Influence de l'enchevêtrement dans les systèmes de preuves interactives quantiques

Thomas Vidick
Sous la direction de Julia Kempe
LRI, université Paris-Sud

27 juillet 2006

Remerciements

Ce stage a été effectué au Laboratoire de Recherche en Informatique (LRI) de l'université Paris-Sud, dans le groupe Algorithmique et Complexité dirigé par Miklos Santha.

Je tiens à remercier chaleureusement Julia Kempe pour avoir bien voulu encadrer ce stage, ainsi que pour sa grande diponibilité, sa créativité et son dynamisme à toute épreuve. Julia m'aura montré l'importance de poser les bonnes questions, et mon seul regret est d'en remporter beaucoup plus dans mes cartons que je n'ai pu en résoudre lors de ce stage !

Je remercie également toute les membres de l'équipe Algorithmique et Complexité pour leur accueil, et pour avoir fait du laboratoire un lien d'échange si agréable. Finalement, je remercie Thang Nguyen pour son amitié lors de ce stage, que nous avons effectué avec la même directrice.

Table des matières

1 Introduction

Dans les années 80, Feynman a été le premier a envisager la mécanique quantique d'un point de vue calculatoire, en remarquant que la simulation de systèmes quantiques sur un ordinateur classique semblait nécéssiter une augmentation de la complexité exponentielle en la taille du système. Il demanda si cela était inévitable, et s'il était possible de fabriquer un ordinateur quantique universel. Deutsch, en 85, a défini le modèle de la machine de Turing quantique, et Yao a montré que le modèle du circuit quantique, également défini par Deutsch, lui était équivalent.

Le démonstration le plus frappante de la puissance de calcul d'un ordinateur quantique, s'il pouvait être construit, a été donnée par Shor en 94, lorsqu'il a prouvé l'existence d'algorithmes quantiques en temps polynomial pour la factorisation et le logarithme discret.

Ce résultat a lancé l'étude des algorithmes et des classes de complexité quantiques. Le domaine du « Calcul Quantique » s'est rapidement développé, et constitue maintenant un domaine d'étude à part entière. L'introduction des règles de calcul quantiques a également permis d'améliorer notre compréhension de phénomènes purement classiques, et certains résultats ont trouvé une preuve élégante à travers le formalisme quantique ([Aar05, KdW04] par exemple).

Dans ce mémoire, nous nous intéressons plus particulièrement à l'étude des systèmes de preuves interactives quantiques à plusieurs prouveurs. Un des phénomènes les plus intéressants révélés par les lois de la mécanique quantique est l'*enchevêtrement* entre des particules, qui fait que l'observation de l'état de particules distantes dans l'espace-temps peut produire des résultats corrélés entre eux, corrélations qui seraient impossibles à obtenir classiquement [CHSH69].

Dans le cadre des systèmes de preuves interactives à deux prouveurs, l'enchevêtrement peut être vu comme une ressource partagée par les prouveurs, leur permettant de coordonner leurs réponses aux questions d'un vérifieur soupçonneux, même s'il leur est interdit de communiquer directement.

Ce mémoire est organisé de la façon suivante. Nous commençons par donner quelques rappels, non exhaustifs, liés au formalisme du calcul quantique. Ensuite, nous présentons une sélection de résultats connus sur les systèmes de preuves interactives à un seul prouveur, d'abord classiques puis quantiques ; ces résultats serviront de base et d'éclairage à la partie 5, consacrée aux protocoles de preuves interactives à plusieurs prouveurs.

Nos contributions sont regroupées dans les parties 5.1.3, 5.2, 5.3 et 5.4, dont tous les résultats sont originaux, sauf mention explicite du contraire. Nous étudions plusieurs modèles de preuves interactives à deux prouveurs, du plus particulier au plus général. En particulier, dans la partie 5.1.3 nous mettons en évidence un lien entre preuves interactives à deux prouveurs et algorithmes d'approximation, lien précisé dans le cadre du problème MAXCUT. Dans la partie 5.2 nous généralisons un résultat de [Weh06]. Finalement, en 5.4 nous montrons que deux prouveurs et deux messages suffisent à simuler un prouveur et trois messages, lorsque ces prouveurs partagent de l'enchevêtrement.

2 Préliminaires

Dans cette section, nous donnons quelques définitions et notations qui nous seront nécessaires dans la suite. C'est également l'occasion de rappeler quelques-uns des principes de base du calcul quantique. Nous supposons cependant une certaine familiarité avec ces principes, et le lecteur pourra en cas de besoin se reporter à des livres de référence tels que [NC00] et [KSV01].

2.1 Notations

On note Σ un alphabet fini, en général $\Sigma = \{0,1\}$. On désignera par *poly* l'ensemble des fonctions $f : \mathbb{N} \to \mathbb{N}$ satisfaisant aux deux conditions suivantes :

- Il existe un polynôme p tel que $\forall n \in \mathbb{N},\ f(n) \leq p(n)$.
- $f(n)$ est calculable en temps polynomial en n.

On notera $\mathcal{F}, \mathcal{G}, \mathcal{N}$ des espaces de Hilbert de dimension finie. Notre espace de travail élémentaire, correspondant à un qubit, est $\mathbb{C}^2$. On le note également $\mathcal{B}$ lorsqu'il est muni de sa base canonique $\{|0\rangle, |1\rangle\}$. On note ainsi $\mathcal{B}^{\otimes n}$ l'espace $\mathbb{C}^{2^n}$ muni de la base $\{|x_1, \ldots, x_n\rangle : x_j \in \mathbb{B}\}$, où $\mathbb{B} = \{0,1\}$.

$L(\mathcal{F})$ désignera l'ensemble des opérateurs linéaires sur l'espace $\mathcal{F}$ de dimension 2^n, et on l'identifiera généralement avec l'ensemble des matrices de taille $2^n \times 2^n$ à coefficients complexes. On note $D(\mathcal{F})$ l'ensemble des matrices densité sur $\mathcal{F}$, c'est-à-dire l'ensemble des matrices hermitiennes positives de trace 1. $U(\mathcal{F})$ est l'ensemble des matrices unitaires sur $\mathcal{F}$.

On rappelle qu'en toute généralité, un système quantique isolé de n qubits est décrit par un vecteur unitaire $|\Psi\rangle$ de $\mathcal{B}^n$. Un système quantique de n qubits non isolé est décrit par une matrice densité $\rho \in D(\mathcal{B}^n)$. L'évolution d'un système quantique est décrit par une matrice unitaire $U \in U(\mathcal{B}^n)$.

Si $\mathcal{F}, \mathcal{G}$ sont deux espaces hermitiens de dimension respectivement 2^n et 2^p, alors $\mathcal{N} = \mathcal{F} \otimes \mathcal{G}$ est un espace hermitien de dimension 2^{n+p}. Si $\rho \in D(\mathcal{N})$, ρ admet une décomposition

$$\rho = \sum_{i=1}^{p} \sigma_i \otimes \gamma_i \qquad \sigma_i \in L(\mathcal{F}),\ \gamma_i \in L(\mathcal{G})$$

On définit alors l'application trace partielle

$$\mathrm{Tr}_{\mathcal{G}} : D(\mathcal{N}) \to D(\mathcal{F})$$

par

$$\forall \rho \in D(\mathcal{N}) \qquad \mathrm{Tr}_{\mathcal{G}}(\rho) = \sum_{i=1}^{p} \mathrm{Tr}\,(\gamma_i)\, \sigma_i$$

2.2 Circuits quantiques

Le modèle de calcul sur lequel sont basés les systèmes de preuves interactives quantiques est celui du circuit quantique. Soit A est un ensemble ordonné de k qubits, et $\mathcal{A}$ un espace hermitien de dimension 2^k décrivant l'ensemble des états quantiques sur les qubits de A. Pour $U \in U(\mathcal{A})$, on note $U[\mathsf{A}]$ l'action de U sur les qubits de A, si on désire préciser que

l'on fait agir U sur le registre A, ce qui est parfois nécessaire lorsque l'on considère des états d'un système plus grand.

Définition 1 *Soit $\mathcal{U}$ un ensemble fixé d'opérateurs unitaires (on appelle $\mathcal{U}$ une base, ou un ensemble de portes, alors que ses éléments sont appelés des portes). Un* circuit quantique sur la base $\mathcal{U}$ *est une séquence $U_1[\mathsf{A}_1], \ldots, U_L[\mathsf{A}_L]$, où $U_j \in \mathcal{U}$ et A_j est un ensemble ordonné de qubits.*

L'opérateur réalisé par ce circuit est $U = U_L[\mathsf{A}_L] \ldots U_1[\mathsf{A}_1]$ ($U : \mathcal{B}^{\otimes n} \to \mathcal{B}^{\otimes n}$). L est appelé la taille *du circuit.*

Pour les besoins des sections suivantes, nous étendons cette définition pour autoriser l'utilisation de qubits *auxiliaires* par un circuit quantique.

Définition 2 *Un circuit quantique Q de type (n, k) est la donnée d'un circuit quantique R sur un ensemble A de $n+p$ qubits, pour un certain $p \in \mathbb{N}$, comme décrit dans la section précédente, et d'un ensemble ordonné de* qubits de sortie S *de cardinal k.*

Si V est l'opérateur réalisé par le circuit R, alors l'opérateur réalisé par le circuit Q est $U = \mathrm{Tr}_{\mathsf{A}\setminus\mathsf{S}}\left(V \cdot (I_p \otimes |0\rangle^{\otimes p})\right)$. C'est-à-dire que Q commence par ajouter p qubits auxiliaires initialisés à $|0\rangle^{\otimes p}$ à son entrée, puis exécute le circuit R sur l'état total, et enfin ne renvoie que les qubits de S en sortie. Par abus de notation, on notera

$$Q|0\rangle = U|0\rangle^{\otimes n} = \mathrm{Tr}_{\mathsf{A}\setminus\mathsf{S}}\left(V(|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes p})\right)$$

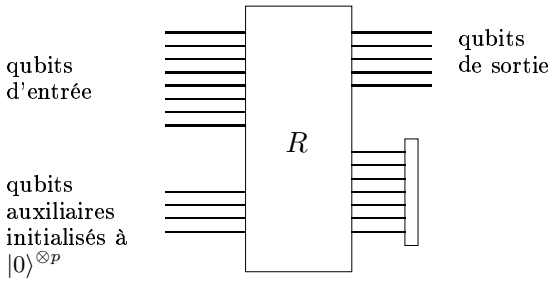

FIG. 1 – Le circuit Q

On note que les qubits de sortie d'un circuit du type décrit ci-dessus peuvent être enchevêtrés avec les autres qubits, et donc un tel circuit renvoie en général une matrice densité, même lorsqu'il est exécuté sur un état pur.

Le choix de la base est important puisqu'il influe sur la taille du circuit. Comme il y a une quantité indénombrable de matrices unitaires de taille 2^n, une base complète devrait contenir une infinité (indénombrable) de portes. Nous allons nous contenter d'une base de cardinalité finie, qui permet cependant d'approcher efficacement tous les opérateurs unitaires.

Définition 3 *Soient*

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad CNOT = \begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{pmatrix} \qquad et \qquad \pi/8 = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}$$

H est la porte de Hadamard, $CNOT$ est le non controlé, et $\pi/8$ est la rotation d'angle $\pi/8$. On nomme l'ensemble $\{H, CNOT, \pi/8\}$ la base standard.

Proposition 4 *L'ensemble $\{H, CNOT, \pi/8\}$ est universel dans le sens où tout opérateur unitaire U sur un nombre constant de qubits peut être réalisé avec précision δ par un circuit de taille poly(log(1/δ)) sur la base standard (la notion d'approximation est celle qui dérive naturellement de la norme matricielle usuelle).*

On dira qu'une famille $\{Q_x\}$ de circuits est *uniformément générée en temps polynomial* s'il existe une procédure déterministe qui, prenant en entrée x, renvoie une description du circuit Q_x (en n'utilisant que des portes de la base standard) et fonctionne en temps polynomial en $|x|$. Les actions entreprises par les différentes parties interagissant dans un protocole de preuve interactive quantique seront décrites par des circuits quantiques. Les actions du vérifieur, dont la puissance est limitée, seront essentiellement décrites par des familles de circuits uniformément générées en temps polynomial (nous serons plus précis dans la section correspondante), alors que le prouveur est autorisé à utiliser des circuits faisant intervenir des opérateurs unitaires arbitraires, et n'est pas limité à la base standard.

2.3 Distinguabilité des états quantiques

Les états que l'on considère seront donnés par des matrices densité, spécifiées avec une certaine précision. Une matrice densité correspond à une distribution de probabilités pour chacune des mesures que l'on pourrait effectuer dessus. Il est donc naturel de dire que deux matrices densité sont proches lorsque, pour chaque mesure que l'on pourrait effectuer sur ces matrices densité, les distributions de probabilités sur les différents résultats possibles de cette mesure, lorsqu'elle est appliquée à chacune des deux matrices, sont proches. Nous commençons donc par nous intéresser aux mesures sur les distributions de probabilités.

Soit w une distribution de probabilités discrète sur les résultats obtenus par un certain appareil. Supposons que l'appareil soit défectueux, c'est-à-dire qu'il donne le bon résultat avec probabilité $1-\epsilon$ et le mauvais avec probabilité ϵ. Si w' est la distribution de probabilités sur les résultats de l'appareil défectueux, alors

$$\sum_j |w'_j - w_j| \leq 2\,\epsilon$$

Réciproquement, si cette inégalité est vérifiée, alors w' peut être exprimé comme la succession de deux processus : le premier effectue un tirage aléatoire selon la loi w, et le second perturbe le résultat avec probabilité ϵ. La distance naturelle sur les distributions de probabilités est donc la norme ℓ^1

$$\|w - w'\|_1 = \sum_j |w'_j - w_j|$$

Généralisons cette définition à des matrices densité arbitraires.

Définition 5 *La* norme trace *d'un opérateur linéaire A est*

$$\|A\|_{tr} = \mathrm{Tr}\left(\sqrt{A\,A^*}\right)$$

La proposition suivante fait le lien avec les distributions de probabilités sur les résultats des différentes mesures que l'on peut effectuer sur un système quantique décrit par une matrice densité.

Proposition 6 *Soient ρ, γ deux matrices densité. Alors*

$$\|\rho - \gamma\|_{tr} = \max_U |\,\mathrm{Tr}\; U(\rho - \gamma)|$$

où le maximum est pris sur toutes les matrices unitaires.

Si $\{\Pi_0, \Pi_1\}$ sont deux projecteurs orthogonaux associés, correspondant à une mesure projective binaire, alors l'opérateur $U = \Pi_0 - \Pi_1$ est unitaire. La proposition précédente se réécrit

$$|\,\mathrm{Tr}\,(\Pi_0\rho) - \mathrm{Tr}\,(\Pi_0\gamma)| + |\,\mathrm{Tr}\,(\Pi_1\rho) - \mathrm{Tr}\,(\Pi_1\gamma)| \leq \|\rho - \gamma\|_{\mathrm{tr}}$$

Ainsi, la mesure projective $\{\Pi_0, \Pi_1\}$ permet de distinguer ρ de γ (ie, donne un résultat différent sur ρ et sur γ) avec probabilité au plus $\|\rho - \gamma\|_{\mathrm{tr}}$. La norme trace mesure donc la probabilité maximale avec laquelle une mesure permet de distinguer deux matrices densité.

Nous introduisons une deuxième mesure de la proximité de deux états quantiques, parfois plus pratique à utiliser que la norme trace : la *fidélité*.

Définition 7 *Soient $\rho, \gamma \in D(\mathcal{N})$ deux matrices densité. La fidélité $F(\rho, \gamma)$ de ρ et de γ est définie par*

$$F(\rho,\gamma) = \max\{|\langle\xi|\eta\rangle|^2 \,:\, \mathrm{Tr}_{\mathcal{F}}(|\xi\rangle\langle\xi|) = \rho,\, \mathrm{Tr}_{\mathcal{F}}(|\eta\rangle\langle\eta|) = \gamma\}$$

où le maximum est pris sur toutes les purifications $|\xi\rangle$, $|\eta\rangle$ de ρ et γ sur tous les espaces auxiliaires $\mathcal{F}$ de dimension $\dim\mathcal{F} = \dim\mathcal{N}$.

La fidélité est reliée à la norme trace par les propriétés suivantes.

Proposition 8 *1.* $F(\rho,\gamma) = \|\sqrt{\rho}\sqrt{\gamma}\|_{tr}^2$

2. $\left(1 - \dfrac{\|\rho-\gamma\|_{tr}}{2}\right)^2 \leq F(\rho,\gamma) \leq 1 - \left(\dfrac{\|\rho-\gamma\|_{tr}}{2}\right)^2$

2.4 Opérateurs de mesure

Nous rappelons rapidement ici le formalisme utilisé pour décrire les opérations de mesure en mécanique quantique, sans donner de détails. En cas de besoin, on pourra se référer à [NC00].

Soit $\mathcal{F}$ un espace hermitien, et $\rho \in D(\mathcal{F})$ une matrice densité décrivant l'état d'un système quantique. Le type de mesure le plus général que l'on puisse effectuer sur ρ s'appelle une *mesure positive*, ou POVM (*positive operator valued measure*). Une telle mesure est

décrite par une collections $\{X_a,\, a \in A\}$ de matrices positives se sommant à l'identité : $\Sigma_a X_a = \mathrm{Id}$. Lorsque cette mesure est appliquée au système ρ, on obtient le résultat $a \in A$ avec probabilité $\mathrm{Tr}\,(X_a \rho)$. Dans le cas où $\rho = |\Psi\rangle\langle\Psi|$ correspond à un état pur, la probabilité d'obtenir a devient $\langle\Psi|X_a|\Psi\rangle$.

