Université de Montréal

Structure de la distribution de probabilités de l'état GHZ sous l'action de mesures de von Neumann locales

par
Claude Gravel

Département d'informatique et de recherche opérationnelle
Faculté des arts et des sciences

Mémoire présenté à la Faculté des arts et des sciences
en vue de l'obtention du grade de Maître ès sciences (M.Sc.)
en informatique

Avril 2011

Université de Montréal
Faculté des arts et des sciences

Ce mémoire intitulé:

Structure de la distribution de probabilités de l'état GHZ sous l'action de mesures de von Neumann locales

présenté par:

Claude Gravel

a été évalué par un jury composé des personnes suivantes:

Pierre McKenzie,	président-rapporteur
Gilles Brassard,	directeur de recherche
Alain Tapp,	membre du jury

Mémoire accepté le: . . . . . .

RÉSUMÉ

Dans ce mémoire, je démontre que la distribution de probabilités de l'état quantique Greenberger-Horne-Zeilinger (GHZ) sous l'action locale de mesures de von Neumann indépendantes sur chaque qubit suit une distribution qui est une combinaison convexe de deux distributions. Les coefficients de la combinaison sont reliés aux parties équatoriales des mesures et les distributions associées à ces coefficients sont reliées aux parties réelles des mesures. Une application possible du résultat est qu'il permet de scinder en deux la simulation de l'état GHZ. Simuler, en pire cas ou en moyenne, un état quantique comme GHZ avec des ressources aléatoires, partagées ou privées, et des ressources classiques de communication, ou même des ressources fantaisistes comme les boîtes non locales, est un problème important en complexité de la communication quantique. On peut penser à ce problème de simulation comme un problème où plusieurs personnes obtiennent chacune une mesure de von Neumann à appliquer sur le sous-système de l'état GHZ qu'il partage avec les autres personnes. Chaque personne ne connaît que les données décrivant sa mesure et d'aucune façon une personne ne connaît les données décrivant la mesure d'une autre personne. Chaque personne obtient un résultat aléatoire classique. La distribution conjointe de ces résultats aléatoires classiques suit la distribution de probabilités trouvée dans ce mémoire. Le but est de simuler classiquement la distribution de probabilités de l'état GHZ. Mon résultat indique une marche à suivre qui consiste d'abord à simuler les parties équatoriales des mesures pour pouvoir ensuite savoir laquelle des distributions associées aux parties réelles des mesures il faut simuler. D'autres chercheurs ont trouvé comment simuler les parties équatoriales des mesures de von Neumann avec de la communication classique dans le cas de 3 personnes, mais la simulation des parties réelles résiste encore et toujours.

Mots clés: GHZ, non-localité, simulation de l'intrication, mesure de von Neumann équatoriale, mesure de von Neumann réelle

ABSTRACT

In this Master's thesis, I show that the probability distribution of the Greenberger-Horne-Zeilinger quantum state (GHZ) under local action of independent von Neumann measurements follows a convex distribution of two distributions.The coefficients of the combination are related to the equatorial parts of the measurements, and the distributions associated with those coefficients are associated with the real parts of the measurements. One possible application of my result is that it allows one to split into two pieces the simulation of the GHZ state. Simulating, in worst case or in average, a quantum state like the GHZ state with random resources, shared or private, as well as with classical communication resources or even odd resources like nonlocal boxes is a very important in the theory of quantum communication complexity. We can think of this simulation problem as a problem in which many people get the description of a von Neumann measurement. Each party does not know the description of any other measurements belonging to the other parties. Each party after having applied his measurement on the subsystem of the state that he shares with the others gets a classical outcome. The joint distribution of the outcomes of every parties follows the distribution studied in this thesis in the case of the GHZ state. My result indicates that in order to simulate the distribution, we can first simulate the equatorial parts of the measurements in order to know which distribution associated to the real parts of the measurements to simulate. Other researchers have found how to simulate the equatorial parts of the von Neumann measurements with classical resources in the case of 3 parties, but it is still unknown how to simulate the real parts.

Keywords: GHZ, non-locality, simulation of entanglement, equatorial von Neumann measurement, real von Neumann measurement

TABLE DES MATIÈRES

LISTE DES ANNEXES

NOTATION

$(\tau, \omega, \varphi, \psi)$	paramètres pour une matrice de $U(2)$; voir théorème (2.2.1)
$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	matrice identité
$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	matrice de Pauli
$\sigma_2 = \begin{pmatrix} 0 & -\imath \\ \imath & 0 \end{pmatrix}$	matrice de Pauli
$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	matrice de Pauli
$\lvert\cdot\rangle$	ket (vecteur)
$\langle\cdot\rvert$	bra (vecteur) - conjugaison transposée de $\lvert\cdot\rangle$
$n \in \mathbb{N}$	nombre de joueurs, de transformations locales (entrées), de mesures (sorties)
$a = a_1 a_2 \cdots a_n \in \{0,1\}^n$	chaîne booléenne (résultats des mesures dans la base standard)
$\lvert a\rangle = \otimes_{j=1}^{n} \lvert a_j\rangle$	raccourci de notation
$\lvert\Psi\rangle = \frac{1}{\sqrt{2}}\lvert 0^n\rangle + \frac{1}{\sqrt{2}}\lvert 1^n\rangle$	état quantique GHZ
$\mathbf{P}$	distribution discrète de probabilités
(θ, ϕ)	coordonnées sphériques (sur la sphère)
arg	argument (phase) d'un nombre complexe

REMERCIEMENTS

Je remercie mon directeur de recherche, Gilles Brassard, pour tout ce que j'ai appris de lui ainsi que de ses suggestions lors de la rédaction de ce mémoire. De même, je remercie Marc Kaplan pour les discussions que nous avons eues concernant le chapitre 3 de ce mémoire.

CHAPITRE 1

INTRODUCTION

Ce mémoire s'inscrit à la frontière de la physique quantique et de l'informatique quantique. Sa lecture présuppose un certain niveau de connaissances dans ces domaines. L'ouvrage de [12] est une bonne source de références préparant à la lecture de ce mémoire.

Le point de départ de mon résultat, qui fut ma motivation originale, est la simulation de l'état quantique Greenberger-Horne-Zeilinger (GHZ). Simuler GHZ signifie simuler la distribution de probabilités de cet état quantique et, plus spécifiquement, la simuler avec des ressources aléatoires, partagées ou privées, ainsi que des ressources classiques de communication (un canal classique de communication). Qu'est-ce que cela veut dire ? Allons-y comme suit intuitivement. Supposons que n personnes se partagent un état quantique intriqué, c'est-à-dire un état qui ne peut pas se factoriser complètement ou partiellement en produits tensoriels. Par exemple, dans ce mémoire, je m'intéresse à l'état $|\Psi\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle$ dit GHZ en l'honneur Greenberger, Horne et Zeilinger (voir [6]). Chaque personne possède la description d'une mesure de von Neumann qu'elle peut appliquer sur sa partie de GHZ. Soient ces n mesures M_j pour $j \in \{1,\ldots,n\}$. Il est très important dans ce qui suit que la i^{e} personne ne connaisse pas M_j pour $i \neq j$. Lorsqu'on dit que ces n personnes appliquent conjointement et indépendamment leurs mesures, on veut dire qu'ils appliquent $\otimes_{j=1}^{n} M_j$ à $|\Psi\rangle$. En appliquant ces mesures, ils obtiennent des résultats aléatoires $|b_j\rangle$. La 1^{re} personne obtient $|b_1\rangle$, la 2^{e} obtient $|b_2\rangle$, etc. La mécanique quantique affirme que ces résultats aléatoires sont les vecteurs propres de M_j. La distribution conjointe de ces résultats est ce que nous cherchons à simuler classiquement. Chaque mesure de von Neumann peut être représentée par un point sur la sphère en trois dimensions (dite de Bloch). Un point sur la sphère peut être représenté sphériquement par $(\theta,\phi) \in [0,2\pi) \times [0,\pi)$. Ce que mon résultat indique est que la distribution

de probabilités est une combinaison convexe de deux distributions. Les coefficients de la combinaison sont reliés aux θ_j qui représentent les parties équatoriales des mesures M_j et les deux distributions associées à ces coefficients sont reliées aux ϕ_j qui représentent les parties réelles des mesures M_j.

Pour analyser la structure de la distribution de probabilité dénoté **P**, je procéderai légérement différemment, mais de façon équivalente, en supposant que les n personnes transforment l'état $|\Psi\rangle$ en appliquant des transformations unitaires U_j indépendamment l'une de l'autre. En faisant cela, la base représentée par les vecteurs propres est transformée pour devenir ce que l'on appelle la base standard de calcul en informatique quantique. Les vecteurs propres sont donc $|a_j\rangle$ où $a_j \in \{0,1\}$. Ainsi, les n personnes mesurent donc dans la base standard de calcul après avoir appliqué $U = \otimes_{j=1}^{n} U_j$ à l'état $|\Psi\rangle$. La distribution conjointe obtenue est $\mathbf{P}(a)$ où $a = a_1 \cdots a_n \in \{0,1\}^n$. Plus précisement, mon résultat sera à propos de la structure $\mathbf{P}(a) = |\langle a|U|\Psi\rangle|^2$.

Être capable de simuler **P** classiquement a fait l'objet de nombreuses recherches. En effet, lorsqu'on dit « simuler GHZ » ou « simuler l'intrication », cela signifie simuler **P**. Comment ? Avec des variables aléatoires partagées et avec des ressources classiques de communication. Pour les notions de complexité de la communication comme les définitions de protocoles en pire cas, en moyenne ou bien les définitions de variables aléatoires partagées, etc, je suggère le livre de Kushilevitz et Nisan [7]. Mon résultat concerne la structure de **P** et n'est pas un résultat de complexité de la communication en soi. Tentons de faire un peu l'historique du problème. À l'origine, ils y a eu A. Einstein, B. Podolsky et N. Rosen (trio EPR) en 1935 qui ont cru démontrer que la mécanique quantique (de Copenhague) ne pouvait être complète, car celle-ci ne prévoit pas la possibilité de reproduire les corrélations quantiques avec des variables cachées (variables aléatoires partagées) qu'exhibe $|\Psi\rangle$ lorsque $n = 2$. Les corrélations sont les moments de la distributions **P**. Dans [3], il est montré qu'il est impossible de reproduire ces corrélations avec seulement des variables aléatoires. Maudlin [10] a proposé de rajouter des ressources de communication classique pour reproduire les corrélations. Maudlin fit cette suggestion

sans avoir eu vent de la théorie de la complexité de la communication des informaticiens. C'est à partir de ce moment que la théorie de la complexité de la communication devint plus importante afin de reproduire **P**. Une suite d'articles se sont succédés tentant de simuler **P** avec $n = 2$ et $n = 3$ en moyenne ou en pire et avec des types différents de mesures. Ces articles sont : [2, 4, 13, 16, 17].

