Elekes-Szabó, weak general position, and generic nilprogressions

Martin Bays

LYMOTS 2022-01-05

Joint work with Jan Dobrowolski and Tingxiang Zou

Contents

1 Elekes-Szabó and general position conditions

1.1 Coarse pseudofinite dimension

Fix a non-principal ultrafilter $\mathcal{U}$ on $\mathbb{N}$.
For a set A, an **internal** subset of $A^{\mathcal{U}}$ is an element X of $\mathbb{P}(A)^{\mathcal{U}}$,
i.e. $X = \prod_{i\to\mathcal{U}} X_i$ where $X_i \subseteq A$.

Let $X \subseteq A^{\mathcal{U}}$ be internal.

The **non-standard cardinality** of X is $|X| = \lim_{i\to\mathcal{U}} |X_i| \in \mathbb{N}^{\mathcal{U}} \cup \{\infty\}$;
X is **pseudofinite** iff $|X| < \infty$.

For a given "gauge" $N = \lim_{i\to\mathcal{U}} N_i \in \mathbb{N}^{\mathcal{U}} \setminus \mathbb{N}$,
the Hrushovski-Wagner **coarse pseudofinite dimension** of X with respect to N is

$$\boldsymbol{\delta}(X) = \boldsymbol{\delta}_N(X) = \mathrm{st}(\log_N |X|) \in \mathbb{R}_{\geq 0} \cup \{\pm\infty\}.$$

Note $\boldsymbol{\delta}(X \times Y) = \boldsymbol{\delta}(X) + \boldsymbol{\delta}(Y)$, and $\boldsymbol{\delta}(X \cup Y) = \max(\boldsymbol{\delta}(X), \boldsymbol{\delta}(Y))$.

Say X is **broad** if $0 < \boldsymbol{\delta}(X) < \infty$, i.e. $N^{\frac{1}{n}} < |X| < N^n$ for some $n \in \mathbb{N}$.

1.2 1-dimensional Elekes-Szabó

Say an algebraic surface $V \subseteq \mathbb{C}^3$ is **coherent** if there are pseudofinite $X_1, X_2, X_3 \subseteq \mathbb{C}^{\mathcal{U}}$ with (for a suitable gauge) $\boldsymbol{\delta}(X_i) = 1$ and $\boldsymbol{\delta}(V(\mathbb{C}^{\mathcal{U}}) \cap (X_1 \times X_2 \times X_3)) = 2$.

The graph $\{x + y = z\}$ of addition is coherent,
witnessed by an arithmetic progression $X_i := [-N, N] = \prod_{i\to\mathcal{U}}\{-N_i, \ldots, N_i\}$.
Similarly for multiplication, and for the group operation of an elliptic curve.

Coherence is preserved under a finite-to-finite algebraic correspondence on a co-ordinate,
e.g. $\{x^2 + y^3 = z^5\}$ is coherent.

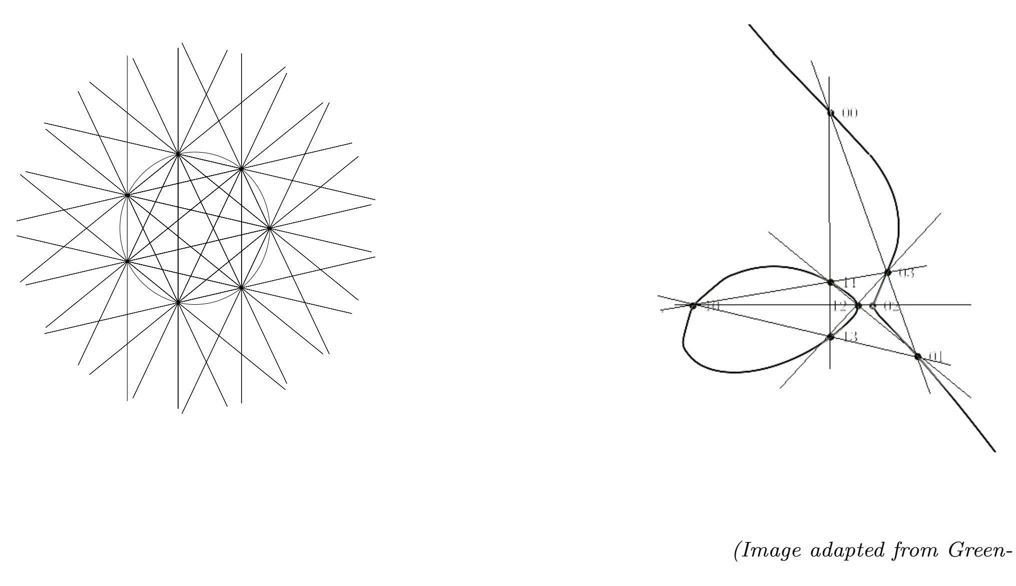
To rule out degenerate cases: call an algebraic surface $V \subseteq \mathbb{C}^3$ a "**ternary correspondence**" if it projects dominantly to any pair of co-ordinates.

