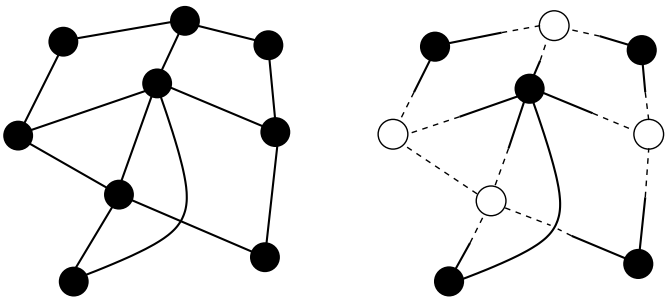
Séminaire BOURBAKI Novembre 2011
64ème année, 2011-2012, n^{o} 1045

DIFFICULTÉ D'APPROXIMATION
[d'après Khot, Kindler, Mossel, O'Donnell,...]

par **Pierre PANSU**

INTRODUCTION

Ce soir, je dois recevoir n invités. Je dois les répartir sur deux tables. Je les connais bien, je sais quelle solide inimitié certains éprouvent pour d'autres. Par exemple, je dois absolument éviter de placer L... et M... à la même table. Et de même pour N... et P.... Mais il y a trop de couples ennemis. Je vais tout de même chercher un plan de table qui maximise le nombre de couples séparés. En termes combinatoires, je forme un graphe dont les sommets sont mes invités et les arêtes les liens d'inimitié. Il s'agit de trouver un coloriage des sommets en deux couleurs (noir et blanc) qui maximise le nombre d'arêtes bicolores. Par exemple, le graphe ci-dessous à gauche a 13 arêtes, le coloriage proposé à droite a 11 arêtes bicolores, on ne peut pas faire mieux. Je dis que la *coupe maximale* du graphe vaut 11.



Le problème MAX CUT consiste à écrire un algorithme qui prend en entrée un graphe à n sommets et un entier k et retourne un coloriage avec au moins k arêtes bicolores, s'il en existe, ou bien s'arrête s'il n'en existe pas.

C'est le prototype des problèmes de *recherche* (il s'agit de trouver une solution à un ensemble de contraintes). On remarque que, étant donné un coloriage, vérifier s'il y a au moins k arêtes bicolores peut se faire rapidement, en temps polynomial (ici, au plus quadratique) en la taille du coloriage, i.e en le nombre de sommets. Cette propriété caractérise les problèmes de recherche de la *classe* NP. Cette classe est très vaste. Elle contient en particulier le problème de trouver une preuve d'un théorème (vérifier une

Ce travail a bénéficié d'une aide de l'Agence Nationale de la Recherche portant la référence ANR-10-BLAN 0116.

preuve convenablement écrite peut se faire en temps polynomial en la longueur de la preuve). Néanmoins, MAX CUT est NP-*complet* au sens suivant. Tout problème de la classe NP se ramène à MAX CUT, par un prétraitement qui ne prend qu'un temps polynomial en la taille des données. Si un jour on trouve un algorithme qui résout MAX CUT en temps polynomial, il en sera de même pour tous les problèmes NP. Peu de gens y croient (c'est la célèbre conjecture $P \neq NP$), si bien que la résolution de MAX CUT est considérée comme inaccessible au calcul.

À défaut d'une solution exacte, on se contenterait volontiers d'une solution approchée. Étant donné $\alpha < 1$, une α-*approximation* de MAX CUT est un algorithme polynomial qui retourne un coloriage réalisant α fois la coupe maximale. Cette notion s'étend à tout problème d'optimisation combinatoire, où les instances sont des fonctions à valeurs réelles sur des ensembles finis qu'il s'agit de maximiser (pour les problèmes de minimisation, on garde la même terminologie, avec $\alpha > 1$). On s'autorise des tirages au hasard [1]. Dans ce cas, on demande que la solution retournée par l'algorithme soit satisfaisante avec probabilité $> 1/2$.

Définition 0.1. — *Soit $\alpha < 1$. On dit qu'un problème d'approximation combinatoire est* α-approximable *s'il possède une α-approximation.*

Par exemple, tirer la couleur de chaque sommet au hasard indépendamment donne une 1/2-approximation de MAX CUT.

On peut faire mieux. En 1994, Michel Goemans et David Williamson [GW] ont proposé une α-approximation de MAX CUT pour tout $\alpha < \alpha_{GW} = 0.8785672057848516...$. On a de bonnes raisons de penser que cette borne est optimale, i.e. que le problème MAX CUT est NP-difficile à approcher au-delà de la constante α_{GW}. Subhash Khot, Guy Kindler, Elchanan Mossel et Ryan O'Donnell [KKMO] l'ont prouvé sous une hypothèse a priori plus forte que $P \neq NP$, connue sous le nom de Conjecture des Jeux Uniques (UGC).

Dans cet exposé, on donnera un aperçu
- de l'étonnante efficacité des relaxations semi-définies, méthode de construction d'algorithmes inaugurée par M. Goemans et D. Williamson (d'aucuns la font remonter à [Lo]) ;
- des questions mathématiques qui surgissent de l'analyse de ces relaxations semi-définies ;
- de l'émergence de résultats de difficulté d'approximation, depuis le théorème PCP.

1. C'est une commodité. Cela ne joue un rôle essentiel dans aucun des algorithmes présentés ci-dessous. Tous peuvent être transformés en algorithmes déterministes.

Le présent texte constitue une suite de l'exposé de Bernard Chazelle dans ce séminaire, [Ch], dont la lecture est chaudement recommandée.

Je remercie les participants du groupe de lecture de complexité algorithmique (ENS, 2009-2010) et du trimestre « Géométrie métrique, groupes et algorithmes » (IHP, janvier-mars 2011) pour leur aide au fil des mois, et Assaf Naor pour sa vision d'ensemble du sujet.

1. UN ALGORITHME D'APPROXIMATION POUR MAX CUT

1.1. Relaxations semi-définies

On se propose de donner une idée de la méthode de relaxation semi-définie. Il s'agit d'un procédé de construction d'algorithmes d'approximation. Il n'est pas systématique (il n'y a pas une relaxation semi-définie canonique pour chaque problème combinatoire). On peut seulement présenter la démarche sur des exemples. Nous avons choisi trois problèmes d'optimisation qui ont donné lieu à des développements mathématiques intéressants : MAX CUT, SPARSEST CUT et MAX ACYCLIC SUBGRAPH. On commence par MAX CUT. Ce problème a tout pour plaire : un intérêt historique, c'est le premier succès de la méthode ; un saut d'intégralité intéressant, une étude d'inapproximabilité spectaculaire.

1.2. L'algorithme de Goemans et Williamson pour MAX CUT

THÉORÈME 1.1 (M. Goemans et D. Williamson, [GW]). — *MAX CUT est α-approximable pour tout $\alpha < \alpha_{GW} = 0.878...$.*

1.2.1. Arithmétisation. — On commence par formuler algébriquement le problème combinatoire. Soient G un graphe, V l'ensemble de ses sommets, $E \subset V \times V$ l'ensemble de ses arêtes. On choisit de représenter un coloriage de G par une fonction $x : V \to \{-1, 1\}$. On choisit d'exprimer le nombre d'arêtes bicolores par la fonction

$$OBJ(x) = \sum_{(u,v)\in E} \frac{1}{2}(1 - x_u x_v).$$

Calculer la coupe maximale de G, c'est maximiser la fonction OBJ sur le cube discret $\{-1, 1\}^V$, i.e. sur l'ensemble des fonctions $x : V \to \mathbb{R}$ qui satisfont aux contraintes

$$\forall v \in V,\ x_v^2 = 1.$$

Notons $OBJ(G)$ le maximum.

1.2.2. Relaxation. — On plonge le cube discret dans un espace plus vaste. On se donne un espace euclidien ℓ_2 et on considère les applications $y : V \to \ell_2$. On remplace chaque produit $x_u x_v$ par un produit scalaire $y_u \cdot y_v$. Les contraintes deviennent

$$\forall v \in V,\ y_v \cdot y_v = 1.$$

La fonction objectif devient

$$SDP(y) = \sum_{(u,v)\in E} \frac{1}{2}(1 - y_u \cdot y_v).$$

Remarquer que la restriction de SDP aux applications y qui prennent leurs valeurs dans une droite coïncide avec OBJ. Il en est de même des contraintes, donc

$$\max SDP \geq \max OBJ.$$

Admettons pour l'instant qu'il existe un algorithme qui, avec une précision arbitraire, détermine en temps polynomial l'application $y_{\max} : V \to \ell_2$ qui maximise SDP sous les contraintes imposées. Notons $SDP(G)$ le maximum. La fonction

$$n \mapsto \min_{|V|=n} \frac{OBJ(G)}{SDP(G)}$$

s'appelle le saut d'intégralité (`integrality gap`) de la relaxation choisie.

1.2.3. Procédure d'arrondi. — Pour compléter la méthode en un algorithme d'approximation, on construit maintenant un coloriage x à partir de la solution $y_{\max}$ du problème continu. Cela donnera simultanément une minoration du saut d'intégralité, et donc du facteur d'approximation réalisé par l'algorithme.

On voit $y_{\max}$ comme un plongement du graphe G dans la sphère unité. On tire un hyperplan vectoriel H uniformément au hasard. Il sépare les sommets en deux parties, voilà le coloriage x_H cherché.

1.2.4. Analyse. — Pour chaque arête (u, v), la probabilité que H sépare y_u de y_v vaut $\frac{1}{\pi}\arccos(y_u \cdot y_v)$. En effet, l'intersection de l'hyperplan avec le plan engendré par y_u de y_v est une droite vectorielle tirée uniformément au hasard dans ce plan, la probabilité qu'elle sépare y_u de y_v est proportionnelle à l'angle entre y_u et y_v. Par conséquent, l'espérance du nombre d'arêtes bicolores dans le coloriage aléatoire obtenu est

$$\mathbb{E}_H(OBJ(x_H)) = \sum_{(u,v)\in E} \frac{1}{\pi}\arccos(y_u \cdot y_v).$$

Il vient

$$\mathbb{E}_H(OBJ(x_H)) \geq \alpha_{GW} \times SDP(G)$$

où $\alpha_{GW} = 0.878...$ est le minimum de la fonction $t \mapsto \dfrac{\frac{1}{\pi}\arccos(t)}{\frac{1}{2}(1-t)}$ sur $[-1, 1]$. Par conséquent, pour tout graphe G, $\frac{OBJ(G)}{SDP(G)} \geq \alpha_{GW}$, donc le saut d'intégralité de la relaxation de Goemans-Williamson est $\geq \alpha_{GW}$.

Par symétrie, avec probabilité 1/2, $OBJ(x_H) \geq \alpha_{GW} SDP(G)$, donc le facteur d'approximation de l'algorithme obtenu serait au moins α_{GW} si on savait calculer exactement $SDP(G)$ en temps polynomial. On ne sait le faire qu'avec une précision donnée à l'avance. On a au moins obtenu une α-approximation pour tout $\alpha < \alpha_{GW}$.

1.3. Saut d'intégralité

La détermination exacte du saut d'intégralité de la relaxation de Goemans et Williamson est un joli problème de géométrie. La minoration par α_{GW} a été aisée à obtenir. L'inégalité inverse n'est pas aussi simple.

THÉORÈME 1.2 (U. Feige, G. Schechtman, [FS]). — *Le saut d'intégralité de la relaxation de Goemans-Williamson est exactement α_{GW}.*

Autrement dit, il existe des graphes pour lesquels $\frac{OBJ(G)}{SDP(G)}$ est arbitrairement proche de α_{GW}. Ces graphes sont des approximations finies du graphe infini suivant. Les sommets sont tous les points de la sphère unité de l'espace de Hilbert séparable. Deux sommets y_1 et y_2 sont reliés par une arête si et seulement si la fonction $t \mapsto \dfrac{\frac{1}{\pi}\arccos(t)}{\frac{1}{2}(1-t)}$ atteint son minimum en $y_1 \cdot y_2$. Il y a une mesure de probabiité naturelle sur l'ensemble des arêtes. U. Feige et G. Schechtman montrent que parmi tous les coloriages de ce graphe, ceux définis par des hyperplans maximisent la probabilité qu'une arête soit coupée. C'est une propriété isopérimétrique de la sphère, qui est prouvée par symétrisation par rapport à des hyperplans.

2. PROGRAMMATION SEMI-DÉFINIE

Nous avons passé sous silence un ingrédient essentiel, l'existence d'algorithmes polynomiaux pour optimiser une quantité comme SDP. Remarquer que l'application inconnue $y : V \to \ell_2$ n'intervient qu'à travers les produits scalaires $y_u \cdot y_v$. Autrement dit, SDP est en fait une fonction de la matrice de Gram A de coefficients $A_{uv} = y_u \cdot y_v$. Une condition nécessaire et suffisante sur une matrice A pour qu'elle soit la matrice de Gram d'un n-uplet de vecteurs est que

– A est symétrique, de taille n ;
– A est positive au sens large, i.e. pour tout vecteur Y, $Y^\top AY \geq 0$.

Notons $\mathcal{P}$ le cône convexe des matrices $n \times n$ symétriques positives au sens large. Calculer $SDP(G)$, c'est maximiser la fonction affine $\sum_{(u,v)\in E} \frac{1}{2}(1 - A_{uv})$ sur le convexe obtenu en coupant $\mathcal{P}$ avec le plan affine défini par les équations $A_{vv} = 1$, $v \in V$. Les algorithmes polynomiaux de la programmation linéaire (méthode de l'ellipsoïde, méthode du point intérieur) permettent de le faire. On a donné le nom de *programmation semi-définie* à cette extension de la programmation linéaire.

