LINEAR APPROXIMATE GROUPS

EMMANUEL BREUILLARD, BEN GREEN, AND TERENCE TAO

ABSTRACT. This is an informal announcement of results to be described and proved in detail in [3]. We give various results on the structure of approximate subgroups in linear groups such as $\mathrm{SL}_n(k)$. For example, generalising a result of Helfgott (who handled the cases $n = 2$ and 3), we show that any approximate subgroup of $\mathrm{SL}_n(\mathbb{F}_q)$ which generates the group must be either very small or else nearly all of $\mathrm{SL}_n(\mathbb{F}_q)$. The argument is valid for all Chevalley groups $G(\mathbb{F}_q)$.

CONTENTS

1. INTRODUCTION

In this note we announce some new results on approximate subgroups in linear groups. We begin by recalling the notion of an approximate group, first introduced (in the non-abelian setting) in [29]. See [19] for a more extensive motivating discussion.

Definition 1.1 (Approximate groups). *Let $K \geqslant 1$. A nonempty finite set A in some ambient group G is called a K-approximate group if*

(i) *It is symmetric, i.e. if $a \in A$ then $a^{-1} \in A$, and the identity lies in A;*

(ii) *There is a symmetric subset $X \subseteq G$ with $|X| \leqslant K$ such that $A \cdot A \subseteq X \cdot A$, where $A \cdot A = \{a_1 a_2 : a_1, a_2 \in A\}$ is the product set of A with itself.*

Note in particular that a 1-approximate group in G is the same thing as a finite subgroup of G. For the rest of the paper we will assume that $K \geqslant 2$, and in this regime there are K-approximate groups which are not close to genuine groups; the simplest

---

1991 *Mathematics Subject Classification.* 20G40, 20N99 .

example is that of a geometric progression $\{g^n : |n| \leqslant N\}$, and there also exist higher-dimensional and nilpotent generalisations of this. Again, [19] may be consulted for further discussion.

Many papers have been written in which the aim is to classify a certain class of approximate groups. For example, the Freĭman-Ruzsa theorem [28] provides a description of approximate subgroups of the integers $\mathbb{Z}$. "Classification" in this context must be interpreted quite loosely. The following notion of *control*, first introduced in [30], has proved very useful in this context.

Definition 1.2 (Control). *Suppose that A and B are two sets in some ambient group, and that $K \geqslant 1$ is a parameter. We say that A is K-controlled by B, or that B K-controls A, if $|B| \leqslant K|A|$ and there is some set X in the ambient group with $|X| \leqslant K$ and such that $A \subseteq (X \cdot B) \cap (B \cdot X)$.*

Given this definition, one may describe the classification problem for approximate groups as follows: given some class $\mathcal{C}$ of approximate groups, find some smaller, more highly-structured, class of approximate groups $\mathcal{C}'$ such that every object in $\mathcal{C}$ is efficiently controlled by an object in $\mathcal{C}'$.

NOTATION. The letter C always denotes an absolute constant, but different instances of the notation may refer to different constants. If C depends on some other parameter (for example, if we are working in SL_n, C might need to depend on n) then we will indicate this dependence with subscripts. If A is a finite set then $|A|$ denotes the cardinality of A. The letter K is reserved for the positive real parameter appearing in the definition of approximate group. For non-negative quantities X, Y, we use $X \lesssim Y$ or $Y \gtrsim X$ to denote the estimate $X \leqslant K^C Y$, and $X \sim Y$ to denote the estimates $X \lesssim Y \lesssim X$. The symbol p always denotes a prime number, and $\mathbb{F}_p$ denotes the field of order p. Finally, we use $A^k := \{a_1 \ldots a_k : a_1, \ldots, a_k \in A\}$ to denote the k-fold product set of a collection A of group elements, noting that if A is a K-approximate group then $|A^k| \leqslant K^{k-1}|A|$ for all positive integers k.

model-theoretic work of Hrushovski [23], without which we would not have started this project.

NOTE ADDED IN PROOF. Simultaneously with the release of this announcement, Pyber and Szabo[27] have independently announced a set of results which have significant overlap with those presented here, in particular establishing an alternate proof of Theorem 2.3. There are some similarities in common in the argument (in particular, in the reliance on Lemma 4.2) but the arguments and results are slightly different in other respects.

