Thin groups and superstrong approximation
MSRI Publications
Volume **61**, 2013

Growth in linear groups

LÁSZLÓ PYBER AND ENDRE SZABÓ

We give a description of nongrowing subsets in linear groups over arbitrary fields, which extends the product theorem for simple groups of Lie type. We also give an account of various related aspects of growth in linear groups.

1. A polynomial inverse theorem in linear groups

The following theorem was proved independently in 2010 by Breuillard, Green and Tao [Breuillard et al. 2011a] and the authors [Pyber and Szabó 2010].

Theorem 1 (product theorem). *Let L be a finite simple group of Lie type of rank r and A a generating set of L. Then either $A^3 = L$ or*

$$|A^3| > |A|^{1+\varepsilon},$$

where ε depends only on r.

For $G = \mathrm{PSL}(2, p)$, p prime, this is a famous result of Helfgott [2008]. Other special cases that preceded the general proof include $G = \mathrm{PSL}(3, p)$ [Helfgott 2011] and $G = \mathrm{PSL}(2, q)$, q a prime power [Dinai 2011; Varjú 2012].

In [Pyber and Szabó 2010] we give various examples which show that in the above result the dependence of ε on r is necessary. In particular we construct generating sets of $\mathrm{SL}(n, 3)$ of size $2^{n-1} + 4$ with $|A^3| < 100|A|$ for $n \geq 3$.

For the groups $G = \mathrm{PSL}(n, q)$ (which are simple groups of Lie type of rank $n - 1$) the product theorem can be reformulated as follows: If A is a generating set of G, such that $|A^3| < K|A|$ for some number $K \geq 1$, then A has at most $K^{c(n)}$ (i.e., polynomially many) elements. This reformulation turns out to be quite useful when we seek an extension of the product theorem which describes nongrowing subsets of linear groups.

The product theorem has quickly become a central result of finite asymptotic group theory with many applications. To describe a few of these we introduce some graph-theoretic terminology. The *diameter*, diam X, of an undirected graph $X = (V, E)$ is the largest distance between two of its vertices. The *girth* of X is the length of the shortest cycle in X. Given a subset A of the vertex set V

László Pyber is supported in part by OTKA NK78439 and K84233. Endre Szabó is supported in part by OTKA NK81203 and K84233.

the *expansion* of A, $c(A)$, is defined to be the ratio $|\sigma(X)|/|X|$ where $\sigma(X)$ is the set of vertices at distance 1 from A. A graph is a C-*expander* for some $C > 0$ if for all subsets A of V with $|A| < |V|/2$ we have $c(A) \geq C$. A family of graphs is an *expander family* if all of its members are C-expanders for some fixed positive constant C.

A subset S of a group G is called *symmetric* if it is inverse-closed (throughout the paper S will denote a symmetric subset). The Cayley graph $\mathrm{Cay}(G, S)$ is a graph whose vertices are the elements of G and which has an edge from x to y if and only if $x = sy$ for some $s \in S$. Then the diameter of $\mathrm{Cay}(G, S)$ is the smallest number d such that $S^d = G$.

The following classical conjecture is due to Babai. (It first appeared in print in [Babai and Seress 1992].)

Conjecture 2. *For every nonabelian finite simple group L and every symmetric generating set S of L we have* $\operatorname{diam}\mathrm{Cay}(L, S) \leq C(\log|L|)^c$ *where c and C are absolute constants.*

The product theorem easily implies the following.

Corollary 3. *Conjecture 2 holds for simple groups of Lie type of bounded rank.*

The following conjecture of Liebeck, Nikolov, and Shalev is more recent:

Conjecture 4 [Liebeck et al. 2012]. *There exists an absolute constant c such that if L is a finite simple group and A is a subset of L of size at least two*, *then L is a product of N conjugates of A for some $N \leq c\log|L|/\log|A|$.*

By a deep (and widely applied) theorem of Liebeck and Shalev [2001] the conjecture holds when S is a conjugacy class or, more generally, a normal subset (that is a union of conjugacy classes).

Theorem 5. *Conjecture 4 holds for simple groups of Lie type of bounded rank.*

This is proved in [Gill et al. 2011] using the product theorem and an extra trick which handles small subsets S.

Breuillard, Green, Guralnick and Tao have announced a deep result of similar flavour:

Theorem 6 [Breuillard et al. 2013]. *Let G be a simple group of Lie type of rank r. Then for two random elements x, y the Cayley graph* $\mathrm{Cay}(G, \{x, y\})$ *is an $\varepsilon(r)$ expander with probability going to* 1 *as* $|G| \to \infty$, *where $\varepsilon(r)$ depends only on r.*

As an open problem Lubotzky [2012] suggested deciding whether this holds for all nonabelian finite simple groups with an absolute constant ε.

The proof of Theorem 6 is based on the product theorem, some results in [Breuillard et al. 2012a] and the proof scheme (termed the Bourgain–Gamburd expansion machine in [Tao 2012]) first used in the proof of the following theorem.

Theorem 7 [Bourgain and Gamburd 2008]. *For any* $0 < \delta \in \mathbb{R}$ *there exists* $\varepsilon = \varepsilon(\delta) > 0$ *such that for every prime* p, *if* S *is a symmetric set of generators of* $G = \mathrm{SL}(2, p)$ *such that girth of the Cayley graph* $\mathrm{Cay}(G; S)$ *is at least* $\delta \log p$ *then* $\mathrm{Cay}(G; S)$ *is an* ε*-expander.*

It seems quite plausible that this result extends to all nonabelian finite simple groups. In view of the girth bounds in [Gamburd et al. 2009] this would imply Theorem 6. At present however such an extension is not even known to hold for the groups $\mathrm{SL}(2, q)$, q a prime power.