Les *mesures projectives* sont une classe a priori plus restreinte d'opérateurs de mesure : elles sont données par une collection $\{\Pi_a,\, a \in A\}$ de projecteurs associés. Cependant, il est connu qu'un POVM peut toujours être simulé par une mesure projective sur un état plus grand, en ajoutant des qubits auxiliaires. Ainsi, dans ce rapport nous nous restreindrons souvent à considérer des mesures projectives, cependant cela n'entraîne pas de perte de généralité.

3 Preuves interactives classiques

Selon la définition de Cook-Levin, un système de preuves NP est constitué de deux machines de Turing A et B, respectivement le *prouveur* et le *vérifieur*. Le prouveur dispose d'une puissance en temps illimitée, alors que le vérifieur est polynomial. Les deux sont déterministes, possèdent une entrée commune x, et interagissent de la manière suivante : A calcule une chaîne y de longueur polynomiale à partir de x, et l'écrit sur un ruban spécial que B peut lire. B calcule alors une fonction $f_L(x, y)$ et accepte si et seulement si $f_L(x, y) = 1$.

La classe NP capture ainsi les langages L tels qu'une preuve d'appartenance d'une certaine entrée $x \in \Sigma^*$ à L puisse être écrite une fois pour toutes (cette preuve dépend de x et de L), et vérifiée de manière efficace par la suite. En 1985, Goldwasser, Micali et Rackoff [GMR85] proposent de généraliser cette définition, et de considérer des systèmes de preuves *interactifs*. L'idée est que l'on va autoriser la machine B à poser des questions à A, chaque question pouvant dépendre des réponses reçues aux questions précédentes. Ceci « rend la vie beaucoup plus simple » comme ils le disent eux-même, B pouvant, en fonction des réponses de A, demander des éclaircissements sur telle ou telle partie de la preuve.

On définit ainsi une *machine de Turing interactive* MTI. Une telle machine dispose d'un ruban de travail, d'un ruban d'aléas, d'un ruban d'entrée, et de deux rubans spéciaux de communication, l'un réservé à la lecture et l'autre à l'écriture. Deux MTI forment une paire de machines de Turing interactives si elles partagent le même ruban d'entrée, et si l'une écrit sur le ruban à lecture seule de l'autre et vice-versa.

Définition 9 *Soient $c, s : \mathbb{N} \to [0, 1]$, $m : \mathbb{N} \to \mathbb{N}$ des fonctions telles que $s < c$ et $m \in poly$. On note $IP_{c,s}(m)$ la classe des langages L tels qu'il existe une paire (A, B) de machines de Turing interactives vérifiant :*

- *Pour tout $x \in L$ écrit sur le ruban d'entrée commun à A et à B, après que A et B aient échangé $m(|x|)$ messages, B accepte avec probabilité au moins $c(|x|)$.*
- *Pour tout $x \notin L$ et toute machine de Turing interactive A', la paire (A', B) accepte l'entrée x avec probabilité au plus $s(|x|)$, après que $m(|x|)$ messages aient été échangés.*

On dira alors que (A, B) *est un* système de preuve interactif *pour* L.

La puissance de ces protocoles de preuves interactives fut étudiée dans les dix années qui suivirent leur introduction, culminant en une nouvelle définition de la classe NP, comme l'ensemble des langages admettant des preuves vérifiables de manière *efficace*.

Nous allons d'abord rappeler les principaux résultats concernant les systèmes de preuves interactives, puis nous en verrons une application à la *difficulté d'approximation*. Cette application nous a été utile dans le cadre d'un protocole de preuve interactive quantique à deux prouveurs pour le problème 3-DIMENSIONAL-MATCHING, et à travers lui pour la classe NP, dont nous n'avons pas eu le temps de terminer l'étude avant la soumission de ce rapport, mais qui est cependant brièvement discuté dans la partie 6.

3.1 Les théorèmes PCP

À la fin des années 80, Ben-Or, Goldwasser, Kilian et Wigderson [BOGKW88] généralisent la classe IP en introduisant les preuves interactives à plusieurs prouveurs : le vérifieur peut maintenant poser des question à un grand nombre de prouveurs, qui ne communiquent pas entre eux et n'ont pas accès aux échanges de messages qui ont lieu entre le vérifieur et les autres prouveurs.

Soient $P_1, \ldots, P_k$ des machines de Turing interactives de puissance de calcul non bornée, et V une machine de Turing interactive tournant en temps polynomial. Chaque P_i a un ruban de communication en écriture seule qui lui sert à envoyer des messages à V. V a k rubans en écriture seule qui lui servent à envoyer des messages aux P_i. On appelle $(P_1, \ldots, P_k, V)$ un *protocole interactif à* k *prouveurs*.

Définition 10 *Soient* $c, s : \mathbb{N} \to [0,1]$, $m : \mathbb{N} \to \mathbb{N}$ *des fonctions telles que* $s < c$ *et* $m \in poly$, *et* k *un entier. On note* $MIP_{c,s}(k, m)$ *la classe des langages* L *tels qu'il existe un protocole interactif à* k *prouveurs* $(P_1, \ldots, P_k, V)$ *vérifiant*

- *Pour tout* $x \in L$ *écrit sur le ruban d'entrée commun à* V *et aux* P_i, *après que* V *aie envoyé au plus* $m(|x|)$ *message à chaque* P_i, *et reçu leurs* $k \cdot m(|x|)$ *réponses,* V *accepte avec probabilité au moins* $c(|x|)$.
- *Pour tout* $x \notin L$ *et toute* k*-uplet de machines de Turing interactives* $(P_1, \ldots, P_k)$, V *accepte l'entrée* x *avec probabilité au plus* $s(|x|)$, *après avoir envoyé au plus* $m(|x|)$ *messages à chaque prouveur, et reçu leurs réponses.*

[BOGKW88] prouvent que l'on peut toujours se ramener à un protocole de preuve à deux prouveurs. Peu après l'introduction de ces systèmes de preuves interactives, leur puissance exceptionnelle, qui n'était pas du tout soupçonnée jusque là, est établie :

Théorème 11
[Sha92] $IP = PSACE$
[BFL91, FL92] $MIP = MIP(2,1) = NEXP$

Ainsi, tout langage dans NEXP peut être vérifié par une machine de Turing probabiliste en temps polynomial. L'introduction de l'interactivité apporte ainsi un gain de puissance

considérable. Dans le but de mieux comprendre les systèmes de preuves interactives, Arora et Safra (et d'autres avant eux) proposent de faire apparaître les *ressources* utilisées par un système de preuve interactive explicitement dans la définition de la classe de complexité. Ces ressources sont principalement la quantité d'aléas utilisée par le vérifieur, ainsi que le nombre de messages échangés, ou plus précisément le nombre de bits communiqués par l'ensemble des prouveurs au vérifieur. Ceci donne la définition de la classe de complexité PCP (pour probabilistically checkable proofs) :

Définition 12 *[AS92] Un système PCP est la donnée d'une machine de Turing probabiliste en temps polynomial (le vérifieur) ayant accès à un ruban spécial π (la preuve). Si r, q sont des fonctions de $\mathbb{N}$ dans $\mathbb{N}$, on dira qu'un vérifieur est (r,q)-restreint si, sur chaque entrée de longueur n, il utilise au plus $r(n)$ bits d'aléas, et lit au plus $q(n)$ bits de la preuve.*

Soient $c, s : \mathbb{N} \to [0,1]$ telles que $s < c$. La classe $PCP_{c,s}[r,q]$ consiste en l'ensemble des langages L pour lesquels il existe un vérifieur V (r,q)-restreint tel que

- *Pour tout $x \in L$, il existe une preuve π telle que $V(x)$ accepte π avec probabilité au moins $c(|x|)$.*
- *Pour tout $x \notin L$, et toute preuve π, $V(x)$ accepte π avec probabilité au plus $s(|x|)$.*

En faisant varier les paramètres r et q, on obtient un large éventail de classes de complexité : par exemple, trivialement $\mathrm{NP} = \mathrm{PCP}_{1,1/2}[0, poly(n)]$. $\mathrm{NEXP} = \mathrm{MIP}$ se réécrit également $\mathrm{NEXP} = \mathrm{PCP}_{1,1/2}[poly(n), poly(n)]$. En descendant ce résultat à NP, et après plusieurs améliorations successives, on aboutit au théorème PCP :

Théorème 13 *[AS92, ALM+92] $NP = PCP_{1,1/2}[O(\log n), O(1)]$.*

La constante sous-entendue par le $O(1)$ a par la suite été abaissée à 3, ce qui est optimal. Une machine de Turing probabiliste peut donc vérifier tout langage de NP en temps polynomial, en utilisant seulement un nombre logarithmique de bits d'aléas, et en utilisant cet aléas pour regarder seulement trois bits de la preuve.

3.2 Application à la difficulté d'approximation

Dans cette section, nous montrons comment le théorème PCP permet d'obtenir des résultats d'inapproximabilité de certains problèmes combinatoires, en nous concentrant sur l'exemple de 3-DIMENTIONAL-MATCHING (3DM). Nous commençons par décrire ce problème, puis nous donnons un théorème d'inapproximabilité le concernant.

Définition 14 *Une instance $3DM$ de taille n est la donnée de trois ensembles U, V, W de cardinalité n, et d'un sous-ensemble $M \subset U \times V \times W$. On dira qu'il s'agit d'une instance positive s'il existe deux bijections $\pi : U \to V$ et $\sigma : U \to W$ telles que*

$$\forall u \in U \qquad (u, \pi(u), \sigma(u)) \in M$$

Dans le cas contraire, on dira qu'il s'agit d'une instance négative.

Théorème 15 *[GJ79] Le problème $3DM$ est NP-complet.*

Démonstration. La preuve procède par réduction à partir de 3-SAT. Nous la décrivons brièvement car elle sevira à établir l'inapproximabilité. Soit φ une instance 3-SAT. On note $(\varphi_j)_{j=1,\dots,m}$ les clauses apparaissant dans φ, et $(x_i)_{i=1,\dots,n}$ les variables. La construction de l'intance 3DM correspondante se fait en trois étapes.

- On commence par introduire des variables $x_i[j], \neg x_i[j] \in U, a_i[j] \in V$ et $b_i[j] \in W$ pour tous (i,j) tels que soit x_i, soit $\neg x_i$ apparaisse dans φ_j. On insére les triplets $(x_i[j], a_i[j], b_i[j])$ et $(\neg x_i[j], a_i[j'], b_i[j])$ dans M, où j' est le premier indice $j' > j$ (modulo m) tel que x_i apparaisse dans $\varphi_{j'}$. Ces triplets sont des triplets d'*assignation de vérité.*
- Ensuite, pour chaque clause φ_j, on introduit des *variables de satisfaction* $c_1[j] \in V$ et $c_2[j] \in W$, et l'on insère tous les triplets $(x_i[j], c_1[j], c_2[j])$ ou $(\neg x_i[j], c_1[j], c_2[j])$ tels que respectivement x_i ou $\neg x_i$ apparaisse dans φ_j.
- Finalement, on introduit des *variables poubelle* $p_{i,k}[j] \in V$ et $q_{i,k}[j] \in W$, pour tout (i,j) tel que soit x_i, soit $\neg x_i$ apparaisse dans φ_j, et tout $k \in \{1,\dots,4\}$. On inclut alors tous les triplets $(x_l[j], p_{i,k}[j], q_{i,k}[j])$ et $(\neg x_l[j], p_{i,k}[j], q_{i,k}[j])$, pour k allant de 1 à 4, tels que soit x_l, soit $\neg x_l$ apparaisse dans φ_j.

Il n'est alors pas difficile de voir qu'une instance 3-SAT conduit à une instance 3DM positive si et seulement si la formule 3-SAT était satisfiable. L'idée est que tous les triplets correspondant aux $a_i[j]$ et $b_i[j]$ consistent à déterminer une assignation consistante des variables ; les triplets correspondant aux $c_1[j]$ et $c_2[j]$ garantissent que la clause φ_j est satisfiable, et finalement les variables poubelle servent essentiellement à ce que U, V et W aient même cardinalité.

Montrons à présent que ce problème admet un « fossé », c'est-à-dire qu'il est dur de faire la différence entre des instances positives, et des instances qui sont loin d'être positives. Commençons par montrer l'existence d'un fossé pour 3-SAT.

Définition 16 *On note ϵ-gap-3-SAT le problème suivant : étant donnée une formule 3-SAT, déterminer si toutes ses clauses sont simultanément satisfiables, ou bien si au plus une fraction $1-\epsilon$ de ses clauses sont simultanément satisfiables.*

Proposition 17 *Il existe un $\epsilon_1 > 0$ tel que ϵ_1-gap-3-SAT soit NP-complet.*

Démonstration. Ce problème est clairement dans NP. Pour montrer que tout problème s'y réduit, l'idée est d'utiliser un PCP pour NP. Soit donc $L \in$ NP et, selon le théorème 13, un vérifieur V utilisant $O(\log n)$ bit d'aléas, faisant un nombre constant q de requêtes à une preuve π, et tel que, si $x \in L$ alors il existe π tel que $V(x)$ accepte π avec certitude, alors que si $x \notin L$, pour toute preuve π, $V(x)$ accepte avec probabilité au plus $1/2$, c'est-à-dire qu'au moins la moitié de ses chaînes d'aléas le conduisent à rejeter π.

Pour chaque chaîne r de $O(\log n)$ bits d'aléas, le vérifieur regarde q bits $i_1,\dots,i_q$ de la preuve. Il prend alors sa décision en fonction de ces bits, c'est-à-dire qu'il calcule une fonction booléenne $f_{r,x} : \{0,1\}^q \to \{0,1\}$ et accepte si et seulement si $f_{r,x}(i_1,\dots,i_q) = 1$. On peut transformer $f_{r,x}$ de manière standard en un ensemble d'au plus 2^q clauses à 3 variables parmi $i_1,\dots,i_q$ telles que $f_{r,x}(i_1,\dots,i_q) = 1$ si et seulement si toutes ces clauses sont satisfiables. En procédant de cette manière, on obtient $2^{O(\log n)} \cdot 2^q = poly(n)$ clauses,

correspondant à toutes les chaînes d'aléas. Or, on sait que, si $x \in L$, il existe une preuve que $V(x)$ accepte avec probabilité 1. C'est-à-dire qu'il existe une assignation des variables i_k telle que toutes les clauses soient satisfaites. Par contre, si $x \notin L$, au plus la moitié des chaînes d'aléas r conduisent le vérifieur à accepter, et donc au moins la moitié des $f_{r,x}$ s'évaluent à 0, et au moins une des clauses correspondantes n'est pas satisfaite par l'assignation correspondant à π. Ainsi, en posant $\epsilon_1 = 1/2^{q+1}$, une fraction au plus $1 - \epsilon_1$ des $poly(n)$ clauses que l'on a obtenues sont simultanément satisfiables.

La valeur optimale pour ϵ est 1/8. Il n'est pas difficile de voir qu'une stratégie gloutonne, consistant à prendre les clauses une par une et à assigner les variables non encore déterminées de manière à satisfaire la clause si possible conduit à une assignation satisfaisant une fraction 7/8 des clauses en moyenne. On peut prouver que ceci est optimal en utilisant le PCP de Hastad [Hås01].

Le fossé que l'on a obtenu pour ϵ_1-gap-3-SAT s'étend à 3DM.

Définition 18 *On note ϵ-gap-3DM le problème suivant : étant donnée une instance (U, V, W, M) de 3DM, déterminer s'il s'agit d'une instance positive ou si, pour toutes bijections $\pi : U \to V$ et $\sigma : U \to W$, au plus une fraction $1 - \epsilon$ des triplets $(u, \pi(u), \sigma(u))$, pour $u \in U$, sont dans M.*

Proposition 19 *Il existe un $\epsilon_2 > 0$ tel que ϵ_2-gap-3DM soit NP-complet.*

Démonstration On réduit à partir de ϵ_1-gap-3-SAT. Posons $\epsilon_2 = \epsilon_1/6$. Supposons que l'on aie deux bijections π et σ telles qu'une fraction supérieure à $1 - \epsilon_2 = (6 - \epsilon_1)/6$ des triplets $(u, \pi(u), \sigma(u))$ soient dans M. Nous ignorons tous les triplets qui ne sont pas dans M. Comme on l'a vu lors de la réduction de 3-SAT à 3DM, un choix de triplets valides correspond à une assignation des variables. Ici, on obtient donc une assignation partielle, que l'on étend à toutes les variables x_i de manière arbitraire. On remarque que chaque $x_i[j]$ intervient dans au plus 6 triplets. Comme on a supposé qu'une fraction $(6-\epsilon_1)/6$ des triplets étaient valides, c'est qu'au moins une fraction $1 - \epsilon_1$ de ces triplets correspondent à des triplets de satisfaction. Les clauses qui apparaissent dans ces triplets sont toutes satisfaites par l'assignation que l'on a construite (car π et σ ont des bijections). On satisfait donc une fraction $1 - \epsilon_1$ des clauses, et donc l'instance ϵ_1-gap-3-SAT était positive, ce qui conclut la réduction.

4 Preuves interactives quantiques avec un seul prouveur

Nous présentons les principaux systèmes de preuves interactives quantiques avec un seul prouveur qui ont été étudiés jusqu'à présent, et nous en donnons les principales propriétés. Ceci nous permet de rappeler certains résultats fondamentaux concernant ces systèmes de preuves, que l'on réutilisera ensuite dans le cadre des systèmes à plusieurs prouveurs. Nous donnons également des problèmes complets pour chacune de ces classes, en les exprimant de manière cohérente, ce qui permet de voir leurs différences d'expressivité comme des changements de quantificateurs il existe/quel que soit dans les problèmes considérés.

4.1 La classe QIP

Les systèmes de preuves interactives quantiques ont été introduits en 1999 par A. Kitaev et J. Watrous [KW00], en analogie avec les systèmes de preuves interactives classiques. De manière informelle, un système de preuve interactif quantique est composé de deux parties : un vérifieur disposant d'un ordinateur quantique, et qui doit s'exécuter en temps polynomial, et un prouveur qui n'est limité que par les lois de la mécanique quantique. Le prouveur et le vérifieur communiquent à travers un canal quantique. Le but du prouveur est de convaincre le vérifieur de l'appartenance d'une entrée x commune à un langage L. Le vérifieur doit veiller à controler les informations que lui fournit le prouveur, car il ne peut faire confiance à ce dernier.

