Séminaire BOURBAKI Janvier 2023
74e année, 2022–2023, no 1203, p. 225 à 249
doi : 10.24033/ast.1212

ALGÈBRES DE VON NEUMANN, PRODUITS TENSORIELS, CORRÉLATIONS QUANTIQUES ET CALCULABILITÉ
[*d'après* Ji, Natarajan, Vidick, Wright et Yuen]

par **Mikael de la Salle**

Introduction

Le but de ce texte est de présenter la résolution récente de problèmes qui sont longtemps restés ouverts en algèbres d'opérateurs. Commençons par les énoncer.

Le problème de plongement de Connes (1976) demande si tout facteur II_1 admet un plongement approximatif dans le facteur II_1 hyperfini $\mathscr{R}$. Autrement dit, s'il peut être réalisé comme une sous-algèbre de von Neumann d'un ultraproduit d'algèbres de matrices. C'est une façon précise de demander si les algèbres de matrices forment un modèle suffisant pour comprendre tous les phénomènes locaux dans les algèbres de von Neumann finies.

Le problème peut être énoncé de manière équivalente sans avoir à introduire de vocabulaire d'algèbres de von Neumann. Étant donné un groupe Γ, un *caractère* est une fonction $\varphi\colon \Gamma \to \mathbf{C}$ définie positive [(1)], invariante par conjugaison et normalisée par $\varphi(1) = 1$. Les caractères qui interviennent dans la théorie des représentations des groupes finis (de la forme $\gamma \mapsto \frac{1}{d}\mathrm{Tr}(\pi(\gamma))$ pour une représentation unitaire de dimension finie d) sont des exemples de caractères, que nous appellerons caractères de dimension finie. Mais il y en a bien d'autres pour les groupes infinis, par exemple la fonction indicatrice de $\{1\}$, ou plus généralement de tout sous-groupe distingué d'indice infini. Le problème de plongement de Connes est équivalent à la question « Tout caractère du groupe libre à deux générateurs est-il limite simple d'une suite de caractères de dimension finie ? » Si on pose la question seulement pour les caractères de la forme $\varphi = \chi_N$ pour un sous-groupe distingué N, on obtient une autre question importante (elle toujours ouverte) « Tout groupe est-il hyperlinéaire ? », un affaiblissement de la question de Gromov « Tout groupe est-il sofique ? » (qui correspond à demander si χ_N est limite simple de caractères de dimension finie provenant de représentations à valeurs dans les groupes de matrices de permutations).

(1) C'est-à-dire, pour toute famille finie $\gamma_1, \dots, \gamma_n \in \Gamma$, la matrice $(\varphi(\gamma_i^{-1}\gamma_j))_{i,j\leqslant n}$ est positive

La conjecture de Kirchberg (1993) porte sur les produits tensoriels de C^*-algèbres. Une façon courte de l'énoncer est : y a-t-il une unique norme de C^*-algèbre sur $\mathscr{C} \otimes \mathscr{C}$, où $\mathscr{C}$ est la C^*-algèbre universelle engendrée par une suite dénombrable d'unitaires. Par la propriété universelle de $\mathscr{C}$, cette conjecture a de nombreuses reformulations très différentes ; le lecteur intéressé pourra en savoir beaucoup plus sur ces formes (et beaucoup d'autres choses) dans le livre de Pisier (2020), qui est entièrement dédié à ce sujet.

Le problème de Tsirelson est lié aux fondements de la mécanique quantique et, via les inégalités de Bell, à la fameuse expérience d'Alain Aspect démontrant le phénomène d'intrication quantique et qui lui a valu le prix Nobel. Dans cette expérience, Aspect mesure des corrélations entre certaines observables entre systèmes physiques. Il observe que celles-ci sont incompatibles avec la théorie des variables cachées proposée par Einstein, Podolski et Rosen, mais qu'elles sont bien compatibles avec le formalisme mathématique de la mécanique quantique reposant sur les espaces de Hilbert. Jusqu'à preuve du contraire, le monde physique est donc bien quantique et les espaces de Hilbert sont nécessaires à sa description. Tsirelson (1980, 1993) étudie différentes variantes de ce formalisme mathématique, et notamment (il y a là un petit raccourci) une distinction entre espaces de dimension finie et espaces de dimension infinie. Tsirelson (1993) affirme, sans preuve, que, pour ces deux modèles, les corrélations possibles sont essentiellement les mêmes, dans le sens où toute corrélation dans le modèle avec des espaces de Hilbert de dimension infinie est une limite de corrélations dans le modèle avec des espaces de dimension finie. C'est en effet naturel, puisqu'un espace de Hilbert est une union filtrante de ses sous-espaces de dimension finie. Ce n'est que dans les années 2000, avec l'explosion de la théorie quantique de l'information, que ces travaux de Tsirelson ont été étudiés attentivement (Navascués, Pironio et Acín, 2008) ; Tsirelson reconnaît alors qu'il a été un peu rapide et son affirmation devient donc le problème de Tsirelson.

De manière remarquable et pas du tout évidente, ces trois problèmes sont équivalents (et sont parfois appelés *conjectures*, même si Kirchberg est le seul à avoir énoncé sa question comme une conjecture). Le chemin le plus délicat, l'équivalence entre le problème de Connes et la conjecture de Kirchberg a été démontrée par Kirchberg, 1993. L'équivalence entre le problème de Tsirelson et la conjecture de Kirchberg a été démontrée plus récemment par Fritz (2012) et Junge et al. (2011) pour une direction, et Ozawa (2013) pour l'autre.

En janvier 2020, la solution de toutes ces questions a été déposée sur arXiv par une équipe de cinq informaticiens.

Théorème 0.1 (Ji et al., 2020a). *Le problème de Connes–Kirchberg–Tsirelson a une réponse négative.*

Autrement dit, il existe un facteur II_1 qui n'est pas plongeable dans un ultraproduit d'algèbres de matrices ; il y a au moins deux normes de C^*-algèbres sur $\mathscr{C} \otimes \mathscr{C}$;

il existe des inégalités de Bell qui distinguent strictement les corrélations quantiques dans le modèle de la mécanique quantique où l'on autorise des espaces de Hilbert de dimension infinie de celles dans le modèle où seuls des espaces de Hilbert de dimension finie (mais arbitraire) sont autorisés. On peut donc imaginer qu'il existe une expérience physique qui pourrait démontrer expérimentalement que les espaces de Hilbert de dimension infinie sont indispensables pour décrire le monde physique…

Le théorème 0.1 est énoncé dans Ji et al. (2020a), mais sa longue preuve est répartie aussi dans Bavarian, Vidick et Yuen (2022) et Ji et al. (2020b, 2022). Elle repose également sur plusieurs autres travaux antérieurs, notamment Natarajan et Wright (2019). Ce travail est très long et difficile. Il repose sur des idées nouvelles, mais aussi sur des décennies d'avancées en informatique théorique, informatique quantique et théorie quantique de l'information. La première version proposée reposait d'ailleurs sur des résultats dont la preuve s'est avérée fausse, et qui ont demandé aux auteurs un travail considérable de correction (Ji et al., 2020b, 2022). Il est illusoire d'en présenter une preuve complète en quelques pages. Le but de ce texte est de présenter de manière très superficielle la stratégie générale de la preuve telle que je la comprends. On s'éloignera par moments de l'approche initiale, en tentant d'être le plus compréhensible possible pour un public de mathématiciens. Par exemple, on essaiera de ne parler de classes de complexité que quand c'est vraiment nécessaire, là où les auteurs de l'article initial concentrent leurs efforts à démontrer un énoncé de complexité (MIP*=RE) dont ils déduisent assez directement le résultat mathématique. L'article original et l'excellent survol de Vidick (2022b) sont des très bons endroits pour comprendre les aspects informatiques. Une autre différence notable est qu'on réfutera directement le problème de Connes, là où les auteurs, sans doute motivés par un sens physique dont je manque cruellement, réfutaient d'abord le problème de Tsirelson. Du point de vue mathématique, cela revient à étudier uniquement des états traciaux sur des algèbres de von Neumann là où les auteurs étudient des états arbitraires, et je pense que cela ajoute beaucoup de difficultés inutiles.

Ce texte est dédié à Eberhard Kirchberg (1946–2022) et Boris Tsirelson (1950–2020), deux grands noms de l'analyse fonctionnelle et protagonistes centraux de cette histoire, qui sont décédés peu après l'annonce de sa résolution.

Je voudrais remercier les très nombreux collègues qui ont accepté de répondre à toutes mes questions, parfois naïves. Les lister tous serait trop long, mais mentionnons au moins les auteurs Thomas Vidick et Henry Yuen, mais aussi Guillaume Aubrun, Laurent Bartoldi, Michael Chapman, Emilie Elkiaer, Omar Fawzi, Cécilia Lancien, Amine Marrakchi, Paul Meunier, Sophie Morel, Étienne Moutot, Alexander Müller-Hermes, Magdalena Musat, Pascal Koiran, Mikael Rørdam, Bruno Sévennec, Todor Tsankov… Je remercie plus particulièrement Guillaume Aubrun et Thomas Vidick pour leur relecture attentive et constructive de ce texte.

1. Algèbres de von Neumann et calculabilité

1.1. Algèbres de von Neumann traciales et approximation par des algèbres de matrices

Une algèbre de von Neumann $\mathscr{M}$ est une algèbre d'opérateurs sur un espace de Hilbert $\mathscr{H}$, stable par l'adjoint, contenant l'identité de $\mathscr{H}$ et fermée pour la topologie préfaible [(2)]. Une algèbre de von Neumann est dite finie si elle admet un *état tracial* (ou simplement une trace) $\tau : \mathscr{M} \to \mathbf{C}$: une forme linéaire préfaiblement continue, normalisée par $\tau(1) = 1$ et vérifiant $\tau(x^*x) = \tau(xx^*) > 0$ pour tout $x \in \mathscr{M}$ non nul. La paire $(\mathscr{M}, \tau)$ est appelée une algèbre de von Neumann traciale.

Les exemples évidents d'algèbres de von Neumann traciales sont les algèbres de matrices $(M_d(\mathbf{C}), \mathrm{tr} := \frac{1}{d}\mathrm{Tr})$. Et ces exemples permettent d'en construire beaucoup d'autres avec la technique d'ultraproduit : si $\mathscr{U}$ est un ultrafiltre sur un ensemble I, et si $d_i \in \mathbf{N}$ pour tout I, on peut définir l'ultraproduit $\prod_{\mathscr{U}}(M_{d_i}(\mathbf{C}), \mathrm{tr})$ comme le quotient de $\prod_i M_{d_i}(\mathbf{C})$, l'espace des suites bornées en norme d'opérateur, par $\{(x_i) \in \prod_i M_{d_i}(\mathbf{C}) \mid \lim_{\mathscr{U}} \mathrm{tr}(x_i^* x_i) = 0\}$. Muni de la trace $\tau((x_i)) = \lim_{\mathscr{U}} \mathrm{tr}(x_i)$, c'est une algèbre de von Neumann traciale. Le problème de plongement de Connes demande s'il y a d'autres algèbres de von Neumann traciales que les sous-algèbres de von Neumann de tels ultraproduits. La construction GNS (Bekka, Harpe et Valette, 2008, Theorem C.4.10) et le fait que toute algèbre de von Neumann traciale finiment engendrée peut être réalisée dans une algèbre de von Neumann traciable engendrée par deux unitaires justifient l'équivalence entre cette forme du problème de Connes et celle donnée dans l'introduction.

