Coarse approximate subgroups in weak general position and Elekes-Szabó problems for nilpotent groups

Tingxiang Zou
joint work with Martin Bays and Jan Dobrowolski

1 Motivation

1.1 The Elekes-Szabó problem

• Let $V \subseteq \mathbb{C}^n$ be an irreducible algebraic variety over $\mathbb{C}$. Let $N \in \mathbb{N}$ and $X_i \subseteq \mathbb{C}$ with $|X_i| \leq N$ for $1 \leq i \leq n$. Then

$$|V \cap \prod_{1\leq i\leq n} X_i| \leq O_V(N^{\dim(V)}).$$

• Say V admits no power-saving if the exponent $\dim(V)$ is optimal, i.e. there is no $\epsilon > 0$ such that $|V \cap \prod_{1\leq i\leq n} X_i| \leq O_{V,\epsilon}(N^{\dim(V)-\epsilon})$ for all N and $X_i \subseteq \mathbb{C}$ with $|X_i| \leq N$.

• Simplest non-trivial case: $n = 3$ and $\dim(V) = 2$, what are those V which admit no power-saving?

Example: The graph $\Gamma_+ \subseteq \mathbb{C}^3$ of addition in $(\mathbb{C}, +, 0)$ has no power-saving: $X_N := [-N/2, N/2] \cap \mathbb{Z}$, then $|\Gamma_+ \cap (X_N)^3| \geq N^2/2$.

• For irreducible varieties $V \subseteq \prod_{i\leq n} W_i$ and $V' \subseteq \prod_{i\leq n} W'_i$, we say V is in co-ordinatewise correspondence with V' if the generics $(a_1, \ldots, a_n) \in V$ and $(a'_1, \ldots, a'_n) \in V'$ are co-ordinatewise interalgebraic with each other.

> **Elekes-Szabó (2012): How to find groups? (and how to use them in Erdős geometry?)**
> Let $V \subseteq \mathbb{C}^3$ be an irreducible surface (i.e. $\dim(V) = 2$) admitting no power-saving. Then V either projects to some curve, i.e. $\dim(\pi_{ij}(V)) = 1$ for some $i \neq j \in \{1, 2, 3\}$, or is in co-ordinatewise correspondence with the graph $\Gamma_+ := \{(g, h, g + h) : g, h \in G\} \subseteq G^3$ of multiplication for some one-dimensional complex algebraic group G.

Philosophy: "whenever we find a lot of unexpected coincidences, then somewhere in the background there lurks a large group of symmetries."

Non-standard set-up:

- Work in $\mathbb{K} := \mathbb{C}^{\mathcal{U}}$ for some non-principal ultrafilter $\mathcal{U}$ and in a language $\mathcal{L}$ expanding $\mathcal{L}_{ring}$.
- An internal set $X \subseteq \mathbb{K}^n$ is a set of the form $X = \prod_{s\to\mathcal{U}} X_s$ with $X_s \subseteq \mathbb{C}^n$.
- Let $\xi \in (\mathbb{R}^{\mathcal{U}} \setminus \mathbb{R})_{>0}$ be a nonstandard real number. Define the coarse dimension $\boldsymbol{\delta}$ with respect to ξ on internal sets as $\boldsymbol{\delta}(X) := \mathrm{st}(\log |X|/\log \xi) \in \mathbb{R}^{\geq 0} \cup \{\pm\infty\}$.
- We call a set X broad if it is internal and $0 < \boldsymbol{\delta}(X) < \infty$, note in this case X must be pseudofinite.

Remark: An irreducible $V \subseteq \mathbb{C}^n$ admits no power saving is equivalent to existing broad sets $X_1, \ldots, X_n \subseteq \mathbb{C}^{\mathcal{U}}$ such that $\boldsymbol{\delta}(X_i) = \boldsymbol{\delta}(X_j)$ for all i, j and $\boldsymbol{\delta}(V \cap \prod_{1\leq i\leq n} X_i) = \dim(V)\boldsymbol{\delta}(X_i)$.