Formellement, un *vérifieur quantique* est une fonction $V : \Sigma^* \to \Sigma^*$ calculable en temps polynomial en la longueur de son entrée. Pour chaque $x \in \Sigma^*$, $V(x)$ est interprété comme un $k(|x|)$-tuple $(V_1(x), \ldots, V_{k(|x|)}(x))$, pour une certaine fonction k bornée par un polynôme. Pour chaque i, $V_i(x)$ est la description d'un circuit quantique agissant sur $q_V(|x|)+q_M(|x|)$ qubits, où q_V et q_M sont deux fonctions bornées par des polynômes. Les $q_V(|x|)$ premiers qubits sont interprétés comme l'espace propre du vérifieur, alors que les $q_M(|x|)$ autres constituent l'espace des messages. Finalement, le premier qubit de l'espace privé du vérifieur est désigné comme étant le qubit de sortie.

Un *prouveur quantique* est défini de manière analogue : c'est une fonction $P : \Sigma^* \to \Sigma^*$, sur laquelle on n'impose aucune restriction de calculabilité. Pour chaque $x \in \Sigma^*$, $P(x)$ est interprété comme un $l(|x|)$-tuple $(P_1(x), \ldots, P_{l(|x|)}(x))$, pour une certaine fonction l bornée par un polynôme. Pour chaque i, $P_i(x)$ est la description d'un circuit quantique agissant sur $q_P(|x|) + q_M(|x|)$ qubits, où q_M est une fonction bornée par un polynôme, mais il n'y a pas de restriction sur q_P. Les $q_P(|x|)$ premiers qubits sont interprétés comme l'espace propre du vérifieur, alors que les $q_M(|x|)$ autres constituent à nouveau l'espace des messages.

Un prouveur et un vérifieur quantiques seront dits *compatibles* si, pour toute entrée x, chaque $V_i(x)$ et $P_i(x)$ s'accordent sur le nombre de qubits de l'espace des messages, et si $k(|x|) = \lfloor m(|x|)/2 + 1 \rfloor$ et $l(|x|) = \lfloor m(|x|)/2 + 1/2 \rfloor$ pour une certaine fonction m, représentant le nombre de messages échangés. On dira dans ce cas que V est un vérifieur à m messages, et P un prouveur à m messages. Dans toute la suite, on suppose toujours que les couples formés d'un prouveur et d'un vérifieur que l'on considère sont compatibles.

Étant donnés un vérifieur V, un prouveur P, et une entrée x, on définit un circuit $(V,P)(x)$ agissant sur $q(|x|) = q_V(|x|) + q_M(|x|) + q_P(|x|)$ qubits de la façon suivante. Si $m(|x|)$ est impair, les circuits

$$P_1(x),\, V_1(x), \ldots,\, P_{(m(|x|)+1)/2}(x),\, V_{(m(|x|)+1)/2}(x)$$

sont appliqués les uns à la suite des autres, soit aux $q_V(|x|) + q_M(|x|)$ qubits du vérifieur, soit aux $q_P(|x|) + q_M(|x|)$ du prouveur. Si $m(|x|)$ est pair, c'est le vérifieur qui applique le premier circuit : on exécute la séquence

$$V_1(x),\, P_1(x), \ldots,\, P_{m(|x|)/2}(x),\, V_{m(|x|)/2+1)}(x)$$

Finalement, pour une entrée x, la probabilité que le couple (V,P) accepte x est définie comme étant la probabilité d'obtenir $|1\rangle$ lors d'une mesure du qubit de sortie du vérifieur dans la base canonique $(|0\rangle, |1\rangle)$, après exécution du circuit $(V,P)(x)$ sur l'état initial $|0\rangle^{\otimes q(|x|)}$.

Nous pouvons à présent définir la classe de complexité QIP :

Définition 20 *Soient $m : \mathbb{N} \to \mathbb{N}$ et $c, s : \mathbb{N} \to [0,1]$ des fonctions telles que $s(n) < c(n)$ pour tout n. On note $QIP_{c,s}(m)$ la classe des langages L tels qu'il existe un vérifieur V à m messages tel que*

- *Il existe un prouveur P à m messages tel que, pour tout $x \in L$, $(V,P)(x)$ accepte avec probabilité au moins $c(|x|)$.*
- *Pour tout prouveur P à m messages, et tout $x \notin L$, $(V,P)(x)$ accepte avec probabilité au plus $s(|x|)$.*

On appelle c le paramètre de complétude du protocole, et s est son paramètre de correction. On notera de plus $QIP(m) = QIP_{1,\frac{1}{2}}(m)$ pour tout m.

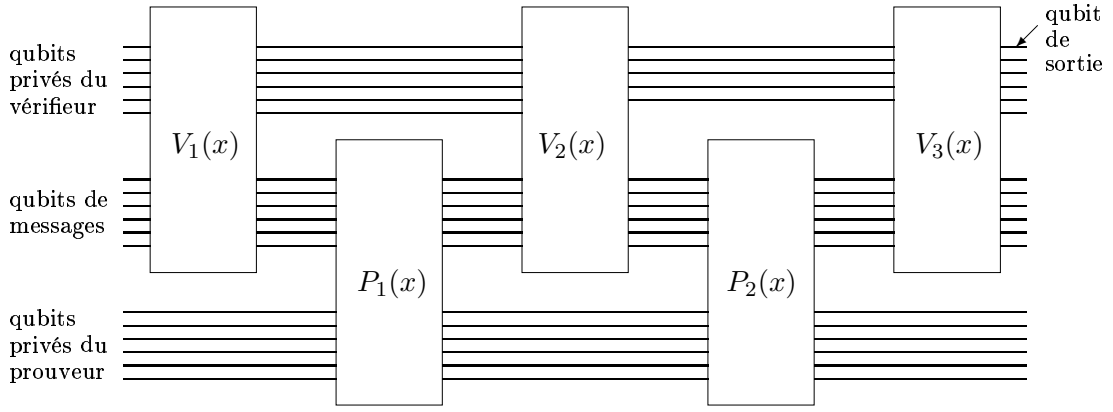

FIG. 2 – Schéma d'un système de preuve interactive quantique

La question naturelle que l'on se pose à propos des protocoles de preuves interactives quantiques est leur expressivité. En particulier, comment se compare-t-elle à celle de la classe de preuves interactives classiques IP ?

Nous remarquons que l'inclusion IP $\subset$ QIP n'est pas triviale. En effet, la traduction naturelle d'un protocole IP en un protocole QIP consiste pour le vérifieur à envoyer l'encodage des questions classiques qu'il aurait posées dans le protocole classique dans des états quantiques de la base canonique, et à systématiquement mesurer les réponses qu'il reçoit du prouveur dans la base canonique. Cependant, ceci n'empêche pas le prouveur d'enchevêtrer ses différentes réponses entre elles, et ainsi d'éventuellement piéger le vérifieur. Dans ce sens, Raz a prouvé un « théorème PCP quantique » [Raz05] qui montre essentiellement que la classe de complexité correspondant à des systèmes de preuves interactives à deux tours (quatre messages), où le premier tour est quantique et le deuxième classique, correspond à la classe NEXP, et est ainsi beaucoup plus puissante à la fois que la classe correspondant à deux tours classiques, puisque IP = PSPACE [Sha92], et que la classe correspondant à deux tours quantiques puisque, comme nous allons le voir, QIP $\subset$ EXP.

Cependant, Watrous a prouvé, en suivant la preuve classique, que PSPACE admettait un système de preuves interactives quantiques avec un nombre constant de messages [Wat99]. En termes de classes de complexité, les inclusions suivantes sont connues

Théorème 21 *[KW00], [Wat99]* $PSPACE \subset QIP_{1,\frac{1}{2}}(3) \subset EXP$

La preuve de la deuxième inclusion passe par l'utilisation de la *programmation semi-définie*. Dans un protocole de preuves interactives quantiques, l'action du prouveur, bien que computationellement illimitée, est régie par les lois de la mécanique quantique ; en particulier les circuits qu'il applique à chaque étape peuvent être décrits par des matrices unitaires, et l'état des ses registres est une matrice densité.

Soit (V_1, V_2) un vérifieur pour un protocole QIP à trois messages. On note V, M et P les registres respectivement du vérifieur, des messages et du prouveur, et $\mathcal{V}$, $\mathcal{M}$ et $\mathcal{P}$ les espaces de Hilbert correspondants. On note finalement q_{V}, q_{M} et q_{P} les nombres de qubits de chacun des trois registres. Définissons les opérateurs

$$T_1 : \begin{cases} D(\mathcal{M}) \longrightarrow D(\mathcal{V}) \\ \rho \quad \longmapsto \mathrm{Tr}_{\mathcal{M}}\left(V_1(|0^{q_{\mathsf{M}}}\rangle\langle 0^{q_{\mathsf{M}}}| \otimes \rho)V_1^*\right) \end{cases}$$

et

$$T_2 : \begin{cases} D(\mathcal{B}^{q_{\mathsf{V}}-1+q_{\mathsf{M}}}) \longrightarrow D(\mathcal{V}) \\ \rho \qquad\quad \longmapsto \mathrm{Tr}_{\mathcal{M}}\left(V_2^*(|1\rangle\langle 1| \otimes \rho)V_2\right) \end{cases}$$

Il est alors clair que l'existence d'un prouveur se faisant accepter avec probabilité 1 implique l'existence de deux matrices densité ρ_1 et ρ_2 telles que $T_1(\rho_1) = T_2(\rho_2)$. On montre réciproquement que, si la probabilité maximale pour un prouveur d'être accepté est inférieure à $1/2$, alors pour toutes matrices densité ρ_1 et ρ_2,

$$\|T_1(\rho_1) - T_2(\rho_2)\| \geq 2^{-q_{\mathsf{V}}-4}$$

À partir de là, il n'est pas difficile de se ramener à la résolution d'un problème de programmation semi-définie sur des matrices de taille exponentielle, tel que la détermination de la valeur de la solution optimale avec une précision exponentielle suffise à déterminer s'il existe un prouveur pouvant se faire accepter avec probabilité 1, ou si au contraire aucun prouveur

ne peut se faire accepter avec probabilité supérieure à 1/2. Comme on connaît des algorithmes polynomiaux de résolution des programmes semi-définis, on en déduit l'inclusion QIP(3) $\subset$ EXP.

La preuve de cette inclusion souligne le lien naturel entre preuves interactives quantiques et programmation semi-définie, lien qui naît des lois de la mécanique quantique : un état quantique est défini par une matrice densité, c'est-à-dire une matrice positive de trace 1. Nous donnerons à la partie 5.1.3 une application de ce lien dans le cadre des systèmes de preuves à plusieurs prouveurs, en les reliant à un algorithme d'approximation pour MAXCUT.

Nous terminons en donnant une propriété de réduction de l'erreur et du nombre de messages prouvées par Kitaev et Watrous lors de l'introduction de la classe QIP.

Proposition 22 *[KW00] Soient $k, p \in poly$, $\epsilon \in poly^{-1}$, et $c, s : \mathbb{N} \to [0,1]$ telles que $\forall n \in \mathbb{N}, c(n) - s(n) \geq \epsilon(n)$. Alors $QIP_{c,s}(k) \subset QIP_{1,2^{-p}}(3)$.*

4.2 Protocoles Arthur-Merlin quantiques

Les jeux de type Arthur-Merlin, introduits par Babai [Bab85] dans le cas classique puis par Marriott et Watrous [MW04] dans le cas quantique, constituent une classe restreinte de preuves interactives, dans laquelle le résultat des tirages aléatoires effectués par Arthur est public. Arthur désigne le vérifieur, et Merlin le prouveur. Comme Merlin est tout-puissant, et connaît les choix aléatoires effectués par Arthur au fur et à mesure que celui-ci les fait, il n'est pas nécessaire à Arthur d'envoyer de messages à Merlin ; Merlin peut les déterminer lui-même en se basant sur l'aléas public. Nous nous intéressons plus particulièrement ici aux deux classes de complexité suivantes.

Définition 23 *On note $QMA_{c,s}$ l'ensemble des langages admettant un système de preuve quantique de type Arthur-Merlin à un seul message, de paramètres de complétude c et correction s.*

On note $QMAM_{c,s}$ l'ensemble des langages admettant un système de preuve quantique de type Arthur-Merlin à trois messages, de paramètres de complétude c et correction s.

Les protocoles du type QMA consistent simplement en la donnée d'un circuit V pour le vérifieur, à appliquer sur le message qui lui est envoyé par Merlin, consistué d'un état quantique pur. QMA est ainsi un analogue quantique naturel de la classe NP.

NP est la classe des langages admettant une preuve de longueur polynomiale, vérifiable en temps polynomial. La question de savoir si deux preuves pourraient nous être plus utiles qu'une seule ne se pose pas, puisque il suffirait de juxtaposer les deux preuves en une seule, dont la longueur resterait polyomiale. Cependant, avec des preuves quantiques, les choses ne sont pas si simples : deux états quantiques peuvent être plus utiles qu'un seul, car, dans le cas où l'on a deux Merlins, l'on sait que chacun des deux nous envoie un état pur ; alors que dans le cas d'un seul prouveur, il nous est impossible de savoir si la preuve qui nous est donnée se décompose bien en un produit tensoriel $|\Psi_1\rangle \otimes |\Psi_2\rangle$. Dans la partie suivante nous nous intéressons aux protocoles de preuves interactives à plusieurs prouveurs et, en

anticipant un peu, nous allons présenter ici un argument justifiant que 3 prouveurs (et donc k prouveurs pour $k \geq 3$) ne sont pas plus utiles que deux, selon [KMY03]. La question de savoir si deux prouveurs sont plus utiles qu'un seul reste une question ouverte (cf la section 6).

4.2.1 L'algorithme C-SWAP

Nous commençons par décrire un algorithme important dans le cadre de la vérification des systèmes de preuves quantiques, le test C-SWAP. Nous réutiliserons à plusieurs reprises cet algorithme dans les protocoles à deux prouveurs de la prochaine section.

Algorithme C-SWAP
On suppose que l'on dispose de trois registres quantiques B, R_1 et R_2. B contient un unique qubit dans l'état $|0\rangle$, alors que R_1 et R_2 contiennent respectivement les matrices densité sur n qubits ρ et σ. L'algorithme procède comme suit :

1. Appliquer la transformation de Hadamard H à B.
2. Utiliser B comme qubit de contrôle pour échanger R_1 et R_2 : si B est dans l'état $|1\rangle$, alors échanger les contenus de R_1 et de R_2, et ne rien faire si B est dans l'état $|0\rangle$.
3. Appliquer la transformation de Hadamard à B. Mesurer B dans la base canonique, et accepter si le résultat est $|0\rangle$.

L'utilité de cet algorithme provient du lemme suivant.

Lemme 24 *La probabilité que la paire de matrices densité (ρ, σ) soit acceptée par l'algorithme C-SWAP est exactement* $1/2 + \mathrm{Tr}\,(\rho\sigma)/2$.

Démonstration. La preuve n'est pas difficile. Nous la donnons dans le cas où ρ et σ sont des états purs, cas auquel on se ramène dans le cas de matrices densité quelconques. Supposons donc que ρ et σ soient de la forme

$$\rho = |\varphi\rangle\langle\varphi| \qquad \text{et} \qquad \sigma = |\Psi\rangle\langle\Psi|$$

Au début de l'algorithme, les registres B, R_1 et R_2 sont dans l'état $|0\rangle|\varphi\rangle|\Psi\rangle$. Après exécution de la première transformation de Hadamard et de l'échange controlé, cet état devient

$$\frac{1}{\sqrt{2}}\big(|0\rangle|\varphi\rangle|\Psi\rangle + |1\rangle|\Psi\rangle|\varphi\rangle\big)$$

Puis on applique à nouveau une transformation de Hadamard. En regroupant les termes en fonction du premier qubit, l'état total est alors

$$\frac{1}{2}\Big(|0\rangle\big(|\varphi\rangle|\Psi\rangle + |\Psi\rangle|\varphi\rangle\big) + |1\rangle\big(|\varphi\rangle|\Psi\rangle - |\Psi\rangle|\varphi\rangle\big)\Big)$$

La probabilité de mesurer le premier qubit dans l'état $|0\rangle$ est donné par

$$\begin{aligned} P(0) &= \frac{1}{4}\||\varphi\rangle|\Psi\rangle + |\Psi\rangle|\varphi\rangle\|^2 \\ &= \frac{1}{2} + \frac{1}{2}|\langle\varphi|\Psi\rangle|^2 \end{aligned}$$

Or $\mathrm{Tr}\,(\rho\,\sigma) = |\langle\varphi|\Psi\rangle|^2$, ce qui prouve le lemme dans le cas des états purs.

La preuve de ce lemme montre que, dans le cas d'états purs, la probabilité de succès de l'algorithme C-SWAP est liée au produit scalaire $|\langle\varphi|\Psi\rangle|^2$: si les états $|\varphi\rangle$ et $|\Psi\rangle$ sont identiques, alors le test accepte avec probabilité 1, alors que si ces états sont orthogonaux sa probabilité de succès n'est que de $1/2$. Le test C-SWAP est donc un test qui nous permet de déterminer la proximité de deux états.

Considérons à présent un langage L dont l'appartenance puisse être prouvée par un protocole de type Arthur-Merlin, à un message et trois prouveurs. Soit $x \in \Sigma^*$, et V le vérifieur correspondant. On est dans l'un des deux cas suivants :

1. Soit il existe trois états $|\Psi_1\rangle$, $|\Psi_2\rangle$ et $|\Psi_3\rangle$ tels que V accepte avec probabilité au moins c sur l'entrée $|\Psi_1\rangle \otimes |\Psi_2\rangle \otimes |\Psi_3\rangle$: c'est le cas $x \in L$.
2. Soit, pour tout triplet d'états $|\Psi_1\rangle$, $|\Psi_2\rangle$ et $|\Psi_3\rangle$, V accepte avec probabilité au plus s sur l'entrée $|\Psi_1\rangle \otimes |\Psi_2\rangle \otimes |\Psi_3\rangle$: c'est le cas $x \notin L$.

