Discrete spheres and arithmetic progressions in product sets

Dmitry Zhelezov

Chalmers University of Technology
University of Gothenburg

Graz, January 4-8 2016

Sums and Products

Let A be a set. The sumset and the product set are defined as follows.

$$\begin{aligned} A + A &= \{a_1 + a_2, a_{1,2} \in A\} \\ A.A &= \{a_1 a_2, a_{1,2} \in A\}. \end{aligned}$$

Conjecture (P. Erdős and E. Szemerédi)

$$\max(|A.A|, |A + A|) \geq c_\epsilon |A|^{2-\epsilon},$$

General idea

A set cannot be multiplicatively and additively structured at the same time

Sums and Products

Let A be a set. The sumset and the product set are defined as follows.

$$\begin{aligned} A + A &= \{a_1 + a_2, a_{1,2} \in A\} \\ A.A &= \{a_1 a_2, a_{1,2} \in A\}. \end{aligned}$$

Conjecture (P. Erdős and E. Szemerédi)

$$\max(|A.A|, |A + A|) \geq c_\epsilon |A|^{2-\epsilon},$$

General idea

A set cannot be multiplicatively and additively structured at the same time

Sums and Products

Let A be a set. The sumset and the product set are defined as follows.

$$\begin{aligned} A+A &= \{a_1+a_2, a_{1,2} \in A\} \\ A.A &= \{a_1 a_2, a_{1,2} \in A\}. \end{aligned}$$

Conjecture (P. Erdős and E. Szemerédi)

$$\max(|A.A|, |A+A|) \geq c_\epsilon |A|^{2-\epsilon},$$

General idea

A set cannot be multiplicatively and additively structured at the same time

Our setting

$$\begin{aligned} \text{Multiplicative structure} &= A \text{ is a product set (i.e. } = B.B) \\ \text{Additive structure} &= A \text{ contains a very long AP} \end{aligned}$$

Question

Let B be a set of integers. Assume that $B.B$ contains an AP of size M. How small can the set B be ? Can B be, say, of size $|M|^{0.99}$?

Main result

Theorem (Z. 2015)

Let B be an integer set. If $B.B$ contains an AP of size M then

$$|B| \geq \pi(M) + c\frac{M^{2/3}}{\log^2 M},$$

where π is the prime counting function and $c > 0$ is a constant. Moreover, there are examples with

$$|B| \leq \pi(M) + M^{2/3}.$$

Remark. Rumors [PPP] are that there are examples with

$$|B| \leq \pi(M) + c'\frac{M^{2/3}}{\log^2 M}.$$

Main result

Theorem (Z. 2015)

Let B be an integer set. If $B.B$ contains an AP of size M then

$$|B| \geq \pi(M) + c\frac{M^{2/3}}{\log^2 M},$$

where π is the prime counting function and $c > 0$ is a constant. Moreover, there are examples with

$$|B| \leq \pi(M) + M^{2/3}.$$

Remark. Rumors [PPP] are that there are examples with

$$|B| \leq \pi(M) + c'\frac{M^{2/3}}{\log^2 M}.$$

Toy example

- Let $\{1, \ldots, M\} \subset B.B$ and $N = \pi(M)$.
- Clearly
$$2 = p_1, p_2, \ldots, p_N \in B.B$$
- Define a 'reduced' p-adic valuation $\rho : [1, M] \to \mathbb{F}_3^N$ as
$$\rho(x)_i = \mathrm{ord}_{p_i}(x) \mod 3.$$
- In particular,
$$\begin{aligned} \rho(p_1) &= (1, 0, \ldots, 0); \\ \rho(p_2) &= (0, 1, \ldots, 0); \\ &\vdots \\ \rho(p_N) &= (0, 0, \ldots, 1); \end{aligned}$$

Toy example

- Let $\{1, \ldots, M\} \subset B.B$ and $N = \pi(M)$.
- Clearly
$$2 = p_1, p_2, \ldots, p_N \in B.B$$
- Define a 'reduced' p-adic valuation $\rho : [1, M] \to \mathbb{F}_3^N$ as
$$\rho(x)_i = \mathrm{ord}_{p_i}(x) \mod 3.$$
- In particular,
$$\begin{aligned}
\rho(p_1) &= (1, 0, \ldots, 0); \\
\rho(p_2) &= (0, 1, \ldots, 0); \\
&\vdots \\
\rho(p_N) &= (0, 0, \ldots, 1);
\end{aligned}$$

