348

ASTÉRISQUE

2012

SÉMINAIRE BOURBAKI
VOLUME 2010/2011
EXPOSÉS 1027-1042

(1028) *Crible en expansion*

Emmanuel KOWALSKI

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Séminaire BOURBAKI Novembre 2010
63e année, 2010-2011, no 1028, p. 17 à 64

CRIBLE EN EXPANSION

par **Emmanuel KOWALSKI**

1. INTRODUCTION

L'objet de ce rapport est de présenter des travaux récents qui étendent les méthodes de crible depuis leur cadre classique, vers des situations nouvelles caractérisées par l'apparition d'ensembles discrets « à croissance exponentielle », provenant tout particulièrement de groupes discrets tels que $\mathrm{SL}_m(\mathbf{Z})$ ou ses sous-groupes suffisamment « grands », en un certain sens.

Un exposé récent de Sarnak [**55**] indique en partie les premières motivations de ces travaux (liées à l'équation de Markov et aux géodésiques de la surface modulaires). Les premiers résultats généraux concernant ces problèmes sont apparus vers 2005 sous forme de prépublications, et Bourgain, Gamburd et Sarnak ont publié un article présentant ses aspects particuliers [**5**]. D'autres applications, dont certaines ont une saveur géométrique très différente, sont aussi apparues indépendamment vers cette période, tout d'abord (un peu implicitement) dans certains travaux de Rivin [**52**].

L'aspect le plus crucial des applications des méthodes de crible dans ces nouvelles situations est qu'elles dépendent de propriétés d'expansion ou de « trou spectral », que ce soit d'un point de vue discret ou combinatoire (lié aux graphes expanseurs ou à la Propriété (τ) de Lubotzky [**40**]) ou d'un point de vue plus géométrique (généralisant par exemple l'inégalité de Selberg $\lambda_1 \geqslant 3/16$ pour la première valeur propre non-nulle de l'opérateur de Laplace sur les surfaces modulaires de congruence classiques).

Les développements existant (ou en cours de rédaction) se traduisent, en définitive, par l'existence aujourd'hui d'estimations de crible très générales qui font intervenir des objets discrets à croissance exponentielle. Ces inégalités ont un potentiel d'application considérable – y compris pour des questions qui sont, *a priori*, sans rapport avec la théorie analytique des nombres –, dû en grande partie aux nombreux cas nouveaux où la propriété de trou spectral désirée a été démontrée. Les théorèmes d'expansion

pour les groupes linéaires finis sont particulièrement impressionnants (à commencer par l'article **[26]** de Helfgott dans le cas de SL_2 qui a été le point de départ de ces progrès), ainsi que ceux concernant l'application de méthodes ergodiques aux réseaux dans des groupes semisimples ayant la Propriété (τ) (en particulier les travaux de Gorodnik et Nevo **[21]**).

Avant de se diriger vers le cœur de ce rapport, nous commençons par énoncer un résultat simple qui provient du crible en expansion. Rappelons pour cela tout d'abord que $\Omega(n)$ est la fonction arithmétique qui donne le nombre de facteurs premiers, comptés avec multiplicité, d'un entier $n \neq 0$, étendue à 0 en posant $\Omega(0) = +\infty$.

THÉORÈME 1.1. — *Soit $\Lambda \subset \mathrm{SL}_m(\mathbf{Z})$ un sous-groupe Zariski-dense, par exemple, le groupe L engendré par les éléments*

$$\begin{pmatrix} 1 & \pm 3 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ \pm 3 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}), \tag{1}$$

dans le cas $m = 2$

Soit f une fonction polynôme non-constante à coefficients entiers en m variables, par exemple $f = X_1 \cdots X_m$. Soit $x_0 \in \mathbf{Z}^m - \{0\}$ un vecteur fixé. Il existe un entier $r = r(f, x_0, \Lambda) \geqslant 1$ tel que l'ensemble

$$\mathcal{O}_f(x_0; r) = \{\gamma \in \Lambda \mid \Omega(f(\gamma \cdot x_0)) \leqslant r\}$$

est Zariski-dense *dans SL_m, et en particulier est infini. Plus précisément, il existe un tel r pour lequel $\mathcal{O}_f(x_0; r)$ est un ensemble* non mince, *au sens de* **[57]**, Def. 3.1.1].