For the above applications of the product theorem it is essential that the size of a generating set A is bounded by a polynomial of the tripling constant $K = |A^3|/|A|$ (unless A is very large). For a discussion of related issues, see [Tao 2012]. Guided by this insight, and remarks of Helfgott [2011, page 764] and Breuillard, Green and Tao [Breuillard et al. 2012b, Remark 1.8], and various discussions on Tao's blog, we proved in 2012 the following polynomial inverse theorem, which significantly improves the results in [Pyber and Szabó 2010].

Theorem 8 [Pyber and Szabó $\geq$ 2012]. *Let* S *be a symmetric subset of* $\mathrm{GL}(n, \mathbb{F})$ *satisfying* $|S^3| \leq K|S|$ *for some* $K \geq 1$, *where* $\mathbb{F}$ *is an arbitrary field. Then* S *is contained in the union of polynomially many* (*more precisely* $K^{c(n)}$) *cosets of a finite-by-soluble subgroup* Γ *normalised by* S.

Moreover, Γ *has a finite subgroup* P *normalised by* S *such that* Γ/P *is soluble*, *and* S^3 *contains a coset of* P.

The theorem extends and unifies several earlier results. Most importantly (to us) it contains the product theorem (for symmetric sets) as a special case. For subsets of $\mathrm{SL}(2, p)$ and $\mathrm{SL}(3, p)$ similar results were obtained by Helfgott [2008; 2011].

In characteristic zero Theorem 8 was first proved in [Breuillard et al. 2011a]. The earliest result in this direction for subsets of $\mathrm{SL}(2, \mathbb{R})$ is due to Elekes and Király [2001]. The proof in [Breuillard et al. 2011a] uses the fact that a virtually soluble subgroup of $\mathrm{SL}(n, \mathbb{C})$ has a soluble subgroup of n-bounded index, which is no longer true in positive characteristic.

Finally the theorem implies a result of Hrushovski for linear groups over arbitrary fields obtained by model-theoretic tools [Hrushovski 2012]. In his theorem the structure of Γ is described in a less precise way and the number of covering cosets is only bounded by some large function of n and K.

It seems possible that a result similar to Theorem 8 can be proved with H nilpotent (possibly at the cost of loosing the normality of H and P in $\langle S \rangle$). Indeed in characteristic zero such a result follows by combining [Breuillard et al. 2011a] with [Breuillard and Green 2011], and for prime fields it follows from [Pyber and Szabó 2010] and the results of [Gill and Helfgott 2010] for soluble groups. In general this may be technically quite challenging even though soluble linear groups have a nilpotent-by-abelian subgroup of n-bounded index.

It may also be possible that a more general polynomial inverse theorem holds (see [Breuillard 2014]). We pose the following question which bypasses abelian and finite obstacles.

Question 9. *Let S be a finite symmetric subset of an arbitrary group G such that $|S^3| \leq K|S|$ for some $K \geq 1$. Is it true that S is contained in $K^{c(G)}$ cosets of some virtually soluble subgroup of G?*

The above question may be viewed as a counterpart of the polynomial Freiman–Ruzsa Conjecture which asserts that (a variant of) Freiman's famous Inverse theorem holds with polynomial constants. The existence of some huge bound $f(K)$ for the number of covering cosets, as above, follows from the very general inverse theorem of Breuillard, Green and Tao [Breuillard et al. 2012b]. See [Breuillard 2014] for a detailed discussion of these issues.

Theorem 8 shows that the answer is positive for the groups $G = \mathrm{SL}(n, \mathbb{F})$. It would interesting to investigate this question for various groups of intermediate word growth, such as the Grigorchuk groups (see, e.g., [de la Harpe 2000]).

It would be extremely interesting if the number of cosets required would be bounded by K^c for some absolute constant c for all groups G. Obtaining such a result for all linear groups G (in which c does not depend on the dimension) already seems to require some essential new ideas.

2. Applications of the Sarnak–Xue–Gowers trick

A subset X of a group G is called product-free if there are no solutions to $xy = z$ with $x, y, z \in X$.

Answering a question in [Babai and Sós 1985], Gowers [2008] showed that the group $G = \mathrm{PSL}(2, p)$ has no product-free subset of size greater than $c|G|^{8/9}$ for some $c > 0$. Gowers' proof is closely related to an argument of Sarnak and Xue [1991], which also plays an important role in the proof of Theorem 7.

Notation. For any group G let $\deg_{\mathbb{C}}(G)$ denote the minimum degree of a nontrivial complex representation.

It was observed in [Nikolov and Pyber 2011], that as a byproduct of the results of [Gowers 2008] one obtains the following extremely useful corollary.

Corollary 10. *Let G be a group of order n such that $\deg_{\mathbb{C}}(G) = k$. If A is a subset of G such that $|A| > n/k^{1/3}$, then we have $A^3 = G$.*

For groups of Lie type rather strong lower bounds on the minimal degree of a complex representation are known [Landazuri and Seitz 1974]. Combining these bounds with Corollary 10 we obtain the following proposition, which of course implies the product theorem for very large subsets.