Definition: Let $V \subseteq \prod_{i\leq n} W_i$ be irreducible variates with $\dim(W_i) = d$ for all $i \leq n$ and $\dim(V) = kd$. We call V admits no powering-saving witnessed by $(X_i)_{i\leq n}$ for some broad sets $X_i \subseteq W_i$, if $\boldsymbol{\delta}(X_i) = \boldsymbol{\delta}(X_j)$ and $\boldsymbol{\delta}(V \cap \prod_{1\leq i\leq n} X_i) = k\boldsymbol{\delta}(X_i)$.

• Higher dimensional case:

> **Theorem** (Elekes-Szabó 2012)
> Let $V \subseteq W_1 \times W_2 \times W_3$ be irreducible varieties with $\dim(V) = 2\dim(W_i) = 2d$ and $\dim(\pi_{ij})(V) = 2d$ for all $i \neq j \in \{1, 2, 3\}$. Suppose V admits no power-saving witnessed by broad sets $X_i \subseteq W_i(\mathbb{C}^{\mathcal{U}}), i \in \{1, 2, 3\}$ **in coarse general position**. Then V is in co-ordinatewise correspondence with the graph $\Gamma_G := \{(g, h, g + h) : g, h \in G\} \subseteq G^3$ of multiplication for some d-dimensional connected **commutative** complex algebraic group G.

• A broad subset $X \subseteq W$ for an irreducible variety W over $\mathbb{C}^{\mathcal{U}}$ is called in coarse general position (cgp) if $\boldsymbol{\delta}(X \cap V) = 0$ for any proper subvariety $V \subseteq W$ over $\mathbb{C}^{\mathcal{U}}$.

Remarks:

- Without the cgp assumption, there is no guarantee to find a group.
- Bays-Breuillard 2018: Given a commutative complex algebraic group G, there exists broad cgp set $X \subseteq G(\mathbb{C}^{\mathcal{U}})$ which witnesses Γ_G admitting no power-saving (i.e. $\boldsymbol{\delta}(\Gamma_G \cap X^3) = 2\boldsymbol{\delta}(X)$) by setting X to be ultraproducts of generalised arithmetic progressions with increasing size of independent generics as generators.

? Why abelian groups ?

• Coarse general position is a strong assumption.

> **Observation** (Breuillard-Wang 2016)
> Let G be a connected algebraic group over $\mathbb{C}^{\mathcal{U}}$. Suppose the graph of multiplication Γ_G admits no power-saving witnessed by a broad set $X \subseteq G$ in coarse general position. Then G is abelian.

Question: Can we find a condition weaker than cgp so that other groups also appear in the Elekes-Szabó theorem in the case $V = \Gamma_G$ where Γ_G is the graph of multiplication of some complex algebraic group?

1.2 Approximate subgroups

Definition: A subset X in a group G is called a K-approximate subgroup if $e_G \in X$, $X = X^{-1}$ and $XX \subseteq ZX$ for some $Z \subseteq G$ with $|Z| \leq K$. If X is a broad set in some ultraproduct, we call X a coarse approximate subgroup if X is a K-approximate subgroup for $K \in \mathbb{R}^{\mathcal{U}}$ with $\boldsymbol{\delta}(K) = 0$.

Prototypical examples:

- Generalised arithmetic progressions in abelian groups:
  $\mathcal{A}(x_1, \ldots, x_k; N) := \sum_{i\leq k} c_i x_i$ where $c_i \in [-N, N] \cap \mathbb{Z}$.
- Nilprogressions of rank k and length N in nilpotent groups of nilpotency class s: $P(x_1, \ldots, x_k; N)$ collection of words using $\{x_i^{\pm1}, i \leq k\}$ and each x_i and its inverse appear at most N-times between them. They are $C_{k,s}$-approximate subgroups for some $C_{k,s} \in \mathbb{N}$.

• No power-saving for graphs of group multiplication implies existence of coarse approximate subgroups.

> **The Balog-Szemerédi-Gowers theorem** (Tao, 2008)
> Let G be an ultraproduct of groups and Γ_G be its graph of multiplication. Suppose there are broad sets A, B, C witnessing that Γ_G admits no power-saving. Then there exists a broad coarse approximate subgroup X such that $\boldsymbol{\delta}(X) = \boldsymbol{\delta}(A) = \boldsymbol{\delta}(xX \cap A)$ for some $x \in G$.

