GROWTH IN GROUPS II: FINITE GROUPS OF LIE TYPE

NICK GILL

Our ultimate aim over the next few lectures is to prove the following theorem:

Theorem 1. *Let G be a finite simple group of Lie type of rank r; let K be a finite field and take $\epsilon > 0$. Then there exist positive constants C, δ which depend only on r and ϵ such that for all $A \subset G(K)$ be a set such that $\langle A \rangle = G(K)$, and $|A| \leq |G|^{1-\epsilon}$ we have the following inequality.*

$$|A \cdot A \cdot A| \geq C|A|^{1+\delta}.$$

The approach we take is based on recent proofs of (variants of) this result announced in [BGT, PS]. It is important to note that this approach differs substantially from the original proofs for the case $K = \mathbb{Z}/p\mathbb{Z}$ and $G = SL_2, SL_3$ which were due to Helfgott [Hel08, Hel].

Although the new proofs are based heavily on Helfgott's work, they have no (direct) recourse to the incidence theorems used by Helfgott. A proper understanding of this area of mathematics would require a treatment of such theorems, but we have no time to do that here.

1. A summary of the argument

First a little notation: for a set A inside a group G define

$$A_k = \{a_1 \cdots a_k \mid a_1, \dots, a_k \in A \cup A^{-1}\}.$$

Now set G to be a finite simple group of Lie type, A a set of generators of G. We assume that A violates Thm. 1, and we aim to reach a contradiction. There are five steps to achieve this.

(P1) We begin by showing that there is a torus T in G such that $A_k \cap T(K)$ contains regular elements, for some small value k. In this case we say that T is *involved.* The proof of this result uses the idea of *escape from subvarieties.*

(P2) Next we show that the intersection with the involved torus T must be large: $|A_k \cap T(K)| \gg |A|^{C-\delta}$ for some k and C.

(P3) Bounds of Helfgott then allow us to conclude that the intersection of A_k with particular subtori of T is small; in particular the regular elements of $A_k \cap T(K)$ form a set of size at least $|A|^{1-\delta}$.

(P4) Now we apply a *pivot argument* to conclude that every conjugate of T is involved.

(P5) Simple arithmetic then allows us to conclude that A is *just about the whole group.* This violates the assumption that $|A| \leq |G|^{1-\epsilon}$ and we are done.

The rest of this lecture will be spent expanding this brief summary as far as we can without using algebraic geometry.

2. Background

2.1. **Regular elements and tori.** Our aim is for this lecture to be mainly an exercise in arithmetic combinatorics. However we can't avoid some (easy) technical machinery from algebraic groups. We collect the salient points here as they apply to SL_n. More information is available in the standard texts [Bor91, Hum97, Spr09].

Let $G = SL_n$, K a field, $\overline{K}$ its algebraic closure. A *maximal torus* in G is a maximal set of matrices T that are simultaneously diagonalizable in $G(\overline{K})$. Such a set is isomorphic as a group to $\overline{K}^{n-1}$; hence we define the *rank* of G to equal $n-1$.

A *regular element* in $G(K)$ is an element g with eigenvalues all distinct. The centralizer of g in $G(\overline{K})$ is a maximal torus. We will write $\Sigma(K)$ for the set of regular elements in $G(K)$.

The normalizer of a maximal torus T in $G(\overline{K})$ is a group N such that $N(\overline{K})/T(\overline{K}) \cong W$, the *Weyl group* of SL_n. The group W is isomophic to S_n.

2.2. **Boundedness.** Let $a, b \in \mathbb{R}$ with $a, b > 0$. We write $a \ll_b$ or $a = O(b)$ to mean $a \leq Cb$ where C is an absolute constant. We write $a \ll_{c_1,c_2,\dots,c_n} b$ or $a = O_{c_1,c_2,\dots,c_n}(b)$ to mean that $a \leq Cb$ where C is a constant depending only on $c_1, c_2, \dots, c_n$.