Theorem (Elekes-Szabó '12)**.** *A ternary correspondence $V \subseteq \mathbb{C}^3$ is coherent if and only if it is in co-ordinatewise finite-to-finite correspondence with the graph of addition in a 1-dimensional algebraic group.*

1.3 Example: Orchard problem

Problem: Find large finite subsets of $\mathbb{R}^2$ with many collinear triples.
One precise formulation: Find $X \subseteq (\mathbb{R}^2)^{\mathcal{U}}$ with $\boldsymbol{\delta}(X) = 1$ and
$\boldsymbol{\delta}(\{(x_1, x_2, x_3) \in X^3 : x_1, x_2, x_3 \text{ are distinct and collinear}\}) \geq 2$.

Solutions: Take X a length N arithmetic progression in a plane cubic curve.



(Image adapted from Green-Tao)

Theorem (Elekes-Szabó '13)**.** *There are no solutions with X on an irreducible plane curve of degree > 3.*

1.4 Higher-dimensional Elekes-Szabó

Elekes-Szabó can be seen as a matter of modularity of the geometry of acl.
It goes through in higher dimension, but we need a minimality condition to ensure exchange.

Definition. A be a broad pseudofinite subset X of an irreducible algebraic variety V is in **coarse general position** (**cgp**) in V if $\boldsymbol{\delta}(X \cap W) = 0$ for any proper subvariety $W \subsetneq V$.

If W_1, W_2, W_3 are varieties, a subvariety $V \subseteq \prod_i W_i$ is **cgp-coherent** if there are cgp $X_i \subseteq W_i$ with $\boldsymbol{\delta}(X_i) = 1$ and $\boldsymbol{\delta}(V \cap \prod_i X_i) = 2$.

As before, V is a "**ternary correspondence**" if it projects dominantly and with generically finite fibres to any pair $W_i \times W_j$ of co-ordinates. (In particular, $\dim(V) = 2\dim(W_i)$.)

Theorem (Elekes-Szabo '12, B-Breuillard '18)**.** *A ternary correspondence $V \subseteq \prod_i W_i$ is cgp-coherent if and only if it is in co-ordinatewise finite-to-finite correspondence with the graph of addition in a commutative algebraic group.*

1.5 Coherence without cgp

What happens if we relax the cgp hypothesis?
Some general position condition is necessary to rule out degenerate situations.
The following example shows that "X_i is Zariski-dense in W_i" is insufficient.

Example. Suppose $W_1 = W_2 = W_3 =: W$,
where W is an arbitrary variety containing a commutative algebraic group G as a subvariety.
Let $V \subseteq W^3$ be a ternary correspondence (with everywhere finite fibres),
such that $V \cap G^3$ is the graph of addition.
Let $X_1 = X_2$ be the union of an arithmetic progression in G of length N,
and a Zariski-dense subset of W of size $\log(N)$,
and let X_3 be the image $\{z : (x, y, z) \in V, (x, y) \in X_1 \times X_2\}$.

Then $\boldsymbol{\delta}(X_i) = 1$ for $i = 1, 2, 3$, and $\boldsymbol{\delta}(V \cap \prod X_i) = 2$.

This example suggests the following definition.

Definition. A broad pseudofinite subset X of an irreducible algebraic variety V is in **weak general position** (**wgp**) in V if $\boldsymbol{\delta}(X \cap W) < \boldsymbol{\delta}(X)$ for any proper subvariety $W \subsetneq V$.