En fait, on peut maximiser une fonction affine sur un convexe dès qu'on dispose d'un oracle indiquant si un point de l'espace appartient ou non au convexe, en un temps

dépendant de façon adéquate de la complexité du convexe et de la précision souhaitée. Dans le cas du cône convexe $\mathcal{P}$, l'oracle consiste à calculer la plus petite valeur propre avec une précision donnée. Pour tout convexe en dimension finie, il existe un oracle ayant les propriétés requises, [NN], [Ne]. Donc, en théorie, maximiser une fonction affine sur un convexe est faisable en temps polynomial.

En pratique, la programmation linéaire proprement dite (le convexe est un polyèdre) a été implémentée industriellement depuis des décennies, elle est capable de traiter des données de grande taille ($n = 10^7$). Il existe des implémentations « de laboratoire » de la programmation semi-définie (le convexe est l'intersection du cône $\mathcal{P}$ avec un polyèdre de l'espace des matrices symétriques), qui sont pour l'instant limitées à des tailles inférieures à $n = 10^4$.

3. ALGORITHMES D'APPROXIMATION POUR SPARSEST CUT

SPARSEST CUT a aussi un intérêt historique. C'est en étudiant ce problème et les questions de flots qui lui sont reliées que N. Linial, E. London et Yu. Rabinovich ont introduit la méthode des plongements dans les espaces de Banach en algorithmique. L'étude des sauts d'intégralité conduit à des problèmes de plongements qui ont été beaucoup étudiés, par exemple en lien avec la théorie des groupes. À la différence de MAX CUT, son seuil d'approximabilité tend (conjecturalement) vers l'infini avec la taille des instances.

3.1. Le problème SPARSEST CUT

Définition 3.1. — *On se donne un graphe $G = (V, E)$ avec un poids $m_{u,v}$ pour chaque arête $(u, v) \in E$ et une demande $D_{u,v}$ pour chaque couple $(u, v) \in V \times V$ de sommets. On considère les partitions des sommets en $V = S \cup \bar{S}$ et on s'intéresse à la quantité*

$$OBJ(S) = \frac{\sum_{\{(u,v)\in S\times\bar{S}\,;\,(u,v)\in E\}} m_{u,v}}{\sum_{u\in S}\sum_{v\in\bar{S}} D_{u,v}}.$$

Le problème SPARSEST CUT consiste, étant donné un graphe fini G, à calculer une partition qui minimise OBJ.

Cas particulier des poids et demandes uniformes (i.e. $m_{u,v} = D_{u,v} = 1$). Dans ce cas,

$$OBJ(S) = \frac{\#\partial S}{\#S\,\#\bar{S}},$$

$\min OBJ$ s'appelle la *constante de Cheeger* de G. Elle exprime une propriété isopérimétrique du graphe. Elle est reliée au spectre du laplacien sur G, à la vitesse de mélange de la marche aléatoire sur G, à la notion d'expanseur. Donc le problème SPARSEST CUT uniforme consiste à calculer la constante de Cheeger d'un graphe fini.

Le calcul exact de $\min OBJ$ est NP-complet. Mais une partition (presque) optimale est fréquemment utilisée dans des algorithmes (« diviser pour régner »). D'où l'intérêt pour des algorithmes d'approximation.

3.2. Approche de SPARSEST CUT par la programmation linéaire

3.2.1. Arithmétisation. — Soit $S \subset V$, soit 1_S la fonction caractéristique de S. La fonction objectif s'écrit

$$OBJ(S) = 2\frac{\sum_{(u,v)\in E} m(uv)|1_S(u) - 1_S(v)|}{\sum_u \sum_v |1_S(u) - 1_S(v)|}.$$

Soit $d(u,v) = |1_S(u) - 1_S(v)|$. C'est une semi-distance sur V, induite par une application vers l'espace métrique à 2 points $\{0,1\}$. Le cône convexe engendré par ces semi-distances est exactement l'ensemble des semi-distances plongeables dans L_1, [A]. Notons $\mathcal{L}_1$ l'ensemble des semi-distances plongeables dans L_1. Par conséquent,

$$\begin{aligned}\min OBJ &= 2\min_{d\in\mathcal{L}^1} \frac{\sum_{(u,v)\in E} m_{u,v}d(u,v)}{\sum_u \sum_v D_{u,v}d(u,v)} \\ &= \min\{ \sum_{(u,v)\in E} m_{u,v}d(u,v) \,|\, d \in \mathcal{L}_1, \sum_u \sum_v D_{u,v}d(u,v) = 1\}.\end{aligned}$$

Il s'agit d'un problème de programmation linéaire, car pour chaque ensemble X à n points, l'ensemble des semi-distances sur X plongeables dans L_1 est un cône polyédral convexe. Malheureusement, ce cône a un nombre exponentiellement grand de facettes, voir [DL], ce qui fait que la programmation linéaire n'en donne pas une solution en temps polynomial. D'ailleurs, le problème de décider si un espace métrique fini est plongeable ou non dans L_1 est NP-complet.

3.2.2. Relaxation. — Oublions la condition de plongeabilité dans L_1. Sur la fonction d, il ne reste que les contraintes de symétrie et d'inégalité triangulaire, qui sont en nombre quadratique. Le problème de programmation linéaire obtenu, noté LP, est résoluble en temps polynomial.

3.2.3. Procédure d'arrondi. — Elle est due à N. Linial, E. London, Y. Rabinovich, 1995, [LLR]). Elle s'appuie sur le théorème suivant.

Théorème 3.2 (J. Bourgain, 1985, [Bou]). — *Tout espace métrique à n points se plonge dans L_2 (et donc dans L_1) avec distorsion au plus $O(\log(n))$. C'est optimal (*[LLR]*).*

[LLR] montre que le plongement de Bourgain est calculable en temps polynomial, et sa dimension est polynomiale. Il reste à convertir une métrique $d \in \mathcal{L}_1$, i.e. plongeable dans L_1, en une partition $V = S \coprod \bar{S}$. Une métrique plongeable dans $\mathbb{R} = \ell_1^1$ s'écrit aisément comme combinaison linéaire positive de métriques à valeurs dans $\{0,1\}$. Une métrique plongeable dans ℓ_1^N est la somme de N métriques plongeables dans ℓ_1^1. On en tire une partition $S \coprod \bar{S}$ qui réalise $OBJ(d')$.

Corollaire 3.3. —

$$\min LP \leq \min OBJ \leq C\ \log(n) \min LP,$$

ce qui montre que LP fournit une approximation de $\min OBJ$ *à un facteur multiplicatif* $\log(n)$ *près.*

Preuve. La métrique d' plongeable dans L_1 qui est $O(\log(n))$-proche de la solution d de LP satisfait

$$\min LP \leq OBJ(d') \leq C\ \log(n) \min OBJ = C\ \log(n) \min LP.$$

3.3. Approche de SPARSEST CUT via la programmation semi-définie

3.3.1. Arithmétisation. — On réécrit

$$OBJ(S) = 2\frac{\sum_{(u,v)\in E} m_{u,v}|1_S(u) - 1_S(v)|^2}{\sum_u \sum_v D_{u,v}|1_S(u) - 1_S(v)|^2}.$$

3.3.2. Relaxation. — On remplace les fonctions $x : V \to \{0, 1\}$ par des fonctions $y : V \to \ell^2$, en gardant la contrainte

$$\forall u,\, v,\, w \in V, \quad |y(u) - y(v)|^2 \leq |y(u) - y(w)|^2 + |y(w) - y(v)|^2,$$

satisfaite par les fonctions caractéristiques. Cela ramène à un problème de programmation semi-définie, noté SDP.

Soit $d(u, v) = |x(u) - x(v)|^2$. C'est une semi-distance sur V, et $d^{1/2}$ est induite par un plongement dans l'espace euclidien.

Définition 3.4. — *On dit qu'une semi-distance d est* de type négatif *si $d^{1/2}$ est induite par un plongement dans un espace de Hilbert. On note $\mathcal{NEG}$ l'ensemble des semi-distances de type négatif.*

Par conséquent,

$$\min SDP = \min\left\{ \sum_{(u,v)\in E} m_{u,v} d(u, v)\,;\, d \in \mathcal{NEG},\, \sum_u \sum_v D_{u,v} d(u, v) = 1 \right\}.$$

À nouveau, si toute métrique de type négatif se plonge dans L_1 avec distorsion $\leq L$,

$$\min SDP \leq \min OBJ \leq L \min OBJ.$$

Ceci conduit à poser

Définition 3.5 (M. Goemans [Go], N. Linial [L]). — *Soit GL_n la borne inférieure des réels L tels que toute semi-distance de type négatif sur un ensemble à n points soit induite par une application à valeurs dans L_1, de distorsion $\leq L$.*

On a montré que $\min OBJ$ est calculable en temps polynomial à un facteur multiplicatif GL_n près.

3.3.3. Procédure d'arrondi. — Supposons connu un algorithme qui construit en temps polynomial un plongement d'un espace de type négatif dans L_1 de distorsion $\leq L$. Le procédé de N. Linial, E. London et Y. Rabinovich [LLR] permet d'en déduire une partition qui réalise le minimum de OBJ à L près.

3.4. Saut d'intégralité : majoration

Il est facile de voir que le saut d'intégralité de la relaxation semi-définie étudiée est exactement GL_n (voir [CKN]). Reste à évaluer GL_n. Pour avoir une borne supérieure, il faut un raffinement du théorème de Bourgain.

Théorème 3.6 (S. Arora, J. Lee, A. Naor, 2005, [ALN]). — *Soit $d \in \mathcal{NEG}$ une semi-métrique de type négatif sur un ensemble à n points. Alors (X, d) se plonge aussi dans L_2 avec distorsion $O(\sqrt{\log(n)}\log(\log(n)))$. Un tel plongement est calculable en temps quadratique en n.*

Remarque 3.7. — C'est presque optimal, puisque l'ensemble des sommets du n-cube ℓ_1 ne se plonge pas dans ℓ_2 avec distorsion $< \sqrt{n}$ (P. Enflo, 1969, [E]).

Corollaire 3.8. — $GL_n = O(\sqrt{\log(n)}\log(\log(n)))$.

En effet, L_2 se plonge isométriquement dans L_1.

3.5. Saut d'intégralité : minoration

Inversement, pour minorer GL_n, il faut des exemples d'espaces métriques finis de type négatif qui se plongent mal dans L_1. Ce n'est pas simple. La distorsion des plongements dans L_2 est assez bien comprise. Elle est liée au spectre du laplacien discret. En revanche, la distorsion des plongements dans L_1 est plus mystérieuse. En 2005, S. Khot et N. Vishnoi ont construit des exemples pour lesquels ils montrent que la distorsion croît au moins comme une puissance de $\log\log n$, [KV]. J. Lee et A. Naor ont eu l'idée d'utiliser les boules du groupe d'Heisenberg discret $\mathrm{Heis}_{\mathbb{Z}}$. Il s'agit du groupe des matrices unipotentes $\left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \right\}$ à coefficients entiers. On choisit comme boule unité B un système générateur fini symétrique quelconque (par exemple, les 8 matrices dont les coefficients sont compris entre -1 et 1). Cela produit une distance invariante à gauche d_B dont la boule de rayon n B^n (l'ensemble des produits de n éléments de B) contient en gros n^4 éléments. J. Lee et A. Naor montrent qu'il existe sur $\mathrm{Heis}_{\mathbb{Z}}$ une distance d équivalente à d_B, invariante à gauche, qui est de type négatif, [LN].

Théorème 3.9 (J. Cheeger, B. Kleiner, A. Naor, [CKN]). — *Tout plongement de B^n dans L_1 a une distorsion au moins égale à $(\log n)^\delta$ pour $\delta = 2^{-32}$.*

On conjecture que la valeur optimale de δ est $1/2$, ce qui prouverait que le saut d'intégralité GL_n est de l'ordre de $\sqrt{\log n}$.

La preuve du théorème 3.9 repose sur l'autosimilarité de l'espace métrique $(\mathrm{Heis}_{\mathbb{Z}}, d_B)$. $\mathrm{Heis}_{\mathbb{Z}}$ est un sous-groupe cocompact du groupe de Lie $\mathrm{Heis}_{\mathbb{R}}$ (de la même façon que $\mathbb{Z}^3$ dans $\mathbb{R}^3$). $\mathrm{Heis}_{\mathbb{R}}$ possède une distance invariante à gauche d_{CC} (équivalente à d_B) qui est exactement auto-similaire : elle possède des homothéties h_t,

$$d_{CC}(h_t(x), h_t(y)) = t\, d_{CC}(x, y).$$

Si GL_n était borné, il en résulterait que l'espace métrique $(\mathrm{Heis}_{\mathbb{R}}, d_{CC})$ admet un plongement bi-lipschitzien dans L_1 (car une ultra-limite d'espaces L_1 est encore un espace L_1, [K], [BDK]). Le problème combinatoire est alors converti en un problème d'analyse. Il y a une notion de différentiabilité associée aux homothéties h_t, [Pa], et un théorème à la Rademacher : les fonctions lipschitziennes et, plus généralement, les applications lipschitziennes à valeurs dans un espace de Banach V possédant la propriété de Radon-Nikodym, possèdent presque partout une différentielle, qui est un homomorphisme de groupe de $\mathrm{Heis}_{\mathbb{R}}$ dans V. Un tel homomorphisme n'est jamais injectif, ce qui empêche d'être bi-lipschitzien. Cet argument est dû à S. Semmes, [S], lorsque V est de dimension finie, à J. Cheeger et B. Kleiner, [CK1], en général. Malheureusement, L_1 n'a pas la propriété de Radon-Nikodym. J. Cheeger et B. Kleiner, [CK2], ont inventé une notion de différentiabilité spécialement adaptée à L_1. Elle repose sur le fait qu'une semi-distance induite par une application à valeurs dans L_1 est l'intégrale d'une famille de semi-distances prenant les valeurs 0 et 1, i.e. correspondant à des sous-ensembles de l'espace de départ (fait qui remonte à la thèse de P. Assouad, [A]). Voici ce que le théorème de différentiabilité devient dans le cas de $\mathrm{Heis}_{\mathbb{R}}$ (voir une généralisation dans [AKL]).

