Recognizing groups in Erdős geometry and model theory

Artem Chernikov

UMD/UCLA

Mathematics Münster Mid-term Conference

25 March 2024, Münster, Germany

History: arithmetic and geometric progressions

Given two sets A, B in a field K, we define

- their *sumset* $A + B = \{a + b : a \in A, b \in B\}$,
- their *productset* $A \cdot B = \{a \cdot b : a \in A, b \in B\}$.

Example

Let $A_n := \{1, 2, \ldots, n\}$.

- $|A_n + A_n| = 2\,|A_n| - 1 = O\left(|A_n|\right)$.
- Let $\pi(n)$ be the number of primes in A_n. As the product of any two primes is unique up to permutation, by the Prime Number Theorem we have $|A_n \cdot A_n| \geq \frac{1}{2}\pi(n)^2 = \Omega\left(|A_n|^{2-o(1)}\right)$.

History: sum-product phenomenon

- This generalizes to arbitrary arithmetic progressions: their sumsets are as small as possible, and productsets are as large as possible.
- For a geometric progression, the opposite holds: productset is as small as possible, sumset is as large as possible.
- These are the two extreme cases of the following result.
- [Erdős, Szemerédi] There exists some $c \in \mathbb{R}_{>0}$ such that: for every finite $A \subseteq \mathbb{R}$,

$$\max\{|A+A|, |A \cdot A|\} = \Omega\left(|A|^{1+c}\right).$$

- Conjecture (widely open): holds with exponent $2 - \varepsilon$ for any $\varepsilon > 0$.

Elekes: generalization to polynomial expansion

- Since polynomials combine addition and multiplication, a "typical" polynomial $f \in \mathbb{R}[x, y]$ should satisfy

$$|f(A \times B)| = \Omega\left(n^{1+c}\right)$$

  for some $c = c(f)$ and all finite $A, B \subseteq \mathbb{R}$ with $|A| = |B| = n$.
- Doesn't hold when only one of the operations occurs between the two variables:
  - f is *additive*, i.e. $f(x, y) = g(h(x) + i(y))$ for some univariate polynomials g, h, i
    (as then $|f(A \times B)| = O(n)$ for A, B such that $h(A), i(B)$ are arithmetic progressions).
  - f is *multiplicative*, i.e. $f(x, y) = g(h(x) \cdot i(y))$ for some univariate polynomials g, h, i
    (as then $|f(A \times B)| = O(n)$ for A, B such that $h(A), i(B)$ are geometric progressions).

Elekes-Rónyai

- But these are the only exceptions!
- [Elekes, Rónyai] Let $f \in \mathbb{R}[x, y]$ be a polynomial of degree d that is not additive or multiplicative. Then for all $A, B \subseteq \mathbb{R}$ with $|A| = |B| = n$ one has

$$|f(A \times B)| = \Omega_d\left(n^{\frac{4}{3}}\right).$$

- The improved bound and the independence of the exponent from the degree of f is due to [Raz, Sharir, Solymosi].
- Analogous results hold with $\mathbb{C}$ instead of $\mathbb{R}$ (and slightly worse bounds).
- The exceptional role played by the additive and multiplicative forms suggests that (algebraic) groups play a special role — made precise by [Elekes, Szabó].

Elekes-Szabó theorem

- [Elekes-Szabó'12] provide a conceptual generalization: for any algebraic surface $R(x_1, x_2, x_3) \subseteq \mathbb{R}^3$ so that the projection onto any two coordinates is finite-to-one, exactly one of the following holds:
  1. (power saving) there exists $\gamma > 0$ s.t. for any finite $A_i \subseteq_n \mathbb{R}$ we have
  $$|R \cap (A_1 \times A_2 \times A_3)| = O(n^{2-\gamma}).$$
  2. (locally equivalent to a group) There exist open sets $U_i \subseteq \mathbb{R}$ and $V \subseteq \mathbb{R}$ containing 0, and analytic bijections with analytic inverses $\pi_i : U_i \to V$ such that
  $$\pi_1(x_1) + \pi_2(x_2) + \pi_3(x_3) = 0 \Leftrightarrow R(x_1, x_2, x_3)$$
  for all $x_i \in U_i$.
- Alternative regime: working over $\mathbb{C}$, for R irreducible get that it is in coordinate-wise finite-to-finite algebraic correspondence with the graph of addition on a 1-dimensional algebraic group.
- If $f(x_1, x_2, x_3) = x_3 - x_1 - x_2$, arithmetic progressions witness no power saving.

Generalizations of the Elekes-Szabó theorem

Let $R \subseteq X_1 \times \ldots \times X_r$ be a (semi-)algebraic variety with finite-to-one projection onto any $r-1$ coordinates, $\dim(X_i) = m$.

