad \forall V \in \{S, T\}, \quad \forall k \in I_{UV}, \quad m_k^a = m_U^{\xi_k} \quad \text{et} \quad m_k^b = m_V^{\xi_k}.$$

---

2. Cela serait un peu comme en thermodynamique où les variables connues  $(\psi_g, \psi_e)$  correspondraient à la température et la pression d'un gaz, et où les variables  $\xi$  seraient les positions et vitesses les molécules constituant le gaz.



Comme Alice et Bob choisissent aléatoirement leur mesures  $U$  et  $V$  dans  $\{Q, R\}$  et  $\{S, T\}$ , respectivement, et comme  $N$  est grand, on voit que, pour  $U \in \{Q, R\}$  et  $V \in \{S, T\}$ , on a

$$m_{UV} = \frac{\sum_{k \in I_{UV}} m_U^{\xi_k} m_V^{\xi_k}}{\#I_{UV}} \approx \frac{\sum_{k=1}^N m_U^{\xi_k} m_V^{\xi_k}}{N}.$$

Ainsi

$$m \approx \frac{\sum_{k=1}^N m_Q^{\xi_k} m_S^{\xi_k} + m_R^{\xi_k} m_S^{\xi_k} + m_R^{\xi_k} m_T^{\xi_k} - m_Q^{\xi_k} m_T^{\xi_k}}{N}.$$

Or pour chaque  $k$  on a

$$m_Q^{\xi_k} m_S^{\xi_k} + m_R^{\xi_k} m_S^{\xi_k} + m_R^{\xi_k} m_T^{\xi_k} - m_Q^{\xi_k} m_T^{\xi_k} = (m_Q^{\xi_k} + m_R^{\xi_k}) m_S^{\xi_k} + (m_R^{\xi_k} - m_Q^{\xi_k}) m_T^{\xi_k}$$

Mais  $m_Q^{\xi_k} + m_R^{\xi_k}$  ne peut prendre que les valeurs  $-2, 0$  ou  $+2$ . Lorsque  $m_Q^{\xi_k} + m_R^{\xi_k} = 0$  alors  $m_R^{\xi_k} - m_Q^{\xi_k} = \pm 2$  et lorsque  $m_Q^{\xi_k} + m_R^{\xi_k} = \pm 2$  alors  $m_R^{\xi_k} - m_Q^{\xi_k} = 0$ . Ainsi  $(m_Q^{\xi_k} + m_R^{\xi_k}) m_S^{\xi_k} + (m_R^{\xi_k} - m_Q^{\xi_k}) m_T^{\xi_k}$  ne peut prendre que les valeurs  $+2$  ou  $-2$ . On en conclut  $|m| \leq 2$ . Il s'agit de l'inégalité de Bell pour cette expérience particulière avec Alice et Bob.

### 3.6.3 Téléportation quantique

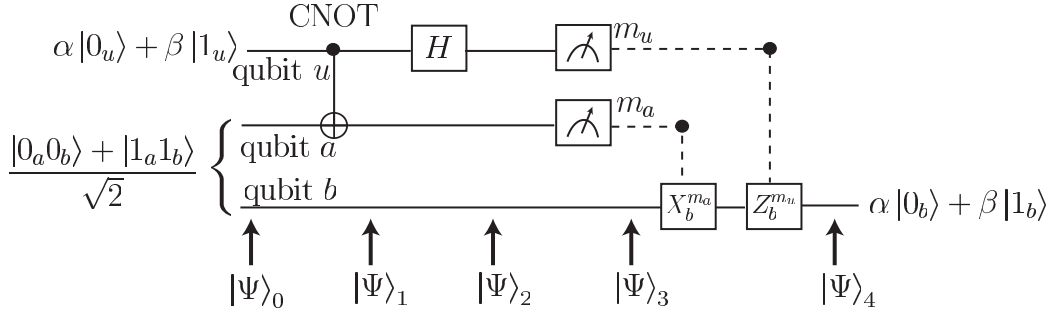


FIGURE 3.3 – Le circuit et les diverses étapes correspondant à la téléportation d’Alice (qubit  $a$ ) vers Bob (qubit  $b$ ) du qubit  $u$  de fonction d’onde,  $\alpha |0_u\rangle + \beta |1_u\rangle$ , avec  $\alpha, \beta \in \mathbb{C}$  tels que  $|\alpha|^2 + |\beta|^2 = 1$ .

Nous prenons ici les conventions de l’informatique quantique avec  $|0\rangle \equiv |e\rangle$  et  $|1\rangle \equiv |g\rangle$ . La mesure du qubit  $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$  est associée à l’opérateur de mesure  $M = |1\rangle\langle 1|$  : elle donne 0 avec la probabilité  $|\alpha|^2$  et 1 avec la probabilité  $|\beta|^2$ .

On appelle *porte quantique élémentaire* toutes transformations unitaires à un ou deux qubits. Un *circuit quantique* est alors composé de portes quantiques élémentaires. S'il ne comporte pas d'opérations de mesure par essence irréversible, il est réversible. Il correspond alors à une transformation unitaire plus élaborée qui se décompose en produit de transformations unitaires élémentaires (voir la sous-section 3.8.2).

On appelle transformation de Hadamard (porte de Hadamard)  $H$ , l'opération unitaire sur un simple qubit définie par

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

La transformation unitaire  $X$  correspond à  $\sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|$  : elle porte sur un simple qubit et échange  $|0\rangle$  et  $|1\rangle$  :

$$X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle.$$

La transformation unitaire  $Z$  correspond à  $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$  porte sur un simple qubit, laisse  $|0\rangle$  inchangé et change  $|1\rangle$  en  $-|1\rangle$  :

$$Z|0\rangle = |0\rangle, \quad Z|1\rangle = -|1\rangle.$$

La porte CNOT (Control NOT) est une transformation unitaire noté  $C_{not}$  sur un 2-qubit, le premier qubit jouant le rôle de bit de contrôle et le second qubit jouant le rôle du bit qui bascule lorsque le bit de contrôle est à 1 :

$$C_{not}|00\rangle = |00\rangle, \quad C_{not}|01\rangle = |01\rangle, \quad C_{not}|10\rangle = |11\rangle, \quad C_{not}|11\rangle = |10\rangle.$$

La porte CNOT est donc la transformation unitaire :

$$|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$$

Comme illustrée sur la figure 3.3, nous considérons la téléportation d'Alice vers Bob du qubit  $|\psi_u\rangle = \alpha|0_u\rangle + \beta|1_u\rangle$ . Nous avons rajouté l'indice  $u$  pour bien dissocier le support physique sur les deux états  $|0_u\rangle$  et  $|1_u\rangle$  de l'information quantique contenue dans les amplitudes de probabilité  $\alpha, \beta \in \mathbb{C}$ . On suppose donc qu'au départ Alice (qubit avec l'indice  $a$ ) et Bob (qubit avec l'indice  $b$ ) dispose d'un paire de qubits intriqués dont l'état quantique est

$$|\phi_{ab}^+\rangle = \frac{|0_a 0_b\rangle + |1_a 1_b\rangle}{\sqrt{2}}.$$

La procédure de téléportation de  $|\psi_u\rangle$  d'Alice vers Bob est alors formée par les étapes suivantes schématisées sur la figure 3.3 :

**étape 0 :** initialement, l'état quantique du système composite formé par le qubit à téléporter, celui d'Alice et celui de Bob est le produit tensoriel de  $|\psi_u\rangle$  avec  $|\phi_{ab}^+\rangle$  :

$$\begin{aligned} |\Psi\rangle_0 &= (\alpha |0_u\rangle + \beta |1_u\rangle) \otimes \left( \frac{|0_a 0_b\rangle + |1_a 1_b\rangle}{\sqrt{2}} \right) \\ &= \alpha |0_u\rangle \left( \frac{|0_a 0_b\rangle + |1_a 1_b\rangle}{\sqrt{2}} \right) + \beta |1_u\rangle \left( \frac{|0_a 0_b\rangle + |1_a 1_b\rangle}{\sqrt{2}} \right). \end{aligned}$$

Dans ce qui suit on omet systématiquement le signe de produit tensoriel  $\otimes$  : par exemple  $|0_u\rangle \otimes |1_a 0_b\rangle = |0_u 1_a 0_b\rangle = |0_u 1_a\rangle \otimes |0_b\rangle$ . On suppose dans ce schéma qu'Alice dispose des deux premiers qubit  $u$  et  $a$  et que Bob est loin et ne dispose que du troisième  $b$ .