Théorème 3.10 (B. Franchi, R. Serapioni, F. Serra Cassano, [FSS])
Pour tout ensemble $S \subset Heis_{\mathbb{R}}$ de périmètre fini, en presque tout point du bord de S (au sens du périmètre), les h_t-dilatés de S convergent vers un demi-espace vertical.

La distance associée à un demi-espace vertical provient du groupe $\mathbb{R}^2$, quotient de $\mathrm{Heis}_{\mathbb{R}}$ par son centre. Le théorème 3.10 entraîne qu'en presque tout point, lorsqu'on la dilate, la distance induite par un plongement lipschitzien de $\mathrm{Heis}_{\mathbb{R}}$ dans L_1 converge vers la distance induite par une application qui factorise par $\mathbb{R}^2$, c'est impossible pour une application bi-lipschitzienne. On conclut qu'il n'existe pas de plongement bi-lipschitzien de $\mathrm{Heis}_{\mathbb{R}}$ dans L_1, et donc que GL_n tend vers $+\infty$.

Pour obtenir une borne inférieure effective sur GL_n, J. Cheeger, B. Kleiner et A. Naor utilisent une idée un peu différente. Ils prouvent que les ensembles qui figurent dans l'expression comme intégrale de distances de coupure d'une application lipschitzienne à valeurs dans L_1 sont asymptotiquement monotones à petite échelle. Monotone signifie qu'ils coupent toute géodésique bi-infinie suivant une demi-droite. Ce résultat s'applique à une classe d'espaces sources assez large, et non seulement à $\mathrm{Heis}_{\mathbb{R}}$, voir [CK3]. C'est cette propriété qui donne lieu à un énoncé quantitatif, et conduit au théorème 3.9.

A. Naor a suggéré une autre approche du théorème 3.9, par le biais d'inégalités fonctionnelles. Cette approche donne l'exposant optimal pour les applications de $\text{Heis}_{\mathbb{R}}$ dans L_p, $p > 1$, voir [ANT].

Comme on le voit, le calcul du saut d'intégralité de la relaxation semi-définie proposée par M. Goemans et N. Linial pour SPARSEST CUT a donné lieu à des développements géométriques poussés. Cette relaxation donne actuellement la meilleure solution connue du problème SPARSEST CUT général. Toutefois, dans le cas particulier où les poids sont tous égaux, S. Arora, E. Hazan et S. Kale, [AHK], ont donné en 2004 un algorithme polynomial différent qui calcule $\min OBJ$ à un facteur $O(\sqrt{\log(n)})$ près. Donc rien ne prouve pour l'instant que la programmation semi-définie soit la meilleure approche possible pour SPARSEST CUT. D'ailleurs, les seules meilleures inférieures de complexité connues actuellement sont les suivantes :

– Sous l'hypothèse $P \neq NP$, il existe un $\epsilon > 0$ tel que SPARSEST CUT n'est pas $1 + \epsilon$-approximable, [AMS].
– Sous l'hypothèse UGC (voir plus loin), pour toute constante C, SPARSEST CUT n'est pas C-approximable, [CKKRS].

4. MAX ACYCLIC SUBGRAPH ET L'INÉGALITÉ DE GROTHENDIECK

On détaille un problème de gain par rapport au tirage au hasard : un tirage au hasard donne un facteur d'approximation qui est optimal (c'est assez fréquent), on s'intéresse alors au second terme dans un développement asymptotique du seuil.

La solution décrite le relie aux inégalités de Grothendieck, qui constituent un chapitre important de l'analyse fonctionnelle. Ces mêmes inégalités soulèvent des questions algorithmiques. Pour l'une d'entre elles, le problème de Grothendieck ℓ_p, on a une solution spectaculaire : c'est une famille à un paramètre de problèmes dont le seuil d'approximabilité est non trivial, il est connu exactement.

4.1. Le problème MAX ACYCLIC SUBGRAPH

On considère cette fois des graphes finis orientés. On dit qu'un graphe orienté est *acyclique* s'il ne contient aucun sous-graphe isomorphe à un cycle avec toutes les arêtes orientées dans le bon sens. Étant donné un graphe fini orienté G, on note $MAS(G)$ le nombre maximal d'arêtes qui ensemble forment un sous-graphe acyclique.

Ce problème est NP-complet. En voici une 1/2-approximation. Soit G un graphe fini orienté. Choisir une numérotation arbitraire des sommets, conserver toutes les arêtes dont les numéros des sommets sont croissants. Cela donne un premier sous-graphe acyclique, à e^+ arêtes. Conserver ensuite toutes les arêtes dont les numéros des sommets sont décroissants. Le second graphe est aussi acyclique et a e^- arêtes. La réunion des deux recouvre G, donc $e^+ + e^- \geq |E| \geq MAS(G)$.

Peut-on faire mieux ? On sait que

– Sous l'hypothèse $P \neq NP$, MAX ACYCLIC SUBGRAPH n'est pas α-approximable pour $\alpha > \frac{65}{66}$, [N].
– Sous l'hypothèse UGC (voir plus loin), MAX ACYCLIC SUBGRAPH n'est pas α-approximable pour $\alpha > \frac{1}{2}$, [GMR].

On se pose une question plus fine. Pour un graphe à N arêtes, $MAS(G) \geq \frac{1}{2}N$. On cherche un facteur d'approximation pour le *gain* $gain(G) = MAS(G) - \frac{1}{2}N$.

Théorème 4.1 (M. Charikar, K. Makarychev, Yu. Makarychev, [CrMM])

Le gain d'un graphe orienté est $\frac{\text{const.}}{\log n}$-approximable. Autrement dit, il existe c et un algorithme polynomial qui prend en entrée un graphe à n sommets et N arêtes et retourne un sous-graphe acyclique à N' arêtes tel que

$$N' - \frac{1}{2}N \geq \frac{c}{\log n}(MAS(G) - \frac{1}{2}N).$$

On verra plus loin qu'on ne peut pas améliorer le facteur $\frac{C}{\log n}$ en un facteur constant, sous l'hypothèse UGC.

4.2. L'algorithme de M. Charikar, K. Makarychev et Yu. Makarychev

4.2.1. Formulation en termes de permutations. — Soit $G = (V, E)$ un graphe orienté. On pose, pour u, $v \in V$,

$$w_{u,v} = \begin{cases} 1 & \text{si } (u,v) \text{ est une arête orientée,} \\ -1 & \text{si } (v,u) \text{ est une arête orientée,} \\ 0 & \text{sinon.} \end{cases}$$

Si $\sigma : V \to \{1, \cdots, n\}$ est une numérotation des sommets, on pose

$$AS(\sigma) = \sum_{\{(u,v) \in V \times V \,;\, \sigma(u) < \sigma(v)\}} w_{u,v}.$$

À tout sous-graphe acyclique à N' arêtes correspond une numérotation telle que $AS(\sigma) = N' - \frac{1}{2}N$. Il suffit donc de maximiser AS sur les bijections σ. La méthode s'applique plus généralement à toute matrice antisymétrique W. On suit la description donnée dans [KN1].

4.2.2. Réduction aux matrices extraites. — Soit W une matrice carrée. On note $\|W\|_{\text{cut}}$ la plus grande des sommes des coefficients des matrices extraites de W. Autrement dit,

$$\|W\|_{\text{cut}} = \max_{S,T \subset V} |\sum_{u \in S} \sum_{v \in T} w_{u,v}|.$$

Soient S, $T \subset V$. Comme $\sum_{u,\, v \in S \cap T} w_{u,v} = 0$, on peut supposer que $S \cap T = \varnothing$. Étant donnée une numérotation σ qui passe d'abord par S, puis par T, soit σ' la numérotation

qui en diffère en ce que T est traversé en premier, puis S, et soit σ'' la numérotation inverse de σ'. Alors

$$AS(\sigma) + AS(\sigma'') = 2\sum_{u\in S}\sum_{v\in T} w_{u,v}.$$

On conclut que

$$MAS(G) - \frac{1}{2}N = \max AS \geq \|W\|_{\text{cut}}.$$

4.2.3. Arithmétisation. — On est ramené à trouver un procédé de calcul approché de $\|W\|_{\text{cut}}$. Remarquer que

$$\|W\|_{\text{cut}} = \max_{x,\,x':V\to\{0,1\}} x^\top W x'.$$

Quitte à perdre un facteur 4, et au prix de remplacer W par une matrice plus grande mais toujours antisymétrique, on peut remplacer dans cette expression les vecteurs à valeurs dans $\{0,1\}$ par des vecteurs à valeurs dans $\{-1,1\}$. On considère donc la fonction objectif

$$OBJ(x,x') = x^\top W x'$$

sur les couples de fonctions booléennes x, $x' : V \to \{-1,1\}$. Par construction, $\max OBJ \leq \|W\|_{\text{cut}}$.

4.2.4. Relaxation. — On remplace les fonctions booléennes x, x' par des applications y, y' à valeurs dans la sphère unité d'un espace ℓ_2 et la fonction objectif par

$$SDP(y,y') = \sum_{u,\,v\in V} w_{u,v}\, y_u \cdot y'_v.$$

La programmation semi-définie fournit en temps polynomial une valeur approchée à ϵ-près de $\max SDP$, pour tout $\epsilon > 0$.

4.2.5. Analyse. — L'ingrédient principal est le théorème classique suivant.

Théorème 4.2 (A. Grothendieck, [G]). — *Il existe une constante universelle K_G telle que, pour toute matrice réelle A,*

$$\max_{|y_u|=|y'_v|=1} \sum_{u,\,v\in V} a_{u,v}\, y_u \cdot y'_v \leq K_G \max_{x_u,\,x'_v=\pm 1} \sum_{u,\,v\in V} a_{u,v} x_u x'_v.$$

Ceci montre que $\max OBJ \max SDP \leq K_G \max OBJ \leq \|W\|_{\text{cut}}$. À partir de la solution (y,y') maximisant SDP, la procédure d'arrondi décrite ci-dessous fournit des fonctions booléennes (x,x'), et donc des sous-ensembles $S, T \subset V$ tels que $\sum_{S\times T} w_{u,v} \geq$ const.$\|W\|_{\text{cut}}$, d'où une numérotation σ telle que $AS(\sigma) \geq$ const.$\|W\|_{\text{cut}}$. Reste à voir que $\|W\|_{\text{cut}} \geq \frac{\text{const.}}{\log n} \max AS$. Pour cela, on utilise à nouveau l'inégalité de Grothendieck et une estimation de sommes d'exponentielles.

4.2.6. Procédure d'arrondi. — On en trouve dans toutes les preuves de l'inégalité de Grothendieck. Celle qui donne la meilleure constante a longtemps été due à J.-L. Krivine, [Kr], mais son record a été battu récemment, [BMMN].

4.3. Inégalité de Grothendieck ℓ_p

On s'intéresse à des variantes de la méthode du paragraphe précédent pour des matrices symétriques. Ces variantes n'ont pas d'applications combinatoires pour l'instant. En revanche, elles constituent une famille de problèmes dont le seuil d'approximabilité est connu exactement.

L'inégalité de Grothendieck s'applique aussi bien aux matrices symétriques qu'aux matrices antisymétriques. Dans le cas symétrique, elle donne un procédé (par programmation semi-définie) pour calculer approximativement le maximum d'une forme quadratique sur la boule unité de ℓ_∞.

4.3.1. Le problème de Grothendieck ℓ_p. — Il s'agit de maximiser une forme quadratique $OBJ(t) = t^\top At$ dont les coefficients diagonaux sont nuls sur la boule unité de l'espace $\ell_p^n = \mathbb{R}^n$ muni de la norme ℓ_p.

C'est facile si $p = 2$ ($\max OBJ$ est la plus grande valeur propre de A). Pour $p = 1$, le problème est α-approximable pour tout $\alpha > 1$, [AN]. Pour $p = \infty$, le problème est $\log n$-approximable, mais probablement non $(\log n)^\gamma$-approximable pour $\gamma < 1/6$, voir un énoncé précis dans [KS].

Pour $p \in [2, +\infty[$, le seuil optimal d'approximabilité est connu exactement.

Théorème 4.3 (A. Naor, G. Schechtman, [NS] [2]). — *Pour $p > 2$, soit γ_p la norme L_p d'une gaussienne standard. Alors le problème de Grothendieck ℓ_p est α-approximable pour tout $\alpha < \gamma_p^2$.*

Théorème 4.4 (V. Guruswami, P. Raghavendra, R. Saket, Y. Wu, [GRSW])

Sous l'hypothèse $P \neq NP$, le problème de Grothendieck ℓ_p n'est pas α-approximable pour $\alpha > \gamma_p^2$.

Le théorème 4.3 résulte d'une généralisation de l'inégalité de Grothendieck avec constante optimale γ_p^2. Pour toute matrice A,

$$\max_{\{y_i \in \ell_2\,;\, \sum_i |y_i|_2^p \leq 1\}} \sum_{i,j} a_{ij} y_i \cdot y_j \leq \gamma_p^2 \max_{\{x_i \in \mathbb{R}\,;\, \sum_i |x_i|^p \leq 1\}} \sum_{i,j} a_{ij} x_i x_j.$$

L'algorithme consiste à minimiser le premier membre, ce qui est possible, car il s'agit d'une forme linéaire en les coefficients de la matrice de Gram $Y_{ij} = y_i \cdot y_j$, à maximiser sur le convexe des matrices symétriques positives telles que $\sum_i Y_{ii}^{p/2} \leq 1$.

5. DIFFICULTÉ D'APPROXIMATION

Comment peut-on prouver qu'il n'existe pas d'algorithme qui calcule une solution d'une instance d'un problème $\mathcal{O}$ de la classe NP en temps polynomial en la taille de l'instance ? Actuellement, on ne sait pas faire.