Nous voulons prouver que L peut être reconnu par un protocole à seulement deux prouveurs. Construisons un nouveau vérifieur V' à partir de V. V' a comme registre de travail le même registre V que V, plus un registre B constitué d'un seul qubit initialisé dans l'état $|0\rangle$.

1. V' reçoit deux états $|D_1\rangle$ dans les registres R_1, S_1 et $|D_2\rangle$ dans les registres R_2, S_2.
2. V' effectue chacun des deux tests suivants avec probabilité $1/2$:
   (a) Test de séparabilité. Appliquer l'algorithme C-SWAP aux trois registres B, S_1 et S_2.
   (b) Test de consistance. Appliquer V aux registres V, R_1, R_2 et S_1. Accepter si V aurait accepté.

La complétude de ce protocole est simple à voir : si les états $|\Psi_1\rangle$, $|\Psi_2\rangle$ et $|\Psi_3\rangle$ correspondaient à une stratégie optimale des prouveurs dans le protocole à trois prouveurs, alors ici si le premier prouveur envoie l'état $|\Psi_1\rangle \otimes |\Psi_3\rangle$ et le deuxième prouveur envoie $|\Psi_2\rangle \otimes |\Psi_3\rangle$, leur probabilité de succès est $c' = (1 + c)/2$, puisqu'ils passent le test de séparabilité avec probabilité 1.

La correction est plus délicate, et nous ne donnons pas l'argument complet ici (cf. [KMY03]). L'idée est que, si les deux états envoyés par les prouveurs passent le test de séparabilité, c'est qu'ils sont proches (en fidélité) d'états du type $|\Psi_1\rangle\otimes|\Psi_3\rangle$ et $|\Psi_2\rangle\otimes|\Psi_3\rangle$. S'ils passent le test de consistance, c'est que les trois états $|\Psi_1\rangle$, $|\Psi_2\rangle$ et $|\Psi_3\rangle$ correspondaient à une stratégie des prouveurs qui aurait été acceptée par le protocole à 3 prouveurs. Or ceci n'est possible qu'avec probabilité au plus s, et l'on en déduit la correction du protocole.

4.2.2 Lien avec QIP

Classiquement, les liens entre les protocoles de type Arthur-Merlin et les protocoles de preuves interactives (à aléas privés) sont les suivants.

Théorème 25 *Pour toute fonction $m : \mathbb{N} \to \mathbb{N}$ à croissance au plus polynomiale, on note $AM(m)$ la classe des langages admettant un système de preuves interactives du type Arthur-Merlin dans lequel Arthur et Merlin échangent $m(|x|)$ messages sur l'entrée x. Alors :*

- *[Bab85] $AM(m) = AM(2)$*
- *[GS86] $IP(k) \subset AM(m+2) \subset IP(m+2)$.*

Nous présentons ici un résultat analogue dans le cas quantique, qui montre que l'expressivité des protocoles Arthur-Merlin à trois messages est la même que celle des protocoles de preuves interactives quantiques avec trois messages. Ainsi, si un langage admet un système de preuves QIP, on peut supposer que l'aléas utilisé par le vérifieur dans ce système est public.

Théorème 26 *[MW04] QMAM=QIP*

Démonstration. Soit $L \in \mathrm{QIP}_{1,2^{-n}}(3)$, et soit V le vérifieur correspondant, donné par les deux transformations unitaires V_1 et V_2. Le protocole QMAM pour L est le suivant.

1. Recevoir un registre V de la part de Merlin.
2. Jeter une pièce au hasard, et envoyer le résultat à Merlin.
3. Recevoir un registre M de la part de Merlin. Si la pièce de l'étape précédente était tombée sur pile, appliquer V_2 à (V, M) et accepter si et seulement si le résultat d'une mesure du qubit de sortie donne $|1\rangle$. Si la pièce était tombée sur face, appliquer V_1^* à (V, M) et accepter si et seulement si tous les qubits de V sont dans l'état $|0\rangle$.

Il est facile de voir que ce protocole est correct : Arthur vérifie que Merlin est bien capable de faire passer ses registres d'un état correspondant à l'état initial à un état acceptant. Le point clef est que Arthur possède le registre V dès le départ, et donc l'état de ce registre est indépendant du jeter de pièce qui est effectué à la deuxième étape du protocole.

4.3 Preuves zero-knowledge

La classe des langages admettant des systèmes de preuves interatives quantiques zero-knowledge constitue un intermédiaire intéressant entre les classes QMA et QIP. Nous nous intéressons ici à la classe QSZK des langages admettant une preuve zero-knowledge statistique, introduite par J. Watrous [Wat02]. Intuitivement, on dira qu'un protocole du type QIP est zero-knowledge statistique si la "vue" qu'a le vérifieur à chacune des étapes de l'exécution du protocole (ie la matrice densité décrivant l'état du registre privé du vérifieur et de celui des messages) peut être générée par un circuit calculable en temps polynomial (le "simulateur"), avec une précision (mesurée par la norme trace) arbitrairement grande. Ainsi, le prouveur ne donne aucune information au vérifieur, puisque ce dernier aurait aussi bien pu générer lui-même la "vue" qu'il a du protocole.

Étant donnée une collection $\{\rho_y\}$ de matrices densité de tailles k_y, on dira que cette collection est *préparable en temps polynomial* s'il existe une famille de circuits quantiques $\{Q_y\}$ de type (n_y, k_y) uniformément générée en temps polynomial telle que, pour tout y, $\rho_y = Q_y|0\rangle$.

Étant donnés un vérifieur V et un prouveur P, on définit $\text{vue}_{V,P}(x,j)$ comme la matrice densité décrivant l'état réduit du vérifieur et du registre de messages après que j messages aient été échangés lors de l'exécution du protocole (V,P) sur l'entrée x.

Définition 27 *Soient V un vérifieur et P un prouveur quantiques. On dit que (V,P) est un* système de preuves interactives quantique zero-knowledge statistique *pour le langage L si*

- *(V,P) est un système de preuves interactives quantiques pour L, et*
- *il existe un ensemble $\{\sigma_{x,j}\}$ de matrices densité préparables en temps polynomial, et une fonction δ décroissant plus vite que l'inverse de tout polynôme, tels que*

$$\|\sigma_{x,j} - vue_{V,P}(x,j)\|_{tr} < \delta(|x|)$$

pour tout $x \in L$ et tout message j.

Définition 28 *On définit la classe $QSZK_{c,s}$ comme l'ensemble des langages admettant un système de preuves interactives quantiques zero-knowledge statistique, tels que le système de preuves interactives quantique sous-jacent aie une correction s et une complétude c.*

Nous citons le théorème suivant, qui permet de situer QSZK par rapport à QIP. Sa preuve découle immédiatement du problème complet pour QSZK décrit dans la section suivante.

Théorème 29 *[Wat02] Tout langage admettant une preuve zero-knowledge statistique admet un système de preuves interactives quantiques avec seulement deux messages. On peut de plus supposer que l'aléas est public, et donc ce langage admet un système de preuves Arthur-Merlin quantique avec deux messages.*

4.4 Problèmes complets

Nous décrivons dans cette section des problèmes complets pour chacune des classes de complexité que nous avons introduites dans les sections précédentes, en donnant à chaque fois une idée des raisons pour lesquelles ces problèmes sont complets. Ils nous seront utiles dans la section suivante, où l'on prouve certaines inclusions entre classes de complexité. On peut également remarquer que les trois problèmes proposés ici sont de natures très proches : il s'agit à chaque fois de distinguer des états produits par des circuits quantiques, mais avec des restrictions différentes. Les différences d'expressivité de chacune des classes considérées sont ainsi nettement visibles.

4.4.1 QMA

[JWB03] Identity check. Soit x la description classique d'un circuit quantique U_x de complexité polynômiale en $|x|$, et $0 \leq \mu < \delta \leq 1$ tels que $\delta - \mu$ décroisse moins vite que l'inverse d'un polynôme. Il s'agit de décider si U_x est proche de la transformation triviale :

Entrée :	Le circuit U_x.
Oui :	Pour tout $\phi \in [0, 2\pi[$, $\|U_x - e^{i\phi}\,\mathrm{Id}\,\| \geq \delta$.
Non :	Il existe un angle $\phi \in [0, 2\pi[$ tel que $\|U_x - e^{i\phi}\,\mathrm{Id}\,\| \leq \mu$.

Les instances positives correspondent aux unitaires ayant au moins une valeur prore très différente de $e^{i\phi}$, et ce pour tout ϕ, ce qui revient à dire que U_x a deux valeurs propres très différentes. Les instances négatives correspondent à des unitaires ayant toutes leurs valeurs propres proches de $e^{i\phi}$ pour un certain ϕ, donc toutes proches les unes des autres. Dans le premier cas, si l'on dispose de vecteurs propres correspondant à deux valeurs propres différentes (ils nous sont donnés par Merlin), alors on peut utiliser la procédure standard d'*estimation de phase* pour estimer les valeurs propres correspondantes et vérifier qu'elles sont distinctes. Dans le deuxième cas, ceci est impossible. Le problème "Identity check" est donc dans QMA.

La complétude est un peu plus difficile. Le cadre général pour QMA est la donnée d'un circuit quantique U, et il s'agit de déterminer s'il existe un vecteur $|\Psi\rangle$ tel que l'état $U(|\Psi\rangle \otimes |0\dots0\rangle)$ soit tel que son premier qubit (le qubit de sortie) aie une grande probabilité d'être dans l'état $|1\rangle$. L'idée consiste à construire un circuit $Z = U^*VU$, où V est l'application d'une phase ϕ sur un qubit auxiliaire, controlé par le qubit de sortie de U. On vérifie alors que Z est loin de $e^{i\phi}\,\mathrm{Id}$ pour tout ϕ si U avait de grandes probabilités d'accepter, et proche d'un $e^{i\phi}\,\mathrm{Id}$ dans le cas contraire.

4.4.2 QSZK

[Wat02] Quantum State Distinguishability. Soient $0 \leq \alpha < \beta^2 \leq 1$[1].

Entrée :	Deux circuits Q_0 et Q_1 de même type (m, k).
Oui :	$\|(Q_0 - Q_1)\|0\rangle\|_{tr} \geq \beta$.
Non :	$\|(Q_0 - Q_1)\|0\rangle\|_{tr} \leq \alpha$.

Il y a un protocole quantique interactif simple pour ce problème : le vérifieur prépare au hasard $Q_0|0\rangle$ ou $Q_1|0\rangle$, et envoie la matrice densité correspondante au prouveur. Il attend en réponse du prouveur un unique bit. Il accepte si et seulement si ce bit correspond au circuit qu'il avait exécuté. Ce protocole n'est cependant pas zero-knowledge, car le simulateur ne peut prédire le bit renvoyé par le prouveur qu'avec probabilité $1/2(1 - \beta + \alpha)$. On modifie donc le protocole ci-dessus : à partir des circuits Q_0 et Q_1 le vérifieur commence par calculer deux circuits R_0 et R_1 tels que

$$\|(Q_0 - Q_1)|0\rangle\|_{tr} \geq \beta \implies \|(R_0 - R_1)|0\rangle\|_{tr} \geq 1 - 2^{-n}$$

et

$$\|(Q_0 - Q_1)|0\rangle\|_{tr} \leq \alpha \implies \|(R_0 - R_1)|0\rangle\|_{tr} \leq 2^{-n}$$

ce qui peut se faire en temps polynomial, l'idée étant de combiner deux type de répétition parallèle des circuits Q_0 et Q_1.

Le vérifieur exécute alors le protocole ci-dessus avec les circuits R_0 et R_1 jouant le rôle de Q_0 et de Q_1. Le simulateur a à présent une probabilité exponentiellement faible de se tromper, et le protocole est zero-knowledge.

La complétude est plus difficile, nous en donnons simplement l'intuition. Il s'agit en fait du même type de preuve que l'on rencontre lors de l'étude des protocoles zero-knowledge

[1] Le β^2, a priori surprenant, permet d'amplifier le « gap » $\beta - \alpha$: voir plus bas.

classiques. Soit L un langage admettant un système de preuves interactives quantiques zero-knowledge, et soit V le vérifieur correspondant. Comme le protocole est zero-knowledge, c'est qu'il existe un simulateur quantique produisant des matrices densité $\rho_0, \ldots, \rho_{k-1}$ et $\sigma_1, \ldots, \sigma_k$, où ρ_i désigne l'état des qubits des registres du vérifieur et des messages juste avant que le prouveur aie effectué la transformation P_i, et σ_i désigne l'état de ces mêmes registres juste après l'action du prouveur. On peut donc calculer, en temps polynomial en la longueur de l'entrée x, deux circuits Q_0 et Q_1 vérifiant

$$Q_0|0\rangle = \rho_1 \otimes \ldots \otimes \rho_{k-1} \qquad \text{et} \qquad Q_1|0\rangle = \sigma_1 \otimes \ldots \otimes \sigma_{k-1}$$

L'idée est alors que, si ces deux états sont proches (pour la norme trace), c'est qu'il existe un prouveur qui correspond aux états du simulateur, et donc que l'entrée x devrait être acceptée, par correction du simulateur. Si ces deux états sont très loin, c'est que la sortie du simulateur correspond à une séquence de transformations impossibles à réaliser physiquement, et donc que l'entrée x devrait être rejetée.

4.4.3 QIP

[RW05] Images proches. Soient $c, s \in [0,1]$ tels que $s < c$. On définit le problème à promesse $CI_{c,s}$ de la manière suivante :

Entrée :	Deux circuits quantiques (Q_0,Q_1) de même type (n, m).
Oui :	Il existe deux états mixtes sur n qubits ρ_0 et ρ_1 tels que $F(Q_0(\rho_0), Q_1(\rho_1)) \geq c$
Non :	Pour tous les états mixtes sur n qubits ρ_0 et ρ_1, $F(Q_0(\rho_0), Q_1(\rho_1)) \leq s$

Donnons un protocole de preuve interactive quantique à 3 messages pour ce problème. Le prouveur commence par envoyer la matrice densité ρ_0 au vérifieur, qui lui applique le circuit Q_0. Il envoie alors au prouveur les qubits qui ne sont *pas* désignés comme des qubits de sortie dans le circuit Q_0. Le prouveur applique une transformation, et renvoie le registre de messages au vérifieur, qui applique finalement Q_1^* sur ses registres, et vérifie que les qubits auxiliaires utilisés par le circuit Q_1 sont bien tous dans l'état $|0\rangle$.

Dans le cas où il existe une matrice de densité ρ_1 telle que $F(Q_0(\rho_0), Q_1(\rho_1)) \geq c$, par définition de la fidélité le prouveur peut, en agissant uniquement sur les qubits qui ne sont pas les qubits de sortie des circuits, transormer $Q_0(\rho_0)$ en un état qui aie fidélité au moins c avec $Q_1(\rho_1)$. Ce prouveur est accepté avec probabilité c.

Dans le cas où $F(Q_0(\rho_0), Q_1(\rho_1)) \leq s$ pour tous ρ_0 et ρ_1, une transformation laissant invariants les qubits de sortie transforme $Q_0(\rho_0)$ en un état qui est loin de $Q_1(\rho_1)$ pour tout ρ_1, et qui a donc une probabilité au plus s de remettre les qubits auxiliaires dans l'état $|0\rangle$ après application de Q_1^*.

La complétude de ce problème pour QIP découle de la preuve de QIP $\subset$ EXP de [KW00]. Soit (V_1, V_2) le vérifieur d'un protocole QIP(3) pour un langage L. L'idée est que le circuit Q_0 va désigner la première action V_1 du vérifieur, et le circuit Q_1 va désigner l'inverse de sa deuxième action V_2^*. Ainsi, $Q_0(\rho_0)$ désigne l'état du registre du vérifieur juste avant l'action du prouveur, et $Q_1(\rho_1)$ l'état de ce même registre juste après l'action

du prouveur. Le fait que ces états aient grande fidélité signifie que le prouveur peut nous faire passer de l'un à l'autre, et donc qu'il existe un prouveur qui se fait accepter avec grande probabilité.

5 Preuves interactives quantiques avec plusieurs prouveurs

De la même manière que la classe QIP a été introduite sur le modèle de la classe IP, il est naturel de considérer une extension quantique de MIP. La généralisation la plus simple consiste à autoriser le vérifieur et les prouveurs à posséder des machines quantiques, et à communiquer avec le vérifieur par l'intermédiaire d'un canal quantique - mais en interdisant toujours toute forme de communication entre les prouveurs. La classe correspondante, QMIP, a été introduite par Kobayashi et Matsumoto en 2001 [KM03]. Comme dans le cas de QIP, il n'y a pas de relation a priori entre MIP et QMIP. Cependant, on a vu (théorème 11) que MIP(m,k) = MIP(2,1), c'est-à-dire que la puissance des protocoles classiques s'exprime pleinement si l'on restreint le nombre de prouveurs à deux, et si le vérifieur pose au plus une question à chacun d'entre eux. Or, l'on peut simuler un protocole classique à deux messages par un protocole quantique à deux messages sans difficulté : dans ce cas, le fait d'être quantique n'est d'aucune utilité au prouveur, et donc MIP = MIP(2,1) $\subset$ QMIP.

De NEXP = MIP on tire alors immédiatement NEXP $\subset$ QMIP. Pour voir que l'inclusion réciproque est vraie, il suffit de vérifier que toute stratégie des prouveurs peut être implémentée en utilisant un espace au plus égal à deux fois l'espace réservé aux messages, qui est borné par un polynôme. Il est alors possible de deviner les unitaires appliquées par chacun des prouveurs, et de calculer leur probabilité de succès (qui s'exprime simplement comme la trace d'un opérateur de taille exponentielle) en espace réduit. C'est ce que font Matsumoto et Kobayashi dans [KM03], prouvant QMIP = NEXP, et ainsi QMIP = MIP.

