Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 342 (2006) 717–721
COMPTES RENDUS
MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Number Theory/Mathematical Analysis

New results on expanders

Jean Bourgain [a,1], Alex Gamburd [a,b]

[a] *Institute for Advanced Study, Einstein Drive, Princeton, NJ 08540, USA*
[b] *Department of Mathematics, University of California, Santa Cruz, CA 95064, USA*

Received 10 February 2006; accepted 21 February 2006

Available online 11 April 2006

Presented by Jean Bourgain

Abstract

Based on purely analytical methods, we exhibit new families of expanders in $\mathrm{SL}_2(p)$ (p prime) and SU(2), contributing to conjectures of A. Lubotzky and P. Sarnak. ***To cite this article: J. Bourgain, A. Gamburd, C. R. Acad. Sci. Paris, Ser. I 342 (2006).***

Résumé

Nouveaux résultats sur les expanseurs. En utilisant d'une approche purement analytique, nous obtenons de nouvelle familles d'expanseurs dans des groupes $\mathrm{SL}_2(p)$ (p primier) et SU(2). Nos résultats contribuent à des conjectures de A. Lubotzky et P. Sarnak. ***Pour citer cet article : J. Bourgain, A. Gamburd, C. R. Acad. Sci. Paris, Ser. I 342 (2006).***

Version française abrégée

Nous présentons une novelle méthode, basée sur des techniques de combinatoire arithmétique pour produire des systèmes d'expanseurs dans les groupes $\mathrm{SL}_2(p)$ et SU(2). Voici quelques exemples de résultats obtenus. Soient $g_1, g_2 \in \mathrm{SL}_2(\mathbb{Z})$ des éléments engendrant un groupe libre. Alors $\{g_1, g_2\}$ forment un expanseur dans $G = \mathrm{SL}_2(p)$ pour tout p premier ou suffisamment grand. Plus précisément, il existe $\delta = \delta(g_1, g_2) > 0$ tel que si $f \in L^2(G)$ est de moyenne nulle, on ait

$$\|f - f_{g_1}\|_2 + \|f - f_{g_2}\|_2 \geqslant \delta \|f\|_2$$

où $f_g(x) = f(gx)$.

Auparavant, seulement des cas particuliers de ce phénomène étaient connus : pour des systèmes $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ engendrant un groupe d'indice fini (voir Selberg [17]) et Γ engendrant un groupe dont l'ensemble limite est de dimension suffisamment grande (voir Gamburd [9]).

E-mail addresses: bourgain@math.ias.edu (J. Bourgain), gamburd@math.ias.edu (A. Gamburd).

[1] Supported by NSF grant DMS 0322370.

1631-073X/$ – see front matter
doi:10.1016/j.crma.2006.02.032

On obtient un résultat semblable dans SU(2). Si $g_1, g_2 \in \mathrm{SU}(2)$ engendrent un groupe libre et satisfont une « condition diophantienne non-commutative » (ce qui est le cas en particulier pour des éléments algébriques) alors $\{g_1, g_2\}$ est un expanseur dans SU(2).

Notre approche combine des résultats classiques en théorie des représentations et des techniques combinatoires. Les phénomènes « somme-produit » dans les corps finis $\mathbb{F}_p$ et $\mathbb{F}_{p^2}$ (voir [4]) et $\mathbb{R}$ (voir [1]) y jouent un rôle essentiel.

1. Introduction

Given an undirected d-regular graph $\mathcal{G}$ and a subset X of V, the *expansion of* $X, c(X)$, is defined to be ratio $|\partial(X)|\backslash|X|$, where $\partial(X) = \{y \in \mathcal{G}\colon \text{distance } (y, X) = 1\}$. The *expansion coefficient* of a graph $\mathcal{G}$ is defined as follows:

$$c(\mathcal{G}) = \inf\left\{c(X) \mid |X| < \frac{1}{2}|\mathcal{G}|\right\}.$$