Du point de vue de la simulation de la distribution **P**, mon résultat donne une marche à suivre. En effet, il affirme que la distribution **P** est une combinaison convexe de deux distributions qui seront dénotées $\mathbf{P}_1$ et $\mathbf{P}_2$. Afin de simuler **P**, il suffit donc de simuler un bit aléatoire permettant de décider laquelle de $\mathbf{P}_1$ ou $\mathbf{P}_2$ sera simulée. Ce bit est relié aux coefficients de la combinaison, les coefficients multipliant $\mathbf{P}_1$ et $\mathbf{P}_2$. La combinaison étant convexe, la somme des coefficients est égale à 1 et ils définissent ainsi une distribution dite de Bernoulli, biaisée en général. Par la suite, il faut simuler $\mathbf{P}_1$ ou $\mathbf{P}_2$ qui sont des distributions sur l'ensemble $\{0,1\}^n$. La simulation de la distribution de Bernoulli n'est reliée qu'aux phases des nombres complexes définissant les transformations U_j des n personnes. De façon équivalente, la simulation de la distribution de Bernoulli n'est reliée qu'aux parties équatoriales des mesures de von Neumann M_j si l'on adopte cette façon de travailler. Quant à la simulation de $\mathbf{P}_1$ ou de $\mathbf{P}_2$, elle est reliée aux amplitudes des nombres complexes définissant les transformations U_j des n personnes. De façon équivalente, la simulation de $\mathbf{P}_1$ ou de $\mathbf{P}_2$ est reliée aux parties réelles des mesures de von Neumann M_j si l'on adopte cette façon de travailler. Le coût de la simulation de **P** (pire cas ou moyenne) est donc réduit à la somme des coûts pour simuler la distribution de Bernoulli représentée par les coefficients de la combinaison et des distributions $\mathbf{P}_1$ ou $\mathbf{P}_2$. La partie principale de ce mémoire ne concerne que la structure de **P**. Néanmoins, dans le chapitre 3, il sera question de la simulation de ces distributions ainsi que des équivalences entre les mesures de von Neumann et les transformations unitaires.

CHAPITRE 2

STRUCTURE DE LA DISTRIBUTION DE PROBABILITÉ

Avant de montrer le résultat de ce mémoire, voici quelques rappels utiles. Il faut se reporter à la liste des notations (page viii) pour les notations qui ne sont pas introduites explicitement ci-dessous, par exemple les matrices de Pauli.

2.1 Définitions, rappels et retour sur la notation

Tout au long de ce mémoire, $n \in \mathbb{N}$ désigne le nombre d'entrées (transformations) ou le nombre de sorties (bits) à l'exception des deux définitions suivantes.

Définition 2.1.1 (matrice unitaire à coefficients dans $\mathbb{C}$ - groupe $U(n)$)**.** Une matrice unitaire U à coefficients dans $\mathbb{C}$ est une matrice telle que $U^\dagger = U^{-1}$ où $U^\dagger$ dénote la transposée conjuguée de la matrice U. Les matrices unitaires de taille $n \times n$ forment un groupe dénoté $U(n)$ lorsque muni de l'opération multiplicative usuelle des matrices. On a toujours que $|\det U| = 1$. Voir [1, 15] pour plus d'information.

Définition 2.1.2 (matrice unitaire *spéciale* à coefficients dans $\mathbb{C}$ - groupe $SU(n)$)**.** Une matrice unitaire spéciale U à coefficients dans $\mathbb{C}$ est une matrice telle que $U^\dagger = U^{-1}$ pour laquelle la condition $\det U = 1$ est respectée. Les matrices unitaires spéciales de taille $n \times n$ forment un groupe dénoté $SU(n)$ lorsque muni de l'opération multiplicative usuelle des matrices. Voir [1, 15] pour plus d'information.

Remarque 2.1.1. Pour $i \in \{1,2,3\}$, les matrices de Pauli $\sigma_i \in U(2) \setminus SU(2)$, car $\sigma_i \sigma_i^\dagger = 1$ et $\det \sigma_i = -1$. Un autre exemple de transformation qui est un élément de $U(2) \setminus SU(2)$ est la transformation d'Hadamard couramment utilisée en informatique quantique mais que ne sera pas utilisée dans ce mémoire. La transformation H d'Hadamard est donnée

par

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

Rappel 2.1.1 (état pur GHZ)**.** $|\Psi\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle$ dénote l'état quantique GHZ à n joueurs.

Remarque 2.1.2 (la lettre **P**)**.** La lettre **P** sert à dénoter la distribution de probabilités sur l'ensemble $\{0,1\}^n$ ($n \in \mathbb{N}$) définie par $\mathbf{P}(a) = |\langle a|U|\Psi\rangle|^2$ lorsque $a \in \{0,1\}^n$, $U = \otimes_j^n U_j$ et $U_j \in U(2)$. La distribution **P** est celle obtenue lorsque n transformations unitaires sont appliquées à $|\Psi\rangle$ suivies de n mesures dans la base standard de calcul produisant des bits $a_j \in \{0,1\}$ et $a = a_1 \cdots a_n$ (la concaténation) est parfois dénoté sous la forme d'un vecteur c'est-à-dire $a = (a_1, \ldots, a_n)$. Pour plus d'information sur les probabilités quantiques en général, voir [11].

Voici un rappel de la définition d'une distribution *locale* de probabilités. On se servira uniquement de cette définition ultérieurement pour affirmer que certaines distributions possèdent cette propriété.

Définition 2.1.3 (distribution locale)**.** Soit Λ une variable aléatoire ayant k réalisations possibles λ_i de probabilité non-nulle pour $i = 1, \ldots, k$. Étant données des transformations unitaires fixées U_j avec $j = 1, \ldots, n$, on dit d'une distribution $\mathbf{Q} : \{0,1\}^n \to [0,1]$ qu'elle est *locale* par rapport à Λ et aux transformations U_j si, pour tout $a_1 a_2 \cdots a_n \in \{0,1\}^n$, la factorisation

$$\mathbf{Q}_{\{U_j\}_{j=1}^n}(a_1, \ldots, a_n) = \sum_{i=1}^{k} \prod_{j=1}^{n} \mathbf{Q}_{U_j,\lambda_i}(a_j) \mathrm{Prob}(\Lambda = \lambda_i)$$

est valide.

Remarque 2.1.3. Sans entrer dans les détails, simuler classiquement une distribution locale ne coûte rien du point de vue de la complexité de la communication.

2.2 Structure de la distribution

Dans ce qui suit, $n \in \mathbb{N}$, $j = 1, \ldots, n$, $a_j \in \{0,1\}$ et $U_j \in U(2)$. Le résultat principal de ce mémoire concerne la structure de la distribution de probabilité $\mathbf{P}$ sur l'ensemble $\{0,1\}^n$ où

$$\begin{aligned} \mathbf{P}(a) &= |\langle a|U|\Psi\rangle|^2 \\ \langle a| &= \bigotimes_{j=1}^{n} \langle a_j| \\ U &= \bigotimes_{j=1}^{n} U_j \\ |\Psi\rangle &= \tfrac{1}{\sqrt{2}}|0^n\rangle + \tfrac{1}{\sqrt{2}}|1^n\rangle. \end{aligned}$$

Le théorème suivant donne une représentation possible pour les matrices unitaires. Les preuves de ces théorèmes peuvent être trouvées dans le livre [1, 14, 15].

Théorème 2.2.1. Pour tout $U \in U(2)$, ils existent $\varphi \in [0, 2\pi)$, $\psi \in [0, 2\pi)$, $\omega \in [0, 2\pi)$ et $\tau \in \{0,1\}$ uniques tel que

$$U = \begin{pmatrix} e^{\imath\varphi}\cos\omega & -\imath^{\tau}e^{-\imath\psi}\sin\omega \\ \imath^{\tau}e^{\imath\psi}\sin\omega & (-1)^{\tau}e^{-\imath\varphi}\cos\omega \end{pmatrix}.$$

Remarques 2.2.1.

1. Si $\tau = 0$ dans le théorème précédent (2.2.1), alors $U \in SU(2)$.
2. Si $\tau = 0$, $\varphi = 0$ et $\psi = 0$ dans le théorème précédent (2.2.1), alors U est une rotation.
3. Si $\tau = 1$ et $\varphi = 0$ dans le théorème précédent (2.2.1), alors U est aussi hermitienne c'est-à-dire $U = U^{\dagger}$. Dans ce cas, U est donc une involution de groupe c'est-à-dire un élément d'ordre 2.
4. La matrice de Pauli σ_1 correspond aux paramètres $\omega = \frac{\pi}{2}$, $\varphi = 0$, $\psi = -\frac{\pi}{2}$ et $\tau = 1$.

5. La matrice de Pauli σ_2 correspond aux paramètres $\omega = \frac{\pi}{2}$, $\varphi = 0$, $\psi = 0$ et $\tau = 1$.

6. La matrice de Pauli σ_3 correspond aux paramètres $\omega = 0$, $\varphi = 0$, $\psi = 0$ et $\tau = 1$.

7. La matrice d'Hadamard correspond aux paramètres $\omega = \frac{\pi}{4}$, $\varphi = 0$, $\psi = -\frac{\pi}{2}$ et $\tau = 1$.

