Available online at www.sciencedirect.com
ScienceDirect
C. R. Acad. Sci. Paris, Ser. I 346 (2008) 619–623
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Group Theory

Random walks and expansion in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$

Jean Bourgain *, Alex Gamburd

School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA

Received and accepted 15 April 2008

Available online 20 May 2008

Presented by Jean Bourgain

Abstract

Let $S = \{g_1, \ldots, g_k\}$ be a set of elements of $\mathrm{SL}_d(\mathbb{Z})$ generating a Zariski dense subgroup of $\mathrm{SL}_d(\mathbb{R})$ and let p be a sufficiently large prime. Consider the family of Cayley graphs $\mathcal{G}(\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z}), \pi_{p^n}(S)) = \mathcal{G}_n$, where we vary n. Then $\{\mathcal{G}_n\}$ forms an expander family. ***To cite this article: J. Bourgain, A. Gamburd, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Résumé

Marches au hasard et l'expansion en $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. Soit $S = \{g_1, \ldots, g_k\}$ un sous-ensemble de $\mathrm{SL}_d(\mathbb{Z})$ engendrant un sous-groupe de $\mathrm{SL}_d(\mathbb{R})$ Zariski dense. On considère les graphes de Cayley $\mathcal{G}(\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z}), \pi_{p^n}(S)) = \mathcal{G}_n$, où l'on varie n. Alors $\{\mathcal{G}_n\}$ forment une famille d'expanseurs. ***Pour citer cet article : J. Bourgain, A. Gamburd, C. R. Acad. Sci. Paris, Ser. I 346 (2008).***

Version française abrégée

Dans cette Note, nous présentons une extension de résultats obtenus dans [3] et [6,7] sur les propriétés d'expansion de certains graphes de Cayley sur les groupes $\mathrm{SL}_d(q) = \mathrm{SL}_d(\mathbb{Z}/q\mathbb{Z})$. Nous fixons des elements $\{g_1, \ldots, g_k\} = S$ de $\mathrm{SL}_d(\mathbb{Z})$ et supposons que S engendre un sous-groupe Λ dont l'adhérence de Zariski $\bar{\Lambda}^z = \mathrm{SL}_d$. Fixons aussi un nombre premier p suffisamment grand et considérons les graphes de Cayley $\mathcal{G}_n = \mathcal{G}(\mathrm{SL}_d(p^n), \pi_{p^n}(S))$ sur $\mathrm{SL}_d(p^n)$, où π_q dénote la réduction mod q. Selon le théorème de Matthews–Vaserstein–Weisfeiler, ces graphes sont connexes. Nous démontions que $\{\mathcal{G}_n\}$ forment une famille d'expanseurs à coefficient d'expansion $c(\mathcal{G}_n)$ minoré par une constante $c(S, p) > 0$ (pour $d = 2$, la constante ne dépend que de S). Pour $d = 2$, le problème d'expansion des graphes $\mathcal{G}(\mathrm{SL}_2(q), \pi_q(S))$ a eté étudié dans [3] pour q un nombre premier et dans [6,7] pour q un produit simple de nombres premier ; on obtient une minoration du coefficient d'expansion par une constante $c(S)$ indépendante de q, á condition que $(q, q_0(S)) = 1$. Dans le cas $q = p^n$, p fixé et $n \to \infty$, considéré ici, l'approche fait intervenir, outre des méthodes de combinatoire arithmétique, aussi, certaines techniques probabilistes, en particulier la thèorie des produits aléatoires de matrices.

* Corresponding author.
E-mail addresses: bourgain@ias.edu (J. Bourgain), agamburd@ias.edu (A. Gamburd).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2008.04.006

1. Statement of the results and comments

The general setup considered in [6] and [7] and here is as follows.