Toy example

- Let $\{1, \ldots, M\} \subset B.B$ and $N = \pi(M)$.
- Clearly
$$2 = p_1, p_2, \ldots, p_N \in B.B$$
- Define a 'reduced' p-adic valuation $\rho : [1, M] \to \mathbb{F}_3^N$ as
$$\rho(x)_i = \mathrm{ord}_{p_i}(x) \mod 3.$$
- In particular,
$$\begin{aligned} \rho(p_1) &= (1, 0, \ldots, 0); \\ \rho(p_2) &= (0, 1, \ldots, 0); \\ &\vdots \\ \rho(p_N) &= (0, 0, \ldots, 1); \end{aligned}$$

Toy example

- Let $\{1, \ldots, M\} \subset B.B$ and $N = \pi(M)$.
- Clearly
$$2 = p_1, p_2, \ldots, p_N \in B.B$$
- Define a 'reduced' p-adic valuation $\rho : [1, M] \to \mathbb{F}_3^N$ as
$$\rho(x)_i = \mathrm{ord}_{p_i}(x) \mod 3.$$
- In particular,
$$\begin{aligned} \rho(p_1) &= (1, 0, \ldots, 0); \\ \rho(p_2) &= (0, 1, \ldots, 0); \\ &\vdots \\ \rho(p_N) &= (0, 0, \ldots, 1); \end{aligned}$$

Toy example

We have $\{1, \ldots, M\} \subset B.B$ and thus

$$\rho(\{1, \ldots, M\}) \subseteq \rho(B) + \rho(B).$$

In particular,

$$\mathrm{Span}(\rho(\{1, \ldots, M\})) \subseteq \mathrm{Span}(\rho(B)).$$

But $\rho(p_1), \ldots, \rho(p_N)$ is a basis in $\mathbb{F}_3^N$ and thus

$$\pi(M) = N \leq |\rho(B)| \leq |B|.$$

Toy example

We have $\{1, \ldots, M\} \subset B.B$ and thus

$$\rho(\{1, \ldots, M\}) \subseteq \rho(B) + \rho(B).$$

In particular,

$$\mathrm{Span}(\rho(\{1, \ldots, M\})) \subseteq \mathrm{Span}(\rho(B)).$$

But $\rho(p_1), \ldots, \rho(p_N)$ is a basis in $\mathbb{F}_3^N$ and thus

$$\pi(M) = N \leq |\rho(B)| \leq |B|.$$

We can do better by considering elements in $[1, M]$ with a few prime factors.

Discrete spheres

Let S^l_k be the set of all $\{0,1\}$ vectors in $\mathbb{F}^l_3$ with exactly k non-zero coordinates. We will call S^l_k a *discrete sphere* of dimension l and weight k.

For example,

$$\{\rho(p_1), \ldots, \rho(p_N)\} = S^N_1,$$

and

$$\rho(\{p_i p_j p_k, i \neq j \neq k\}) = S^N_3.$$

We can do better by considering elements in $[1, M]$ with a few prime factors.

Discrete spheres

Let S_k^l be the set of all $\{0, 1\}$ vectors in $\mathbb{F}_3^l$ with exactly k non-zero coordinates. We will call S_k^l a *discrete sphere* of dimension l and weight k.

For example,

$$\{\rho(p_1), \dots, \rho(p_N)\} = S_1^N,$$

and

$$\rho(\{p_i p_j p_k, i \neq j \neq k\}) = S_3^N.$$

We can do better by considering elements in $[1, M]$ with a few prime factors.

Discrete spheres

Let S^l_k be the set of all $\{0, 1\}$ vectors in $\mathbb{F}^l_3$ with exactly k non-zero coordinates. We will call S^l_k a *discrete sphere* of dimension l and weight k.