Proposition 11. *Let A be a subset of $G = \mathrm{PSL}(n, q)$ of size at least $2|G|/q^{\frac{n-1}{3}}$. Then we have $A^3 = G$.*

Another interesting application is the following "Waring-type" theorem:

Theorem 12 [Nikolov and Pyber 2011]. *Let w be a nontrivial group word. Let L be a finite simple group of Lie type of rank r over the field $\mathbb{F}_q$. Let W be any subset of $w(L)$ such that $|W| \geq |w(L)|/q^{r/13}$. Then there exists a positive integer N depending only on w such that if $|L| > N$ then*

$$W^3 = L.$$

Earlier, as the main result of a difficult paper, Shalev [2009] has obtained the same result in the case $W = w(L)$ (allowing L to be also an alternating group).

An advantage of the above sparse version is that one can impose further restrictions on W. For example one can require that no two elements of W are inverses each other, or images of each other under Frobenius automorphisms. It would be interesting to obtain a sparse "Waring-type" theorem for the alternating groups.

The proof of Theorem 12 is relatively short compared to the one in [Shalev 2009]. One only has to show that for simple groups of Lie type the sets $w(L)$ are large enough.

Larsen, Shalev and Tiep, in a major recent work [Larsen et al. 2011], have shown that in fact, for a nontrivial word w, $w(L)^2 = L$ holds for large enough finite simple groups.

In certain situations, in which Corollary 10 cannot be applied directly, the following extension due to Babai, Nikolov and Pyber has turned out to be quite useful.

Lemma 13 [Babai et al. 2008]. *Let G be a group of order n such that $\deg_{\mathbb{C}}(G) = k$. Let $A_1, \ldots, A_t$ ($t \geq 3$) be nonempty subsets of G. If*

$$\prod_{i=1}^{t} |A_i| \geq \frac{n^t}{k^{t-2}},$$

then $\prod_{i=1}^{t} A_i = G$.

A major result of Nikolov and Segal [2007a; 2007b] states that finite index subgroups of finitely generated profinite groups are open, as conjectured by Serre. Improving their methods, the same authors later proved the following theorem, which also implies Serre's conjecture:

Theorem 14 [Nikolov and Segal 2011]. *Let $d, q \in \mathbb{N}$ and G a finite d-generated group. Let G^q be the subgroup of G generated by the q-th powers. There exists a function $f(d, q)$ such that every element of G^q is a product of at most $f(d, q)$ powers x^q.*

Recently Nikolov and Segal [2012] obtained much shorter proofs as well as vast generalisations of their results. Lemma 13 is a key tool in obtaining them.

Lemma 13 was also used to improve a result from [Liebeck and Pyber 2001]:

Theorem 15 [Babai et al. 2008]. *Let L be a finite simple group of Lie type in characteristic p. Then L is a product of five Sylow p-subgroups.*

As an illustration of the proof consider the Ree groups $L = {}^2F_4(q)$ (a difficult case in [Liebeck and Pyber 2001]). Take a pair of Sylow p-subgroups U and V in L such that $U \cap V = \{1\}$. Using the tables in [Kleidman and Liebeck 1990] it follows that

$$\frac{|L|}{|UV|} < \deg_{\mathbb{C}}(L)^{1/2}.$$

Hence Lemma 13 with $t = 4$ immediately gives

$$L = (UV)(VU)(UV)(VU) = UVUVU.$$

Combining Theorem 15 with an argument from [Liebeck and Pyber 2001] one obtains a similar improvement of another result in [Liebeck and Pyber 2001].

Theorem 16. *Let $\mathbb{F}$ be a field of characteristic p and G a finite subgroup of* $\mathrm{GL}(n, \mathbb{F})$ *generated by its Sylow p-subgroups. If p is sufficiently large compared to n then G is a product of* 5 *of its Sylow p-subgroups.*

This is a generalisation of the following curious result, originally obtained by model-theoretic tools.

Theorem 17 [Hrushovski and Pillay 1995]. *Let p be a prime, and G a subgroup of* $\mathrm{GL}(n, p)$ *generated by elements of order p. Then G can be written as a product $G = C_1 C_2 \dots C_k$ where the C_i are cyclic subgroups of order p and k depends only on n.*

Returning to our main theme next we present a (previously unpublished) "baby version" of the product theorem. This result was in fact the starting point of the authors' joint work concerning growth in groups. It is proved by a "greedy argument" based on Corollary 10. The proof of the product theorem may be viewed as an analogous greedy argument based on certain Larsen–Pink type inequalities (see Section 3).

First we quote two combinatorial results which also play an important role in the proof of the product theorem. As noted in [Helfgott 2011], the first one is essentially due to Ruzsa (see [Ruzsa 2010; Ruzsa and Turjányi 1985]).

Proposition 18 [Helfgott 2011]. *Let $1 \in S$ be a symmetric finite subset of a group and $k \geq 3$ an integer. Then*

$$\frac{|S^k|}{|S|} \leq \left(\frac{|S^3|}{|S|}\right)^{k-2}.$$

That is, if a small power of S is much larger than S itself, then S^3 is already much larger than S.

The next lemma is a slight extension of a result from [Helfgott 2011].

Lemma 19 [Pyber and Szabó 2010]. *Let $1 \in S$ be a symmetric finite subset of a group G, and H a subgroup of G. Then for all integers $k > 0$ one has*

$$\frac{|S^k \cap H|}{|S^2 \cap H|} \leq \frac{|S^{k+1}|}{|S|}.$$

That is, growth in any subgroup H implies growth in G itself.

Here is the simplest version of our "baby product theorem".