1.2. Approximation de caractères et calculabilité

Plutôt que de travailler avec des caractères sur un groupe donné (le groupe libre à deux générateurs) comme dans l'introduction, on travaillera avec une famille de groupes, indexée par les paires (n, m) d'entiers positifs, et on n'étudiera les caractères qu'en restriction à des parties finies de plus en plus grandes. Cela permettra de faire entrer en jeu des notions de calculabilité. Concrètement, notons

- $\Gamma_{n,m} = (\mathbf{Z}/n\mathbf{Z})^{*m}$ le produit libre de m copies du groupe fini cyclique d'ordre n,
- $S_{n,m} \subset \Gamma_{n,m}$ sa partie génératrice finie donnée par l'union des m copies de $\mathbf{Z}/n\mathbf{Z}$,
- pour tout entier $d \geqslant 1$, $C_d(n, m) \subset \mathbf{C}^{S_{n,m}^2}$ l'enveloppe convexe des restrictions à $S_{n,m}^2$ (la boule de rayon 2, c'est-à-dire l'ensemble des produits de deux éléments de $S_{n,m}$) de caractères de dimension $\leqslant d$ de $\Gamma_{n,m}$,

[(2)] $B(\mathscr{H})$ est le dual des opérateurs à trace sur $\mathscr{H}$

- $C_{<\infty}(n,m) = \cup_d C_d(n,m)$.
- pour tout $\varepsilon > 0$, $f_\varepsilon(n,m)$ le plus petit entier d tel que $C_\infty(n,m)$ est contenu dans le ε-voisinage [3] de $C_d(n,m)$.

L'énoncé suivant est une variante d'arguments de Navascués, Pironio et Acín (2008).

Proposition 1.1. *Si le problème de plongement de Connes avait une réponse positive, alors la fonction $(k,n,m) \mapsto f_{\frac{1}{k}}(n,m)$ serait majorée par une fonction calculable $\mathbf{N}^3 \to \mathbf{N}$.*

Démonstration. Supposons que le problème de Connes ait une réponse positive. En particulier, pour tout n, m, $C_{<\infty}(n,m)$ est dense dans $C(n,m)$, l'ensemble des restrictions à $S^2_{n,m}$ de caractères de $\Gamma_{n,m}$. Être un caractère, c'est donné par une famille dénombrable d'inégalités, que l'on peut énumérer explicitement. Notons $C^d(n,m)$ le polytope calculable donné comme les restrictions à $S^2_{n,m}$ des fonctions ne vérifiant que les d premières inégalités. Clairement, $C^d(n,m)$ décroît vers $C(n,m)$. On a donc une approximation *par dessus* de $C(n,m)$. En parallèle, en décrivant une partie $\frac{1}{d}$-dense des matrices unitaires de taille d et d'ordre n, on peut obtenir une suite calculable contenue dans $C_d(n,m)$ et approchant $C_{<\infty}(n,m)$ *par dessous*. Le plus petit d tel que l'approximation par dessous est $\frac{1}{k}$-dense dans l'approximation par dessus est donc fini (car on a supposé que $C_{<\infty}(n,m)$ est dense dans $C(n,m)$) et calculable. C'est clairement un majorant de $f_{\frac{1}{k}}(n,m)$. □

Le théorème principal est

Théorème 1.2 (Ji et al., 2020a). *La fonction $(k,n,m) \mapsto f_{\frac{1}{k}}(n,m)$ n'est pas majorée par une fonction calculable.*

Il a toujours été clair pour moi que la raison pour laquelle le problème de plongement de Connes ou la conjecture de Kirchberg étaient difficiles est qu'il y a beaucoup de choses qu'on ne comprend pas dans les algèbres d'opérateurs de dimension infinie (et en particulier dans la notion de commutation en dimension infinie), contrairement à la dimension finie où tout est limpide. Il est frappant que le théorème 1.2, duquel la réfutation du problème de Connes découle directement, ne porte pas du tout sur les algèbres d'opérateurs de dimension infinie. Il affirme, contrairement à l'intuition, que les algèbres d'opérateurs de dimension finie sont *extrêmement compliquées*, non pas du point de vue leur description mathématique, mais du point de vue de la calculabilité.

[3] Pour fixer les idées, disons qu'on a muni $\mathbf{C}^{S^2_{n,m}}$ de la norme ℓ_∞, mais n'importe quelle autre norme raisonnable (dans le sens comparable à la norme ℓ_∞ à des constantes calculables près) conviendrait. L'existence de $f_\varepsilon(n,m)$ est immédiate par compacité.

Une des fonctions non calculables les plus élémentaires est la fonction d'arrêt des machines de Turing. La preuve du théorème 1.2 passe par une réduction à cette fonction d'arrêt. Un énoncé plus précis duquel le théorème 1.2 découle facilement (exercice) est le suivant.

Théorème 1.3 (Ji et al., 2020a). *Il existe un fonction calculable qui, évaluée en une machine de Turing M, renvoie toujours un triplet (n, m, φ) avec $\varphi \in (\mathbf{C}^{S^2_{n,m}})^*$ et vérifiant*

$$\sup_{C<\infty(n,m)} \varphi \begin{cases} = 1 & \text{si } M \text{ s'arrête,} \\ \leqslant \frac{1}{2} & \text{sinon.} \end{cases}$$

La forme linéaire φ dans ce théorème n'est pas arbitraire, elle est de la forme « valeur d'un jeu ».

2. Jeux

La notion de jeu que nous considérons ici est celle de jeu à deux joueurs et une manche, introduite dans le contexte de preuve interactive à deux joueurs par Ben-Or et al. (1988). Nous ne considérerons d'ailleurs que des versions symétriques. Comme c'est la seule notion de jeu que nous considérerons, nous utiliserons simplement le mot jeu.

Dans tout ce texte, un jeu est donc la donnée de $\mathscr{G} = (\mathscr{X}, \mu, \mathscr{A}, D)$ où $\mathscr{X}$ et $\mathscr{A}$ sont des ensembles finis, μ est une mesure de probabilité sur $\mathscr{X} \times \mathscr{X}$ et $D\colon \mathscr{X} \times \mathscr{X} \times \mathscr{A} \times \mathscr{A} \to \{0,1\}$ est une fonction symétrique.

2.1. Aparté : interprétation des jeux

La raison pour laquelle on parle de jeu est la suivante. Il faut imaginer qu'il y a trois protagonistes : un arbitre et deux joueurs. L'arbitre peut communiquer avec les joueurs, mais les joueurs ne peuvent communiquer entre eux. $\mathscr{X}$ est *l'ensemble des questions*, $\mathscr{A}$ est *l'ensemble des réponses possibles*. L'arbitre tire au hasard une paire $(x, y) \in \mathscr{X} \times \mathscr{X}$ selon la loi μ. Il communique la question x au premier joueur, et la question y au second joueur ; la question posée à chaque joueur est donc inconnue de l'autre. En retour, le premier joueur donne une réponse a parmi les réponses possibles, et le second joueur répond b. Les joueurs gagnent tous les deux si $D(x, y, a, b) = 1$, et perdent tous les deux sinon. Il s'agit donc d'un jeu coopératif ; l'intérêt des joueurs est de trouver la stratégie qui optimise la probabilité de gagner.

Là où les choses se compliquent, c'est quand on se demande quelles sont les stratégies possibles. Une *stratégie classique*, c'est une stratégie où la réponse de chaque joueur est une fonction déterministe de sa question : $a = f(x)$ et $b = g(y)$. On peut aussi imaginer des stratégies où les joueurs ont accès à une source d'aléa indépendante des questions. Mais une telle stratégie peut être vue comme une combinaison convexe de stratégies déterministes, et donc ne peut améliorer la probabilité de gagner.

Une *stratégie quantique*, c'est une stratégie où les joueurs sont autorisés à partager de l'intrication quantique. Mathématiquement, cela veut dire qu'il existe un espace de Hilbert $\mathscr{H}$, un vecteur unité $\psi \in \mathscr{H}$, et, pour tout x, deux partitions de l'unité $(p_a^x)_{a\in A}$ et $(q_b^x)_{b\in B}$ dans $B(\mathscr{H})$ tels que $[p_a^x, q_b^y] = 0$ pour tout $x, y \in \mathscr{X}$ et $a, b \in \mathscr{A}$. Alors la probabilité que les joueurs répondent a, b à x, y est $\langle p_a^x q_b^y \psi, \psi\rangle$. Le formalisme de la mécanique quantique dit précisément que c'est le genre de choses que les joueurs peuvent faire sans communiquer. La probabilité de gain de cette stratégie est donc

$$\sum_{x,y\in\mathscr{X},a,b\in\mathscr{A}} \mu(x,y)D(x,y,a,b)\langle p_a^x q_b^y \psi, \psi\rangle. \tag{1}$$

Dans la suite, on ne considèrera que des formes très particulières de stratégies, qui correspondent au cas où $\mathscr{H} = L^2(\mathscr{M}, \tau)$, ψ est l'image dans $L^2(\mathscr{M}, \tau)$ de l'identité de $\mathscr{M}$, et où il y a des partitions de l'unité $(e_a^x)_{a\in\mathscr{A}}$ dans $\mathscr{M}$ pour tout $x \in \mathscr{X}$, telles que p_a^x est la multiplication à gauche par e_a^x et q_b^y est la multiplication à droite par e_b^y. Ces stratégies sont habituellement appelées stratégies synchrones (Paulsen et al., 2016), mais comme c'est la seule forme de stratégie que l'on considèrera, on les appellera simplement stratégies.