**étape 1 :** Alice applique une porte CNOT sur les qubits  $u$  et  $a$ , le qubit  $u$  étant celui de contrôle. Ainsi  $|\Psi\rangle_0$  devient

$$|\Psi\rangle_1 = \alpha |0_u\rangle \left( \frac{|0_a 0_b\rangle + |1_a 1_b\rangle}{\sqrt{2}} \right) + \beta |1_u\rangle \left( \frac{|1_a 0_b\rangle + |0_a 1_b\rangle}{\sqrt{2}} \right)$$

**étape 2 :** Alice applique une transformation de Hadamard  $H$  sur le qubit  $u$ . Ainsi  $|\Psi\rangle_1$  devient

$$\begin{aligned} |\Psi\rangle_2 &= \left( \frac{\alpha(|0_u\rangle + |1_u\rangle)}{\sqrt{2}} \right) \left( \frac{|0_a 0_b\rangle + |1_a 1_b\rangle}{\sqrt{2}} \right) + \dots \\ &\quad \dots + \left( \frac{\beta(|0_u\rangle - |1_u\rangle)}{\sqrt{2}} \right) \left( \frac{|1_a 0_b\rangle + |0_a 1_b\rangle}{\sqrt{2}} \right) \\ &= |0_u 0_a\rangle \left( \frac{\alpha |0_b\rangle + \beta |1_b\rangle}{2} \right) + |0_u 1_a\rangle \left( \frac{\alpha |1_b\rangle + \beta |0_b\rangle}{2} \right) + \dots \\ &\quad \dots + |1_u 0_a\rangle \left( \frac{\alpha |0_b\rangle - \beta |1_b\rangle}{2} \right) + |1_u 1_a\rangle \left( \frac{\alpha |1_b\rangle - \beta |0_b\rangle}{2} \right) \end{aligned}$$

**étape 3 :** Alice mesure ses deux qubits selon l'opérateur  $|1_u\rangle\langle 1_u|$  pour  $u$  et  $|1_b\rangle\langle 1_b|$  pour  $a$ . On note  $m_u \in \{0, 1\}$  (resp.  $m_a \in \{0, 1\}$ ) la mesure de  $u$  (resp.  $a$ ) obtenue par Alice. Juste après la mesure  $|\Psi\rangle_3$  est le projeté de  $|\Psi\rangle_2$  sur l'espace propre associé au résultat  $(m_u, m_a)$ . Comme, il y a 4 résultats différents possibles (équiprobables ici) on a 4 états quantiques possibles :

$m_u$	$m_a$	$ \Psi\rangle_3$
0	0	$ 0_u 0_a\rangle (\alpha  0_b\rangle + \beta  1_b\rangle)$
0	1	$ 0_u 1_a\rangle (\alpha  1_b\rangle + \beta  0_b\rangle)$
1	0	$ 1_u 0_a\rangle (\alpha  0_b\rangle - \beta  1_b\rangle)$
1	1	$ 1_u 1_a\rangle (\alpha  1_b\rangle - \beta  0_b\rangle)$

**étape 4 :** Alice communique à Bob par un canal de communication classique le résultat de ses mesures  $m_u$  et  $m_a$ . Bob effectue, selon les valeurs de  $m_u$  et  $m_a$ , les opérations suivantes sur le qubit  $b$  :

$m_u$	$m_a$	opération effectuée par Bob
0	0	ne rien faire
0	1	permuter $ 0_b\rangle$ et $ 1_b\rangle$
1	0	changer $ 1_b\rangle$ en $- 1_b\rangle$
1	1	changer $ 1_b\rangle$ en $ 0_b\rangle$ et $ 0_b\rangle$ en $- 1_b\rangle$

Avec les définitions de  $X$  et  $Z$ , Bob en fait appliquer l'opérateur  $Z_b^{m_u} X_b^{m_a}$  à  $|\Psi\rangle_3$  pour obtenir

$$|\Psi\rangle_4 = |m_u m_a\rangle (\alpha |0_b\rangle + \beta |1_b\rangle).$$

A la fin de ces 4 étapes, les amplitudes de probabilité  $\alpha$  et  $\beta$ , initialement sur  $u$ , sont transférées sur  $b$ . Lors de ce transfert, l'état  $|\psi_u\rangle$  à téléporter est projeté sur  $|m_u\rangle$ . Il n'y a donc pas eu clonage de  $|\psi_u\rangle$  mais transfert des amplitudes de probabilité définissant  $u$  sur  $b$ . Noter que ce protocole en 4 étapes n'utilise pas la connaissance de  $\alpha$  et  $\beta$  : il reste le même, quel que soient  $\alpha$  et  $\beta$ . Alice a donc transmis à Bob une quantité "en principe infinie d'information" puisque  $\alpha$ ,  $\beta$  sont des nombres complexes et donc nécessitent une infinité de bits classiques pour les coder. Bob sait qu'à la fin, après le message  $(m_u, m_a)$  envoyé par Alice et les transformations sur  $b$  qu'il en déduit, il possède une copie exacte du qubit initial  $|\psi_u\rangle$  sur le sien. Cependant, Alice et Bob n'ont aucune idée des valeurs de  $\alpha$  et  $\beta$ . Du fait que Bob doit attendre le message classique d'Alice  $(m_u, m_a)$  pour lancer l'opération  $Z_b^{m_u} X_b^{m_a}$ , il ne peut y avoir transfert d'information à une vitesse supérieure à celle de la lumière alors que la réduction du paquet d'ondes liée aux mesures d'Alice semble être instantanée. On peut montrer (c'est un excellent exercice) qu'il est impossible à Bob de se rendre compte, par quelque mesure que ce soit sur  $b$ , qu'Alice a manipulé et/ou effectué une mesure sur  $u$  et  $a$  avant d'avoir reçu le message  $(m_u, m_a)$  envoyé par Alice.

## 3.7 Cryptographie quantique

### 3.7.1 Distribution de clés secrètes par BB84

Il s'agit d'un protocole, proposé par Bennett et Brassard en 1984 [7], pour la distribution d'une clé de chiffrement sur un canal public par échange de qubits dans des états quantiques non orthogonaux. Ce protocole est le suivant : Alice prépare, de façon aléatoire, un grand nombre de qubits dans 4

états possibles et les envoie, les uns après les autres, à Bob qui, à leur arrivée, les mesure de façon aléatoire selon deux opérateurs de mesure. Ainsi pour l'envoi numéro  $k$ ,

- Alice prépare de façon aléatoire le qubit numéro  $k$  dans l'état quantique  $|\psi\rangle_k$  choisit aléatoirement (probabilité de  $1/4$ ) entre les 4 états quantiques suivants :

$$|0_z\rangle = |e\rangle, \quad |1_z\rangle = |g\rangle, \quad |0_x\rangle = \frac{|g\rangle + |e\rangle}{\sqrt{2}} \quad \text{et} \quad |1_x\rangle = \frac{|g\rangle - |e\rangle}{\sqrt{2}}$$

Alice note alors le type d'état envoyé à Bob à l'étape  $k$ . En particulier le qubit no  $k$  est dit de type  $u_k = x$  si  $|\psi\rangle_k = |0_x\rangle, |1_x\rangle$  et de type  $u_k = z$  si  $|\psi\rangle_k = |0_z\rangle, |1_z\rangle$ .