Theorem 20. *Let S be a symmetric generating set of the group $G = \mathrm{SL}(n, q)$ (where $q \geq 4$ is a prime power) and H a subgroup of G isomorphic to $\mathrm{SL}(2, q)$. If S contains H then either $S^3 = G$ or*

$$|S^3| > |S| \cdot q^{1/1000}.$$

Proof. We have $\deg_{\mathbb{C}}(H) \geq (q-1)/2$. Assume first that S^6 does not contain all conjugates of H in G. Since S generates G, there exists a conjugate H_0 of H such that H_0 is contained in S^6, and an S-conjugate, say H_0^s, of H_0 is not contained in S^6. Then we have

$$|S^2 \cap H_0^s| \leq |H_0| \cdot \deg_{\mathbb{C}}(H)^{-1/3},$$

since otherwise S^6 would contain H_0^s by Corollary 10. It follows from the assumptions on H_0 that H_0^s is contained in S^8. Hence by Lemma 19 we have

$$\frac{|S^9|}{|S|} \geq \frac{|S^8 \cap H_0^s|}{|S^2 \cap H_0^s|} \geq \deg_{\mathbb{C}}(H)^{1/3}.$$

By Proposition 18 this implies

$$\left(\frac{|S^3|}{|S|}\right)^7 \geq \frac{|S^9|}{|S|} \geq \deg_{\mathbb{C}}(H)^{1/3}.$$

Therefore

$$|S^3| \geq |S| \cdot \deg_{\mathbb{C}}(H)^{1/27} = |S| \cdot \left(\frac{q-1}{2}\right)^{\frac{1}{27}},$$

and our statement follows in this case.

Assume now that S^6 contains all conjugates of H, but $S^3 \neq G$. In this case S^6 contains a noncentral conjugacy class C of G together with C^{-1}. By a result of Lawther and Liebeck [1998] (see also [Ellers et al. 1999]), if $\mathcal{K}$ is any noncentral conjugacy class of $\mathrm{SL}(n, q)$ $(q \geq 4)$, then $(\mathcal{K} \cup \mathcal{K}^{-1})^{40n} = \mathrm{SL}(n, q)$.

This implies $S^{240n} = G$. On the other hand, since $S^3 \neq G$, by Proposition 11 (which also holds for $\mathrm{SL}(n, q)$), we have $|S| \leq 2|G|/q^{(n-1)/3}$. By Proposition 18,

$$\left(\frac{|S^3|}{|S|}\right)^{240n-2} \geq \frac{|S^{240n}|}{|S|} = \frac{|G|}{|S|} \geq \frac{1}{2}\, q^{(n-1)/3},$$

and our statement follows. □

Note that in the above result the exponent of q in the growth is independent of n.

Essentially the same result continues to hold when G is an arbitrary simple group of Lie type over $\mathbb{F}_q$. More significantly, if in Theorem 20 we replace H by any subgroup with $\deg_{\mathbb{C}}(H) \geq q^{O(1)}$, we still obtain the conclusion $|S^3| \geq |S| \cdot q^{O(1)}$ (unless $S^3 = G$). Here H could be, say, a Suzuki subgroup, or a subfield subgroup $\mathrm{SL}(n, q_0)$ for some $\mathbb{F}_{q_0} \leq \mathbb{F}_q$.

Definition 21. A family of finite groups G_i is an expanding family if, for some natural number k, there exist generating subsets S_i of G_i of size at most k such that the graphs $\mathrm{Cay}(G_i, S_i)$ form an expander family.

Kassabov, Lubotzky, and Nikolov proved that all finite simple groups, except possibly the Suzuki groups, form an expanding family (see the announcement [Kassabov et al. 2006] for references). The same is now known for the Suzuki groups as well by [Breuillard et al. 2011b], and more generally by Theorem 6.

As an important tool in the proof of this result Lubotzky [2011] has shown that a simple group of Lie type of rank r over the field $\mathbb{F}_q$ (not a Suzuki group) decomposes as a product of $f(r)$ subgroups isomorphic to $\mathrm{SL}(2, q)$ or $\mathrm{PSL}(2, q)$. The argument in [Lubotzky 2011] is based on model theory. Theorem 20, extended to simple groups of Lie type, immediately yields another proof of this result, which (assuming known results) is both elementary and short.

Another group-theoretic proof, that gives a quadratic bound for $f(r)$, which uses Lemma 13 in a different way, is given in [Liebeck et al. 2011]. That proof does not yield growth results, and does not apply to, say, Suzuki subgroups.

Somewhat surprisingly the following affine variant of Theorem 20 is also true.

Lemma 22. *Let H be a d-generated finite group with* $\deg_{\mathbb{C}}(H) > K^{21}$, *and A a $\mathbb{Z}H$-module. Let $0 \in S \subseteq A$ be a symmetric H-invariant set generating A. Then* (*with multiplicative notation*) *either* $|S^3| > K \cdot |S|$ *or S^{7d} contains the submodule* $[H, A]$.

This plays an essential role in the proof of the polynomial inverse theorem (Theorem 8) in the case of linear groups over finite fields.

We end this section with a question vaguely related to superstrong approximation (see, e.g., [Breuillard 2014]).

Question 23. *Let G_i be an expanding family of finite groups. Is it true that for all i and every symmetric generating set S_i of G_i we have*

$$\operatorname{diam}\operatorname{Cay}(G_i, S_i) \leq C(\log|G_i|)^c,$$

where the constants c and C depend only on the family?

Note that answering an earlier question of Lubotzky and Weiss [Lubotzky and Weiss 1993] in the negative, in [Alon et al. 2001] some expanding families of groups G_i are constructed together with bounded sized generating sets S_i such that the corresponding Cayley graphs do not form an expander family (see also [Meshulam and Wigderson 2004]). The alternating groups also have these properties, but the fact that they form an expanding family was proved somewhat later in the breakthrough paper of Kassabov [2007].