Let $S = \{g_1, \dots, g_k\}$ be a subset of $\mathrm{SL}_d(\mathbb{Z})$ and $\Lambda = \langle S \rangle \subset \mathrm{SL}_d(\mathbb{Z})$ the subgroup generated by S. We assume Λ Zariski dense in SL_d. According to the theorem of Matthews–Vaserstein–Weisfeiler, there is some integer $q_0 = q_0(S)$ such that $\pi_q(\Lambda) = \mathrm{SL}_d(q)$, assuming $(q, q_0) = 1$. Here π_q denotes the reduction mod q. Partly motivated by questions of prime sieving, it was conjectured in [6,7] that the Cayley graphs $\mathcal{G}(\mathrm{SL}_d(q), \pi_q(S))$ form an expander family, with expansion coefficient minorated by a constant $c = c(S)$. For $d = 2$, we verified this conjecture in [3,6,7] provided q is assumed square free (in fact, for q prime, even stronger results are obtained in [3]). At the other end, there are moduli of the form $q = p^n$ where we fix p say and let $n \to \infty$. The combinatorics involved here turns out to be significantly different, starting from the sum–product theorem in the residue ring $\mathbb{Z}/p^n\mathbb{Z}$. We also rely on a 'multi-scale' approach, reminiscent of the Solovay–Kitaev algorithm in quantum computation. In fact our treatment for this type of moduli turns out to be rather robust, in the sense that we do not have to enter the finer aspects of the group structure (of course crucial use is made of the strong approximation property and also the irreducibility of certain representations). The method applies to the case $d > 2$ as well and provides the first results towards the above conjecture in this setting. Our main result is the following:

Theorem. *Let $S = \{g_1, \dots, g_k\}$ be a finite subset of $\mathrm{SL}_d(\mathbb{Z})$ generating a subgroup Λ which is Zariski dense in SL_d. Let p be a sufficiently large prime.*

Then the Cayley graphs $\mathcal{G}(\mathrm{SL}_d(p^n), \pi_{p^n}(S))$ form an expander family as $n \to \infty$. The expansion coefficients are minorated by a positive number $c(S, p) > 0$; if $d = 2$, we may further drop the dependence on p, i.e. $c(S, p) = c(S)$.

Let us take the set S symmetric, i.e. $S = \{g_1, \dots, g_k, g_1^{-1}, \dots, g_k^{-1}\}$ to which we associate the probability measure

$$\nu = \frac{1}{|S|} \sum_{g \in S} \delta_g$$

on SL_d (δ_x denotes the Dirac measure at x). The theorem stated above has the following implication for which we do not know a more direct proof:

Corollary 1. *Let S and ν be as above. Let $\mathfrak{S}$ be a nontrivial algebraic subvariety of $\mathrm{SL}_d(\mathbb{C})$. Then the convolution powers $\nu^{(\ell)}$ of ν satisfy*

$$\nu^{(\ell)}(\mathfrak{S}) < \mathrm{e}^{-c\ell} \quad \text{for } \ell \to \infty \tag{1}$$

for some $c > 0$ (win fact c depends only on ν and the degree of $\mathfrak{S}$).

Assume now q a sufficiently large prime and G a proper subgroup of $\mathrm{SL}_d(q)$. From the work of Nori on the strong approximation property, it follows that G satisfies a nontrivial algebraic equation (mod q). We may then invoke Corollary 1 to obtain

Corollary 2. *Let again S and ν be as above and let q be a sufficiently large prime. Let G be a proper subgroup of $\mathrm{SL}_d(q)$. We denote $\pi_q[\nu]$ also by ν. There is an estimate*

$$\nu^{(\ell)}(G) < Cc^{-c\ell} \quad \text{for } \ell < \log q \tag{2}$$

where the constants c, C only depend on S.

Corollary 2 is of significance to establish the Conjecture mentioned in the beginning for other moduli q (besides q of the form $q = p^n$ with fixed p). Recalling the approach in [3] (see also next section), the conjecture for $\mathrm{SL}_d(q)$ (q prime say) will result by combining Lemma 2, Corollary 2 with a 'product theorem' in $\mathrm{SL}_d(q)$, of the form

$$|A.A.A| > |A|^{1+\varepsilon} \tag{3}$$

whenever $A \subset \mathrm{SL}_d(q)$ generates the full group and $|A| < |\mathrm{SL}_d(q)|^{1-\delta}$, with $\varepsilon = \varepsilon(\delta) > 0$ ((3) was proven by H. Helfgott [9] if $d = 2$ and he also announced the result for $d = 3$).