JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 29, Number 1, January 2016, Pages 95–146
S 0894-0347(2014)00821-3
Article electronically published on October 31, 2014

GROWTH IN FINITE SIMPLE GROUPS OF LIE TYPE

LÁSZLÓ PYBER AND ENDRE SZABÓ

Contents

1. Introduction

In a spectacular breakthrough, Helfgott [27] proved that generating sets of $SL(2,p)$ grow rapidly under multiplication.

Theorem 1 (Helfgott)**.** *Let $L = SL(2,p)$, p a prime, and A a generating set of L. Let δ be a constant, $0 < \delta < 1$.*
(a) If $|A| < |L|^{1-\delta}$ then

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

where ε depends only on δ.
(b) If $|A| > |L|^{1-\delta}$ then $A^k = L$ where k depends only on δ.

Here and elsewhere, A^k denotes the subset $\{a_1 a_2 \cdots a_k | a_i \in A\}$ of G.

It was observed in [45] that a result of Gowers [25] implies that (b) holds for an arbitrary simple group of Lie type L with $k = 3$ for some $\delta(r)$ which depends only

Received by the editors June 11, 2014 and, in revised form, September 15, 2014.
2010 *Mathematics Subject Classification.* Primary 20F69; Secondary 20G15, 20D06.
Key words and phrases. Growth, finite simple groups, algebraic groups.
The first author is supported in part by OTKA 78439 and K84233.
The second author is supported in part by OTKA NK81203, K84233 and by the MTA Rényi "Lendület" Groups and Graphs Research Group.

on the Lie rank r of L. It remained an important problem to prove an analog of the (rather more difficult) part (a) as was done by Helfgott for the groups $SL(3,p)$ in [28], and by Dinai [16] and Varjú [54] for the groups $SL(2,q)$, q a prime power.

We prove the following.

Theorem 2. *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.

We also give some examples in Section 12 which show that in the above result the dependence of ε on r is necessary. Moreover, we construct generating sets A of $SL(n,3)$ of size $2^{n-1}+4$ with $|A^3| < 100|A|$ for $n \geq 3$, i.e., generating sets of constant growth.

Theorem 2 was introduced in [48]. The same day, independently, similar results were introduced by Breuillard, Green, and Tao [9] for finite Chevalley groups.[1]

Somewhat earlier, Gill and Helfgott [23] showed that small generating sets (of size at most $p^{n+1-\delta}$ for some $\delta > 0$) in $SL(n,p)$ grow.

Helfgott's work [27] has been the starting point of, and inspiration to, much recent work by Bourgain, Gamburd, Sarnak, and others.

Let G be a finite group and A a symmetric (i.e., closed under inversion) set of generators of G. The Cayley graph $\Gamma = \Gamma(G,A)$ is the 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 $s \in A$. Then $\operatorname{diam}(\Gamma)$, the diameter of Γ, is the smallest number d such that $A^d = G$.

In [5] Bourgain and Gamburd proved the following.

Theorem 3 (Bourgain, Gamburd)**.** *Let A be a symmetric finite subset of $SL(2,\mathbb{Z})$ generating a subgroup Λ which is Zariski dense in $SL(2)$. Then the family of Cayley graphs $\Gamma(SL(2,p),\pi_p(A))$ forms an expander family as the prime p goes to ∞. Here π_p denotes reduction modulo p.*

Bourgain, Gamburd, and Sarnak [7] proved that the same holds for square free moduli. This result was used in [7] as a building block in a combinatorial sieve method for primes and almost primes on orbits of various subgroups of $SL(2,\mathbb{Z})$ as they act on $\mathbb{Z}^m$ (for $m \geq 2$).

Combining Theorem 2 with [6, Theorem 1.2] we immediately obtain that the analog of Theorem 3 holds for Zariski dense subgroups Λ of $SL(n,\mathbb{Z})$. For an account of far reaching developments in this area (many of which rely on Theorem 2) see [42].

Another consequence of Theorem 2 is the following.

Theorem 4. *Let L be a finite simple group of Lie type of rank r. For every symmetric set A of generators of L we have*

$$\operatorname{diam}\big(\Gamma(L,A)\big) < \big(\log|L|\big)^{c(r)}$$

where the constant $c(r)$ depends only on r.

[1] Breuillard, Green, and Tao [10] cover all simple groups of Lie type apart from the infinite families of Ree groups (personal communication from Ben Green). The strategy of proofs in [10] and in the present article is roughly the same, although the details of the arguments are quite different at times.

