Recognizing groups in model theory and Erdős geometry

Artem Chernikov
(joint with Y.Peterzil and S. Starchenko)

UCLA

MSRI Model Theory Seminar

"Berkeley", Oct 19, 2020

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

- $|A_n + A_n| = 2|A_n| - 1 = O(|A_n|)$.
- 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 $A \subseteq \mathbb{R}$,

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

- They conjecture: holds with $1 + c = 2 - \varepsilon$ for any $\varepsilon > 0$.
- [Solymosi], [Konyagin, Shkredov] Holds with $1 + c = \frac{4}{3} + \varepsilon$ for some sufficiently small $\varepsilon > 0$.

Elekes: generalization to polynomials

- 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 in this type of theorems — made precise by [Elekes, Szabó].

Definable hypergraphs

- We fix a structure $\mathcal{M}$, definable sets $X_1, \ldots, X_s$, and a definable relation $Q \subseteq \bar{X} = X_1 \times \ldots \times X_s$.
- E.g. $\mathcal{M} = (\mathbb{C}, +, \times)$ and $Q, X_i \subseteq \mathbb{C}^{d_i}$ are constructible sets; or $\mathcal{M} = (\mathbb{R}, +, \times)$ and $Q, X_i \subseteq \mathbb{R}^{d_i}$ are semi-algebraic sets.
- Write $A_i \subseteq_n X_i$ if $A_i \subseteq X_i$ with $|A_i| \leq n$.
- By a *grid on* $\bar{X}$ we mean a set $\bar{A} \subseteq \bar{X}$ with $\bar{A} = A_1 \times \ldots \times A_s$ and $A_i \subseteq X_i$.
- By an *n-grid on* $\bar{X}$ we mean a grid $\bar{A} = A_1 \times \ldots \times A_s$ with $A_i \subseteq_n X_i$.

Fiber-algebraic relations

- A relation $Q \subseteq \bar{X}$ is *fiber-algebraic* if there is some $d \in \mathbb{N}$ such that for any $1 \leq i \leq s$ we have

$$\mathcal{M} \models \forall x_1 \ldots x_{i-1} x_{i+1} \ldots x_s \exists^{\leq d} x_i \, Q\left(x_1, \ldots, x_s\right).$$

- E.g. if $Q \subseteq X_1 \times X_2 \times X_3$ is fiber-algebraic, then for any $A_i \subseteq_n X_i$ we have $|Q \cap A_1 \times A_2 \times A_3| \leq dn^2$.
- Conversely, let a fiber-algebraic $Q \subseteq \mathbb{C}^3$ be given by $x_1 + x_2 - x_3 = 0$, and let $A_1 = A_2 = A_3 = \{0, \ldots, n-1\}$. Then

$$|Q \cap A_1 \times A_2 \times A_3| = \frac{n\left(n+1\right)}{2} = \Omega\left(n^2\right).$$

- This indicates that the upper and lower bounds match for the graph of addition in an abelian group (up to a constant) — and the Elekes-Szabó principle suggests that in many situations this is the only possibility.

Grids in general position

- We assume $\mathcal{M}$ is equipped with an integer-valued dimension dim on definable sets. E.g. Zariski dimension on algebraic subsets of $\mathbb{C}^d$, or topological dimension on semialgebraic subsets of $\mathbb{R}^d$.
- Let X be $\mathcal{M}$-definable and $\mathcal{F}$ a (uniformly) $\mathcal{M}$-definable family of subset of X. For $\ell \in \mathbb{N}$, a set $A \subseteq X$ is *in $(\mathcal{F}, \ell)$-general position* if $|A \cap F| \leq \ell$ for every $F \in \mathcal{F}$ with $\dim(F) < \dim(X)$.
- Let X_i, $i = 1, \ldots, s$, be $\mathcal{M}$-definable sets and $\bar{\mathcal{F}} = (\mathcal{F}_1, \ldots, \mathcal{F}_s)$, where $\mathcal{F}_i$ is a definable family of subsets of X_i. A grid $\bar{A}$ on $\bar{X}$ is in $(\bar{\mathcal{F}}, \ell)$-*general position* if each A_i is in $(\mathcal{F}_i, \ell)$-general position.

General position: an example

- E.g. if X is strongly minimal and $\mathcal{F}$ is any definable family of subsets of X, then for any large enough $\ell = \ell(\mathcal{F}) \in \mathbb{N}$, every $A \subseteq X$ is in $(\mathcal{F}, \ell)$-general position.
- On the other hand, let $X = \mathbb{C}^2$ and let $\mathcal{F}_d$ be the family of all algebraic curves of degree d. If $\ell < d$, then any set $A \subseteq X$ is not in $(\mathcal{F}_d, \ell)$-general position.