If W_1, W_2, W_3 are varieties, a subvariety $V \subseteq \prod_i W_i$ is **wgp-coherent** if there are wgp $X_i \subseteq W_i$ with $\boldsymbol{\delta}(X_i) = 1$ and $\boldsymbol{\delta}(V \cap \prod_i X_i) = 2$.

1.6 Examples of wgp-coherence

Example.

$$A := \begin{bmatrix} 1 & [-N, N] & [-N^2, N^2] \\ 0 & 1 & [-N, N] \\ 0 & 0 & 1 \end{bmatrix}$$

witnesses that the graph of the group operation in the Heisenberg group is wgp-coherent.

Example (BB'18). The graph of $* : \mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{C}^2$

$$(a_1, b_1) * (a_2, b_2) = (a_1 + a_2 + b_1^2 b_2^2, b_1 + b_2)$$

is wgp-coherent (witnessed by $[-N^4, N^4] \times [-N, N]$),
but is not in co-ordinatewise correspondence with the graph of a group operation.

Working hypothesis: Iterated abelian groups are the only source of wgp-coherence.

1.7 Test case: higher orchard

$S \subseteq \mathbb{C}^3$ an algebraic surface, e.g. cubic.
$V := \{(x, y, z) : x, y, z \in S \text{ and } x, y, z \text{ are distinct collinear}\}$.
For what S is V wgp-coherent?
Expectation: S has to be the union of three planes.

2 ES in a group

Question 1. *For which connected algebraic groups $(G; \cdot)$ is the graph $\Gamma_\cdot \subseteq G^3$ wgp-coherent?*

I.e. when do there exist wgp $X_1, X_2, X_3 \subseteq G$ with $\boldsymbol{\delta}(X_i) = 1$
and $\boldsymbol{\delta}(\{(x_1, x_2, x_3) \in \prod_i X_i : x_1 \cdot x_2 = x_3\}) = 2$?

For cgp-coherence, by the ES result above the answer is: iff G is abelian.

Theorem 1 (B-Dobrowolski-Zou)**.** *The graph of multiplication in a connected algebraic group G is wgp-coherent iff G is nilpotent.*

As we see below, the forward direction is not really new. But the converse is.

2.1 Balog-Szemerédi-Gowers-Tao and reduction to approximate subgroups

Coherence implies large "energy",

$$\boldsymbol{\delta}(\{(x_1, x_2, x_1', x_2') \in X_1 \times X_2 \times X_1 \times X_2 : x_1 \cdot x_2 = x_1' \cdot x_2'\}) = 3.$$

Tao's version of Balog-Szemerédi-Gowers obtains from this an approximate subgroup,
some coset of which has large intersection with X_1.

Definition. An internal subset $X \subseteq G$ is a **coarse approximate subgroup**
if X is broad,
and $e \in X = X^{-1}$,
and $XX \subseteq KX$ for some internal K with $\boldsymbol{\delta}(K) = 0$.

Then BSGT essentially[1] reduces Question 1 to:

Question 2. *Which connected algebraic groups G admit a wgp coarse approximate subgroup?*

2.2 Wgp coarse approximate subgroup ⇒ nilpotent

For this we can either directly use the result of Breuillard-Green-Tao that approximate subgroups of $\mathrm{GL}_n(\mathbb{C})$ are nilpotently controlled, or we can parallel the proof of that result as follows.

Suppose $X \subseteq G$ is a wgp coarse approximate subgroup.

- Replace X with a $\bigwedge$-internal subgroup $H \leq G$ with $X \subseteq H$ and $\boldsymbol{\delta}(H) = \boldsymbol{\delta}(X)$.
  ($H := \bigcap_{n\in\mathbb{N}} X^{\lfloor \log_2(\log_{|K|} N) \rfloor - n}$)
- BGT(+Hrushovski(+Jordan)): A simple complex linear algebraic group has no broad $\bigwedge$-internal Zariski-dense subgroup.
- It follows that we may assume G is solvable.
- If G is not nilpotent, an argument of Breuillard-Green then cooks out a broad $\bigwedge$-internal subfield of $\mathbb{C}^{\mathcal{U}}$, contradicting sum-product theorems.
  The wgp hypothesis is used to obtain broadness of quotients of H and hence of this field.