Classiquement, on peut imaginer un relâchement de l'hypothèse de non-communication entre les prouveurs, en les autorisant à partager une source d'aléas public. En effet, on sait qu'en complexité de la communication, le partage d'aléas peut avoir un effet important : par exemple, le calcul de l'égalité a une complexité de communication de $O(1)$ bits dans le modèle avec aléas partagé, alors que sans aléas partagé il nécéssite $\Omega(\sqrt{n})$ bits de communication. Cependant, dans le cadre des systèmes de preuves interactifs, on voit facilement que le fait de partager de l'aléas n'est d'aucune utilité aux prouveurs : si c'était le cas, c'est qu'il existerait une chaîne d'aléas telle que, si les prouveurs partagent cette chaîne, alors leur probabilité (sur les actions du vérifieur) de gain serait supérieure à celle qu'ils auraient sans partager de chaîne. Mais, comme les prouveurs sont tout-puissants et peuvent communiquer avant que le protocole ne commence, ils peuvent déterminer la chaîne d'aléas qui maximise leurs chances de succès à l'avance, et utiliser cette chaîne. Ainsi, le fait de supposer qu'ils partagent de l'aléas ne modifie en rien leur capacité à convaincre le vérifieur.

De manière analogue, les lois de la mécanique quantique nous permettent de relâcher de manière intéressante l'hypothèse de non-communication entre les prouveurs en les autori-

sant à partager de l'enchevêtrement. Dans ce cas, l'argument de convexité donné ci-dessus ne marche plus, car chacun des prouveurs peut agir sur sa partie de l'enchevêtrement en fonction des questions qu'il reçoit du vérifieur, obtenant des résultats corrélés entre eux de manière non-déterministe. L'expressivité de cette nouvelle classe, notée QMIP*, n'est pas claire : d'une part, l'enchevêtrement peut permettre aux deux prouveurs de tricher, en coordonnant leurs réponses, et ainsi réduire l'expressivité de QMIP* par rapport à celle de QMIP. D'autre part, ce même enchevêtrement peut permettre au vérifieur d'être plus exigeant par rapport aux prouveurs, et ainsi peut-être résoudre des problèmes plus complexes. La position de QMIP* par rapport à celle de NEXP n'est donc pas du tout évidente a priori.

Dans le but d'étudier l'expressivité de ce nouveau modèle de preuves interactives, nous allons considérer plusieurs modèles réduits, en imposant des limitations sur les communications entre le vérifieur et le prouveur, et sur la nature des réponses du prouveur. Classiquement, la situation est claire, puisque, même si les réponses des prouveurs sont limitées à 1 bit, et si le vérifieur ne base sa décision que sur le XOR des deux bits qu'il reçoit en réponse à ses questions, l'expressivité reste égale à NEXP [CHTW04]. En fait, le résultat original, basé sur un PCP de Hastad [Hås01] avec une complexité en questions très faible, montre que la classe des langages admettant un système de preuve interactif comme celui que l'on vient de décrire, avec la restriction supplémentaire que la longueur totale des messages échangés soit logarithmique, est NP. Il est souvent admis dans la littérature que les résultats sur les PCPs s'étendent à NEXP, avec des augmentations en quantité d'aléas et en nombre de questions appropriées, cependant ceci n'est pas toujours immédiat.

5.1 $\oplus$MIP$^*(2)$

La classe $\oplus$MIP$^*(2)$ a été introduite dans [CHTW04]. Il s'agit de la classe à deux prouveurs quantiques la plus simple qui soit : le vérifieur pose une question (classique) à chacun des deux prouveurs, qui répondent par un seul bit. Le vérifieur prend sa décision en se basant uniquement sur le XOR des deux bits qu'il a reçus. Nous commençons par décrire cette classe, puis nous donnons un exemple de protocole démontrant le rôle de l'enchevêtrement dans les systèmes de preuves à plusieurs prouveurs, et enfin nous présentons un théorème de Tsirelson qui nous permet de montrer l'inclusion $\oplus$MIP$^*(2) \subset$ EXP, en suivant la preuve de S. Wehner [Weh06].

Soient S et T deux ensembles finis, π une distribution de probabilités sur $S \times T$ et V une fonction de $S \times T$ dans $\{0,1\}$, appelée *fonction de valuation*. Alors π et V définissent un jeu non local de la manière suivante : une paire de questions $(s,t) \in S \times T$ est choisie de manière aléatoire suivant la distribution π. s est envoyé au joueur 1 (que l'on nommera Aurélie dans toute la suite) et t est envoyé au joueur 2 (prénommé Benoît). Chacun des deux joueurs doit renvoyer un bit $a, b \in \{0,1\}$ en réponse. Aurélie et Benoît ne peuvent pas communiquer une fois que le jeu a commencé, mais ils peuvent se mettre d'accord sur une stratégie *a priori*. Ils gagnent le jeu si et seulement si $a \oplus b = V(s,t)$.

On note $\omega_c(G)$ la valeur classique d'un tel jeu, c'est-à-dire la probabilité maximale avec laquelle les deux joueurs peuvent gagner :

$$\omega_c(G) = \max_{a,b} \sum_{(s,t)\in S\times T} \pi(s,t)\left(1 \oplus a(s) \oplus b(t) \oplus V(s,t)\right)$$

où le maximum est pris sur toutes les fonctions $a, b : S \times T \to \{0,1\}$.

Considèrons à présent des prouveurs quantiques autorisés à partager de l'enchevêtrement. Aurélie et Benoît se rencontrent avant que le jeu ne commence, et créent un état quantique $|\Psi\rangle$ biparti enchevêtré dont ils gardent chacun la moitié des qubits. Pour chaque question $s \in S$, Aurélie dispose d'une mesure projective $X_s = X_s^0 - X_s^1$ sur sa partie de l'état $|\Psi\rangle$. De même, Benoît dispose de mesures projectives $Y_t = Y_t^0 - Y_t^1$ pour chaque question $t \in T$. Lorsqu'ils reçoivent leur question, les deux joueurs effectuent la mesure correspondante sur leur partie de l'état $|\Psi\rangle$. La probabilité de répondre (a,b) à la question (s,t) est ainsi donnée par

$$P(a,b|s,t) = \langle\Psi|X_s^a \otimes Y_t^b|\Psi\rangle$$

On définit la valeur quantique du jeu G par

$$\omega_q(G) = \max_{X_s,Y_t} \sum_{(s,t)\in S\times T} \pi(s,t) \sum_{a,b\in\{0,1\}} \left(1 \oplus a \oplus b \oplus V(s,t)\right) \langle\Psi|X_s^a \otimes Y_t^b|\Psi\rangle$$

où le maximum est pris sur toutes les collections de mesures projectives $\{X_s, Y_t\}_{(s,t)\in S\times T}$. Posons

$$\tau(G) = \frac{1}{2} \sum_{(s,t)\in S\times T} \sum_{c\in\{0,1\}} \pi(s,t)\left(c \oplus 1 \oplus V(s,t)\right)$$

C'est la valeur de la stratégie triviale consistant à répondre 0 ou 1 avec probabilité $1/2$. En regroupant les couples a et b ayant le même XOR, on obtient alors l'expression équivalente suivante pour $\omega_q(G)$:

$$\omega_q(G) = \tau(G) + \frac{1}{2} \max_{X_s,Y_t} \sum_{(s,t)\in S\times T} \pi(s,t)\,(-1)^{V(s,t)} \langle\Psi|X_s \otimes Y_t|\Psi\rangle \tag{1}$$

Définition 30 *On dira qu'un jeu G est un jeu $\oplus MIP^*(2)$ s'il est du type décrit ci-dessus.*

5.1.1 Un exemple : l'inégalité CHSH

Dans un article intitulé "On the Einstein Podolsky Rosen paradox", publié en 1964, J.S. Bell prouve que, si l'on admet la validité du *principe des causes locales*, et indépendemment de toute théorie physique, il existe une borne supérieure sur les corrélations d'évènements distants. Le principe des causes locales affirme que des évènements ayant lieu dans une certaine région de l'espace-temps sont indépendants de paramètres externes qui pourraient être contrôlés, au même instant, par des agents situés dans une région distante de l'espace-temps. La preuve de Bell du fait que ce principe est incompatible avec la mécanique quantique et été qualifiée de "plus profonde découverte de la science" (H.P. Stapp, 1975).

Le théorème de Bell s'applique à tout système physique ayant des variables binaires, dont les valeurs sont arbitrairement notées 1 et -1. Une version plus générale de ce théorème, appelée l'inégalité CHSH, a été démontré par J.F. Clauser, M. Horne, A. Shimony et R.A. Holt.

Théorème 31 *[CHSH69] Supposons la validité du principe des causes locales. Soit une paire de photons émis dans des directions opposées. Deux observateurs distants testent la polarisation linéaire du photon qu'ils ont reçu. Chacun a le choix entre deux tests, suivant deux angles distincts, chaque test ayant un résultat* 1 *ou* -1*. On note* a *et* c *les variables aléatoires donnant le résultat des deux tests du premier observateur, et* b *et* d *celles du deuxième observateur. Alors*

$$|\langle ab\rangle + \langle bc\rangle + \langle cd\rangle - \langle da\rangle| \leq 2 \qquad \textit{(CHSH)}$$

où $\langle x\rangle$ *désigne la valeur moyenne de la variable aléatoire* x*.*

Nous allons donner une interprétation de la violation de cette inégalité par les lois de la mécanique quantique dans le cadre des jeux à deux joueurs.

Soient $S = T = \{0,1\}$, π la distribution uniforme sur $S \times T$ et V la fonction de valuation définie par

$$\forall (s,t) \in S \times T \qquad V(s,t) = s \wedge t$$

Si les deux joueurs Aurélie et Benoît ne partagent pas d'enchevêtrement, on peut décrire leur comportement par quatre variables aléatoires $a(0), a(1)$ correspondant aux réponses d'Aurélie aux questions 0 et 1 respectivement, et $b(0)$, $b(1)$ correspondant aux réponses de Benoît aux questions 0 et 1. Les variables aléatoires $(-1)^{a(0)}$, $(-1)^{a(1)}$, $(-1)^{b(0)}$ et $(-1)^{b(1)}$ satisfont les hypothèses de l'inégalité CHSH, et donc

$$|\langle (-1)^{a(0)+b(0)}\rangle + \langle (-1)^{a(0)+b(1)}\rangle + \langle (-1)^{a(1)+b(0)}\rangle - \langle (-1)^{a(1)+b(1)}\rangle| \leq 2$$

Or, la valeur classique de G est donnée par

$$\begin{aligned} \omega_c(G) &= \max_{a,b} \sum_{(s,t)\in\{0,1\}^2} \frac{1}{4}\big(1 \oplus a(s) \oplus b(t) \oplus (s \wedge t)\big) \\ &= \frac{1}{2} - \frac{1}{8} \max_{a,b} \big((-1)^{a(0)+b(0)} + (-1)^{a(0)+b(1)} + (-1)^{a(1)+b(0)} - (-1)^{a(1)+b(1)}\big) \end{aligned}$$

On obtient ainsi $$\omega_c(G) \leq \frac{3}{4}$$

et l'on vérifie aisément qu'il existe une stratégie classique déterministe permettant de gagner avec probabilité $3/4$.

La preuve du fait que la théorie de la mécanique quantique n'admettait pas de modèle à variables aléatoires locales cachées est passée par la vérification expérimentale de la violation de l'inégalité CHSH par des variables aléatoires résultant de tests de polarisation effectués sur des paires de photons corrélés. En utilisant ce fait, nous pouvons décrire une stratégie quantique ayant une probabilité de succès strictement supérieure à celle de la meilleure stratégie classique.

Soit $$|\Psi\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

l'état enchevêtré partagé par Aurélie et Benoît. Définissons

$$\begin{aligned} |\varphi_0(\theta)\rangle &= \cos\theta|0\rangle + \sin\theta|1\rangle \\ |\varphi_1(\theta)\rangle &= -\sin\theta|0\rangle + \cos\theta|1\rangle \end{aligned}$$

Les mesures d'Aurélie et de Benoît sont alors données par

$$\begin{aligned} X_0^a &= |\varphi_a(0)\rangle\langle\varphi_a(0)| \\ X_1^a &= |\varphi_a(\pi/4)\rangle\langle\varphi_a(\pi/4)| \\ Y_0^b &= |\varphi_b(\pi/8)\rangle\langle\varphi_b(\pi/8)| \\ Y_1^b &= |\varphi_b(-\pi/8)\rangle\langle\varphi_b(-\pi/8)| \end{aligned}$$

pour $a, b \in \{0,1\}$. Étant donné notre choix de $|\Psi\rangle$, on a

$$\langle\Psi|X \otimes Y|\Psi\rangle = \frac{1}{2}\,\mathrm{Tr}\,\left({}^tX\,Y\right)$$

pour tous X et Y. On vérifie alors aisément que, dans tous les cas, la bonne réponse est donnée avec probabilité $\cos^2(\pi/8) \simeq 0.85 > 3/4$, et la mauvaise réponse est donnée avec probabilité $\sin^2(\pi/8)$.

5.1.2 Le théorème de Tsirelson

Nous donnons dans cette section une preuve simple d'un théorème de Tsirelson qui va nous permettre de relier la valeur quantique d'un jeu G du type $\oplus\mathrm{MIP}^*(2)$ à une maximisation sur des produits scalaires de vecteurs réels en grande dimension.

Théorème 32 *(Tsirelson [Tsi80]) Soient S et T des ensembles finis, et soit $|\Psi\rangle$ un état quantique pur de support inclus dans un espace de Hilbert biparti $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$ pour lequel $\dim\mathcal{A} = \dim\mathcal{B} = n$. Pour chaque $s \in S$ soit X_s une observable sur $\mathcal{A}$ de valeurs propres ±1, et pour chaque $t \in T$, soit Y_t une observable sur $\mathcal{B}$ de valeurs propres ±1. Alors il existe des vecteurs réels unitaires x_s and y_t de $\mathbb{R}^{2n^2}$ tels que $\langle\Psi|X_s \otimes Y_t|\Psi\rangle = x_s \cdot y_t$, pour tous $s \in S$ et $t \in T$.*

Réciproquement, soient S et T des ensembles finis, et x_s et y_t des vecteurs unitaires de $\mathbb{R}^N$ pour tous $s \in S$ et $t \in T$. Soient $\mathcal{A}$ et $\mathcal{B}$ des espaces de Hilbert de dimension $2^{\lceil N/2\rceil}$, $\mathcal{H} = \mathcal{A} \otimes \mathcal{B}$, et soit $|\Psi\rangle$ un état enchevêtré quelconque de $\mathcal{H}$. Alors il existe des observables X_s sur $\mathcal{A}$ et Y_t sur $\mathcal{B}$ de valeurs propres ±1 telles que $\langle\Psi|X_s \otimes Y_t|\Psi\rangle = x_s \cdot y_t$, pour tous $s \in S$ et $t \in T$.

Démonstration.

1. Pour tous s, t, soit $x_s = X_s \otimes I|\Psi\rangle$ et $y_t = I \otimes Y_t|\Psi\rangle$. Comme X_s, Y_t ont ±1 pour seules valeurs propres, et $|\Psi\rangle$ est normé, x_s et y_t sont de norme 1, et

$$\forall (s,t) \in S \times T \qquad x_s \cdot y_t = \langle\Psi|X_s \otimes I \cdot I \otimes Y_t|\Psi\rangle = \langle\Psi|X_s \otimes Y_t|\Psi\rangle$$

2. Nous prouvons ce sens dans un cadre légèrement restreint : nous supposons que

$$|\Psi\rangle = |\Psi_N\rangle = |\Psi_1\rangle^{\otimes N} \qquad \text{où} \qquad |\Psi_1\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

est une paire EPR. Nous allons utiliser certaines propriétés des matrices de Pauli

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \qquad \text{et} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Nous commençons par quelques observations simples.

(a) $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathrm{Id}$

(b) $\sigma_x\sigma_y = -\sigma_y\sigma_x$, $\sigma_x\sigma_z = -\sigma_x\sigma_z$ et $\sigma_z\sigma_y = -\sigma_y\sigma_z$

(c) $\sigma_x \otimes \sigma_x|\Psi_1\rangle = \sigma_y \otimes \sigma_y|\Psi_1\rangle = \sigma_z \otimes \sigma_z|\Psi_1\rangle = |\Psi_1\rangle$

(d) $\sigma_x \otimes \sigma_y|\Psi_1\rangle$, $\sigma_x \otimes \sigma_z|\Psi_1\rangle$ et $\sigma_y \otimes \sigma_z|\Psi_1\rangle$ sont tous orthogonaux à $|\Psi_1\rangle$.