Selon le théorème (2.2.1), toute matrice unitaire 2×2 peut donc être représentée par un quadruplet. Ainsi, pour tout $j = 1, \ldots, n$, soient les quadruplets $(\omega_j, \psi_j, \varphi_j, \tau_j)$ correspondant à U_j et les nombres complexes α_j et β_j définis par :

$$\begin{aligned} \alpha_j &= e^{\imath\varphi_j} \cos\omega_j \\ \beta_j &= e^{\imath\psi_j} \sin\omega_j. \end{aligned}$$

On peut donc écrire pour $U_j \in U(2)$ que

$$U_j = \begin{pmatrix} \alpha_j & -\imath^{\tau_j}\bar{\beta}_j \\ \imath^{\tau_j}\beta_j & (-1)^{\tau_j}\bar{\alpha}_j \end{pmatrix}.$$

Théorème 2.2.2. Soient $n \in \mathbb{N}$ joueurs se partageant l'état $|\Psi\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle$. Les n joueurs recoivent une transformation unitaire U_j où $j = 1, \ldots, n$. Chaque joueur applique sa transformation localement sur sa partie et mesure par la suite dans la base standard de calcul. Les résultats de mesures (les sorties) sont des bits $a_j \in \{0,1\}$ où $j = 1, \ldots, n$.

Soient U_j les données des joueurs comme dans le théorème 2.2.1 et, de plus, soient $a = a_1 \cdots a_n \in \{0,1\}^n$ et $\gamma = \sum_{j=1}^n (\varphi_j + \psi_j) \in \mathbb{R}/2\pi\mathbb{Z}$ et $\kappa = \frac{\pi}{2}\sum_{j=1}^n \tau_j \in \mathbb{R}/2\pi\mathbb{Z}$. La distribution $\mathbf{P}$, définie par $\mathbf{P}(a) = |\langle a|U|\Psi\rangle|^2$ où $U = \otimes_{j=1}^n |U_j\rangle$, est une combinaison convexe de deux distributions de probabilités comme suit

$$\mathbf{P}(a) = \cos^2\left(\tfrac{\gamma-\kappa}{2}\right)\mathbf{P}_1(a) + \sin^2\left(\tfrac{\gamma-\kappa}{2}\right)\mathbf{P}_2(a),$$

où

$$\begin{aligned}
\mathbf{P}_1(a) &= \frac{1}{2}\big(\mathrm{f}_1(a)+\mathrm{f}_2(a)\big)^2,\\
\mathbf{P}_2(a) &= \frac{1}{2}\big(\mathrm{f}_1(a)-\mathrm{f}_2(a)\big)^2,\\
\mathrm{f}_1(a) &= \prod_{j=1}^{n}\cos\big(\omega_j-\tfrac{\pi}{2}a_j\big) \text{ et}\\
\mathrm{f}_2(a) &= \prod_{j=1}^{n}-\sin\big(\omega_j-\tfrac{\pi}{2}a_j\big).
\end{aligned}$$

Démonstration. Premièrement, il faut calculer les compositions $U_j|0\rangle$ et $U_j|1\rangle$ étant donné que

$$\mathbf{P}(a)=|\langle a|U|\Psi\rangle|^2=\left|\bigotimes_{j=1}^{n}\langle a_j|\bigotimes_{j=1}^{n}U_j\left(\tfrac{1}{\sqrt{2}}\bigotimes_{j=1}^{n}|0\rangle+\tfrac{1}{\sqrt{2}}\bigotimes_{j=1}^{n}|1\rangle\right)\right|^2.$$

Les calculs donnent

$$U_j|0\rangle=\begin{pmatrix}e^{\imath\varphi_j}\cos\omega_j\\ \imath^{\tau_j}e^{\imath\psi_j}\sin\omega_j\end{pmatrix} \text{ et } U_j|1\rangle=\imath^{\tau_j}\begin{pmatrix}-e^{-\imath\psi_j}\sin\omega_j\\ \imath^{\tau_j}e^{-\imath\varphi_j}\cos\omega_j\end{pmatrix}.$$

Maintenant soient les fonctions $x_j:\{0,1\}\to\{\varphi_j,\psi_j\}$ pour tout $j=1,\ldots,n$ telles que

$$x_j(a_j)=\begin{cases}\varphi_j & \text{si } a_j=0\\ \psi_j & \text{si } a_j=1\end{cases}$$

De plus, soient les fonctions $s:\{0,1\}^n\to\mathbb{R}/2\pi\mathbb{Z}$, $t:\{0,1\}^n\to\mathbb{R}/2\pi\mathbb{Z}$ et les constantes

$\gamma \in \mathbb{R}/2\pi\mathbb{Z}$, $\kappa \in \mathbb{R}/2\pi\mathbb{Z}$ définies respectivement par

$$\begin{aligned} \gamma &= \sum_{j=1}^{n} (\varphi_j + \psi_j), \\ s(a) &= \sum_{j=1}^{n} x_j(a_j), \\ \kappa &= \frac{\pi}{2} \sum_{j=1}^{n} \tau_j, \\ t(a) &= \frac{\pi}{2} \sum_{j=1}^{n} \tau_j a_j. \end{aligned}$$

Puisque

$$\begin{aligned} \mathbf{P}(a) &= |\langle a|U|\Psi\rangle|^2 && (2.1) \\ &= \left| \bigotimes_{j=1}^{n} \langle a_j| \bigotimes_{j=1}^{n} U_j \left(\tfrac{1}{\sqrt{2}} \bigotimes_{j=1}^{n} |0\rangle + \tfrac{1}{\sqrt{2}} \bigotimes_{j=1}^{n} |1\rangle \right) \right|^2 && (2.2) \\ &= \left| \tfrac{1}{\sqrt{2}} \prod_{j=1}^{n} \langle a_j|U_j|0\rangle + \tfrac{1}{\sqrt{2}} \prod_{j=1}^{n} \langle a_j|U_j|1\rangle \right|^2, && (2.3) \end{aligned}$$

on a donc par définition des fonctions x_j que les arguments complexes (phases) des termes des produits de la ligne (2.3) s'écrivent comme

$$\begin{aligned} \arg \langle a_j|U_j|0\rangle &= x_j(a_j) + \tau_j a_j \frac{\pi}{2} && (2.4) \\ \arg \langle a_j|U_j|1\rangle &= -x_j(a_j \oplus 1) + \tau_j a_j \frac{\pi}{2} + \tau_j \frac{\pi}{2}. && (2.5) \end{aligned}$$

Maintenant, les produits de la ligne (2.3) s'écrivent

$$\prod_{j=1}^{n}\langle a_j|U_j|0\rangle = \prod_{j=1}^{n}\cos\left(\omega_j - a_j\frac{\pi}{2}\right)e^{\iota\arg\langle a_j|U_j|0\rangle} \tag{2.6}$$

$$= \mathrm{f}_1(a)\exp\left(\iota\sum_{j=1}^{n}\arg\langle a_j|U_j|0\rangle\right) \tag{2.7}$$

$$\prod_{j=1}^{n}\langle a_j|U_j|1\rangle = \prod_{j=1}^{n}-\sin\left(\omega_j - a_j\frac{\pi}{2}\right)e^{\iota\arg\langle a_j|U_j|1\rangle} \tag{2.8}$$

$$= \mathrm{f}_2(a)\exp\left(\iota\sum_{j=1}^{n}\arg\langle a_j|U_j|1\rangle\right). \tag{2.9}$$

De plus, par définition de la fonction s et de la constante γ, on a que

$$\sum_{j=1}^{n}x_j(a_j) = \left(s(a)-\frac{\gamma}{2}\right)+\frac{\gamma}{2} \tag{2.10}$$

$$-\sum_{j=1}^{n}x_j(a_j\oplus 1) = s(a)-\gamma$$

$$= \left(s(a)-\frac{\gamma}{2}\right)-\frac{\gamma}{2}. \tag{2.11}$$

Grâce à (2.10) et à (2.11), on a que

$$\langle a|U|\Psi\rangle = e^{\iota\left(t(a)+s(a)-\frac{\gamma}{2}\right)}\left(\frac{e^{\iota\frac{\gamma}{2}}\mathrm{f}_1(a)+e^{-\iota\left(\frac{\gamma}{2}-\kappa\right)}\mathrm{f}_2(a)}{\sqrt{2}}\right) \tag{2.12}$$

$$= e^{\iota\left(t(a)+s(a)-\frac{\gamma-\kappa}{2}\right)}\left(\frac{e^{\iota\frac{\gamma-\kappa}{2}}\mathrm{f}_1(a)+e^{-\iota\frac{\gamma-\kappa}{2}}\mathrm{f}_2(a)}{\sqrt{2}}\right) \tag{2.13}$$

$$= e^{\iota\left(t(a)+s(a)-\frac{\gamma-\kappa}{2}\right)}\left(\left(\frac{\mathrm{f}_1(a)+\mathrm{f}_2(a)}{\sqrt{2}}\right)\cos\left(\frac{\gamma-\kappa}{2}\right)+\right.$$

$$\left.\iota\left(\frac{\mathrm{f}_1(a)-\mathrm{f}_2(a)}{\sqrt{2}}\right)\sin\left(\frac{\gamma-\kappa}{2}\right)\right) \tag{2.14}$$

Par conséquent, la distribution de probabilité $\mathbf{P}$ sur l'ensemble $\{0,1\}^n$ s'écrit comme

$$\begin{aligned}
\mathbf{P}(a) &= |\langle a|U|\Psi\rangle|^2 && (2.15)\\
&= \left|e^{\imath\left(t(a)+s(a)-\frac{\gamma-\kappa}{2}\right)}\right|^2 \left|\left(\frac{\mathrm{f}_1(a)+\mathrm{f}_2(a)}{\sqrt{2}}\right)\cos\left(\frac{\gamma-\kappa}{2}\right)+\right.\\
&\qquad \left.\imath\left(\frac{\mathrm{f}_1(a)-\mathrm{f}_2(a)}{\sqrt{2}}\right)\sin\left(\frac{\gamma-\kappa}{2}\right)\right|^2 && (2.16)\\
&= \cos^2\left(\frac{\gamma-\kappa}{2}\right)\mathbf{P}_1(a)+\sin^2\left(\frac{\gamma-\kappa}{2}\right)\mathbf{P}_2(a). && (2.17)
\end{aligned}$$