For example,

$$\{\rho(p_1), \ldots, \rho(p_N)\} = S^N_1,$$

and

$$\rho(\{p_i p_j p_k, i \neq j \neq k\}) = S^N_3.$$

Now, define

$$\begin{aligned} P_1 &= \{p\}, \quad M^{1/3} < p \leq M, \\ P_2 &= \{\, p_i p_j p_k \,\}, \quad p_{i,j,k} \leq M^{1/3}, i \neq j \neq k \end{aligned}$$

so that

$$P_1, P_2 \subseteq \{1, \ldots, M\} \subseteq B.B.$$

Moreover,

$$\rho(P_1 \cup P_2) = S_1^{|P_1|} \oplus S_3^{\pi(M^{1/3})} \subseteq \rho(B) + \rho(B).$$

Now, define

$$\begin{aligned} P_1 &= \{p\}, \quad M^{1/3} < p \le M, \\ P_2 &= \{\, p_i p_j p_k \,\}, \quad p_{i,j,k} \le M^{1/3}, i \ne j \ne k \end{aligned}$$

so that

$$P_1, P_2 \subseteq \{1, \ldots, M\} \subseteq B.B.$$

Moreover,

$$\rho(P_1 \cup P_2) = S_1^{|P_1|} \oplus S_3^{\pi(M^{1/3})} \subseteq \rho(B) + \rho(B).$$

It is 'conceivable' to assume that

$$B = B_1 \bigsqcup B_2$$

such that

$$\begin{aligned} S_1^{|P_1|} &\subseteq \rho(B_1) + \rho(B_1). \\ S_3^{\pi(M^{1/3})} &\subseteq \rho(B_2) + \rho(B_2) \end{aligned}$$

Then (recall $N = \pi(M)$)

$$|B| = |B_1| + |B_2| \geq |P_1| + |B_2| = \pi(M) - \pi(M^{1/3}) + |B_2|.$$

Our aim is to prove that

$$|B_2| \gg \pi(M^{1/3})^2 \gg \frac{M^{2/3}}{\log^2 M}.$$

It is ‘conceivable’ to assume that

$$B = B_1 \bigsqcup B_2$$

such that

$$\begin{aligned} S_1^{|P_1|} &\subseteq \rho(B_1) + \rho(B_1). \\ S_3^{\pi(M^{1/3})} &\subseteq \rho(B_2) + \rho(B_2) \end{aligned}$$

Then (recall $N = \pi(M)$)

$$|B| = |B_1| + |B_2| \geq |P_1| + |B_2| = \pi(M) - \pi(M^{1/3}) + |B_2|.$$

Our aim is to prove that

$$|B_2| \gg \pi(M^{1/3})^2 \gg \frac{M^{2/3}}{\log^2 M}.$$

It is 'conceivable' to assume that

$$B = B_1 \bigsqcup B_2$$

such that

$$\begin{aligned} S_1^{|P_1|} &\subseteq \rho(B_1) + \rho(B_1). \\ S_3^{\pi(M^{1/3})} &\subseteq \rho(B_2) + \rho(B_2) \end{aligned}$$

Then (recall $N = \pi(M)$)

$$|B| = |B_1| + |B_2| \geq |P_1| + |B_2| = \pi(M) - \pi(M^{1/3}) + |B_2|.$$

Our aim is to prove that

$$|B_2| \gg \pi(M^{1/3})^2 \gg \frac{M^{2/3}}{\log^2 M}.$$

Lemma (Main Lemma)

Assume that $S_3^n \subseteq B + B$. Then

$$|B| \gg n^2.$$

Trivial bound:

$$|B| \gg |S_3^n|^{1/2} \gg n^{3/2}.$$

Obviously, the bound is tight: one can take

$$B = S_1^n \cup S_2^n.$$

Lemma (Main Lemma)

Assume that $S_3^n \subseteq B + B$. Then

$$|B| \gg n^2.$$

Trivial bound:

$$|B| \gg |S_3^n|^{1/2} \gg n^{3/2}.$$

Obviously, the bound is tight: one can take

$$B = S_1^n \cup S_2^n.$$

Lemma (Main Lemma)

Assume that $S_3^n \subseteq B + B$. Then

$$|B| \gg n^2.$$

Trivial bound:

$$|B| \gg |S_3^n|^{1/2} \gg n^{3/2}.$$

Obviously, the bound is tight: one can take

$$B = S_1^n \cup S_2^n.$$

Let B_1, B_2 be two disjoint copies of B.

- Build a bipartite graph H on (B_1, B_2) with (b_1, b_2) adjacent iff $b_1 + b_2 \in S_3$
- Start with the identity

$$\sum_{(v_1,v_2)\in B_1\times B_1} |N(v_1)\cap N(v_2)| = \sum_{w\in B_2} d^2(w). \qquad (1)$$

- If one could prove that (1) is at most n^4 then by C-S

$$|B|n^4 \geq |B_2| \sum_{w\in B_2} d^2(w) \geq \left(\sum_{w\in B_2} d_H(w)\right)^2 = E(H)^2 \gg n^6.$$

Therefore, $|B| \gg n^2$.