2. STATEMENT OF RESULTS

In a celebrated paper [21], H. Helfgott provided a satisfactory solution to the classification problem for the group $\mathrm{SL}_2(\mathbb{F}_p)$. His methods adapt easily to (and in fact are rather easier in) $\mathrm{SL}_2(\mathbb{C})$, which was studied earlier by Chang [10]. His arguments give the following result.

Theorem 2.1 (Helfgott). *Suppose that $A \subseteq \mathrm{SL}_2(k)$ is a K-approximate group.*

  (i) *If $k = \mathbb{C}$ then A is K^C-controlled by B, an* abelian *K^C-approximate subgroup of $\mathrm{SL}_2(k)$;*
  (ii) *If $k = \mathbb{F}_p$ then A is K^C-controlled either by a* solvable *K^C-approximate subgroup of $\mathrm{SL}_2(k)$ or by $\mathrm{SL}_2(k)$ itself.*

Helfgott's theorem has found many applications, for example to proving that certain Cayley graphs are expanders [4] and to certain nonlinear sieving problems [7]. For these applications only the following somewhat weaker statement is necessary.

Theorem 2.2 (Helfgott). *Suppose that $A \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ is a K-approximate group that generates $\mathrm{SL}_2(\mathbb{F}_p)$. Then A is K^C-controlled by either $\{id\}$ or by $\mathrm{SL}_2(\mathbb{F}_p)$ itself.*

Very recently, this result has been extended to fields $\mathbb{F}_q$ of prime power order $q = p^j$ by Dinai[14]. An extension to $\mathrm{SL}_n(\mathbb{F}_p)$ in the case of small A (specifically, $|A| \leqslant p^{n+1-\delta}$ for some $\delta > 0$) was also recently announced by Gill and Helfgott[17].

The proof that such a statement suffices for the sieving work of Bourgain, Gamburd and Sarnak [7] is contained in a very recent preprint of Varjú [33]; the original argument of [7] required a careful analysis of the *proof* of Helfgott's result.

Our first main result generalises Theorem 2.2 as follows.

Theorem 2.3. *Let k be a finite field. Suppose that $A \subseteq \mathrm{SL}_n(k)$ is a K-approximate group that generates $\mathrm{SL}_n(k)$. Then A is K^{C_n}-controlled by either $\{\mathrm{id}\}$ or by $\mathrm{SL}_n(k)$ itself.*

In a much longer second paper [22], Helfgott proved this result when $n = 3$, at least in the case when $k = \mathbb{F}_p$ is a prime field. It is known, thanks to work of Bourgain-Gamburd [5] and Varjú [33] respectively, that such a statement suffices in order to fully generalise the aforementioned results on expanders and on the affine sieve. We shall state some of these applications and others in §7.

In proving Theorem 2.3 we can quote extensively from Helfgott's paper [22]. However the structure of the proof seems clearer when one establishes the following result of greater generality.

Theorem 2.4. *Let k be a finite field and let $G(k)$ be a Chevalley group[1]. Suppose that $A \subseteq G(k)$ is a K-approximate group that generates $G(k)$. Then A is $K^{C_{\dim(G)}}$-controlled by either $\{\mathrm{id}\}$ or by $G(k)$ itself.*

Note that the constant $C_{\dim(G)}$ does not depend on the field k.

There is a more significant advantage of working in simple groups more general that SL_n. Over $\mathbb{C}$, for example, the general structure theory of algebraic groups implies, roughly speaking, that every Zariski-closed subgroup of $\mathrm{GL}_n(\mathbb{C})$ admits a quotient by a normal solvable subgroup which is a direct product of simple complex Lie groups. By exploiting this theory, an analogue of Theorem 2.3 over $\mathbb{C}$, and the main result of [2], we are able to establish the following result.

Theorem 2.5. *Suppose that $A \subseteq \mathrm{GL}_n(\mathbb{C})$ is a K-approximate subgroup. Then A is CK^{C_n}-controlled by B, a CK^{C_n}-approximate group that generates a nilpotent group of nilpotency class (step) at most $n - 1$.*

We are also able to say something about the structure of K-approximate subgroups of $\mathrm{GL}_n(k)$ where k is a finite field, at least in the case $k = \mathbb{F}_p$, but this seems to be very substantially more difficult and it is not yet clear what the final form of such a result will be.

Qualitative forms of the above theorems follow from the work of Hrushovski [23]. The main novelty of our work lies in the polynomial dependence on the approximation parameter K, which is absolutely essential for applications. The powers C_n and $\dim(G)$ are in principle explicitly computable. However, if one is willing to sacrifice such information a key portion of the argument (the proof of the Larsen-Pink inequalities, described in §5) can be significantly simplified by the use of an ultrafilter argument.