Note also that since nonabelian finite simple groups form an expanding family, a positive answer to Question 23 would imply Babai's conjecture.

3. On the proof of the product theorem

In this section we describe the main ideas in the proof of the product theorem for $\mathrm{SL}(n, q)$. Simple groups of Lie type can be handled by essentially the same argument. A far-reaching generalisation of the argument plays an important role in the proof of the polynomial inverse theorem.

In the course of the proof we obtain various results which say that if L is a "nice" subgroup of an algebraic group G, generated by a set A, then A grows in some sense. These were motivated by earlier results of Helfgott [2008; 2011], Hrushovski and Pillay [1995], and Theorem 20.

Assume for example that A generates $L = \mathrm{SL}(n, q)$ (q a power of a prime p), which is a subgroup of $G = \mathrm{SL}(n, \overline{\mathbb{F}}_p)$, and "$A$ does not grow", in the sense that $|A^3|$ is not much larger than $|A|$. Using an "escape from subvarieties" argument, Helfgott [2011] proved the following useful lemma: *If T is a maximal torus in G then $|T \cap A|$ is not much larger than $|A|^{1/(n+1)}$.* This is natural to expect for dimensional reasons since $\dim T / \dim G = (n-1)/(n^2-1) = 1/(n+1)$.

In particular we see that, if A contains a maximal torus of L, then A is a very large subset of L, hence $A^3 = L$ by Corollary 10. This consequence of Helfgott's lemma is very similar to our baby product theorem.

What is the right generalisation of these results? Our first answer to this question which is subsumed by [Pyber and Szabó 2010, Theorem 49], is the following inequality.

Theorem 24 [Pyber and Szabó 2009]. *Let $\varepsilon > 0$ be a fixed constant. Let G be a linear algebraic group defined over $\mathbb{F}_q$ which satisfies the following conditions*:

(a) *The centraliser of $G(\mathbb{F}_q)$ (the group of $\mathbb{F}_q$-points) in G is finite.*

(b) *$G(\mathbb{F}_q)$ does not normalise any closed subgroup $H < G$ with $0 < \dim H < \dim G$.*

Let $1 \in A$ be a generating set of $G(\mathbb{F}_q)$ and V a subvariety of G of positive dimension. If $A \cap V$ is large enough (i.e., greater than some appropriate function of ε, $\dim G$, and the degrees of the varieties G and V) then

$$|A^m| \geq |A \cap V|^{(1-\varepsilon)\dim G/\dim V},$$

for some m which depends only on ε and $\dim G$.

Taking G to be $\mathrm{SL}(n, \overline{\mathbb{F}}_p)$ and T a maximal torus in G we obtain Helfgott's lemma. Here we use the fact, essential to Helfgott's approach, that if A^3 is not much larger than A then A^m is not much larger either (see Proposition 18).

Breuillard, Green, and Tao arrived at a somewhat stronger inequality [Breuillard et al. 2011a], by taking hints from [Hrushovski 2012]. (Our inequality was obtained in March 2009, independently of [Hrushovski 2012].) For a formulation of their result, which they call a Larsen–Pink type inequality, see [Breuillard 2014] in this volume.

Anyway, the inequality says that if a generating set of $L = \mathrm{SL}(n, q)$ does not grow then it is distributed in a "balanced way" in L.

How do we break this balance? We have to start conjugating! More precisely, we have to answer another question. Which are the "interesting subvarieties" to which Theorem 24 should be applied to? Centralisers and conjugacy classes, as explained below.

For an element x consider the conjugation map $g \to x^g$. The image of this map is $cl(x)$, the conjugacy class of x in G, and the fibres are cosets of the centraliser $\mathscr{C}_G(x)$. For the closure $\overline{cl(x)}$ of the set $cl(x)$ this implies that

$$\dim \mathscr{C}_G(x) + \dim \overline{cl(x)} = \dim G.$$

It follows that an upper bound for $|A \cap \overline{cl(x)}|$ implies a lower bound for $|A \cap \mathscr{C}_G(x)|$ which matches the upper bound given by Theorem 24.

Maximal tori are the centralisers of their regular semisimple elements (that is elements with all eigenvalues distinct).

Let us say that A *covers* a maximal torus T if $|T \cap A|$ contains a regular semisimple element. We obtain a fundamental dichotomy:

Lemma [Pyber and Szabó 2010, Lemma 60]. *Assume that a generating set A does not grow.*

(i) *If A does not cover a maximal torus T then $|T \cap A|$ is not much larger than $|A|^{1/(n+1)-1/(n^2-1)}$.*

(ii) *If A covers T then $|T \cap AA^{-1}|$ is not much smaller than $|A|^{1/(n+1)}$.*

To break the balance when A is not very large, we only have to start conjugating tori with elements of A. That is, an argument analogous to the proof of our baby product theorem based on the above dichotomy completes the proof of the product theorem.

4. On the proof of the polynomial inverse theorem

A large part of the proof of the polynomial inverse theorem (Theorem 8), which is already contained in [Pyber and Szabó 2010], is to show that if S is a symmetric subset of $\mathrm{GL}(n, \overline{\mathbb{F}})$ such that $|S^3| \leq K|S|$, then S is contained in the union of polynomially many cosets of a soluble-by-finite subgroup.

For the proof of this we first establish a generalisation of Theorem 24, called the spreading theorem [Pyber and Szabó 2010, Theorem 49]. Roughly speaking it says the following.