2.2. Stratégies

Une stratégie pour le jeu $\mathscr{G}$ est la donnée de $\mathscr{S} = (\mathscr{M}, \tau, p)$ où $(\mathscr{M}, \tau)$ est une algèbre de von Neumann traciale et $p = (p_a^x)_{a\in\mathscr{A}}^{x\in\mathscr{X}}$ est une famille de projections orthogonales dans $\mathscr{M}$ telle que pour tout x, $(p_a^x)_{a\in\mathscr{A}}$ est une partition de l'unité :

$$\forall x \in \mathscr{X}, \sum_{a\in\mathscr{A}} p_a^x = 1.$$

La valeur d'une stratégie $\mathscr{S}$ pour le jeu $\mathscr{G}$ est

$$\mathrm{val}(\mathscr{G}, \mathscr{S}) = \sum_{x,y\in\mathscr{X},a,b\in\mathscr{A}} \mu(x,y)D(x,y,a,b)\tau(p_a^x p_b^y).$$

De manière évidente, $\mathrm{val}(\mathscr{G}, \mathscr{S}) \in [0, 1]$, et $\mathrm{val}(\mathscr{G}, \mathscr{S}) = 1$ si et seulement si $p_a^x p_b^y = 0$ pour tout (x, y) dans le support de μ et tout a, b tel que $D(x, y, a, b) = 0$. On dira qu'une stratégie est parfaite si sa valeur est égale à 1 ; on dira qu'elle est bonne si sa valeur est proche de 1. Une partie importante de l'analyse mathématique des jeux sera de comprendre ce qui se passe pour une stratégie qui est bonne.

On note aussi

$$\mathrm{val}(\mathscr{G}, \mathscr{M}) = \sup\{\mathrm{val}(\mathscr{G}, \mathscr{S})\}$$

où le supremum est pris sur toutes les stratégies où l'algèbre de von Neumann est un coin de $\mathscr{M}$, c'est-à-dire de la forme $(q\mathscr{M}q, \frac{1}{\tau(q)}\tau)$ pour q une projection non nulle dans $\mathscr{M}$.

Par exemple, si $\mathscr{M}$ est une algèbre de von Neumann commutative, on retrouve presque [4] la valeur classique d'un jeu, à savoir

$$\mathrm{val}(\mathscr{G},\mathscr{M}) = \sup\Big\{ \sum_{x,y\in\mathscr{X}} \mu(x,y) D(x,y,f(x),f(y)) \mid f\colon \mathscr{X} \to \mathscr{A} \Big\}.$$

Enfin on notera

$$\mathrm{val}(\mathscr{G},d) = \mathrm{val}\big(\mathscr{G}, M_d(\mathbf{C})\big)$$

la valeur optimale d'une stratégie sur des algèbres de matrices de taille $\leqslant d$, et

$$\mathrm{val}(\mathscr{G},<\infty) = \sup_d \mathrm{val}(\mathscr{G},d).$$

Le lecteur savant aura remarqué que $\mathrm{val}(\mathscr{G},<\infty) = \mathrm{val}(\mathscr{G},\mathscr{R})$, si $\mathscr{R}$ est le facteur II_1 hyperfini.

Par la transformée de Fourier, se donner une partition de l'unité $(p_1,\dots,p_n)$ dans $\mathscr{M}$, c'est la même chose que ce donner un unitaire $u = \sum_k e^{2i\pi\frac{k}{n}} p_k \in \mathscr{M}$ vérifiant $u^n = 1$. Se donner une stratégie pour $\mathscr{G}$, c'est donc se donner un unitaire $u(x)$ dans $\mathscr{M}$ d'ordre $|\mathscr{A}|$ pour tout $x \in \mathscr{X}$. Il découle de la définition que $\mathrm{val}(\mathscr{G},\mathscr{S})$ est alors une fonction linéaire des corrélations $\tau(u(x)^k u(y)^\ell)$. Le résultat suivant est donc une forme plus fine du théorème 1.3.

Théorème 2.1. *Il existe une fonction calculable qui à une machine de Turing associe un jeu $\mathscr{G}(M)$ tel que*

$$\mathrm{val}(\mathscr{G}(M),<\infty) \begin{cases} = 1 & \text{si } M \text{ s'arrête,} \\ \leqslant \frac{1}{2} & \text{sinon.} \end{cases}$$

On verra que l'interprétation en termes de jeux à deux joueurs n'est peut-être pas la seule valable. Il est parfois pertinent de voir un jeu comme une manière de définir des algèbres de von Neumann traciales par générateurs et relations. Les jeux fournissent alors un contexte pertinent pour parler de manière quantitative d'approximations de telles algèbres de von Neumann.

Commençons par donner deux exemples très simples mais importants de ce phénomène. Pour ces exemples, comme souvent plus tard, il est plus agréable d'autoriser que l'ensemble des réponses possibles puisse dépendre de la question posée ; autrement dit, $\mathscr{A}$ n'est plus simplement un ensemble fini mais une collection $(\mathscr{A}(x))_{x\in\mathscr{X}}$ d'ensembles finis, et $D(x,y,a,b) \in \{0,1\}$ pour tous $x,y \in \mathscr{X}$ et $a \in \mathscr{A}(x), b \in \mathscr{A}(y)$ [5]. Pour définir un jeu, les valeurs de $D(x,y,\cdot,\cdot)$ pour (x,y) en dehors du support de μ ne jouent aucun rôle ; on se permettra donc de ne pas les définir.

[4] car ici, la stratégie des deux joueurs doivent coïncider : $f = g$.

[5] On retombe sur la notion plus restrictive en choisissant un ensemble fini avec une injection de $\mathscr{A}(x)$ pour tout x, et en déclarant $D = 0$ là où D n'était initialement pas défini.

2.3. Jeu de commutation

Le *jeu de commutation* est le jeu où

- $\mathscr{X} = \{x_1, x_2, y\}$, $\mathscr{A}(x_i) = \{-1, 1\}$ et $\mathscr{A}(y) = \{-1, 1\} \times \{-1, 1\}$,
- $\mu = \frac{1}{2}(\delta_{(x_1,y)} + \delta_{(x_2,y)})$,
- $D(x_1, y, a, (a', b')) = 1_{a=a'}$ et $D(x_2, y, b, (a', b')) = 1_{b=b'}$.

La propriété importante de ce jeu est qu'une stratégie de valeur proche de 1 doit être composée de projections qui commutent presque.

Lemme 2.2. *Le jeu de commutation admet des stratégies parfaites. Si une stratégie a valeur $1 - \varepsilon$ sur le jeu de commutation, alors sa restriction (p_{-1}, p_1) et (q_{-1}, q_1) à x_1 et x_2 respectivement vérifie*

$$\left\| [p_1 - p_{-1}, q_1 - q_{-1}] \right\|_2^2 \leqslant 64\varepsilon. \tag{2}$$

Démonstration. Le jeu a des stratégies parfaites en dimension 1, par exemple $p_1^{x_1} = p_1^{x_2} = p_{1,1}^{y} = 1$ (et tous les autres p_a^x nuls).

Si (p_1, p_{-1}) et (q_1, q_{-1}) est la restriction d'une stratégie de valeur $\geqslant 1 - \varepsilon$, il existe une partition de l'unité $(r_{a,b})_{(a,b)\in\{-1,1\}\times\{-1,1\}}$ telle que

$$\frac{1}{2}\sum_{a,b} \tau(p_a r_{a,b}) + \tau(q_b r_{a,b}) \geqslant 1 - \varepsilon.$$

Définissons $p'_a = r_{a,1} + r_{a,-1}$ et $q'_b = r_{1,b} + r_{-1,b}$. L'inégalité précédente devient $\eta_1 + \eta_2 \leqslant 4\varepsilon$, où $\eta_1 = \sum_a \|p_a - p'_a\|_2^2$ et $\eta_2 = \sum_b \|q_b - q'_b\|_2^2$. Autrement dit, la famille $\{p_a, q_b \mid a, b \in \{-1, 1\}\}$ est proche de la famille $\{p'_a, q'_b \mid a, b \in \{-1, 1\}\}$, qui est constituée de projections qui commutent. Elles commutent donc presque, ce qu'il fallait démontrer. □

2.4. Le jeu d'anticommutation

Le jeu d'anticommutation (ou jeu du carré magique) est un jeu à 15 questions, dont deux spécifiques x_1, x_2 dont les réponses attendues sont $\mathscr{A}(x_1) = \mathscr{A}(x_2) = \{-1, 1\}$. Ce qui est important n'est pas la définition précise du jeu, mais le fait qu'une stratégie à valeur proche de 1 force une forme d'anti-commutation :

Lemme 2.3. *Le jeu d'anticommutation admet des stratégies parfaites en dimension* 4*.*

Si (p_{-1}, p_1) et (q_{-1}, q_1) sont les restrictions à x_1 et x_2 d'une stratégie pour le jeu d'anticommutation de valeur $\geqslant 1 - \varepsilon$, alors

$$\left\| (p_1 - p_{-1})(q_1 - q_{-1}) + (q_1 - q_{-1})(p_1 - p_{-1}) \right\|_2^2 \leqslant 432\varepsilon.$$

Informellement, dans le jeu d'anticommutation, le but des joueurs est de convaincre l'arbitre qu'ils savent remplir un carré 3×3 avec des ± 1, de sorte que le produit des valeurs sur chaque ligne est 1 et sur chaque colonne est -1. Par un argument de parité, il s'agit bien sûr d'une tâche impossible, mais la force de l'intrication quantique (ou de la non-commutativité) est que les joueurs qui partagent suffisamment d'intrication peuvent convaincre l'arbitre qu'ils ont mené à bien cette tâche.

De manière plus précise, le jeu est défini de la façon suivante. L'ensemble des questions est $\mathscr{X} = C \cup L$, l'union disjointe d'un carré 3×3 noté $C = \{1,2,3\}^2$ et de l'ensemble L des lignes et colonnes qui le constituent. Les questions spécifiques sont $x_1 = (1,1) \in C$ et $x_2 = (2,2) \in C$. Définissons $\alpha(\ell) = 1$ pour chaque ligne ℓ et $\alpha(\ell) = -1$ pour chaque colonne ℓ. Pour $c \in C$, on définit $\mathscr{A}(c) = \{-1,1\}$, et pour une ligne ou colonne ℓ, on définit $\mathscr{A}(\ell) \subset \prod_{c\in\ell}\{-1,1\}$ par

$$\mathscr{A}(\ell) = \big\{(b_c)_c \in \{-1,1\}^\ell \big| \prod_{c\in\ell} b_c = \alpha(\ell)\big\}.$$

La distribution μ est la distribution uniforme sur $\{(c,\ell) \mid c \in \ell\}$. Et $D(c,\ell,a,b) = 1_{a=b_c}$.

Preuve du lemme 2.3. Pour définir une stratégie parfaite en dimension 4, il suffit de construire, pour tout $c \in C$, un unitaire auto-adjoint $U_c \in \mathscr{U}(4)$ tel que, pour tout $\ell \in L$, les $(U_c)_{c\in\ell}$ commutent et $\prod_{c\in C} U_c = \alpha(\ell)$. En effet, les projections spectrales $p^c_{\pm 1}$ de U_c ($U_c = p^c_1 - p^c_{-1}$), et $p^\ell_b = \prod_{c\in\ell} p^c_{b_c}$ formeront alors une stratégie parfaite. Pour construire de tels U_c, on considère deux unitaires auto-adjoints de taille 2 σ^X, σ^Z tels que $\sigma^X\sigma^Z = -\sigma^Z\sigma^X$ [6] et on définit les $(U_c)_c$ comme dans la figure 1.