Il ne reste qu'à démontrer que $\mathbf{P}_1$ et $\mathbf{P}_2$ sont des distributions de probabilités. Il est clair que $\mathbf{P}_1$ et $\mathbf{P}_2$ sont non-négatives pour tout $a \in \{0,1\}^n$. Il faut donc démontrer que $\sum \mathbf{P}_1(a) = 1$. (La preuve pour $\mathbf{P}_2$ est similaire.) Pour le montrer, on se sert des faits que f_1^2 et f_2^2 sont des distributions et, par conséquent, $(1/2)(\mathrm{f}_1^2+\mathrm{f}_2^2)$ est une distribution et

$$\frac{1}{2}\sum_{a\in\{0,1\}^n}\left(\mathrm{f}_1^2(a)+\mathrm{f}_2^2(a)\right)=1.$$

De plus, on se sert du fait simple que

$$\sum_{a\in\{0,1\}^n}(-1)^{a_1+\ldots+a_n}=0.$$

Ainsi, on démontre que

$$\begin{aligned}
\sum_{a\in\{0,1\}^n}\mathbf{P}_1(a) &= \sum_{a\in\{0,1\}^n}\frac{1}{2}\left(\mathrm{f}_1(a)+\mathrm{f}_2(a)\right)^2\\
&= \frac{1}{2}\sum_{a\in\{0,1\}^n}\left(\mathrm{f}_1^2(a)+\mathrm{f}_2^2(a)\right)\\
&\qquad +(-1)^n\prod_{j=1}^{n}\cos\omega_j\sin\omega_j\sum_{a\in\{0,1\}^n}(-1)^{a_1+\ldots+a_n}\\
&= 1. \qquad \blacksquare
\end{aligned}$$

Remarque 2.2.1. Outre le théorème mentionné précédemment pour représenter par un quadruplet une transformation unitaire 2×2, l'astuce importante utilisée pour démontrer le théorème est de mettre en évidence une partie de la phase de l'expression $\langle a|U|\Psi\rangle$ qui n'est pas « intéressante », en l'occurrence $e^{t\left(t(a)+s(a)-\frac{\gamma-\kappa}{2}\right)}$. Notons que Shor utilise la même astuce pour analyser son célèbre algorithme.

Le théorème (2.2.2) montre que la distribution $\mathbf{P}$ sur $\{0,1\}^n$ est une combinaison linéaire convexe des distributions $\mathbf{P}_1$ et $\mathbf{P}_2$ qui s'expriment en fonction des produits des modules (amplitudes) f_1 et f_2. Le prochain corollaire établit un lien entre les paramètres des opérations unitaires et les expressions composant $\mathbf{P}$.

Corollaire 2.2.1 (Événements statistiques intéressants, choix de paramètres intéressants et interprétations probabilistes). Pour tout $j = 1,\ldots,n$, soient les quadruplets $(\omega_j, \psi_j, \varphi_j, \tau_j)$ définissant les transformations unitaires V_j spécifiques suivantes.

1. f_1^2 est la distribution locale de probabilité obtenue lorsque $\otimes_{j=1}^n V_j$ est appliquée à l'état $|0^n\rangle$ et $(\omega_j, \psi_j, \varphi_j, \tau_j) = (\omega_j, 0, 0, 0)$ pour tout $j = 1,\ldots,n$.

2. f_2^2 est la distribution locale de probabilité obtenue lorsque $\otimes_{j=1}^n V_j$ est appliquée à l'état $|1^n\rangle$ et $(\omega_j, \psi_j, \varphi_j, \tau_j) = (\omega_j, 0, 0, 0)$ pour tout $j = 1,\ldots,n$.

3. $\mathbf{P}_1$ est la distribution de probabilité obtenue lorsque $\otimes_{j=1}^n V_j$ est appliquée à $|\Psi\rangle$ et que $(\omega_j, \psi_j, \varphi_j, \tau_j) = (\omega_j, 0, 0, 0)$ pour tout $j = 1,\ldots,n$.

4. $\mathbf{P}_2$ est la distribution de probabilité obtenue lorsque $\otimes_{j=1}^n V_j$ est appliquée à $|\Psi\rangle$ et que $(\omega_j, \psi_j, \varphi_j, \tau_j) = (\omega_j, 0, 0, 0)$ pour tout $j = 1,\ldots,n-2$, $(\omega_j, \psi_j, \varphi_j, \tau_j) = (\omega_j, 0, 0, 1)$ pour $j = n-1, n$. (Seulement deux des paramètres τ_j doivent être égaux à 1. On aurait pu prendre n'importe quels indices au lieu de $n-1$ et n.)

5. $\mathbf{P}_2$ peut aussi être obtenue lorsque $\otimes_{j=1}^n V_j$ est appliquée à $|\Psi\rangle$ et que $(\omega_j, \psi_j, \varphi_j, \tau_j) = (\omega_j, 0, 0, 0)$ pour tout $j = 1,\ldots,n-1$, $(\omega_j, \psi_j, \varphi_j, \tau_j) = (\omega_j, 0, -\frac{\pi}{2}, 1)$ pour $j = n$. Ce qui revient à opérer σ_3 suivie d'une rotation sur le n^{e} sous-système.

6. $\frac{1}{2}(\mathrm{f}_1^2+\mathrm{f}_2^2)=\frac{1}{2}(\mathbf{P}_1+\mathbf{P}_1)$ est la distribution de probabilité obtenue lorsque $\otimes_{j=1}^n V_j$ est appliquée à $|\Psi\rangle$ et $(\omega_j,\psi_j,\varphi_j,\tau_j)=(\omega_j,0,0,0)$ pour tout $j=1,\ldots,n-1$ et $(\omega_n,\psi_n,\varphi_n,\tau_n)=(\omega_j,0,0,1)$. L'intérêt de la chose est que malgré les apparences, cette distribution est locale.

7. La distribution de Bernoulli avec paramètre $\cos^2\big((\gamma-\kappa)/2\big)$ ou $\sin^2\big((\gamma-\kappa)/2\big)$ correspond à la distribution de la somme $(a_1+\ldots+a_n)$ mod 2 (parité) obtenue en appliquant $\otimes_{j=1}^n V_j$ à $|\Psi\rangle$ *lorsque* les angles ω_j sont restreints à $\{\pi/4,3\pi/4,5\pi/4,7\pi/4\}$ c'est-à-dire lorsque

$$V_j=\begin{pmatrix} e^{\imath\varphi_j}\cos\omega_j & -\imath^{\tau_j}e^{-\imath\psi_j}\sin\omega_j \\ \imath^{\tau_j}e^{\imath\psi_j}\sin\omega_j & \imath^{2\tau_j}e^{-\imath\varphi_j}\cos\omega_j \end{pmatrix} \text{ et } \omega_j\in\{\pi/4,3\pi/4,5\pi/4,7\pi/4\}.$$

Démonstration. Les preuves de (1), (2), (3), (4), (5), (6) sont immédiates. Pour démontrer (7), on remarque que si $\omega_j\in\{\pi/4,3\pi/4,5\pi/4,7\pi/4\}$ alors

$$\mathbf{P}(a_1,\ldots,a_n)=\frac{1}{2^n}+\frac{(-1)^{n+\Sigma_{j=1}^n a_j}}{2^n}\left(\prod_{j=1}^n\sin(2\omega_j)\right)\cos(\gamma-\kappa).$$

De plus, pour tout $j=1,\ldots,n$

$$\sin(2\omega_j)\in\{-1,+1\}\Longrightarrow\prod_{j=1}^n\sin(2\omega_j)\in\{-1,+1\}.$$

Puisqu'exactement la moitié des éléments de $\{0,1\}^n$ ont une parité paire et l'autre moitié ont une parité impaire, alors on a que

$$\begin{aligned}\mathrm{Prob}\Big(\sum_{j=1}^n a_j=b\Big) &= 2^{n-1}\left(\frac{1}{2^n}+\frac{(-1)^{n+b}}{2^n}\left(\prod_{j=1}^n\sin(2\omega_j)\right)\cos(\gamma-\kappa)\right)\\ &= \frac{1}{2}+\frac{(-1)^{n+b}}{2}\left(\prod_{j=1}^n\sin(2\omega_j)\right)\cos(\gamma-\kappa).\end{aligned}$$

Par conséquent,

$$\text{Prob}\Big(\sum_{j=1}^{n} a_j = b\Big) \;=\; \begin{cases} \cos^2\left(\frac{\gamma-\kappa}{2}\right) & \text{si} \begin{cases} n+b \text{ est pair et } \prod_{j=1}^{n}\sin(2\omega_j) = 1 \\ \text{ou} \\ n+b \text{ est impair et } \prod_{j=1}^{n}\sin(2\omega_j) = -1 \end{cases} \\ \sin^2\left(\frac{\gamma-\kappa}{2}\right) & \text{si} \begin{cases} n+b \text{ est impair et } \prod_{j=1}^{n}\sin(2\omega_j) = 1 \\ \text{ou} \\ n+b \text{ est pair et } \prod_{j=1}^{n}\sin(2\omega_j) = -1 \end{cases} \end{cases}$$

■

Remarque 2.2.2. Les termes $\cos^2\left(\frac{\gamma-\kappa}{2}\right)$ et $\sin^2\left(\frac{\gamma-\kappa}{2}\right)$ sont les coefficients de la combinaison convexe pour la distribution $\mathbf{P}$ d'où la pertinence de (7). Au chapitre 3, quand on abordera brièvement la simulation de $\mathbf{P}$, il faudra donc s'intéresser à $\text{Prob}\Big(\sum_{j=1}^{n} a_j = b\Big)$ pour savoir si on doit simuler $\mathbf{P}_1$ ou $\mathbf{P}_2$.