Let B_1, B_2 be two disjoint copies of B.

- Build a bipartite graph H on (B_1, B_2) with (b_1, b_2) adjacent iff $b_1 + b_2 \in S_3$
- Start with the identity

$$\sum_{(v_1,v_2)\in B_1\times B_1} |N(v_1)\cap N(v_2)| = \sum_{w\in B_2} d^2(w). \tag{1}$$

- If one could prove that (1) is at most n^4 then by C-S

$$|B|n^4 \geq |B_2| \sum_{w\in B_2} d^2(w) \geq \left(\sum_{w\in B_2} d_H(w)\right)^2 = E(H)^2 \gg n^6.$$

Therefore, $|B| \gg n^2$.

Let B_1, B_2 be two disjoint copies of B.

- Build a bipartite graph H on (B_1, B_2) with (b_1, b_2) adjacent iff $b_1 + b_2 \in S_3$
- Start with the identity

$$\sum_{(v_1,v_2)\in B_1\times B_1} |N(v_1)\cap N(v_2)| = \sum_{w\in B_2} d^2(w). \tag{1}$$

- If one could prove that (1) is at most n^4 then by C-S

$$|B|n^4 \geq |B_2| \sum_{w\in B_2} d^2(w) \geq \left(\sum_{w\in B_2} d_H(w)\right)^2 = E(H)^2 \gg n^6.$$

Therefore, $|B| \gg n^2$.

But unfortunately, the sum on the previous slide can be as large as n^5 :'(

Indeed, take

$$B = S_1^n \cup S_2^n.$$

Remedy: carefully excise some edges from the graph H such that for the resulting graph H' holds

- $$E(H') \gg n^3$$
- $$\sum_{(v_1,v_2)\in B_1\times B_1} |N_{H'}(v_1)\cap N_{H'}(v_2)| \ll n^4.$$

But unfortunately, the sum on the previous slide can be as large as n^5 :'(

Indeed, take

$$B = S_1^n \cup S_2^n.$$

Remedy: carefully excise some edges from the graph H such that for the resulting graph H' holds

- $$E(H') \gg n^3$$
- $$\sum_{(v_1,v_2)\in B_1\times B_1} |N_{H'}(v_1) \cap N_{H'}(v_2)| \ll n^4.$$

But unfortunately, the sum on the previous slide can be as large as n^5 :'(

Indeed, take

$$B = S_1^n \cup S_2^n.$$

Remedy: carefully excise some edges from the graph H such that for the resulting graph H' holds

- $$E(H') \gg n^3$$
- $$\sum_{(v_1,v_2)\in B_1\times B_1} |N_{H'}(v_1) \cap N_{H'}(v_2)| \ll n^4.$$

Crucial observation: ‘irreducibility’ of the 2-sphere

Assume that there existed a decomposition of a two-sphere

$$S_2^n = B_1 + B_2$$

with

$$|B_1| \approx n^{0.9} \quad |B_2| \approx n^{1.1}.$$

Then we could have taken

$$\begin{aligned} B_1' &= B_1 + S_1^n \\ B_2' &= B_2 \\ B &= B_1' \cup B_2'. \end{aligned}$$

Clearly, $|B| \leq n^{1.9}$ but

$$S_3^n \subseteq S_2^n + S_1^n \subseteq (B_1 + B_2) + S_1^n \subseteq B + B.$$

Crucial observation: 'irreducibility' of the 2-sphere

Assume that there existed a decomposition of a two-sphere

$$S_2^n = B_1 + B_2$$

with

$$|B_1| \approx n^{0.9} \quad |B_2| \approx n^{1.1}.$$

Then we could have taken

$$\begin{aligned} B_1' &= B_1 + S_1^n \\ B_2' &= B_2 \\ B &= B_1' \cup B_2'. \end{aligned}$$

Clearly, $|B| \le n^{1.9}$ but

$$S_3^n \subseteq S_2^n + S_1^n \subseteq (B_1 + B_2) + S_1^n \subseteq B + B.$$

References

D. Zhelezov, *Discrete spheres and APs in product sets*, arXiv:1510.05411.