? In complex algebraic groups when can we have coarse approximate subgroups ?

> **Theorem** (Breuillard-Green-Tao 2011)
> Suppose X is a broad coarse approximate subgroup in $\mathrm{GL}_n(\mathbb{C}^{\mathcal{U}})$. Then there exists a **nilpotent** algebraic subgroup H and a coarse approximate subgroup $A \subseteq H$ such that $\boldsymbol{\delta}(X) = \boldsymbol{\delta}(A)$ and $X \subseteq ZA$ for some $Z \subseteq \mathrm{GL}_n(\mathbb{C}^{\mathcal{U}})$ with $\boldsymbol{\delta}(Z) = 0$.

Conclusion: the reasonable groups that can and should appear in the Elekes-Szabó theorem for graph of complex group multiplications are nilpotent algebraic groups.

2 The main result

2.1 Weak general position

• Let V be an irreducible variety over $\mathbb{C}^{\mathcal{U}}$. A broad set $X \subseteq V$ is called in weak general position (wgp) if $\boldsymbol{\delta}(X \cap W) < \boldsymbol{\delta}(X)$ for any proper subvariety $W \subseteq V$ over $\mathbb{C}^{\mathcal{U}}$.

> **Main theorem** (Bays, Dobrowolski, Z.)
> Let $G = G(\mathbb{C}^{\mathcal{U}})$ be a connected algebraic group defined over $\mathbb{C}$ and $\Gamma_G \subseteq G^3$ be its graph of multiplication. The following are equivalent.
>
> (i) Γ_G has no power-saving witnessed by some broad wgp sets $A, B, C \subseteq G$.
> (ii) G is nilpotent.
> (iii) There exists a broad wgp coarse approximate subgroup $X \subseteq G$.

2.2 Generic Mordell-Lang

• In a nilpotent complex algebraic group, how can we find wgp coarse approximate subgroups?

Idea: Take nilprogressions with independent generic elements as generators.

Obstacle: Taking nilprogressions of nonstandard infinite rank (number of generators) doesn't work for nilpotent groups.

? Are generalised arithmetic progressions of finite rank wgp in connected commutative complex algebraic groups ?

• Yes, if G is a semi-abelian variety by Mordell-Lang.

> **Mordell-Lang (semi-abelian, char=0, uniformity)**
> (Faltings, Vojta, McQuillan.; Scanlon 2001)
> Let $S = S(\mathbb{C})$ be a complex semi-abelian variety and Δ be a finitely generated subgroup. Let $(W_b)_{b\in B}$ be an algebraic family of proper subvarieties of S. Then there are proper algebraic subgroups $H_1, \ldots, H_m$ such that for any $b \in B$ there are $a_{1,b}, \ldots, a_{m,b}$ and $I \subseteq \{1, \ldots, m\}$ with
> $$(W_b \cap \Delta)^{\mathrm{zar}} = \bigcup_{i\in I} a_{i,b} + H_i.$$

Proof of wgp in the semi-abelian case: Let $\mathcal{A}(x_1, \ldots, x_n; N^*) \subseteq S^{\mathcal{U}}$ be a generalised arithmetic progression in some semi-abelian variety $S = S(\mathbb{C})$ with $x_1, \ldots, x_n$ independent generics in S and $0 < \boldsymbol{\delta}(N^*) < \infty$. Let $\Delta := \langle x_1, \ldots, x_n\rangle$. Suppose $W := \prod_{s\in\mathcal{U}} W_s$ is a proper subvariety of $S^{\mathcal{U}}$. Then $W \cap \mathcal{A}(x_1, \ldots, x_n; N^*) \subseteq W \cap \Delta^{\mathcal{U}}$, and each $W_s \cap \Delta \subseteq \bigcup_{i\in I_s} a_{i,s} + H_i$. As any non-zero element in Δ is generic and H_i is proper, any translate of H_i can contain at most one element in Δ. Hence $|W_s \cap \Delta| \leq m$ and $|W \cap \mathcal{A}(x_1, \ldots, x_n; N^*)| \leq m$.