2. Améliorant un résultat un peu plus faible de [KNS].

5.1. Réductions

Tous les résultats existants sont conditionnels à l'hypothèse $P \neq NP$, ou à d'autres hypothèses voisines. On part d'un problème $\mathcal{C}$ connu pour être NP-complet (cas de l'hypothèse $P \neq NP$), et on effectue une *réduction* de $\mathcal{C}$ à $\mathcal{O}$. Un problème de décision, c'est une partition des instances entre instances acceptées et instances rejetées. Par exemple, la version décision de MAX CUT fixe un réel s et divise les graphes en

- graphes acceptés : ceux pour lesquels la fraction maximale d'arêtes bicolores dans un coloriage est $\geq s$, et
- graphes rejetés : ceux pour lesquels la fraction maximale d'arêtes bicolores dans un coloriage est $< s$.

Une réduction de $\mathcal{C}$ à $\mathcal{O}$ consiste, pour chaque instance I de $\mathcal{C}$, à construire (en temps polynomial en la taille de I) une instance I' de $\mathcal{O}$, de sorte que

- si I est acceptée, I' est acceptée ;
- si I est rejetée, I' est rejetée.

Clairement, s'il existe un algorithme polynomial pour $\mathcal{O}$, il y en a un pour $\mathcal{C}$, et donc pour tous les problèmes de la classe NP (par définition). Cela contredit $P \neq NP$.

On manipulera une classe de problèmes (dits « de promesse ») un peu plus vaste. Pour ces problèmes, on admet des instances ni acceptées ni rejetées, et sur lesquels un algorithme a le droit de se tromper. Par exemple, étant donnés deux réels $c \geq s$, le problème (c, s)-MAX CUT accepte les graphes pour lesquels la fraction maximale d'arêtes bicolores dans un coloriage est $\geq c$, et rejette les graphes pour lesquels la fraction maximale d'arêtes bicolores dans un coloriage est $< s$. On peut parler de réduction (même définition) et donc de NP-complétude pour de tels problèmes.

Le lien avec la difficulté d'approximation est simple. Par exemple, si (c, s)-MAX CUT est NP-complet, alors, sous l'hypothèse $P \neq NP$, MAX CUT n'est pas s/c-approximable. En effet, un algorithme de s/c-approximation construit pour tout graphe G un coloriage avec une fraction f d'arêtes bicolores au moins égale à $s/c \times$ coupe maximale(G). Si $f < s$, alors coupe maximale(G) $< s/\alpha \leq c$ donc on rejette G. Sinon, on est certain que coupe maximale(G) $\geq f \geq s$, et on accepte G sans se tromper. L'algorithme résout donc le problème (c, s)-MAX CUT en temps polynomial, et $P = NP$, contradiction.

5.2. Le théorème PCP

C'est l'aboutissement d'une histoire qui commence avec la logique formelle : des règles pour rédiger les preuves (Frege) qui permettent de les vérifier en temps polynomial (Gödel). Cook et Levin constatent que la vérification est une succession d'opérations locales, c'est le mécanisme qui est à l'origine de l'existence de problèmes NP-complets. On peut même rédiger les preuves de façon qu'il suffise de vérifier la consistance de triplets de bits.

Si on s'autorise des tirages au hasard et une marge d'erreur, la tâche de vérification peut être réduite : le théorème PCP (`Probabilistically Checkable Proofs`) affirme

qu'il suffit de vérifier un nombre borné de triplets pour affirmer qu'une preuve est correcte avec une probabilité d'erreur infime.

Le théorème PCP possède une formulation équivalente en termes de difficulté d'approximation. Considérons le problème E3SAT : les instances sont des systèmes de formules booléennes en n variables sous forme disjonctive ternaire, i.e. $a \vee b \vee c$ où a, b et c sont trois variables distinctes ou leurs négations (par exemple, $X_1 \vee \bar{X}_2 \vee X_4$). On cherche à maximiser la fraction d'équations qui possèdent une solution commune, i.e. la fraction de formules rendues vraies par un même choix des valeurs (Vrai ou Faux) des variables.

Théorème 5.1 (S. Arora, S. Safra, [AS] (complété par [ALMSS]))

Il existe $s < 1$ tel que le problème $(1, s)$-MAX E3SAT est NP-complet. Autrement dit, il est NP-difficile de décider, pour tout système de formules booléennes disjonctives ternaires, si on se trouve dans l'une ou l'autre des situations suivantes :

– *il existe une solution commune aux N équations ;*

– *au plus sN équations peuvent être résolues simultanément.*

En d'autres termes, sous l'hypothèse $P \neq NP$, le problème MAX E3SAT n'est pas s-approximable.

Nous renvoyons à [Ch] pour l'histoire et la signification de ce beau théorème. Dans les années 2000, de nouvelles preuves de ce théorème ont été trouvées, voir [D], mais elles restent assez difficiles. Elles ne donnent pas la valeur optimale de s.

5.3. Jeux et répétition parallèle

L'obtention de bornes optimales d'approximabilité s'est faite en deux étapes. La première est la construction de familles de problèmes de seuils d'approximabilité arbitrairement petits. Nous donnons un exemple d'un tel problème, la recherche de stratégies pour les jeux répétés.

On s'intéresse à des jeux coopératifs à deux joueurs. Des couples de questions (q, q') sont tirés suivant une distribution connue. Les joueurs doivent donner des réponses $r = S(q)$ et $r' = S(q')$ sans savoir quelle question a été posée à l'autre. Un prédicat connu à l'avance indique quelles combinaisons de questions et réponses (r, r', q, q') sont gagnantes. Dans un *jeu projectif*, ce prédicat prend la forme suivante : pour chaque question q, chaque question q' et chaque réponse possible r du premier joueur, il y a une unique réponse $r' = \pi_{qq'}(r)$ du second qui les fait gagner tous les deux. Les joueurs cherchent une stratégie commune S qui maximise la probabilité de gain,

$$\text{Valeur du jeu} = \max_S \mathbb{P}_{(q,q')}(S(q') = \pi_{qq'}(S(q))).$$

Dans le jeu, il y a deux paramètres, le nombre n de questions et le nombre k de réponses possibles. Il s'agit donc d'une famille JEUX PROJECTIFS[k] de problèmes d'optimisation combinatoire indexée par k. Une instance de JEUX PROJECTIFS[k] est un jeu projectif à k réponses par question. Dans la littérature, ce problème est parfois appelé LABEL COVER[k].

Théorème 5.2. — *On s'intéresse aux jeux projectifs. Soient n le nombre de questions et k le nombre de réponses par question. Pour tout $\epsilon > 0$, il existe k tel qu'il est NP-difficile de décider entre les deux cas de figure suivants (sachant qu'on est dans l'un des deux).*

1. *La valeur du jeu est* 1.
2. *La valeur du jeu est* $< \epsilon$.

En particulier, le seuil d'approximabilité de JEUX PROJECTIFS[k] tend vers 0 *quand k tend vers l'infini.*

C'est une conséquence folklorique du théorème 5.1 et du théorème de répétition parallèle de Ran Raz (1995), [R1, R2]. Ce théorème affirme que, lorsqu'un jeu est répété ℓ fois (chaque joueur se voit poser ℓ questions tirées indépendamment et donne ℓ réponses, en suivant une stratégie qui repose sur les ℓ questions), la valeur du jeu répété décroît exponentiellement avec ℓ, de façon uniforme.

Il existe depuis peu des preuves directes du théorème 5.2, voir [DH, MR].

5.4. Vers des seuils d'approximabilité optimaux

La seconde étape consiste à utiliser de judicieux *tests de dictature*. On va expliquer le principe de la méthode sur un exemple, le problème MAX E3LIN2. On suit les notes de cours [Ki].

5.4.1. Le problème MAX E3LIN2. — Une instance de E3LIN2 est un système linéaire sur le corps à deux éléments dont chaque équation est *ternaire*, i.e. fait intervenir exactement 3 variables. En notation multiplicative (les variables sont à valeurs dans $\{-1,+1\}$), chaque équation s'écrit sous la forme $aX_{i_1}X_{i_2}X_{i_3} = 1$, où $a \in \{-1,+1\}$. On cherche à maximiser la fraction d'équations qui possèdent une solution commune. Il est immédiat (par l'algèbre linéaire) de décider si un tel système possède une solution. Donc $(1,1)$-MAX E3LIN2 est dans P. Tirer les valeurs des variables indépendamment et uniformément au hasard donne une solution à la moitié des équations, en moyenne. Cela fournit un algorithme de 1/2-approximation.

Théorème 5.3 (J. Håstad, [H2]). — *Pour tous $\epsilon > 0$, $\delta > 0$, $(1-\epsilon, \frac{1}{2}+\delta)$-MAX E3LIN2 est NP-complet. En particulier, le seuil d'approximabilité de MAX E3LIN2 est* 1/2.

5.4.2. Interprétation en termes de tests. — Dans la démonstration du théorème 5.3, les instances de E3LIN2 sont, plutôt que des systèmes linéaires ternaires, des distributions de probabilités I sur l'ensemble (fini) des équations linéaires ternaires en n variables (commodité technique). Tirons une équation au hasard selon la distribution I. On peut voir le choix d'un vecteur $X \in \{-1,+1\}^n$ comme une tentative de prouver que I doit être acceptée.

– Si I est acceptée, il existe un vecteur $X \in \{-1,+1\}^n$ tel que, sous I, $\mathbb{P}_I(X$ résout l'équation$) \geq c = 1-\epsilon$. On appelle cette étape le *test de complétude*. Si l'instance I doit être acceptée, il en existe une preuve qui est convaincante avec probabilité $\geq c$.
– Si I est rejetée, alors pour tout $X \in \{-1,+1\}^n$, sous I, $\mathbb{P}_I(X$ résout l'équation$) < s = \frac{1}{2}+\delta$. On appelle cette étape le *test de sûreté*. Si l'instance I doit être rejetée, aucune preuve n'est convaincante avec probabilité $\geq s$.

Le test porte sur 3 bits seulement de la preuve X. En ce sens, le théorème 5.3 est un raffinement ultime du théorème PCP : lire trois bits tirés au hasard d'une preuve convenablement codée suffit pour se convaincre de sa consistance, avec une probabilité d'erreur $< 1/2$.

5.4.3. Réduction. — La démonstration du théorème 5.3 repose sur une réduction depuis JEUX PROJECTIFS$[k]$ pour un k quelconque.

Il s'agit d'associer à un jeu I à n questions une distribution de probabilité I' sur l'ensemble des équations linéaires ternaires en n' variables, de sorte que

– *Complétude.* Si le jeu possède une stratégie de valeur proche de 1, il existe un vecteur $X \in \{-1,+1\}^n$ qui résout presque toute équation au sens de la distribution I'.
– *Sûreté.* S'il existe un vecteur $X \in \{-1,+1\}^n$ qui résout les équations avec probabilité (sous I') au moins $s > \frac{1}{2}$, alors le jeu possède une stratégie dont la valeur est bornée inférieurement.

On choisit $n' = 2^k n$. On note Q l'ensemble (à n éléments) des questions, et R l'ensemble (à k éléments) des réponses. À chaque question q, on associe 2^k variables $X_{q,t} \in \{-1,+1\}$, où l'indice t décrit $\{-1,+1\}^R$. $Q \times Q$ est muni de la distribution de probabilité qui fait partie intégrante du jeu. On décrit une variable aléatoire à valeurs dans l'ensemble des équations ternaires en les inconnues $X_{q,t}$ comme suit. On tire au hasard un couple de questions (q,q'), on tire au hasard indépendamment trois vecteurs x, y, $z \in \{-1,+1\}^R$ suivant les lois de Bernoulli $\mathcal{B}(\frac{1}{2})^{\otimes k}$, $\mathcal{B}(\frac{1}{2})^{\otimes k}$ et $\mathcal{B}(1-\epsilon)^{\otimes k}$, on tire $a \in \{-1,+1\}$ suivant $\mathcal{B}(\frac{1}{2})$ et on produit l'équation

$$aX_{q',x}X_{q,\Pi_{qq'}(y)}X_{q',axyz} = 1,$$

où on a noté $\Pi_{qq'}(y)$ le vecteur de composantes $(\Pi_{qq'}(y))_i = y_{\pi_{qq'}(i)}$.

La loi de cette variable représente l'instance cherchée, de taille $2^k n$, de E3LIN2.

5.4.4. Interprétation en termes de codage. — Ce qui se déroule sous nos yeux, c'est le codage d'une preuve. Du côté jeux, la preuve que la valeur d'un jeu est $\geq c$, c'est la stratégie S, c'est-à-dire la collection des réponses $S(q) \in R$, $q \in Q$. On code chaque élément r de R sous la forme d'une fonction booléenne sur $\{-1,+1\}^R$, la fonction qui à $x \in \{-1,+1\}^R$ associe sa r-ième coordonnée x_r (une telle fonction est appelée *dictateur*, car la r-ième coordonnée décide toute seule de la valeur de la fonction). Ce code est extrêmement coûteux (chaque réponse est représentée par un mot de longueur 2^{2^k}), mais cela n'a aucune importance. La stratégie S est donc codée en une phrase constituée de n fonctions booléennes.

À chaque phrase (i.e. une suite de fonctions booléennes $f_q : \{-1,+1\}^R \to \{-1,+1\}$, $q \in Q$), on peut associer le vecteur X donné par

$$X_{q,t} = f_q(t).$$

Réciproquement, un vecteur détermine uniquement une phrase, en général incompréhensible, car les fonctions qui la constituent ne sont pas toutes des dictateurs. L'art du décodage est de reconstituer une phrase compréhensible à partir d'une phrase ayant subi un brouillage modéré. L'agencement des équations est choisi de sorte que si X résout un peu plus de la moitié des équations, alors le procédé de décodage qu'on va décrire reconstitue une stratégie S qui a une probabilité bornée inférieurement (quoique faible) de gagner.

