Jean Bourgain

Institute for Advanced Study
Princeton, NJ 08540

February 13, 2008

CONJECTURE

Let S be a finite subset of $SL_d(\mathbb{Z})$ generating a Zariski dense subgroup. Then there is $q_0 \in \mathbb{Z}$ such that the family of Cayley graphs

$$\mathcal{G}\Big(SL_d(\mathbb{Z}/q\mathbb{Z}), \pi_q(S)\Big)$$

with $q \in \mathbb{Z}_+, (q, q_0) = 1$ forms a family of expanders

$$c(\mathcal{G}) = c_q(\mathcal{G}_q) > c(S) > 0$$

$$c(\mathcal{G}) = \text{expansion coefficient of } \mathcal{G}$$

$$= \text{ inf } \Big\{\frac{|\partial X|}{|X|} \text{ where } |X| < \frac{1}{2}|V|\Big\}$$

(partly motivated by problems of prime sieving)

Connectedness of the graph

strong approximation property

Matthews, Vaserstein, Weisfeiler (1984)

Pink (2000)

Theorem. *Let* G *be a Zariski dense subgroup of* $SL_d(\mathbb{Z})$*. There is* $q_0 \in \mathbb{Z}$ *such that* $\pi_q(G) = SL_d(\mathbb{Z}/q\mathbb{Z})$ *if* $(q, q_0) = 1$

π_q: reduction mod q

CASE $\mathbf{d = 2}$

(I) $\mathbf{q = p}$ (prime) **B–Gamburd**

(based on work of Helfgott)

Theorem. *Let $S_p = \{g_1, g_1^{-1}, \dots, g_k, g_k^{-1}\}$ be a symmetric generating set for $SL_2(p)$, such that*

$$\textit{girth } \Big(\mathcal{G}(SL_2(p), S_p)\Big) > \tau \log p$$

($\tau > 0$ independent of p).

Then the expansion coefficient of $\mathcal{G}\Big(SL_2(p), S_p)$ admits a uniform lower bound $c(\tau) > 0$.

Problem. Remove the large girth assumption

(II) q squarefree   B-Gamburd-Sarnak

Proof of the Conjecture for $d = 2$, q squarefree

$$q = \prod p_j$$

$$SL_2(\mathbb{Z}/q\mathbb{Z}) \simeq \prod_j SL_2(\mathbb{Z}/p_j\mathbb{Z})$$

Applications to prime sieving

Theorem. (BGS)
Let G be a finitely generated non-elementary subgroup of $SL_2(\mathbb{Z})$. Then there is a positive integer $r = r(G)$ such that the set

$$\{g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G | abcd \text{ has at most } r \text{ prime factors}\}$$

is Zariski dense

(III) $\mathbf{q = p^n}$ (B–Gamburd)

Proof of the Conjecture for $d = 2$ and moduli q of the form p^n, with uniformity in p and n.

Part of the argument relates to Solovay–Kitaev algorithm

If we fix p and let $n \to \infty$, the argument may be extended to $d > 2$

Theorem. *Assume $\langle S \rangle$ Zariski dense in $SL_d(\mathbb{Z})$. Let $q = p^n$, p sufficiently large prime, and*

$$\mathcal{G} = \mathcal{G}\Big(SL_d(\mathbb{Z}/q\mathbb{Z}), \pi_q(S)\Big)$$

$\mathbf{d = 2}$: $\quad \mathbf{c}(\mathcal{G}) > \mathbf{c}(\mathbf{S}) > \mathbf{0}$

$\mathbf{d > 2}$: $\quad \mathbf{c}(\mathcal{G}) > \mathbf{c}(\mathbf{p}, \mathbf{S}) > \mathbf{0}$

$SL_2(p^n)$ with p fixed, $n \to \infty$

$\leftrightarrow$

$SU(2)$

Theorem. (B–Gamburd, 06)

Let $k \geq 2$ *and* $g_1, \ldots, g_k$ *algebraic elements in* $G = SU(2)$

Consider the Hecke operator

$$T : L^2(G) \to L^2(G) \quad Tf(x) = \sum_{j=1}^{k} \Big(f(g_j x) + f(g_j^{-1} x) \Big)$$

Then there is a spectral gap

$$\lambda_1(T) < 2k - \gamma$$

where $\gamma = \gamma(g_1, \ldots, g_k) > 0$ *may be controlled by a noncommutative diophantine property*

Applications to Banach–Ruziewiez problem, quantum-computation, orientations in the Conway-Radin quaquaversal tilings, ...