This was first proved by Helfgott [27] for $L = SL(2,p)$, as a consequence of Theorem 1. Theorem 4 follows from Theorem 2 by the same argument.

A classical conjecture of Babai [3] states that Theorem 4 should hold with an absolute exponent c independent from r and, furthermore, the diameter of any Cayley graph of the finite alternating groups should be polynomially bounded in their degree.

Simple groups of Lie type can be treated as subgroups of simple algebraic groups. In fact, instead of concentrating on simple groups, we work in the framework of arbitrary linear algebraic groups over algebraically closed fields. We set up a machinery which can be used to obtain various results on growth of subsets in linear groups, including Theorem 2.

Subgroups of $SL(n,p)$ generated by elements of order p were investigated in detail by Nori [44] and Hrushovski-Pillay [32]. Using the above machinery we also obtain the following.

Theorem 5. *Let $P \leq SL(n,p)$, p a prime, be a perfect subgroup which is generated by its elements of order p. Let A be a symmetric set of generators of P. Then*

$$\operatorname{diam}\big(\Gamma(P,A)\big) \leq \big(\log|P|\big)^{M(n)}$$

where the constant $M(n)$ depends only on n.

Theorem 5 is a surprising extension of the fact (included in Theorem 4) that simple subgroups of $SL(n,p)$, n bounded, have polylogarithmic diameter (see also Remark 76). For an unexpected application of Theorem 5 in arithmetic geometry, see [38].

As another application of our algebraic group machinery we derive the second main result of this article.

Theorem 6. *Let $\mathbb{F}$ be an arbitrary field and $A \subseteq SL(n,\mathbb{F})$ a finite subset such that $|A^3| \leq \mathcal{K}|A|$ for some $\mathcal{K}$. Then there is a virtually soluble normal subgroup Γ of $\langle A\rangle$ and a bound m depending only on n such that the subset A can be covered by $\mathcal{K}^m$, i.e., polynomially many, cosets of Γ.*

The first result of this type was obtained by Elekes and Király [18]. Using deep model-theoretic tools Hrushovski, among many other results, has obtained a qualitative version of Theorem 6 (see [31, Corollary 5.11]), in which the number of cosets of Γ covering A is at most $f(\mathcal{K},n)$ for some function f. Hrushovski's article contains material closely related to ours. Indeed, his article was mentioned by Breuillard, Green, and Tao [10] as an essential source of inspiration for their work. Our work was more influenced by an earlier work of Hrushovski and Pillay [32].

In characteristic 0, Theorem 6 was first proved by Breuillard, Green, and Tao [10]. Actually, in that case, using [11] they deduce a stronger conclusion: one can even require Γ to be nilpotent.

The following conjecture, due to Helfgott (see the comments after [28, Theorem 1.1]), is stated explicitly in [29].

Conjecture 7. *Let A be a symmetric subset of $SL(n,\mathbb{F})$ satisfying $|A^3| \leq \mathcal{K}|A|$ for some $\mathcal{K} \geq 1$, where $\mathbb{F}$ is an arbitrary field. Then A is contained in the union of $\mathcal{K}^{c(n)}$ cosets of a finite-by-nilpotent subgroup Γ normalized by A.*

Moreover, Γ has a finite subgroup P normalized by A such that Γ/P is nilpotent, and $A^{c(n)}$ contains P.

This was proved, as mentioned above, in characteristic 0 in [10], and for subsets of $SL(3,\mathbb{F}_p)$ in [28].

Theorem 6 constitutes a major step towards the verification of this conjecture. Indeed, in [50] we prove, using Theorem 2 and Theorem 6, that a weaker version of Conjecture 7 (with Γ/P soluble) holds.

1.1. **Methods.** The proofs of Helfgott combine group theoretic arguments with some algebraic geometry, Lie theory, and tools from additive combinatorics such as the sum-product theorem of Bourgain, Katz, andTao [8]. Our argument relies on a deeper understanding of the algebraic group theory behind his proofs and an extra trick, but not on the sum-product theorem.

We prove 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 [27], [28] and Hrushovski-Pillay [32].