$\sigma^X \otimes 1$	$1 \otimes \sigma^X$	$\sigma^X \otimes \sigma^X$
$1 \otimes \sigma^Z$	$\sigma^Z \otimes 1$	$\sigma^Z \otimes \sigma^Z$
$-\sigma^X \otimes \sigma^Z$	$-\sigma^Z \otimes \sigma^X$	$\sigma^X\sigma^Z \otimes \sigma^Z\sigma^X$

Figure 1 – La stratégie parfaite du jeu d'anticommutation

Une rapide inspection de chaque ligne et chaque colonne permet de se convaincre des propriétés requises.

Soit (p^c_{-1}, p^c_1) (pour $c \in C$) et $(p^\ell_b)_{b\in\mathscr{A}(\ell)}$ (pour $\ell \in L$) une stratégie de valeur $\geqslant 1-\varepsilon$, de sorte que $(p_{-1}, p_1) = (p^{1,1}_{-1}, p^{1,1}_1)$ et $(q_{-1}, q_1) = (p^{2,2}_{-1}, p^{2,2}_1)$. Pour tout $c \in C$, définissons $U^c = p^c_{-1} - p^c_1$. Pour tout $\ell \in L$ et tout $c \in \ell$, on pose

[6] Par exemple les matrices de Pauli $\sigma^X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ et $\sigma^Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

$U^\ell(c) = \sum_{b\in\mathscr{A}(\ell)} b_c p^\ell_b$. Soit

$$\eta_{c,\ell} = \|U^c - U^\ell(c)\|_2 = 2\sqrt{1 - \sum_{b\in\mathscr{A}(\ell)} \tau(p^c_{b_c} p^\ell_b)}.$$

L'hypothèse que la stratégie a valeur $\geqslant 1-\varepsilon$, implique

$$\frac{1}{18}\sum_\ell \sum_{c\in\ell} \eta^2_{c,\ell} = \int \eta^2_{c,\ell} d\mu(c,\ell) \leqslant 4\varepsilon.$$

Et donc, si pour $\ell \in L$ on pose $\eta_\ell = (\sum_{c\in\ell} \eta^2_{c,\ell})^{\frac{1}{2}}$, on obtient

$$\sum_\ell \eta^2_\ell \leqslant 24\varepsilon.$$

Les matrices U^c et U^ℓ_c sont toutes des unitaires auto-adjointes. Par définition de $\mathscr{A}(\ell)$, si c, c', c'' sont les trois points de ℓ, alors $U^\ell(c) = \alpha(\ell) U^\ell(c') U^\ell(c'')$. On en déduit que

$$\|U^c - \alpha(\ell) U^{c'} U^{c''}\|_2 \leqslant \eta_{c,\ell} + \eta_{c',\ell} + \eta_{c'',\ell} \leqslant \sqrt{3}\eta_\ell.$$

Dans ce qui suit, on dénote *hi* la *i*-ème ligne, et *vj* la *j*-ième colonne. On écrira aussi $M \simeq_\delta N$ si $\|M-N\|_2 \leqslant \sqrt{3}\delta$. On a donc

$$\begin{aligned} U^{11}U^{22} &\simeq_{\eta_{h1}+\eta_{v2}} -U^{13}U^{12}U^{12}U^{32} = -U^{13}U^{32} \\ &\simeq_{\eta_{v3}+\eta_{h3}} U^{23}U^{33}U^{33}U^{31} = U^{23}U^{31} \\ &\simeq_{\eta_{h2}+\eta_{v1}} -U^{22}U^{21}U^{21}U^{11} = -U^{22}U^{11}. \end{aligned}$$

On en déduit

$$\|U^{11}U^{22} + U^{22}U^{11}\|_2 \leqslant \sum_\ell \sqrt{3}\eta_\ell \leqslant \sqrt{18\sum_\ell \eta^2_\ell}.$$

Le lemme en découle, puisqu'on a déjà justifié que $\sum_\ell \eta^2_\ell \leqslant 24\varepsilon$, et $18\cdot 24 = 432$. □

2.5. Stabilité

Les jeux de commutation et d'anticommutation ont des points communs, qu'on retrouvera souvent par la suite :

- ▷ ils ont un petit nombre de questions dont on se préoccupe vraiment ; les autres sont seulement là pour garantir de fortes conclusions sur les restrictions à ces questions particulières de bonnes stratégies.
- ▷ ils sont stables, dans le sens où une stratégie de valeur proche de 1 est nécessairement proche d'une stratégie parfaite.

Pour rendre la notion de stabilité précise, il faut savoir comparer des stratégies. Comme dans le cas des résultats de stabilité pour les représentations de groupes (De Chiffre, Ozawa et Thom, 2019 ; Gowers et Hatami, 2017), il est pertinent de s'autoriser à comparer des stratégies de dimensions différentes mais proches. [7]

Définition 2.4. On dit qu'une stratégie $\mathscr{S}' = (q_a^x)_{a\in\mathscr{A}}^{x\in\mathscr{X}} \subset (\mathscr{N}, \tau_{\mathscr{N}})$ pour $\mathscr{G}$ est ε-proche d'une autre stratégie $\mathscr{S} = (p_a^x)_{a\in\mathscr{A}}^{x\in\mathscr{X}} \subset (\mathscr{M}, \tau)$ si :

- ▷ Il existe une projection $e \in \mathscr{M}_\infty = \mathscr{M} \otimes B(\ell_2)$ de trace finie telle que $\mathscr{N} = e\mathscr{M}_\infty e$ avec trace $\tau_{\mathscr{N}} = \frac{1}{\tau\otimes\mathrm{Tr}(e)}\tau \otimes \mathrm{Tr}\big|_{e\mathscr{M}_\infty e}$.
- ▷ Il existe une isométrie partielle $w \in P\mathscr{M}_\infty(1_{\mathscr{M}} \otimes e_{1,1})$ telle que

$$\tau(1 - w^*w) \leqslant \varepsilon, \tau_{\mathscr{N}}(P - ww^*) \leqslant \varepsilon,$$

- ▷ $\mathbf{E}_x \sum_{a\in\mathscr{A}} \|P_a^x - w^*Q_a^x w\|_2^2 \leqslant \varepsilon$, où l'espérance est par rapport à $\frac{1}{2}(\mu_1 + \mu_2)$, la moyenne des deux marginales de μ.

On peut vérifier que si $\mathscr{S}$ et $\mathscr{S}'$ sont ε-proches, alors $\mathrm{val}(\mathscr{G}, \mathscr{S}) - \mathrm{val}(\mathscr{G}, \mathscr{S}') = O(\sqrt{\varepsilon})$.

Définition 2.5. Un jeu $\mathscr{G}$ est stable avec module $\delta\colon [0,1] \to [0,1]$ si toute stratégie pour $\mathscr{G}$ de valeur $\geqslant 1 - \varepsilon$ est $\delta(\varepsilon)$-proche d'une stratégie parfaite.

Une inspection de la preuve des lemmes 2.2 et 2.3 montre que les jeux de commutation et d'anticommutation sont stables avec module $\delta(\varepsilon) = O(\varepsilon)$.

2.6. Compression de jeu, un survol

L'idée principale introduite par Ji et al. (2020a), et l'ingrédient principal dans la preuve du théorème 2.1, est une procédure de *compression d'un jeu*, qui transforme un jeu compliqué à définir en un nouveau jeu, plus simple à définir, mais dont les bonnes stratégies sont elles-mêmes compliquées, et doivent nécessairement encoder de bonnes stratégies pour le jeu original. En un sens, la compression transfère donc de la complexité du côté de la définition d'un jeu vers celui de ses bonnes stratégies.

Pour rendre cette idée de compression plus précise, il faut expliquer comment la complexité d'un jeu est mesurée. La notion précise semblerait artificielle et nécessite un peu de travail pour être définie. Pour se faire une idée, il vaut peut-être mieux commencer par considérer un modèle (trop simpliste pour que ce qui suit puisse être correct), où la complexité naïve d'un jeu $\mathscr{G} = (\mathscr{X}, \mu, \mathscr{A}, D)$ est donnée par deux entiers $m = \lceil \log|\mathscr{X}| \rceil$, $n = \lceil \log|\mathscr{A}| \rceil$, le logarithme du nombre de questions et du nombre de réponses respectivement. Dans ce modèle trop simple, compresser un jeu,

[7] Il pourrait être préférable de parler de stabilité flexible comme dans le cas des groupes, mais c'est la seule notion de stabilité que l'on considèrera dans ce texte.

cela signifie donc réduire le nombre de questions et le nombre de réponses. Il y a pour cela trois étapes distinctes.

Étape 1 (introspection, ou diminution du nombre de questions) : Il s'agit, étant donné un jeu $\mathscr{G}^{(0)}$ de complexité naïve $(m^{(0)}, n^{(0)})$, de définir un nouveau jeu $\mathscr{G}^{(1)}$ de complexité naïve $(m^{(1)} = \mathrm{polylog}(m^{(0)}), n^{(1)} \leqslant m^{(0)} + n^{(0)})$, et qui vérifie la propriété essentielle

$$\mathrm{val}(\mathscr{G}^{(1)}, d) \geqslant 1 - \delta \implies d \geqslant (1-\varepsilon)e^{m^{(0)}} \text{ et } \mathrm{val}(\mathscr{G}^{(0)}, d) \geqslant 1 - \varepsilon$$

pour tout $\delta > 0$ et $d \in \mathbf{N}$, où $\varepsilon = C\delta$ pour une constante C.

Étape 2 (PCP, ou Diminution du nombre de réponses) : Il s'agit, étant donné un jeu $\mathscr{G}^{(1)}$ de complexité naïve $(m^{(1)}, n^{(1)})$, de définir un nouveau jeu $\mathscr{G}^{(2)}$ de complexité naïve $(m^{(2)}, n^{(2)})$ avec $\max(m^{(2)}, n^{(2)}) = \mathrm{poly}(m^{(1)}, \log n^{(1)}))$, et qui vérifie la propriété essentielle

$$\mathrm{val}(\mathscr{G}^{(2)}, d) \geqslant 1 - \gamma \implies \mathrm{val}(\mathscr{G}^{(1)}, d) \geqslant 1 - \delta$$

pour tout $\gamma > 0$ et $d \in \mathbf{N}$, où $\delta = \mathrm{poly}(m^{(1)}, \log n^{(1)})\gamma^c + o(1)$.