2.3 Calcul des distributions marginales et de la distribution conditionnelle du n^{e} bit

Dans ce qui suit, $n \geq 2$. Premièrement, on s'attardera au calcul de la distribution marginale $\mathbf{P}(a_{i_1},\ldots,a_{i_m})$ lorsque $i_j \in I$, $I \in \mathscr{P}(\{1,\ldots,n\})$, $\text{card}(I) = m$, $j \in \{1,\ldots,m\}$, $I \neq \emptyset$ et $I \neq \{1,\ldots,n\}$. Deuxièmement, on s'attardera au calcul de la distribution conditionnelle du n^{e} bit étant donné $a_1,\ldots,a_{n-1}$.

Théorème 2.3.1. Soient $n \geq 2$, $I \in \mathscr{P}(\{1,\ldots,n\})$, $\text{card}(I) = m$, $I = \{i_1,\ldots,i_m\}$, $I \neq \emptyset$ et $I \neq \{1,\ldots,n\}$, on a que

$$\mathbf{P}(a_{i_1},\ldots,a_{i_m}) = \frac{1}{2}\left(\prod_{j=1}^{m}\cos^2\left(\omega_{i_j} - \frac{\pi}{2}a_{i_j}\right) + \prod_{j=1}^{m}\sin^2\left(\omega_{i_j} - \frac{\pi}{2}a_{i_j}\right)\right).$$

Démonstration. Il n'est nécessaire que de regarder le cas $I = \{1,2,\ldots,n-1\}$ c'est-à-dire le cas où $\text{card}(I) = n-1$ et $n \notin I$, car, par symétrie, on déduit facilement les autres cas. Il faut remarquer d'abord que

$$\begin{aligned}
\mathbf{P}(a_1,\ldots,a_n) &= \cos^2\left(\frac{\gamma-\kappa}{2}\right)\mathbf{P}_1(a) + \sin^2\left(\frac{\gamma-\kappa}{2}\right)\mathbf{P}_2(a) \\
&= \frac{1}{2}\left(\prod_{j=1}^{n}\cos^2\left(\omega_j - \frac{\pi}{2}a_j\right) + \prod_{j=1}^{n}\sin^2\left(\omega_j - \frac{\pi}{2}a_j\right)\right) + \\
&\qquad (-1)^{n+\Sigma_{j=1}^{n}a_j}\left(\prod_{j=1}^{n}\cos(\omega_j)\sin(\omega_j)\right)\cos(\gamma-\kappa).
\end{aligned}$$

Par définition de la distribution marginale, on a que

$$\mathbf{P}(a_1,\ldots,a_{n-1}) = \mathbf{P}(a_1,\ldots,a_{n-1},0) + \mathbf{P}(a_1,\ldots,a_{n-1},1).$$

Par conséquent,

$$\begin{aligned}
\mathbf{P}(a_1,\ldots,a_{n-1}) &= \frac{1}{2}\left(\prod_{j=1}^{n-1}\cos^2\left(\omega_j - \frac{\pi}{2}a_j\right) + \prod_{j=1}^{n-1}\sin^2\left(\omega_j - \frac{\pi}{2}a_j\right)\right) + \\
&\qquad \left((-1)^{n+\Sigma_{j=1}^{n-1}a_j} + (-1)^{n+1+\Sigma_{j=1}^{n-1}a_j}\right)\left(\prod_{j=1}^{n}\cos(\omega_j)\sin(\omega_j)\right)\cos(\gamma-\kappa) \\
&= \frac{1}{2}\left(\prod_{j=1}^{n-1}\cos^2\left(\omega_j - \frac{\pi}{2}a_j\right) + \prod_{j=1}^{n-1}\sin^2\left(\omega_j - \frac{\pi}{2}a_j\right)\right).
\end{aligned}$$

Par symétrie, on obtient le résultat voulu.

■

Remarque 2.3.1. Pour tout $I \in \mathscr{P}(\{1,\ldots,n\})$ tel que $I \neq \emptyset$ et $I \neq \{1,\ldots,n\}$, la distribution marginale associée à l'ensemble d'indices I est *locale*.

Maintenant, on va regarder de plus près la distribution conditionnelle $\mathbf{P}(a_n|a_1,\ldots,a_{n-1})$, ce qui est possible étant donné que l'on connaît la distribution marginale de $\mathbf{P}(a_1,\ldots,a_{n-1})$.

Théorème 2.3.2. Soient

$$\begin{aligned} u &= \prod_{j=1}^{n-1} \cos(\omega_j - \frac{\pi}{2} a_j) \\ v &= \prod_{j=1}^{n-1} -\sin(\omega_j - \frac{\pi}{2} a_j) \\ t &= \arctan\left(\frac{v}{u}\right). \end{aligned}$$

Étant donnés les $(n-1)$ premiers bits $a_1, \ldots, a_{n-1}$, la distribution conditionnelle du n^{e} bit est donnée par

$$\begin{aligned} \mathbf{P}(a_n | a_1, \ldots, a_{n-1}) &= \cos^2\left(\omega_n - \frac{\pi}{2} a_n - t\right) \cos^2\left(\frac{\gamma - \kappa}{2}\right) + \\ &\qquad \cos^2\left(\omega_n - \frac{\pi}{2} a_n + t\right) \sin^2\left(\frac{\gamma - \kappa}{2}\right). \end{aligned}$$

Démonstration. Par définition, on a que

$$\mathbf{P}(a_n | a_1, \ldots, a_{n-1}) = \frac{\mathbf{P}(a_1, \ldots, a_n)}{\mathbf{P}(a_1, \ldots, a_{n-1})}.$$

Ainsi, en fixant les $(n-1)$ premiers bits $a_1, \ldots, a_{n-1}$ et en posant

$$\begin{aligned} u &= \prod_{j=1}^{n-1} \cos(\omega_j - \frac{\pi}{2} a_j) \\ v &= \prod_{j=1}^{n-1} -\sin(\omega_j - \frac{\pi}{2} a_j) \\ t &= \arctan\left(\frac{v}{u}\right) \end{aligned}$$

et en utilisant le fait que pour tout $p,q \in \mathbb{R}$ et $x \in [0,2\pi)$,

$$\begin{aligned} p\cos(x)+q\sin(x) &= \sqrt{p^2+q^2}\cos(x+h) \\ h &= \arctan\Big(\frac{q}{p}\Big)+\begin{cases} 0 & \text{si } p\leq 0 \\ \pi & \text{si } p>0 \end{cases} \end{aligned}$$

alors, on a que $\mathbf{P}(a_n|a_1,\ldots,a_{n-1})\mathbf{P}(a_1,\ldots,a_{n-1}) = \bigstar$ (économie d'écriture),

$$\begin{aligned} \bigstar &= \left(\frac{u\cos\left(\omega_n-\frac{\pi}{2}a_n\right)+v\big(-\sin\left(\omega_n-\frac{\pi}{2}a_n\right)\big)}{\sqrt{2}}\right)^2\cos^2\Big(\frac{\gamma-\kappa}{2}\Big)+ \\ &\quad \left(\frac{u\cos\left(\omega_n-\frac{\pi}{2}a_n\right)-v\big(-\sin\left(\omega_n-\frac{\pi}{2}a_n\right)\big)}{\sqrt{2}}\right)^2\sin^2\Big(\frac{\gamma-\kappa}{2}\Big) \\ &= \frac{1}{2}(u^2+v^2)\bigg(\cos^2\Big(\omega_n-\frac{\pi}{2}a_n-t\Big)\cos^2\Big(\frac{\gamma-\kappa}{2}\Big)+ \\ &\qquad \cos^2\Big(\omega_n-\frac{\pi}{2}a_n+t\Big)\sin^2\Big(\frac{\gamma-\kappa}{2}\Big)\bigg) \\ &= \mathbf{P}(a_1,\ldots,a_{n-1})\bigg(\cos^2\Big(\omega_n-\frac{\pi}{2}a_n-t\Big)\cos^2\Big(\frac{\gamma-\kappa}{2}\Big)+ \\ &\qquad \cos^2\Big(\omega_n-\frac{\pi}{2}a_n+t\Big)\sin^2\Big(\frac{\gamma-\kappa}{2}\Big)\bigg). \end{aligned}$$

Il n'est pas important d'ajouter π à t lorsque $u>0$ étant donné que l'on élève au carré le cosinus. Par conséquent,

$$\begin{aligned} \mathbf{P}(a_n|a_1,\ldots,a_{n-1}) &= \cos^2\Big(\frac{\gamma-\kappa}{2}\Big)\cos^2\Big(\omega_n-\frac{\pi}{2}a_n-t\Big) \\ &\quad +\sin^2\Big(\frac{\gamma-\kappa}{2}\Big)\cos^2\Big(\omega_n-\frac{\pi}{2}a_n+t\Big). \end{aligned}$$

■

Remarque 2.3.2. $\mathbf{P}(a_n|a_1,\ldots,a_{n-1})$ est une combinaison convexe de deux distributions.

CHAPITRE 3

DES MESURES DE VON NEUMANN GÉNÉRALES AUX MESURES ÉQUATORIALES ET RÉELLES

3.1 Correspondances entres certaines transformations unitaires et certaines mesures sur la sphère de Bloch

Pour ce chapitre, le lecteur peut consulter les livres [8, 9].

Rappel 3.1.1 (mesure sur un qubit)**.** Une mesure sur un qubit est un opérateur hermitien représenté par un triplet $(x,y,z) \in \mathbb{R}^3$ tel que

$$M = x\sigma_1 + y\sigma_2 + z\sigma_3 = \begin{pmatrix} z & x-\imath y \\ x+\imath y & -z \end{pmatrix} \quad \text{et} \quad x^2+y^2+z^2 = 1.$$

Remarque 3.1.1 (paramétrisation d'une mesure sur un qubit)**.** Par conséquent, en utilisant les coordonnées sphériques, la paire (θ,ϕ) peut être utilisée pour représenter une mesure sur un qubit. On a que $x = \cos\theta\cos\phi$, $y = \sin\theta\cos\phi$ et $z = \sin\phi$ où $(\theta,\phi) \in [0,2\pi) \times [0,\pi)$.

Définition 3.1.1 (mesure réelle sur un qubit)**.** Une mesure $M = x\sigma_1 + y\sigma_2 + z\sigma_3$ est *réelle* si $y = 0$.