Generic correspondence with group multiplication

- Let $Q \subseteq \bar{X}$ be a definable relation and $(G, \cdot)$ a type-definable group in $\mathbb{M}^{\mathrm{eq}}$ which is connected (i.e. $G = G^0$).
- We say that Q is in a *generic correspondence with multiplication in* G if there exist elements $g_1, \ldots, g_s \in G(\mathbb{M})$, where $\mathbb{M}$ is a saturated elementary extension of $\mathcal{M}$, such that:
  1. $g_1 \cdot \ldots \cdot g_s = 1_G$;
  2. $g_1, \ldots, g_{s-1}$ are independent generics in G over $\mathcal{M}$, i.e. each g_i doesn't belong to any definable set of dimension smaller than G definable over $\mathcal{M} \cup \{g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_{s-1}\}$;
  3. For each $i = 1, \ldots, s$ there is a generic element $a_i \in X_i$ interalgebraic with g_i over $\mathcal{M}$, such that $\models Q(a_1, \ldots, a_s)$.
- If X_i are irreducible (i.e. can't be split into two definable sets of the same dimension), then (3) holds for all $g_1, \ldots, g_s \in G$ satisfying (1) and (2), providing a generic finite-to-finite correspondence between Q and the graph of $(s-1)$-fold multiplication in G.

The Elekes-Szabó principle

Let $X_1, \ldots, X_s$ be irreducible definable sets in $\mathcal{M}$ with $\dim(X_i) = k$. We say that $\bar{X}$ satisfies the *Elekes-Szabó principle* if for any irreducible fiber-algebraic definable relation $Q \subseteq \bar{X}$, one of the following holds.

1. *Q admits power saving*: there exist some $\varepsilon \in \mathbb{R}_{>0}$ and some definable families $\mathcal{F}_i$ on X_i such that: for any $\ell \in \mathbb{N}$ and any n-grid $\bar{A} \subseteq \bar{X}$ in $(\bar{\mathcal{F}}, \ell)$-general position, we have

$$|Q \cap \bar{A}| = O_\ell\left(n^{(s-1)-\varepsilon}\right).$$

2. Q is in a generic correspondence with multiplication in a type-definable *abelian* group of dimension k.

Known cases of the Elekes-Szabó principle

1. [Elekes, Szabó'12] $\mathcal{M} \models \mathrm{ACF}_0$, $s = 3$, k arbitrary;
2. [Raz, Sharir, de Zeeuw'18] $\mathcal{M} \models \mathrm{ACF}_0$, $s = 4$, $k = 1$;
3. [Bays, Breuillard'18] $\mathcal{M} \models \mathrm{ACF}_0$, s and k arbitrary, recognized that the arising groups are abelian (they work with a more relaxed notion of general position and arbitrary codimension, however no bounds on ε);
4. [C., Starchenko'18] $\mathcal{M}$ is any strongly minimal structure interpretable in a *distal* structure, $s = 3$, $k = 1$.

Related work: [Raz, Sharir, de Zeeuw'15], [Wang'15]; [Bukh, Tsimmerman' 12], [Tao'12]; [Hrushovski'13]; [Raz, Shem-Tov'18]; [Jing, Roy, Tran'19].

Main theorem

Theorem

The Elekes-Szabó principle holds in the following two cases:

1. *$\mathcal{M}$ is a stable structure interpretable in a distal structure, with respect to $\mathfrak{p}$-dimension.*
2. *$\mathcal{M}$ is an o-minimal structure, with respect to the usual dimension (in this case, on a type-definable generic subset of $\bar{X}$, we get a definable coordinate-wise bijection of Q with the graph of multiplication of G).*

- Moreover, the bound on the power saving exponent ε is explicit.

The *o*-minimal case, over the reals

- The main difference between stable and *o*-minimal cases is that in the stable case "generically" means "almost everywhere", and in the *o*-minimal case it means "on some open definable set" (that may be very small).
- Assume $\mathcal{M} = (\mathbb{R}, <, \ldots)$ is *o*-minimal, with $\mathbb{R}$ the field of real numbers.
- Then, using the theory of *o*-minimal groups, in the group case of the Main Theorem the conclusion can be made more explicit as follows:
- there is an abelian Lie group G of dimension k, an open neighborhood of identity $U \subseteq G$, for each $i = 1, \ldots, s$ open definable $V_i \subseteq X_i$ and definable homeomorphisms $\pi_i \colon V_i \to U$ such that for all $x_i \in V_i$ we have

$$Q(x_1, \ldots x_s) \Longleftrightarrow \pi_1(x_1) \cdot \ldots \cdot \pi_s(x_s) = e.$$

- In particular, this answers a question of Elekes-Szabó.