Il est important de noter – comme cela sera rappelé plus bas – que Λ peut très bien avoir un indice infini dans $\mathrm{SL}_m(\mathbf{Z})$. C'est le cas, par exemple, du groupe L engendré par les matrices (1) (ce qu'on peut voir, par exemple, en déterminant un domaine fondamental pour l'action de L par homographies sur le demi-plan de Poincaré et en vérifiant que son aire hyperbolique est $+\infty$.)

Notations

Nous rappelons quelques notations essentielles.

– La lettre p désignera toujours un nombre premier ; on désigne en particulier par $\mathbf{F}_p$ le corps fini $\mathbf{Z}/p\mathbf{Z}$, et on écrit plus généralement $\mathbf{F}_q$ pour un corps fini à q éléments. Pour un ensemble X, $|X|$ désigne son cardinal, qui est un entier positif ou bien $+\infty$; pour un graphe Γ, $|\Gamma|$ est le nombre de sommets.

– Les notations de Landau et Vinogradov $f = O(g)$ et $f \ll g$ sont synonymes ; $f(x) = O(g(x))$ pour tout $x \in D$ signifie qu'il existe une constante « implicite » $C \geqslant 0$ (qui peut dépendre d'autres paramètres, qui seront indiqués explicitement) telle que $|f(x)| \leqslant Cg(x)$ pour tout $x \in D$. Cette définition *diffère* de celle de N.

Bourbaki [**1**, Chap. V], puisque cette dernière est de nature topologique. Par contre, les notations $f(x) \sim g(x)$ et $f = o(g)$ ont dans ce texte le sens asymptotique de loc. cit. On écrira $f \asymp g$ pour $f \ll g$ et $g \ll f$ simultanément.

Remerciements

Je remercie chaleureusement J. Bourgain, N. Dunfield, E. Fuchs, A. Gamburd, F. Jouve, A. Kontorovich, H. Oh, L. Pyber, P. Sarnak, D. Zywina pour leur aide, remarques et corrections concernant ce texte. En particulier, les discussions avec O. Marfaing durant la préparation de son rapport de Master sur ce sujet [**43**] ont été très utiles.

2. MOTIVATION

Les méthodes de crible concernent les propriétés multiplicatives des entiers, ou de sous-ensembles d'entiers. Il est donc naturel de chercher, pour étendre ces méthodes, à décrire des ensembles d'entiers inhabituels. Afin de présenter l'esprit du sujet, nous donnons dans cette section deux exemples de tels ensembles. L'un d'entre eux est un cas particulièrement plaisant du « crible en orbite » de Bourgain, Gamburd et Sarnak, considéré dans [**5**] : il s'agit de l'ensemble des courbures d'empilements de cercles apolloniens. Le second est peut-être encore plus surprenant : il concerne l'ordre du premier groupe d'homologie entière de certaines variétés de dimension 3 aléatoires. Nous le traiterons moins en détail dans la suite, mais il s'agit néanmoins d'un exemple révélateur de la diversité des applications possibles du crible.