- Quand Bob reçoit  $|\psi\rangle_k$ , il choisit aléatoirement de le mesurer selon  $\sigma_{v_k}$  où  $v_k$  est tiré au sort dans  $\{x, z\}$  avec probabilité  $1/2$  pour  $z$  et  $x$ . Il note le résultat de la mesure de  $\sigma_{v_k}$  ( $\pm 1$ ) mais aussi le type de la mesure, i.e.,  $v_k$ .

Après l'envoi d'un grand nombre  $N$  de qubits, Alice et Bob communiquent par un canal classique et public pour s'échanger les informations suivantes :

- Alice envoie à Bob la séquence des types de qubits qu'elle lui a envoyés, i.e. elle envoie  $(u_k)_{1 \leq k \leq N}$ .
- Bob envoie à Alice la séquence des types de mesures (pas le résultat) qu'il a effectués, i.e., il lui envoie  $(v_k)_{1 \leq k \leq N}$ .

Ainsi les  $k$  pour lesquels  $u_k = v_k$  (pour environ la moitié des qubits envoyés), Alice et Bob sont sûr de partager la même valeur de qubit :

- si Bob a mesuré  $+1$  alors  $|\psi\rangle_k = |0_{u_k}\rangle$  et alors Alice et Bob partagent sans l'avoir divulgué publiquement le bit classique 0.
- si Bob a mesuré  $-1$  alors  $|\psi\rangle_k = |1_{u_k}\rangle$  et alors Alice et Bob partagent sans l'avoir divulgué le bit classique 1.

Supposons qu'Oscar ait intercepté les qubits lors de leur transmission par Alice et qu'il ait aussi écouté leur communication classique. A chaque réception de  $|\psi\rangle_k$  Oscar ne peut pas le cloner pour en garder une copie pour lui, le renvoyer à Bob, attendre les échanges par le canal classique des  $(u_k)_{1 \leq k \leq N}$  et  $(v_k)_{1 \leq k \leq N}$  et faire alors la mesure sur le clone du qubit no  $k$  selon  $\sigma_{v_k}$ . S'il veut renvoyer  $|\psi\rangle_k$  à Bob et acquérir de l'information sur ce qubit, il est en fait obligé de mesurer soit selon  $\sigma_x$  soit selon  $\sigma_z$  avant de connaître le choix  $u_k$  de d'Alice. Aussi, il a une chance sur deux de prendre le mauvais choix et donc il perturbera nécessairement l'état du qubit no  $k$  une fois sur deux. L'impossibilité de clonage vient du fait que les 4 sortes de qubits envoyés par Alice ne sont pas tous orthogonaux deux à deux (voir la preuve de non clonage).

Enfin Alice et Bob échangent une dernière série d'informations sur le canal classique et public : pour une part non négligeable des  $k$  tels que  $u_k = v_k$ , ils décident d'échanger publiquement les valeurs des bits 0 ou 1 associés aux qubits  $|\psi\rangle_k$ . Si pour chaque  $k$ , les valeurs sont les mêmes, ils sont alors convaincus qu'il n'y a pas eu d'interception avec gain d'information de la part d'Oscar. Si pour un nombre non négligeable de tels  $k$ , les valeurs ne sont pas les mêmes, ils savent que les  $|\psi\rangle_k$  ont été perturbés par les activités malveillantes d'Oscar. Alice et Bob savent ainsi si le reste des bits qu'ils partagent et qu'ils n'ont pas communiqués publiquement peut être considéré comme un secret qu'eux-seuls connaissent. Ce secret peut alors servir de clé de chiffrement à un algorithme classique de cryptographie.

Ce protocole est simple et très astucieux. Il repose fondamentalement sur l'impossibilité de cloner des états non orthogonaux. Il est proposé dans plusieurs produits commerciaux où les qubits sont transmis via des photons de polarisations différentes et leur transmission d'Alice à Bob se fait au moyen d'une fibre optique de plusieurs dizaines de kilomètres de long.

### 3.7.2 Clés secrètes par partage d'états intriqués

Il s'agit d'un protocole imaginé par Ekert en 1991 [17]. Il a la même utilité que BB84. En revanche, il est nettement plus difficile à réaliser en pratique à grande échelle (avec Alice et Bob à plusieurs kilomètres de distance). L'intrication d'un 2-qubit est très sensible aux interactions avec l'environnement et à la perte d'intrication que ces interactions engendrent. Il s'agit du phénomène dit de la dé-cohérence. En fait la réalisation de ce protocole est de fait un test des inégalités de Bell et donc une expérience délicate à réaliser.

En reprenant les notations introduites pour décrire le protocole BB84, l'idée d'Ekert est la suivante : Alice prépare un grand nombre  $N$  de 2-qubits tous dans le même état

$$|\psi\rangle_k = \frac{|gg\rangle + |ee\rangle}{\sqrt{2}}$$

Pour chaque 2-qubit, Alice garde le premier qubit et envoie le second à Bob. Ainsi, à la fin de l'échange physique, Alice et Bob partagent un grand nombre  $N$  de qubits intriqués de façon maximale. Si Oscar intercepte le qubit envoyé à Bob et fait une mesure : il détruit nécessairement l'intrication car, sa mesure induit une réduction du paquet d'ondes : la fonction d'onde du 2-qubit devient un produit tensoriel entre une fonction d'onde pour le qubit d'Alice et une autre pour le qubit de Bob (intercepté par Oscar et qu'Oscar renvoie à Bob après l'avoir mesuré). Ainsi, toute interception par Oscar avec gain d'information détruit l'intrication entre Alice et Bob.

Alice et Bob, à partir de leur  $N$  qubits intriqués, décident de construire une clé de chiffrement connue d'eux seuls. Pour cela ils disposent d'un canal public de transmission, canal a priori écouté par Oscar. Ils vont se ramener à la fin du protocole BB84. Indépendamment l'un de l'autre, Alice et Bob décident de mesurer leur qubit no  $k$  selon  $\sigma_{u_k}$  pour Alice et  $\sigma_{v_k}$  pour Bob. Après avoir fait chacun  $N$  mesures, ils échangent publiquement les  $u_k$  et  $v_k$ . Ils se retrouvent alors exactement dans la même situation qu'à la fin de BB84 après l'échange des  $u_k$  et  $v_k$ . Ils procèdent alors de la même façon pour se convaincre que les  $N$  qubits étaient au départ bien intriqués et donc que leur transmission n'a pas été perturbée par Oscar.

## 3.8 Introduction au calcul quantique

### 3.8.1 Portes et circuits logiques classiques

Cette sous-section est un résumé suggestif des liens entre classes de complexité et circuits logiques. Un exposé rigoureux dépasse totalement le cadre de ce cours. Cependant, il est utile pour aborder le calcul quantique d'avoir une idée même imprécise de ces liens.