Theorem. *p fixed and sufficiently large*

$$S = \{g_1, \dots, g_k, g_1^{-1}, \dots, g_k^{-1}\} \subset SL_d(\mathbb{Z})$$

such that

$$< \pi_p(S) >= SL_d(\mathbb{Z}/p\mathbb{Z})$$

Then

$$\mathcal{G}\Big(SL_d(\mathbb{Z}/p^n\mathbb{Z}), \pi_{p^n}(S)\Big) = \mathcal{G}_n$$

is expander family

INGREDIENTS

(1) Reduction to non-existence of certain 'approximative subgroups' of $SL_d(\mathbb{Z}/q\mathbb{Z})$

- Spectral multiplicity argument
- Non-commutative Balog-Szemeredi-Gowers

(2) Theory of random matrix products

(3) Construction of large sets of commuting elements

(4) Sum-product theorem in $\mathbb{Z}/q\mathbb{Z}$

(5) Solovay-Kitaev type multi-scale construction

Corollary. *Assume*

$$S = \{g_1, \dots, g_k, g_1^{-1}, \dots, g_k^{-1}\} \subset SL_d(\mathbb{Z})$$

generates a Zariski-dense group and consider the probability measure

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

Let $\mathfrak{S}$ be a nontrivial algebraic subvariety of $SL_d(\mathbb{C})$. Then the convolution powers $\nu^{(\ell)}$ of ν satisfy

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

for some $c = c(S, \mathfrak{S}) > 0$

Main Proposition

Assume $\langle$supp $\nu\rangle$ Zariski dense

$$q = p^n \qquad (p \text{ fixed}, n \to \infty)$$

For all $\gamma > 0$, there is $c = c(\nu, p, \gamma)$ such that

$$\|\nu^{(\ell)}\|_\infty < q^\gamma |SL_d(\mathbb{Z}/q\mathbb{Z})|^{-1} \text{ for } \ell > C. \log q$$

Expansion property then follows from Sarnak–Xue trace argument using the fact that a faithful irreducible representation of $SL_d(\mathbb{Z}/q\mathbb{Z})$ has dimension at least $\sim q$.

$\Rightarrow$ lower bounds on eigenvalue multiplicities in regular representation

Reduction to 'Approximate groups'

Proposition. (non-commutative BSG)

Let G be a finite group, $N = |G|$.

Suppose $\mu \in \mathcal{P}(G)$ a symmetric probability measure on G s.t.

$$\|\mu\|_\infty < N^{-\gamma}$$

and

$$\|\mu\|_2 > N^{-\frac{1}{2}+\gamma}$$

with $\gamma > 0$ an arbitrary given constant.
Assume further

$$\|\mu * \mu\|_2 > N^{-\varepsilon}\|\mu\|_2$$

with $0 < \varepsilon < \varepsilon(\gamma)$.

Then there is $H \subset G$ subset with the following properties

(1) $H = H^{-1}$

(2) $|H| < N^{1-\gamma}$

(3) *There is $X \subset G, |X| < N^{\varepsilon'}$ with $H.H \subset X.H \cap H.X$*

(4) $\mu(x_0 H) > N^{-\varepsilon'}$ *for some $x_0 \in G$*

where $\varepsilon' \sim \varepsilon$

Random matrix products

Bougerol–Lacroix (Birkhauser 86)

Guivarch (ETDS 90)

We use the assumption that $\langle \text{supp} \ \nu \rangle$ is Zariski dense

Proposition 1. *(simplicity of the eigenvalues)*

$$\nu^{(\ell)} \left\{ g \Big|^{g \text{ diagonalizable with distinct eigenvalues } \lambda_1, \dots, \lambda_d}_{\frac{1}{\ell} \log |\lambda_j| \approx \gamma^{(j)} = \text{Lyapounov exponent}} \right\}$$

$$> 1 - e^{-c\ell}$$

Proposition 2. *(escaping hyperplanes)*

$$\nu^{(\ell)} \{ g \Big| \text{Tr}\, g \xi g^{-1} \eta = 0 \} < e^{-c\ell}$$

whenever $\xi, \eta \neq 0, \text{Tr}\, \xi = 0 = \text{Tr}\, \eta$.

Here $c = c(\nu) > 0$.