In particular, $a \ll_{c_1,c_2,\dots,c_n} 1$ (or $a = O_{c_1,c_2,\dots,c_n}(1)$) will mean that a is bounded in terms of $c_1, c_2, \dots, c_n$ alone.

Similar conventions apply for $\gg$. We will also need to bound vectors. Let

$$\vec{d} = (d_0, d_1, d_2, \dots, d_n, 0, 0, \dots). \qquad (d_i \text{ non-negative})$$

We write $\vec{d} \ll_a 1$ to mean that both n and $d_0, d_1, \dots, d_n$ are bounded in terms of a alone.

Similarly $a \ll_{\vec{d}} 1$ means that a is bounded in terms of n and $d_0, d_1, \dots, d_n$ alone.

2.3. **Arithmetic combinatorics.** We begin with a very simple lemma.

Lemma 2.1. *Let G be a finite group. Let $A \subset G$. Suppose $|A| > \frac{1}{2}|G|$. Then $A \cdot A = G$.*

Proof. Suppose there is a $g \in G$ not in $A \cdot A$. Then, for every $x \in G$, either x or gx^{-1} is not in A. As x goes over all elements of G, we see that no more than one out of every two elements of G can lie in A. In other words, $|A| \leq \frac{1}{2}|G|$. Contradiction. □

The next result has its origins in the concept of *Rusza distance.*

Lemma 2.2 (Tripling lemma)**.** [Hel08, Lem. 2.2] *Let $k > 2$ be an integer. Let A be a finite subset of a group G. Suppose that*

$$|A_k| \geq C|A|^{1+\epsilon}.$$

for some $C, \epsilon \geq 0$. Then

$$|A \cdot A \cdot A| \geq C'|A|^{1+\epsilon'}$$

where $C', \epsilon' > 0$ depend only on C, ϵ, and k.

Proof. We begin with a claim: let B, C, D be finite subsets of a group G. Then

$$|BD^{-1}||C| \leq |BC^{-1}||CD^{-1}|. \tag{2.1}$$

To prove this claim we construct a one-to-one function

$$i : BD^{-1} \times C \to BC^{-1} \times CD^{-1}.$$

For very $e \in BD^{-1}$ fix a pair $(b_e, d_e) \in B \times D$ such that $E = b_e d_e^{-1}$. Define $i(e,c) = (b_e c^{-1} c d_e^{-1})$. Clearly we can recover e from $i(e,c)$ (multiply the coordinates). Since (b_e, d_e) depends only on e we can then recover (b_e, d_e). From $i(e,c)$ and (b_e, d_e) we can recover c. Thus i is one-to-one.

Now apply the claim with $B = A_{n-2}$, $C = A$, and $D^{-1} = D = A_2$, Then (2.1) implies that

$$\frac{|A_{n-2}A_2|}{|A|} \leq \frac{|A_{n-2} \cdot A^{-1}|}{|A|} \frac{|A \cdot A_2|}{|A|} \leq \frac{|A_{n-1}|}{|A|} \frac{|A_3|}{|A|}.$$

Induction on n implies that

$$\frac{|A_n|}{|A|} \leq \left(\frac{|A_3|}{|A|} \right)^{n-2}.$$

We are left with the job of bounding $\frac{|A_3|}{|A|}$ from above by a power of $|A \cdot A \cdot A||A|$. We use (2.1) again:

$$\begin{aligned} |AAA^{-1}||A| &= |AAA^{-1}||A^{-1}| \leq |AAA||A^{-1}A^{-1}| \leq |AAA|^2, \\ |AA^{-1}A||A| &= |AA^{-1}A^{-1}||AA| = |AAA^{-1}||AA| \leq |AAA^{-1}||AAA|. \end{aligned}$$

The remaining triples involving A and A^{-1} can be reduced to these two cases easily enough. □