En appliquant successivement ces deux étapes, en partant d'un jeu $\mathscr{G}^{(0)}$ de complexité naïve $(n^{(0)}, m^{(0)}) \leqslant N$, on obtiendrait ainsi un jeu $\mathscr{G}^{(2)}$ de complexité naïve $(n^{(2)}, m^{(2)}) \leqslant \mathrm{poly}(\log N)$, et dont les valeurs satisfont

$$\mathrm{val}(\mathscr{G}^{(2)}, d) \geqslant 1 - \frac{1}{(\log N)^C} \implies d \geqslant \frac{1}{2}2^N \text{ et } \mathrm{val}(\mathscr{G}^{(1)}, d) \geqslant \frac{1}{2}.$$

C'est déjà bien car on a significativement diminué la complexité naïve, mais ce n'est pas suffisant, car le but est d'itérer cette procédure de compression, on voudrait donc avoir une implication du type

$$\mathrm{val}(\mathscr{G}^{(2)}, d) \geqslant \frac{1}{2} \implies d \geqslant \frac{1}{2}n^{(0)} \text{ et } \mathrm{val}(\mathscr{G}^{(0)}, d) \geqslant \frac{1}{2}.$$

C'est résolu par la troisième étape.

Étape 3 (Répétition parallèle) : Étant donné un jeu $\mathscr{G}^{(2)}$ de complexité naïve $(n^{(2)}, m^{(2)})$ et un paramètre $\gamma \in (0,1)$, il existe un nouveau jeu $\mathscr{G}^{(3)}$ de complexité naïve $(m^{(3)} = km^{(2)}, n^{(3)} = kn^{(2)})$ avec $k = \mathrm{poly}(m^{(2)}, \frac{1}{\gamma})$, et qui vérifie la propriété

$$\mathrm{val}(\mathscr{G}^{(3)}, d) \geqslant \frac{1}{2} \implies \mathrm{val}(\mathscr{G}^{(2)}, d) \geqslant 1 - \gamma$$

pour tout $d \in \mathbf{N}$.

De ces trois étapes, seule la troisième est valide pour la notion de complexité naïve. Pour les deux premières, il faudra des notions de complexité plus fines pour que les énoncés deviennent corrects. En particulier, pour la deuxième étape, qui repose sur

des variantes du théorème PCP (pour preuve vérifiable de manière probabiliste), la complexité qui entre en jeu sera une forme de complexité algorithmique, qui mesure le temps nécessaire à une machine de Turing pour calculer $D(x, y, a, b)$.

Les preuves de ces trois étapes sont toutes difficiles. La première est celle qui est la plus innovante. Les deux autres s'inspirent de résultats très importants mais antérieurs en informatique théorique : le théorème PCP de Arora, Lund et al. (1998) et Arora et Safra (1998) et le théorème de répétition parallèle de Raz (1998). Le lecteur pourra se plonger dans les exposés de Chazelle (2003) et Pansu (2013) pour en savoir plus sur ces théorèmes et leur pertinence. Pour un mathématicien ignorant de complexité algorithmique comme moi, l'étape la plus difficile est très nettement la deuxième. Et si j'ai lu sa preuve suffisamment longtemps et attentivement pour me convaincre qu'elle est correcte, je ne pense pas avoir vraiment compris ce qui s'y passe. Ce serait très satisfaisant si on pouvait trouver une autre preuve du théorème 1.2 qui reste du côté de la calculabilité et ne fait pas intervenir de notions de complexité algorithmique.

Dans la suite de ce texte, je présenterai rapidement ces trois étapes, et enfin j'expliquerai un peu plus en détails comment, une fois énoncées avec les notions correctes de complexité, elles permettent de prouver le théorème 2.1.

3. Introspection

Dans la suite de l'exposé, on notera $\mathbf{F}_2$ le corps fini à 2 éléments.

La première étape, celle d'introspection, a pour but de transformer un jeu $\mathscr{G}^{(0)}$ en un jeu $\mathscr{G}^{(1)}$ en réduisant de manière exponentielle le nombre de questions, sans trop augmenter le nombre de réponses.

On ne sait mener à bien cette étape d'introspection que pour des jeux dans la distribution de question $\mu^{(0)}$ est très particulière. C'est un problème ouvert intéressant, posé par Ji et al. (2020a), que d'étendre cette procédure d'introspection à des distributions plus générales.

Initialement, les distributions admissibles étaient ce que les auteurs appelaient conditionnellement linéaires, mais une condition plus générale et un peu plus facile à définir est suffisante : pour un entier N, il existe deux partitions $(E_x)_{x\in\mathscr{X}^{(0)}}$ et $(F_x)_{x\in\mathscr{X}^{(0)}}$ de $\mathbf{F}_2^N$ en sous-espaces affines tels que $\mu^{(0)}(x, y) = 2^{-N}|E_x \cap F_y|$. On dira donc qu'un jeu est de complexité de questions N si la distribution de questions est de cette forme. Le nombre de questions $m^{(0)}$ de $\mathscr{G}^{(0)}$ est alors au plus 2^N ; le paramètre N joue donc le rôle de $m^{(0)}$ dans la section précédente.

De manière un peu plus concrète, en suivant le principe général, le jeu $\mathscr{G}^{(1)}$ aura deux questions centrales « Introspecte-toi ! (1) » et « Introspecte-toi ! (2) », dont la réponse attendue est une paire $(x, a) \in \mathscr{X}^{(0)} \times \mathscr{A}^{(0)}$. Le reste des questions est là pour s'arranger qu'une bonne stratégie pour ce jeu est nécessairement, pour ces questions,

de la forme $q_x^1 \otimes p_a^x$ et $q_x^2 \otimes p_a^x$ pour des partitions de l'unité $(q_x^1)_{x\in\mathscr{X}}$ et $(q_x^2)_{x\in\mathscr{X}}$ vérifiant $\tau(q_x^1 q_y^2) = \mu(x,y)$, et une bonne stratégie p pour $\mathscr{G}^{(0)}$. On peut aussi reformuler ce qui précède dans le langage ludique : en posant la question « Introspecte-toi ! (1) », l'arbitre demande au joueur de générer pour lui-même une paire de questions (x,y) selon la distribution μ, de ne retenir que la première question x, d'y répondre honnêtement a et de lui renvoyer la paire (x,a). Symétriquement pour le deuxième joueur. Une stratégie de la forme $q_x^1 \otimes p_a^x$ et $q_x^2 \otimes p_a^x$ est ce qu'on appelle une stratégie honnête ; toutes les autres questions sont là pour s'arranger pour que les joueurs n'ont pas la possibilité de tricher et n'ont d'autre choix que de suivre une stratégie qui est proche d'une stratégie honnête.

Pour obtenir cela, on utilisera un résultat de stabilité pour les groupes de Heisenberg sur le corps à deux éléments $\mathbf{F}_2$,

$$H_{2N+1} = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1_N & b \\ 0 & 0 & 1 \end{pmatrix} \right\} \subset \mathrm{GL}_{N+2}(\mathbf{F}_2).$$

Le groupe H_{2N+1} est une extension centrale de $\mathbf{F}_2^{2N}$ par $\mathbf{F}_2$. Sa théorie des représentations est très singulière. Il a 2^{2N} représentations irréductibles de dimension 1 : celles qui sont triviales sur le centre et proviennent donc de représentations du groupe abélien $\mathbf{F}_2^{2N}$. Il a une seule représentation irréductible qui n'est pas triviale sur le centre. Elle est de dimension 2^N et le centre agit par $\{\mathrm{id}, -\mathrm{id}\}$. Elle peut aussi être décrite par deux représentations unitaires $\sigma^X, \sigma^Z \colon \mathbf{F}_2^N \to \mathscr{U}(2^N)$ qui vérifient

$$\sigma^X(a)\sigma^Z(b) = (-1)^{\sum_i a_i b_i} \sigma^Z(b)\sigma^X(a).$$

Autrement dit, les unitaires $\sigma^X(a)$ et $\sigma^Z(b)$ commutent ou anti-commutent selon la valeur de $\langle a,b\rangle := \sum_i a_i b_i \in \mathbf{F}_2$. Comme la notation l'indique, ces représentations peuvent être réalisées à l'aide des matrices de Pauli

$$\sigma^X(a) = \otimes_{i=1}^n (\sigma^X)^{a_i}, \quad \sigma^Z(b) = \otimes_{i=1}^n (\sigma^Z)^{b_i}.$$

Notons $(\tau_a^X)_{a\in\widehat{\mathbf{F}_2^N}}$ et $(\tau_a^Z)_{a\in\widehat{\mathbf{F}_2^N}}$ les partitions de l'unité correspondant, via la transformée de Fourier, aux représentations σ^X et σ^Z.

En combinant les jeux de commutation ou d'anticommutation, on peut produire un jeu qui prend en compte cette représentation, et de manière économique en termes de questions.

Théorème 3.1. *Pout tout entier N, il existe un jeu $\mathscr{G}_N$ de complexité de questions $O(\log N)$, avec $|\mathscr{A}| = 2^N$. Il a deux questions particulières $X, Z \in \mathscr{X}_N$ vérifiant $\mu_N(X) = \mu_N(Z) = \frac{1}{4}$, et $\mathscr{A}(x) = \mathscr{A}(z) = \mathbf{F}_2^N$. Ce jeu est stable avec module $\varepsilon \mapsto O(\varepsilon)$. De plus, toute stratégie parfaite est sur une algèbre de la forme $(M_{2^N}(\mathbf{C}) \otimes \mathscr{N}, \mathrm{tr} \otimes \tau')$ où $p_a^X = \tau_a^X \otimes 1_{\mathscr{N}}$ et $p_b^Z = \tau_b^Z \otimes 1_{\mathscr{N}}$ pour tout $a, b \in \mathbf{F}_2^N$.*

En particulier, une stratégie de dimension finie et de valeur $\geqslant 1-\varepsilon$ doit être en dimension $\geqslant (1-O(\varepsilon))2^N$ (et même en dimension $O(\varepsilon)$-proche d'un multiple de 2^N).

Toute la force de l'étape d'introspection est contenue dans ce résultat : il y a besoin d'un nombre polynomial de questions, la dimension nécessaire des bonnes stratégies est exponentielle, la stabilité est de module linéaire.

Une autre propriété importante pour l'utilisation de ce résultat pour l'introspection est qu'en restriction à la question X, une bonne stratégie pour $\mathscr{G}$ contient en particulier un générateur de variable aléatoire presque uniforme dans $\mathbf{F}_2^N$ (simplement parce que $\mathrm{tr}(\tau_a^X) = 2^{-N}$ pour tout $a \in \mathbf{F}_2^N$). Il est donc possible pour les joueurs d'utiliser cette source d'aléa d'origine quantique pour engendrer les variables aléatoires de loi $\mu^{(0)}$, et on peut définir un jeu qui force les joueurs à le faire. Pour cela, nous allons voir qu'il suffit d'ajouter un petit nombre (6) de questions à $\mathscr{G}_N$ pour obtenir un nouveau jeu qui permet de mener à bien l'étape d'introspection.