2.3 Nilprogressions

It remains to show that any nilpotent complex algebraic group admits a wgp coarse approximate subgroup. We will find one as a nilprogression of pseudofinite length.

Definition 2. Given elements $a_1, \ldots, a_r$ of a group H and $m \in \mathbb{N}$,
the **nilprogression** generated by $\overline{a}$ of length m is the set $P(\overline{a}, m) \subseteq H$ of words in a_i and a_i^{-1} in which for each i, the number of occurences of a_i or a_i^{-1} is at most m.

For H nilpotent, $|P(\overline{a}, m)| < O(m^{O(1)})$, and $P(\overline{a}, m)$ is a $O_{H,r}(1)$-approximate subgroup.

Now fix G a non-trivial connected nilpotent complex algebraic group.

Given $r \in \mathbb{N}$, set

$$P_r := P(\overline{a}, N) \subseteq G(\mathbb{C}^{\mathcal{U}}),$$

where $\overline{a} \in G^r(\mathbb{C})$ is algebraically generic
(i.e. $\mathrm{trd}(\overline{a}/C_0) = \dim G^r = r \dim G$ where G is defined over C_0).

Then P_r is a coarse approximate subgroup.

The difficulty is to show:

Lemma 1. *For large enough $r \in \mathbb{N}$, P_r is wgp in G.*

Remark 3. One might think to instead try to take $r \in \mathbb{N}^{\mathcal{U}} \setminus \mathbb{N}$.
For commutative G this works, and one can even get cgp this way.
But e.g. for the Heisenberg group, $|P_r| \approx N^{2\binom{r}{2}+r}$ while $|P_r \cap Z(G)| \approx N^{2\binom{r}{2}}$,
so wgp fails (since $\mathrm{st}\left(\frac{\binom{r}{2}}{\binom{r}{2}+r}\right) = 1$).

2.4 Reducing to commutative G

We first reduce Lemma 1 to the case that G is commutative.

Rough idea for G of nilpotency class 2:

- Work in the Lie algebra $\mathfrak{g}$ with a generic nilbox

  $$B_r := \sum_i [-N, N] \cdot b_i + \sum_{i<j} [-N^2, N^2] \cdot [b_i, b_j]$$

  where $\exp(b_i) = a_i$.

  (Then $\exp(B_r) \approx P_r$; e.g. $a_2^n a_1^n = a_1^n a_2^n [a_2, a_1]^{n^2}$.)
- Then $B_r/\mathfrak{g}'$ and $\mathfrak{g}' \cap B_r$ are generalised arithmetic progressions,
  $\sum_i [-N, N] \cdot b_i/\mathfrak{g}'$ and $\sum_{i<j} [-N^2, N^2] \cdot [b_i, b_j]$.
- If $W \subsetneq G$ is a proper subvariety,
  either $W/G' \subseteq G/G'$ is proper or the fibres $W \cap cG'$ are generically proper.
  In either case we can apply the abelian case to bound $|W \cap \exp(B_r)|$.

Generally, we inductively quotient by the last non-trivial term $\mathfrak{g}_n$ in the descending central series. Complications:

- Sometimes short Lie monomials in generics are already in $\mathfrak{g}_n$ (e.g. free k-Engel Lie algebras).
- The monomials themselves might not have generic image in G_n; but by Zilber indecomposability, if we take r large enough, we get enough independent generics in G_n by taking suitable disjoint Lie polynomials in the b_i.

2.5 G commutative

We want to see that $P_r = [-N, N]^r \cdot \overline{a} = \sum_{i=1}^r [-N, N] a_i$ is wgp in G for large enough r.

2.5.1 Case 1: $G = \mathbb{G}_a^d$

$[-N, N]^d$ is wgp in $\mathbb{G}_a^d$,
since for $W \subsetneq G$ a proper subvariety, $W \cap [-N, N]^d < O(N^{\dim W})$.
Hence $P_d = [-N, N]^d \cdot \overline{a}$ is also wgp.

Similarly, P_r is wgp for $r \geq d$.