To illustrate our strategy we outline the proof of Theorem 2 in the simplest case, when A generates $L = SL(n,q)$, q a prime-power. Assume that "A does not grow", i.e., $|AAA|$ is not much larger than $|A|$. Using an "escape from subvarieties" argument, it is shown in [28] that if T is a maximal torus in L then $|T \cap A|$ is not much larger than $|A|^{1/(n+1)}$. This is natural to expect for dimensional reasons since $\dim(T)/\dim(L) = (n-1)/(n^2-1) = 1/(n+1)$.

We use a rather more powerful escape argument. The first part of our article is devoted to establishing the necessary tools in great generality (in particular, the Spreading Theorem 40).

Now T is equal to $L \cap \bar{T}$ where $\bar{T}$ is a maximal torus of the algebraic group $SL(n,\overline{\mathbb{F}_q})$. Let T_r denote the set of regular semisimple elements in T. Note that $T \setminus T_r$ is contained in a subvariety $V \subsetneq \bar{T}$ of dimension $n-2$. By the above-mentioned escape argument $\left|(T\setminus T_r)\cap A\right|$ is not much larger than $|A|^{\dim(V)/\dim(L)} = |A|^{1/(n+1)-1/(n^2-1)}$.

By [28], or by our escape argument, A does contain regular semisimple elements. If a is such an element then consider the map $SL(n) \to SL(n)$, $g \to g^{-1}ag$. The image of this map is contained in a subvariety of dimension $n^2-1-(n-1)$ since $\dim\left(\mathcal{C}_{SL(n)}(a)\right) = n-1$. By the escape argument we obtain that for the conjugacy class $\mathrm{cl}(a)$ of a in L, $\left|\mathrm{cl}(a)\cap A^{-1}aA\right|$ is not much larger than $|A|^{(n^2-n)/(n^2-1)}$. Now $\left|\mathrm{cl}(a)\cap A^{-1}aA\right|$ is at least the number of cosets of the centralizer $C_L(a)$ which contain elements of A . It follows that $\left|AA^{-1}\cap C_L(a)\right|$ is not much smaller than $|A|^{1/(n+1)}$. Of course $C_L(a)$ is just the (unique) maximal torus containing a.

Informally, we say that a maximal torus is *full* if its intersection with a small power of AA^{-1} is not much smaller than $|A|^{1/(n+1)}$. This notion is needed for later reference in Section 8.

Let us say that A *covers* a maximal torus T if $T\cap A$ contains a regular semisimple element. We obtain the following fundamental dichotomy (see Lemma 50).

Assume that a generating set A does not grow

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

ii) If A covers T then $\left|T\cap AA^{-1}\right|$ is not much smaller than $|A|^{1/(n+1)}$ (hence T is a full torus). In fact $\left|T_r\cap AA^{-1}\right|$ is not much smaller than $|A|^{1/(n+1)}$.

It is well known that if A doesn't grow then $B = AA^{-1}$ doesn't grow either ([27, proof of Lemma 2.2], see Proposition 56), hence the above dichotomy applies to B.

Let us first assume that B covers a maximal torus T but does not cover a conjugate $T' = g^{-1}Tg$ of T for some element g of L . Since A generates L we have such a pair of conjugate tori where g is in fact an element of A. Consider those cosets of T' which intersect A. Each of the, say, t cosets contains at most $|B \cap T'|$ elements of A, i.e., not much more than $|B|^{1/(n+1)-1/(n^2-1)}$ which in turn is not much more than $|A|^{1/(n+1)-1/(n^2-1)}$. Therefore, $|A|$ is not much larger than $t|A|^{1/(n+1)-1/(n^2-1)}$.

On the other hand, $A\big(A^{-1}(BB^{-1})A\big)$ has at least $t\big|T \cap BB^{-1}\big|$ elements which is not much smaller than $t|A|^{1/(n+1)}$. Therefore, $(AA^{-1})^3A$ is not much smaller than $|A|^{1+1/(n^2-1)}$ which contradicts the assumption that A does not grow (see Proposition 56).

We obtain that B covers all conjugates of some maximal torus T. Now the conjugates of the set T_r are pairwise disjoint (e.g., since two regular semisimple elements commute exactly if they are in the same maximal torus). The number of these tori is $|L : N_L(T)| > c(n)|L : T|$ for some constant which depends only on n. Each of them contains not much less than $|B|^{1/(n+1)}$ regular semisimple elements of BB^{-1}. Altogether we see that $|A|$ is not much smaller than $q^{n^2-n}|A|^{1/(n+1)}$ and finally that $|A|$ is not much less than $|L|$. In this case by [45] we have $AAA = L$.