For a subvariety V of positive dimension we define the *concentration* of a finite set S in V as $(\log|S \cap V|)/\dim V$.

Let S be a finite subset in a connected linear algebraic group G such that $\mathscr{C}_G(S)$ is finite. If G has a subvariety X in which S has much larger concentration than in G then we can find a connected closed subgroup $H \leq G$ normalised by S in which a small power of S has similarly large concentration. (When G is the simple algebraic group used to define a finite group of Lie type L and S generates L then H turns out to be G itself.)

Next we have to introduce certain "generalised tori". If G is a simple algebraic group then a maximal torus T can be obtained as the centraliser of a regular semisimple element of T. Moreover, most elements of T are regular semisimple. Since T is abelian, it coincides with its centraliser $\mathscr{C}_G(T)$.

In an arbitrary nonnilpotent linear algebraic group G we consider a class of subgroups we call CCC-subgroups with similar properties. Our CCC-subgroups are the connected centralisers of connected subgroups (which explains the name).

For a subvariety X denote by X^{gen} the set of all $(\dim G)$-tuples $\underline{g} \in \prod^{\dim G} X$ such that the connected centralisers $\mathscr{C}_G(\underline{g})^0$ and $\mathscr{C}_G(X)^0$ are equal.

It turns out that if X is a CCC-subgroup then X^{gen} is a dense open subset of $\prod^{\dim G} X$. Moreover, if Y is another CCC-subgroup, then $X^{\mathrm{gen}} \cap Y^{\mathrm{gen}} = \varnothing$. Finally we have $\mathscr{C}_G(\mathscr{C}_G(X)^0)^0 = X$.

If we replace the tori in the proof of the product theorem with CCC-subgroups, the proof goes through, and shows that a small power of S has very large concentration in some subgroup H of G normalised by S.

An induction argument then shows that S is contained in polynomially many cosets of some soluble-by-finite subgroup, as we wanted.

With various additional arguments this result can be upgraded as follows.

Theorem 25 [Pyber and Szabó 2010]. *Let* $1 \in S$ *be a finite symmetric subset of* $\mathrm{GL}(n, \mathbb{F})$ *such that* $|S^3| \leq K|S|$ *for some* $K \geq 1$. *Then* S *can be covered by polynomially many cosets of some soluble-by-finite subgroup* Γ *normalised by* S. *Moreover*, Γ *has a soluble normal subgroup* H *such that* $\Gamma \subset S^6 H$.

This is essentially a polynomial version of a result of Hrushovski [2012].

Since a soluble-by-finite subgroup of $\mathrm{GL}(n, \mathbb{C})$ has a soluble subgroup of bounded index, Theorem 25 implies the polynomial inverse theorem for fields of characteristic zero. As mentioned before, the characteristic zero case was first obtained in [Breuillard et al. 2011a].

In the rest of this section $\mathbb{F}$ denotes a field of characteristic $p > 0$.

To complete the proof of Theorem 8 next we have to settle the case of finite linear groups.

Definition 26. As usual, $O_p(G)$ denotes the maximal normal p-subgroup of a finite group G. A group is called *perfect*, if it has no abelian quotients. A finite group is called *quasisimple* if it is a perfect central extension of a finite simple group. We denote by $\mathrm{Lie}^*(p)$ the set of central products of quasisimple groups of Lie type of characteristic p.

The following deep result is essentially due to Weisfeiler [1984].

Proposition 27. *Let* G *be a finite subgroup of* $\mathrm{GL}(n, \mathbb{F})$. *Then* G *has a normal subgroup* H *of index at most* $f(n)$ *such that* $H \geq O_p(G)$ *and* $H/O_p(G)$ *is the central product of an abelian* p'*-group and quasisimple groups of Lie type of characteristic* p, *where the bound* $f(n)$ *depends on* n.

It was proved by Collins [2008] that for $n \geq 71$ one can take $f(n) = (n+2)!$. Remarkably a (noneffective) version of the above result was obtained by Larsen and Pink [2011] without relying on the classification of finite simple groups.

It is an easy consequence of Weisfeiler's theorem, that if $\deg_{\mathbb{C}}(G)$ is "large" then in fact $G/O_p(G)$ is in $\mathrm{Lie}^*(p)$. For such groups one can use Lemma 22 inductively to prove that if a symmetric set S with $|S^3| \leq K|S|$ projects onto $G/O_p(G)$, then in fact $S^3 = G$.

This result, and the product theorem are the main ingredients in the proof of the polynomial inverse theorem at least in the case finite linear groups.

The following classical theorem of Malcev (see, e.g., [Wehrfritz 1973]) makes it possible to use finite group theory to study properties of finitely generated linear groups.

Proposition 28. *Let* Γ *be a finitely generated subgroup of* $\mathrm{GL}(n, \mathbb{F})$. *For every finite set of elements* $g_1, \dots, g_t$ *of* Γ *there exists a finite field* $\mathbb{K}$ *of the same characteristic and a homomorphism* $\phi : \Gamma \to \mathrm{GL}(n, \mathbb{K})$ *such that* $\phi(g_1), \dots, \phi(g_t)$ *are all distinct.*

In the final part of the proof of the polynomial inverse theorem we have to further upgrade Theorem 25. Due to some lucky coincidences this can be done by combining the finite case with Malcev's theorem.