2.5.2 Case 2: G is semiabelian

Fact 1 (Mordell-Lang)**.** *If $\Gamma \leq G$ is a finitely generated subgroup,*
and $W \subseteq G$ is an irreducible subvariety,
and $W \cap \Gamma$ is Zariski-dense in W,
then W is a coset of an algebraic subgroup of G.

Take $\Gamma := \langle \overline{a} \rangle$.
By the genericity and rigidity,
no $\gamma \in \Gamma \setminus \{0\}$ is in a proper algebraic subgroup of G.

So if $W \subseteq G$ is infinite and $W \cap \Gamma$ is Zariski-dense in W,
then $W = G$.

So if $W \subsetneq G$ is a proper subvariety, $\Gamma \cap W(\mathbb{C})$ is finite.

Moreover, for an algebraic family W_b of proper subvarieties,
$|\Gamma \cap W_b(\mathbb{C})|$ is bounded uniformly in b (Scanlon).

Hence $P_r = [-N, N]^r \cdot \overline{a}$ is in (very) general position, certainly wgp.

2.5.3 Case 3: G arbitrary

A connected commutative algebraic group G can be written as $G = G_0 \oplus V_0$,
where $G_0 = G[\infty]^{\mathrm{Zar}}$ is **almost semiabelian**, i.e. connected with Zariski-dense torsion,
and V_0 is a vector group $V_0 \cong \mathbb{G}_a^n$.

We obtain the following "generic Mordell-Lang" result for G in terms of this decomposition.
Let $\Gamma := \langle \overline{a} \rangle$.

Theorem 4 (BDZ)**.** *If $W \subseteq G$ is an infinite irreducible subvariety and $W \cap \Gamma$ is Zariski-dense in W,*
then $W = G_0 + W_0$ for some irreducible subvariety $W_0 \subseteq V_0$.

Moreover, this holds uniformly in the sense that it also holds for $\Gamma^{\mathcal{U}}$.

Combined with the $\mathbb{G}_a^n$ case, this suffices to show that P_r is wgp for $r \geq \dim(V_0)$,
completing the proof of Theorem 1.

Remark: Mordell-Lang for arbitrary f.g. subgroups of arbitrary commutative algebraic groups is an open problem (without a clear conjectural statement).

2.6 Sketch proof of Theorem 4

Basic idea: adapt Hrushovski's DCF proof of char 0 function field Mordell-Lang to our setting of a generic f.g. subgroup of a fixed commutative algebraic group G.

(For G semiabelian this is not new; c.f. Hrushovski-Pillay "Effective bounds for the number of transcendental points on subvarieties of semi-abelian varieties".)

- We can assume we are working in $K \models \mathrm{DCF}_0$,
  and G is defined over the constant field $C \leq K$,
  and Γ is generic over C.
- Consider the logarithmic derivative

  $$0 \to G(C) \to G(K) \xrightarrow{\mathrm{lD}} LG(K) \to 0.$$
- Set $H := \mathrm{lD}^{-1}(\langle \mathrm{lD}(\Gamma) \rangle_C)$, a finite Morley rank subgroup of $G(K)$.
- Given $W \subsetneq G$, WMA by quotienting that W is stabilised by no non-trivial almost semiabelian subgroup.
- Let $\pi : G \to S$ be the maximal semiabelian quotient.
- One sees (roughly[2]) that $(\mathrm{lD}_S^{-1} \circ L\pi \circ lD)(W \cap H)$ is almost internal to C;
  but the socle of $\pi(H)$,
  the maximal connected definable subgroup which is almost internal to C,
  is $S(C)$. So $L\pi(lD(W \cap H))$ is a point.
- Suppose for contradiction $S \neq \{0\}$.
  Then by the genericity, also $lD(W \cap H)$ is point.
  So after translating, $W \cap H \subseteq G(C)$,
  so W has a Zariski-dense set of constant points,
  so W is over C,
  contradicting the genericity.

---

[1] I'm lying here slightly. In fact, only part of the wgp condition on X_1 passes to the coarse approximate subgroup obtained from BSGT: it is Zariski dense and the image in any non-trivial group quotient is broad. Luckily, this suffices to prove nilpotence.

[2] Actually we should pass to an appropriate (still Z-dense) subset of $W \cap H$