---

[1]That is, a group associated to one of the Dynkin diagrams $A_n, B_n, C_n, D_n, E_6, E_7, E_8, F_4$ or G_2. It is likely that our results hold in greater generality (for example for all simple groups of Lie type) but we have not yet checked this.

3. A new proof of Helfgott's SL_2 result

To illustrate the main ideas in our paper, we give a reasonably detailed sketch of the proof of Theorem 2.3 in the case $n = 2$. The result is due to Helfgott, at least when $k = \mathbb{F}_p$ is a prime field. So are some of the ideas, and indeed we begin by quoting a lemma from [21]. Recall that a *maximal torus* of $\mathrm{SL}_2(\overline{k})$ a maximal, connected, abelian, diagonalisable algebraic subgroup of $\mathrm{SL}_2(\overline{k})$, or in other words a subgroup conjugate to the group $\{\left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{smallmatrix}\right) : \lambda \neq 0\}$ of diagonal matrices.

Throughout this section, k is a finite field and $A \subseteq \mathrm{SL}_2(k)$ is a K-approximate group generating $\mathrm{SL}_2(k)$. We make free use of the notation $\sim, \lesssim, \gtrsim$ introduced in the introduction, all with reference to this same parameter K.

Lemma 3.1 (Helfgott). *Let $T \subseteq \mathrm{SL}_2(\overline{k})$ be a maximal torus containing at least one element of A other than the identity. Then*

$$|A^{20} \cap T| \sim |A|^{1/3}.$$

The upper bound is [22, Corollary 5.4], whilst the lower bound follows from [22, Corollary 5.10] (or rather the proof of it). Helfgott does not explicitly obtain the power 20 but it is likely that this would follow from his arguments; in any case the exact power is totally unimportant for this sketch.

Helfgott established an analogous result in SL_n for $n \geqslant 3$ under the assumption that T contains a *regular semisimple* element of A, that is to say a matrix with distinct eigenvalues. Note that a special feature of SL_2 is that all semisimple (diagonalisable) elements other than $\pm\,\mathrm{id}$ are regular semisimple. One of the main ingredients of our paper is a further generalisation of the upper-bound portion of Lemma 3.1 to the case where SL_2 is replaced by an arbitrary simple group of Lie type and T is replaced by an arbitrary algebraic subvariety V of bounded "complexity". To do this we adapt an argument of Larsen and Pink [24]; the details are sketched in §5. In the special case that V is a torus containing a regular semisimple element of A we can obtain a corresponding *lower* bound by placing an upper bound on the intersection of $A^{O(1)}$ with conjugacy classes, much as Helfgott does in [21, 22]. This is discussed further in §5, and in this way we obtain a complete generalisation of Lemma 3.1 to arbitrary Chevalley groups.

Returning now to the SL_2 setting, let us say that a torus $T \subseteq \mathrm{SL}_2(k)$ is *involved* with A if $A^2 \cap T$ contains at least one regular semisimple element of A (which, in the case of $\mathrm{SL}_2(k)$, is equivalent to asserting that $A^2 \cap T$ is not contained in $\{\mathrm{id}, -\,\mathrm{id}\}$). The crucial observation concerning this notion is as follows.

Lemma 3.2 (Conjugation invariance in SL_2). *Suppose that $|A| > CK^C$ for a sufficiently large C. Then the set of involved tori is invariant under conjugation by all elements of $\mathrm{SL}_2(k)$.*

Proof. Since A generates $\mathrm{SL}_2(k)$, it suffices to show that if T is involved and if $a \in A$ then $\tilde{T} := a^{-1}Ta$ is also involved. Let us look at the sets xTy as x, y range over A^2. These are all cosets of tori in $\mathrm{SL}_2(\overline{k})$ and, by Lemma 3.1, there are $\lesssim |A|^{4/3}$ of them, since for each fixed $x, y \in A^2$ there are $\gtrsim |A|^{1/3}$ values of $x' \in A^{22}$ with $xT = x'T$ and $\gtrsim |A|^{1/3}$ values of $y' \in A^{22}$ with $Ty = Ty'$, yet the total number of cosets $x'Ty'$ with $x', y' \in A^{22}$ is at most $|A^{22}|^2 \lesssim |A|^2$. *A fortiori* there are $\lesssim |A|^{4/3}$ sets of the form $x\tilde{T}y$ as x, y range over A.