Consequences (mod Q)

Proposition 1′. *Let* $Q \in \mathbb{Z}_+$ *(large) and* $\ell > \log Q$. *Then*

$$\nu^{(\ell)}\{g \in SL_d(\mathbb{Z}) | \mathit{Res}\ (P_g, P_g') \equiv 0 (\mathit{mod}\, Q)\} < Q^{-c}$$

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

Proposition 2′. *Let* $Q \in \mathbb{Z}_+$, $\ell > \log Q$.
There is an uniform estimate

$$\nu^{(\ell)}\{g \in SL_d(\mathbb{Z}) |\ \mathit{Tr}\ g\xi g^{-1}\eta \equiv 0 (\mathit{mod}\, Q_1)\} < Q^{-c}$$

whenever $\xi, \eta \in$ *Mat*$_d(\mathbb{Z})$ *satisfy*

$$\pi_Q(\xi) \neq 0, \pi_Q(\eta) \neq 0$$

$$\mathit{Tr}\ \xi = 0 = \mathit{Tr}\, \eta$$

Here $Q_1 = Q^c, c = c(d) \in \mathbb{Z}$

Lifting mod $\mathbf{Q} \longrightarrow \mathbb{C}$

Use of effective Bezout theorem

Proposition. (Berenstein–Yger, Acta 91)

Let $p_1, \ldots, p_N \in \mathbb{Z}[x_1, \ldots, x_n]$ *without common zeros in* $\mathbb{C}^n$,

$\deg p_j \le D \quad (D \ge 3)$.

$h(p_j) \le h$

Then there is an integer $\Delta \in \mathbb{Z}_+$ *and polynomials* $q_1, \ldots, q_N \in \mathbb{Z}[x_1, \ldots, x_n]$ *such that*

$$p_1 q_1 + \cdots + p_N q_N = \Delta$$

and

$$\deg q_j \le n(2n+1)D^n$$

$$\log \Delta + \sum h(q_j) < C(n)[h + \log N + D \log D]$$

In the application $n, D < C(d)$ and $h \sim \ell$

Commuting elements
(Helfgott's argument)

Lemma. *There are elements* $g_2, \ldots, g_{d^2}$ *in* $H^{(6)} \subset Mat_d(\mathbb{Z})$ *and* $q_0 = p^{m_0}$, $m_0 < \varepsilon n$ *such that* $\|g_i\| < q_0$ *and* $\{1, g_2, \ldots, g_{d^2}\}$ *are linearly independent.*

Take $g_1 = 1$ and consider the map

$$\mathrm{Mat}_d(\mathbb{Z}/q\mathbb{Z}) \to (\mathbb{Z}/q\mathbb{Z})^{d^2} : \; g \mapsto (\mathrm{Tr}\, g g_i)_{1 \le i \le d^2}$$

which multiplicity is at most $q^{C\varepsilon}$.

Restrict map to $H.H \Rightarrow$ large set of traces

$\Rightarrow$ small conjugacy classes

$\Rightarrow$ large set of commuting elements

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

(1) $\mathit{Res}(P_h, P'_h) \neq 0 \qquad (\mathit{mod}\, p^{m_0})$

(2) $|S| > q^c$

(3) $gh = hg \quad (\mathit{mod}\, q)$

Diagonalize $h \in SL_d(\mathbb{Z})$ considering an extension field K of $\mathbb{Q}$.

Let $\mathcal{P}$ be a prime divisor of (p) in the ring of integers O of K. Then

$$h = \sum_{i=1}^{d} \mu_i \; e_i \otimes e_i \qquad \prod_{i \neq j} (\mu_i - \mu_j) \notin \mathcal{P}^{m_0}$$

In this basis, each $g \in S$ has representation

$$g = \sum \lambda_i \; e_i \otimes e_i \qquad (\text{mod}\, \mathcal{P}^{n-m_0})$$

(we assume $\mathcal{P}$ unramified)

(Uniform) sum-product theorem in $\mathbb{Z}/q\mathbb{Z}$

The following statements are uniform in the modulus $q \in \mathbb{Z}_+$

Theorem. *Given* $0 < \delta_1, \delta_2 < 1$, *there are* $\varepsilon > 0$ *and* $\delta_3 > 0$ *such that the following holds*

Let $q \in \mathbb{Z}_+$, *large enough, and* $A \subset \mathbb{Z}/_q\mathbb{Z}$ *satisfy*