Soient maintenant $x = (x_1, x_2, x_3)$ et $y = (y_1, y_2, y_3)$ deux vecteurs de $\mathbb{R}^3$ unitaires, et posons

$$X = x_1\,\sigma_x + x_2\,\sigma_y + x_3\,\sigma_z \qquad \text{et} \qquad Y = y_1\,\sigma_x + y_2\,\sigma_y + y_3\,\sigma_z$$

Les quatre observations ci-dessus montrent que X et Y sont des matrices hermitiennes de carré l'identité, donc des observables à valeurs propres dans $\{\pm 1\}$. De plus, on vérifie facilement que

$$\langle\Psi_1|X \otimes Y|\Psi_1\rangle = x_1y_1 + x_2y_2 + x_3y_3 = x \cdot y$$

Il nous reste à montrer comment cette construction se généralise en de plus grandes dimensions. Pour tout $k \in \{1, \ldots, \lceil N/2\rceil\}$, soient

$$X_{2k} = I_2^{\otimes k} \otimes \sigma_x \otimes \sigma_z^{\otimes \lceil N/2\rceil - k - 1} \qquad \text{et} \qquad X_{2k-1} = I_2^{\otimes k} \otimes \sigma_y \otimes \sigma_z^{\otimes \lceil N/2\rceil - k - 1}$$

Nous avons ainsi défini une collection de N matrices hermitiennes sur $\lceil N/2\rceil$ qubits, de carré égal à l'identité et qui anticommutent. Posons $x_s = (x_s^1, \ldots, x_s^N)$ et $y_t = (y_t^1, \ldots, y_t^N)$. En utilisant de plus le fait que, si $i \neq j$, alors $X_i \otimes X_j|\Psi_N\rangle$ est orthogonal à $|\Psi_N\rangle$, il n'est pas difficile de voir qu'en posant

$$X_s = \sum_{i=1}^{N} x_s^i\, X_i \qquad \text{et} \qquad Y_t = \sum_{i=1}^{N} y_t^i\, Y_i$$

X_s et Y_t sont bien des observables sur $\lceil N/2\rceil$ qubits, à valeurs propres dans $\{\pm 1\}$, et elles vérifient

$$\forall (s,t) \in S \times T \qquad \langle\Psi_N|X_s \otimes Y_t|\Psi_N\rangle = \sum_{i=1}^{N} x_s^i\, y_t^i = x_s \cdot y_t$$

Étant donné un jeu G à deux joueurs partageant de l'enchevêtrement, ce théorème nous permet d'exprimer de manière simplifiée la valeur du gain maximal à ce jeu, en réécrivant l'expression (1) :

$$\omega_q(G) = \tau(G) + \frac{1}{2} \max_{x_s, y_t} \sum_{s,t} \pi(s,t)(-1)^{V(s,t)} x_s \cdot y_t \tag{2}$$

où la maximisation se fait sur tous les vecteurs $x_s, y_t \in \mathbb{R}^{\min(|S|,|T|)}$. On voit alors apparaître une connexion naturelle avec les problèmes de programmation semi-définie.

Définition 33 *$\oplus MIP^*_{c,s}(2)$ désigne l'ensemble des langages L tels que, pour tout mot x de longueur n, il existe un jeu à deux joueurs G_x, calculable en temps polynomial en n, tel que*

- *Si $x \in L$, alors $\omega_q(G_x) \geq c(|x|)$.*
- *Si $x \in L$, alors $\omega_q(G_x) \leq s(|x|)$.*

L'expression (2) implique l'inclusion $\oplus\mathrm{MIP}^*(2) \subset \mathrm{EXP}$. En fait, S. Wehner a montré l'inclusion plus précise

Théorème 34 *[Weh06] Pour tous $c, s : \mathbb{N} \to [0,1]$ tels que $0 \leq s < c \leq 1$,*

$$\oplus MIP^*_{c,s}(2) \subset QIP_{c,s}(2)$$

Idée de la preuve. Soit $L \in \oplus\mathrm{MIP}^*_{c,s}(2)$, et, pour tout $x \in \Sigma^*$, G_x le jeu correspondant. À partir de G_x nous allons définir un vérifieur $V(x)$ tel que le protocole $\mathrm{QIP}(2)$ correspondant aie les mêmes paramètres de correction et de complétude que ceux de G_x. G_x est donné par des ensembles de questions S et T, une distribution de probabilités π sur $S \times T$, et une fonction de valuation V.

Le vérifieur $V(x)$ commence par tirer un couple $(s,t) \in S \times T$ au hasard selon la distribution π, puis il prépare l'état $|0\rangle|0,s\rangle + |1\rangle|1,t\rangle$, où le premier qubit correspond au registre privé V du vérifieur, et les autres au registre des messages M. Le vérifieur envoie le registre M au prouveur, qui effectue une certaine transformation et le lui renvoie. Enfin, le vérifieur effectue la mesure

$$\begin{cases} P_0 & = |\Psi^+_{st}\rangle\langle\Psi^+_{st}| \\ P_1 & = |\Psi^-_{st}\rangle\langle\Psi^-_{st}| \\ P_2 & = \mathrm{Id} - P_0 - P_1 \end{cases}$$

où $|\Psi^\pm_{st}\rangle = |0\rangle|0,s\rangle \pm |1\rangle|1,t\rangle$, sur les registres V et M. S'il obtient un bit $c \in \{0,1\}$, il prend la décision qu'il aurait prise dans le protocole initial, sinon il rejette immédiatement.

En supposant que le prouveur effectue une transformation arbitraire, en la décomposant sur le registre M et sur son registre privé P, et en calculant la probabilité maximale de succès du prouveur face au vérifieur $V(x)$, on obtient une expression en tout point semblable à (2), avec la même maximisation sur des vecteurs unitaires, qui correspondent ici à l'état de l'espace privé du prouveur. Ainsi, la probabilité maximale de succès d'un prouveur au jeu G_x est la même que la probabilité maximale de succès d'un prouveur face à $V(x)$, ce qui prouve le théorème.

On observe finalement qu'une stratégie optimale pour le prouveur consiste simplement à mettre une phase $(-1)^{a(s)}$ sur l'état $|0,s\rangle$ et $(-1)^{b(t)}$ sur l'état $|1,t\rangle$, où $a(s)$ et $b(t)$ sont les réponses données à la question (s,t) par des prouveurs optimaux pour le jeu G_x.

5.1.3 MAXCUT

Nous avons vu dans la section précédente, à travers le théorème de Tsirelson, qu'il y avait un lien naturel entre systèmes de preuves interactifs et programmation semi-définie. Dans cette partie nous allons prouver l'existence d'une connexion précise entre l'algorithme d'approximation pour MAXCUT et un système de preuve naturel du type $\oplus\mathrm{MIP}^*(2)$ pour

ce même problème. Cette connexion est nouvelle, et nous pensons que les sytèmes de preuves interactifs quantiques peuvent fournir un cadre simple pour l'expression d'algorithmes d'approximation, permettant peut-être de trouver de meilleurs algorithmes pour certains problèmes. En effet, un protocole naturel dans le formalisme quantique peut se traduire en un algorithme d'approximation fastidieux lorsqu'il est exprimé en termes de maximisation de matrices positives.

Soit $G = (V, E)$ un graphe non orienté. On note

$$\text{MAXCUT}(G) = \max_{W \subset V} (W \times (V \backslash W)) \cap E$$

Le problème d'optimisation consistant à calculer MAXCUT(G) pour un graphe G de taille $n = |V|$ est NP-complet. Goemans et Williamson ont montré dans un article célèbre [GW95] que l'ont pouvait déterminer une valeur approchée (à un facteur $\alpha \simeq 0.878$ près) de MAXCUT(G) en temps polynomial randomisé, en faisant recours à la programmation semi-définie. Leur approche consiste à exprimer la taille de la coupe maximale de G comme le maximum d'un programme quadratique sur les entiers, puis à considérer une relaxation de ce programme, en autorisant les variables à être des vecteurs de $\mathbb{R}^n$. La relaxation est un programme semi-défini et se résoud en temps polynomial. Une solution approchée est alors obtenue en projetant les vecteurs obtenus sur un espace aléatoire de dimension 1.

Après de nombreuses tentatives pour améliorer la constante d'approximation α, Khot, Kindler, Mossel et O'Donnell [KKMO04] ont finalement montré en 2005 que, si la conjecture Unique Games était vraie, alors pour tout $\epsilon > 0$ il était impossible d'approcher MAXCUT(G) à un facteur $\alpha + \epsilon$ près.

Nous allons retrouver la même constante d'approximation que Goemans et Williamson à partir d'un protocole de preuve interactive à deux prouveurs pour MAXCUT(G). L'idée est que le vérifieur va tirer une arête du graphe au hasard, et, soit envoyer chacun des deux sommets la constituant à chacun des deux prouveurs, soit envoyer le même sommet aux deux prouveurs. Le but pour les prouveurs sera de renvoyer une réponse différente s'ils ont reçu deux noeuds différents, et une réponse identique s'ils ont reçu le même noeud. Si le protocole était classique, une stratégie optimale pour les prouveurs serait de se mettre d'accord à l'avance sur une coupe maximale, et d'attribuer des 1 à tous les sommets de la coupe, des 0 aux autres. Cependant, dans le cas où l'on autorise les prouveurs à partager de l'enchevêtrement, ils peuvent tenter d'utiliser cet enchevêtrement pour coordonner leurs réponses. Nous allons voir ci-dessous que la marge de manoeuvre qui leur est permise par l'enchevêtrement leur permet de tricher d'un facteur exactement égal à celui de l'algorithme d'approximation de Goemans et Williamson.

Nous commençons par décrire le protocole $\oplus\text{MIP}^*(2)$ pur MAXCUT que nous considérons, puis nous prouvons sa correction.

Soit $m = |E|$. Pour $i \in V$ on note Δ_i le degré du noeud i, et $\Delta = \Sigma_i \Delta_i$ le degré total de G. Définissons une mesure de probabilité sur $V^2 = \{1, \ldots, n\}^2$ par

$$\forall (i,j) \in \{1,\dots,n\}^2 \qquad \pi(i,j) = \begin{cases} \dfrac{1}{\Delta+m} & \text{si } (i,j) \in E \\ \dfrac{\Delta_i}{\Delta+m} & \text{si } i=j \in V \\ 0 & \text{sinon} \end{cases}$$

On considère un vérifieur qui prend les décisions suivantes

$$\forall (i,j) \in \{1,\dots,n\}^2 \qquad V(i,j) = \begin{cases} 1 & \text{si } i \neq j \\ 0 & \text{si } i = j \end{cases}$$

Ce choix est tel que

$$\tau(G) = \frac{1}{2} \sum_{(s,t)\in S\times T} \sum_{c\in\{0,1\}} \pi(s,t)\left(c \oplus 1 \oplus V(s,t)\right) = \frac{1}{2}$$

Soit $(X,Y) = (\{x_i\}_{i\in V}, \{y_i\}_{i\in V}) \in \mathbb{S}^n \times \mathbb{S}^n$ une stratégie quelconque des joueurs Aurélie et Benoît dans le protocole décrit ci-dessus, comme donnée par le théorème de Tsirelson. Soit

$$f(X,Y) = \frac{1}{2} + \frac{1}{2} \sum_{(i,j)\in\{1,\dots n\}^2} \pi(i,j)(-1)^{V(i,j)} x_i \cdot y_j$$

la probabilité de succès de cette stratégie, et soit X_0, Y_0 une stratégie optimale : $f(X_0,Y_0) = \max_{X,Y} f(X,Y)$. Nous allons montrer que, étant donné notre choix de poids $\pi(i,j)$ affectés à chacun des couples de sommets, la stratégie gagnante est une stratégie symétrique : on peut supposer que $X_0 = Y_0$. Comme f est bilinéaire symétrique,

$$\begin{aligned} \frac{1}{2}\Big(f(X,Y) \;+\; f(Y,X)\Big) - f\left(\frac{X+Y}{2}, \frac{X+Y}{2}\right) & \\ = \; \frac{1}{2(\Delta+m)} \sum_{i\in V} \Delta_i (x_i \cdot y_i - 1) & \\ + \frac{1}{4(\Delta+m)} \sum_{(i,j)\in E} \big(- x_i \cdot y_j - x_j \cdot y_i + x_i \cdot x_j + y_i \cdot y_j \big) & \\ = \; \frac{1}{4(\Delta+m)} \sum_{(i,j)\in V} \big(- 4 + 2x_i \cdot x_j + 2y_i \cdot y_j + (x_i - y_i)\cdot(x_j - y_j) \big) & \end{aligned}$$

Or, pour tous vecteurs unitaires, $2x_i \cdot y_i + 2x_j \cdot y_j + (x_i - y_i)\cdot(x_j - y_j) \leq 4$ (ceci peut se voir à l'aide d'un calcul de différentielle). Comme $f(X,Y) = f(Y,X)$, on obtient

$$f\left(\frac{X+Y}{2}, \frac{X+Y}{2}\right) \geq f(X,Y)$$

Comme le maximum de f sur les vecteurs unitaires est également son maximum sur la boule unité, on en déduit que le maximum de f est également atteint en $\big((X+Y)/2, (X+Y)/2\big)$, c'est-à-dire que l'on peut supposer que la stratégie gagnante est symétrique. Sa valeur est alors

$$f(X,X) = \frac{\Delta}{\Delta+m} - \sum_{(i,j)\in V} \pi(i,j)\, x_i \cdot x_j$$

Or, si $k = \text{MAXCUT}(G)$, Goemans et Williamson ont montré que

$$k \leq \max_{x_i, y_i \in \mathbb{S}^n} \frac{1}{2} \sum_{(i,j)\in V} (1 - x_i \cdot x_j) \leq \alpha \cdot k$$

ce qui donne ici, comme $\Delta = m/2$,

$$\frac{1}{3} + \frac{k}{3m} \leq \max_{X,Y} f(X,Y) \leq \frac{1}{3} + \frac{\alpha k}{3m}$$

Définissons le problème à promesse APPROX-MAXCUT(k, ϵ) :

Entrée : Un graphe $G = (V, E)$, un entier k et un réel $\epsilon > 0$.
Oui : $\frac{1}{|E|}\text{MAXCUT}(G) \geq k$.
Non : $\frac{1}{|E|}\text{MAXCUT}(G) \leq \frac{k}{\alpha} - \epsilon$.

Ce qui précède prouve le théorème suivant.

Théorème 35 *Pour tout entier k et tout réel $\epsilon > 0$,*

$$\textit{APPROX-MAXCUT}(k, \epsilon) \in \oplus \textit{MIP}^*_{c,s}(2)$$

où $c = (1 + k)/3$ et $s = (1 + k - \alpha\epsilon)/3$.

La probabilité de gagner à ce jeu $\oplus\text{MIP}^*(2)$ donne donc une approximation de la taille de la coupe maximale de G à un facteur α près. Dans le cas de MAXCUT, ceci est optimal. Cependant, nous espérons que dans le cadre d'autres problèmes, pour lesquels un algorithme d'approximation optimal n'est pas connu, cette approche puisse donner naissance à des algorithmes performants et innovants.

5.2 $\oplus$MIP avec des questions non nécessairement orthogonales

La classe $\oplus\text{MIP}^*(2)$ ne change pas si l'on considère que les deux prouveurs sont quantiques, et que le vérifieur leur envoie une question au choix parmi un ensemble fini d'états quantiques orthogonaux : les prouveurs peuvent mesurer l'état qui leur est envoyé et en déduire la question classique qui leur est posée. Par contre, la situation change si les états ne sont pas orthogonaux : dans ce cas, il est impossible de les différencier parfaitement.

Définition 36 *Un jeu $\oplus$qMIP* est la donnée de*
- *deux ensembles S, T,*
- *pour tous $s \in S$ et $t \in T$, des états purs $|\varphi_s\rangle$ et $|\varphi_t\rangle$ (les questions),*
- *une distribution de probabilités π sur $S \times T$,*
- *une fonction V de $S \times T$ dans $\{0, 1\}$: la fonction de valuation.*

Définition 37 *Soient $c, s : \mathbb{N} \to [0, 1]$ deux fonctions telles que $s(n) < c(n)$ pour tout n. La classe $\oplus$qMIP* contient l'ensemble des langages L tels que*
- *Pour tout $x \in L$, il existe un jeu G_x du type $\oplus$qMIP*, calculable à partir de x en temps polynomial en $|x|$, et deux prouveurs A et B pour ce jeu dont la probabilité de succès est au moins $c(|x|)$.*

– *Pour tout $x \notin L$, il existe un jeu G_x du type $\oplus$qMIP*, calculable à partir de x en temps polynomial en $|x|$, tel que la probabilité de succès de n'importe quel couple de prouveurs (A, B) à ce jeu soit inférieure à $s(|x|)$.*

Un jeu $\oplus$MIP$^*(2)$ est clairement un jeu $\oplus$qMIP*, mais l'inverse n'est pas vrai. Nous allons prouver que, malgré le potentiel gain de puissance accordé au vérifieur, qui peut essayer de piéger les prouveurs, l'inclusion suivante reste vraie :

Théorème 38 *$\oplus qMIP^*_{c,s} \subset QIP_{c,s}(2)$ pour tous paramètres de complétude et de correction c et s.*

Démonstration. La preuve de ce théorème se fait en trois étapes. Nous commençons par donner l'expression de la valeur (ie la probabilit maximale de succès de deux prouveurs) d'un jeu quantique G du type $\oplus$qMIP*, puis nous définissons un jeu G' pour QIP(2). Nous montrons ensuite que, si Aurélie et Benoît sont deux prouveurs pour G, alors il existe un prouveur Charles pour G' dont la probabilité de succès est exactement la même que celle du couple (Aurélie, Benoît) au jeu G. Nous montrons finalement la réciproque, c'est-à-dire que, si Charles est un prouveur pour G', alors il existe deux prouveurs pour G atteignant la même probabilité de succès. Ceci suffira à établir le théorème.

