Expanders and good distribution

François Hennecart
(*Institut Camille Jordan Lyon St-Étienne*)

Combinatorial and Additive Number Theory 2016
Graz
2016, 4-8 January

Background 1 - Expanders

An *expander* (of level $\alpha \in]0,1[$) is a function $f(x,y) \in \mathbf{Z}_p[x,y]$ satisfying

$$\text{for any } A \subset \mathbf{Z}_p \text{ with } |A| = p^\alpha, \quad \mathbf{Card}(f(A,A)) \gg |A|^{1+\rho(\alpha)} \quad (\rho(\alpha) > 0)$$

where $f(A,A) = \{f(a,b),\ a,b \in A\}$.

Examples

- $x + y$ is **not** an expander
- xy is **not** an expander
- $x^2 + xy$ is an expander of any level (Bourgain - 2005)
- $xy + x^2y^2$ is **not** an expander ($xy + x^2y^2 = \frac{(2xy+1)^2-1}{4}$)
- $u(x) + x^k v(y)$ is an expander of any level, except degenerate cases for u, v (Hegyvári–H. - 2009)
- $x^2y + xy^2$ is **not known to be or not to be** an expander (even for some given level)

Background 2 - Good distribution

Definition. A set (or a multiset) $M = (m_1, \ldots, m_k)$ in $\mathbf{Z}_p$ is *well distributed with level* η (in the arithmetic way) if

for any *interval* $I = \{a, a+q, \ldots, a+(|I|-1)q\}$ with $|I| = p^\eta$

$$\|M \cap I\| \gg \frac{\|M\| |I|}{p}, \qquad \|M\| = k = \text{length of } M.$$

We define similarly the notion of *good geometrical distribution* by considering the trace of M on geometric instead of arithmetic progressions.

Good arithmetic distribution for M follows from sharp upper bounds for exponential sums (Fourier coefficients of the characteristic function of M)

$$\max_{r \neq 0 \bmod p} \left| \sum_{j=1}^{k} e_p(rm_j) \right| \qquad e_p(x) = \exp\left(\frac{2\pi i x}{p}\right)$$

A criterion for good distribution

Criterion. Assume that $M = (m_1, \ldots, m_k)$ and that

$$S(M) := \max_{r \neq 0 \bmod p} \left| \sum_{j=1}^{k} e_p(rm_j) \right| \ll \frac{\|M\|}{p^\theta}, \qquad \theta > 0.$$

Then M is (arithmetically) well distributed (a.w.d.) for any level $\eta > 1 - \theta$.

Proof. Let I be an interval and write $I = J + J$ where J is also an interval with $|J| \geq |I|/2$. Then

$$\|M \cap I\| \geq \frac{\|M \cap (J + J)\|}{|J|}$$

$$\|M \cap (J + J)\| = \frac{1}{p} \sum_{r \in \mathbf{Z}_p} \sum_{m \in M} \sum_{u,v \in J} e_p(r(m - u - v))$$

$$\frac{\|M\||J|^2}{p} - \|M \cap (J + J)\| \leq S(M) \times \frac{1}{p} \sum_{r \neq 0} \left| \sum_{u \in J} e_p(ru) \right|^2 < \frac{\|M\||J|}{p^\theta}$$

A criterion for good distribution

Then

$$\|M \cap I\| \gg \frac{\|M\||J|^2}{p|J|} \gg \frac{\|M\||J|}{p} \gg \frac{\|M\||I|}{p}$$

whenever $|J| \gg p^{1-\theta}$. **QED**

For testing the good distribution in the multiplicative way of a multiset M of $\mathbf{Z}_p^*$ we use the following:

Criterion for good geometric distribution.
Let $M = (m_1, \dots, m_k)$ is a multiset and assume that

$$T(M) := \max_{\substack{\chi \in \widehat{\mathbf{Z}_p^*} \\ \chi \neq \chi_0}} \left| \sum_{j=1}^{k} \chi(m_j) \right| \ll \frac{\|M\|}{p^\theta}$$

Then M is (geometrically) well distributed (g.w.d.) for any level $\eta > 1 - \theta$.

Binary functions and good distribution

Let $f(x, y) \in \mathbf{Z}_p$ be a binary function. We ask the question of good distribution (with some level $\rho(\alpha)$) for any multiset

$$M = \Big(f(a, b), \; a, b \in A \Big)$$

with $A \subset \mathbf{Z}_p$ of size $|A| \asymp p^{\alpha}$.

Definition. If it is the case we write shortly that f is a.w.d. (or g.w.d.) with level $(\alpha, \rho(\alpha))$.

Question 1. Is it true that any expander $f(x, y)$ has both good arithmetical and geometrical ditribution for some level $(\alpha, \rho(\alpha)), \; \alpha < 1$? ???

Question 2. Do there exist binary functions which are not expanders but have good distribution (in both ways) ? YES, think to $xy + x^2y^2$.

Question 3. Is $x^2y + xy^2 = xy(x + y)$ both arith. and geom. well distributed ? (Recall that we do not know if it is an expander) YES

$xy^2 + x^2y$ is a.w.d.