By the pigeonhole principle, we can thus find $m \gtrsim |A|^{2/3}$ distinct pairs $(b_i, c_i) \in A \times A$, $i = 1, \dots, m$, such that

$$(3.1) \qquad\qquad b_1 \tilde{T} c_1 = \cdots = b_m \tilde{T} c_m.$$

Without loss of generality there are $l \gtrsim |A|^{1/3}$ different values of b_i appearing here, say $b_1, \dots, b_l$. Since each $b_i \tilde{T} b_i^{-1}$ is a subgroup, it is easy to see that (3.1) in fact implies that

$$b_1 \tilde{T} b_1^{-1} = b_2 \tilde{T} b_2^{-1} = \cdots = b_l \tilde{T} b_l^{-1},$$

and hence that $b_1^{-1} b_i$ lies in the normaliser $N_{\mathrm{SL}_2}(\tilde{T})$ for all $i = 1, \dots, l$. But the order of the group $N_{\mathrm{SL}_2}(\tilde{T})/\tilde{T}$ is two (one can easily compute this directly: this group is called the *Weyl group*), and therefore we may find some fixed i and at least $l/2$ values of j such that $(b_1^{-1} b_i)^{-1}(b_1^{-1} b_j) = b_i^{-1} b_j \in \tilde{T}$. This implies that $|A^2 \cap \tilde{T}| \gtrsim |A|^{1/3}$ and hence, *a fortiori*, $\tilde{T}$ is involved. $\square$

Remark. The arguments here were inspired by the proof that every approximate field is almost a field, a general form of the sum-product theorem. The idea originated in [8] and is also described in [31, Section 2.8]. Indeed, if A is a finite subset of a field k, say that an element $\xi \in k$ is *involved* with A if the set $A + \xi A$ has cardinality strictly less than $|A|^2$. If A is approximately closed under addition and multiplication in a certain sense, one can show by arguments not dissimilar to those above that the set of involved elements is finite and is closed under addition and multiplication, i.e. is a genuine finite subfield of k. This might also be a good place to mention that, unlike Helfgott, we make no appeal to results on the sum-product phenomenon. In fact we are able to deduce the sum-product phenomena from Theorem 2.3 in the case $n = 2$ and the so-called Katz-Tao lemma [31, Lemma 2.53], thereby providing a different proof of these results.

Given Lemma 3.2 it is quite an easy matter to complete the proof of Theorem 2.3 in the case $n = 2$. Consider the conjugation action of $G = \mathrm{SL}_2(k)$ on the set $X = \{T_1, \dots, T_m\}$ of involved tori (note that these tori are defined over $\overline{k}$, and need not be defined over k). By another application of Lemma 3.1 and the fact that distinct tori intersect only at $\{\mathrm{id}, -\mathrm{id}\}$ (a special feature of SL_2) it follows that $m \lesssim |A|^{2/3}$.

Thus the orbit of T_1 under this conjugation action has size at most $m \sim |A|^{2/3}$, whereas the stabiliser of T_1 is $N(T_1) \cap G$, a set of size $\sim |G|^{1/3}$ (by direct verification). It follows from the orbit-stabiliser theorem that

$$|A|^{2/3}|G|^{1/3} \gtrsim |G|,$$

and therefore $|A| \gtrsim |G|$. This means, of course, that A is K^C-controlled by G, and the proof is complete. $\qquad\square$

4. Sets that generate SL_n

Let k be a finite field. Let us see what changes must be made to the argument of the previous section in order to make it work when $n \geqslant 3$, that is to say to prove Theorem 2.3 in general. As previously mentioned, the analogue of Lemma 3.1 is the following. Through this section $A \subseteq \mathrm{SL}_n(k)$ is a K-approximate group which generates $\mathrm{SL}_n(k)$. All absolute constants, including those implicit in the $\sim, \lesssim$ and $\gtrsim$ notation, are allowed to depend on n.

Lemma 4.1 (Helfgott). *Suppose that $T \subseteq \mathrm{SL}_n(\overline{k})$ is a maximal torus containing at least one regular semisimple element of A. Then*

$$|A^C \cap T| \sim |A|^{1/(n+1)}.$$

Let us now say that a torus $T \subseteq \mathrm{SL}_n(\overline{k})$ is *involved* with A if $A^2 \cap T$ contains at least one regular semisimple element. We have the following direct analogue of Lemma 3.2.