La conception des ordinateurs actuels repose sur la notion de porte logique, une application  $f$  de  $\{0, 1\}^n$  vers  $\{0, 1\}^m$  : on dispose de  $n$  bits classiques en entrée et on obtient  $m$  bits classiques en sortie. Quand  $m = 1$  on parle alors de fonction booléenne. D'une façon très schématique (voir [24]), il est toujours possible de réaliser une porte logique donnée par un circuit classique. Ce dernier est construit par assemblage de quelques portes logiques dites universelles où  $n, m \leq 2$ . Par exemple, il est possible de réaliser n'importe quelle fonction logique  $f : \{0, 1\}^n \mapsto \{0, 1\}$  par un circuit dit booléen formé des trois portes logiques universelles, AND, XOR et NOT :

- AND:  $\{0, 1\}^2 \ni (x_1, x_2) = x \mapsto f(x) = \begin{cases} 1, & \text{si } x_1 = x_2 = 1; \\ 0, & \text{sinon.} \end{cases}$
- XOR:  $\{0, 1\}^2 \ni (x_1, x_2) = x \mapsto f(x) = \begin{cases} 1, & \text{si } x_1 \neq x_2; \\ 0, & \text{sinon.} \end{cases}$
- NOT:  $\{0, 1\} \ni x \mapsto f(x) = \begin{cases} 1, & \text{si } x = 0; \\ 0, & \text{sinon.} \end{cases}$

Le calcul d'une famille de fonctions booléennes indexées par  $n$  entier positif,  $f_n(x) : \{0, 1\}^n \mapsto \{0, 1\}$ , est considéré comme facile si le nombre  $c_n$  de portes universelles du circuit qui calcule  $f_n$  croît de façon polynômiale avec  $n$  : il existe  $\alpha, \beta > 0$  tel que, pour tout  $n > 0$ ,  $c_n \leq \alpha n^\beta$ . Le calcul de  $f_n$  est dit difficile si  $c_n$  croît de façon exponentielle ( $c_n \geq \alpha \beta^n$  pour  $\alpha > 0$  et  $\beta > 1$ ).

Le lien avec les classes de complexité introduites en section 1.6 est direct.

Prenons un problème de décision. On peut simplement lui associer une fonction booléenne de la forme  $f_n(x) : \{0, 1\}^n \mapsto \{0, 1\}$  où  $n$  est le nombre de bit nécessaire pour le stockage des données. On choisit alors  $f_n(x) = 1$  pour caractériser les instances positives du problème. Si le problème est dans  $\mathbf{P}$ , alors cela équivaut à dire que le calcul de  $f_n$  est facile.

Prenons un exemple. Les données  $x = (r, s)$  sont formées par deux entiers positifs  $r$  et  $s$  d'au plus  $n/2$  bits chacun. La question est :  $r$  et  $s$  ont-ils un diviseur non trivial ? Ainsi on a  $f_n(r, s) = \begin{cases} 0, & \text{si } r \wedge s = 1; \\ 1, & \text{sinon.} \end{cases}$  Ce problème est dans  $\mathbf{P}$ . De l'algorithme d'Euclide donnant le PGCD, on déduit l'architecture d'un circuit logique qui calcule  $f_n$ . Ce circuit utilise un nombre de portes élémentaires, AND, XOR et NOT, qui croît polynômialement avec  $n$  (cf la sous-section 2.1.3).

### 3.8.2 Portes et circuits logiques quantiques

Les unités de calcul quantique sont les qubits évoluant dans des superpositions de deux états orthogonaux  $|0\rangle$  et  $|1\rangle$ . Les  $n$ -qubit vivent dans l'espace de Hilbert  $\mathcal{H}_n = \mathbb{C}^{2^n}$  de dimension notée  $N = 2^n$ . Pour  $x$  entier entre 0 et  $N - 1 = 2^n - 1$ , on note  $|x\rangle$  le  $n$ -qubit associé à la décomposition en base 2 de  $x : x = \sum_{k=0}^{n-1} x_k 2^k$ , chaque  $x_k \in \{0, 1\}$  et

$$|x\rangle = |x_0\rangle \otimes |x_1\rangle \otimes \dots \otimes |x_k\rangle \otimes \dots \otimes |x_{n-1}\rangle = |x_0, x_1, \dots, x_k, \dots, x_{n-1}\rangle.$$

Ainsi si  $x \neq y$ ,  $|x\rangle$  et  $|y\rangle$  sont orthogonaux. L'ensemble des  $|x\rangle$ ,  $x = 0, \dots, N - 1$ , forme donc une base orthonormée de  $\mathcal{H}_n$ . L'état général d'un  $n$ -qubit  $|\psi\rangle$  est donc donné par

$$\mathcal{H}_n \ni |\psi\rangle = \sum_{x=0}^{N-1} \psi_x |x\rangle = \sum_{x_0, \dots, x_{n-1} \in \{0, 1\}} \psi_{x_0 \dots x_{n-1}} |x_0, \dots, x_{n-1}\rangle$$

où chaque  $\psi_x \in \mathbb{C}$  et  $\sum_{x=0}^{N-1} |\psi_x|^2 = 1$ .

Une *porte logique quantique* sur un  $r$ -qubit est une transformation unitaire  $U$  de  $\mathcal{H}_r = \mathbb{C}^{2^r}$  dans lui-même. Un circuit quantique est donc un dispositif idéal qui réalise une transformation unitaire associée à une évolution selon l'équation différentielle de Schrödinger.

Toute porte logique quantique peut être réalisée avec un nombre fini de portes quantiques CNOT à deux qubits et de portes quantiques à un seul qubit :

- CNOT : transformation unitaire  $U_{\text{CNOT}}$  à deux qubit définie sur la base canonique des  $|x_0, x_1\rangle$  par  $U_{\text{CNOT}} |x_0, x_1\rangle = |x_0, x_0 \oplus x_1\rangle$  où  $\oplus$  désigne l'addition modulo 2.



- La porte à un seul qubit est une transformation unitaire de  $\mathcal{H}_1 = \mathbb{C}^2$  arbitraire. Elle peut être décomposée en un produit, à une phase globale près  $e^{i\theta}$  ( $\theta \in \mathbb{R}$ ), de trois transformations élémentaires :

$$e^{i\theta} e^{-i\alpha Z/2} e^{-i\beta X/2} e^{-i\gamma Z/2}$$

avec  $\alpha$ ,  $\beta$  et  $\gamma$  trois paramètres réels. On note ici par  $X$ ,  $Y$  et  $Z$  les trois matrices de Pauli (qui sont aussi des transformations unitaires et donc des portes à un seul qubit) :

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad Y = i|1\rangle\langle 0| - i|0\rangle\langle 1|, \quad Z = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

Une porte très utilisée est la porte d'Hadamard  $H = (X + Z)/\sqrt{2}$  :

$$H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \langle 0| + (|0\rangle - |1\rangle) \langle 1| = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|).$$

La porte CNOT à deux qubits et les portes à un seul qubit sont donc universelles. La démonstration de ce résultat déborde le cadre de ce cours (voir [24] pour une preuve détaillée).

A toute fonction booléenne (classique)  $\{0, 1\}^n \ni x \mapsto f_n(x) \in \{0, 1\}$ , il est possible d'associer une porte logique quantique  $U_{f_n}$ , transformation unitaire de  $\mathcal{H}_n \otimes \mathcal{H}_1$ . Cette transformation est définie par sa valeur sur chaque élément de la base canonique  $|x\rangle \otimes |q\rangle$  où  $x \in \{0, 1\}^n$  et  $q \in \{0, 1\}$  :

$$U_{f_n}(|x\rangle \otimes |q\rangle) = |x\rangle \otimes |q \oplus f_n(x)\rangle \quad (3.9)$$

où  $\oplus$  est l'addition modulo 2.