Facts: Let G be a connected commutative complex algebraic group. Then G is an extension of a semi-abelian variety by a vector group, i.e. we have the following exact sequence:

$$0 \to V \to G \xrightarrow{\pi} S \to 0,$$

where V is a vector group, i.e. isomorphic to $\mathbb{G}_a^n$ for some n and S is semi-abelian.

Let $G_0 := (G[\infty])^{\mathrm{zar}}$ be the Zariski closure of torsion points in G, then $\pi(G_0) = S$ and $G = G_0 \oplus V_0$ for some vector subgroup $V_0 \leq G$.

> **Generic Mordell-Lang (commutative, char=0, weak uniformity)** (BDZ)
> Let $G = G_0 \oplus V_0$ be a connected commutative complex algebraic group. Let $r > 0$ and $\bar{g} \in G^r$ be a generic point in G^r. Let $\Delta = \langle \bar{g}\rangle$ be the finitely generated subgroup of G and $(\mathbb{C}^*, \Delta^*) \succcurlyeq (\mathbb{C}, \Delta)$ be an elementary extension.
> Let $W \subseteq G(C^*)$ be an infinite irreducible subvariety over $\mathbb{C}^*$. Suppose $W = (W \cap \Delta^*)^{\mathrm{zar}}$. Then there exists some irreducible subvariety $W' \subseteq V_0(\mathbb{C}^*)$ such that
> $$W = G_0(\mathbb{C}^*) + W'.$$

Remark: The proof follows the strategy and techniques developed in [Hrushovski 1996] and subsequent papers using the theory of DCF_0, and is closely related to [Hrushovski and Pillay, 2000].

> **Corollary**
> Let $G = G_0 \oplus V_0$ be a connected commutative complex algebraic group. Then there is $r = \max\{\dim(V_0), 1\} \in \mathbb{N}^{>0}$ such that for any $\ell \geq r$, for any tuple $(g_1, \ldots, g_\ell) \in G^\ell$ generic in G^ℓ, any broad generalised arithmetic progression $\mathcal{A}(g_1, \ldots, g_\ell; N^*)$ generated by $\{g_1, \ldots, g_\ell\}$ is wgp.

2.3 Wgp nilprogressions

> **Theorem** (BDZ)
> Let G be a connected nilpotent complex algebraic group. Then there is $r \in \mathbb{N}^{>0}$ depending on G such that for any $\ell \geq r$, for any tuple $(g_1, \ldots, g_\ell) \in G^\ell$ generic in G^ℓ, any broad nilprogression $P(g_1, \ldots, g_\ell; N^*)$ generated by $\{g_1, \ldots, g_\ell\}$ is wgp.

Remark: We work with nilboxes in the Lie algebra $\mathfrak{g}$ of G and induct on the nilpotency class of G.

References:

• Martin Bays and Emmanuel Breuillard. Projective geometries arising from Elekes-Szabó problems, *arXiv:1806.03422*, 2018.

• Emmanuel Breuillard, Ben Green, and Terence Tao. Approximate subgroups of linear groups. *Geom. Funct. Anal.*, 21(4):774–819, 2011.

• Emmanuel Breuillard and Hong Wang. Erdős geometry and the group configuration. *Oberwolfach report, Model Theory Workshop*, 2016.

• György Elekes and Endre Szabó. How to find groups? (and how to use them in Erdős geometry?). *Combinatorica*, 32(5):537–571, 2012.

• Ehud Hrushovski. The Mordell-Lang conjecture for function fields. *J. Amer. Math. Soc.*, 9:667-690, 1996.

• Ehud Hrushovski. On pseudo-finite dimensions. *Notre Dame J. Form. Log.*, 54(3-4):463–495, 2013.

• Ehud Hrushovski and Anand Pillay. Effective bounds for the number of transcendental points on subvarieties of semi-abelian varieties. *Amer. J. Math.*, 122(3): 439-450, 2000.

• László Pyber and Endre Szabó. Growth in finite simple groups of Lie type. *J. Amer. Math. Soc.*, 29:95-146, 2016.

• Thomas Scanlon. Uniformity in the Mordell-Lang conjecture. *ArXiv:math/0105238*, 2001.

• Terence Tao. Product set estimates for non-commutative groups. *Combinatorica*, 28: 547–594, 2008.