(i) Définition du jeu G'

Soient Aurélie et Benoît deux prouveurs pour le jeu G. Après réception de leur question quantique, ils appliquent chacun une mesure projective binaire, que l'on note respectivement $A = A_0 - A_1$ et $B = B_0 - B_1$, sur l'état qu'ils ont reçu, ainsi que sur leur registre propre, éventuellement enchevêtré avec celui de l'autre prouveur, et en déduisent leur réponse. On remarque par ailleurs que A et B sont des matrices hermitiennes à valeurs propres dans $\{\pm 1\}$, donc telles que $A^2 = B^2 = \mathrm{Id}$; comme $A^* = A$ et $B^* = B$ on en déduit que A et B sont également unitaires, et peuvent donc être vues comme des transformations quantiques plutôt que des mesures. Nous exploiterons ce fait en **(ii)**. Aurélie et Benoît partagent un état enchevêtré $|\Psi\rangle$ arbitraire ; étant données des questions $|\varphi_s\rangle$ et $|\varphi_t\rangle$, ils répondent (a, b) avec probabilité

$$P_G(a, b|s, t) = \langle \varphi_s \otimes \Psi \otimes \varphi_t | A_a \otimes B_b | \varphi_s \otimes \Psi \otimes \varphi_t \rangle$$

La valeur du jeu G pour les prouveurs Aurélie et Benoît est définie par

$$\omega_{A,B}(G) = \sum_{s,t,c} \pi(s, t) V(c|s, t) P_G(c|s, t)$$

où $P_G(0|s, t) = P_G(0, 0|s, t) + P_G(1, 1|s, t)$, $P_G(1|s, t) = P_G(0, 1|s, t) + P_G(1, 0|s, t)$ et $V(c|s, t) = c \oplus 1 \oplus V(s, t)$. On a ainsi

$$\begin{aligned} P_G(0|s, t) - P_G(1|s, t) &= \langle \varphi_s \otimes \Psi \otimes \varphi_t | (A_0 \otimes B_0 + A_1 \otimes B_1 \\ &\qquad - A_1 \otimes B_0 - A_0 \otimes B_1) | \varphi_s \otimes \Psi \otimes \varphi_t \rangle \\ &= \langle \varphi_s \otimes \Psi \otimes \varphi_t | A \otimes B | \varphi_s \otimes \Psi \otimes \varphi_t \rangle \end{aligned}$$

Comme $P_G(c|s, t) = \frac{1}{2}\big(1 + (-1)^c (P(0|s, t) - P(1|s, t))\big)$ (les probabilités somment à 1), la valeur de G est

$$\omega_{A,B}(G) = \frac{1}{2}\left(\sum_{s,t,c}\pi(s,t)V(c|s,t)\big(1+(-1)^c\langle\varphi_s\otimes\Psi\otimes\varphi_t|A\otimes B|\varphi_s\otimes\Psi\otimes\varphi_t\rangle\big)\right)$$

Définissons à présent un jeu G' pour QIP(2). Le vérifieur dispose de quatre registres quantiques V_1, V_2, M_1 et M_2. Les deux premiers sont ses registres privés et les deux derniers forment le registre de messages. Le vérifieur tire une question (s,t) au hasard suivant la distribution de probabilités π, et prépare ses quatre registres dans l'état

$$|0\rangle|\varphi_t\rangle|0\rangle|\varphi_s\rangle + |1\rangle|\varphi_s\rangle|1\rangle|\varphi_t\rangle$$

Il envoie alors les deux registres M_1 et M_2 au prouveur, qui effectue sa transformation, et lui renvoie les deux registres de messages. Le vérifieur effectue alors des échanges entre les différents registres en sa possession, en controllant sur l'état de son premier registre. Si ce premier registre est dans l'état $|0\rangle$, alors le vérifieur ordonne ses registres dans l'ordre $\mathsf{V}_1,\mathsf{M}_1,\mathsf{M}_2,\mathsf{V}_2$. S'il est dans l'état $|1\rangle$, alors le vérifieur ordonne ses registres dans l'ordre $\mathsf{V}_1,\mathsf{M}_1,\mathsf{V}_2,\mathsf{M}_2$. Le vérifieur mesure finalement ses deux premiers registres à l'aide de la mesure projective

$$\begin{cases} P_0 &= |\Psi^+\rangle\langle\Psi^+| \\ P_1 &= |\Psi^-\rangle\langle\Psi^-| \\ P_2 &= I - P_0 - P_1 \end{cases}$$

où $$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle \pm |11\rangle\big)$$

S'il obtient un résultat $c\in\{0,1\}$ alors il conclut que le XOR des deux bits dans le jeu G était c et il prend la décision correspondante, sinon il rejette immédiatement.

(ii) De G à G'

Dans cette section nous prouvons que, si Aurélie et Benoît sont deux prouveurs pour le jeu G, alors il existe un prouveur Charles pour G' tel que

$$\forall(s,t)\in S\times T \qquad P_G(0|s,t) - P_G(1|s,t) = P_{G'}(0|s,t) - P_{G'}(1|s,t)$$

Comme l'expression de $\omega(G)$ ne fait intervenir que $P_G(0|s,t) - P_G(1|s,t)$, ceci suffira à prouver l'inégalité $\omega(G')\geq\omega(G)$, où l'on définit $\omega(G')$ comme la probabilité maximale qu'a un prouveur de se faire accepter par le vérifieur du jeu G'. L'inégalité inverse sera prouvée en (**iii**).
Soient ainsi Aurélie et Benoît deux prouveurs pour G qui partagent un état $|\Psi\rangle$. Définissons un prouveur Charles pour G'. Charles reçoit les registres M_1 et M_2 de la part du vérifieur. Il possède un troisième registre P_1, qu'il initialise dans l'état $|\Psi\rangle$. Le prouveur a donc en sa possession les trois derniers registres de l'état total

$$|0\rangle|\varphi_t\rangle|0\rangle|\varphi_s\rangle|\Psi\rangle + |1\rangle|\varphi_s\rangle|1\rangle|\varphi_t\rangle|\Psi\rangle$$

En controlant sur le registre M_1, Charles applique les unitaires $A\otimes I$ et $B\otimes I$, où l'identité agit sur la partie de $|\Psi\rangle$ qui appartenait à l'autre prouveur. L'état total devient

$$|0\rangle|\varphi_t\rangle|0\rangle A\otimes I(|\varphi_s\rangle|\Psi\rangle) + |1\rangle|\varphi_s\rangle|1\rangle B\otimes I(|\varphi_t\rangle|\Psi\rangle)$$

Charles renvoie les registres M_1 et M_2 au vérifieur. Ce dernier effectue les échanges de registres que l'on a décrits ci-dessus, obtenant l'état

$$|\varphi\rangle = |0\rangle|0\rangle A \otimes I(|\varphi_s\rangle|\Psi\rangle|\varphi_t\rangle) + |1\rangle|1\rangle I \otimes B(|\varphi_s\rangle|\Psi\rangle|\varphi_t\rangle)$$

où l'identité a été étendue pour agir sur $|\varphi_t\rangle$ dans le premier cas, et $|\varphi_s\rangle$ dans le second. En mesurant dans la base $|\Psi^{\pm}\rangle$, le vérifieur obtient les résultats $0, 1$ avec probabilité

$$P_{G'}(0|s,t) = \langle\varphi|P_0|\varphi\rangle = \frac{1}{2}\big(1 + \langle\varphi_s \otimes \Psi \otimes \varphi_t|(A \otimes I) \cdot (I \otimes B)|\varphi_s \otimes \Psi \otimes \varphi_t\rangle\big)$$

(le 1 vient de $AA^* = BB^* = 1$) et

$$P_{G'}(1|s,t) = \langle\varphi|P_1|\varphi\rangle = \frac{1}{2}\big(1 - \langle\varphi_s \otimes \Psi \otimes \varphi_t|(A \otimes I) \cdot (I \otimes B)|\varphi_s \otimes \Psi \otimes \varphi_t\rangle\big)$$

Ainsi

$$P_{G'}(0|s,t) - P_{G'}(1|s,t) = \langle\varphi_s \otimes \Psi \otimes \varphi_t|A \otimes B|\varphi_s \otimes \Psi \otimes \varphi_t\rangle = P_G(0|s,t) - P_G(1|s,t)$$

ce qui établit ce sens de la preuve.

(iii) De G' à G

Réciproquement, nous prouvons dans cette section que, si Charles est un prouveur pour le jeu G', alors il existe des prouveurs Aurélie et Benoît pour G tels que

$$P_G(0|s,t) - P_G(1|s,t) = P_{G'}(0|s,t) - P_{G'}(1|s,t)$$

Soit Charles un prouveur pour le jeu G'. Commençons par évaluer la probabilité qu'a Charles d'être accepté par le vérifieur. En toute généralité, Charles applique une transformation unitaire C aux registres M_1 et M_2 qu'il reçoit du vérifieur, ainsi qu'à son registre propre P_1, initialisé à $|0\rangle^{\otimes p}$. Nous décrivons l'action de C de la manière suivante :

$$\begin{aligned} C|0\rangle|\varphi_s\rangle|0\rangle^{\otimes p} &= |0\rangle|\alpha_s^0\rangle + |1\rangle|\alpha_s^1\rangle \\ C|1\rangle|\varphi_t\rangle|0\rangle^{\otimes p} &= |0\rangle|\beta_t^0\rangle + |1\rangle|\beta_t^1\rangle \end{aligned}$$

Comme le vérifieur effectue des échanges de registres après avoir reçu la réponse du prouveur, nous allons devoir décomposer les états manipulés sur ces différents registres, ce qui complique un peu les notations. Nous pouvons supposer, sans perte de généralité, que $|\alpha_s^1\rangle = |\beta_t^0\rangle = 0$ puisque cette partie de l'état sera rejetée par le vérifieur : cela ne fait qu'augmenter les chances de succès du prouveur. Décomposons

$$|\alpha_s^0\rangle = \sum_i |i\rangle|\alpha_s^i\rangle \qquad \text{et} \qquad |\beta_t^1\rangle = \sum_i |i\rangle|\beta_t^i\rangle$$

où $\{|i\rangle\}$ est une base de l'espace engendré par les $\{|\varphi_s\rangle, |\varphi_t\rangle\}$, correspondant au registre M_2, et les $|\alpha_s^i\rangle, |\beta_t^i\rangle$ sont des vecteurs arbitraires (ni unitaires, ni orthogonaux), correspondant au registre P_1. Une telle décomposition peut s'obtenir à partir de la décomposition de Schmidt des états $|\alpha_s^0\rangle$ et $|\beta_t^1\rangle$. Le prouveur renvoie les registres M_1 et M_2 au vérifieur, qui effectue ses substitutions pour obtenir l'état

$$\sum_i \big(|0\rangle|0\rangle|i\rangle|\varphi_t\rangle|\alpha_s^i\rangle + |1\rangle|1\rangle|\varphi_s\rangle|i\rangle|\beta_t^i\rangle\big)$$

Il mesure et obtient le résultat 0 avec probabilité

$$P_{G'}(0|s,t) = \frac{1}{2}\big(1 + \sum_{i,j} \langle i|\varphi_s\rangle\langle\varphi_t|j\rangle\langle\alpha_s^i|\beta_t^j\rangle\big)$$

Définissons à présent deux prouveurs Aurélie et Benoît pour G. Aurélie et Benoît partagent un nombre de paires EPR égal à la dimension de l'espace engendré par les vecteurs $\{|\alpha_s^0\rangle, |\beta_t^1\rangle\}$, que l'on note $\Sigma_k |k\rangle \otimes |k\rangle$, où le premier $|k\rangle$ appartient à Aurélie et le deuxième à Benoît. Avant que le jeu ne commence, Aurélie et Benoît initialisent un certain nombre de registres à $|0\rangle$, copient (par XOR) leur $|k\rangle$ sur un autre registre, produisant l'état $\Sigma_k |k,k\rangle \otimes |k,k\rangle$, et préparent également un registre de la même dimension que celui contenant les $|k\rangle$ dans la superposition uniforme $\Sigma_j |j\rangle$. Avant de recevoir leurs questions de la part du prouveur, Aurélie et Benoôit sont ainsi dans l'état enchevêtré

$$\sum_{i,j,k} |0\rangle|0\rangle|0^p\rangle|i\rangle|k\rangle|i,k\rangle \otimes |0\rangle|1\rangle|0^p\rangle|j\rangle|k\rangle|j,k\rangle$$

Lorsqu'il reçoivent leur question du prouveur, ils la placent entre leurs deuxième et troisièmes registres, ce qui donne l'état

$$\sum_{i,j,k} |0\rangle|0\rangle|\varphi_s\rangle|0^p\rangle|i\rangle|k\rangle|i,k\rangle \otimes |0\rangle|1\rangle|\varphi_t\rangle|0^p\rangle|j\rangle|k\rangle|j,k\rangle$$

Aurélie et Benoît appliquent chacun une transformation de Hadamard sur leur premier qubit, puis appliquent C aux registres deux, trois et quatre, en controlant sur le premier registre. Ceci donne l'état

$$\sum_{i,j,k} \Big(|0\rangle|0\rangle|\varphi_s\rangle|0^p\rangle|i\rangle|k\rangle + |1\rangle|0\rangle|\alpha_s^0\rangle|i\rangle|k\rangle\Big)|i,k\rangle$$

$$\otimes\Big(|0\rangle|1\rangle|\varphi_t\rangle|0^p\rangle|j\rangle|k\rangle + |1\rangle|1\rangle|\beta_t^0\rangle|j\rangle|k\rangle\Big)|j,k\rangle$$

Puis, en controlant sur son premier qubit, Aurélie copie (XOR) son sixième registre sur son quatrième si ce qubit est dans l'état $|0\rangle$, et échange les registres trois et quatre avec les registres cinq et six si ce qubit est dans l'état $|1\rangle$. Benoît fait de même. Finalement, ils appliquent à nouveau une transformation de Hadamard sur leur premier qubit. Ils sont maintenant dans l'état

$$\sum_{i,j,k} \Big(|0\rangle\Big[|0\rangle|\varphi_s\rangle|k\rangle|i\rangle|k\rangle + |0\rangle|i\rangle|k\rangle|\alpha_s^0\rangle\Big] + |1\rangle\Big[|0\rangle|\varphi_s\rangle|k\rangle|i\rangle|k\rangle - |0\rangle|i\rangle|k\rangle|\alpha_s^0\rangle\Big]\Big)|i,k\rangle$$

$$\otimes\Big(|0\rangle\Big[|1\rangle|\varphi_t\rangle|k\rangle|j\rangle|k\rangle + |1\rangle|j\rangle|k\rangle|\beta_t^0\rangle\Big] + |1\rangle\Big[|1\rangle|\varphi_t\rangle|k\rangle|j\rangle|k\rangle - |1\rangle|j\rangle|k\rangle|\beta_t^0\rangle\Big]\Big)|j,k\rangle$$

Ils mesurent finalement leur premier qubit dans la base standard et envoient le résultat au vérifieur. La distribution de probabilités jointe sur leurs réponses vérifie

$$\begin{aligned} P_G(0,0|s,t) &= \sum_{i,j,k} \big(1 + \langle\varphi_s|i\rangle\langle\alpha_s^i|k\rangle\big)\big(1 + \langle\varphi_t|j\rangle\langle\beta_t^j|k\rangle\big) \\ P_G(1,1|s,t) &= \sum_{i,j,k} \big(1 - \langle\varphi_s|i\rangle\langle\alpha_s^i|k\rangle\big)\big(1 - \langle\varphi_t|j\rangle\langle\beta_t^j|k\rangle\big) \end{aligned}$$

Puisque pour tous i, j

$$\sum_k \langle\alpha_s^i|k\rangle\langle\beta_t^j|k\rangle = \langle\alpha_s^i|\beta_t^j\rangle$$

en sommant $P_G(0|s,t) = P_G(0,0|s,t) + P_G(1,1|s,t)$ on obtient, comme on le voulait,

$$P_G(0|s,t) - P_G(1|s,t) = P_{G'}(0|s,t) - P_{G'}(1|s,t)$$

5.3 $\oplus$MIP avec des matrices densité

Nous continuons à généraliser les systèmes de preuves quantiques considérés. Jusqu'à présent, le vérifieur envoyait une question, classique ou quantique, choisie parmi un ensemble prédéterminé, à chacun des deux prouveurs, mais ces questions correspondaient toujours à des états purs. Nous considérons maintenant le cas où les questions posées peuvent correspondre à des matrices densité, c'est-à-dire à des états qui restent enchevêtrés avec l'espace privé du vérifieur, ce qui permettra a priori au vérifieur d'avoir un plus grand contrôle sur les prouveurs. Formellement,

Définition 39 *Un jeu $\oplus$QMIP* est la donnée de*
- *deux ensembles S, T,*
- *pour tous $s \in S$ et $t \in T$, des matrices densité ρ_s et γ_t,*
- *une distribution de probabilités π sur $S \times T$,*
- *une fonction V de $S \times T$ dans $\{0,1\}$: la fonction de valuation.*

Définition 40 *Soient $c, s : \mathbb{N} \to [0,1]$ deux fonctions telles que $s(n) < c(n)$ pour tout n. La classe $\oplus$QMIP* contient l'ensemble des langages L tels que*
- *Pour tout $x \in L$, il existe un jeu G_x du type $\oplus$QMIP*, calculable à partir de x en temps polynomial en $|x|$, et deux prouveurs A et B pour ce jeu dont la probabilité de succès est au moins $c(|x|)$.*
- *Pour tout $x \notin L$, il existe un jeu G_x du type $\oplus$QMIP*, calculable à partir de x en temps polynomial en $|x|$, tel que la probabilité de succès de n'importe quel couple de prouveurs (A,B) à ce jeu soit inférieure à $s(|x|)$.*

En général, une matrice densité ρ_s se décompose en $\rho_s = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$, et il semblerait donc qu'un jeu $\oplus$QMIP* se réduise à un jeu $\oplus$qMIP*. En fait, ceci n'est pas le cas, car le nombre d'états $|\Psi_i\rangle$ apparaissant dans la décomposition ci-dessus peut être exponentiel en le nombre de qubits, et donc non calculable par le vérifieur. Le recours à des matrices densité permet donc d'une certaine manière au vérifieur de poser un nombre exponentiel de questions à la fois, et donc d'être beaucoup plus fin dans son analyse.

Le gain de puissance obtenu est difficile à évaluer. Nous pouvons montrer que la puissance du vérifieur dans ce type de protocole est au moins celle d'un vérifieur zero-knowledge.