5.4.5. Test de dictature. — Dans un premier temps, on va identifier, parmi les fonctions booléennes $\{-1,+1\}^R \to \{-1,+1\}$, celles qui sont proches de dictateurs.

On remarque que les dictateurs sont des fonctions linéaires, i.e. dans notre notation multiplicative, elles satisfont, pour tous x, $y \in \{-1,+1\}^R$,

$$f(x)f(y)f(xy) = 1.$$

D'où le test de linéarité : tirer x, y uniformément au hasard et calculer $f(x)f(y)f(xy)$. On montre aisément que, si $\mathbb{P}_{x,y}(f(x)f(y)f(xy) = 1) \geq \frac{1}{2} + \delta$, alors la distance de Hamming de f aux fonctions linéaires est $\leq \frac{1}{2} - \delta$. Noter que le test ne nécessite que la connaissance de trois bits dans le mot que constitue f.

Parmi les fonctions linéaires, les dictateurs ont la particularité d'être impairs, i.e. $f(-x) = -f(x)$. On modifie le test en conséquence : on tire en outre un $a \in \{-1,+1\}$ et on calcule $af(x)f(y)f(axy)$. Les dictateurs passent le test à coup sûr, et le test, outre les fonctions éloignées des fonctions linéaires, rejette en sus la fonction constante 1, par exemple.

Parmi les fonctions linéaires, les dictateurs possèdent encore une particularité : ils sont sensibles au bruit. Si on change le signe de chaque bit de y indépendamment avec probabilité ϵ (ce qui revient à multiplier y par un vecteur indépendant z tiré selon $\mathcal{B}(1-\epsilon)^{\otimes k}$), alors $\mathbb{P}_{y,z}(f(y) \neq f(yz))$ vaut $1-\epsilon$ pour les dictateurs, et au plus $(1-\epsilon)^3$ pour les autres fonctions linéaires impaires. Cela conduit au choix suivant.

Proposition 5.4 (Test de dictature de Håstad). — *Tirer au hasard indépendamment trois vecteurs x, y, $z \in \{-1,+1\}^R$ suivant les lois de Bernoulli $\mathcal{B}(\frac{1}{2})^{\otimes k}$, $\mathcal{B}(\frac{1}{2})^{\otimes k}$ et $\mathcal{B}(1-\epsilon)^{\otimes k}$, tirer indépendamment $a \in \{-1,+1\}$ suivant $\mathcal{B}(\frac{1}{2})$. Calculer*

$$af(x)f(y)f(axyz).$$

Accepter f si le résultat est 1, rejeter f sinon. Ce test a les propriétés suivantes.

- *Complétude. Si f est un dictateur, alors f est acceptée avec probabilité $\geq 1-\epsilon$.*
- *Sûreté. Si f est acceptée avec probabilité $\geq 1-\epsilon-\alpha$, alors f est à distance de Hamming $< \alpha$ d'un dictateur.*

5.4.6. Décodage aléatoire. — En réalité, l'objectif n'est pas tellement de détecter les fonctions f qui sont proches de dictateurs. Ce qu'on cherche, c'est à associer à f quelconque une coordonnée $r = r(f)$, d'une façon invariante par certains homorphismes de groupes (de sorte que $r(f \circ \Pi_{qq'}) = \pi_{qq'}(r(f))$ par exemple). Le décodage n'a pas besoin d'être très performant. Il suffit que l'égalité $r(f_{q'}) = r(f_q \circ \Pi_{qq'})$ se produise avec probabilité bornée inférieurement dès que $\mathbb{P}(f \text{ passe le test}) \geq \frac{1}{2} + \delta$.

On construit une variable aléatoire à valeurs dans les décodages $f \mapsto r(f)$ comme suit. On utilise la transformation de Fourier-Walsh (pour le groupe abélien $\{-1,+1\}^R$). On écrit

$$f = \sum_{T \subset R} \hat{f}_T \chi_T, \tag{1}$$

où les χ_T sont les caractères du groupe $\{-1,+1\}^R$, $\chi_T(x) = \prod_{i \in T} x_i$. Si $f : \{-1,+1\}^R \to \{-1,+1\}$ est booléenne, $\|f\|_2 = 1$, donc l'identité de Parseval donne $\sum_{T \subset R} \hat{f}_T^2 = 1$. On peut donc voir les carrés des coefficients de Fourier $\hat{f}_T^2$ comme une distribution de probabilité sur les sous-ensembles de R. On tire $T(f)$ au hasard suivant cette distribution (en éliminant les ensembles trop grands ou de taille paire). On tire ensuite au hasard un élément $r(f)$ de $T(f)$.

Proposition 5.5. — *On modifie le test de la proposition 5.4 comme suit. Il porte désormais sur un couple (f,g) de fonctions booléennes sur $\{-1,+1\}^R$. Avec les mêmes choix de variables aléatoires x, y, z, a, on accepte (f,g) si et seulement si $af(x)g(y)f(axyz) = 1$. Le test obtenu a les propriétés suivantes. Pour tout $\delta > 0$, il existe $\delta'(\delta, \epsilon) > 0$ indépendant de k tel que*

- *Complétude. Si f et g sont des dictateurs, alors (f,g) est accepté avec probabilité $\geq 1 - 2\epsilon$.*
- *Sûreté. Si (f,g) est accepté avec probabilité $\geq \frac{1}{2} + \delta$, alors $\mathbb{P}(r(f) = r(g)) \geq \delta'$.*

5.4.7. Preuve du théorème 5.3. — Complétude. On code une stratégie en une phrase constituée de dictateurs, qu'on convertit en un vecteur X. Par construction, X est solution d'une équation aléatoire si et seulement si le couple de fonctions $(f_{q'}, f_q \circ \Pi_{qq'})$ passe le test, c'est vrai avec probabilité $\geq 1 - 2\epsilon$.

Sûreté. Un vecteur X, c'est une suite de fonctions booléennes f_q. Considérons la stratégie S définie par $S(q) = r(f_q)$. Si X est solution d'une équation aléatoire avec probabilité $\geq \frac{1}{2} + \delta$, alors, pour une proportion $\geq \frac{\delta}{2}$ des couples (q, q'), le couple $(f_{q'}, f_q \circ \Pi_{qq'})$ passe le test avec probabilité $\geq \frac{1}{2} + \frac{\delta}{2}$. Avec probabilité $\geq \delta'$, $\pi_{qq'}(r(f_{q'})) = r(f_q \circ \Pi_{qq'})$, donc la stratégie gagne avec probabilité $\geq \frac{\delta\delta'}{2}$, le jeu a une valeur $\geq \delta'' := \frac{\delta\delta'}{2}$.

On a donc bien construit une réduction de $(1 - 2\epsilon, \delta'')$-JEUX PROJECTIFS$[k]$ à $(1 - \epsilon, \frac{1}{2} + \delta)$-MAX 3LIN2.

6. LE CAS DE MAX CUT

MAX CUT peut être vu comme un problème MAX E2LIN2 restreint. La donnée d'un graphe $G = (V, E)$ équivaut à celui du système d'équations suivant. Il y a une variable x_u par sommet et une équation $x_u x_v = -1$ par arête (u, v). La construction d'une réduction analogue à celle décrite pour MAX E3LIN2 nécessiterait un test de dictature à 2 requêtes, ce que personne n'a réussi à faire marcher jusqu'à présent. En revanche, on est parvenu à trouver une réduction depuis un problème plus restreint que les jeux projectifs, les jeux uniques.

6.1. Jeux uniques

Définition 6.1. — *Un* jeu unique *est un jeu qui est projectif dans les deux sens, i.e. les réponses gagnantes sont à la fois de la forme $r' = \pi_{qq'}(r)$ et $r = \pi_{q'q}(r')$. Autrement dit, les applications $\pi_{qq'}$ sont supposées bijectives.*

Il est immédiat de décider si la valeur d'un jeu unique vaut 1 ou non. En effet, la stratégie de valeur 1 est uniquement déterminée par la réponse à une question (les autres réponses s'en déduisent de proche en proche). Par conséquent, $(1, 1)$-JEUX UNIQUES$[k]$ est dans P. À part ce détail, les jeux uniques sont-ils réellement plus faciles que les jeux projectifs généraux ?

Conjecture 6.2 (S. Khot, [Kh1], Unique Games Conjecture)
On s'intéresse aux jeux uniques. Soient n le nombre de questions et k le nombre de réponses par question. Pour tous $\epsilon > 0$, $\delta > 0$, il existe k tel qu'il est NP-difficile de décider entre les deux cas de figure suivants (sachant qu'on est dans l'un des deux).

1. *La valeur du jeu est $\geq 1 - \epsilon$.*
2. *La valeur du jeu est $< \delta$.*

D'une certaine façon, UGC est équivalente à un problème isopérimétrique sur les graphes, qui porte sur les ensembles de sommets assez petits, voir [RS].

Il existe des algorithmes d'approximation pour JEUX UNIQUES$[k]$. Par exemple, l'algorithme de E. Chlamtac, K. Makarychev et Yu. Makarychev donne, pour tout jeu unique de valeur $1 - \epsilon$, une stratégie dont la probabilité de gain vaut au moins $1 - \epsilon O(\sqrt{\log k \log n})$, [CcMM]. Il existe un algorithme sous-exponentiel qui donne une approximation en $1 - \epsilon^\alpha$, pour un $\alpha > 0$, [ABS]. Cela peut donner l'impression que le problème des jeux uniques est moins difficile que les problèmes NP-complets.

Les opinions sont partagées sur la conjecture des jeux uniques (UGC). En revanche, personne ne parie sur le fait que le problème des jeux uniques est dans P. Si bien qu'on peut s'en servir comme hypothèse de référence pour prouver des résultats de difficulté d'approximation, comme on le fait pour $P \neq NP$. Ce programme a eu un succès inattendu : pour de nombreux problèmes, le seuil exact d'approximabilité sous l'hypothèse UGC est connu. On pourra consulter avec profit les survols [Kh2] et [Kh3].

6.2. Difficulté d'approximation de MAX CUT

On rappelle qu'on dispose d'une α-approximation de MAX CUT pour tout $\alpha < \alpha_{GW}$, la constante de Goemans et Williamson.

Théorème 6.3 (S. Khot, G. Kindler, E. Mossel, R. O'Donnell [KKMO])
Sous l'hypothèse UGC, MAX CUT ne possède pas d'α-approximation pour $\alpha > \alpha_{GW}$. Autrement dit, le seuil d'approximabilité de MAX CUT (sous UGC) est α_{GW}.

6.2.1. La réduction. — De nouveau, pour alléger l'exposé, on élargit la notion de graphe : un graphe pondéré est une distribution de probabilité sur les arêtes du graphe complet, i.e. l'ensemble des paires de points d'un ensemble V. La coupe maximale d'un graphe pondéré est le maximum sur les coloriages de la probabilité qu'une arête tirée au hasard soit bicolore.

Pour tous $\epsilon' > 0$, $\delta > 0$ et k entier, on va construire $\epsilon > 0$, $\delta' > 0$ indépendants de k et une réduction de $(1-\epsilon, \delta')$-JEUX UNIQUES$[k]$ à $(1-\epsilon', \alpha_{GW}+\delta)$-MAX CUT. Sous la conjecture UGC, cela prouvera que MAX CUT ne possède pas de $\frac{\alpha_{GW}+\delta}{1-\epsilon'}$-approximation.

Étant donné un jeu unique J à n questions et k réponses, on considère l'ensemble $V = Q \times \{-1,+1\}^R$. Il s'agit de construire une distribution de probabilité sur l'ensemble des paires de points de V (baptisées arêtes) telle que

- S'il existe une stratégie qui gagne avec probabilité $\geq 1-\epsilon$, alors il existe un coloriage de V tel que les arêtes sont bicolores avec probabilité $\geq 1-\epsilon'$.
- S'il existe un coloriage de V tel que les arêtes sont coupées avec probabilité $\geq \alpha_{GW}+\delta$, alors il existe une stratégie qui gagne avec probabilité $\geq 1-\epsilon$.

Soit $c \in [0,1]$. La distribution voulue est la loi de la variable aléatoire à valeurs dans l'ensemble des arêtes, définie comme suit. On tire au hasard deux couples de questions (q,q') et (q,q''). On tire au hasard indépendamment deux vecteurs x' et $z \in \{-1,+1\}^R$ suivant $\mathcal{B}(\frac{1}{2})^{\otimes k}$ et $\mathcal{B}(1-c)^{\otimes k}$, on considère $x'' = z\Pi_{qq''}^{-1} \circ \Pi_{qq'}(x') \in \{-1,1\}^R$ et on produit l'arête $((q',x'),(q'',x''))$. On note G le graphe pondéré ainsi défini.

6.2.2. Complétude. — À une stratégie S correspond un coloriage de V : le sommet $(q,x) \in \{-1,1\}^R$ est colorié par sa $S(q)$-ième coordonnée (coloriage dictatorial). Si c est égal à 1 (i.e. tous les bits de $\Pi_{qq''}^{-1} \circ \Pi_{qq'}(x')$ sont renversés), la probabilité que l'arête $((q',x'),(q'',x''))$ soit coupée est égale à la probabilité que $S(q'') = \pi_{qq''} \circ \pi_{qq'}^{-1}(S(q'))$, i.e. à la valeur de la stratégie S. Lorsque $c \neq 1$, cette probabilité est au pire multipliée par c, d'où coupe maximale$(G) \geq c$ valeur(J).