1. [Elekes, Szabó'12] $r = 3$, any m (grids in *general position*, correspondence with a complex algebraic group of dim $= m$);
2. [Raz, Sharir, de Zeeuw'18] $r = 4$, $m = 1$;
3. [Raz, Shem-Tov'18] $m = 1$, R of the form $f(x_1, ..., x_{r-1}) = x_r$;
4. [Hrushovski'13] Pseudofinite dimension, connection to *modularity* of certain matroids;
5. Related work: [Raz, Sharir, de Zeeuw'15], [Wang'15]; [Bukh, Tsimmerman' 12], [Tao'12]; [Jing, Roy, Tran'19];
6. [Bays, Breuillard'18] any r and m, any co-dim over $\mathbb{C}$, recognized that groups are abelian — but no bounds on γ;
7. [C., Peterzil, Starchenko'21] Any r and m, any R definable in an *o-minimal structure* and explicit bounds on γ.
8. [Bays, Dobrowolski, Zou'21] Relaxing general position/abelianity to nilpotence in special cases.
9. [C., Peterzil, Starchenko'24] Any r, m, any co-dim, bounds.

One-dimensional semi-algebraic case

Theorem (C., Peterzil, Starchenko)

Assume $r \geq 3$, $R \subseteq \mathbb{R}^r$ is semi-algebraic, such that the projection of R to any $r-1$ coordinates is (generically) finite-to-one. Then exactly one of the following holds.

1. *For any finite $A_i \subseteq_n \mathbb{R}$, $i \in [r]$, we have*

$$|R \cap (A_1 \times \ldots \times A_r)| = O_R\left(n^{r-1-\gamma}\right),$$

   where $\gamma = \frac{1}{3}$ if $r \geq 4$, and $\gamma = \frac{1}{6}$ if $r = 3$.

2. *There exist open sets $U_i \subseteq \mathbb{R}, i \in [r]$, an open set $V \subseteq \mathbb{R}$ containing 0, and homeomorphisms $\pi_i : U_i \to V$ such that*

$$\pi_1(x_1) + \cdots + \pi_r(x_r) = 0 \Leftrightarrow R(x_1, \ldots, x_r)$$

   for all $x_i \in U_i, i \in [r]$.

Grids in general position

- When $R \subseteq X_1 \times \ldots \times X_r$ with $\dim(X_i) = m > 1$, it is necessary to restrict to grids in *general position*.
- A set $A \subseteq X_i$ is in (D, ν)*-general position* if $|A \cap Y| \leq \nu$ for every algebraic subset $Y \subseteq X$ with dimension $< m$ and degree $\leq D$.
- A grid $A = A_1 \times \ldots \times A_r$ is in (D, ν)*-general position* if each $A_i \subseteq X_i$ is in (D, ν)*-general position*.
- Example: if $m = 1$ and D is fixed, then for ν large enough every set $A \subseteq \mathbb{C}$ is in (D, ν)-general position.

General semi-algebraic case

Theorem (C., Peterzil, Starchenko)

Assume $r \geq 3$, $R \subseteq X_1 \times \cdots \times X_r$ are semi-algebraic with $\mathbf{dim}\,(\boldsymbol{X_i}) = \boldsymbol{m}$, *and the projection of R to any $r-1$ coordinates is finite-to-one. Then one of the following holds.*

1. *There exists $D = D(R)$ such that for any ν and any finite $A_i \subseteq_n X_i$* ***in*** (D, ν)***-general position****, $i \in [r]$, we have*

$$|R \cap (A_1 \times \ldots \times A_r)| = O_{R,\nu}\left(n^{r-1-\gamma}\right),$$

   for $\gamma = \frac{1}{8m-5}$ if $s \geq 4$, and $\gamma = \frac{1}{16m-10}$ if $s = 3$.

2. *There exist semialgebraic relatively open sets $U_i \subseteq X_i$, $i \in [s]$,* ***an abelian Lie group*** $(G, +)$ ***of dimension*** *m and an open neighborhood $V \subseteq G$ of 0, and semi-algebraic homeomorphisms $\pi_i : U_i \to V$, $i \in [s]$, such that for all $x_i \in U_i, i \in [s]$*

$$\pi_1(x_1) + \cdots + \pi_s(x_s) = 0 \Leftrightarrow R(x_1, \ldots, x_s).$$

Remarks

1. In fact, our theorem is for R definable in an arbitrary o-minimal expansion of $\mathbb{R}$ — so R can be defined not only using polynomial (in-)equalities, but also e.g. using e^x and restricted analytic functions. Recently generalized to arbitrary co-dimension (this is codim 1 case).
2. We also have an analog over algebraically closed fields of characteristic 0 (here we get a finite-to-finite correspondence with an algebraic group), and more generally for differentially closed fields, etc.
3. One ingredient — improved Szemeredi-Trotter style incidence bounds in o-minimal structures ([Basu, Raz], [C., Galvin, Starchenko]).
4. Another – a higher arity generalization of the (abelian) Group Configuration theorem of Zilber and Hrushovski on recognizing groups from a "generic chunk" (and more generally — local version of the coordinatization of projective geometries). We discuss a simple purely combinatorial special case:

First ingredient: Recognizing groups, 1

1. Assume that $(G, +, 0)$ is an abelian group, and consider the r-ary relation $R \subseteq \prod_{i \in [r]} G$ given by $x_1 + \ldots + x_r = 0$.
2. Then R is easily seen to satisfy the following two properties, for any permutation of the variables of R:

$$\forall x_1, \ldots, \forall x_{r-1} \exists! x_r R(x_1, \ldots, x_r), \tag{P1}$$

$$\forall x_1, x_2 \forall y_3, \ldots y_r \forall y_3', \ldots, y_r' \Big(R(\bar{x}, \bar{y}) \wedge R(\bar{x}, \bar{y}') \rightarrow \tag{P2}$$

$$\big(\forall x_1', x_2' R(\bar{x}', \bar{y}) \leftrightarrow R(\bar{x}', \bar{y}')\big)\Big).$$

We show a converse, assuming $r \geq 4$:

Recognizing groups, 2

Theorem (C., Peterzil, Starchenko)

Assume $r \in \mathbb{N}_{\geq 4}$, $X_1, \ldots, X_r$ and $R \subseteq \prod_{i \in [r]} X_i$ are sets, so that R satisfies (P1) and (P2) for any permutation of the variables. Then there exists an abelian group $(G, +, 0_G)$ and bijections $\pi_i : X_i \to G$ such that for every $(a_1, \ldots, a_r) \in \prod_{i \in [r]} X_i$ we have

$$R(a_1, \ldots, a_r) \iff \pi_1(a_1) + \ldots + \pi_r(a_r) = 0_G.$$

- If $X_1 = \ldots = X_r$, property (P1) is equivalent to saying that the relation R is an $(r-1)$-*dimensional permutation* on the set X_1, or a *Latin* $(r-1)$-*hypercube*, as studied by Linial and Luria. Thus the condition (P2) characterizes, for $r \geq 3$, those Latin r-hypercubes that are given by the relation "$x_1 + \ldots + x_{r-1} = x_r$" in an abelian group.
- If R is semi-algebraic and X_i are semi-algebraic, then G and π_i can be chosen semi-algebraic as well.

Some remarks

- For $r = 4$, and fixed a_3, a_4, $R(x_1, x_2, a_3, a_4)$ is the graph of a bijection $f_{a_3,a_4} : X_1 \to X_2$ by (P1).
- Let $\mathcal{F} := \{f_{a_3,a_4} : (a_3, a_4) \in X_3 \times X_4\}$.
- Fix any $f_0 \in \mathcal{F}$. For $f, f' \in \mathcal{F}$, let $f + f' := f \circ f_0^{-1} \circ f'$.
- Then one shows $(\mathcal{F}, +)$ is an abelian group with identity f_0 using (P2) for various permutations of the coordinates.
- In the general case, have to work with only generically defined finite-to-finite correspondences (in *o*-minimal — on infinitesimal neighborhoods in some non-standard extension of $\mathbb{R}$), and the group is built on their germs.

Counting edges in bipartite graphs

- Let $G = (A, B, I)$ with $I \subseteq A \times B$ be a bipartite graph.
- For $k \in \mathbb{N}$, let $K_{k,k}$ be the complete bipartite graph with each part of size k. Cauchy-Schwarz gives you:

Fact

[Kővári, Sós, Turán, '54] For each $k \in \mathbb{N}$ there is some $c \in \mathbb{R}$ such that: for any bipartite graph G and $A \subseteq U, B \subseteq V$ with $|A| = |B| = n$, if $I(A, B)$ is $K_{k,k}$-free, then $|I(A, B)| \leq cn^{2-\frac{1}{k}}$.

- So if G is $K_{2,2}$-free, then $|I(A, B)| = O(n^{\frac{3}{2}})$.
- Optimal up to a constant! Witnessed by the point–line incidence graph on the affine plane over $\mathbb{F}_{p^n}$ as $n \to \infty$.

Example: point-line incidences on the plane

- Let $I \subseteq \mathbb{R}^2 \times \mathbb{R}^2$ be the incidence relation between points and lines on the real plane, i.e.

$$I(x_1, x_2; y_1, y_2) \iff x_2 = y_1 x_1 + y_2.$$

- Then I is semialgebraic and $K_{2,2}$-free (for any two points belong to at most one line, and vice versa).
- Utilizing the geometry of the reals (cell decomposition / polynomial method):

Fact (Szémeredi-Trotter '83)

For A a set of n points and B a set of n-lines, $|I(A, B)| = O\left(n^{\frac{4}{3}}\right)$.