Let $A \subset \mathbf{Z}_p$ with $|A| = p^\alpha$ $(\alpha > 1/2)$ and for $\gcd(r,p) = 1$

$$S_r := \left| \sum_{x,y \in A} e_p\big(r(xy^2 + x^2y)\big) \right| \le \sum_{y \in A} \left| \sum_{x \in A} e_p\big(r(xy^2 + x^2y)\big) \right|$$

By Cauchy inequality

$$S_r^2 \le |A| \left(\sum_{y \in \mathbf{Z}_p} \sum_{x_1, x_2 \in A} e_p\Big(r\big((x_1 - x_2)y^2 + (x_1^2 - x_2^2)y\big)\Big) \right)$$

Separating the case $x_1 = x_2$ in the inner sum and using the bound $O(\sqrt{p})$ for Gauss quadratic sums

$$S_r \le \sqrt{|A|}\Big(p|A| + |A|^2\sqrt{p}\Big)^{1/2} \le 2|A|^{3/2}p^{1/4} \ll \frac{|A|^2}{p^{1/4-\alpha/2}}$$

$xy^2 + x^2y$ is a.w.d. continued

Let $\alpha > 1/2$.

Proposition 1. $xy^2 + x^2y$ is both a.w.d. and g.w.d. with level $(\alpha, 5/4 - \alpha/2)$.

Proposition 2. $xy^2 + x^2y$ is a.w.d. with level $(\alpha, 11/8 - 3\alpha/4)$. [arguing more effectively when evaluating by Gauss sums]

And for $\alpha \leq 1/2$?

Proposition 3. There exists two positive number $\alpha_0 < 1/2$ and γ_0 such that $xy^2 + x^2y$ is a.w.d. with level $(\alpha, 1 - \gamma_0)$ for any $\alpha \geq \alpha_0$.

Again we want to bound

$$S_r := \Big| \sum_{x,y \in A} e_p(r(xy^2 + x^2y)) \Big| \qquad r \neq 0$$

We copy an argument due to Bourgain (2005) (in the context of extractors) which gives $S_r \ll |A|^2 p^{-\gamma}$ when $p^{1/2-\delta} \ll |A| \leq p^{1/2}$.

The case $1/2 \geq \alpha > 1/2 - \delta_0$

Vinogradov type approach : starting from S_r and by Cauchying 'many' times we reduce the problem to get a sharp bound for

$$S_r^{16} \ll |A|^{24} \sum_{\xi,\eta \in \mathbf{Z}_p^2} \nu(\xi)\nu(\eta)e_p(r\xi\cdot\eta)$$

$$\ll p|A|^{24} \left(\sum_{\xi \in \mathbf{Z}_p^2} \nu(\xi)^2\right)^{1/2} \left(\sum_{\eta \in \mathbf{Z}_p^2} \nu(\eta)^2\right)^{1/2}$$

$\nu(\xi)$ is the number of solutions $x_i \in A$ to

$$\begin{aligned} \xi_1 &= x_1 - x_2 + x_3 - x_4 \\ \xi_2 &= x_1^2 - x_2^2 + x_3^2 - x_4^2 \end{aligned}$$

An efficient tool: bounds for incidences

Let P be a set of points in $\mathbf{F}^2$ and L be a set of lines in $\mathbf{F}^2$.

$$\mathrm{Inc}(P, L) = \mathbf{Card}\{(\pi, \lambda) \in P \times L \text{ such that } \pi \in \lambda\}$$

A trivial bound is

$$\mathrm{Inc}(P, L) \ll |P||L|^{1/2} + |P|^{1/2}|L|$$

A typical result (valid for $\mathbf{F} = \mathbf{R}$) is

$$\mathrm{Inc}(P, L) \ll |P| + |L| + |P|^{2/3}|L|^{2/3} \quad \text{(Szemerédi–Trotter, 1983)}$$

A result for $\mathbf{F} = \mathbf{Z}_p$

$$\mathrm{Inc}(P, L) \ll \max(|P|, |L|)^{3/2-\delta} \text{(Bourgain–Katz–Tao, 2004)}$$

(δ is an effective absolute constant, $1/900$ is admissible by Tim Jones 2015 ?)

Application

Consider the number $\sum_{\xi \in \mathbf{Z}_p^2} \nu(\xi)^2$ of solutions $x_i \in A$ (with $|A| = p^\alpha$) to

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= x_5 + x_6 + x_7 + x_8 \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 &= x_5^2 + x_6^2 + x_7^2 + x_8^2 \end{aligned}$$

(Observation : trivial bound is $O(|A|^6)$)

Let $\nu(\xi, t)$ the number of solutions $(x_1, x_2, x_4) \in A^3$ to

$$\begin{aligned} \xi_1 &= x_1 - x_2 + t - x_4 \\ \xi_2 &= x_1^2 - x_2^2 + t^2 - x_4^2 \end{aligned}$$

with $x_1 \neq x_2$. By eliminating x_4 we get the equation of a line in $\mathbf{Z}_p^2$

$$\lambda_{x_1,x_2}: \quad \xi_2' = \xi_2 + 2\xi_1^2 = 2(x_1 - x_2 + t)\xi_1 - (x_1 - x_2 + t)^2 + x_1^2 - x_2^2 + t$$

We may apply an incidence theorem!