A finite simple group of Lie type can be obtained as a "very large" subgroup of G^σ, the group of fixpoints of a Frobenius map σ of some simple algebraic group G. The proof of Theorem 2 relies basically on the fact that G^σ does not normalize any non-trivial σ-invariant connected closed subgroup of G. In particular, $\mathcal{C}_G(G^\sigma)$ is finite. Our proof of this fact depends on Hrushovski's twisted Lang-Weil estimates [30]. Using a result of Martin Liebeck this can be avoided (see Remark 69). In particular, the growth exponent $\varepsilon(r)$ in Theorem 2 is effective.[2] Computing a lower bound on $\varepsilon(r)$ from our proof would not be very enlightening, especially since for small subsets A the bound would be absurdly small.

Examples given in Section 12 show that in Theorem 2 we must have $\varepsilon(r) = O(1/r)$. We believe that this is the right order of magnitude.

In the main body of this article, the above argument is lifted to the level of algebraic groups. Moreover, it is generalized to accommodate not necessarily simple algebraic groups. This generalized proof-scheme will yield Theorem 2, Theorem 5, and Theorem 6 as special cases. Indeed, for the proof of Theorem 6 (in arbitrary characteristic) this seems to be the right approach.

Next, we will briefly describe the contents of the various sections of this article.

In Section 2, we collect some basic definitions and useful facts from algebraic geometry. In Section 3, we consider the "concentration" of a finite set α in a closed set X as the relative size of $\alpha \cap X$ in X (see Definition 18). We investigate how concentration behaves under various morphisms. In Section 4, we collect various facts concerning algebraic groups and obtain some useful lemmas.

[2]This, among many other effective results, is needed to make the work of Golsefidy and Sarnak on the affine sieve effective; see [24, page 1086 and page 1101] for a detailed discussion. Indeed, one of our reasons to make Theorem 2 effective was the possibility of such an application. As noted by Breuillard, Green, and Tao, their results in [10] are not effective due to their reliance on ultrafilters; see [10, page 789] for a discussion.

In Section 5, using the results obtained earlier we establish our main technical tool, the Spreading Theorem 40. In a very special case it says the following. Let α be a finite subset generating $SL(n,q)$ in $G = SL(n,\overline{\mathbb{F}_p})$. If G has a closed subset X in which α has much larger concentration than in G then a small power of α has similarly large concentration in G itself, i.e., α grows.[3]

In Section 6, we consider a class of closed subgroups of algebraic groups called "CCC-subgroups". In not necessarily simple algebraic groups, CCC-subgroups can be used in our generalized proof-scheme as substitutes for maximal tori. In Section 7, we generalize the above "fundamental dichotomy" from maximal tori in $SL(n,q)$ to arbitrary CCC-subgroups in algebraic groups.

In Section 8, we obtain an abstract version of Theorem 2, and an analogous result to be used in the proof of Theorem 6 (see Theorem 54). In Section 9, we complete the proof of Theorem 6 by an inductive argument using Theorem 54(a).

In Section 10, we prove Theorem 2. In fact, we obtain a more general result (see Lemma 67) which will be used also in an inductive argument proving Theorem 5. In Section 11, we complete the proof of Theorem 5 using the Nori correspondence between p-generated subgroups of $SL(n,p)$ and certain closed subgroups of $SL(n,\overline{\mathbb{F}_p})$.

Various examples related to our theorems appear at the end of Section 11 and in Section 12.

Appendix A contains large chunks of proofs of more or less straightforward intermediate results that would cloud the understanding of the general scheme of proof. Finally, Appendix B contains a result concerning the group of fixpoints of Frobenius maps in simple algebraic groups, which Martin Liebeck kindly proved for us. As mentioned above, this can be used to give a slightly different proof of Theorem 2.

2. Dimension and degree

In this section we collect some basic definitions from algebraic geometry, and state a number of useful facts for later reference. Most of this is well known, and we suggest [33, Chapter I] and [26, Chapter I] for general reference.

Throughout this article, $\overline{\mathbb{F}}$ denotes an arbitrary algebraically closed field. We use affine algebraic geometry, i.e., all occurring sets will be subsets of some affine space $\overline{\mathbb{F}}^m$ for some integer $m > 0$, and we define all of them via m-variate polynomials whose coefficients belong to $\overline{\mathbb{F}}$. Below we make this more precise.