Lemma 4.2. *Suppose that $|A| \geqslant CK^C$ for sufficiently large $C = C_n$. Then the set of involved tori is invariant under conjugation by the whole group $\mathrm{SL}_n(k)$.*

Proof. The argument is almost exactly the same as that used to prove Lemma 3.2. Everything works in precisely the same way, using the fact that the Weyl group $N_G(T)/T$ is finite and bounded in size independently of k, up until the very last line where it is shown that $|A^2 \cap \tilde{T}| \gtrsim |A|^{1/(n+1)}$. It does not follow quite so immediately from this that $\tilde{T}$ is involved. Writing $\tilde{T}_{\mathrm{rss}}$ for the set of regular semisimple elements of $\tilde{T}$, it suffices to show that

$$|A^2 \cap (\tilde{T} \setminus \tilde{T}_{\mathrm{rss}})| \lesssim |A|^{1/(n+1)-\delta}$$

for some $\delta = \delta_n > 0$. The set $\tilde{T} \setminus \tilde{T}_{\mathrm{rss}}$ is contained in a finite union of "deficient" subtori of dimension at most $n-2$ (note that the dimension of a maximal torus is $n-1$). Hence the key is to bound the number of points of A^2 inside a deficient torus by $\lesssim |A|^{1/(n+1)-\delta}$.

A bound of this type follows from the rather general Larsen-Pink-type inequalities to be presented in the next section, though it may well also follow by modifying Helfgott's approach in [22, Section 5] (which does, in any case, resemble the Larsen-Pink argument). $\qquad\square$

To finish the proof of Theorem 2.3 we proceed much as before, examining the conjugation action of $G = \mathrm{GL}_n(k)$ on the set $X = \{T_1, \ldots, T_m\}$ of involved maximal tori. There is one new issue here, which is that it is not immediately clear that there is even *one* involved torus. That this is so follows from an application of the "escape from subvarieties" Lemma of Eskin-Mozes-Oh [15], much used in Helfgott's papers. This lemma guarantees that, after replacing A by A^C if necessary, that a positive proportion of the elements of A are regular semisimple.

To obtain the bound $m \lesssim |A|^{n/(n+1)}$ we need only combine Lemma 4.1 with the observation that each regular semisimple element of A lies on a *unique* maximal torus. The rest of the argument proceeds as before. □

5. A LARSEN-PINK-TYPE INEQUALITY

Suppose that $A \subseteq G(k)$, where G is a Chevalley group. In the last section we saw, in the case $G = \mathrm{SL}_n$, how useful it is to have upper bounds on $|A \cap V|$ for various varieties V, specifically maximal tori, deficient tori and conjugacy classes (the latter to get the lower bounds for tori in Lemmas 3.1 and 4.1, as described below). It turns out that bounds of this type are available in considerable generality. To obtain them, we adapt an argument of Larsen and Pink [24]. The idea of using the Larsen-Pink inequality was inspired by a similar adaptation of that inequality to a model-theoretic setting in [23].

Thus far, we have been dealing only with finite fields k. When k is uncountably infinite it makes no sense to say that A generates $G(k)$. It turns out that the correct substitute is the notion of *sufficiently Zariski-dense*. We say that $A \subseteq G(\overline{k})$ is M-sufficiently Zariski dense if A is not contained in any proper subvariety of *complexity at most M*, that is to say defined by at most M polynomials of degree at most M. The notion of sufficiently Zariski-dense takes a little getting used to. For example, $A = \mathrm{SL}_2(\mathbb{F}_p)$ is M-sufficiently Zariski-dense in $\mathrm{SL}_2(\overline{\mathbb{F}}_p)$ when $M \geqslant M_0(p)$, even though A generates only a very tiny portion of $\mathrm{SL}_2(\overline{\mathbb{F}}_p)$.

Lemma 5.1 (Larsen-Pink inequality for approximate groups). *Let k be any field, suppose that $G(k)$ is a Chevalley group, and let M be a parameter. Then there is an $M_0 = M_0(G, M)$ with the following property. Suppose that A is M_0-sufficiently Zariski-dense. Then for any subvariety V of complexity at most M we have*

$$|A \cap V| \leqslant C|A^C|^{\dim V / \dim G}$$

where $C = C(G, M)$. In particular, if A is a K-approximate group for some $K \geqslant 1$, then we have

$$(5.1) \qquad |A^m \cap V| \leqslant C_m K^{C_m} |A|^{\dim V / \dim G}$$

for any $m \geqslant 1$, where $C_m = C_m(G, M)$.