Proposition 3.2. *Étant données deux partitions $\underline{E} = (E_x)_{x\in\mathscr{X}^{(0)}}$ et $\underline{F} = (F_x)_{x\in\mathscr{X}^{(0)}}$ de $\mathbf{F}_2^N$ en sous-espaces affines et un ensemble $\mathscr{A}$, il existe un jeu $\mathscr{G}$ de complexité de questions $O(\log N)$ et avec $\leqslant 2^N|\mathscr{A}|$ réponses qui est stable avec module $\varepsilon \mapsto O(\varepsilon)$. De plus, il a deux questions particulières $I1, I2$ telles que $\mu(I1) = \mu(I2) \geqslant c$ (pour un c indépendant de N), dont les réponses possibles sont $\mathscr{X}\times\mathscr{A}$, et telle que toute stratégie parfaite est, en restriction à $I1$, $I2$, de la forme $(\sum_{v\in E_x}\tau_v^X)\otimes p_a^x$, et $(\sum_{v\in F_x}\tau_v^X)\otimes p_a^x$ pour des partitions de l'unité $(p_a^x)_{a\in\mathscr{A}}$ pour tout $x\in\mathscr{X}^{(0)}$.*

Les partitions $q_x^1 = \sum_{v\in E_x}\tau_v^X$ et $q_x^2 = \sum_{v\in F_x}\tau_v^X$ vérifient bien $\mathrm{tr}(q_x^1 q_y^2) = 2^{-N}|E_x\cap F_y|$. Si on partait d'un jeu $\mathscr{G}^{(0)}$ dont la distribution de questions est donnée par les partitions $\underline{E}$ et $\underline{F}$, en ajoutant au jeu obtenu dans la proposition 3.2 la paire de questions $(I1, I2)$ posée avec probabilité $\geqslant c$, avec fonction de décision $D(I1, I2, (x,a), (y,b)) = D^{(0)}(x,y,a,b)$, on obtient bien un jeu qui vérifie, pour notre notion un peu plus précise de la complexité des questions, la conclusion de la partie introspection de la partie 2.6.

La raison pour laquelle on peut traiter des partitions en sous-espaces affines (mais pas en parties arbitraires) est donnée par la direction « si » (respectivement « seulement si ») du lemme suivant. Dans ce lemme, pour une partie $E \subset \mathbf{F}_2^N$, on note $E_0 = \{a \in \mathbf{F}_2^N \mid a + E = E\}$ le plus grand sous-espace vectoriel tel que E est une union d'espaces affines parallèles à E_0. Par exemple, si E est un sous-espace affine, E_0 est sa partie linéaire. On notera $\cdot^\perp$ l'orthogonal pour la forme $\langle a, b\rangle = \sum_i a_i b_i$.

Lemme 3.3. *Étant données deux parties $E, F \subset \mathbf{F}_2^N$, les projections $\sum_{v\in E}\tau_v^X$ et $\sum_{v\in F}\tau_v^Z = 0$ commutent si et seulement si $E_0^\perp \subset F_0$.*

Pour expliquer comment cette propriété de commutation intervient, donnons la description explicite d'un jeu $\mathscr{G}(\underline{E})$ qui ne dépend que d'une partition, avec une seule

question d'introspection I, et qui vérifie l'analogue de la conclusion de la proposition 3.2 : en restriction à I ses stratégies parfaites sont de la forme $(\sum_{v\in E_x}\tau_v^X)\otimes p_a^{1,x}$ pour une partition de l'unité $(p_a^x)_{a\in\mathscr{A}}$ pour tout $x\in\mathscr{X}^{(0)}$. Une petite modification permet d'obtenir la proposition 3.2.

L'ensemble des questions de $\mathscr{G}(\underline{E})$ est $\mathscr{X}_N\cup\{E,I,L\}$ (pour Échantillonne, Introspecte et Lis). La mesure μ est $\frac{1}{2}(\mu_N+\mu')$ où μ' est la mesure uniforme sur l'ensemble des quatre arêtes de la figure 2. [8]

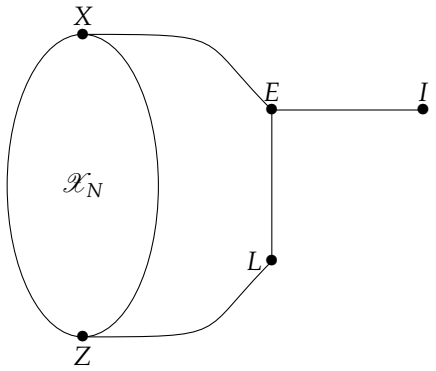

Figure 2 – Les questions du jeu $\mathscr{G}(\underline{E})$

L'ensemble des réponses possibles pour chaque question est

- $\mathscr{A}(x)=\mathscr{A}_N(x)$ si $x\in\mathscr{X}_N$,
- $\mathscr{A}(E)=\{(w,a)\mid w\in\mathbf{F}_2^N, a\in\mathscr{A}\}$,
- $\mathscr{A}(I)=\{(x,b)\mid x\in\mathscr{X}^{(0)}, b\in\mathscr{A}\}$,
- $\mathscr{A}(L)=\{(y,\varphi,c)\mid x\in\mathscr{X}^{(0)},\varphi\in(E_x)_0^*, a\in\mathscr{A}\}$.

La fonction de décision est

- $D=D_N$ en restriction à $\mathscr{G}_N$,
- $D(X,E,w,(v,a))=1_{v=w}$,
- $D(E,I,(v,a),(x,b))=1_{a=b}1_{v\in E_x}$,
- $D(E,L,(v,a),(y,\varphi,c))=1_{a=c}1_{v\in E_y}$,
- $D(L,Z,(y,\varphi,c),w)=1_{\varphi(v)=\langle v,w\rangle\forall v\in(E_y)_0}$.

Voyons comment construire des stratégies parfaites pour le jeu $\mathscr{G}(\underline{E})$. Commençons par une stratégie parfaite q pour $\mathscr{G}_N$; par le théorème 3.1 elle est sur une algèbre de la

[8] Le lecteur attentif remarquera que cette mesure n'est pas de la forme discutée précédemment, mais une petite modification qui n'affecte pas ce qui suit permet de s'y ramener, c'est le contenu de Ji et al., 2020a, §6.3.

forme $M_{2^N}(\mathbf{C}) \otimes \mathscr{N}$ et en restriction à X, Z elle est de la forme $\tau_a^X \otimes 1_{\mathscr{N}}$ et $\tau_a^Z \otimes 1_{\mathscr{N}}$. Alors, pour toute famille $\{(p_a^x)_{a\in\mathscr{A}} \mid x \in \mathscr{X}^{(0)}\}$ de partitions de l'unité dans $(\mathscr{N}, \tau)$, on peut étendre cette stratégie parfaite de $\mathscr{G}_N$ en une stratégie parfaite de $\mathscr{G}(\underline{E})$, en posant

- ▷ $q^E_{w,a} = \tau^X_w \otimes p^x_a$ où $x \in \mathscr{X}^{(0)}$ est caractérisé par $w \in E_x$,
- ▷ $q^I_{x,a} = (\sum_{x\in E_x} \tau^X_w) \otimes p^x_a$,
- ▷ $q^L_{y,\varphi,c} = (\sum_{x\in E_y} \tau^X_w)(\sum_{w|\langle v,w\rangle=\varphi(v)\forall v\in E_{y,0}} \tau^Z_w) \otimes p^x_c$.

Le seul point qui mérite une justification est le fait que q^L est bien constitué de projections, c'est-à-dire que les deux projections $\sum_{x\in E_y} \tau^X_w$ et $\sum_{w|\langle v,w\rangle=\varphi(v)\forall v\in E_{y,0}} \tau^Z_w$ commutent. C'est justifié par le petit résultat d'algèbre linéaire du lemme 3.3. Il est alors immédiat de vérifier que cette stratégie est parfaite pour $\mathscr{G}(\underline{E})$.

Réciproquement, il n'est pas bien dur (on n'a ajouté que 3 questions) de déduire de la stabilité de $\mathscr{G}_N$ la stabilité de $\mathscr{G}(\underline{E})$.

4. PCP

La deuxième étape, celle de vérification probabiliste de preuve, a pour but de transformer un jeu $\mathscr{G}^{(1)}$ en un jeu $\mathscr{G}^{(2)}$ en réduisant le nombre de réponses, sans trop augmenter le nombre de questions.

De manière concrète, certaines des questions du jeu seront « Si la paire de questions posée était (x, y), donne-moi une preuve courte que tu es capable de produire (a, b) tel que $D(x, y, a, b) = 1$. » Les autres questions sont là pour garantir que les joueurs n'ont d'autre choix que de jouer honnêtement. Pour cela, l'argument repose de manière essentielle sur des idées qui sont devenues classiques en informatique théorique : le théorème PCP (pour preuve vérifiable de manière probabiliste), qui de manière informelle affirme qu'un problème de décision NP peut être vérifié de façon probabiliste en ayant accès à un nombre constant de bits de la preuve et en utilisant un nombre logarithmique de bits aléatoires. Ici le problème de décision est « déterminer s'il existe (a, b) tel que $D(x, y, a, b) = 1$ », il est donc naturel que la complexité d'un jeu soit mesurée par la complexité algorithmique de la fonction D plutôt que par le nombre de réponses.

Pour définir de manière plus précise cette notion de complexité, il vaut mieux changer légèrement la définition d'un jeu. Un jeu devient donc la donnée de $(\mathscr{X}, \mu, \mathscr{A}, \mathscr{D})$ où $\mathscr{X}, \mathscr{A}$ sont des ensembles de la forme $\mathbf{F}_2^k, \mathbf{F}_2^\ell$, μ est une distribution de la forme considérée dans la section d'introspection, et $\mathscr{D}$ est une machine de Turing à 4 entrées. Cela donne lieu à un jeu dans le sens précédent si $\mathscr{D}$ a la propriété que $\mathscr{D}$ termine quand elle prend pour argument $(x, y, a, b) \in \mathscr{X} \times \mathscr{X} \times \mathscr{A} \times \mathscr{A}$, et renvoie un élément de $\{0, 1\}$. La complexité de la fonction de décision est mesurée par deux paramètres : la taille de la description de $\mathscr{D}$, et le temps maximum d'exécution de

$\mathscr{D}$ lorsque x, y, a, b varient. Pour prendre en compte l'étape d'introspection où la distribution des questions devient encodée dans la fonction de décision, il faudra aussi mesurer la complexité algorithmique nécessaire pour décrire la mesure μ, mais on ignorera ce point pour simplifier.