Definition 8. A subset $Z \subseteq \overline{\mathbb{F}}^m$ is *Zariski closed*, or simply *closed*, if it can be defined as the common zero-set of some m-variate polynomials. This defines a topology on $\overline{\mathbb{F}}^m$. Each subset of $\overline{\mathbb{F}}^m$ inherits this topology, called the *Zariski topology*. For an arbitrary subset $X \subseteq \overline{\mathbb{F}}^m$ we denote by $\overline{X}$ the *closure* of X. The complements of closed subsets are called *open*. An open dense subset of a closed set is called *locally closed*.[4]

Definition 9. A locally closed subset $X \subseteq \overline{\mathbb{F}}^m$ is called *irreducible* if it has the following property: whenever X is the union of finitely many closed subsets of X, it must be equal to one of them.

[3] A very similar result called the Larsen-Pink inequality has been established by Breuillard, Green, and Tao in [10]. Several special cases of this inequality were obtained earlier by Helfgott [28], in particular when X is a maximal torus.

[4] In [26] irreducible locally closed subsets of affine spaces are called *quasi-affine varieties*.

Fact 10. *Let $X \subseteq \overline{\mathbb{F}}^m$ be a locally closed subset. Then there are finitely many closed subsets X_i of X which are irreducible, and maximal among the irreducible closed subsets of X. Then $X = \bigcup_i X_i$ is the* irreducible decomposition *of X and these X_i are the* irreducible components *of X.*

Definition 11. Let $X \subseteq \overline{\mathbb{F}}^m$ be a locally closed subset. We consider chains $X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$ where the X_i are nonempty, irreducible closed subsets of X. The largest possible length n of such a chain is called the *dimension* of X, denoted by $\dim(X)$.

Definition 12. Let $X \subseteq \overline{\mathbb{F}}^m$ be a locally closed subset. An *affine* subspace of $\overline{\mathbb{F}}^m$ is a translate of a linear subspace. If X is irreducible then we consider all affine subspaces $L \subseteq \overline{\mathbb{F}}^m$ such that $\dim(X)+\dim(L) = m$ and $X \cap L$ is finite. The *degree* of X is the largest possible number of intersection points: $\deg(X) = \max_L |X \cap L|$. In general, the degree of X is defined as the sum of the degrees of its irreducible components.

Remark 13. Let $X \subseteq \overline{\mathbb{F}}^m$ be a locally closed subset. Using [22, Examples 8.4.11 and 8.4.12.(c)] it follows that $\deg(X)$ is equal to the degree of the closure of X in $\mathbb{P}^m$, the projectivization of $\overline{\mathbb{F}}^m$, see also [26, Ex. I.2.9 and Definition before Prop. I.7.6]. We will use this equality in the proofs of the basic facts below.

Remark 14. Let $X \subseteq \overline{\mathbb{F}}^m$ be a locally closed subset. Then $\dim(X) = 0$ iff X is finite. A finite subset $X \subset \overline{\mathbb{F}}^m$ is always closed, and satisfies $\deg(X) = |X|$.

Definition 15. Let $X \subseteq \overline{\mathbb{F}}^m$ and $Y \subseteq \overline{\mathbb{F}}^n$ be locally closed subsets. A function $f : X \to Y$ is called a *morphism* if it is the restriction to X of a map $\phi : \overline{\mathbb{F}}^m \to \overline{\mathbb{F}}^n$ whose n coordinates are m-variate polynomials. (A morphism is an *isomorphism* if its inverse is also a morphism.) The graph of f, denoted by $\Gamma_f \subseteq X \times Y \subseteq \overline{\mathbb{F}}^{m+n}$, is locally closed. We define the *degree* of f to be $\deg(f) = \deg(\Gamma_f)$. Note that if the defining polynomials all have degree at most Δ then $\deg(f) \le \Delta^m \deg(X) \deg(Y)$ (see Fact 16.(g) and (d) and below).

The following fact is standard.

Fact 16. *Let $X, Y \subseteq \overline{\mathbb{F}}^m$ be locally closed subsets.*

(a) The dimension and the degree of X are equal to the dimension and the degree of its closure $\overline{X}$.

(b) Any closed subset of X has dimension at most $\dim(X)$.