Définition 3.1.2 (mesure équatoriale sur un qubit)**.** Une mesure $M = x\sigma_1 + y\sigma_2 + z\sigma_3$ est *équatoriale* si $z = 0$.

Le prochain corollaire explique en terme de mesures ce que la partie convexe de **P** (distribution de Bernoulli) et les deux distributions $\mathbf{P}_1$ et $\mathbf{P}_2$ signifient. En effet, on donne l'équivalence en terme de mesures de von Neumann des matrices unitaires impliquées dans le corollaire (2.2.1). Un joueur, au lieu d'appliquer une transformation unitaire sur sa partie et d'ensuite mesurer dans la base standard de calcul, fait une mesure de

von Neumann obtenant ainsi des valeurs propres ± 1. En effet, ici -1 remplace 1 dans la base standard de calcul et $+1$ remplace 0 puisque la vecteur propre $|0\rangle = |+1\rangle$ et $-|1\rangle = |-1\rangle$. De façon générale, le spectre (ensemble des valeurs propres) d'une mesure $M = x\sigma_1 + y\sigma_2 + z\sigma_3$ telle que $x^2+y^2+z^2 = 1$ est $\{-1,+1\}$. Une transformation unitaire U est donnée par

$$U = \begin{pmatrix} \alpha & -\imath^\tau \bar{\beta} \\ \imath^\tau \beta & (-1)^\tau \bar{\alpha} \end{pmatrix} \text{ et } \alpha = e^{i\varphi}\cos\omega,\ \beta = e^{i\psi}\sin\omega$$

Si U est connue, alors, en effectuant le changement de base, on a que $M = U\,\mathrm{diag}(1,-1)U^\dagger$. Par conséquent, en dénotant $w = x + \imath y$,

$$M = \begin{pmatrix} z & \bar{w} \\ w & -z \end{pmatrix} = \begin{pmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \bar{\alpha} & \bar{\beta} \\ -\beta & \alpha \end{pmatrix}$$

donne

$$\begin{aligned} z &= |\alpha|^2 - |\beta|^2 = \cos 2\omega \quad \text{et} \\ w &= 2\imath^\tau \bar{\alpha}\beta = \imath^\tau e^{i(\psi-\varphi)}\sin 2\omega. \end{aligned}$$

Pour représenter une mesure M, les coordonnées sphériques $(\theta,\phi) \in [0,2\pi) \times [0,\pi)$ peuvent être utilisées pour obtenir une interprétation géométrique. Ici, puisque $z = \sin\phi = \cos 2\omega$, alors on a que $\phi = \frac{\pi}{2} + 2\omega$ et puisque $w = e^{\imath(\psi-\varphi+\tau\frac{\pi}{2})}\sin(2\omega)$, alors on a que $\theta = \psi - \varphi + \tau\frac{\pi}{2}$.

Corollaire 3.1.1.

1. Une matrice unitaire U représentée par $(\omega,0,0,0)$ correspond à une mesure réelle sur la sphère de Bloch.

2. Une matrice unitaire U représentée par $(\omega,\varphi,\psi,\tau)$ où $\omega \in \{\pi/4, 3\pi/4, 5\pi/4, 7\pi/4\}$ correspond à une mesure équatoriale sur la sphère de Bloch.

3. En dénotant par $b_j \in \{-1,+1\}$ pour $j \in \{1,\ldots,n\}$ les sorties observées lorsque

des mesures sur la sphère de Bloch sont réalisées, on a que

$$a_1 + \ldots + a_n \equiv 0 \mod 2 \quad \Leftrightarrow \quad b_1 \cdots b_n = +1$$
$$a_1 + \ldots + a_n \equiv 1 \mod 2 \quad \Leftrightarrow \quad b_1 \cdots b_n = -1.$$

3.2 Un mot sur la simulation classique de la distribution $\mathbf{P}(a) = |\langle a|U|\Psi\rangle|^2$

Grâce au corollaire (2.2.1), si des protocoles pour simuler classiquement avec de la communication, en pire cas ou en moyenne, et avec des variables aléatoires partagées les distributions $\mathbf{P}_1$, $\mathbf{P}_2$ ainsi que la partie convexe de $\mathbf{P}$ étaient connus, alors il serait possible de simuler la distribution $\mathbf{P}$. Le corollaire (3.2.1) suivant est équivalent au corollaire (2.2.1) à la différence qu'il est exprimé en utilisant la notion de mesures de von Neumann. Le corollaire (3.2.1) affirme que le problème de la simulation de $\mathbf{P}$ sous l'action locale de mesures de von Neumann peut être scindé en deux problèmes, celui de la simulation reliée aux mesures équatoriales et celui de la simulation reliée aux mesures réelles.

Corollaire 3.2.1. Soit un protocole $\mathrm{P}_{\mathrm{GHZ-R}}$ permettant de simuler les distributions $\mathbf{P}_1$ ou $\mathbf{P}_2$. De plus, soit un protocole $\mathrm{P}_{\mathrm{GHZ-E}}$ pour simuler une distribution de Bernoulli (partie convexe) de paramètre $\cos^2\big((\gamma-\kappa)/2\big)$. Si $\mathrm{P}_{\mathrm{GHZ-E}}$ et $\mathrm{P}_{\mathrm{GHZ-R}}$ existent avec des coûts pire cas ou en moyenne, alors on peut créer un protocole que l'on dénote par $\mathrm{P}_{\mathrm{GHZ}}$ pour simuler la distribution $\mathbf{P}$ tel que $\mathrm{Coût}(P_{GHZ}) \leq \mathrm{Coût}(P_{GHZ-E}) + \mathrm{Coût}(P_{GHZ-R}) + n$.

Démonstration. D'abord les entrées et la sortie de $\mathrm{P}_{\mathrm{GHZ}}$ sont respectivement les paramètres décrivant les transformations unitaires c'est-à-dire $\{(\varphi_j, \psi_j, \omega_j, \tau_j)\}_{j=1}^n$ et un élément $a \in \{0,1\}^n$. Les entrées et la sortie de $\mathrm{P}_{\mathrm{GHZ-E}}$ sont respectivement $\{(\varphi_j, \psi_j, \tau_j)\}_{j=1}^n$ et un bit $c \in \{0,1\}$ tel que $\mathrm{Prob}(c=0) = \cos^2\big((\gamma-\kappa)/2\big)$. Les entrées et la sorties de $\mathrm{P}_{\mathrm{GHZ-R}}$ sont respectivement $\{(\omega_j, \tau_j)\}_{j=1}^n$ et un élément $a \in \{0,1\}^n$ tel que $\mathrm{Prob}(a|c=0) = \mathbf{P}_1(a)$.

On crée $\mathrm{P}_{\mathrm{GHZ}}$ comme suit :

1. $\mathrm{P}_{\mathrm{GHZ}}$ appelle $\mathrm{P}_{\mathrm{GHZ-E}}$ en sous-routine sur entrée $\{(\varphi_j, \psi_j, \tau_j)\}$ pour $j = 1, \ldots, n$. $\mathrm{P}_{\mathrm{GHZ-E}}$ retourne c et, si $c = 0$, alors $\mathrm{P}_{\mathrm{GHZ}}$ branche à (2) sinon $\mathrm{P}_{\mathrm{GHZ}}$ branche à (3).

2. $\mathrm{P}_{\mathrm{GHZ}}$ appelle $\mathrm{P}_{\mathrm{GHZ-R}}$ en sous-routine sur entrée $\{(\omega_j, 0)\}$ pour $j = 1, \ldots, n$. $\mathrm{P}_{\mathrm{GHZ}}$ retourne $a = a_1 \cdots a_n$.

3. $\mathrm{P}_{\mathrm{GHZ}}$ appelle $\mathrm{P}_{\mathrm{GHZ-R}}$ en sous-routine sur entrée $\{(\omega_j, 0)\}$ pour $j = 1, \ldots, n-2$ et $\{(\omega_j, 1)\}$ pour $j = n-1, n$. $\mathrm{P}_{\mathrm{GHZ}}$ retourne $a = a_1 \cdots a_{n-1} a_n$.

Clairement $\mathbf{P}(a)$ est la probabilité de la valeur retournée par $\mathrm{P}_{\mathrm{GHZ}}$ et $\mathrm{Coût}(P_{GHZ}) \leq \mathrm{Coût}(P_{GHZ-E}) + \mathrm{Coût}(P_{GHZ-R}) + n$. Les n bits supplémentaires sont nécessaires pour simuler la partie équatoriale qui consiste à simuler la distribution de la parité c'est-à-dire $\mathrm{Prob}\left(\sum_{j=1}^{n} a_j = c\right)$. Sans perte de généralité, les joueurs peuvent se restreindre à $\omega_j = \pi/4$ pour simuler la partie équatoriale. Les $(n-1)$ premiers joueurs communiquent au n^{e} joueur leurs résultats et ce dernier simule sa « partie » et retourne c aux autres joueurs, ce qui fait un total de n bits.

■

3.2.1 Localité des distributions marginales et simulation de la distribution conditionnelle du n^{e} bit

Dans cette section, on se demande ce qu'il en est de simuler $\mathbf{P}(a_1, \ldots, a_n)$ en utilisant le fait que $\mathbf{P}(a_1, \ldots, a_n) = \mathbf{P}(a_1, \ldots, a_{n-1})\mathbf{P}(a_n | a_1, \ldots, a_{n-1})$. En effet, comme il a été démontré au chapitre 1, toutes les distributions marginales sont locales, et, par conséquent, il ne coûte rien de simuler $\mathbf{P}(a_1, \ldots, a_{n-1})$. Il semble donc que la grande difficulté de simuler $\mathbf{P}(a_1, \ldots, a_n)$ imcombe à la n^{e} personne lorsque $n \geq 2$. La distribution conditionnelle $\mathbf{P}(a_n | a_1, \ldots, a_{n-1})$ est donnée par

$$\begin{aligned} \mathbf{P}(a_n | a_1, \ldots, a_{n-1}) \quad = \quad & \cos^2\left(\frac{\gamma - \kappa}{2}\right) \cos^2\left(\omega_n - \frac{\pi}{2} a_n - t\right) \\ & + \sin^2\left(\frac{\gamma - \kappa}{2}\right) \cos^2\left(\omega_n - \frac{\pi}{2} a_n + t\right). \end{aligned}$$

où

$$\begin{aligned} t &= \arctan\left(\frac{v}{u}\right), \\ u &= \prod_{j=1}^{n-1} \cos(\omega_j - \frac{\pi}{2} a_j), \\ v &= \prod_{j=1}^{n-1} -\sin(\omega_j - \frac{\pi}{2} a_j). \end{aligned}$$

D'abord, la n^{e} personne doit déterminer laquelle de $\cos^2\left(\omega_n - \frac{\pi}{2} a_n - t\right)$ ou de $\cos^2\left(\omega_n - \frac{\pi}{2} a_n + t\right)$ est pertinente en simulant la partie convexe. Par la suite, la n^{e} personne doit avoir une idée de la distribution de t.