Pour mettre en place les idées du théorème PCP classique dans le contexte de jeux et de leurs stratégies quantiques, cette deuxième étape repose sur un autre énoncé particulièrement délicat de stabilité quantitative pour certains jeux très particuliers, obtenu dans Ji et al. (2020b, 2022) pour palier à l'erreur critique qu'ils avaient trouvée dans la preuve de Vidick (2016, 2020). L'énoncé précis est très technique et long à énoncer, il ne sera pas reproduit ici.

Dans Ji et al. (2020a), ce théorème de stabilité était aussi utilisé pour obtenir une forme du théorème 3.1 un peu plus faible mais suffisante. L'amélioration et la simplification présentée dans le théorème 3.1, qui a été obtenue dans de la Salle (2022), repose sur des arguments plus élémentaires de graphes expanseurs et de stabilité pour les groupes.

5. Répétition parallèle

Étant donné un jeu $\mathscr{G} = (\mathscr{X}, \mathscr{A}, \mu, D)$ et un entier $n \geqslant 1$, la répétition en parallèle n fois de $\mathscr{G}$ est le jeu

$$\mathscr{G}^n = (\mathscr{X}^n, \mathscr{A}^n, \mu^{\otimes n}, D^{\otimes n})$$

où

$$D^{\otimes n}\big((x_i)_{i=1}^n, (y_i)_{i=1}^n, (a_i)_{i=1}^n, (b_i)_{i=1}^n\big) = \prod_{i=1}^n D(x_i, y_i, a_i, b_i).$$

Le premier réflexe naïf est de s'attendre à ce que la valeur de $\mathscr{G}^n$ est la puissance n-ième de la valeur de $\mathscr{G}$. C'est faux : il existe un jeu très simple dont la valeur classique (au sens de la sous-section 2.1) et la valeur classique de $\mathscr{G}^2$ sont toutes les deux égales à $\frac{1}{2}$ (Aubrun, 2021, Example 1). Le théorème de répétition parallèle de Raz (1998) affirme que, pour tout jeu de valeur < 1, la valeur classique de $\mathscr{G}^n$ décroît exponentiellement avec n, à un taux qui ne dépend que du nombre de réponses et de la valeur classique. Plus précisément, il affirme que si $\mathscr{G}$ a valeur classique $\leqslant 1 - \varepsilon$, alors $\mathscr{G}^n$ a valeur classique $\leqslant C\exp(-C\varepsilon^{32}n/\log\mathscr{A})$ pour une constante C explicite. Il y a maintenant de nombreuses preuves de cet énoncé, où la constante 32 peut être abaissée à 3. J'apprécie particulièrement la présentation de Aubrun (2021).

La question de savoir si le théorème de répétition parallèle est vrai pour les différentes valeurs quantiques d'un jeu reste un problème ouvert. Une forme a été obtenue par Bavarian, Vidick et Yuen (2022), suffisante pour ce qui suit. Il s'applique à certains types de jeu, appelés des jeux ancrés.

Étant donné un jeu $\mathscr{G} = (\mathscr{X}, \mathscr{A}, \mu, D)$, on peut définir un nouveau jeu $\widetilde{\mathscr{G}} = (\widetilde{\mathscr{X}}, \widetilde{\mathscr{A}}, \widetilde{\mu}, \widetilde{D})$, dit *ancré*, de la manière suivante : $\widetilde{\mathscr{X}} = \mathscr{X} \cup \{\perp\}$, $\widetilde{\mathscr{A}} = \mathscr{A}$,

$$\widetilde{\mu} = \frac{1}{4}\sum_{x,y} \mu(x,y)(\delta_{(x,y)} + \delta_{(\perp,y)} + \delta_{(x,\perp)} + \delta_{(\perp,\perp)})$$

et

$$\widetilde{D}(x,y,a,b) = \begin{cases} D(x,y,a,b) & \text{si } x,y \in \mathscr{X} \\ 1 & \text{si } x = \perp \text{ ou } y = \perp . \end{cases}$$

Autrement dit, on a ajouté une question $\perp$ qui est toujours gagnante, et pour engendrer une paire de questions pour $\widetilde{\mathscr{G}}$, l'arbitre commence par tirer au hasard une paire de questions (x,y) pour $\mathscr{G}$, et indépendamment avec probabilité $\frac{1}{2}$, remplace chaque question par la question gagnante.

Le théorème de répétition parallèle quantique qui suit ne s'applique que pour des jeux qu'on appellera paresseux (en référence aux marches aléatoires paresseuses) si $\mu(x,x) \geqslant \sum_{y \neq x} \frac{1}{2}(\mu(x,y) + \mu(y,x))$ pour tout $x \in \mathscr{X}$. Si $\mathscr{G}$ est un jeu arbitraire, le nouveau jeu ou l'on remplace μ par $\frac{1}{2}(\mu + \sum_{x,y} \frac{1}{2}(\mu(x,y) + \mu(y,x))\delta_{(x,x)})$ est un jeu paresseux.

Théorème 5.1. *Il existe une constante C telle que pour tout jeu paresseux $\mathscr{G} = (\mathscr{X}, \mathscr{A}, \mu, D)$ et tout entier d,*

$$\mathrm{val}((\widetilde{\mathscr{G}})^n, d) \leqslant C \exp\Big(-\frac{(1 - \mathrm{val}(\mathscr{G}, d))^C}{C \log |\mathscr{A}|} n\Big).$$

Démonstration. Ce théorème est le seul pour lequel la notion plus restrictive de stratégie que l'on considère rend les choses un tout petit peu plus difficiles. En effet, on peut définir la valeur asynchrone et de dimension d d'un jeu $\mathscr{G}$, notée $\mathrm{val}_{\mathrm{async}}(\mathscr{G}, d)$, comme le maximum de la quantité (1) où $\mathscr{H} = \mathbf{C}^{d^2}$. Alors le travail très difficile de Bavarian, Vidick et Yuen (2022) démontre exactement ce théorème pour la valeur asynchrone, sans l'hypothèse que le jeu soit paresseux. Le théorème pour la valeur (synchrone) considérée dans ce texte découle du résultat beaucoup plus facile par Vidick (2022a), qui affirme que, si $\mathscr{G}$ est un jeu paresseux, alors

$$\mathrm{val}_{\mathrm{async}}(\mathscr{G}, d) \geqslant 1 - \varepsilon \implies \mathrm{val}(\mathscr{G}, d) \geqslant 1 - K\varepsilon^{\frac{1}{K}}$$

pour tout entier d et tout $\varepsilon \geqslant 0$, où K est une constante universelle. Il est peut-être important de noter que c'est pour cette dernière inégalité que j'ai choisi d'autoriser des stratégies à valeurs $M_k(\mathbf{C})$ pour $k \leqslant d$ (et pas seulement dans $M_d(\mathbf{C})$) dans la définition de $\mathrm{val}(\mathscr{G}, d)$. □

6. Le théorème de compression

Il est maintenant temps d'énoncer une forme précise du théorème de compression, qui peut être obtenu en combinant avec soin les trois étapes qui ont été superficiellement évoquées ci-dessus. Pour son utilisation ultérieure, le théorème de compression sera donné non pas pour des jeux individuels, mais pour des familles de jeux qui sont données de manière uniforme par une machine de Turing.

Une propriété des jeux construits dans l'étape d'introspection est que la distribution de questions ne dépend que de l'entier N, et pas de la distribution des questions $\mu^{(0)}$ du jeu $\mathscr{G}^{(0)}$. En exploitant cette propriété, on peut donc mettre en place un théorème de compression où la suite des distributions de questions est une suite fixée de plus en plus complexe, et les réponses possibles sont également fixées. Autrement dit, on construit une suite explicite $(\mathscr{X}_n, \mu_n, \mathscr{A}_n)$ (des jeux dont il manque la fonction de décision) où la mesure μ_n est donnée comme dans la section 3 par deux partitions de $\mathbf{F}_2^{N_n}$, pour une suite bien choisie d'entiers N_n qui tend vers l'infini. [9]

On considère alors l'ensemble $\mathscr{E}$ des machines de Turing à 2 entrées, qu'on appellera les décideurs. Un décideur $\mathscr{D}$ de $\mathscr{E}$ sera valable si pour tout n, tout $z = (x, y, a, b) \in \mathscr{X}_n \times \mathscr{X}_n \times \mathscr{A}_n \times \mathscr{A}_n$, $\mathscr{D}(n, z)$ termine et renvoie un élément de $\{0, 1\}$. On notera $\mathrm{Temps}_n(\mathscr{D})$ le maximum pour tout z du temps de calcul de $\mathscr{D}(n, z)$. Un décideur valable permet donc de définir une suite de jeux $\mathscr{G}_n(\mathscr{D}) = (\mathscr{X}_n, \mu_n, \mathscr{A}_n, \mathscr{D}(n, \cdot))$.

Théorème 6.1 (Théorème de compression). *Il existe une machine de Turing* $\mathrm{COMPRESS} : \mathscr{E} \to \mathscr{E}$ *de complexité polynomiale et une autre machine de Turing* $f : \mathscr{E} \to \mathbf{N}$ *telle que, pour tout* $\mathscr{D} \in \mathscr{E}$, $\mathscr{D}' = \mathrm{COMPRESS}(\mathscr{D})$ *vérifie les propriétés suivantes :*

- $\mathscr{D}'$ *est valable et de complexité* $\mathrm{Temps}_n(\mathscr{D}') \leqslant \mathrm{poly}(N_n)$ *pour tout* n.
- *si* $\mathscr{D}$ *est valable alors pour tout* $n \geqslant f(\mathscr{D})$ *tel que* $\mathrm{Temps}_n(\mathscr{D}) \leqslant N_n^n$, *on a les deux implications suivantes :*
  1. *si* $\mathscr{G}_n(\mathscr{D})$ *a une stratégie parfaite commutative* [10] *de dimension finie, alors* $\mathscr{G}_{n-1}(\mathscr{D}')$ *aussi.*
  2. *si* $\mathrm{val}(\mathscr{G}_{n-1}(\mathscr{D}'), d) > \frac{1}{2}$, *alors* $d \geqslant N_n$ *et* $\mathrm{val}(\mathscr{G}_n(\mathscr{D}), d) > \frac{1}{2}$.

Expliquons comment le théorème de compression permet de déduire le théorème principal, le théorème 2.1. On définit une nouvelle machine de Turing F à 4 entrées (interprétées comme (R, M, n, z) avec R une machine de Turing à 4 entrées, M une machine de Turing à 0 entrée, n un entier et $z \in \mathscr{X}_n \times \mathscr{X}_n \times \mathscr{A}_n \times \mathscr{A}_n$) de la façon suivante :

[9] Informellement, la compression transforme un jeu de complexité N en un jeu de complexité $\mathrm{polylog} N$. Il n'est donc pas surprenant qu'un choix possible est de prendre pour N_n qui croît presque comme une tour d'exponentielles, mais avec $\log N_{n+1} = o(N_n^\varepsilon)$ pour tout $\varepsilon > 0$. Par exemple, $N_n = a_n^n$ où $a_1 = 1$ et $a_{n+1} = 2^{a_n}$.