(c) The irreducible components $X_i \le X$ satisfy

$$\dim(X_i) \le \dim(X) = \max_j \big(\dim(X_j)\big) ,$$

$$\deg(X_i) \le \deg(X) = \sum\nolimits_j \deg(X_j) .$$

It follows that there are at most $\deg(X)$ components and at least one of them has the same dimension $\dim(X_i) = \dim(X)$.

(d) The subsets $X \cap Y$, $\overline{X} \cup \overline{Y}$, $X \setminus \overline{Y}$, and $X \times Y$ are also locally closed with the following bounds:

$$\begin{aligned} \dim(\overline{X} \cup \overline{Y}) &= \max\big(\dim(X), \dim(Y)\big) \\ \deg(\overline{X} \cup \overline{Y}) &\le \deg(X) + \deg(Y) \\ \dim(X \setminus \overline{Y}) &\le \dim(X) \end{aligned}$$

$$\begin{aligned}
\deg(X \setminus \overline{Y}) &\leq \deg(X) \\
\dim(X \cap Y) &\leq \min\big(\dim(X), \dim(Y)\big) \\
\deg(X \cap Y) &\leq \deg(X)\deg(Y) \\
\dim(X \times Y) &= \dim(X) + \dim(Y) \\
\deg(X \times Y) &= \deg(X)\deg(Y)
\end{aligned}$$

(e) Suppose that X is irreducible. Then each nonempty open subset $U \subset X$ is dense in X with $\dim(X \setminus U) < \dim(X)$.

(f) The direct product of irreducible locally closed subsets is again irreducible.

(g) If X is the common zero locus of degree d polynomials, then it is the common zero locus of at most $(d+1)^m$ of them, and $\deg(X) \leq d^m$. On the other hand, a closed subset X is the common zero locus of polynomials of degree at most $\deg(X)$.

(h) Let $Z \subseteq \overline{\mathbb{F}}^m \times \overline{\mathbb{F}}^n$ be a locally closed subset, and $V \subseteq \overline{\mathbb{F}}^m$ be its projection. Then $\deg\big(\overline{V}\big) \leq \deg(Z)$.

Sketch of proof. By [26, Prop. I.1.10] $\dim(X) = \dim(\overline{X})$, and $\deg(X) = \deg(\overline{X})$ since X and $\overline{X}$ have the same projective closure. Hence (a) holds. Part (b) is [26, Ex. I.1.10.(a)]. Part (c) follows immediately from Definition 11 and Definition 12. Part (e) follows from [26, Ex. I.1.6 and Ex. I.1.10.(d)] and (f) follows from [26, Ex. I.3.15.(a) and Ex. I.1.6].

In (d) the statements about the union, about the difference, and the one about $\dim(X \cap Y)$ follow from (c) and (a). The formula for $\deg(X \cap Y)$, after projectivization, is (an appropriate version of) Bézout's theorem (see [22, Example 8.4.6]). Part (a) and [26, Ex. I.3.15.(d)] imply that $\dim(X \times Y) = \dim(X) + \dim(Y)$.

To calculate $\deg(X \times Y)$ we switch to the projective closures $\overline{X}, \overline{Y} \subseteq \mathbb{P}^n$, and $\overline{X \times Y} \subseteq \mathbb{P}^{2n}$. By [22, Example 8.4.5] the *ruled join* $J(\overline{X}, \overline{Y}) \subseteq \mathbb{P}^{2n+1}$ has degree $\deg(\overline{X})\deg(\overline{Y})$, and $\overline{X \times Y}$ can be identified with a generic hyperplane section of $J(\overline{X}, \overline{Y})$. By Bézout's theorem (d) follows.

The first part of (g) is Lemma 78 in Appendix A. The second part of (g) is established in [43, Introduction] in the first two paragraphs of the proof Theorem 1.

In (h) we may assume that Z is irreducible. Using Chevalley's theorem (see [26, Ex. II.3.19]) and [26, E. II.3.18.(b)] we obtain a locally closed set W open and dense in V. Consider generic affine subspaces $M \subseteq \overline{\mathbb{F}}^m$ and $N \subseteq \overline{\mathbb{F}}^n$ of dimensions $m - \dim\big(\overline{V}\big)$ resp. $n - \dim(Z) + \dim(\overline{V})$. They are transversal to $\overline{V}$ resp. to the generic fibers of the projection $Z \to V$ and M avoids $\overline{V} \setminus W$. Hence, $\deg\big(\overline{V}\big) = \big|N \cap \overline{V}\big| = \big|N \cap W\big| \leq \big|(M \oplus N) \cap Z\big| \leq \deg(Z)$. □

In the following fact (a) yields an effective version of Chevalley's theorem on the fibers of morphisms (see [26, Ex. II.3.22.(e)]).