CHAPITRE 4

CONCLUSION

Dans ce mémoire, j'ai démontré que la distribution discrète de probabilités **P** est une combinaison convexe de deux distributions, $\mathbf{P}_1$ et $\mathbf{P}_2$. Les coefficients de la combinaison sont associés aux phases des nombres complexes définissant les transformations locales unitaires. Les distributions associées à ces coefficients sont associées aux modules des nombres complexes définissant les transformations locales unitaires.

Du point de vue de la complexité de la communication, l'utilité du résultat réside dans le fait qu'il permet de scinder la simulation de l'état GHZ en deux problèmes. Les deux problèmes sont la simulation de la distribution correspondant aux coefficients de la combinaison convexe et celui de la simulation des distributions associées à ces coefficients.

Parmi les questions ouvertes, on peut se demander si $\mathbf{P}_1$ et $\mathbf{P}_2$ sont locales. On sait que f_1^2, f_2^2 et $(1/2)(\mathbf{P}_1+\mathbf{P}_2) = (1/2)(\mathrm{f}_1^2+\mathrm{f}_2^2)$ sont locales. Quant aux distributions marginales, elles sont toutes locales peu importe le type des transformations unitaires ou, de façon équivalente, des mesures de von Neumann.

BIBLIOGRAPHIE

[1] M. Artin, *Algebra*, Prentice Hall, Upper Saddle River, New Jersey, 1991.

[2] J.-D. Bancal, C. Branciard et N. Gisin, "Simulation of equatorial von Neumann measurements on GHZ states using nonlocal resources", *Advances in Mathematical Physics* **2010**:293245, 2010.

[3] J.S. Bell, "On the Einstein-Podolsky-Rosen paradox", *Physics* **1**:195–200, 1964.

[4] G. Brassard, R. Cleve et A. Tapp, "Cost of exactly simulating quantum entanglement with classical communication", *Physical Review Letters* **83**:1874–1877, 1999.

[5] A. Einstein, B. Podolsky et N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?", *Physical Review* **47**:777–780, 1935.

[6] D. M. Greenberger, M. A. Horne et A. Zeilinger, "Going beyond Bell's theorem", in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht), pp. 69–72, 1989.

[7] E. Kushilevitz et N. Nisan, *Communication Complexity*, Cambridge, University Press, New York, 1997.

[8] G. Ludwig, *Foundations of Quantum Mechanics I*, Springer-Varlag, New York, 1985.

[9] G. Ludwig, *Foundations of Quantum Mechanics II*, Springer-Varlag, New York, 1985.

[10] T. Maudlin, "Bell's inequality, information transmission, and prism models", *Biennial Meeting of the Philosophy of Science Association*, pp. 404–417, 1992.

[11] P. A. Meyer, *Quantum probability for probabilists (2^e édition)*, Springer-Verlag, Berlin, 1995.

[12] M. A. Nielsen et I. L. Chuang *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000

[13] O. Regev et B. Toner, "Simulating quantum correlations with finite communication", *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, pp. 384–394, 2007.

[14] G. Roos, *Géométrie et analyse : Méthodes hilbertiennes*, Dunod, Paris, 2002.

[15] K. Spindler, *Abstract Algebra with Applications Volume 1: Vector Spaces and Groups*, Dekker, New York, 1994.

[16] M. Steiner, "Towards quantifying non-local information transfer: finite-bit non-locality", *Physics Letters A* **270**:239–244, 2000.

[17] B. Toner et D. Bacon, "Communication cost of simulating Bell correlations", *Physical Review Letters* **91**:187904, 2003.

Annexe I

Code Matlab

Le programme suivant en Matlab n'a pour but que de comparer la formule originelle $\mathrm{Tr}(|a\rangle\langle a|U\rho U^{\dagger})$ lorsque $U=\otimes_{j=1}^{n}U_j$ avec la formule $\cos^2\left(\frac{\gamma-\kappa}{2}\right)\mathbf{P}_1(a)+\sin^2\left(\frac{\gamma-\kappa}{2}\right)\mathbf{P}_2(a)$ afin de vérifier empiriquement les développements théoriques dans le but de convaincre les sceptiques qui n'auraient pas lu la preuve. (Le but premier était cependant de faire de l'analyse asymptotique numériquement avec ma formule. En effet, grâce à ma formulation, il est possible de regarder le comportement asymptotique de **P** de façon numérique. On ne peut rien faire avec la trace numériquement parce que les produits tensoriels font exploser la mémoire lorsque $n>14$ ou $n>15$, tout dépend de la quantité de mémoire.) Les deux formules sont comparées en utilisant des transformations unitaires aléatoires. On peut récupérer les paramètres $(\varphi_j,\psi_j,\omega_j,\tau_j)$ définissant les transformations à la sortie du programme. Chaque exécution du programme génère de nouvelles transformations aléatoires. Le programme prend deux arguments : le premier étant le nombre de transformations (personnes) et le deuxième étant un « flag » permettant d'indiquer au programme de générer des transformations correspondant à des mesures équatoriales ou des transormations unitaires générales.
Il ne faut que taper « help ProbU2GHZ » (ne pas écrire « help ProbU2GHZ ; ») dans la ligne de commande de Matlab pour savoir comment l'utiliser.

Voici un exemple de sortie dans le cas général avec $n=4$.

```
>>  [om ph vp ta] = ProbU2GHZ(4,'G');

(formule originelle) Prob(0000 =      0) = 0.107490275647
(formule nouvelle  ) Prob(0000 =      0) = 0.107490275647
```

```
(formule originelle) Prob(0001 =      1) = 0.017104836590
(formule nouvelle  ) Prob(0001 =      1) = 0.017104836590
(formule originelle) Prob(0010 =      2) = 0.030143438194
(formule nouvelle  ) Prob(0010 =      2) = 0.030143438194
(formule originelle) Prob(0011 =      3) = 0.015070620186
(formule nouvelle  ) Prob(0011 =      3) = 0.015070620186
(formule originelle) Prob(0100 =      4) = 0.010312458463
(formule nouvelle  ) Prob(0100 =      4) = 0.010312458463
(formule originelle) Prob(0101 =      5) = 0.076345362036
(formule nouvelle  ) Prob(0101 =      5) = 0.076345362036
(formule originelle) Prob(0110 =      6) = 0.050578091589
(formule nouvelle  ) Prob(0110 =      6) = 0.050578091589
(formule originelle) Prob(0111 =      7) = 0.192954917295
(formule nouvelle  ) Prob(0111 =      7) = 0.192954917295
(formule originelle) Prob(1000 =      8) = 0.192954917295
(formule nouvelle  ) Prob(1000 =      8) = 0.192954917295
(formule originelle) Prob(1001 =      9) = 0.050578091589
(formule nouvelle  ) Prob(1001 =      9) = 0.050578091589
(formule originelle) Prob(1010 =     10) = 0.076345362036
(formule nouvelle  ) Prob(1010 =     10) = 0.076345362036
(formule originelle) Prob(1011 =     11) = 0.010312458463
(formule nouvelle  ) Prob(1011 =     11) = 0.010312458463
(formule originelle) Prob(1100 =     12) = 0.015070620186
(formule nouvelle  ) Prob(1100 =     12) = 0.015070620186
(formule originelle) Prob(1101 =     13) = 0.030143438194
(formule nouvelle  ) Prob(1101 =     13) = 0.030143438194
(formule originelle) Prob(1110 =     14) = 0.017104836590
(formule nouvelle  ) Prob(1110 =     14) = 0.017104836590
(formule originelle) Prob(1111 =     15) = 0.107490275647
(formule nouvelle  ) Prob(1111 =     15) = 0.107490275647
```

```
Somme des probs (formule originelle) = 1.000000000000
Somme des probs (formule nouvelle  ) = 1.000000000000
```

