ELSEVIER

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 $S = \{g_1, \dots, g_k\}$ 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 $\mathbf{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. Soit $S = \{g_1, \dots, g_k\}$ 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 $\mathcal{G}(\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z}), \pi_{p^n}(S)) = \mathcal{G}_n$, òu 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 $\{g_1, \dots, g_k\} = S$ 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 © 2008 Académie des sciences. Published by Elsevier Masson SAS. All rights reserved.
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*

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

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*

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

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 $d = 3$).

The special moduli $q = p^n$ with fixed p turn out to be also of interest in relation to the work of D. Long, A. Lubotzky and A. Reid [10] on Heegaard genus and property τ for hyperbolic 3-manifolds. More precisely, let M be a finite volume hyperbolic 3-manifold. From the result for the $\mathrm{SL}_2(p^n)$ towers, one may then produce a nested co-final family of finite sheeted covers with positive infimal Heegaard gradient. Long et al. [10] also put forward the conjecture that any finitely generated subgroup Γ of $\mathrm{GL}(n, \mathbb{C})$ with semi-simple Zariski closure has a co-final (nested) $\mathcal{L} = \{N_i\}$ of finite index normal subgroups for which Γ has property τ with respect to $\mathcal{L}$. It seems reasonable to believe that moduli $q = p^n$ and the proof of our theorem may provide an approach.

2. Ingredients of the proof

The elements of the argument are the following:

(i) A reduction to non-existence of certain 'approximative subgroups' of $\mathrm{SL}_d(\mathbb{Z}/q\mathbb{Z})$;
(ii) The theory of random matrix products;
(iii) Construction of large sets of commuting elements;
(iv) Sum–product theorem in $\mathbb{Z}/p^n\mathbb{Z}$ and certain extension fields;
(v) Solovay–Kitaev type multi-scale construction.

The basic approach is completely similar to [3]. Following the Sarnak–Xue trace argument [11] based on high multiplicity of nontrivial eigenvalues, the expansion property is deduced from

Proposition 1. *For any $\gamma > 0$, there is $\ell \sim \log q$ such that*

$$\left\|\pi_q[\nu^{(\ell)}]\right\|_\infty < q^\gamma \left|\mathrm{SL}_d(q)\right|^{-1}. \tag{4}$$

Proposition 1 will be applied for a specific, sufficiently small $\gamma > 0$.

Note that in the present setting with $q = p^n$, we require $\ell > C \log q$, with $c = c(\nu, \gamma)$ also depending on p if $d > 2$.

The noncommutative Balog–Szemeredi–Gowers theorem (see [12]) allows then a further reduction to a set-theoretical statement. Denote $N = |\mathrm{SL}_d(q)| = |G|$.

Lemma 2. *Given $\gamma > 0$ and letting $\varepsilon > 0$ be small enough, there is no subset H of G with the following properties*:

$$|H| < N^{1-\gamma}, \tag{5}$$

$$\nu^{(\ell)}(x_0 H) > N^{-\varepsilon} \quad \textit{for some } x_0 \in G \textit{ and } \ell \sim \log q, \tag{6}$$

$$H = H^{-1}. \tag{7}$$

$$\textit{There is } X \subset G,\ |X| < N^\varepsilon \textit{ with } H.H \subset X.H \cap H.X. \tag{8}$$

Recall that H satisfying (7), (8) is referred to as an 'N^ε-approximative group'.

The following two statements are deduced from classical random matrix product theory (cf. [1,8]), based on our assumption that $\langle \operatorname{supp} \nu \rangle$ is Zariski-dense in SL_d, and a transference to the modular setting (using a quantitative Bezout theorem):

Lemma 3. *Let $Q \in \mathbb{Z}_+$ (large) and $\ell > \log Q$. Then*

$$\nu^{(\ell)}\left\{g \in \mathrm{SL}_d(\mathbb{Z}) \mid \operatorname{Res}(P_g, P_g') \equiv 0 (\operatorname{mod} Q)\right\} < Q^{-c} \tag{9}$$

with $c = c(\nu)$ and P_g is the characteristic polynomial of g.