Si la fonction booléenne  $f_n$  est facile à calculer, i.e., s'il est possible de la calculer par un circuit classique ne faisant intervenir qu'un nombre polynômiale en  $n$  des trois portes classiques universelles AND, XOR et NOT, alors la porte quantique  $U_{f_n}$  est aussi facile à calculer, i.e.,  $U_{f_n}$  est calculable par un circuit quantique qui ne fait intervenir qu'un nombre polynômiale en  $n$  de portes quantiques CNOT à deux qubit et de portes quantiques à un seul qubit. Ce résultat dépasse de cadre de ce cours. Sa preuve [24] repose sur la transformation du circuit classique irréversible qui calcule  $f_n$  en un circuit classique réversible qui calcule aussi  $f_n$ . Ce circuit réversible conduit alors directement au circuit quantique réalisant  $U_{f_n}$ .

En résumé, le nombre d'opérations élémentaires reste du même ordre aussi bien pour calculer classiquement un fonction booléenne  $f_n$  que pour calculer quantiquement  $U_{f_n}$ , la porte quantique associé à  $f_n$  par les formules (3.9). Pour obtenir la valeur de  $f_n(x)$  avec le circuit quantique  $U_{f_n}$ , il suffit de calculer  $U_{f_n}$  sur  $|x\rangle \otimes |0\rangle$  et de mesurer le dernier qubit, i.e.  $\mathbb{I} \otimes Z$  : si la mesure donne  $|0\rangle$ , on sait que  $f_n(x) = 0$  ; si elle donne  $|1\rangle$  on sait

alors que  $f_n(x) = 1$ . La grande différence vient du fait que l'on peut aussi lancer un calcul nécessitant le même nombre d'opérations élémentaires avec  $|\psi\rangle \in \mathcal{H}_n \otimes \mathcal{H}_1$  arbitraire. Avec  $|\psi\rangle = \frac{1}{\sqrt{N}} (\sum_x |x\rangle) \otimes |0\rangle$ , on a une sorte de parallélisation du calcul de  $f_n$  car alors

$$U_{f_n} \left( \frac{1}{\sqrt{N}} \left( \sum_x |x\rangle \right) \otimes |0\rangle \right) = \frac{1}{\sqrt{N}} \left( \sum_x |x\rangle \otimes |f_n(x)\rangle \right).$$

On peut alors exploiter cette parallélisation quantique en rajoutant des transformations unitaires simples avant la détection. Si on est assez malin, on en déduit des informations intéressantes sur  $f_n$  plus rapidement que par des évaluations classiques.

En 1994, Peter Shor a proposé un algorithme quantique de complexité polynômiale pour factoriser les grands nombres. Malgré son impact médiatique, nous ne présenterons pas ici cet algorithme. Il est mathématiquement un peu compliqué. Il exploite la transformée de Fourier quantique, version quantique de la FFT. Dans les deux sous-sections suivantes, nous allons simplement illustrer cette parallélisation quantique sur deux algorithmes quantiques plus simples. Un lecteur intéressé par l'algorithme de factorisation pourra consulter par exemple [24] ou la page "Shor's algorithm" dans Wikipedia.

### 3.8.3 Algorithme de Deutsch-Josza (1992)

Soit une fonction booléenne  $f : \{0, 1\}^n \ni x \mapsto f(x) \in \{0, 1\}$ . On note  $N = 2^n$  et  $\mathcal{H}_n = \mathbb{C}^{2^n}$ . On suppose que cette fonction est soit constante, soit balancée<sup>3</sup>. La question est : la fonction est-elle constante ?

Sans autre information structurelle sur la fonction  $f$ , la certification des instances positives à ce problème de décision, i.e., la réponse par oui à coup sûr à la question, nécessite de calculer  $f(x)$  pour au moins la moitié des  $x$  possibles, soit au moins  $N/2 + 1 = 2^{n-1} + 1$  évaluations de  $f$ . l'algorithme de Deutsch-Josza permet de certifier les réponses positives (et donc négative du même coup) avec un seul calcul de la porte quantique associée  $U_f$ .

On note  $H_k$  la porte de Hadamard sur le qubit no  $k$  dans  $\mathcal{H}_n$  :

$$H_k |x\rangle = |x_0\rangle \otimes \dots \otimes |x_{k-1}\rangle \otimes (H |x_k\rangle) \otimes |x_{k+1}\rangle \otimes \dots \otimes |x_{n-1}\rangle.$$

Ainsi  $H_0 \dots H_{n-1} = H^{\otimes n}$  est la porte quantique, produit tensoriel de la porte  $H$  sur un  $n$ -qubit. Cet algorithme procède selon les étapes suivantes

1. On part de l'état  $|\Psi\rangle_0 = |0\rangle \otimes |0\rangle \in \mathcal{H}_n \otimes \mathcal{H}_1$ .

---

3. Une fonction booléenne  $f$  est dite balancée si, et seulement si,  $\#\{x \mid f(x) = 0\} = \#\{x \mid f(x) = 1\}$ .

2. On applique  $H^{\otimes n}$  sur les  $n$  premiers qubits de  $|\Psi\rangle_0$  et  $HX$  sur le dernier. Comme  $H^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$ , on a

$$|\Psi\rangle_1 = \frac{1}{\sqrt{2N}} \left( \sum_x |x\rangle \right) \otimes (|0\rangle - |1\rangle).$$

3. On applique la porte  $U_f$  à  $|\Psi\rangle_1$  pour avoir

$$|\Psi\rangle_2 = U_f |\Psi\rangle_1 = \frac{1}{\sqrt{2N}} \left( \sum_x (-1)^{f(x)} |x\rangle \right) \otimes (|0\rangle - |1\rangle).$$

Il est remarquable de  $|\Psi\rangle_2$  reste un état séparable entre  $\mathcal{H}_n$  et  $\mathcal{H}_1$ . Ainsi, avec un seul appel à  $U_f$  on dispose de l'état

$$|f\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle \in \mathcal{H}_n.$$

Si  $f$  est constante  $|f\rangle$  coïncide au signe près à  $\frac{1}{\sqrt{N}} \sum_x |x\rangle$ ; si  $f$  est équilibrée, alors  $|f\rangle$  est orthogonale à  $\frac{1}{\sqrt{N}} \sum_x |x\rangle$ .

4. On calcule  $H^{\otimes n}|f\rangle$ . Comme  $H^{\otimes n} \left( \frac{1}{\sqrt{N}} \sum_x |x\rangle \right) = |0\rangle$  car  $H^2 = \mathbb{I}_2$ , on voit que
- si  $f$  est équilibrée alors  $H^{\otimes n}|f\rangle$  est orthogonal à  $|0\rangle$
  - si  $f$  est constante alors  $H^{\otimes n}|f\rangle = \pm |0\rangle$ .
5. On conclut en mesurant chacun des  $n$  qubits de  $H^{\otimes n}|f\rangle$  selon  $Z$ . On voit alors que
- si les  $n$  mesures donnent toutes  $|0\rangle$  alors  $f$  est nécessairement constante.
  - sinon, dès que l'on trouve une mesure qui donne  $|1\rangle$ , on est sûr que  $f$  est nécessairement équilibrée.

L'avantage de cet algorithme n'est décisif que si l'on souhaite une réponse sûr. Pour un  $f$  de complexité polynomiale, la certification de la réponse positive à la question "  $f$  est-elle constante ? " est un problème qui est classiquement dans **RP** (cf section 1.6). En effet avec  $r$  évaluations de  $f$  sur des  $x$  tirés au hasard, on se persuade, si la valeur de  $f$  est toujours la même, que  $f$  est bien constante avec une probabilité de se tromper d'au plus  $1/2^r$ .