2.1. Empilements de cercles apolloniens

Soient $(\bigcirc_1, \bigcirc_2, \bigcirc_3)$ trois cercles dans le plan, deux à deux tangents et bordant des disques intérieurs disjoints, de rayons respectifs (r_1, r_2, r_3) et courbures $(c_1, c_2, c_3) = (r_1^{-1}, r_2^{-1}, r_3^{-1})$. Une propriété géométrique très classique est l'existence de deux autres cercles exactement (disons $(\bigcirc_4, \bigcirc_4')$, de courbures (c_4, c_4')), tels que les quadruplets

$$(\bigcirc_1, \bigcirc_2, \bigcirc_3, \bigcirc_4) \text{ et } (\bigcirc_1, \bigcirc_2, \bigcirc_3, \bigcirc_4')$$

comportent quatre cercles tangents deux à deux bordant des disques disjoints, si l'on permet (ce qui est possible tant pour les cercles originaux que pour $\bigcirc_4$ et $\bigcirc_4'$) d'avoir des cercles de rayon *négatifs*, auquel cas le « disque » bordé par un cercle est, par convention, le complément dans le plan du disque borné auquel on pense naturellement (voir Figure 1). Un tel quadruplet est appelé une *configuration de Descartes*.

En effet, Descartes a démontré que, dans une telle configuration, les courbures des quadruplets vérifient les équations quadratiques

$$Q(c_1, c_2, c_3, c_4) = Q(c_1, c_2, c_3, c_4') = 0$$

où Q est la forme quadratique indéfinie donnée par

$$Q(x, y, z, t) = 2(x^2 + y^2 + z^2 + t^2) - (x + y + z + t)^2.$$

Ainsi, s'il se trouve que $(\bigcirc_1, \bigcirc_2, \bigcirc_3, \bigcirc_4)$ ont des courbures entières (positives ou négatives), on obtient une équation de degré 2 pour déterminer c_4', dans laquelle une solution (à savoir c_4) est supposée connue, et est entière : par conséquent, c_4' sera également un entier. Et si l'on veut continuer l'aventure, le même raisonnement indique que, partant des cercles $(\bigcirc_1, \bigcirc_2, \bigcirc_3, \bigcirc_4)$ à courbures entières, il existe d'autres cercles

$$\bigcirc_1', \bigcirc_2', \bigcirc_3',$$

tels que, par exemple, le quadruplet

$$(\bigcirc_1', \bigcirc_2, \bigcirc_3, \bigcirc_4)$$

soit une configuration de Descartes, avec courbure c_1' (et similairement c_2', c_3') entière. Plus précisément, en résolvant l'équation ci-dessus avec la racine connue, on trouve que

$$\begin{aligned}
(c_1', c_2, c_3, c_4) &= (c_1, c_2, c_3, c_4) \cdot {}^t s_1, \\
(c_1, c_2', c_3, c_4) &= (c_1, c_2, c_3, c_4) \cdot {}^t s_2, \\
(c_1, c_2, c_3', c_4) &= (c_1, c_2, c_3, c_4) \cdot {}^t s_3, \\
(c_1, c_2, c_3, c_4') &= (c_1, c_2, c_3, c_4) \cdot {}^t s_4,
\end{aligned}$$

où les matrices $s_1, \dots, s_4$ appartiennent au groupe orthogonal entier $O(Q, \mathbf{Z})$ de la forme quadratique ci-dessus, et sont données par

$$s_1 = \begin{pmatrix} -1 & 2 & 2 & 2 \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \qquad s_2 = \begin{pmatrix} 1 & & & \\ 2 & -1 & 2 & 2 \\ & & 1 & \\ & & & 1 \end{pmatrix},$$

(et s_3, s_4 obtenues *mutatis mutandis*). Notons que $s_i^2 = 1$ pour tout i, et que l'on peut même montrer que ce sont les seules relations satisfaites par ces matrices.

Chacun des quadruplets de courbures ainsi obtenus peut être utilisé pour itérer ce procédé. Autrement dit, si l'on note $\mathscr{A}$ le sous-groupe de $O(Q, \mathbf{Z})$ qui est engendré par les s_i, les entiers apparaissant comme coefficients dans un vecteur de l'orbite $\mathscr{A} \cdot \boldsymbol{c}$ d'un « quadruplet racine » $\boldsymbol{c} = (c_1, \dots, c_4)$, représentent toutes les courbures des cercles qui sont ainsi construits récursivement. On obtient en définitive un *empilement de*