- Importantly: $\frac{4}{3} < \frac{3}{2}$.

Second ingredient: better "incidence bounds" in *o*-minimal structures

- Szémeredi-Trotter theorem has numerous generalizations for semialgebraic graphs, e.g. [Pach, Sharir'98], [Elekes, Szabó'12], [Fox, Pach, Sheffer, Suk, Zahl '15], and to *o*-minimal structures:

Theorem (C., Galvin, Starchenko'16)

If $I \subseteq U \times V$ is a binary relation definable in a distal structure $\mathcal{M}$ (includes o-minimal structures, but also e.g. $\mathbb{Q}_p$) and E is $K_{2,2}$-free, then there is some $\delta > 0$ such that: for all $A \subseteq_n U, B \subseteq_n V$ we have $|I \cap A \times B| = O(n^{\frac{3}{2}-\delta})$.

- The power saving γ in the main theorem can be estimated explicitly in terms of this δ.
- Explicit bounds on δ are known in some special cases: for $E \subseteq M^2 \times M^2$ for an *o*-minimal $\mathcal{M}$, also $O(n^{\frac{4}{3}})$ ([C., Galvin, Starchenko'16] or [Basu, Raz'16]) — optimal.

Recognizing fields

- For the semialgebraic $K_{2,2}$-free point-line incidence relation $R = \{(x_1, x_2; y_1, y_2) \in \mathbb{R}^4 : x_2 = y_1 x_1 + y_2\} \subseteq \mathbb{R}^2 \times \mathbb{R}^2$ we have the (optimal) lower bound $|R \cap (V_1 \times V_2)| = \Omega(n^{\frac{4}{3}})$.
- To define it we use both addition and multiplication, i.e. the field structure.
- This is not a coincidence — any non-trivial lower bound on the exponent of R allows to recover a field from it:

Theorem (joint with A. Basit, S. Starchenko, T. Tao, C. Tran)

Assume that $\mathcal{M} = (M, <, \ldots)$ is o-minimal and $R \subseteq M_{d_1} \times \ldots \times M_{d_r}$ is a definable relation which is $K_{k,\ldots,k}$-free, but $|R \cap \prod_{i \in [r]} V_i| \neq O(n^{r-1})$ for $V_i \subseteq_n M_{x_i}$. Then a real closed field is definable in the first-order structure $(M, <, R)$.

Ingredients

- Optimal Zarankiewicz bound for *semilinear* hypergraphs:

Theorem (BCSTT)

For any integers $r \geq 2, s \geq 0, k \geq 2$ *there are* $\alpha = \alpha(r,s,k) \in \mathbb{R}$ *and* $\beta = \beta(r,s) \in \mathbb{N}$ *such that: for any finite* $K_{k,\ldots,k}$*-free semilinear* r*-hypergraph* $H = (V_1, \ldots, V_r; E)$ *with* $E \subseteq \prod_{i \in [r]} V_i$ *of complexity* $\leq s$ *we have*

$$|E| \leq \alpha n^{r-1} (\log n)^{\beta}.$$

- In particular, $|E| = O(n^{1+\varepsilon})$ for $r = 2$ and any $\varepsilon > 0$.
- The trichotomy theorem for *o*-minimal structures from model theory [Peterzil, Starchenko'98]: any non-trivial matroid defined by algebraic closure in an *o*-minimal structure is either locally modular (behaves like span in a vector space), or a real closed field can be defined.
  In a very special case: let $X \subseteq \mathbb{R}^n$ be a semialgebraic but not semilinear set. Then $\cdot \restriction_{[0,1]^2}$ is definable in $(\mathbb{R}, <, +, X)$.

Thank you!

- György Elekes and Endre Szabó, "How to find groups? (and how to use them in Erdös geometry?)", Combinatorica (2012)
- Artem Chernikov, Kobi Peterzil and Sergei Starchenko, "Model-theoretic Elekes-Szabó for stable and o-minimal hypergraphs", Duke Mathematical Journal, to appear
- Artem Chernikov, Sergei Starchenko, "Model-theoretic Elekes-Szabó in the strongly minimal case", Journal of Mathematical Logic (2021)
- A. Basit, A. Chernikov, S. Starchenko, T. Tao, C. Tran, "Zarankiewicz's problem for semilinear hypergraphs", Forum of Mathematics, Sigma (2021)
- Martin Bays and Emmanuel Breuillard, "Projective geometries arising from Elekes-Szabó problems", Ann. Sci. Ec. Norm. Supér. (2021),