### 3.8.4 Algorithme de recherche de Grover (1996)

Soit une fonction booléenne  $f : \{0, 1\}^n \ni x \mapsto f(x) \in \{0, 1\}$ . On note  $N = 2^n$  et  $\mathcal{H}_n = \mathbb{C}^{2^n}$ . On suppose que cette fonction est nulle sauf pour un seul  $\bar{x}$

pour lequel  $f(\bar{x}) = 1$ . Le problème que l'on se pose est de trouver l'unique solution de  $f(x) = 1$ . Ce problème est typique d'un problème de recherche non structurée, comme celui du nom d'une personne dans un annuaire à partir de son numéro de téléphone.

Sans autre information structurelle sur la fonction  $f$ , il faut dans le pire cas  $N - 1$  appels à la fonction  $f$  pour trouver  $\bar{x}$ . Nous allons voir que sans plus d'information sur la structure de  $f$ , on peut trouver  $\bar{x}$  avec au plus  $\sqrt{N}$  appels à la porte quantique associée à  $f$ ,  $U_f$ . Ainsi, même si  $f$  est de complexité polynômiale, cet algorithme reste de complexité exponentielle mais avec un exposant plus petit. Au lieu de  $2^n$  calculs de  $f$  on passe à  $2^{\frac{n}{2}}$  calculs de  $U_f$ . La porte quantique  $U_f$  héritant de  $f$  sa complexité polynômiale, le gain en nombre d'opérations élémentaires reste appréciable.

Le départ est identique à celui de l'algorithme de Deutsch-Josza avec le passage de  $|0\rangle \in \mathcal{H}_n$  à  $|f\rangle \in \mathcal{H}_n$ . En filigrane de ce passage se cache une transformation unitaire  $O_f$  sur  $\mathcal{H}_n$  définie par :

$$\forall |\psi\rangle \in \mathcal{H}_n, \quad U_f \left( |\psi\rangle \otimes \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right) = (O_f |\psi\rangle) \otimes \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right).$$

Un calcul direct donne la caractérisation de  $O_f$  sur la base canonique de  $\mathcal{H}_n$  :

$$\forall x \in \{0, 1\}^n, \quad O_f |x\rangle = (-1)^{f(x)} |x\rangle.$$

Ainsi, on peut oublier la porte à  $n + 1$  qubits  $U_f$  et restreindre les calculs dans  $\mathcal{H}_n$  avec la porte  $O_f$ . Un calcul de  $O_f$  s'effectue donc avec un seul appel à  $U_f$ .

L'algorithme de Grover repose sur la transformation unitaire suivante :

$$G_f = H^{\otimes n} (2|0\rangle\langle 0| - \mathbb{I}_n) H^{\otimes n} O_f.$$

Cette transformation unitaire est itérée  $m = E\left(\frac{\pi}{4}\sqrt{N}\right)$  fois pour calculer

$$|f_m\rangle = (G_f)^m \left( \frac{1}{\sqrt{N}} \sum_x |x\rangle \right) = (G_f)^m H^{\otimes n} |0\rangle.$$

Les mesures des  $n$  qubits formant  $|f_m\rangle$  donnent avec une probabilité très proche de 1, les  $n$  bits codant  $\bar{x}$ . Il est alors facile de vérifier que cette mesure donne bien  $\bar{x}$  par un seul appel à  $f$ . Bien que reposant sur le grand principe Shadok "plus ça rate, plus ça a des chances de marcher", c'est un algorithme très efficace.

Voyons pourquoi avec  $m = E\left(\frac{\pi}{4}\sqrt{N}\right)$ , la mesure de  $|f_m\rangle$  donne  $\bar{x}$  avec une probabilité très proche de 1 ( $N$  est grand). Cela veut juste dire que  $|f_m\rangle$

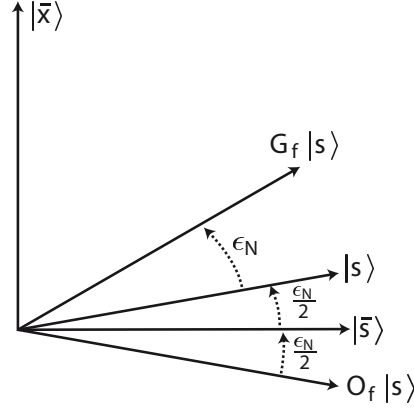


FIGURE 3.4 – la restriction de  $G_f = (2|s\rangle\langle s| - \mathbb{I}_n)O_f$  au plan engendré par les deux vecteurs orthogonaux  $|\bar{s}\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \bar{x}} |x\rangle$  et  $|\bar{x}\rangle$  est la composition de deux symétries orthogonales : une symétrie par rapport à  $|\bar{s}\rangle$  issue de la restriction de  $O_f$  au plan ; une symétrie orthogonale par rapport à  $|s\rangle$ . C'est une rotation d'angle  $\epsilon_N$  proche de  $2/\sqrt{N}$  pour  $N$  grand (angle double de celui entre  $|\bar{s}\rangle$  et  $|s\rangle$ ).

est alors proche de  $|\bar{x}\rangle$  : l'angle entre ces deux vecteurs unitaires doit donc être proche de 0.

On note  $|s\rangle$  l'état totalement symétrique

$$|s\rangle = H^{\otimes n} |0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle.$$

On a  $O_f |s\rangle = |s\rangle - \frac{2}{\sqrt{N}} |\bar{x}\rangle$ . Par ailleurs  $H^{\otimes n}(2|0\rangle\langle 0| - \mathbb{I}_n)H^{\otimes n} = 2|s\rangle\langle s| - \mathbb{I}_n$  car  $H^2 = \mathbb{I}$  et  $H^{\otimes n} |0\rangle = |s\rangle$ . Ainsi on a

$$|f_1\rangle = G_f |s\rangle = (2|s\rangle\langle s| - \mathbb{I}_n) \left( |s\rangle - \frac{2}{\sqrt{N}} |\bar{x}\rangle \right) = \left( 1 - \frac{4}{N} \right) |s\rangle + \frac{2}{\sqrt{N}} |\bar{x}\rangle$$

car  $\langle s|\bar{x}\rangle = 1/\sqrt{N}$ . On a aussi

$$G_f |\bar{x}\rangle = (2|s\rangle\langle s| - \mathbb{I}_n)(-|\bar{x}\rangle) = |\bar{x}\rangle - \frac{2}{\sqrt{N}} |s\rangle.$$

Ainsi  $G_f$  laisse invariant le plan engendré par  $|s\rangle$  et  $|\bar{x}\rangle$ . Ce plan admet comme base orthogonale  $|\bar{x}\rangle$  et  $|\bar{s}\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \bar{x}} |x\rangle$  avec  $|s\rangle = \sqrt{\frac{N-1}{N}} |\bar{s}\rangle + \sqrt{\frac{1}{N}} |\bar{x}\rangle$ .