6.2.3. Sûreté. — Inversement, soit $s \in [0,1]$. Un coloriage du graphe pondéré G est une fonction booléenne sur $Q \times \{-1,+1\}^R$, elle induit une famille $f_q : \{-1,1\}^R \to \{-1,1\}$ de fonctions booléennes sur $\{-1,+1\}^R$. Si la probabilité qu'une arête soit coupée est $> s$, alors en moyenne, la fonction f_q a la propriété suivante.

$$Sens_c(f_q) := \mathbb{P}_{x,z}(f_q(xz) \neq f_q(x)) > s.$$

Ce nombre s'appelle la sensibilité au c-bruit, [BKS]. La fin de la preuve repose sur l'observation que pour une fonction de grande sensibilité au bruit, au moins une des

coordonnées a une grande influence. D'où une stratégie S : tirer $S(q)$ au hasard parmi les coordonnées d'influence supérieure à un certain seuil. On vérifie enfin que la valeur de cette stratégie est bornée inférieurement. Le miracle, c'est que la dépendance en c de s est connue exactement ($s > \frac{1}{\pi}\arccos(1-2c)$), c'est le Théorème MIS (`Majority Is Stablest`). On obtient comme borne inférieure d'approximabilité le maximum des rapports $\frac{s}{c}$, qui coïncide avec la constante de Goemans et Williamson.

6.3. Le Théorème Majority is Stablest

On peut penser à une fonction booléenne $\{-1,+1\}^n \to \{-1,+1\}$ comme à un procédé pour agréger des votes, i.e. produire une décision à partir des votes de n électeurs. Par exemple,

Définition 6.4. — *Le i-ième* dictateur *est* $\mathrm{Dict}_i(x) = x_i$. *La* majorité *est* $\mathrm{Maj}(x) = \mathrm{signe}(\sum x_i)$.

Un procédé d'agrégation devrait avoir les propriétés suivantes.

1. Aucun électeur ne joue de rôle prépondérant.
2. Des erreurs dans le dépouillement des votes ont peu de chance de faire basculer le résultat.

6.3.1. Influence. — La première clause peut se traduire mathématiquement par la notion d'influence d'un électeur. Cette notion est née en probabilités (phénomènes de seuil) dans les années 80 (voir [Ru]), mais on la rencontre implicitement dès les années 70 (voir [M]). Elle a été introduite dans la théorie du choix social par M. Ben Or et N. Linial, [BOL].

Définition 6.5. — *L'*influence $\mathrm{Inf}_i(f)$ *du i-ième électeur sur f est la probabilité que, lorsque le i-ième électeur change d'avis, la valeur de f change.*

$$\mathrm{Inf}_i(f) = \mathbb{P}(f(xe_i) \neq f(x)),$$

où $e_i \in \{-1,+1\}^n$ est le vecteur dont les coordonnées valent 1 sauf la i-ième.

6.3.2. Sensibilité au bruit. — On a déjà rencontré la sensibilité au bruit, au cours de l'étude de MAX CUT. Elle était apparue antérieurement en probabilités, [BKS].

Définition 6.6. — *La* sensibilité au c-bruit *de f est la probabilité que, lorsque chaque vote est modifié indépendamment avec probabilité c, la valeur de f change.*

$$\mathrm{Sens}_c(f) = \mathbb{P}_{x,z}(f(xz) \neq f(x)),$$

où les coordonnées $z_i \in \{-1,+1\}$ sont i.i.d., indépendantes de x, et $\mathbb{P}(z_i = -1) = c$.

Par exemple, pour le dictateur Dict_i,

$$\mathrm{Inf}_i(\mathrm{Dict}_i) = 1, \quad \mathrm{Inf}_j(\mathrm{Dict}_i) = 0 \text{ si } j \neq i \; ; \quad \mathrm{Sens}_c(\mathrm{Dict}_i) = c.$$

Pour la majorité, il résulte du Théorème Central Limite que

$$\mathrm{Inf}_i(\mathrm{Maj}) \sim \frac{2}{\sqrt{\pi n}}; \quad \lim_{n\to\infty} \mathrm{Sens}_c(\mathrm{Maj}) = \frac{1}{\pi}\arccos(1-2c).$$

6.3.3. Le Théorème MIS. — De tous les procédés d'agrégation, la majorité est celui qui satisfait le mieux aux deux critères d'influence et de sensibilité ci-dessus. C'est la substance du Théorème MIS (`Majority is stablest`) (qui complète des résultats antérieurs de [BKS]).

Théorème 6.7 (E. Mossel, R. O'Donnell, K. Oleskiewicz, [MOO])
Soit $c \in [0, \frac{1}{2}]$. De toutes les fonctions booléennes $\{-1,+1\}^n \to \{-1,+1\}$, de moyenne nulle, dont les influences sont petites, Maj est celle dont la sensibilité au c-bruit est asymptotiquement la plus faible, lorsque n tend vers l'infini. Si $c \in [\frac{1}{2}, 1]$, Maj a la sensibilité au c-bruit la plus forte (sans condition de moyenne nulle).

En fait, l'énoncé est non asymptotique : pour tout $\epsilon > 0$, il existe $\tau(\epsilon)$ indépendant de n tel que, si toutes les influences $\mathrm{Inf}_i(f) < \tau$, alors $\mathrm{Sens}_c(f) \geq \frac{1}{\pi}\arccos(1-2c) - \epsilon$ pour $c \in [0, \frac{1}{2}]$ (si moyenne nulle), $\mathrm{Sens}_c(f) \leq \frac{1}{\pi}\arccos(1-2c) - \epsilon$ pour $c \in [\frac{1}{2}, 1]$.

La preuve du théorème 6.7 repose sur

1. Principe d'invariance : on remplace le cube discret $\{-1,+1\}^n$, muni de la mesure de probabilité uniforme, par l'espace gaussien, i.e. l'espace euclidien $\mathbb{R}^n$ muni de la mesure gaussienne γ_n, de densité $(2\pi)^{-n/2}\exp(-|x|^2/2)$.
2. Dans l'espace gaussien, un argument de symétrisation dû à Ehrhard et Borell montre que parmi les fonctions de moyenne nulle, à valeurs dans $[-1,1]$, les fonctions « signe de forme linéaire » maximisent Sens_c, $c < \frac{1}{2}$.
3. Soit $c > \frac{1}{2}$. Si $g(x) = \frac{1}{2}(f(x) - f(-x))$, alors $\mathrm{Sens}_c(f) \geq \mathrm{Sens}_c(g) = 1 - \mathrm{Sens}_{1-c}(g) \geq 1 - \frac{1}{\pi}\arccos(1-c) - \epsilon = \frac{1}{\pi}\arccos(c) - \epsilon$.

On détaille maintenant les deux premières étapes.

6.3.4. Principe d'invariance. — Si $f : \{-1,+1\}^n \to \mathbb{R}$, alors f s'étend à $\mathbb{R}^n$ de façon unique en un polynôme de degré partiel 1 (décomposition de Fourier-Walsh, formule (1)). Le principe d'invariance suivant généralise au cas des fonctions non linéaires le Théorème Central Limite. Il exprime quantitativement le fait que, pour certaines fonctions f, les lois de f sur $\{-1,+1\}^n$ et sur $\mathbb{R}^n$ gaussien sont voisines. Il remonte à V. Rotar en 1979, [Ro]. La version ci-dessous est celle de [MOO].

Proposition 6.8. — *Soient x tiré uniformément dans $\{-1,+1\}^n$ et Y tiré indépendamment dans l'espace gaussien. Soit $f : \{-1,+1\}^n \to \mathbb{R}$ de degré $\leq d$. On suppose que les influences satisfont $\mathrm{Inf}_i(f) \leq \tau$. Alors pour toute fonction $\Psi : \mathbb{R} \to \mathbb{R}$ de classe C^4,*

$$|\mathbb{E}(\Psi(f(x))) - \mathbb{E}(\Psi(f(Y)))| \leq \tau 10^d \parallel \Psi \parallel_{C^4} .$$

La preuve consiste à remplacer une par une les variables x_i par les Y_i (c'est pourquoi les influences interviennent). La formule de Taylor permet d'exploiter le fait que les premiers moments des deux variables coïncident, $\mathbb{E}(x_i^p) = \mathbb{E}(Y_i^p)$ pour $p \leq 3$. Enfin, on utilise l'inégalité d'hypercontractivité de Bonami, [B], pour estimer le reste.

6.3.5. La symétrisation d'Ehrhard. — C'est un procédé pour prouver des inégalités fonctionnelles sur l'espace gaussien $(\mathbb{R}^n, \gamma_n)$.

Définition 6.9 (A. Ehrhard, [Eh]). — *Soit $u \in L_2(\mathbb{R}^n, \gamma_n)$ une fonction positive. Sa* symétrisée *est la fonction décroissante u^* définie sur $\mathbb{R}$ par*

$$\gamma_n(\{u > t\}) = \gamma_1(\{u^* > t\}).$$

Théorème 6.10 (C. Borell, [Bor]). — *Soit $u \in L_2(\mathbb{R}^n, \gamma_n)$ une fonction positive. Alors pour $c < \frac{1}{2}$,*

$$\mathrm{Sens}_c(u) \geq \mathrm{Sens}_c(u^*).$$

L'argument utilise le fait que la sensibilité au bruit s'exprime en fonction du semi-groupe d'Ornstein-Uhlenbeck U_t,

$$1 - 2\mathrm{Sens}_c(u) = \langle U_t u, u\rangle \quad \text{pour} \quad e^{-t} = 1 - 2c,$$

pour lequel on a un principe du maximum.

6.4. Autres problèmes de satisfaction de contraintes

Le Théorème MIS, avec ses bornes optimales explicites, semble indispensable à la preuve que nous venons d'esquisser de la difficulté d'approximation de MAX CUT. Il n'en est rien.

Théorème 6.11 (P. Raghavendra, [Ra]). — *Pour une classe de problèmes de satisfaction de contraintes assez vaste (elle contient MAX CUT, MAX E3SAT, MAX E3LIN2,..., mais pas SPARSEST CUT), il existe un procédé systématique qui produit simultanément*

- *un algorithme d'α-approximation par programmation semi-définie, pour $\alpha < \alpha_{\max}$, où $\alpha_{\max}$ n'est en général pas connu, mais est calculable ;*
- *une preuve de difficulté d'approximation sous UGC pour $\alpha > \alpha_{\max}$.*

Ce théorème ne donne d'information utile que pour les problèmes dont le seuil d'approximabilité est une constante.

On explique quelques idées de la preuve dans l'exemple de MAX CUT. La plus frappante est d'associer à chaque instance sur laquelle l'algorithme d'approximation par programmation semi-définie n'est pas très performant une preuve de difficulté d'approximation.

6.4.1. Relaxation. — La relaxation semi-définie n'est pas sensiblement différente de celle de Goemans-Williamson. Elle produit des plongements y du graphe donné G dans la sphère unité S^{n-1} de l'espace euclidien ℓ_2^n qui maximisent la quantité $SDP(y)$. Le maximum est noté $SDP(G)$. Il est supérieur au maximum $OBJ(G)$ de la fonction objectif.

6.4.2. Procédure d'arrondi. — L'étape suivante, c'est la procédure d'arrondi, destinée à obtenir une minoration du saut d'intégralité $\min_G \frac{OBJ(G)}{SDP(G)}$. Elle est fondée sur l'intuition suivante. Soit G un graphe plongé dans la sphère unité. Soit G' l'image de G par une rotation. Soit $G'' = G \coprod G'$. Alors $SDP(G'') = SDP(G)$ alors que $OBJ(G'') \leq OBJ(G)$. Donc la relaxation semi-définie est moins performante sur le graphe G'' que sur G. En itérant le procédé une infinité de fois, et en passant à la limite, on trouve un graphe H_G entièrement symétrique : ses sommets sont tous les points de la sphère unité S^{n-1}, ses arêtes toutes les paires de points, pondérées par une mesure sur l'intervalle $[0, 2]$. Voici la procédure d'arrondi : soit $x : S^{n-1} \to \{-1, +1\}$ un coloriage optimal de H_G ; restreindre x à l'image de G par une rotation tirée au hasard. Il se trouve que le coloriage optimal de H_G est donné par un hyperplan (Théorème 1.2), mais cette information n'est pas indispensable pour la suite.

6.4.3. Saut d'intégralité. — Le saut d'intégralité est calculable algorithmiquement. En effet, pour toute résolution $\epsilon > 0$, il existe d tel que la projection orthogonale de G sur un espace de dimension d tiré au hasard respecte SDP et les contraintes à ϵ près, avec forte probabilité (concentration). À ϵ près, les graphes pondérés en dimension d tombent dans un nombre fini de paquets, qu'il suffit d'explorer systématiquement pour trouver $\min_G \frac{OBJ(G)}{SDP(G)}$ à ϵ près. Toutefois, on n'a aucune garantie sur la complexité de cet algorithme.

6.4.4. Test de dictature. — Soit R un ensemble fini (destiné à être l'ensemble des réponses d'un jeu unique). Étant donné un graphe de référence G (vu comme une distribution de probabilité sur les paires de points d'un ensemble V), on décrit un test de dictature de complétude $c = SDP(G) - \epsilon$ et de sûreté $s = OBJ(G) + \epsilon$ sur les fonctions booléennes sur $\{-1, +1\}^R$. Soit $y : V \to \ell_2$ le plongement solution de la relaxation semi-définie. On choisit pour chaque sommet $v \in V$ une variable aléatoire z_v à valeurs dans $\{-1, +1\}^2$ telle que pour toute arête (u, v),

$$\mathbb{E}(1 - z_u \cdot z_v) = 1 - y_u \cdot y_v$$

(la relaxation semi-définie est ajustée expressément pour fournir ces variables). Étant donnée $f : \{-1, +1\}^R \to \{-1, +1\}$,

- tirer au hasard une arête (u, v) ;
- faire R tirages indépendants de la variable z_u, pour obtenir un vecteur $Z_u \in \{-1, +1\}^R$; faire de même pour v et obtenir Z_v ;
- accepter f si $f(Z_u) \neq f(Z_v)$, rejeter f sinon.