Voici un exemple de sortie dans le cas équatorial avec $n = 5$.

```
>>  [om ph vp ta] = ProbU2GHZ(5,'E');

(formule originelle) Prob(00000 =      0) = 0.061139913779
(formule nouvelle  ) Prob(00000 =      0) = 0.061139913779
(formule originelle) Prob(00001 =      1) = 0.001360086221
(formule nouvelle  ) Prob(00001 =      1) = 0.001360086221
(formule originelle) Prob(00010 =      2) = 0.001360086221
(formule nouvelle  ) Prob(00010 =      2) = 0.001360086221
(formule originelle) Prob(00011 =      3) = 0.061139913779
(formule nouvelle  ) Prob(00011 =      3) = 0.061139913779
(formule originelle) Prob(00100 =      4) = 0.001360086221
(formule nouvelle  ) Prob(00100 =      4) = 0.001360086221
(formule originelle) Prob(00101 =      5) = 0.061139913779
(formule nouvelle  ) Prob(00101 =      5) = 0.061139913779
(formule originelle) Prob(00110 =      6) = 0.061139913779
(formule nouvelle  ) Prob(00110 =      6) = 0.061139913779
(formule originelle) Prob(00111 =      7) = 0.001360086221
(formule nouvelle  ) Prob(00111 =      7) = 0.001360086221
(formule originelle) Prob(01000 =      8) = 0.001360086221
(formule nouvelle  ) Prob(01000 =      8) = 0.001360086221
(formule originelle) Prob(01001 =      9) = 0.061139913779
(formule nouvelle  ) Prob(01001 =      9) = 0.061139913779
(formule originelle) Prob(01010 =     10) = 0.061139913779
(formule nouvelle  ) Prob(01010 =     10) = 0.061139913779
```

```
(formule originelle) Prob(01011 =     11) = 0.001360086221
(formule nouvelle  ) Prob(01011 =     11) = 0.001360086221
(formule originelle) Prob(01100 =     12) = 0.061139913779
(formule nouvelle  ) Prob(01100 =     12) = 0.061139913779
(formule originelle) Prob(01101 =     13) = 0.001360086221
(formule nouvelle  ) Prob(01101 =     13) = 0.001360086221
(formule originelle) Prob(01110 =     14) = 0.001360086221
(formule nouvelle  ) Prob(01110 =     14) = 0.001360086221
(formule originelle) Prob(01111 =     15) = 0.061139913779
(formule nouvelle  ) Prob(01111 =     15) = 0.061139913779
(formule originelle) Prob(10000 =     16) = 0.001360086221
(formule nouvelle  ) Prob(10000 =     16) = 0.001360086221
(formule originelle) Prob(10001 =     17) = 0.061139913779
(formule nouvelle  ) Prob(10001 =     17) = 0.061139913779
(formule originelle) Prob(10010 =     18) = 0.061139913779
(formule nouvelle  ) Prob(10010 =     18) = 0.061139913779
(formule originelle) Prob(10011 =     19) = 0.001360086221
(formule nouvelle  ) Prob(10011 =     19) = 0.001360086221
(formule originelle) Prob(10100 =     20) = 0.061139913779
(formule nouvelle  ) Prob(10100 =     20) = 0.061139913779
(formule originelle) Prob(10101 =     21) = 0.001360086221
(formule nouvelle  ) Prob(10101 =     21) = 0.001360086221
(formule originelle) Prob(10110 =     22) = 0.001360086221
(formule nouvelle  ) Prob(10110 =     22) = 0.001360086221
(formule originelle) Prob(10111 =     23) = 0.061139913779
(formule nouvelle  ) Prob(10111 =     23) = 0.061139913779
(formule originelle) Prob(11000 =     24) = 0.061139913779
(formule nouvelle  ) Prob(11000 =     24) = 0.061139913779
(formule originelle) Prob(11001 =     25) = 0.001360086221
(formule nouvelle  ) Prob(11001 =     25) = 0.001360086221
```

```
(formule originelle) Prob(11010 =     26) = 0.001360086221
(formule nouvelle  ) Prob(11010 =     26) = 0.001360086221
(formule originelle) Prob(11011 =     27) = 0.061139913779
(formule nouvelle  ) Prob(11011 =     27) = 0.061139913779
(formule originelle) Prob(11100 =     28) = 0.001360086221
(formule nouvelle  ) Prob(11100 =     28) = 0.001360086221
(formule originelle) Prob(11101 =     29) = 0.061139913779
(formule nouvelle  ) Prob(11101 =     29) = 0.061139913779
(formule originelle) Prob(11110 =     30) = 0.061139913779
(formule nouvelle  ) Prob(11110 =     30) = 0.061139913779
(formule originelle) Prob(11111 =     31) = 0.001360086221
(formule nouvelle  ) Prob(11111 =     31) = 0.001360086221

Somme des probs (formule originelle) = 1.000000000000
Somme des probs (formule nouvelle  ) = 1.000000000000



Prob(a1 + ... + an = 0) *** cas equatorial

(directe) Prob(sum a_i = 0) = 0.978238620467
(formule) Prob(sum a_i = 0) = 0.978238620467

     sin^2((gamma-kappa)/2) = 0.978238620467
```

Voici le code en Matlab.

```
function [om ph vp ta] = ProbU2GHZ(nn,eq_fl)
%
% INPUTS
% nn : nombre de transformations SU(2)
%      nn est un entier naturel > 0
% eq_fl : 'E' pour équatorial
%         'G' pour général
%
% OUTPUTS
% om : paramètres omega transformations U2
% ph : paramètres phi transformations U2
% vp : paramètres varphi transformations U2
% ta : paramètres tau transformations U2
%
% Exemple : [om ph vp ta] = ProbU2GHZ(6,'E');
% Exemple : [om ph vp ta] = ProbU2GHZ(9,'G');

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% vérification des arguments de la routine - début
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

```
if ( ( (floor(nn)-nn)~=0 ) | (nn<=0)) error('nn doit etre > 0 et entier'); end;
if ( (~strcmp(eq_fl,'G')) & (~strcmp(eq_fl,'E')) ) error('eq_fl doit etre G ou E'); end;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% vérification des arguments de la routine - fin
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% données générales - début
%
% psighz : vecteur représentant ghz
% rho : matrice de densité représentant ghz
% PparitePair : variable active seulement dans le cas equatorial
%               additionne toutes les P(a1,...,an) tels que a1+...+an=0 mod 2
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

psighz = zeros(2^nn,1);
psighz(1,1) = 1/sqrt(2);
psighz(2^nn,1) = 1/sqrt(2);

rho = psighz*psighz';
```

```
P1 = inline('0.5*((prod(cos(x))+prod(-sin(x)))^2)','x');
P2 = inline('0.5*((prod(cos(x))-prod(-sin(x)))^2)','x');
if(strcmp(eq_fl,'E')==1)
 PparitePair = 0;
end;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% données générales - fin
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% inputs début
%
% om : paramètre omega ; transformation U2
% ph : paramètre phi ; transformation U2
% vp : paramètre varphi ; transformation U2
% ta : paramètre tau ; transformation U2
% kappa = somme des tau
% gamma = somme des omega
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

```
if(strcmp(eq_fl,'E')==1)
 %cas équatorial
 %omega = pi/4, 3pi/4, 5pi/4, 7pi/4
 om = 0.25*pi*(2*round(3*rand(1,nn))+1);
else
 %cas général
 om = 2*pi*rand(1,nn);% cas général
end;
vp = 2*pi*rand(1,nn);
ph = 2*pi*rand(1,nn);
ta = round(rand(1,nn));

kappa = sum(ta)*pi*0.5;
gamma = sum(ph+vp);
U=1;
for i1 = 1:1:nn
 Am(:,:,i1) = [exp(i*0.5*(vp(i1)-ph(i1))) 0; 0 exp(-i*0.5*(vp(i1)-ph(i1)))];
 Ap(:,:,i1) = [exp(i*0.5*(vp(i1)+ph(i1))) 0; 0 exp(-i*0.5*(vp(i1)+ph(i1)))];
 Cw(:,:,i1) = [cos(om(i1)) -(i^ta(i1))*sin(om(i1)); (i^ta(i1))*sin(om(i1)) (i^(2*ta(i1)))*cos(om(i1))];
 Ux(:,:,i1) = Am(:,:,i1)*Cw(:,:,i1)*Ap(:,:,i1);
```

```
 U = kron(U,Ux(:,:,i1));
end;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% inputs fin
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


for x1 = 0:1:((2^nn)-1)

  bx1tmp = dec2bin(x1,nn);

  for t1 = 1:1:nn
   bx1(t1) = str2num(bx1tmp(t1));
  end;

  out=1; %vecteur des sorties
  for t1 = 1:1:nn
   v(:,t1) = (bx1(t1)==0)*[1;0]+(bx1(t1)==1)*[0;1];
   out = kron(out,v(:,t1));
  end;
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% avec formule trace - début
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

Mout = out*(out'); %opérateur mesure
pv1(x1+1) = trace(Mout*U*rho*ctranspose(U));
fprintf(1,'\n(formule originelle) Prob(%s = %6d) = %.12f',bx1tmp,x1,pv1(x1+1));

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% avec formule trace - fin
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% avec nouvelle formule - début
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

xinp = om - 0.5*pi*bx1;
pv2(x1+1) = ((cos((gamma-kappa)*0.5))^2)*P1(xinp) + ((sin((gamma-kappa)*0.5))^2)*P2(xinp) ;
fprintf(1,'\n(formule nouvelle  ) Prob(%s = %6d) = %.12f',bx1tmp,x1,pv2(x1+1));
```

```
  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
  % avec nouvelle formule - fin
  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%



  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
  % parite, cas equatorial - début
  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

  if(strcmp(eq_fl,'E')==1)
   if(mod(sum(bx1),2)==0)
    PparitePair = PparitePair +  pv1(x1+1);
   end;
  end;

  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
  % parité, cas équatorial - fin
  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


end;
```

```
fprintf(1,'\n\nSomme des probs (formule originelle) = %.12f',sum(pv1));
fprintf(1,'\nSomme des probs (formule nouvelle  ) = %.12f\n\n',sum(pv2));

if(strcmp(eq_fl,'E')==1)
 fprintf(1,'\n\nProb(a1 + ... + an = 0) *** cas equatorial');
 fprintf(1,'\n\n(directe) Prob(sum a_i = 0) = %.12f', PpairitePair);
 PpariteFormule = 0.5 + 0.5*((-1)^(nn))*prod(sin(2*om))*cos(gamma-kappa);
 fprintf(1,'\n(formule) Prob(sum a_i = 0) = %.12f\n', PpariteFormule);
 if( (mod(nn,2)==0) & (prod(sin(2*om)) == 1) )
  fprintf(1,'\n     cos^2((gamma-kappa)/2) = %.12f\n\n',(cos(0.5*(gamma-kappa)))^2);
 elseif ( (mod(nn,2)==0) & (prod(sin(2*om)) == -1) )
  fprintf(1,'\n     sin^2((gamma-kappa)/2) = %.12f\n\n',(sin(0.5*(gamma-kappa)))^2);
 elseif( (mod(nn,2)==1) & (prod(sin(2*om)) == 1) )
  fprintf(1,'\n     sin^2((gamma-kappa)/2) = %.12f\n\n',(sin(0.5*(gamma-kappa)))^2);
 else % ( (mod(nn,2)==1) & (prod(sin(2*om)) == -1) )
  fprintf(1,'\n     cos^2((gamma-kappa)/2) = %.12f\n\n',(cos(0.5*(gamma-kappa)))^2);
 end;

end;
```