Application, continued

There are $O(|A|^2)$ such lines. For k fixed, we denote

$$\mathcal{C}_k = \left\{(\xi_1, \xi_2') \in \mathbf{Z}_p^2 \mid \xi_1 - x_1 + x_2 - t \in A \text{ for at least } k \text{ pairs } (x_1, x_2) \in A^2\right\}$$

Then

$$\mathrm{Inc}(\mathcal{C}_k, \Lambda) \ll |\mathcal{C}_k|^{3/2-\delta} + |\Lambda|^{3/2-\delta} \ll |\mathcal{C}_k|^{3/2-\delta} + |A|^{3-2\delta}$$

Let $c_k = |\mathcal{C}_k|$. Then

$$c_k \leq \frac{|A|^3}{k} \quad \text{and} \quad c_k k \ll c_k^{3/2-\delta} + |A|^{3-2\delta}$$

$$\sum_{\xi \in \mathbf{Z}_p} \nu(\xi, t)^2 = \sum_{k \leq 2|A|} k^2 (c_k - c_{k+1}) = \sum_{k \leq 2|A|} (2k-1) c_k$$

From this we easily infer that for each $t \in A$

$$\sum_{\xi \in \mathbf{Z}_p} \nu(\xi, t)^2 \ll |A|^{4-\delta}$$

Application, finished

By Cauchy inequality we get the upper bound

$$\sum_{\xi\in\mathbf{Z}_p^2}\nu(\xi)^2=\sum_{\xi\in\mathbf{Z}_p^2}\Big(\sum_{t\in A}\nu(\xi,t)\Big)^2\le|A|\sum_{\xi\in\mathbf{Z}_p^2}\sum_{t\in A}\nu(\xi,t)^2\le|A|^2\times|A|^{4-\delta}$$

instead of the trivial bound $O(|A|^6)$.Returning to our estimation of S_r

$$S_r^{16}\ll p|A|^{30-\delta}$$

Hence for $|A|\gg p^{1/2-\delta/4}$ we have

$$|S_r|\ll|A|^{2-\delta/50}$$

We conclude that

xy^2+x^2y is a.w.d. for any level $(\alpha,1-\delta/50)$ with $\alpha>1/2-\delta/4$.

Remark. Since xy^2+x^2y has degree 3, it is clear that it is not a.w.d. of level $(\alpha,\rho(\alpha))$ with $\alpha\le 1/3$.

Final remark 1: k-source extractor

A k-source extractor (with entropy α) is a k-variate function

$$F : \mathbf{Z}_p^k \longrightarrow \{-1, 1\}$$

such that for any cube $\mathbf{C} = A_1 \times \cdots \times A_k$ with $|A_i| \asymp p^\alpha$ for all i

$$\sum_{\mathbf{x} \in \mathbf{C}} F(\mathbf{x}) \ll \frac{|\mathbf{C}|}{p^{\gamma(\alpha)}} \qquad (\gamma(\alpha) > 0)$$

Let $f : \mathbf{Z}_p^k \longrightarrow \mathbf{Z}_p$ such that

$$\sum_{\mathbf{x} \in \mathbf{C}} e_p(rf(\mathbf{x})) \ll \frac{|\mathbf{C}|}{p^{\gamma'(\alpha)}} \qquad (\gamma'(\alpha) > 0)$$

Bourgain (2005) has shown that by setting

$$F = \operatorname{sgn} \sin\left(\frac{2\pi f}{p}\right)$$

one obtains a k-source extractor.

Final remark 2: Conditional lower bounds

Denoting $f(x, y) = xy^2 + x^2y$ one has (Hegyvári-H., 2013)

$$\max(|f(A, A)|, \min(|2A|, |A^2|)) \gg |A|^{1+\kappa(\alpha)}, \qquad \kappa(\alpha) > 0,$$

if $A \subset \mathbf{Z}_p$, $|A| \asymp p^\alpha$, for any $0 < \alpha < 1$.

Final remark 3: level of good distribution for an expander

The function $f(x, y) = xy + x^2$ is an expander of any level (Bourgain). But clearly it cannot be well distributed with level $\alpha \le 1/2$ since for $A = (0, p^\alpha/2)$ we have

$$f(A, A) \subset (0, p^{2\alpha}/2)$$

Nevertheless we may ask the general question:

Question. Is it true that for any expander $f(x, y)$ of any level $\alpha \in (\alpha_0, 1)$, there exists $\alpha_0' \in (0, 1)$ (depending on f) such that $f(x, y)$ is a.w.d. (resp. g.w.d.) with level α' for any $\alpha' \in (\alpha_0', 1)$?

Vielen Danke

Second announcement

Additive Combinatorics in Bordeaux

`http://acb.math.u-bordeaux.fr/`
(*ready for registration*)