2.4. **A restatement.** The Tripling Lemma, and the notation we have established, allow us to restate Thm. 1 in a form that will be easier for us to attack:

Theorem 2. *Let G be a finite simple group of Lie type of rank r; let K be a finite field, and take $\epsilon > 0$. Then there exists positive $\delta \ll_{r,\epsilon} 1$ such that, for all $A \subset G(K)$ with $\langle A \rangle = G(K)$ and $|A| \leq |G|^{1-\epsilon}$, the following inequality holds:*

$$|A_k| \gg_{r,\epsilon} |A|^{1+\delta}$$

for some $k \ll_{r,\epsilon} 1$

In the remainder of this seminar we write down (part of) the proof of Thm. 2. We note first the hypotheses under which we will operate for the remainder of the lecture.

Hypotheses 1. *Let ϵ and δ be positive numbers and set A a subset of $G(K)$ such that $\langle A \rangle = G(K)$. We assume that, for all positive $k \ll_{r,\delta} 1$,*

$$|A_k| \ll_{r,\delta} |A|^{1+\delta}.$$

Our aim is to show that if we choose δ small enough then we obtain $|A| \geq |G(K)|^{1-\epsilon}$. To do this we follow the steps (P1) to (P5) as outlined in Section 1.

3. Pivoting

We refer to Section 1; the pivot argument takes us from (P3) to (P4); this step is the purpose of this section. We make the following definition.

Definition 1. *A torus T is involved if $A_2 \cap T(K)$ contains a regular element.*

We join the argument at point (P3); thus we are assuming the following to be true:

(P1) There is an involved torus T.

(P2) There exists positive $k \ll_{\delta,r} 1$ such that, if T is an involved torus, then

$$|A_k \cap T(K)| \gg_{\delta,r} |A|^{\frac{\dim T}{\dim G} - O(\delta)}. \tag{3.1}$$

(P3) Let T' be a torus of G and let $\alpha : T \to \mathbb{A}^1$ be a linear character of T'. Write T_0 for the kernel of α. Then

$$|A \cap T_0(K)| \ll_r |A_{k'}|^{\frac{\dim T' - 1}{\dim G}} \tag{3.2}$$

for $k' \ll_n 1$.

Lemma 3.1. *Suppose that T is an involved torus. Then aTa^{-1} is an involved torus, for every $a \in A$.*

Proof. Suppose $T' = aTa^{-1}$ is not involved, where $a \in A$. Consider the map

$$\phi : G \to G/T',\ g \mapsto gT'.$$

If $\phi(g_1) = \phi(g_2)$, then $g_1^{-1} g_2 \in T'$. Since T' is not involved, this implies that $g_1^{-1} g_2$ is a non-regular element of T'.

Now we use (P3). Pick a faithful representation $G \to GL_n$ defined over $\overline{K}$ such that $n \ll_r 1$. (For $G = SL_n$ we can just consider G to be the set of $n \times n$ matrices of determinant 1.) Choose a basis so that T' is a subset of the invertible diagonal matrices, with non-zero entries $t_{11}, \dots, t_{nn}$. For $1 \leq i < j \leq n$ define

$$\phi_{i,j} : T' \to \overline{K},\ t_{ii} - t_{jj}.$$

There are $\frac{1}{2}n(n-1) \ll_r 1$ of these linear characters, and their kernels contain all non-regular elements in T. Fact (P3) therefore implies that the number of non-regular elements in T' is $\ll_r |A|^{\frac{\dim(T')-1}{\dim(G)}}$.

Now pick a set $R \subset A$ of representatives of every preimage $\phi^{-1}(x)$ for $x \in \phi(A)$. Evidently, $|R| = |\phi(A)| \gg_r |A|^{1 - \frac{\dim(T)-1}{\dim(G)}}$.