Lemma 4. *Let $Q \subset \mathbb{Z}_+$ (large) and $\ell > \log Q$. Then, for some $Q_1 = Q^C$*

$$\nu^{(\ell)}\left\{y \in \mathrm{SL}_d(\mathbb{Z}) \mid \operatorname{Tr} g\xi g^{-1}\eta \equiv 0 (\operatorname{mod} Q_1)\right\} < Q^{-c} \tag{10}$$

whenever $\xi, \eta \in \mathrm{Mat}_d(\mathbb{Z})$ satisfy $\pi_Q(\xi) \neq 0$, $\pi_Q(\eta) \neq 0$ and $\operatorname{Tr} \xi = 0 = \operatorname{Tr} \eta$.

Thus Lemma 3 expresses eigenvalue simplicity (mod Q) for a generic element in the ν-random walk and Lemma 4 is a (mod Q) hyperplane escaping property for the action by conjugation on the traceless matrices.

As in [9] and [7], the first step in the amplification of H is the construction of a large set of commuting matrices. Denote for given $s \in \mathbb{Z}_+$, by $H^{(s)}$ the s-fold product of H.

Lemma 5. *There is $h \in H^{(8)}$ and $S \subset H.H$ such that*

$$\operatorname{Res}(P_h, P_h') \neq 0 \ (\mathrm{mod}\ p^{m_0}) \quad \big(\textit{where } m_0 = \mathrm{o}(n)\big), \tag{11}$$

$$|S| > q^c, \tag{12}$$

$$gh = hg (\mathrm{mod}\ p) \quad \textit{for } g \in S. \tag{13}$$

Note that, contrary to [9,7], the exact size of S in (12) is not important.

Diagonalize $h \in \mathrm{SL}_d(\mathbb{Z})$ considering an extension field K of $\mathbb{Q}$. Let $\mathcal{P}$ denote a prime divisor of (p) in the integers O of K. If e is the ramification index of $\mathcal{P}$, it follows from (11), (13) that in the new basis

$$h = \sum_{i=1}^{d} \mu_i (e_i \otimes e_i) \quad \text{with} \prod_{i \neq j} (\mu_i - \mu_j) \notin \mathcal{P}^{em_0} \tag{14}$$

and

$$g = \sum \lambda_i (e_i \otimes e_i) (\mathrm{mod}\ \mathcal{P}^{e(n-m_0)}) \quad \text{for } g \in S. \tag{15}$$

Once a set of diagonal matrices is obtained, we may start to bring scalar sum–product theorems into play. We use the sum–product theorem in $\mathbb{Z}/p^n\mathbb{Z}$ (cf. [2]) and its generalization to algebraic extensions of $\mathbb{Q}$.

Proposition 6. *Let K be an extension of $\mathbb{Q}$ and $\mathcal{P}$ a prime ideal dividing the rational prime p. Let $n \in \mathbb{Z}_+$ and $A \subset O/\mathcal{P}^n$ such that*

$$\pi_{\mathcal{P}^e}(A) \textit{ generates } O/\mathcal{P}^e \ (\textit{where } e \textit{ is the ramification of } \mathcal{P}), \tag{16}$$

$$\big|\pi_{\mathcal{P}^j}(A)\big| > p^{j\delta} \quad \textit{for all } 1 \leqslant j \leqslant n, \tag{17}$$

$$|A| < |O/\mathcal{P}^n|^{1-\delta_1} \tag{18}$$

for some $\delta, \delta_1 > 0$. Then

$$|A.A + A.A| > |A|^{1+\delta'} \tag{19}$$

where $\delta' = \delta'(\delta, \delta_1, [K : \mathbb{Q}]) > 0$.

Of course, if $O = \mathbb{Z}$, assumption (16) may be dropped. For our purpose, we rely on the following statement that only requires an assumption on $|\pi_{\mathcal{P}^n}(A)|$. In fact, it is needed more generally for subsets of a Cartesian product O^w (with w some given power).

Lemma 7. *Let $A \subset O^w$ satisfy*

$$\big|\pi_{\mathcal{P}^n}(A)\big| > p^{n\delta}. \tag{20}$$

Then there are $n_1 < n_2 < Cn$ and $\xi \in O^w$ satisfying

$$n_2 - n_1 > cn, \tag{21}$$

$$\pi_{\mathcal{P}}(\xi) \neq 0, \tag{22}$$

$$\xi\mathbb{Z} \cap \mathcal{P}^{n_1} \subset A' + \mathcal{P}^{n_2}, \quad \textit{for some sum–product set } A' \textit{ of } A. \tag{23}$$

By 'sum–product set', we mean a set of the form $rA^{(s)} - rA^{(s)}$, where rB stands for the r-fold sumset of B, $A^{(s)}$ the s-fold product set of A and r, s bounded. In Lemma 7, we allow the constants also to depend on p, which is given and assumed sufficiently large.