References

[Alon et al. 2001] N. Alon, A. Lubotzky, and A. Wigderson, "Semi-direct product in groups and zig-zag product in graphs: Connections and applications (extended abstract)", pp. 630–637 in *42nd IEEE Symposium on Foundations of Computer Science* (Las Vegas, 2001), IEEE Computer Soc., Los Alamitos, CA, 2001.

[Babai and Seress 1992] L. Babai and Á. Seress, "On the diameter of permutation groups", *European J. Combin.* **13**:4 (1992), 231–243.

[Babai and Sós 1985] L. Babai and V. T. Sós, "Sidon sets in groups and induced subgraphs of Cayley graphs", *European J. Combin.* **6**:2 (1985), 101–114.

[Babai et al. 2008] L. Babai, N. Nikolov, and L. Pyber, "Product growth and mixing in finite groups", pp. 248–257 in *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, ACM, New York, 2008.

[Bourgain and Gamburd 2008] J. Bourgain and A. Gamburd, "Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$", *Ann. of Math.* (2) **167**:2 (2008), 625–642.

[Breuillard 2014] E. Breuillard, "A brief introduction to approximate groups", pp. 23–50 in *Thin groups and superstrong approximation*, edited by H. Oh and E. Breuillard, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014.

[Breuillard and Green 2011] E. Breuillard and B. Green, "Approximate groups, II: The solvable linear case", *Q. J. Math.* **62**:3 (2011), 513–521.

[Breuillard et al. 2011a] E. Breuillard, B. Green, and T. Tao, "Approximate subgroups of linear groups", *Geom. Funct. Anal.* **21**:4 (2011), 774–819.

[Breuillard et al. 2011b] E. Breuillard, B. Green, and T. Tao, "Suzuki groups as expanders", *Groups Geom. Dyn.* **5**:2 (2011), 281–299.

[Breuillard et al. 2012a] E. Breuillard, B. Green, R. Guralnick, and T. Tao, "Strongly dense free subgroups of semisimple algebraic groups", *Israel J. Math.* **192**:1 (2012), 347–379.

[Breuillard et al. 2012b] E. Breuillard, B. Green, and T. Tao, "The structure of approximate groups", *Publ. Math. IHES* **116**:1 (2012), 115–221.

[Breuillard et al. 2013] E. Breuillard, B. Green, R. Guralnick, and T. Tao, "Expansion in finite simple groups of Lie type", preprint, 2013. arXiv 1309.1975

[Collins 2008] M. J. Collins, "Modular analogues of Jordan's theorem for finite linear groups", *J. Reine Angew. Math.* **624** (2008), 143–171.

[Dinai 2011] O. Dinai, "Growth in SL_2 over finite fields", *J. Group Theory* **14**:2 (2011), 273–297.

[Elekes and Király 2001] G. Elekes and Z. Király, "On the combinatorics of projective mappings", *J. Algebraic Combin.* **14**:3 (2001), 183–197.

[Ellers et al. 1999] E. W. Ellers, N. Gordeev, and M. Herzog, "Covering numbers for Chevalley groups", *Israel J. Math.* **111** (1999), 339–372.

[Gamburd et al. 2009] A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev, and B. Virág, "On the girth of random Cayley graphs", *Random Structures Algorithms* **35**:1 (2009), 100–117.

[Gill and Helfgott 2010] N. Gill and H. Helfgott, "Growth in solvable subgroups of $\mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})$", preprint, 2010. arXiv 1008.5264

[Gill et al. 2011] N. Gill, L. Pyber, I. Short, and E. Szabó, "On the product decomposition conjecture for finite simple groups", preprint, 2011. Accepted in *Groups, Geometry, and Dynamics*. arXiv 1111.3497

[Gowers 2008] W. T. Gowers, "Quasirandom groups", *Combin. Probab. Comput.* **17**:3 (2008), 363–387.

[de la Harpe 2000] P. de la Harpe, *Topics in geometric group theory*, University of Chicago Press, Chicago, IL, 2000.

[Helfgott 2008] H. A. Helfgott, "Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$", *Ann. of Math.* (2) **167**:2 (2008), 601–623.

[Helfgott 2011] H. A. Helfgott, "Growth in $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$", *J. Eur. Math. Soc.* **13**:3 (2011), 761–851.

[Hrushovski 2012] E. Hrushovski, "Stable group theory and approximate subgroups", *J. Amer. Math. Soc.* **25**:1 (2012), 189–243.

[Hrushovski and Pillay 1995] E. Hrushovski and A. Pillay, "Definable subgroups of algebraic groups over finite fields", *J. Reine Angew. Math.* **462** (1995), 69–91.

[Kassabov 2007] M. Kassabov, "Symmetric groups and expander graphs", *Invent. Math.* **170**:2 (2007), 327–354.

[Kassabov et al. 2006] M. Kassabov, A. Lubotzky, and N. Nikolov, "Finite simple groups as expanders", *Proc. Natl. Acad. Sci. USA* **103**:16 (2006), 6116–6119.

[Kleidman and Liebeck 1990] P. Kleidman and M. Liebeck, *The subgroup structure of the finite classical groups*, London Math. Soc. Lecture Note Series **129**, Cambridge University Press, 1990.

[Landazuri and Seitz 1974] V. Landazuri and G. M. Seitz, "On the minimal degrees of projective representations of the finite Chevalley groups", *J. Algebra* **32** (1974), 418–443.

[Larsen and Pink 2011] M. J. Larsen and R. Pink, "Finite subgroups of algebraic groups", *J. Amer. Math. Soc.* **24**:4 (2011), 1105–1158.