Théorème 41 *$QSZK_{c,s} \subset \oplus QMIP^*_{1-2c(1-c),(1+s)/2}$ pour tous paramètres de complétude et de correction c et s vérifiant $(1+s)/2 < 1 - 2c(1-c)$.*

Démonstration. Il suffit de montrer que le problème QSD, complet pour QSZK d'après 3.4.2, est dans la classe $\oplus$QMIP*. Soient donc deux circuits quantiques Q_0 et Q_1 de même type (n,k) tels que, soit

$$\|(Q_0 - Q_1)|0\rangle\|_{tr} \geq c$$

soit $$\|(Q_0 - Q_1)|0\rangle\|_{tr} \leq s$$

Définissons un jeu $\oplus$QMIP* sur $S = T = \{0,1\}$ par

$$\forall (s,t) \in S \times T \qquad \pi(s,t) = \frac{1}{4} \quad \text{et} \quad V(s,t) = \{s \neq t\}$$

Les questions correspondantes sont $\rho_s = Q_s|0\rangle$ et $\gamma_t = Q_t|0\rangle$. Dans le cas où $\|(Q_0 - Q_1)|0\rangle\|_{tr} \geq c$, la stratégie des prouveurs consistant à effectuer une mesure permettant de distinguer $Q_0|0\rangle$ de $Q_1|0\rangle$ de manière optimale, et à renvoyer le résultat de cette mesure au prouveur produit la bonne réponse avec probabilité $c^2 + (1-c)^2 = 1 - 2c(1-c)$. Dans le cas où $\|(Q_0 - Q_1)|0\rangle\|_{tr} \leq s$, les prouveurs ne peuvent donner la bonne réponse avec probabilité plus grande que $(1+s)/2$, car ils ne peuvent répondre avec probabilité plus grande que s aux questions $(Q_0|0\rangle, Q_1|0\rangle)$ et $(Q_1|0\rangle, Q_0|0\rangle)$: sinon ils pourraient être utilisés pour distinguer $Q_0|0\rangle$ de $Q_1|0\rangle$ avec probabilité supérieure à s, ce qui est impossible.

5.4 QMIP*

Nous étudions à présent les protocoles de preuves interactives quantiques à deux prouveurs partageant de l'enchevêtrement les plus généraux qui soient, bâtis sur le même principe que la classe QIP (cf la partie 4.1). Très peu de choses sont connues sur cette classe en général : le seul résultat conséquent est le théorème 43 ci-dessous. Nous commençons par en donner une définition formelle, puis nous prouvons que la classe QMIP*, lorsqu'elle est restreinte à un tour seulement, contient QIP.

5.4.1 Définitions

La définition de la classe de complexité QMIP* est l'extension naturelle de la définition de QIP au cas de plusieurs prouveurs. Nous la détaillons ci-dessous, en reprenant la terminologie introduite pour QIP.

Soit k le nombre de prouveurs. Sur une entrée $x \in \Sigma^*$ de taille $n = |x|$, l'espace total sur lequel agira le système de preuve interactive sera constitué de $q(n) = q_V(n) + k\,(q_M(n) + q_P(n))$ qubits. Les $q_V(n)$ premiers qubits sont les qubits privés du vérifieur, alors que chaque registre de $q_M(n) + q_P(n)$ qubits correspond à l'espace des messages et à l'espace privé de chacun des k prouveurs. Les prouveurs ne sont pas autorisés à communiquer entre eux.

Étant données des fonctions à croissance polynomiale $m, q_V, q_M : \mathbb{N} \to \mathbb{N}$, un *vérifieur à m messages (q_V, q_M)-restreint* est une fonction $V : \Sigma^* \to \Sigma^*$ calculable en temps polynomial en la longueur de son entrée. Pour chaque $x \in \Sigma^*$, $V(x)$ est interprété comme un $\lfloor m(n)/2 + 1 \rfloor$-tuple $(V_1(x), \ldots, V_{\lfloor m(n)/2+1 \rfloor}(x))$. Pour chaque i, $V_i(x)$ est la description d'un circuit quantique agissant sur $q_V(n) + kq_M(n)$ qubits. Finalement, le premier qubit de l'espace privé du vérifieur est désigné comme étant le qubit de sortie.

Étant données des fonctions à croissance polynomiale $m, q_M : \mathbb{N} \to \mathbb{N}$, et une fonction $q_P : \mathbb{N} \to \mathbb{N}$, un *prouveur à m messages (q_M, q_P)-restreint* P_i pour $i = 1, \ldots, k$ est défini de manière analogue : c'est une fonction $P_i : \Sigma^* \to \Sigma^*$, sur laquelle on n'impose aucune restriction de calculabilité. Pour chaque $x \in \Sigma^*$, $P_i(x)$ est interprété comme un

$\lfloor m(n)/2+1/2 \rfloor$-tuple $(P_{i,1}(x), \ldots, P_{i,\lfloor m(n)/2+1/2 \rfloor}(x))$. Pour chaque j, $P_{i,j}(x)$ est la description d'un circuit quantique agissant sur $q_P(n) + q_M(n)$ qubits. Les $q_P(n)$ premiers qubits sont interprétés comme l'espace propre du vérifieur, alors que les $q_M(n)$ autres constituent à nouveau l'espace des messages. De plus, si $q_e : \mathbb{N} \to \mathbb{N}$ est une fonction telle que $q_e \leq q_P$, chaque P_i peut avoir au plus $q_e(n)$ qubit parmi ses qubits privés qui sont enchevêtrés, avant que le protocole ne commence, avec les qubits privés des autres prouveurs. Un tel prouveur est dit q_e-a priori-enchevêtré.

Un *système de preuve interactif quantique à m messages et k prouveurs* (q_V, q_M, q_P)-restreint est contitué d'un vérifieur V à m messages (q_V, q_M)-restreint et de k prouveurs à m messages (q_M, q_P)-restreints $P_1, \ldots, P_k$. Un tel système est dit q_e-a priori-enchevêtré si c'est le cas pour les P_i. On définit un circuit $(V, P_1, \ldots, P_k)(x)$ agissant sur $q(n) = q_V(n) + k\,(q_M(n) + q_P(n))$ qubits de la façon suivante. Si $m(n)$ est impair, les circuits

$$P_{1,1}(x), \ldots, P_{k,1}(x)\, V_1(x), \ldots, P_{1,(m(|x|)+1)/2}(x), \ldots, P_{k,(m(|x|)+1)/2}(x)\, V_{(m(|x|)+1)/2}(x)$$

sont appliqués les uns à la suite des autres, soit aux $q_V(n)+q_M(n)$ qubits du vérifieur, soit aux $q_P(n) + q_M(n)$ de chaque prouveur. Si $m(n)$ est pair, c'est le vérifieur qui applique le premier circuit : on exécute la séquence

$$V_1(x),\, P_{1,1}(x), \ldots, P_{k,1}(x), \ldots,\, P_{1,m(|x|)/2}(x), \ldots, P_{1,m(|x|)/2}(x),\, V_{m(|x|)/2+1)}(x)$$

Finalement, pour une entrée x, la probabilité que le couple $(V, P_1, \ldots, P_k)$ accepte x est définie comme étant la probabilité d'obtenir $|1\rangle$ lors d'une mesure du qubit de sortie du vérifieur dans la base canonique $(|0\rangle, |1\rangle)$, après exécution du circuit $(V, P_1, \ldots, P_k)(x)$ sur l'état initial $|0\rangle^{\otimes q(n)}$.

Nous pouvons à présent définir la classe de complexité QMIP* :

Définition 42 *Soient $k, m, q_e : \mathbb{N} \to \mathbb{N}$ et $c, s : \mathbb{N} \to [0,1]$ des fonctions telles que $s(n) < c(n)$ pour tout n. On note $QMIP_{c,s}(k, m, q_e)$ la classe des langages L tels qu'il existe des fonctions $q_V, q_M : \mathbb{N} \to \mathbb{N}$ à croissance polynomiale et un vérifieur V à m messages (q_V, q_M)-restreint tel que, pour toute entrée x de taille n,*

- *Si $x \in L$, il existe une fonction $q_P : \mathbb{N} \to \mathbb{N}$ telle que $q_P \geq q_e$ et des prouveurs $P_1, \ldots, P_k$ à m messages (q_M, q_P)-restreints q_e-a priori-enchevêtrés tels que $(V, P_1, \ldots, P_k)(x)$ accepte avec probabilité au moins $c(n)$.*
- *Si $x \notin L$, pour toute fonction $q_P : \mathbb{N} \to \mathbb{N}$ telle que $q_P \geq q_e$ et tous prouveurs $P_1, \ldots, P_k$ à m messages (q_M, q_P)-restreints et q_e-a priori-enchevêtrés, $(V, P_1, \ldots, P_k)(x)$ accepte avec probabilité au plus $s(n)$.*

On notera de plus QMIP$^*(m)$ l'union des $QMIP^*_{1,1/2}(k, m, q_e)$ sur toutes les fonctions k, m à croissance polynomiale et toutes les fonctions q_e.

Le résultat principal de [KM03] est le suivant :

Théorème 43 *L'union des $QMIP^*_{1,1/2}(k, m, q_e)$ sur toutes les fonctions k, m, q_e à croissance polynomiale est incluse dans NEXP.*

C'est-à-dire que, si les prouveurs partagent au plus une quantité polynomiale d'enchevêtrement a priori, alors la puissance du système de preuve interactive ne dépasse pas celle de NEXP. L'idée de la preuve est de remarquer (et de prouver !) que, avec cette restriction sur l'enchevêtrement, on peut supposer que la taille de l'espace propre des prouveurs est polynomial : on montre qu'il suffit qu'ils aient assez de place pour manipuler des purifications des messages que leur envoie le vérifieur. Les transformations unitaires appliquées par les prouveurs sont alors de taille exponentielle, et on peut les "deviner" et calculer leut probabilité d'être acceptées en temps exponentiel non-déterministe.

5.4.2 Une utilisation de l'enchevêtrement

Nous allons utiliser le protocole QMAM pour QIP donné au théorème 25 pour prouver que la classe QMIP*(2) contient QIP. Cette inclusion est presque immédiate, cependant nous remarquons que le protocole décrit ci-dessous est tel que le vérifieur utilise le fait que les prouveurs partagent de l'enchevêtrement pour être particulièrement exigeant envers eux : deux prouveurs qui ne partagent pas d'enchevêtrement ne pourraient pas réussir à ce protocole (bien sûr, si les prouveurs ne partagent pas d'enchevêtrement, on obtient la classe NEXP, qui contient QIP $\subset$ EXP, donc un protocole existe - mais ce n'est pas celui décrit ici). Ceci contraste avec la plupart des protocoles habituels, dans lesquels l'enchevêtrement est plutôt une ressource qui permet aux prouveurs de tricher : nous sommes ainsi ici dans un cas atypique.

Théorème 44 *QIP* $\subset$ *QMIP**(2)

Démonstration. Soit (V_1, V_2) un vérifieur pour un langage $L \in$ QIP. Nous considérons le vérifieur V suivant pour QMIP*(2) :

1. Jeter une pièce au hasard, et envoyer le résultat au prouveur 2.
2. Recevoir des registres M_1 de la part du premier prouveur, et M_2 de la part du deuxième. Si la pièce de l'étape précédente était tombée sur pile, appliquer V_2 à $(\mathsf{M}_1, \mathsf{M}_2)$ et accepter si et seulement si le résultat d'une mesure du premier qubit de M_1 donne $|1\rangle$. Si la pièce était tombée sur face, appliquer V_1^* à $(\mathsf{M}_1, \mathsf{M}_2)$ et accepter si et seulement si tous les qubits de M_1 sont dans l'état $|0\rangle$.

La correction de ce protocole découle presque immédiatement de celle du protocole QMAM décrit au théorème 25. Nous donnons quelques indications supplémentaires ci-dessous.

Commençons par prouver que, s'il existe un prouveur se faisant accepter par (V_1, V_2) avec probabilité au moins c, alors il existe deux prouveurs P_1 et P_2 se faisant accepter par V avec probabilité c. Le prouveur P_1 possède un unique registre M_1, et P_2 possède un registre M_2 ainsi qu'un registre privé P_2. Avant que le protocole ne commence, les deux prouveurs initialisent leurs registres $(\mathsf{M}_1, \mathsf{M}_2)$ dans l'état enchevêtré $V_1|0\rangle$, avec le registre M_1 correspondant au registre V du protocole QIP, et le regsitre M_2 correspondant au registre M. En fonction du bit qu'il reçoit, le deuxième prouveur effectue la même transformation que celle qu'il aurait effectuée dans le protocole QMAM. Le premier prouveur ne fait rien. Il est clair que la probabilité de gain des deux prouveurs est la même que celle du prouveur du protocole QMAM, elle-même égale à celle du prouveur pour le protocole QIP.

Réciproquement, deux prouveurs pour le protocole QMIP*(2) ne peuvent tricher plus qu'un prouveur pour le protocole QIP. En effet, P_1 ne reçoit pas de question, et l'état qu'il envoie au vérifieur est donc indépendant de la question que P_2 a reçue. De même que dans le protocole QMAM, ceci sert à garantir que le registre $\mathsf{M}_1 = \mathsf{V}$ ne dépend pas du résultat du tirage aléatoire effectué par le vérifieur.

6 Conclusion

Lors de ce stage nous avons étudié l'expressivité de différents modèles de preuves interactives quantiques à plusieurs prouveurs. Nous avons défini plusieurs classes de systèmes de preuves intermédiaires entre celui de [CHTW04] et celui de [KM03], et avons étudié l'effet de nos modifications. Nous avons également établi une connexion surprenante entre algorithmes d'approximation et preuves interactives quantiques à deux prouveurs, et nous avons étudié cette connexion dans le cadre du problème MAXCUT.

La principale question ouverte liée aux systèmes de preuves quantiques à deux prouveurs est la caractérisation de la classe de complexité MIP*, dans laquelle tous les échanges sont classiques, mais les prouveurs disposent d'ordinateurs quantiques et partagent de l'enchevêtrement a priori. On ne sait ni si l'enchevêtrement permet aux prouveurs de tricher, diminuant l'expressivité de cette classe en-dessous de NEXP, ni s'il leur permet de prouver l'appartenance à des langages plus compliqués, la plaçant au-dessus de NEXP, ni si simplement MIP* = NEXP, ce qui est peut-être le résultat le plus probable.

À la fin de se stage, nous avons étudié une question proche en relâchant cette classe de complexité, à savoir : est-ce que QMIP* contient NEXP ? Les résultats d'inapproximabilité esquissés dans la partie 3.2 nous donnent un bon point de départ, et nous avons construit un protocole de preuve interactive quantique pour le problème 3DM qui semble prometteur. Cependant, des contraintes de temps nous ont empêché de terminer la preuve avant la remise de ce mémoire. Ceci constitue la principale piste à explorer, et le principal problème ouvert à considérer, suite à ce stage.

Références

[Aar05] Scott Aaronson. Quantum computing, postselection, and probabilistic polynomial-time. *Electronic Colloquium on Computational Complexity (ECCC)*, (003), 2005.

[ALM+92] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and hardness of approximation problems. In *Proc. 33rd FOCS*, pages 14–23, 1992.

[AS92] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs ; a new characterization of NP. In *Proc. 33rd FOCS*, pages 2–13, 1992.

[Bab85] László Babai. Trading group theory for randomness. In *Proc. 17th STOC*, pages 421–429, 1985.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1 :3–40, 1991.

[BOGKW88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs : How to remove intractability assumptions. In *Proc. 20th STOC*, pages 113–131, 1988.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15) :880–884, Oct 1969.

[CHTW04] Richard Cleve, Peter Høyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *IEEE Conference on Computational Complexity*, pages 236–249, 2004.

[FL92] Uriel Feige and Laszlo Lovasz. Two-prover one-round proof systems : their power and their problems. In *Proc. 24th STOC*, pages 733–744, New York, NY, USA, 1992. ACM Press.

[GJ79] Michael R. Garey and David S. Johnson. *A guide to the theory of NP-completeness*. W.H Freeman and company, 1979.

[GMR85] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems. In *Proc. 17th STOC*, pages 291–304, 1985.

[GS86] Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In *proc. 18th STOC*, pages 59–68, 1986.

[GW95] Michel X. Goemans and David P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *J. ACM*, 42(6) :1115–1145, 1995.

[Hås01] Johan Håstad. Some optimal inapproximability results. *J. ACM*, 48(4) :798–859, 2001.

[JWB03] Dominik Janzing, Pawel Wocjan, and Thomas Beth. Identity check is QMA-complete, 2003.

[KdW04] Iordanis Kerenidis and Ronald de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. *J. Comput. Syst. Sci.*, 69(3) :395–420, 2004.

[KKMO04] Subhash Khot, Guy Kindler, Elchanan Mossel, and Ryan O'Donnell. Optimal inapproximability results for MAX-CUT and other 2-variable CSPs ? In *Proc. 45th FOCS*, pages 146–154, Washington, DC, USA, 2004. IEEE Computer Society.

[KM03] Hirotada Kobayashi and Keiji Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *J. Comput. Syst. Sci.*, 66(3) :429–450, 2003.

[KMY03] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems : Are multiple Merlins more helpful to Arthur ? In *ISAAC*, pages 189–198, 2003.

[KSV01] A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2001.

[KW00] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proc. 32nd STOC*, 2000.

[MW04] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. In *IEEE Conference on Computational Complexity*, pages 275–285, 2004.

[NC00] Michael Nielsen and Issac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[Raz05] Ran Raz. Quantum information and the PCP theorem. In *Proc. 46th FOCS*, pages 459–468, 2005.

[RW05] Bill Rosgen and John Watrous. On the hardness of distinguishing mixed-state quantum computations. In *IEEE Conference on Computational Complexity*, pages 344–354, 2005.

[Sha92] Adi Shamir. IP = PSPACE. *J. ACM*, 39(4) :869–877, 1992.

[Tsi80] Boris Tsirelson. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4 :93–100, 1980.

[Wat99] John Watrous. PSPACE has constant-round quantum interactive proof systems. In *Proc. 40th FOCS*, pages 112–119, 1999.

[Wat02] John Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proc. 43rd FOCS*, pages 459–, 2002.

[Weh06] Stephanie Wehner. Entanglement in interactive proof systems with binary answers. In *STACS*, pages 162–171, 2006.