6.4.5. Analyse du test. — **Complétude**. Si f est le dictateur x_r,

$$\mathbb{P}(f(Z_u) \neq f(Z_v)) = \mathbb{P}_{u,v,z_u,z_v}(z_u \neq z_v) = \frac{1}{2}\mathbb{E}_{u,v}(1 - y_u \cdot y_v) = SDP(G).$$

Sûreté. On suppose que les influences des variables sur f sont uniformément faibles. Une généralisation du principe d'invariance (Proposition 6.8) permet de remplacer les variables booléennes du test par des variables gaussiennes, puis par des variables uniformément distribuées sur la sphère. La fonction f est remplacée par son extension polynomiale (formule (1)). Elle n'est plus booléenne, mais on peut tout de même lui associer un coloriage du graphe symétrique H_G (pour chaque point t de la sphère unité, on tire au hasard sa couleur suivant $\mathcal{B}(f(t))$), et $\mathbb{P}(f(Z_u) \neq f(Z_v))$ est proche de la valeur de la fonction OBJ sur ce coloriage. On conclut que la sûreté est $\leq OBJ(H_G) + \epsilon$.

6.4.6. Réduction. — Elle est très semblable à celle décrite plus haut pour MAX CUT.

6.4.7. Généralisation. — Le théorème 6.11 s'applique à la classe de problèmes suivants. Chaque problème $GCSP(a, R, \mathcal{C})$ est spécifié par la donnée

- d'un entier a, l'arité ;
- d'un ensemble fini R ;
- d'une famille $\mathcal{C}$ de fonctions de coût $R^a \to [-1, 1]$, invariante par les permutations de R.

Une instance du problème $GCSP(a, R, \mathcal{C})$ est la donnée

- d'un ensemble V de variables à valeurs dans R ;
- d'une distribution de probabilité sur les sous-ensembles à k éléments de V ;
- pour tout $S \subset V$ de taille a, d'une fonction de coût $C_S : R^S \to [-1, 1]$ choisie dans la famille $\mathcal{C}$.

Il s'agit de trouver un choix de valeurs des variables, i.e. un élément $y \in R^V$, qui maximise le coût moyen

$$OBJ(y) = \mathbb{E}_S(C_S(y_{|S})).$$

Dans le cas particulier où $R = \{-1, +1\}$ a 2 éléments, les coûts sont à valeurs dans $\{0, 1\}$, et la distribution est uniforme, on retrouve le problème de maximiser la fraction de contraintes satisfaites par des variables booléennes. Par exemple, MAX CUT correspond au cas où $a = 2$ et $\mathcal{C}$ est réduit à la fonction $(x_1, x_2) \mapsto -x_1x_2$, $\{-1, +1\}^2 \to \{-1, +1\}$. MAX E3LIN2 correspond au cas où $a = 3$ et $\mathcal{C}$ est réduit aux deux fonctions $(x_1, x_2, x_3) \mapsto \pm x_1x_2x_3$, $\{-1, +1\}^3 \to \{-1, +1\}$. Pour MAX E3SAT, $a = 3$ et $\mathcal{C}$ contient les 8 fonctions $\{-1, +1\}^3 \to \{-1, +1\}$.

7. HIÉRARCHIES

Après 15 ans d'existence, la méthode de relaxation semi-définie reste plus heuristique que systématique. Il y a pourtant eu de nombreuses tentatives d'en systématiser certaines étapes. Les hiérarchies de Sherali-Adams, Lovasz-Schrijver et Lasserre en font

partie, [SA, LS, La]. On va décrire la méthode de Lasserre. Elle porte sur la seconde étape, le choix d'une relaxation, une fois le problème arithmétisé. L'arithmétisation d'un problème d'optimisation combinatoire produit un sous-ensemble K de $\mathbb{R}^n$ et une fonction objectif à maximiser sur K. Dans le cas (fréquent) où K est défini par des inéquations algébriques et f est un polynôme, la théorie de Lasserre construit automatiquement une suite de relaxations semi-définies dont les maxima convergent en décroissant vers le maximum de f sur K.

7.1. Le Positivstellensatz

On note $\mathcal{P}$ l'espace des polynômes à coefficients réels sur $\mathbb{R}^n$, $\mathcal{P}^*$ son dual. On s'intéresse au cône convexe $\mathcal{Q}_K \subset \mathcal{P}$ des polynômes qui prennent des valeurs strictement positives sur K. Supposons K défini par un système d'inéquations polynomiales $\{g_j \geq 0\,;\, j = 1, \ldots, m\}$. On note $g_0 = 1$ le polynôme constant. L'adhérence $\overline{Q_K}$ contient l'ensemble $\mathcal{R}_K$ des combinaisons linéaires $\sum_{j=0}^m \sigma_j g_j$ où chaque polynôme σ_j est une somme de carrés de polynômes. Le Positivstellensatz est une réciproque partielle.

Théorème 7.1 (M. Putinar [Pu]). — *On suppose qu'il existe $q \in \mathcal{R}_K$ tel que l'ensemble $\{q \geq 0\}$ soit compact. Alors $\mathcal{Q}_K \subset \mathcal{R}_K$. Autrement dit, tout polynôme qui prend des valeurs strictement positives sur K est combinaison linéaire des polynômes g_j à coefficients sommes de carrés.*

7.2. Dualité

Soit $\mathcal{Q}_K^{*1}$ le convexe des formes linéaires sur $\mathcal{P}$ qui prennent des valeurs positives ou nulles sur $\mathcal{Q}_K$, et qui prennent la valeur 1 sur la fonction $g_0 = 1$. Lorsque l'hypothèse du théorème 7.1 est satisfaite, pour $\mu \in \mathcal{P}^*$,

$$\mu \in \mathcal{Q}_K^{*1} \Leftrightarrow \langle \mu, g_0 \rangle = 1 \text{ et } \forall q \in \mathcal{P},\ \forall j = 0, \ldots, m,\ \langle \mu, q^2 g_j \rangle \geq 0.$$

Autrement dit, vérifier qu'une forme linéaire μ appartient à $\mathcal{Q}_K^{*1}$ se ramène à vérifier que les $m+1$ formes quadratiques $F_{\mu,g_j} : q \mapsto \langle \mu, q^2 g_j \rangle$ sur $\mathcal{P}$ sont positives semi-définies.

Si f est un polynôme et $\mu \in \mathcal{Q}_K^{*1}$, alors $\langle \mu, f \rangle \leq \max_K f$, avec égalité lorsque μ est l'évaluation en un point où f atteint son maximum. Par conséquent,

$$\begin{aligned} \max_K f &= \max_{\mathcal{Q}_K^{*1}} \langle \mu, f \rangle \\ &= \max\{\langle \mu, f \rangle\,;\, \begin{cases} \langle \mu, g_0 \rangle = 1, \\ \forall j = 0, \ldots, m, \quad F_{\mu,g_j} \text{ est positive semi-définie.} \end{cases} \}. \end{aligned}$$

Il s'agit d'un problème de programmation semi-définie, mais en dimension infinie. Le r-ème problème de la *hiérarchie de Lasserre* associée au choix (f, g_j) d'arithmétisation du problème combinatoire donné est l'approximation de dimension finie obtenue en projetant le problème sur l'espace $\mathcal{P}_{2r}$ des polynômes de degré $\leq 2r$. Autrement dit, μ est remplacée par sa restriction μ^{2r} à $\mathcal{P}_{2r}$. La forme quadratique F_{μ,g_j} est remplacée par sa restriction $F_{\mu,g_j}^{r_j}$ à $\mathcal{P}_{r_j}$, $r_j = r - \lfloor \frac{\deg(g_j)}{2} \rfloor$ (qui ne dépend que de μ^{2r}). Le problème

projeté Π^r est bien posé dès que $r \geq \max\{\lfloor \frac{\deg(f)}{2} \rfloor, \lfloor \frac{\deg(g_j)}{2} \rfloor,\ j = 1, \ldots, m\}$. On montre (voir [La], Theorem 5.6, page 119) que, lorsque r tend vers l'infini, $\max \Pi^r$ tend vers $\max_K f$.

7.3. Le cas de MAX CUT

$K \subset \mathbb{R}^n$ est le cube discret, défini par les inéquations $g_i = x_i^2 - 1 \geq 0$, $g_{n+i} = 1 - x_i^2 \geq 0$. L'hypothèse du théorème 7.1 est satisfaite par $q = \sum_{i=n+1}^{2n} g_{n+i} = n - |x|^2$.

Soit f la fonction objectif

$$f(x) = \sum_{i,\,j=1}^{n} w_{ij} \frac{1}{2}(1 - x_i x_j).$$

La base canonique de $\mathcal{P}_r$ est indexée par les vecteurs de $\mathbb{N}^n$ dont la somme des composantes est $\leq r$. Pour $r = 1$, $\mu = \mu^2 \in \mathcal{P}_2^*$. Notons A la matrice de la forme quadratique F^1_{μ,g_0} sur $\mathcal{P}_1$,

$$A := \begin{pmatrix} \mu_{00\ldots0} & \mu_{10\ldots0} & \mu_{010\ldots0} & \cdots & \mu_{0\ldots01} \\ \mu_{10\ldots0} & \mu_{20\ldots0} & \mu_{110\ldots0} & \cdots & \mu_{10\ldots01} \\ \mu_{010\ldots0} & \mu_{110\ldots0} & \mu_{020\ldots0} & \cdots & \mu_{010\ldots01} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mu_{0\ldots01} & \mu_{10\ldots01} & \mu_{010\ldots01} & \cdots & \mu_{0\ldots02} \end{pmatrix}.$$

Alors

$$\langle \mu, f \rangle = \sum_{i,\,j=1}^{n} w_{ij} \frac{1}{2}(\mu_{0\ldots0} - \mu_{0\ldots0i0\ldots0j0\ldots0}) = \sum_{i,\,j=1}^{n} w_{ij} \frac{1}{2}(A_{1,1} - A_{i+1,j+1}).$$

Les formes quadratiques F^0_{μ,g_i} habitent l'espace $\mathcal{P}_0$ qui est de dimension 1, elles valent

$$\begin{aligned} F^0_{\mu,g_i} &= \langle \mu, g_i \rangle = \mu_{0\ldots020\ldots0} - \mu_{0\ldots0} = A_{i+1,i+1} - A_{1,1}, \\ F^0_{\mu,g_{n+i}} &= \langle \mu, g_{n+i} \rangle = A_{1,1} - A_{i+1,i+1}. \end{aligned}$$

Lorsque μ varie dans $\mathcal{P}_2^*$, A décrit exactement toutes les matrices symétriques de taille $n+1$. La première contrainte est $1 = \langle \mu, g_0 \rangle = \mu_{00\ldots0} = A_{1,1}$. Si F^0_{μ,g_i} et $F^0_{\mu,g_{n+i}}$ sont positives au sens large, $A_{i+1,i+1} = A_{1,1} = 1$, i.e. les coefficients diagonaux de A sont tous égaux à 1. Les μ_α où $|\alpha| = 1$ n'interviennent que dans la première ligne et la première colonne de A, et ils n'apparaissent pas dans l'expression $\langle \mu, f \rangle$, ils ne jouent donc aucun rôle. Soit B la matrice obtenue en retirant sa première ligne et sa première colonne à A. On est ramené à maximiser $\sum_{i,\,j=1}^{n} w_{ij} \frac{1}{2}(B_{ij} - 1)$ sur les matrices symétriques positives au sens large B de taille n dont les coefficients diagonaux valent 1. C'est exactement équivalent à la relaxation de Goemans-Williamson.

Pour les problèmes d'optimisation sur le cube discret, il y a des procédures d'arrondi naturelles pour la relaxation Π^1 de Lasserre, mais elles ne semblent pas coïncider avec celle de Goemans-Williamson dans le cas particulier de MAX CUT.

Pour en savoir davantage sur les relaxations d'ordre supérieur de MAX CUT, voir [Lau].

8. CONCLUSION

Le succès de la méthode des relaxations semi-définies pour construire des algorithmes d'approximation est frappant (voir notamment le tableau dans [Kh3]). Il semble prometteur de progrès vers des applications pratiques (elles sont limitées actuellement par les implémentations de la programmation semi-définie).

Sur le plan théorique, comment se fait-il que des problèmes combinatoires (typiquement, maximisation sur le cube discret d'une fonction non linéaire et non convexe) puissent se ramener à des problèmes convexes ? Les hiérarchies constituent une première réponse. Il est important d'approfondir la compréhension de ces hiérachies : comment se fait-il que, pour MAX CUT par exemple, la première itération de la hiérachie de Lasserre donne déjà la borne d'approximabilité (conjecturée comme) optimale ? La réponse contribuerait à cerner les limites de la puissance du calcul.

En restant plus proche du courant principal des mathématiques, on peut plus modestement interpréter chaque relaxation semi-définie comme un petit modèle de calcul, à l'intérieur duquel le problème de difficulté d'approximation devient la détermination d'un saut d'intégralité. On a vu dans plusieurs exemples que les problèmes mathématiques qui surgissent alors sont riches et variés, ils font intervenir de la géométrie, de l'analyse, du calcul des probabilités. Ce genre de travaux a certainement une utilité du point de vue de la complexité. Les preuves des théorèmes 6.3 et 6.11 indiquent qu'une bonne compréhension d'un saut d'intégralité peut être la clé d'un résultat de difficulté d'approximation.

La conjecture des jeux uniques occupe une place singulière dans les travaux que nous avons présentés. La difficulté d'approximation sous UGC est étroitement reliée à la méthode de relaxation semi-définie (cf. Théorème 6.11). Est-ce une particularité d'UGC ? Peut-être non. Prouver la difficulté d'approximation sous UGC pourrait n'être qu'une étape vers la difficulté d'approximation sous $P \neq NP$ (cf. Théorème 4.4).

RÉFÉRENCES

[AN] N. ALON, A. NAOR – *Approximating the cut-norm via Grothendieck's inequality*, SIAM J. Comput. **35** (2006), 787–803.

[AKL] L. AMBROSIO, B. KLEINER, E. LE DONNE – *Rectifiability of sets of finite perimeter in Carnot groups : existence of a tangent hyperplane*, J. Geom. Anal. **19** (2009), 509–540.