Sketch proof. The claim is clear when $\dim V = 0$ and $\dim V = \dim G$. Now suppose for sake of contradiction that there exists dimensions d_-, d_+ with $0 < d_- \leqslant d_+ < \dim G$ and varieties V_-, V_+ of dimensions d_-, d_+ respectively such that the claim fails for V_-, V_+, but holds for varieties of dimensions less than d_- or greater than d_+. Using the hypothesis that G is simple and A is sufficiently Zariski-dense, it is possible to conjugate V_- by an element of A so that $V_- \cdot V_+$ has dimension strictly greater than that of V_+. Now, we consider the product map from $(A \cap V_-) \times (A \cap V_+)$ to $(A^2 \cap (V_- \cdot V_+))$. By hypothesis, the cardinality of $(A^2 \cap (V_- \cdot V_+))$ is at most $C|A^C|^{\dim(V_- \cdot V_+)/\dim G}$. On the other hand, from a further application of the hypothesis, the fibres of this map generically have cardinality at most $C|A^C|^{(\dim(V_-)+\dim(V_+)-\dim(V_- \cdot V_+))/\dim G}$. This implies that $(A \cap V_-) \times (A \cap V_+)$ has cardinality at most $C|A^C|^{(\dim(V_-)+\dim(V_+))/\dim(G)}$, which contradicts the construction of V_-, V_+. $\square$

Several details were suppressed in the above sketch, the most obvious of which were the rather loose use of the word "generic" and of the phrase "sufficiently Zariski-dense". It is possible to proceed carefully and make rigorous sense of the sketch, but this requires some rather painful quantitative algebraic geometry. Alternatively, an ultrafilter argument may be employed ; whilst this eliminates the need for such quantitative work, it does mean that the constants appearing in the statement of Lemma 5.1 are ineffective and hence so, ultimately, are those in Theorems 2.3, 2.4, 2.5 and in the applications described in §7. In the longer paper to follow we present both approaches, though we shall keep our discussion of quantitative algebraic geometry to the minimum required to give a rough shape to the constants appearing in our main theorems.

Let us show how, when $G = \mathrm{SL}_2(\mathbb{F}_p)$ (say), we may use the Larsen-Pink inequality to recover the crucial Lemma 3.1 with the constant 20 replaced by 3. First of all, we observe that if A generates $\mathrm{SL}_2(\mathbb{F}_p)$ then A is sufficiently Zariski dense. This follows from Dickson's classification of proper subgroups of $\mathrm{SL}_2(\mathbb{F}_p)$. Now if $a \neq \mathrm{id}$ lies in some torus T then, since a is regular semisimple, T is equal to the centraliser $Z(a)$. This being an algebraic subvariety of dimension 1, the Larsen-Pink inequality immediately gives us the upper bound in Lemma 3.1, namely the inequality

$$|A^3 \cap T| \lesssim |A|^{1/3}.$$

To get a bound in the other direction write $C(a)$ for the conjugacy class of a in $\mathrm{SL}_2(\overline{\mathbb{F}}_p)$ and examine the map $\pi : A \to A^3 \cap C(a)$ defined by $\pi(x) = x^{-1}ax$. Now $C(a)$ is also an algebraic subvariety, this time of dimension 2 (given by $\{x : \mathrm{tr}\, x = \mathrm{tr}\, a\}$), and thus

another application of the Larsen-Pink inequality tells us that

$$|\operatorname{im}\pi| \lesssim |A|^{2/3}.$$

It follows that some fibre of the map π has size $\gtrsim |A|^{1/3}$; but if x, y are two elements in such a fibre we clearly have $xy^{-1} \in Z(a) = T$. Thus we obtain the lower bound

$$(5.2) \qquad\qquad |A^3 \cap T| \gtrsim |A|^{1/3}$$

as well. Let us note once again that the preceding argument is very close to one used by Helfgott in [21] and [22].

Let us conclude this section with some remarks on the proof of Theorem 2.4. The argument is exactly the same as the one we sketched for SL_2 in Section 3, except that the required estimates for points on tori and degenerate tori come from the Larsen-Pink inequalities rather than Helfgott's papers and one needs a little algebraic group theory to establish basic properties of the maximal tori of $G(\overline{k})$ and, in particular, the finiteness of the Weyl group $N_G(T)/T$.