Fact 17. *Let $X \subseteq \overline{\mathbb{F}}^m$ and $Y \subseteq \overline{\mathbb{F}}^n$ be closed subsets and $f : X \to Y$ be a morphism. We define several (open, closed or locally closed) subsets of X and Y. Their dimension is at most $\dim(X)$, and we bound their degrees using an appropriate integer $D = D\big(\dim(X), \deg(f)\big)$.*

(a) There is a partition of $\overline{f(X)}$ into at most D locally closed subsets Y_i of degree at most D such that the closure of each Y_i is the union of partition classes and either $f^{-1}(Y_i) = \emptyset$ or $\dim\big(f^{-1}(y)\big) = \dim(X) - \dim(Y_i)$ for all $y \in Y_i$.

(b) *We have* $\deg\left(\overline{f(X)}\right) \leq \deg(f)$*, and* $f(X)$ *contains a dense open subset* U *of* $\overline{f(X)}$*. If* X *is irreducible then so is* $\overline{f(X)}$*.*

(c) *For each* $y \in f(X)$ *the fiber* $f^{-1}(y) \subseteq X$ *is closed with* $\deg\left(f^{-1}(y)\right) \leq \deg(f)$*. For each closed subset* $T \subseteq Y$ *the subset* $f^{-1}(T)$ *is also closed and its degree is at most* $\deg(T)\deg(f)$*.*

(d) *The degree of the closed complement* $\overline{\overline{f(X)} \setminus f(X)}$ *is at most* D^2*.*

(e) *Suppose that* X *is irreducible. For each* $t \in X$ *we have*

$$\dim\left(f^{-1}\big(f(t)\big)\right) \geq \dim(X) - \dim\left(\overline{f(X)}\right).$$

Those $t \in X$ *where equality holds form an open dense subset* $X_{\min} \subseteq X$ *and* $\deg\left(X \setminus X_{\min}\right) \leq D^2 \deg(f)$*.*

(f) *Let* $S \subseteq X$ *be a closed subset that is the intersection of* X *and a closed subset of degree* d*. Then the degree of the restricted morphism* $f\big|_S$ *is at most* $d \cdot \deg(f)$*, hence* $\deg\left(\overline{f(S)}\right) \leq d \cdot \deg(f)$*.*

Sketch of proof. Lemma 79 in Appendix A is an explicit version of (a).

In (b) we may assume that X is irreducible. Fact 16.(h) implies $\deg(f) = \deg(\Gamma_f) \geq \deg\left(\overline{f(X)}\right)$ and [26, Ex. II.3.19.(b)] gives us U. A decomposition $\overline{f(X)} = A \cup B$ would imply $X = f^{-1}(A) \cup f^{-1}(B)$, hence $\overline{f(X)}$ must be irreducible. This proves (b).

In (c) the fibers $f^{-1}(y)$ and $f^{-1}(T)$ are closed by continuity. Moreover, they are the projections into $\overline{\mathbb{F}}^m$ of the sets $\Gamma_f \cap \left(\overline{\mathbb{F}}^m \times \{y\}\right)$ resp. $\Gamma_f \cap \left(\overline{\mathbb{F}}^m \times T\right)$. Facts 16.(d) and 16.(h) imply the degree bounds.

In (d) the subset $\overline{\overline{f(X)} \setminus f(X)}$ is the union of some partition classes from (a). The degree bound follows.

In (e) the inequality for the dimensions and the openness of $X_{\min}$ follows from [26, Ex. II.3.22.(d)], so $X_{\min}$ is dense by the irreducibility. The subset $X \setminus X_{\min}$ is the inverse image of the union of a number of partition classes of (a), so the degree bound follows from (c).

In (f) we have $\Gamma_{f|_S} = \Gamma_f \cap (S \times \overline{\mathbb{F}}^n)$. The estimates follows from (b) and Fact 16.(d). □

3. Concentration: basic results

Let $\alpha \subseteq \overline{\mathbb{F}}^m$ be a finite subset. An essential part of our general strategy is to find (Zariski-)closed subsets X which contain a large number of elements of α compared to their dimension. To measure the relative size of $\alpha \cap X$ we introduce the following.