Main theorem: stable case

- We choose a saturated elementary extension $\mathbb{M}$ of a *stable* structure $\mathcal{M}$.
- By *a* $\mathfrak{p}$*-pair* we mean a pair $(X, \mathfrak{p}_X)$, where X is an $\mathcal{M}$-definable set and $\mathfrak{p}_X \in S(\mathcal{M})$ is a complete stationary type on X.
- Assume we are given $\mathfrak{p}$-pairs $(X_i, \mathfrak{p}_i)$ for $1 \leq i \leq s$. We say that a definable $Y \subseteq X_1 \times \ldots \times X_s$ is $\mathfrak{p}$-generic if $Y \in \mathfrak{p}_1 \otimes \ldots \otimes \mathfrak{p}_s|_{\mathbb{M}}$.
- Finally, we define the $\mathfrak{p}$-*dimension* via $\dim_{\mathfrak{p}}(Y) \geq k$ if for some projection π of $\bar{X}$ onto k components, $\pi(Y)$ is $\mathfrak{p}$-generic.
- $\mathfrak{p}$-dimension enjoys definability/additivity properties that may fail for Morley rank in general ω-stable theories (e.g. DCF_0).
- However, if X is a definable subset of finite Morley rank k and degree one, taking $\mathfrak{p}_X$ to be the unique type on X of Morley rank k, we have that $k \cdot \dim_{\mathfrak{p}} = \mathrm{MR}$, and the Main Theorem implies that the Elekes-Szabó principle holds with respect to Morley rank in this case.

Distality and abstract incidence bounds, 1

- Distality is used to obtain the following abstract "Szemerédi-Trotter" theorem for relations definable in distal structures, generalizing several results in the literature.

Theorem (C., Galvin, Starchenko'16)

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

- The power saving ε in the main theorem can be estimated explicitly in terms of this δ, and δ — in terms of the size of a *distal cell decomposition* for E.
- Explicit bounds on δ and/or distal cell decompositions are known in some special cases:

Distality and abstract incidence bounds, 2

- [Szemerédi-Trotter'83] $O(n^{\frac{4}{3}})$ for E the point-line incidence relation in $\mathbb{R}^2$.
- Bounds for (semi-)algebraic $R \subseteq M^{d_1} \times M^{d_2}$ with $\mathcal{M} = \mathbb{R}$ [Fox, Pach, Sheffer, Suk, Zahl'15], $\ldots$.
- 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; for $E \subseteq M^{d_1} \times M^{d_2}$ [Anderson'20+].
- For $E \subseteq M^{d_1} \times M^{d_2}$ with $\mathcal{M}$ locally modular o-minimal, $O_\gamma(n^{1+\gamma})$ for an arbitrary $\gamma > 0$ [Basit, C., Starchenko, Tao, Tran'20].
- $\mathrm{ACF}_0, \mathrm{DCF}_0, \mathrm{CCM}$ — stable with distal expansions (but no explicit bounds are known for the latter two).

Recovering groups from abelian s-gons

- Let $\mathcal{M}$ be stable (the *o*-minimal case is analogous, but easier).
- An *s-gon* over A is a tuple $a_1, \ldots, a_s$ such that any $s-1$ of its elements are independent over A, and any element in it is in the algebraic closure of the other ones and A.
- We say that an s-gon is *abelian* if, after any permutation of its elements, we have $a_1 a_2 \mathop{\smile\!\!\!\!\!\!|}_{\mathrm{acl}_A(a_1 a_2) \cap \mathrm{acl}_A(a_3 \ldots a_s)} a_3 \ldots a_s$.
- If $(G, \cdot)$ is a type-definable abelian group, $g_1, \ldots, g_{s-1}$ are independent generics in G and $g_s := g_1 \cdot \ldots \cdot g_{s-1}$, then $g_1, \ldots, g_s$ is an abelian s-gon (associated to G).
- Conversely,

Theorem

Let $s \geq 4$ and $a_1, \ldots, a_s$ be an abelian s-gon. Then there is a type-definable (in $\mathcal{M}^{\mathrm{eq}}$) connected abelian group $(G, \cdot)$ and an abelian s-gon $g_1, \ldots, g_s$ associated to G, such that after a base change each g_i is interalgebraic with a_i.

Distinction of cases in the Main Theorem, 1

- Assume $s \geq 4$ (the case $s = 3$ is reduced to $s = 4$ by a separate argument).
- We may assume $\dim(Q) = s - 1$, and let $\bar{a} = (a_1, \ldots, a_s)$ in $\mathbb{M}$ be a generic tuple in Q over $\mathcal{M}$.
- As Q is fiber-algebraic, $\bar{a}$ is an s-gon over $\mathcal{M}$.

Theorem

One of the following is true:

1. *For $u = (a_1, a_2)$ and $v = (a_3, \ldots, a_s)$ we have $u \mathop{\smile\!\!\!\!\!\!|}_{\mathrm{acl}_M(u) \cap \mathrm{acl}_M(v)} v$.*
2. *Q, as a relation on $U \times V$, for $U = X_1 \times X_2$ and $V = X_3 \times \ldots \times X_s$, is a "pseudo-plane".*

Distinction of cases in the Main Theorem, 2

- In case (2) the incidence bound for distal relations can be applied inductively to obtain power saving $O(n^{(s-1)-\varepsilon})$ for Q.
- Thus we may assume that that for any permutation of $\{1, \ldots, s\}$ we have

$$a_1 a_2 \mathop{\smile\!\!\!\!\!\!|}_{\mathrm{acl}_M(a_1 a_2) \cap \mathrm{acl}_M(a_3 \ldots a_s)} a_3 \ldots a_s,$$

  i.e. the s-gon $\bar{a}$ is abelian.
- Hence the previous theorem can be applied to establish generic correspondence with a type-definable abelian group.

Thank you!