Now, because T is involved, there is a regular element $x \in A_2 \cap T(K)$. Hence $axa^{-1} \in A_4 \cap T'(K)$ is regular. Now (P2) implies that there exist $k \ll_{\delta,r} 1$ such that

$$|A_{4k} \cap T'(K)| \gg_r |A|^{dim(T')/dim(G) - O(\delta)}.$$

Now consider the map

$$\theta : G \times T' \to G,\ (g,t) \mapsto gt$$

The restriction of θ to $R \times (A_{4k} \cap T'(K))$ is injective (and thus has image of size $\gg_r |A|^{1+1/dim(G)-O(\delta)}$). What is more this image is contained in A_{4k+1}. Hence $|A_{4k+1}| \gg_r |A|^{1+1/dim(G)-O(\delta)}$. Now for δ small enough, this implies that A grows, contrary to our assumptions. □

Corollary 3.2 (P4). *Suppose that T is an involved torus. Then gTg^{-1} is an involved torus, for every $g \in G(K)$.*

Proof. This follows immediately from the fact that $\langle A \rangle = G$. □

4. Closing out the argument

We follow the argument from point (P4) to the end. Recall that $\Sigma(K)$ is the set of regular elements in G; as before let $n \ll_r 1$ be such that $G < GL_n$. Note first that (P2) and (P3) imply that for some positive $k \ll_{\delta,r} 1$,

$$|A_k \cap T(K) \cap \Sigma(K)| \gg_{\delta,r} |A|^{\frac{\dim T}{\dim G} - O(\delta)} - \frac{1}{2}n(n+1)|A|^{\frac{\dim T - 1}{\dim G}} \gg |A|^{\frac{\dim T}{\dim G} - O_{r,\delta}(\delta)},$$

provided we choose δ small enough. (In what follows we omit subscripts since all constants depend only on r and δ.)

Now let T_1 and T_2 be distinct tori in G. It is easy to observe that

$$T_1(K) \cap T_2(K) \cap \Sigma(K) = \emptyset \tag{4.1}$$

(To see this, simply use the fact that the centralizer of a regular element is a torus.)

Now this means that the size of A_k must be bounded below by the number of conjugates of T in G multiplied by the number of regular elements that lie in A_k and the intersection of any torus:

$$|A_k| \gg_r \frac{|G(K)|}{|T(K)|} \times |A|^{\frac{\dim T}{\dim G} - O(\delta)}.$$

Now we are assuming that $|A_k| \ll_r |A|^{1+\delta}$. Thus we obtain that

$$|A|^{1+\delta} \gg_r \frac{|G(K)|}{|T(K)|} \times |A|^{\frac{\dim T}{\dim G} - O(\delta)}.$$

$$\implies |A|^{1 - \frac{\dim T}{\dim G} + \delta - O(\delta)} \gg_r |G(K)|^{1 - \frac{\dim T}{\dim G}}.$$

If we choose δ small enough, then this implies that $|A| \gg |G(K)|^{1-\epsilon}$ as required.

References

[BGT] E. Breuillard, B. Green, and T. Tao, *Linear approximate groups*, 2010, Preprint available on the Math arXiv: `http://arxiv.org/abs/1001.4570`.

[Bor91] Armand Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[Hel] H.A. Helfgott, *Growth and generation in $SL_3(\mathbb{Z}/p\mathbb{Z})$*, J. Eur. Math. Soc. (JEMS), To appear.

[Hel08] H. A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. of Math. (2) **167** (2008), no. 2, 601–623.

[Hum97] John F. Humphreys, *A course in group theory*, Oxford Science Publications, Oxford University Press, 1997.

[PS] L. Pyber and E. Szabó, *Growth in finite simple groups of lie type*, 2010, Preprint available on the Math arXiv: `http://arxiv.org/abs/1001.4556`.

[Spr09] T. A. Springer, *Linear algebraic groups*, second ed., Modern Birkhäuser Classics, Birkhäuser Boston Inc., Boston, MA, 2009.