La restriction de  $G_f$  à ce plan est une simple rotation. Comme illustré sur la figure 3.4, la restriction de  $G_f$  à  $(|\bar{s}\rangle, |\bar{x}\rangle)$  est la composition de deux symétries orthogonales : la symétrie par rapport à  $|\bar{s}\rangle$  issue de la restriction de  $O_f$  ( $O_f |\bar{s}\rangle = |\bar{s}\rangle$ ,  $O_f |\bar{x}\rangle = -|\bar{x}\rangle$ ) ; la symétrie orthogonale par rapport à

$|s\rangle$  correspondant à la transformation unitaire  $2|s\rangle\langle s| - \mathbb{I}_n$ . Avec  $\epsilon_N/2$  l'angle entre  $|\bar{s}\rangle$  et  $|s\rangle$ , la restriction de  $G_f$  à  $(|\bar{s}\rangle, |\bar{x}\rangle)$  est la rotation d'angle double, i.e.,  $\epsilon_N$ . Puisque  $|s\rangle = \sqrt{\frac{N-1}{N}} |\bar{s}\rangle + \sqrt{\frac{1}{N}} |\bar{x}\rangle$ ,  $\epsilon_n$  est défini par

$$\cos\left(\frac{\epsilon_N}{2}\right) = \sqrt{\frac{N-1}{N}}, \quad \sin\left(\frac{\epsilon_N}{2}\right) = \sqrt{\frac{1}{N}}.$$

On a donc

$$|f_m\rangle = (G_f)^m |s\rangle = \cos\left(\frac{2m+1}{2}\epsilon_N\right) |\bar{s}\rangle + \sin\left(\frac{2m+1}{2}\epsilon_N\right) |\bar{x}\rangle.$$

Soit  $\theta > 0$ . Puisque  $\epsilon_N = 2/\sqrt{N} + O(N^{-3/2})$ , on voit que pour  $m_\theta = E(\theta\sqrt{N}/2)$ , on a  $\frac{2m+1}{2}\epsilon_N = \theta + O(1/N)$ . Ainsi  $|f_{m_\theta}\rangle = \cos\theta |\bar{s}\rangle + \sin\theta |\bar{x}\rangle + O(1/N)$ . La probabilité que la mesure de  $|f_{m_\theta}\rangle$  donne  $|\bar{x}\rangle$  est donc très proche de  $\sin^2\theta$ . Pour  $\theta = \pi/2$ , on voit donc la mesure de  $|f_{m_{\pi/2}}\rangle$  donne  $|\bar{x}\rangle$  avec une probabilité très proche de 1.

L'algorithme de Grover se généralise au cas où  $f(x) = 1$  admet  $M$  solutions,  $M$  arbitraires. Un lecteur intéressé pourra consulter [24] ou la page "Grover's algorithm" dans Wikipedia.



# Bibliographie

- [1] V. Arnold. *Chapitres Supplémentaires de la Théorie des Equations Différentielles Ordinaires*. Mir Moscou, 1980.
- [2] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49(25) :1804–1807, 1982.
- [3] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment : A new violation of Bell's inequalities. *Physical Review Letters*, 49(2) :91–94, 1982.
- [4] J.-P. Barthélemy, G. Cohen, and A. Lobstein. *Complexité algorithmique*. Masson, Paris, 1992.
- [5] J.-L. Basdevant and J. Dalibard. *Mécanique Quantique*. Ecole Polytechnique, Palaiseau, France, 2002.
- [6] J. Bell. On the Einstein-Poldolsky-Rosen paradox. *Physics*, 1 :195–200, 1964.
- [7] C.H Bennett and G. Brassard. Quantum cryptography : Public-key distribution and tossing. In *Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing*, pages 175–181, 1984.
- [8] J.B. Bost. Fonction analytique de la variable complexe : partie II série de Dirichlet, 2000. Ecole Polytechnique. Cours de majeure de mathématiques.
- [9] J.B. Bost. Le théorème des nombres premiers et la transformation de Fourier. <http://math.polytechnique.fr/xups/vol102.html>, 2002. Actes des journées X-UPS : la fonction zêta.
- [10] J.F. Clauser, M.A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23 :880–884, 1969.
- [11] C. Cohen-Tannoudji, B. Diu, and F. Laloë. *Mécanique Quantique*, volume I& II. Hermann, Paris, 1977.



- [12] B. Degrange. *Introduction à la physique quantique*. Les Presse de l'Ecole des Mines, Paris, 2001.
- [13] J-P. Delahaye. *Merveilleux nombres premiers*. Belin Pour la Science, 2000.
- [14] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6) :644–654, 1976.
- [15] H.M. Edwards. *Riemann's Zeta Function*, chapter Appendice : On the number of primes less than a given magnitude. Dover edition, 1974. English translations of the original 1859 paper of B. Riemann on the Zeta function.
- [16] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47 :777–780, 1935.
- [17] A.K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67 :661–663, 1991.
- [18] M. Garey and D. Johnson. *Computers and Intractability*. Freeman, 1979.
- [19] J. Guckenheimer and P. Holmes. *Nonlinear Oscillations, Dynamical Systems and Bifurcations of Vector Fields*. Springer, New York, 1983.
- [20] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers*. Oxford Science Publication, fith edition edition, 1979.
- [21] S. Haroche and J.M. Raimond. *Exploring the Quantum : Atoms, Cavities and Photons*. Oxford University Press, 2006.
- [22] H.J. Kushner. *Introduction to Stochastic Control*. Holt, Rinehart and Wilson, INC., 1971.
- [23] L. Landau and E. Lifshitz. *Mécanique*. Mir, Moscou, 4th edition, 1982.
- [24] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [25] N. Petit and P. Rouchon. *Automatique : Dynamique et Contrôle des Systèmes*. Mines-ParisTech, 2011.
- [26] R. L. Rivest, A. Shamir, and L. M. Adelman. A method for obtaining digital signatures and public-key cryptosystems. Technical Report MIT/LCS/TM-82, 1977.
- [27] J.A. Sanders and F. Verhulst. *Averaging Methods in Nonlinear Dynamical Systems*. Springer, 1987.
- [28] G. Tenenbaum and M. Mendès-France. *Les nombres premiers*. Presses Universitaires de France, Que sais-je ?, 1997.
- [29] G. Zemor. *Cours de cryptographie*. Cassini, Paris, 2000.

# Annexe A

## Systeme oscillant et moyennisation

Nous rappelons ici les résultats usuels et utilisés ici pour la moyennisation à une fréquence. On pourra consulter [27, 19, 1] pour plus de précision. Un point cependant est moins standard mais il simplifie notablement les calculs de l'approximation aux ordres supérieurs. Il s'agit d'une variante du calcul standard (changement de variables proche de l'identité) que nous avons directement tirée de [23] et qui reprend un calcul dû à Kapitsa pour le mouvement moyen d'une particule dans un champ de force fortement oscillant.

Considérons le système oscillant de dimension  $n$  ;

$$\frac{dx}{dt} = \varepsilon f(x, t, \varepsilon), \quad x \in \mathbb{R}^n$$

avec  $f$  régulière et de période  $T$  par rapport à  $t$  et où  $\varepsilon$  est un petit paramètre positif. Pour  $x$  borné et pour  $\varepsilon$  assez petit, alors il existe un changement de variables, périodique en temps et proche de l'identité, faisant passer de  $x$  à  $z$ ,

$$x = z + \varepsilon w(z, t, \varepsilon)$$

avec  $w$  fonction régulière et de période  $T$  en  $t$ , telle que l'équation différentielle en  $x$  admette, dans les variables  $z$ , la structure suivante :

$$\frac{dz}{dt} = \varepsilon \bar{f}(z, \varepsilon) + \varepsilon^2 f_1(z, t, \varepsilon)$$

avec

$$\bar{f}(z, \varepsilon) = \frac{1}{T} \int_0^T f(z, t, \varepsilon) dt$$

et  $f_1$  régulière de période  $T$  en  $t$ . Il est ainsi possible d'approcher sur l'intervalle de temps  $[0, \frac{T}{\varepsilon}]$  les trajectoires du système oscillant  $\frac{dx}{dt} = \varepsilon f(x, t, \varepsilon)$  par

celles du système moyen  $\frac{dz}{dt} = \varepsilon \bar{f}(z, \varepsilon)$ . Plus précisément, si  $x(0) = z(0)$  alors  $x(t) = z(t) + O(|\varepsilon|)$  pour tout  $t \in [0, \frac{T}{\varepsilon}]$ . Comme l'approximation court sur un intervalle de longueur  $T/\varepsilon$ , on dira par la suite que cette approximation est d'ordre 1. On parle aussi d'*approximation séculaire*.