[AMS] C. AMBÜHL, M. MASTROLILLI, O. SVENSSON – *Inapproximability results for sparsest cut, optimal linear arrangement, and precedence constrained scheduling*, 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 329–337 , IEEE Computer Soc., Los Alamitos, CA (2007).

[ABS] S. ARORA, B. BARAK, D. STEURER – *Subexponential algorithms for unique games and related problems*, 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS), 563–572, IEEE Computer Soc., Los Alamitos, CA (2010).

[AHK] S. ARORA, E. HAZAN, S. KALE – $O(\sqrt{\log n})$ *approximation to sparsest cut in* $\tilde{O}(n^2)$ *time*, SIAM J. Comput. **39** (2010), 1748–1771.

[ALN] S. ARORA, J. LEE, A. NAOR – *Euclidean distortion and the sparsest cut*, J. Amer. Math. Soc. **21** (2008), 1–21.

[ALMSS] S. ARORA, C. LUND, R. MOTWANI, M. SUDAN, M. SZEGEDI – *Proof verification and the hardness of approximation problems*, J. ACM **45** (1998), 501–555.

[AS] S. ARORA, S. SAFRA – *Probabilistic checking of proofs : a new characterization of NP*, J. ACM **45** (1998), 70–122.

[A] P. ASSOUAD – *Espaces métriques, plongements, facteurs*, Thèse de doctorat. Publications Mathématiques d'Orsay, No. 223-7769. U.E.R. Mathématiques, Université Paris XI, Orsay (1977).

[ANT] T. AUSTIN, A. NAOR, R. TESSERA – *Sharp quantitative nonembeddability of the Heisenberg group into superreflexive Banach spaces*, arXiv : 1007.4238

[BKS] I. BENJAMINI, G. KALAI, O. SCHRAMM – *Noise sensitivity of Boolean functions and applications to percolation*, Publ. Math. I.H.É.S. **90** (1999), 5–43.

[BOL] M. BEN OR, N. LINIAL – *Collective coin flipping, robust voting games and minima of Banzhaf values*, 26th Annual IEEE Symposium on Foundations of Computer Science (FOCS 1985), 408–416, IEEE Computer Soc., Los Alamitos, CA (1985).

[B] A. BONAMI – *Étude des coefficients de Fourier des fonctions de* $L^p(G)$, Ann. Inst. Fourier (Grenoble) **20** (1971), 335–402.

[Bor] C. BORELL – *Geometric bounds on the Ornstein-Uhlenbeck velocity process*, Z. Wahrsch. Verw. Gebiete **70** (1985), 1–13.

[Bou] J. BOURGAIN – *On Lipschitz embedding of finite metric spaces in Hilbert space*, Israel J. Math. **52** (1985), 46–52.

[BMMN] M. BRAVERMAN, K. MAKARYCHEV, Yu. MAKARYCHEV, A. NAOR – *The Grothendieck constant is strictly smaller than Krivine's bound*, 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2011), 408–416, IEEE Computer Soc., Los Alamitos, CA (2011).

[BDK] J. BRETAGNOLLE, D. DACUNHA-CASTELLE, J.-L. KRIVINE – *Lois stables et espaces* L^p, Ann. Inst. H. Poincaré Sect. B (N.S.) **2** (1965/1966), 231–259.

[CrMM] M. CHARIKAR, K. MAKARYCHEV, Yu. MAKARYCHEV – *On the advantage over random for maximum acyclic subgraph*, 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS) 625–633, IEEE Computer Soc., Los Alamitos, CA (2007).

[CKKRS] S. CHAWLA, R. KRAUTHGAMER, R. KUMAR, Yu. RABANI, D. SIVAKUMAR – *On the hardness of approximating multicut and sparsest-cut*, Comput. Complexity **15** (2006), 94–114.

[Ch] B. CHAZELLE – *The PCP theorem*, Sém. Bourbaki (2001/02), Exp. n° 895, Astérisque **290** (2003), 19–36.

[CK1] J. CHEEGER, B. KLEINER – *On the differentiability of Lipschitz maps from metric measure spaces to Banach spaces*, Inspired by S. S. Chern, 129–152, Nankai Tracts Math. **11**, World Sci. Publ., Hackensack, NJ (2006).

[CK2] J. CHEEGER, B. KLEINER – *Differentiating maps into L^1, and the geometry of BV functions*, Ann. of Math. **171** (2010), 1347–1385.

[CK3] J. CHEEGER, B. KLEINER – *Metric differentiation, monotonicity and maps to L^1*, Invent. Math. **182** (2010), 335–370.

[CKN] J. CHEEGER, B. KLEINER, A. NAOR – *A $(\log n)^{\Omega(1)}$ integrality gap for the sparsest cut SDP*, 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009), 555–564, IEEE Computer Soc., Los Alamitos, CA (2009).

[CcMM] M. CHLAMTAC, K. MAKARYCHEV, Yu. MAKARYCHEV – *How to play unique games using embeddings*, 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS) 687–696, IEEE Computer Soc., Los Alamitos, CA (2006).

[DL] M. DEZA, M. LAURENT – *Geometry of cuts and metrics*, Algorithms and Combinatorics **15**. Springer-Verlag, Berlin (1997).

[D] I. DINUR – *Probabilisitically Checkable Proofs*, Proceedings of the International Congress of Mathematicians, ICM, Hyderabad (2010).

[DH] I. DINUR, P. HARSHA – *Composition of low-error 2-query PCPs using decodable PCPs*, 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 472–481, IEEE Computer Soc., Los Alamitos, CA (2009).

[Eh] A. EHRHARD – *Symétrisation dans l'espace de Gauss*, Math. Scand. **53** (1983), 281–301.

[E] P. ENFLO – *On the nonexistence of uniform homeomorphisms between L_p-spaces*, Ark. Mat. **8** (1969) 103–105.

[FS] U. FEIGE, G. SCHECHTMAN – *On the optimality of the random hyperplane rounding technique for MAX CUT*, Probabilistic methods in combinatorial optimization. Rand. Struct. Algo. **20** (2002), 403–440.

[FSS] B. FRANCHI, R. SERAPIONI, F. SERRA CASSANO – *On the structure of finite perimeter sets in step 2 Carnot groups*, J. Geom. Anal. **13** (2003), 421–466.

[Go] M. GOEMANS – *Semidefinite programming in combinatorial optimization*, Lectures on mathematical programming (ismp97) (Lausanne, 1997). Math. Programming **79**, (1997), Ser. B, 143–161.

[GW] M. X. GOEMANS, D. P. WILLIAMSON – *Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming*, J. ACM **42** (1995), 1115–1145.

[G] A. GROTHENDIECK – *Résumé de la théorie métrique des produits tensoriels topologiques*, Bol. Soc. Mat. Sao Paulo **8** (1953) 1–79.

[GMR] V. GURUSWAMI, R. MANOKARAN, P. RAGHAVENDRA – *Beating the random ordering is hard : Inapproximability of maximum acyclic subgraph*, 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS) 573–582, IEEE Computer Society, Los Alamitos, CA (2008).

[GRSW] V. GURUSWAMI, P. RAGHAVENDRA, R. SAKET, Y. WU – *Bypassing UGC from some optimal geometric inapproximability results*, Electr. Colloq. Comput. Compl. (ECCC) **17 : 177** (2010).

[H1] J. HÅSTAD – *On approximating NP-hard optimization problems*, Proceedings of the International Congress of Mathematicians, Vol. III (Berlin, 1998). Doc. Math. 1998, Extra Vol. III, 441–450.

[H2] J. HÅSTAD – *Some optimal inapproximability results*, J. ACM **48** (2001), 798–859.

[K] S. KAKUTANI – *Mean ergodic theorem in abstract* (L)*-spaces*, Proc. Imp. Acad., Tokyo **15** (1939). 121–123.

[Kh1] S. KHOT – *On the power of unique 2-prover 1-round games*, 34th Symposium on Theory of Computing (STOC), ACM, New York (2002).

[Kh2] S. KHOT – *Inapproximability of NP-complete problems, discrete Fourier analysis, and geometry*, Proceedings of the International Congress of Mathematicians (Hyderabad, 2010).

[Kh3] S. KHOT – *On the Unique Games Conjecture*, Proc. Conf. Computat. Complexity (2011).

[KKMO] S. KHOT, G. KINDLER, E. MOSSEL, R. O'DONNELL – *Optimal inapproximability results for MAX-CUT and other 2-variable CSPs ?*, SIAM J. Comput. **37** (2007), 319–357.

[KN1] S. KHOT, A. NAOR – *Grothendieck-type inequalities in combinatorial optimisation*, `arXiv:1108.2464`.

[KS] S. KHOT, S. SAFRA – *A two prover one round game with strong soundness*, To appear in 52nd Annual IEEE Symposium on Foundations of Computer Science (2011).

[KV] S. KHOT, N. VISHNOI – *The Unique Games Conjecture, integrality gap for cut problems and the embeddability of negative type metrics into l_1*, 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005) 53–62. IEEE Computer Society, Los Alamitos, CA (2005).

[Ki] G. KINDLER – *Dictatorship testing and hardness of approximation*, Notes of lectures given at Institut Henri Poincaré, february 2011. Downloadable from the blog `http://metric2011.wordpress.com/`

[KNS] G. KINDLER, A. NAOR, G. SCHECHTMAN – *The UGC hardness threshold of the L_p Grothendieck problem*, Math. Oper. Res. **35** (2010), 267–283.

[Kr] J.-L. KRIVINE – *Constantes de Grothendieck et fonctions de type positif sur les sphères*, Adv. in Math. **31** (1979), 16–30.

[La] J.-B. LASSERRE – *Moments, positive polynomials and their applications*, Imperial College Press, London (2009).

[Lau] M. LAURENT – *Semidefinite relaxations for Max-Cut*, The Sharpest Cut, 257–290, MPS/SIAM Ser. Optim., SIAM, Philadelphia, PA, (2004).

[LN] J. LEE, A. NAOR – *L_p metrics on the Heisenberg group and the Goemans-Linial conjecture*, 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006) 99–108. IEEE Computer Society, Los Alamitos, CA (2006).

[L] N. LINIAL – *Finite metric-spaces – combinatorics, geometry and algorithms*, Proceedings of the International Congress of Mathematicians, Vol. III (Beijing, 2002), 573–586, Higher Ed. Press, Beijing (2002).

[LLR] N. LINIAL, E. LONDON, Yu. RABINOVICH – *The geometry of graphs and some of its algorithmic applications*, Combinatorica **15** (1995), 215–245.

[Lo] L. LOVASZ – *On the Shannon capacity of a graph*, IEEE Transactions on Information Theory **25** (1979), 1–7.

[LS] L. LOVASZ, A. SCHRIJVER – *Cones of matrices and set-functions and $0-1$ optimization*, SIAM J. on Optim. **1** (1991), 166–190.

[M] G. MARGULIS – *Probabilistic characteristics of graphs with large connectivity*, Problemy Peredachi Informatsii **10** (1974), 101–108.

[MR] D. MOSHKOVITZ, R. RAZ – *Sub-constant error probabilistically checkable proof of almost-linear size*, Comput. Complexity **19** (2010), 367–422.

[MOO] E. MOSSEL, R. O'DONNELL, K. OLESKIEWICZ – *Noise stability of functions with low influences : invariance and optimality*, Ann. of Math. **171** (2010), 295–341.

[NS] A. NAOR, G. SCHECHTMAN – *An approximation scheme for quadratic form maximization on convex bodies*, manuscrit (2009).

[Ne] A. NEMIROVSKII – *Advances in convex optimization : conic programming*, In International Congress of Mathematicians. Vol. I, pages 413–444. Eur. Math. Soc., Zürich (2007).

[NN] Yu. NESTEROV, A. NEMIROVSKII – *Interior-point polynomial algorithms in convex programming*, SIAM Studies in Applied Mathematics, **13**. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA (1994).

[N] A. NEWMAN – *Approximating the maximum acyclic subgraph*, M.S. Thesis, MIT, June 2000.

[Pa] P. PANSU – *Métriques de Carnot-Carathéodory et quasiisométries des espaces symétriques de rang un*, Ann. of Math. **129** (1989), 1–60.

[Pu] M. PUTINAR – *Positive polynomials on compact semi-algebraic sets*, Indiana Univ. Math. J. **42** (1993), 969–984 .

[Ra] P. RAGHAVENDRA – *Optimal algorithms and inapproximability results for every CSP ?*, 40th Symposium on Theory of Computing (STOC), 245–254, ACM, New York (2008).

[RS] P. RAGHAVENDRA, D. STEURER – *Graph Expansion and the Unique Games Conjecture*, 42th Symposium on Theory of Computing (STOC), 75–764, ACM, New York (2002).

[R1] R. RAZ – *A parallel repetition theorem*, SIAM J. Comput. **27** (1998), 763–803.

[R2] R. RAZ – *$P \neq NP$, Propositional proof complexity, and resolution lower bounds for the weak pigeonhole principle*, Proceedings of the International Congress of Mathematicians, ICM (2002), Vol III, pp. 685–693.

[Ro] V. ROTAR – *Limit theorems for polylinear forms*, J. Multivariate Anal. **9** (1979), 511–530.

[Ru] L. RUSSO – *An approximate zero-one law*, Z. Warsch. Verw. Gebiete **61** (1982), 129–139.

[S] S. SEMMES – *On the nonexistence of bi-Lipschitz parameterizations and geometric problems about A_∞-weights*, Rev. Mat. Iberoamericana **12** (1996), 337–410.

[SA] H.D. SHERALI, W.P. ADAMS – *A hierarchy of relaxations between the continuous and convex hull representations for zero-one programming problems*, SIAM J. on Discr. Math. **3** (1990), 411–430.

Pierre PANSU

CNRS et Université Paris-Sud
UMR CNRS 8628
Département de Mathématiques
Bâtiment 425
F–91405 ORSAY Cédex
E-mail : pierre.pansu@math.u-psud.fr