(i) $|A| < q^{1-\delta_1}$

(ii) $|\pi_{q_1}(A)| > q_1^{\delta_2}$ *whenever* $q_1 | q$ *and* $q_1 > q^\varepsilon$

Then

$$|A + A| + |A.A| > q^{\delta_3}|A|$$

$$q = \prod_j p_j^{m_j}$$

$$\mathbb{Z}/q\mathbb{Z} \simeq \prod_j \mathbb{Z}/p_j^{m_j}\mathbb{Z}$$

Statement for $q = p^m$, p fixed and $m \to \infty$, is a p-adic version of 'discretized ring theorem' for subsets $A \subset \mathbb{R}$

Corollary 1.

Given $\delta > 0$, there is a constant C and $r, s \in \mathbb{Z}_+$, $r, s < C$ such that the following holds

Let $A \subset \mathbb{Z}$ and q of the form $q = p^n$ s.t.

$$|\pi_q(A)| > q^\delta$$

Then there are $q_1 = p^{n_1}, q_2 = p^{n_2}$ such that

(1) $n_1 < n_2 < Cn$ *and* $n_2 - n_1 > \frac{\delta}{4}n$

(2) $\pi_{q_2}(A') \supset \{x \in \mathbb{Z}/q_2\mathbb{Z} | x \equiv 0 (\mathit{mod}\, q_1)\}$ *where*

$$A' = \underbrace{A^{(s)} \pm \cdots \pm A^{(s)}}_{r},$$

$$A^{(s)} = \underbrace{A \cdots A}_{s}$$

Corollary 2. (subsets of Cartesian products $\mathbb{Z}^w$)

Given $\delta > 0$, *there is* $\kappa > 0$ *and* $r, s \in \mathbb{Z}_+$, $r, s < C$ *such that the following holds.*

Let $A \subset \mathbb{Z}^w$ *and* q *of the form* $q = p^n$. *Assume*

$$|\pi_q(A)| > q^\delta$$

Then there are $q_1 = p^{n_1}, q_2 = p^{n_2}$ *and a vector* $\xi \in \mathbb{Z}^w$ *s.t.*

(1) $n_1 < n_2 < Cn$ *and* $n_2 - n_1 > \kappa n$

(2) $\pi_p(\xi) \neq 0$

(3) $\pi_{q_2}(A') \supset \left\{ q_1 t \xi \;|0 \leq t \in \mathbb{Z}, 0 \leq t < \frac{q_2}{q_1} \right\}$

where

$$A' = rA^{(s)} - rA^{(s)} \text{ in the ring } \mathbb{Z}^w$$

Commutators and multi-scale structure

Lemma.

Let $g \equiv 1 (mod\ p^m)$ *and* $h \equiv 1\ (mod\ p^{m'})$

Then

$C(g,h) \equiv 1+[g,h]\ \ (mod\ p^{m+m'+\min(m,m')})$

where

$C(g,h) = ghg^{-1}h^{-1}$ *and* $[g,h] = gh-hg$

Let $q_1 < q_2 < \tilde{q}$ be relatively small divisors of $q = p^n$

Fix $\zeta \in$ Mat$_d(\mathbb{Z})$ such that

$$1 + \tilde{q}\zeta \in H^{(4)} \quad \pi_p(\zeta) \neq 0 \quad \text{Tr } \zeta = 0$$

Let $S \subset H^{(2)}$ be the diagonal set and consider elements

$$g = 1 + q_1 x \in SS^{-1}$$

where

$$x = \sum \sigma_i \, e_i \otimes e_i \qquad \left(\text{mod } \frac{q_2}{q_1}\right)$$

Then

$$C(1+\tilde{q}\zeta, g) = 1+\tilde{q}q_1 \sum_{i\neq j} (\sigma_i - \sigma_j)\zeta_{ij} \, e_i \otimes e_j \;\; (\text{mod } \tilde{q}q_2)$$

and iterating k times with $g^{(1)}, \ldots, g^{(k)} \in SS^{-1}$ as above

$$C\Big(\cdots C(C(1+\tilde{q}\zeta, g^1), g^2)\cdots g^k\Big) =$$

$$1 + \tilde{q}q_1^k \sum_{i\neq j} \prod_{\ell \leq k} (\sigma_i^{(\ell)} - \sigma_j^{(\ell)})\zeta_{ij}(e_i \otimes e_j)$$

$$(\text{mod } \tilde{q}q_1^{k-1}q_2)$$

Let

$$w = \frac{d(d-1)}{2}$$

Consider the ring $\mathbb{Z}^w$ and quotients

Denote

$$A = \{(\sigma_i - \sigma_j)_{1\le i<j\le d} \big| 1 + q_1 x \in SS^{-1}\}$$

H-Commutators $\longrightarrow$ product set $A^{(k)}$

Also

$$(1+\tilde{q}q_1^k z)(1+\tilde{q}q_1^k z') = 1+\tilde{q}q_1^k(z+z') \pmod{\tilde{q}q_1^{k-1}q_2}$$