La fonction  $w(z, t, \varepsilon)$  est donnée par une primitive en temps de  $f - \bar{f}$ . En effet, si l'on remplace  $x$  par  $z + \varepsilon w$  dans  $\frac{d}{dt}x = \varepsilon f$  on obtient

$$\left( I_d + \varepsilon \frac{\partial w}{\partial z} \right) \frac{d}{dt} z = \varepsilon f - \varepsilon \frac{\partial w}{\partial t} = \varepsilon \bar{f} + \varepsilon \left( f - \bar{f} - \frac{\partial w}{\partial t} \right).$$

Comme, pour chaque  $z$ , la fonction  $\int_0^t (f(z, \tau, \varepsilon) - \bar{f}(z, \varepsilon)) d\tau$  est une fonction périodique en  $t$  de période  $T$ , on pose

$$w(z, t, \varepsilon) = \int_0^t (f(z, \tau, \varepsilon) - \bar{f}(z, \varepsilon)) d\tau + c(z, \varepsilon)$$

où la constante d'intégration  $c(z, \varepsilon)$  est choisie comme on veut. On verra plus loin qu'un choix judicieux correspond à  $w$  de moyenne temporelle identiquement nulle. On voit qu'avec un tel  $w$ ,

$$\left( I_d + \varepsilon \frac{\partial w}{\partial z}(z, t, \varepsilon) \right) \frac{d}{dt} z = \varepsilon \bar{f}(z, \varepsilon) + \varepsilon (f(z + \varepsilon w(z, t, \varepsilon), t, \varepsilon) - f(z, t, \varepsilon))$$

et donc

$$\frac{d}{dt} z = \varepsilon \left( I_d + \varepsilon \frac{\partial w}{\partial z}(z, t, \varepsilon) \right)^{-1} \left( \bar{f}(z, \varepsilon) + f(z + \varepsilon w(z, t, \varepsilon), t, \varepsilon) - f(z, t, \varepsilon) \right).$$

On obtient ainsi la forme cherchée,  $\frac{d}{dt} z = \varepsilon \bar{f} + \varepsilon^2 f_1$ , avec

$$\begin{aligned} f_1(z, t, \varepsilon) = & \frac{1}{\varepsilon} \left( \left( I_d + \varepsilon \frac{\partial w}{\partial z}(z, t, \varepsilon) \right)^{-1} - I_d \right) \bar{f}(z, \varepsilon) \\ & + \left( I_d + \varepsilon \frac{\partial w}{\partial z}(z, t, \varepsilon) \right)^{-1} \frac{f(z + \varepsilon w(z, t, \varepsilon), t, \varepsilon) - f(z, t, \varepsilon)}{\varepsilon}. \end{aligned}$$

On remarquera que

$$f_1(z, t, \varepsilon) = \frac{\partial f}{\partial z}(z, t, \varepsilon) w(z, t, \varepsilon) - \frac{\partial w}{\partial z}(z, t, \varepsilon) \bar{f}(z, \varepsilon) + O(\varepsilon).$$

L'approximation du second ordre est alors obtenue en prenant la moyenne de  $f_1$  sur une période. Cette approximation se justifie comme ci-dessus avec un

changement de variables, périodique en temps et du type  $z = \zeta + \varepsilon^2 \varpi(\zeta, t, \varepsilon)$ , c'est à dire proche de l'identité mais à des termes d'ordre 2 en  $\varepsilon$ .

Si, avec un choix adapté de  $c(z, \varepsilon)$ , on prend  $w$  de moyenne temporelle nulle, alors celle de  $\frac{\partial w}{\partial z}$  l'est également. A des termes d'ordre 1 près, la valeur moyenne de  $f_1$  est celle de  $\frac{\partial f}{\partial z} w$ . Ainsi l'approximation d'ordre deux s'écrit pour ce choix particulier de  $w$  :

$$\frac{d}{dt}x = \varepsilon \bar{f} + \varepsilon^2 \overline{\frac{\partial f}{\partial x} w}$$

où le symbole "—" signifie la valeur moyenne en temps sur une période. Les trajectoires du système oscillant  $\frac{d}{dt}x = \varepsilon f$  et celles de l'approximation séculaire d'ordre deux ci-dessus restent proches sur des intervalles de temps de longueur  $\frac{T}{\varepsilon^2}$ .

Une façon plus suggestive et surtout très efficace pour conduire ce calcul sur des exemples physiques est due à Kapitsa (voir [23, page 147]). Elle est la suivante. On décompose  $x = \bar{x} + \delta x$  en une partie non oscillant  $\bar{x}$  d'ordre 0 en  $\varepsilon$  et en une partie oscillante  $\delta x$  d'ordre 1 en  $\varepsilon$  et de moyenne nulle. On obtient alors

$$\frac{d}{dt}\bar{x} + \frac{d}{dt}\delta x = \varepsilon f(\bar{x} + \delta x, t, \varepsilon).$$

Comme  $\delta x = 0(\varepsilon)$ , on pose

$$f(\bar{x} + \delta x, t, \varepsilon) = f(\bar{x}, t, \varepsilon) + \frac{\partial f}{\partial x}(\bar{x}, t, \varepsilon)\delta x + O(\varepsilon^2).$$

Ainsi on a

$$\frac{d}{dt}\bar{x} + \frac{d}{dt}\delta x = \varepsilon f(\bar{x}, t, \varepsilon) + \varepsilon \frac{\partial f}{\partial x}(\bar{x}, t, \varepsilon)\delta x + O(\varepsilon^3).$$

Comme  $\frac{d}{dt}\bar{x} = \varepsilon \bar{f}(\bar{x}, \varepsilon) + O(\varepsilon^2)$ , l'identification des termes oscillant donne

$$\frac{d}{dt}(\delta x) = \varepsilon (f(\bar{x}, t, \varepsilon) - \bar{f}(\bar{x}, \varepsilon))$$

équation qui s'intègre en supposant  $\bar{x}$  constant et avec comme contrainte que  $\delta x$  soit de moyenne nulle. Donc

$$\delta x = \varepsilon \int_0^t (f(\bar{x}, \tau, \varepsilon) - \bar{f}(\bar{x}, \varepsilon)) d\tau + \varepsilon c(\bar{x}, \varepsilon)$$

est une fonction de  $(\bar{x}, t, \varepsilon)$ ,  $\delta x = \delta x(\bar{x}, t, \varepsilon)$ , périodique en  $t$  et de moyenne nulle avec un bon choix de  $c(\bar{x}, \varepsilon)$ . Utilisons maintenant cette fonction  $\delta x(\bar{x}, t, \varepsilon)$  dans l'équation différentielle précédente :

$$\frac{d}{dt}\bar{x} = \varepsilon \bar{f}(\bar{x}, \varepsilon) + \varepsilon \frac{\partial f}{\partial x}(\bar{x}, t, \varepsilon)\delta x(\bar{x}, t, \varepsilon) + O(\varepsilon^3)$$

et prenons la moyenne sur une période. On en déduit alors

$$\frac{d}{dt}\bar{x} = \varepsilon \bar{f}(\bar{x}, \varepsilon) + \varepsilon^2 \bar{f}_1(\bar{x}, \varepsilon)$$

avec

$$\varepsilon \bar{f}_1(\bar{x}, \varepsilon) = \frac{1}{T} \int_0^T \frac{\partial f}{\partial x}(\bar{x}, t, \varepsilon) \delta x(\bar{x}, t, \varepsilon) dt$$

On retrouve bien l'approximation séculaire à l'ordre 2 précédente.