[10] Une stratégie p pour un jeu $\mathscr{G} = (\mathscr{X}, \mu, \mathscr{A}, D)$ est dite commutative si pour tout (x, y) dans le support de μ, et tout $a, b \in \mathscr{A}$, $[p_a^x, p_b^y] = 0$

```
1 Exécute M pendant n étapes ;
2 Si l'exécution s'est arrêtée, retourne F(R,M,n,z)=1 ;
3 Sinon, continue ;
4 Définis un décideur D(n',z')=R(R,M,n',z') ;
5 Calcule D'=COMPRESS(D) ;
6 Retourne D'(n,z).
```

Les étapes 4 et 5 sont des instructions de haut niveau, du type *exécute telle machine de Turing dont le code a été donné en argument, ou bien dont le code a été calculé précédemment, avec telle autre entrée* ; une façon de les rendre précises est d'utiliser des machines de Turing universelles, qui en entrée une paire (M, x) où M est une machine de Turing et x une entrée possible de M, retourne le résultat de $M(x)$ si le calcul de $M(x)$ s'arrête, et tourne indéfiniment sinon. Un point important (mais apparemment absent de la littérature sur les machines de Turing) est qu'il est possible de définir une telle machine de Turing universelle de sorte que son temps de calcul en l'entrée (M, x) est au plus polynomial en $|M|, |x|$ et en le temps de calcul de $M(x)$. On déduit de tout cela, du fait que COMPRESS est de complexité polynomiale et du fait que $\mathrm{Temps}_n(\mathscr{D}') \leqslant \mathrm{poly}(N_n)$ dans le théorème 6.1, que le calcul de $F(R, M, n, z)$ termine toujours en temps $\leqslant \mathrm{poly}(n, |R|, |M|, N_n)$ et renvoie toujours 0 ou 1. En particulier, ce temps d'exécution est $\leqslant N_n^n$ pour tout n assez grand, calculable en termes de $|R|$ et $|M|$.

La fonction calculable du théorème 2.1 est alors définie de la manière suivante. Étant donnée une machine de Turing M à 0 entrée :

```
7 Définis un décideur D(M) par D(M)(n,z) = F(F,M,n,z) ;
8 Calcule N >= f(D(M)) tel que Temps_n(D(M))< N_n^n pour tout n>=N ;
9 Retourne le jeu G_N(D(M)).
```

Là encore, l'étape 7 peut être rendue précise en utilisant une machine de Turing universelle. Le fait que l'étape 8 est toujours faisable découle de la discussion qui suit la description du programme F.

Vérifions la conclusion du théorème 2.1. Soit $n_0 \in \mathbf{N}^* \cup \{\infty\}$ le temps d'arrêt de M. L'observation cruciale est que, lorsque dans la ligne 7 on appelle la fonction $F(F, M, n, z)$, pour un $n < n_0$, le décideur $\mathscr{D}$ qui est calculé dans la ligne 4 du code de F est le décideur $\mathscr{D}(M)$ lui-même. Et donc, si on note $\mathscr{D}'(M) = \mathrm{COMPRESS}(\mathscr{D}(M))$, alors $\mathscr{G}_n(\mathscr{D}(M)) = \mathscr{G}_n(\mathscr{D}'(M))$ pour tout $n < n_0$. En appliquant le théorème 6.1 on obtient donc que, si N est l'entier calculé à l'étape 8, on a pour tout entier n tel que $N \leqslant n < n_0$,

(1) si $\mathscr{G}_{n+1}(\mathscr{D}(M))$ a une stratégie parfaite commutative de dimension finie, alors $\mathscr{G}_n(\mathscr{D}(M))$ aussi.

(2) si $\mathrm{val}(\mathscr{G}_n(\mathscr{D}(M)), d) > \frac{1}{2}$, alors $d \geqslant N_{n+1}$ et $\mathrm{val}(\mathscr{G}_{n+1}(\mathscr{D}(M)), d) > \frac{1}{2}$.

Supposons tout d'abord que M s'arrête, c'est-à-dire $n_0 < \infty$. Il s'agit de montrer que $\mathscr{G}_N(D(M))$ a une stratégie parfaite commutative de dimension finie. Alors par définition de la machine de Turing F, pour tout $n \geqslant n_0$, le décideur $\mathscr{D}(M)$ est trivial dans le sens ou $\mathscr{D}(M)(n,z) = 1$ pour tout z. En particulier, le jeu $\mathscr{G}_n(\mathscr{D}(M))$ a une stratégie parfaite commutative de dimension 1 pour tout $n \geqslant n_0$. Si $n_0 \leqslant N$ on a donc fini. Sinon, par le point (1), on obtient que le jeu $\mathscr{G}_{n_0-1}(\mathscr{D}(M))$ a une stratégie parfaite commutative, et donc aussi le jeu $\mathscr{G}_{n_0-2}(D(M))$, etc. Par récurrence on en déduit que c'est le cas du jeu $\mathscr{G}_n(D(M))$ pour tout $n \geqslant N$, et en particulier pour $n = N$.

Supposons maintenant que M ne s'arrête pas, c'est-à-dire $n_0 = \infty$. Supposons par l'absurde que $\mathrm{val}(\mathscr{G}_N(D(M)), <\infty) > \frac{1}{2}$. Il existe un entier d tel que $\mathrm{val}(\mathscr{G}_N(D(M)), d) > \frac{1}{2}$. Par le point (2), on en déduit que $d \geqslant N_{N+1}$ et $\mathrm{val}(\mathscr{G}_{N+1}(D(M)), d) > \frac{1}{2}$. Par récurrence, on en déduit que $d \geqslant N_n$ et $\mathrm{val}(\mathscr{G}_n(D(M)), d) > \frac{1}{2}$ pour tout $n > N$. Comme $\lim_n N_n = \infty$, on obtient une contradiction. Cela conclut donc la preuve du théorème 2.1.

Références

Arora, S., Lund, C. et al. (1998). « Proof verification and the hardness of approximation problems », *J. ACM* **45** (3), p. 501-555.

Arora, S. et Safra, S. (1998). « Probabilistic checking of proofs : a new characterization of NP », *J. ACM* **45** (1), p. 70-122.

Aubrun, G. (2021). « The Parallel repetition theorem », *Notes disponibles sur la page web de l'auteur*.

Bavarian, M., Vidick, T. et Yuen, H. (2022). « Anchored parallel repetition for nonlocal games », *SIAM J. Comput.* **51** (2), p. 214-253.

Bekka, B., Harpe, P. de la et Valette, A. (2008). *Kazhdan's property* (T). T. 11. New Mathematical Monographs. Cambridge University Press, Cambridge, p. xiv+472.

Ben-Or, M. et al. (1988). « Multi-Prover Interactive Proofs : How to Remove Intractability Assumptions ». In : *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*. Sous la dir. de J. Simon. ACM, p. 113-131.

Chazelle, B. (2003). « The PCP theorem [after Arora, Lund, Motwani, Safra, Sudan, Szegedy] », in : Astérisque 290. Séminaire Bourbaki. Vol. 2001/2002, Exp. No. 895, vii, 19-36.

Connes, A. (1976). « Classification of injective factors. Cases II_1, II_∞, III_λ, $\lambda \neq 1$ », *Ann. of Math.* (2) **104** (1), p. 73-115.

De Chiffre, M., Ozawa, N. et Thom, A. (2019). « Operator algebraic approach to inverse and stability theorems for amenable groups », *Mathematika* **65** (1), p. 98-118.

Fritz, T. (2012). « Tsirelson's problem and Kirchberg's conjecture », *Rev. Math. Phys.* **24** (5), p. 1250012, 67.

Gowers, W. T. et Hatami, O. (2017). « Inverse and stability theorems for approximate representations of finite groups », *Mat. Sb.* **208** (12), p. 70-106.

Ji, Z. et al. (2020a). « MIP*=RE ». arXiv.

——— (2020b). « Quantum soundness of the classical low individual degree test ». arXiv.

——— (2022). « Quantum soundness of testing tensor codes », *Discrete Analysis* **17**, 73 pp.

Junge, M. et al. (2011). « Connes embedding problem and Tsirelson's problem », *J. Math. Phys.* **52** (1), p. 012102, 12.

Kirchberg, E. (1993). « On nonsemisplit extensions, tensor products and exactness of group C^*-algebras », *Invent. Math.* **112** (3), p. 449-489.

Natarajan, A. et Wright, J. (2019). « NEEXP is contained in MIP », in : *2019 IEEE 60th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press, Los Alamitos, CA, p. 510-518.

Navascués, M., Pironio, S. et Acín, A. (2008). « A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. » *New J. Phys.* **10**, p. 073013.

Ozawa, N. (2013). « About the Connes embedding conjecture : algebraic approaches », *Jpn. J. Math.* **8** (1), p. 147-183.

Pansu, P. (2013). « Difficulté d'approximation (d'après Khot, Kindler, Mossel, O'Donnell, ...) », in : Astérisque 352. Séminaire Bourbaki. Vol. 2011/2012. Exposés 1043–1058, Exp. No. 1045, vii, 83-120.

Paulsen, V. I. et al. (2016). « Estimating quantum chromatic numbers », *J. Funct. Anal.* **270** (6), p. 2188-2222.

Pisier, G. (2020). *Tensor products of C^*-algebras and operator spaces—the Connes–Kirchberg problem*. T. 96. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, p. x+484.

Raz, R. (1998). « A parallel repetition theorem », *SIAM J. Comput.* **27** (3), p. 763-803.

Salle, M. de la (2022). « Spectral gap and stability for groups and non-local games ». arXiv.

Tsirelson, B. S. (1980). « Quantum generalizations of Bell's inequality », *Lett. Math. Phys.* **4** (2), p. 93-100.

——— (1993). « Some results and problems on quantum Bell-type inequalities », *Hadronic J. Suppl.* **8** (4), p. 329-345.

Vidick, T. (2016). « Three-player entangled XOR games are NP-hard to approximate », *SIAM J. Comput.* **45** (3), p. 1007-1063.

——— (2020). « Erratum : Three-player entangled XOR games are NP-hard to approximate », *SIAM J. Comput.* **49** (6), p. 1423-1427.

——— (2022a). « Almost synchronous quantum correlations », *J. Math. Phys.* **63** (2), Paper No. 022201, 17.

——— (2022b). « MIP*=RE, A negative resolution to Connes' Embedding Problem and Tsirelson's problem », *Proceedings of the ICM 2022*.

Mikael de la Salle

CNRS – Université Claude Bernard Lyon 1
Institut Camille Jordan
43 boulevard du 11 novembre 1918
F-69622 Villeurbanne Cedex

E-mail : `delasalle@math.univ-lyon1.fr`