H-products $\longrightarrow$ sum sets $A^{(k)} + A^{(k)}$

Apply sum-product results in $(\mathbb{Z}/q\mathbb{Z})^w$

Conclusion. *There are divisors $Q_1 < Q_2$ of q and $\xi \in Mat_d(\mathbb{Z})$ such that*

(1) $\log Q_1 \sim \log Q_2 \sim \log \frac{Q_2}{Q_1} \sim \varepsilon_0 \log q$

(1) $Tr\, \xi = 0$

(3) $\pi_p(\xi) \neq 0$

(4) *There is a suitable product set H' of H s.t.*

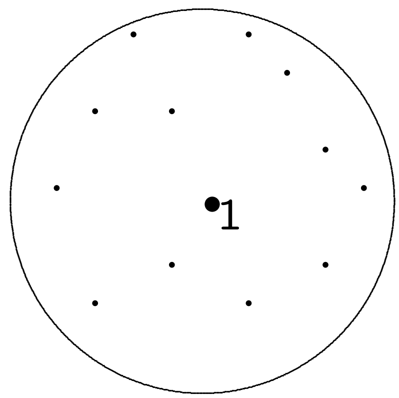
$$\pi_{Q_2}(\{1 + Q_1 t\xi \,\Big|\, t \in \mathbb{Z}\}) \subset \pi_{Q_2}(H')$$

Next, conjugate ξ with elements of H and use the fact that $\{g\xi g^{-1} | g \in H\}$ span full space of traceless matrices mod q_0 where

$$q_0 | q \text{ and } \log q_0 < C\varepsilon \log q \ll \varepsilon_0 \log q$$

Conclusion$'$. *There are divisors $Q_1 < Q_2$ of q as above s.t.*

$$\pi_{Q_2}(\{1+Q_1 x | x \in Mat_d(\mathbb{Z}),\ Tr\, x = 0\}) \subset \pi_{Q_2}(H')$$



$|\ |_p = p$-adic absolute value

We proved that if

$$|1 - g|_p < \frac{1}{Q_1},$$

then there is some $h \in H'$ s.t.

$$|g - h|_p < \frac{1}{Q_2}$$

Here $\log Q_1 \sim \log Q_2 \sim \log \frac{Q_2}{Q_1} \sim \varepsilon_0 \log q$

Further amplification using Solovay-Kitaev algorithm

$$\Rightarrow |H'| > |SL_d(\mathbb{Z}/q\mathbb{Z})|^{1-\varepsilon_0} = N^{1-\varepsilon_0}$$

Contradicts assumptions on H

$$|H'| < N^{C\varepsilon}|H| < N^{1-\gamma+C\varepsilon}$$

Generation problem

$d = 2$ or $d > 2$

<u>$\mathbf{SU(2)}$</u> Let S be a subset of $SU(2)$ which allows to approximate up to ε_0 (ε_0 fixed small constant), $S = S^{-1}$.

It is true that

$$\max_{g \in SU(2)} \min_{h \in \underbrace{S \cdots S}_{\ell}} \|g - h\| < e^{-c\ell} \text{ when } \ell \to \infty?$$

True if S is algebraic.

<u>$\mathbf{SL_2(\mathbb{Z}_p)}$</u> Let $S \subset SL_2(\mathbb{Z}_p), S = S^{-1}$ and

$$\pi_p(S) = SL_2(\mathbb{Z}/p\mathbb{Z})$$

Is there a constant C (possibly independent of S) such that $\forall n$

$$\ell > Cn \Rightarrow \pi_{p^n}(\underbrace{S \cdots S}_{\ell}) = SL_2(\mathbb{Z}/p^n\mathbb{Z})?$$

True if $S \subset SL_2(\mathbb{Z})$.