A family of d-regular graphs $\mathcal{G}_{n,d}$ forms a family of C-expanders if there is a fixed positive constant C, such that

$$\liminf_{n\to\infty} c(\mathcal{G}_{n,d}) \geqslant C. \tag{1}$$

The *adjacency matrix* of $\mathcal{G}$, $A(\mathcal{G})$ is the $|\mathcal{G}|$ by $|\mathcal{G}|$ matrix, with rows and columns indexed by vertices of $\mathcal{G}$, such that the x, y entry is 1 if and only if x and y are adjacent and 0 otherwise. Using the discrete Cheeger–Buser inequality, the condition (1) can be rewritten in terms of the second largest eigenvalue of the adjacency matrix $A(\mathcal{G})$ as follows:

$$\limsup_{n\to\infty} \lambda_1(A_{n,d}) < d. \tag{2}$$

Given a finite group G with a symmetric set of generators S, the Cayley graph $\mathcal{G}(G, S)$ is a graph which has elements of G as vertices and which has an edge from x to y if and only if $x = \sigma y$ for some $\sigma \in S$. Let S be a set of elements in $\mathrm{SL}(2, \mathbb{Z})$. If $\langle S\rangle$, the group generated by S, is a finite index subgroup of $\mathrm{SL}(2, \mathbb{Z})$, Selberg's theorem [17] implies that $\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ (where S_p is a natural projection of S modulo p) from a family of expanders as $p \to \infty$. A basic problem, posed by Lubotzky [13,14] and Lubotzky and Weiss [15], is whether Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$ are expanders with respect to other generating sets.

In [9] it is proved that if S is a set of elements in $\mathrm{SL}(2, \mathbb{Z})$ such that $\langle S\rangle$ is a subgroup of $\mathrm{SL}(2, \mathbb{Z})$, whose Hausdorff dimension of the limit set is greater than $5/6$, then $\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ form a family of expanders.

In [2] we prove that Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$ form expanders with respect to projection of fixed elements in $\mathrm{SL}_2(\mathbb{Z})$ generating a non-elementary subgroup and with respect to elements choosen at random in $\mathrm{SL}_2(\mathbb{F}_p)$.

The question of the spectral gap for finitely generated subgroups of SU(2) is motivated in part by the problem, posed by Ruziewicz in 1921, of whether Lebesgue measure on the n-sphere is unique *finitely* additive rotation-invariant measure defined on the Lebesgue subsets; it is also of interest in connection with problems in quantum computation [7]. As is well known, the existence of a finitely generated subgroup with a spectral gap implies the affirmative answer. For $n = 1$ the answer is negative, using essentially the amenability of SO(2). For $n > 3$ the affirmative answer was obtained in 1980/1 by Margulis and Sullivan, who used Kazhdan's property (T). In 1984 Drinfeld established the affirmative answer in the most difficult case of $n = 2$ by providing the *existence* of an element in the group ring of SU(2) which has a spectral gap.

Drinfeld's method used some sophisticated machinery from the theory of automorphic representations (in particular, Deligne's solution of the Ramanujan conjectures). In [10], a new robust method establishing that certain elements z in the group ring of SU(2) have a spectral gap was presented and consequently the spectral gap property was proven to hold for many subgroups defined via integral Hamilton quaternions.

We prove the spectral gap property for free subgroups of SU(2) generated by elements satisfying a noncommutative Diophantine property, in particular for free subgroups generated by elements with algebraic entries. Our method, following the approach in [10] first exploits the trace formula to reduce the question of the spectral gap to estimating from above the number of returns to a small neighborhood of identity. In [10] the required upper bound was obtained by reduction to an appropriate arithmetic problem. The novelty of our approach is to derive the required upper bound by utilizing the tools of additive combinatorics.

2. Results

First consider the expander problem in $\mathrm{SL}_2(p)$.

Our first result resolves the question completely for projections of fixed elements in $\mathrm{SL}(2,\mathbb{Z})$.

Theorem 1. *Let S be a set of elements in $\mathrm{SL}(2,\mathbb{Z})$. Then $\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S_p)$ form a family of expanders if and only if $\langle S\rangle$ is non-elementary, i.e. the limit set of $\langle S\rangle$ consists of more than two points (equivalently, $\langle S\rangle$ does not contain a solvable subgroup of finite index).*

Our second result resolves the question for random Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. (Given a group G, a random $2k$-regular Cayley graph of G is the Cayley graph $\mathcal{G}(G, \sigma \cup \sigma^{-1})$ where σ is a set of k elements from G, selected independently and uniformly at random.)

Theorem 2. *For any $k \geqslant 2$ random Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$ on k generators are expanders.*

Theorem 1 and Theorem 2 are consequences of the following quantitative result (recall that the girth of a graph is the length of a shortest cycle).