In our application, O^w will be the space of trace-less matrices in $\mathrm{Mat}_d(O)$ and Lemma 7 will be applied with $n = n_0 \sim \kappa n$ (where $q = p^n$ and κ a sufficiently small constant). Returning to the approximative group H, this allows us to deduce:

Lemma 8. *There are positive integers $n_1 < n_2 < n$ and $\xi \in \mathrm{Mat}_d(\mathbb{Z})$ such that*

$$n_1 \sim n_2 \sim n_2 - n_1 \sim \varepsilon_0 n, \tag{24}$$

$$\mathrm{Tr}\,\xi = 0 \quad \textit{and} \quad \pi_p(\xi) \neq 0. \tag{25}$$

There is a suitable product set H' of H with

$$\pi_{p^{n_2}}\big(\{1 + p^{n_1} t\xi \mid t \in \mathbb{Z}\}\big) \subset \pi_{p^{n_2}}(H'). \tag{26}$$

In (24), ε_0 is again an appropriately chosen small constant (in particular, depending on γ in (5)). Replacing ξ by conjugates $g\xi g^{-1}$ with $g \in H$ and invoking Lemma 4, the conclusion of Lemma 8 is further upgraded to:

Lemma 9. *There are positive integers $n_1 < n_2 < n$ satisfying* (24) *and a product set H' of H such that*

$$\pi_{p^{n_2}}\big(\{1 + p^{n_1} x \mid x \in \mathrm{Mat}_d(\mathbb{Z}), \mathrm{Tr}\,x = 0\}\big) \subset \pi_{p^{n_2}}(H'). \tag{27}$$

We are now precisely in a situation to carry out the p-adic variant of the Solovay–Kitaev algorithm to conclude that some further product set H' of H contains $\{g \in \mathrm{SL}_d(p^n) \mid g \equiv 1 (\mathrm{mod}\ p^{n_1})\}$. By (24), this will contradict (5) and the approximative group property (8), implying that $|H'| < p^{\varepsilon'}|H|$.

Recall that the Solovay–Kitaev construction uses Lie-algebra point of view and relies on the following simple fact

Lemma 10. *Let $g, h \in \mathrm{Mat}_d(\mathbb{Z})$ satisfy*

$$g \equiv 1 (\mathrm{mod}\ p^m) \quad \textit{and} \quad h \equiv 1 (\mathrm{mod}\ p^{m'}) \tag{28}$$

with $m \leqslant m'$. Then

$$ghg^{-1}h^{-1} \equiv 1 + [g, h]\ (\mathrm{mod}\ p^{2m+m'}) \tag{29}$$

with $[g, h] = gh - hg$.

Complete proofs will appear in [4,5].

Acknowledgements

The first author was supported in part by the NSF. The second author was supported in part by DARPA, NSF and Sloan Foundation.

References

[1] P. Bougerol, J. Lacroix, Products of Random Matrices with Applications to Schrödinger Operators, Progress in Probability and Statistics, vol. 8, Birkhäuser, 1985.

[2] J. Bourgain, The sum–product theorem $\mathbb{Z}_q$ with q arbitrary, preprint.

[3] J. Bourgain, A. Gamburd, Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. of Math. 167 (2008) 625–642.

[4] J. Bourgain, A. Gamburd, Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$: I, preprint.

[5] J. Bourgain, A. Gamburd, Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$: II, preprint.

[6] J. Bourgain, A. Gamburd, P. Sarnak, Sieving and expanders, C. R. Math. Acad. Sci. Paris, Ser. I 343 (2005) 155–159.

[7] J. Bourgain, A. Gamburd, P. Sarnak, Affine linear sieve, expanders, and sum–product, preprint.

[8] Y. Guivarc'h, Produits de matrices aléatoires et applications aux propriétés géométriques des sous-groupes du groupe linéaire, Ergodic Theory Dynam. Systems 10 (1990) 483–512.

[9] H. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. 167 (2008) 601–623.

[10] D.D. Long, A. Lubotzky, A.W. Reid, Heegaard genus and property 'tau' for hyperbolic 3-manifolds, J. Topol. 1 (1) (2008) 152–158.

[11] P. Sarnak, X. Xue, Bounds for multiplicities of automorphic representations, Duke Math. J. 64 (1991) 207–227.

[12] T. Tao, Product sets estimates for non-commutative groups, Combinatorica, in press.