[Larsen et al. 2011] M. Larsen, A. Shalev, and P. H. Tiep, "The Waring problem for finite simple groups", *Ann. of Math.* (2) **174**:3 (2011), 1885–1950.

[Lawther and Liebeck 1998] R. Lawther and M. W. Liebeck, "On the diameter of a Cayley graph of a simple group of Lie type based on a conjugacy class", *J. Combin. Theory Ser. A* **83**:1 (1998), 118–137.

[Liebeck and Pyber 2001] M. W. Liebeck and L. Pyber, "Finite linear groups and bounded generation", *Duke Math. J.* **107**:1 (2001), 159–171.

[Liebeck and Shalev 2001] M. W. Liebeck and A. Shalev, "Diameters of finite simple groups: sharp bounds and applications", *Ann. of Math.* (2) **154**:2 (2001), 383–406.

[Liebeck et al. 2011] M. W. Liebeck, N. Nikolov, and A. Shalev, "Groups of Lie type as products of SL_2 subgroups", *J. Algebra* **326** (2011), 201–207.

[Liebeck et al. 2012] M. W. Liebeck, N. Nikolov, and A. Shalev, "Product decompositions in finite simple groups", *Bull. Lond. Math. Soc.* **44**:3 (2012), 469–472.

[Lubotzky 2011] A. Lubotzky, "Finite simple groups of Lie type as expanders", *J. Eur. Math. Soc.* **13**:5 (2011), 1331–1341.

[Lubotzky 2012] A. Lubotzky, "Expander graphs in pure and applied mathematics", *Bull. Amer. Math. Soc.* (*N.S.*) **49**:1 (2012), 113–162.

[Lubotzky and Weiss 1993] A. Lubotzky and B. Weiss, "Groups and expanders", pp. 95–109 in *Expanding graphs* (Princeton, NJ, 1992), edited by J. Friedman, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **10**, Amer. Math. Soc., Providence, RI, 1993.

[Meshulam and Wigderson 2004] R. Meshulam and A. Wigderson, "Expanders in group algebras", *Combinatorica* **24**:4 (2004), 659–680.

[Nikolov and Pyber 2011] N. Nikolov and L. Pyber, "Product decompositions of quasirandom groups and a Jordan type theorem", *J. Eur. Math. Soc.* **13**:4 (2011), 1063–1077.

[Nikolov and Segal 2007a] N. Nikolov and D. Segal, "On finitely generated profinite groups, I: Strong completeness and uniform bounds", *Ann. of Math.* (2) **165**:1 (2007), 171–238.

[Nikolov and Segal 2007b] N. Nikolov and D. Segal, "On finitely generated profinite groups, II: Products in quasisimple groups", *Ann. of Math.* (2) **165**:1 (2007), 239–273.

[Nikolov and Segal 2011] N. Nikolov and D. Segal, "Powers in finite groups", *Groups Geom. Dyn.* **5**:2 (2011), 501–507.

[Nikolov and Segal 2012] N. Nikolov and D. Segal, "Generators and commutators in finite groups; abstract quotients of compact groups", *Invent. Math.* **190**:3 (2012), 513–602.

[Pyber and Szabó 2009] L. Pyber and E. Szabó, "Generating simple groups", preprint, 2009, http://www.renyi.hu/~endre/growth.pdf.

[Pyber and Szabó 2010] L. Pyber and E. Szabó, "Growth in finite simple groups of Lie type of bounded rank", preprint, 2010. arXiv 1005.1858

[Pyber and Szabó $\geq$ 2012] L. Pyber and E. Szabó, "A polynomial inverse theorem in linear groups", in preparation.

[Ruzsa 2010] I. Z. Ruzsa, "Towards a noncommutative Plünnecke-type inequality", pp. 591–605 in *An irregular mind*, edited by I. Bárány and J. Solymosi, Bolyai Soc. Math. Stud. **21**, János Bolyai Math. Soc., Budapest, 2010.

[Ruzsa and Turjányi 1985] I. Z. Ruzsa and S. Turjányi, "A note on additive bases of integers", *Publ. Math. Debrecen* **32**:1-2 (1985), 101–104.

[Sarnak and Xue 1991] P. Sarnak and X. X. Xue, "Bounds for multiplicities of automorphic representations", *Duke Math. J.* **64**:1 (1991), 207–227.

[Shalev 2009] A. Shalev, "Word maps, conjugacy classes, and a noncommutative Waring-type theorem", *Ann. of Math.* (2) **170**:3 (2009), 1383–1416.

[Tao 2012] T. Tao, "The Bourgain–Gamburd expansion machine", Blog post, 2012, http://goo.gl/7lF86.

[Varjú 2012] P. P. Varjú, "Expansion in $\mathrm{SL}_d(\mathbb{O}_K/I)$, I square-free", *J. Eur. Math. Soc.* **14**:1 (2012), 273–305.

[Wehrfritz 1973] B. A. F. Wehrfritz, *Infinite linear groups. An account of the group-theoretic properties of infinite groups of matrices*, Ergebnisse der Mat. **76**, Springer, New York, 1973.

[Weisfeiler 1984] B. Weisfeiler, "Post-classification version of Jordan's theorem on finite linear groups", *Proc. Nat. Acad. Sci. U.S.A.* **81**:16, Phys. Sci. (1984), 5278–5279.

pyber@renyi.hu

A. Rényi Institute of Mathematics, Hungarian Academy of Sciences, P.O. Box 127, H-1364 Budapest, Hungary

endre@renyi.hu

A. Rényi Institute of Mathematics, Hungarian Academy of Sciences, P.O. Box 127, H-1364 Budapest, Hungary