Theorem 3. *Let S be a symmetric set in $\mathrm{SL}_2(\mathbb{F}_p)$ and assume girth $(\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S)) > c\log p$, $c > 0$ an arbitrary given constant. Then the expansion coefficient $c(\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S)) > c_1(c) > 0$ (for p sufficiently large).*

Next, we discuss our results for $\mathrm{SU}(2)$.

Let us first recall the notion of 'Diophantine elements' introduced in [10].

Definition. For $k \geqslant 2$, we say that $g_1, g_2, \dots, g_k \in G$ are Diophantine (or satisfy a noncommutative Diophantine condition) if there is $D = D(g_1, \dots, g_k) > 0$ such that for any $m \geqslant 1$ and a word R_m in $g_1, g_2, \dots, g_k$ of length m with $R_m \neq \pm e$ we have

$$\|R_m \pm e\| \geqslant D^{-m}. \tag{3}$$

Here

$$\left\|\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right\| = |a|^2 + |b|^2 + |c|^2 + |d|^2.$$

Note that for $g \in G$ we have

$$\|g \pm e\|^2 = 2\bigl|\mathrm{trace}(g) \mp 2\bigr|. \tag{4}$$

Theorem 4. *Let $\{g_1, \dots, g_k\}$ be a set of elements in $\mathrm{SU}(2)$ generating a free group and satisfying a noncommutative Diophantine property. Then*

$$z_{g_1,\dots,g_k} = g_1 + g_1^{-1} + \dots + g_k + g_k^{-1} \tag{5}$$

has a spectral gap.

The following corollary is an immediate consequence of Theorem 4 and Proposition 4.3 in [10] establishing that elements with algebraic entries are Diophantine.

Corollary 5. *If $\{g_1, \dots, g_k\}$ are elements with algebraic entries (that is $g_1, \dots, g_k \in G \cap M_2(\overline{\mathbb{Q}})$) generating a free group, then $z_{g_1,\dots,g_k}$ has a spectral gap.*

3. Methods

The proof of Theorem 3 consists of two crucial ingredients. The first one is the fact that nontrivial eigenvalues of $\mathcal{G}(\mathrm{SL}_2(\mathbb{F}_p), S)$ must appear with high multiplicity. This follows from a result going back to Frobenius, asserting that the smallest dimension of a nontrivial irreducible representation of $\mathrm{SL}_2(\mathbb{F}_p)$ is $\frac{p-1}{2}$, which is large compared to the size of the group (which is of order p^3). The second crucial ingredient is an upper bound on the number of short closed geodesics, or, equivalently, the number of returns to identity for random walks of length of order $\log|G|$.

The idea of obtaining spectral gap results by exploiting high multiplicity together with the upper bound on the number of short closed geodesics is due to Sarnak and Xue [16]. The novelty of our approach is to derive the upper bound by utilizing the tools of additive combinatorics. In particular, we make crucial use of the noncommutative version of Balog–Szemeredi–Gowers Lemma, obtained by Tao [18,19] and of the result of Helfgott [11], asserting that subsets of $\mathrm{SL}_2(\mathbb{F}_p)$ grow rapidly under multiplication. Helfgott's paper [11], which served as a starting point and an inspiration for our work, builds crucially on sum-product estimates in finite fields due to Bourgain, Glibichuk and Konyagin [5] and Bourgain, Katz and Tao [4].

The structure of the proof of Theorem 4 is very similar to Theorem 3. As mentioned, the trace formula is used the same way as in [10] to reduce the gap problem to estimating the number of returns to a δ-neighborhood of the identity. A bound on these returns follows from an estimate on the convolution powers $\|\nu^{(\ell)} * P_\delta\|_2$ where $\nu = \frac{1}{2k}\sum_{s=1}^{k}(\delta_{g_s} + \delta_{g_s^{-1}})$ and $P_\delta = \frac{\chi_{B(1,\delta)}}{|B(1,\delta)|}$ with $B(1,\delta) = \{x \in \mathrm{SU}(2) \mid \|x-1\| < \delta\}$. That estimate itself results from a 'product theorem' for subsets of SU(2) in a similar vein as Helfgott's [11] (both the statement and the argument). But in the present case, the formulations for a compact group require 'measure' and 'metrical entropy' rather than 'cardinality' in the finite case. The most significant ingredient at this stage of the proof is the metrical counterpart of the finite fields sum–product theorem from [4]. The relevant property is a slight variant of the 'discretized ring conjecture' from [12], proven in [1]. The statement is as follows:

Proposition 6. *For all $0 < \sigma < 1$ and $\kappa > 0$, there is $\varepsilon > 0$ such that the following holds. Let $\delta > 0$ be a small number and $A \subset [-1, 1]$ a union of size-δ intervals satisfying $|A| = \delta^{1-\sigma}$ and $\max_a |A \cap B(a,\rho)| < \rho^\kappa |A|$ for all $\delta < \rho < \delta^\varepsilon$. Then*

$$|A + A| + |A.A| > \delta^{1-\sigma-\varepsilon}. \tag{6}$$

4. Further remarks

1. Proofs of above mentioned results appear in [2,3].

2. If we fix $S \subset \mathrm{SL}_2(\mathbb{Z})$ generating a free group, it is reasonable to expect that $c(\mathcal{G}(\mathrm{SL}_2(\mathbb{Z}_q), S)) > \delta(S) > 0$, $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, for all positive integers q, coprime to some finite set (depending on S) of integers. This follows from Theorem 3 if q is prime. Without entering in details the same basic scheme may be applied in general. The sum-product theorem in $\mathbb{F}_p$ needs here to be substituted by the corresponding result in $\mathbb{Z}_q$ (which is necessarily more restrictive for composite q). These results are presently available (and were developed for slightly different purposes). Precise statements and details will appear shortly.

3. Apart from the Ruziewicz problem and the Solovay–Kitaev algorithm, Theorem 4 and Corollary 5 are also relevant to a number of other problems. For instance an affirmative solution is obtained to the question considered in [8] on the uniform distribution of the orientations in the quaquaversal tilings of $\mathbb{R}^3$, introduced in [6].

References

[1] J. Bourgain, On the Erdös–Volkmann and Katz–Tao ring conjectures GAFA, 13 (2003) 334–365.
[2] J. Bourgain, A. Gamburd, Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$, preprint.
[3] J. Bourgain, A. Gamburd, On the spectral gap for finitely-generated subgroups of SU(2), preprint.
[4] J. Bourgain, N. Katz, T. Tao, A sum–product estimate in finite fields and applications, GAFA 14 (2004) 27–57.
[5] J. Bourgain, A. Glibichuk, S. Konyagin, Estimate for the number of sums and product and for exponential sums in fields of prime order, Proc. LMS, in press.
[6] J. Conway, C. Radin, Quaquaversal tilings and rotations, Invent. Math. 132 (1998) 179–188.
[7] C.M. Dawson, M.A. Nielsen, The Solovay–Kitaev algorithm, Quantum Inf. Comput. 6 (2006) 81–95.

[8] B. Draco, L. Sadun, D. Van Wieren, Growth rates in the quaquaversal tiling, Comput. Geom. 23 (3) (2000) 419–435.
[9] A. Gamburd, Spectral gap for infinite index “congruence” subgroups of $SL_2(\mathbb{Z})$, Israel J. Math. 127 (2002) 157–200.
[10] A. Gamburd, D. Jakobson, P. Sarnak, Spectra of elements in the group ring of $SU(2)$, J. Eur. Math. Soc. 1 (1999) 51–85.
[11] H. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, preprint, 2005.
[12] N. Katz, T. Tao, Some connections between Falconer’s distance set conjecture and sets of Furstenberg type, New York J. Math. 7 (2001) 149–187.
[13] A. Lubotzky, Discrete Groups, Expanding Graphs and Invariant Measures, Progr. Math., vol. 195, Birkhäuser, 1994.
[14] A. Lubotzky, Cayley graphs: eigenvalues, expanders and random walk, in: P. Rowbinson (Ed.), Surveys in Combinatorics, in: London Math. Soc. Lecture Note Ser., vol. 218, Cambridge Univ. Press, 1995, pp. 155–189.
[15] A. Lubotzky, B. Weiss, Groups and expanders, in: J. Friedaman (Ed.), DIMACS Ser. Discrete Math. and Theoret. Comput. Sci., vol. 10, Amer. Math. Soc., 1993, pp. 95–109.
[16] P. Sarnak, X. Xue, Bounds for multiplicatives of automorphic representations, Duke Math. J. 64 (1991) 207–227.
[17] A. Selberg, On the estimation of Fourier coefficients of modular forms, in: Proc. Sympos. Pure Math., vol. VII, Amer. Math. Soc., 1965, pp. 1–15.
[18] T. Tao, Non-commutative sum set estimates, preprint.
[19] T. Tao, V. Vu, Additive Combinatorics, Cambridge University Press, 2006, in press.