6. Sketch proof of Theorem 2.5.

In this section we outline, very briefly, the ideas behind the proof of Theorem 2.5. Recall that in this theorem it was claimed that approximate subgroups of $\mathrm{GL}_n(\mathbb{C})$ are controlled by nilpotent approximate groups.

Let $A \subseteq \mathrm{GL}_n(\mathbb{C})$ be a K-approximate group. The first step of the argument is to show that A is sufficiently Zariski-dense inside *some* algebraic subgroup $G \subseteq \mathrm{GL}_n(\mathbb{C})$ of bounded complexity, and this is achieved by a dimension descent argument.

If G is simple we are already done by Theorem 2.3: in fact $|A| \leqslant K^C$. It follows quickly that the same conclusion holds when G is semisimple (has trivial solvable radical), in which case it is known from the theory of algebraic groups that G is an almost direct product of almost-simple groups. For a general G, we may consider the image of A under the projection $G \to G/\mathrm{Rad}(G)$ onto the semisimple part of G which, by the preceding discussion, is bounded in size by K^C. This easily implies that A is K^C-controlled by a K^C-approximate subgroup of $\mathrm{Rad}(G)$, a solvable group. Finally, this in turn is $K^{C'}$-controlled by a nilpotent $K^{C'}$-approximate group B' by the main result of [2]. If desired, that same paper could be used to further control A by a *nilpotent progression*. $\qquad\square$

7. Applications and further remarks

Some applications of our results regarding the diameter of finite simple groups are mentioned in Helfgott's paper [21] in the SL_2 case and the proofs adapt straightforwardly

to the more general case. For example we get a special case of a conjecture of Babai and Seress ([1, Conjecture 1.7]).

Theorem 7.1 (Diameter of $G(\mathbb{F}_p)$)**.** *Let G be a Chevalley group. Then there is a constant $C = C(G) > 0$ such that the diameter of* every *Cayley graph of $G(\mathbb{F}_p)$ is at most $C \log^C p$.*

Similarly we obtain a logarithmic bound $O(\log p)$ on the diameter of those Cayley graphs of $G(\mathbb{F}_p)$ that are obtained as reduction mod p of a subset of $G(\mathbb{Z})$ which generates a Zariski-dense subgroup, using the strong approximation theorem of Matthews-Weisfeiler-Vasserstein [25] and the Tits alternative [32] to get a logarithmic lower bound on the girth of the Cayley graphs. The same logarithmic bound on the diameter also holds for random Cayley graphs of $G(\mathbb{F}_p)$, because the girth of a random Cayley graph of $G(\mathbb{F}_p)$ is at least logarithmic in p by a result of Gamburd et al. [16].

Helfgott's results on SL_2 were spectacularly applied by Bourgain and Gamburd [4] to show that various families of Cayley graphs on $\mathrm{SL}_2(\mathbb{F}_p)$ are expanders.

In subsequent work of Bourgain and Gamburd [5] and [6], the following theorem is obtained modulo our Theorem 2.3 for SL_n. The following, then, is now unconditional.

Theorem 7.2 (Quotients of $\mathrm{SL}_n(\mathbb{Z})$ as expanders)**.** *Let $n \geqslant 2$. Suppose that S is a finite symmetric subset of $\mathrm{SL}_n(\mathbb{Z})$ generating a Zariski dense subgroup, and write S_p for the reduction of S modulo p. Then the Cayley graphs $\mathcal{G}(\mathrm{SL}_n(\mathbb{F}_p), S_p)$ form a family of expanders as $p \to \infty$.*

It is very likely that the methods of [5, 6] extend to all simple Chevalley groups $G(\mathbb{Z})$, though we have not checked this. If so Theorem 7.2 would hold in that case too.

Finally let us mention once again that as a consequence of our results and the paper of Varjú [33] the "affine sieve" of Bourgain, Gamburd and Sarnak [7] may be applied in much more general contexts. We refer the reader to Varjú's paper for details.

References

[1] L. Babai, A. Seress, *On the diameter of permutation groups*, European J. Combin. 13 (1992),no. 4, 231243.

[2] E. Breuillard, B. Green, *Approximate groups II : the solvable linear case*, preprint arXiv:0907.0927, to appear in Quart. J. of Math.

[3] E. Breuillard, B. Green, T. Tao, *Approximate subgroups of linear groups*, preprint.

[4] J. Bourgain, A. Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. of Math. (2) 167 (2008), no. 2, 625–642.

[5] J. Bourgain, A. Gamburd, *Expansion and random walks in* $SL_d(\mathbb{Z}/p^n\mathbb{Z})$ *II, With an appendix by Bourgain*, J. Eur. Math. Soc. (JEMS) 11 (2009), no. 5, 1057–1103.

[6] J. Bourgain, A. Gamburd, *Expansion and random walks in* $SL_d(\mathbb{Z}/p^n\mathbb{Z})$ *I*, J. Eur. Math. Soc. (JEMS) 10 (2008), no. 4, 987–1011.

[7] J. Bourgain, A. Gamburd, P. Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math, Springeronline (2009).

[8] J. Bourgain, A. Glibichuk, S. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) **73** (2006), no. 2, 380–398.

[9] M.-C. Chang, *Convolution of discrete measures on linear groups*, J. Funct. Anal. **253** (2007), no. 1, 303–323.

[10] M.-C. Chang, *Product theorems in SL_2 and SL_3*, J. Math. Jussieu 7 (1) (2008), pp. 125.

[11] M.-C. Chang, *On product sets in SL_2 and SL_3*, preprint.

[12] M.-C. Chang, *Some consequences of the polynomial Freiman-Ruzsa conjecture*, C. R. Math. Acad. Sci. Paris 347 (2009), no. 11-12, 583–588.

[13] L.E. Dickson, *Linear groups with an exposition of Galois Field Theory*, Chapter XII, Cosimo classics, New York, (2007).

[14] O. Dinai, *Expansion properties of finite simple groups*, preprint.

[15] A. Eskin, S. Mozes, H. Oh, *On uniform exponential growth for linear groups* Invent. Math. 160 (2005), no. 1, 1–30.

[16] A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev, B. Virag, *On the girth of random Cayley graphs*, Random Structures Algorithms 35 (2009), no. 1, 100–117.

[17] N. Gill, H. Helfgott, *Growth of small generating sets in $SL_n(\mathbb{Z}/p\mathbb{Z})$*, preprint.

[18] T. Gowers, *Quasirandom groups*, Combin. Probab. Comput. **17** (2008), no. 3, 363–387

[19] B. Green, *Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak*, preprint.

[20] M. Gromov, *Groups of polynomial growth and expanding maps*, Inst. Hautes Études Sci. Publ. Math. No. **53** (1981), 53–73.

[21] H. Helfgott, *Growth and generation in* $SL_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. (2) 167 (2008), no. 2, 601–623.

[22] H. Helfgott, *Growth in $SL_3(Z/pZ)$*, preprint (2008) arXiv:0807.2027.

[23] E. Hrushovski, *Stable group theory and approximate subgroups*, preprint (2009) arXiv:0909.2190.

[24] M. Larsen, R. Pink, *Finite subgroups of algebraic groups*, preprint (1995).

[25] C. Matthews, L. Vaserstein and B. Weisfeiler, *Congruence properties of Zariski- dense subgroups*, Proc. London Math. Soc, 48 (1984), 514-532.

[26] M. V. Nori, On subgroups of $GL_n(\mathbb{F}_p)$, Invent. Math. 88 (1987), no. 2, 257275.

[27] L. Pyber, E. Szabó, *Growth in finite simple groups of Lie type*, preprint (2010) arXiv:1001.4556

[28] I. Z .Ruzsa, Generalised arithmetic progressions and sumsets, Acta. Math. Hungar. **65** (1994), no. 4, 379–388.

[29] T. Tao, *Product set estimates in noncommutative groups*, Combinatorica **28** (2008), 547–594.

[30] T. Tao, *Freiman's theorem for solvable groups*, preprint.

[31] T. Tao, V. Vu, Additive Combinatorics, Cambridge University Press (2006).

[32] J. Tits, *Free subgroups in linear groups*, Journal of Algebra, **20** (1972), 250-270.

[33] P. Varjú, *Expansion in $SL_d(\mathcal{O}_K/I)$, I squarefree,* preprint.

[34] V. Vu, M. Wood, P. Wood, *Mapping incidences*, preprint.

Laboratoire de Mathématiques, Bâtiment 425, Université Paris Sud 11, 91405 Orsay, FRANCE

E-mail address: emmanuel.breuillard@math.u-psud.fr

Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WA, England

E-mail address: b.j.green@dpmms.cam.ac.uk

Department of Mathematics, UCLA, 405 Hilgard Ave, Los Angeles CA 90095, USA

E-mail address: tao@math.ucla.edu