Definition 18. For each subset $X \subseteq \overline{\mathbb{F}}^m$ with $\dim(\overline{X}) > 0$ we define the *concentration* of α in X as follows:

$$\mu(\alpha, X) \;=\; \frac{\log|\alpha \cap X|}{\dim(\overline{X})}.$$

Throughout this article log stands for the natural logarithm. When $\alpha \cap X = \emptyset$ we set $\mu(\alpha, X) = -\infty$.

In this section we prove various results about concentration. For example, we show that the concentration in a closed subset X does not decrease too much when we take an appropriate irreducible closed subset (see Lemma 20 and Lemma 21)

or when we map X somewhere by a "nice morphism" (Lemma 22). Generalizing Lemma 22 we prove the Transport Lemma 24, an important tool which can be used when we map X somewhere by a morphism which is "not so nice".

As explained below, we will have to consider totally ordered sets α to make various subsets and subgroups we construct uniquely determined (given this ordering). This will play an important role in Section 10.

Proposition 19. *Let $X \subseteq Y \subseteq \overline{\mathbb{F}}^m$ be closed subsets with $\dim(X) > 0$. For all finite sets $\alpha \subset \overline{\mathbb{F}}^m$ with $\alpha \cap X \neq \emptyset$ and for all $n > 0$ we have*

$$0 \leq \mu(\alpha, X) \leq \tfrac{\dim(Y)}{\dim(X)} \cdot \mu(\alpha, Y)\,, \qquad \mu\Big(\prod{}^n \alpha, \prod{}^n X\Big) = \mu(\alpha, X)\,.$$

Proof. Clear from the definition. □

Lemma 20. *Let $Z \subseteq \overline{\mathbb{F}}^m$ be a closed subset with $\dim(Z) > 0$ and $\alpha \subseteq \overline{\mathbb{F}}^m$ a finite subset with $|\alpha \cap Z| > \deg(Z)$. Then there is an irreducible component $Z' \subseteq Z$ such that $\dim(Z') > 0$ and*

$$\mu(\alpha, Z') \geq \mu(\alpha, Z) - \log\big(\deg(Z)\big)\,.$$

Proof. Since Z has at most $\deg(Z)$ irreducible components (see Fact 16.(c)) there is a component $Z' \subseteq Z$ with

$$\big|\alpha \cap Z'\big| \geq \frac{|\alpha \cap Z|}{\deg(Z)} > 1\,. \tag{1}$$

In particular, we have $\dim(Z') > 0$. We take the logarithm of inequality (1), divide the two sides by $\dim(Z')$, and rewrite it in terms of concentrations. Using $\dim(Z') \leq \dim(Z)$ we obtain our statement:

$$\mu(\alpha, Z') \geq \frac{\dim(Z)}{\dim(Z')}\mu(\alpha, Z) - \frac{\log\big(\deg(Z)\big)}{\dim(Z')} \geq \mu(\alpha, Z) - \log\big(\deg(Z)\big). \qquad \square$$

The proof of Lemma 20 involves a choice. For proving Theorem 2 and Theorem 4 it will be important to construct sets, subgroups, etc., which are uniquely determined. To this end we totally order the finite set α, and use this total ordering to make the choices unique. Given this ordering, we will order sets of α-valued sequences and subsets of α lexicographically.

In the rest of this article we state several existence results. However, in the proofs we typically use explicit constructions. When we write that a subset S (or a tuple of elements, etc.) we construct is uniquely determined, we understand that the result of the construction depends uniquely on the input data (which usually involves a totally ordered set α). This will be used to deduce that any automorphism fixing all the elements of α will also fix the set S. We will need this in the proof of Lemma 67. For more details see Section 4 after Remark 31.

Next we prove an "ordered" version of Lemma 20.

Lemma 21. *For all $N > 0$, $\Delta > 0$ there are integers $B = B_{\mathrm{irr}}(N, \Delta) \geq 0$ and $K = K_{\mathrm{irr}}(N, \Delta) \geq 0$ with the following property.*
Let $Z \subseteq \overline{\mathbb{F}}^m$ be a closed subset and $\alpha \subseteq \overline{\mathbb{F}}^m$ a totally ordered finite subset. Suppose that $0 < \dim(Z) \leq N$, $\deg(Z) \leq \Delta$ and $|\alpha \cap Z| \geq K$. Then we can choose an irreducible closed subset $Z' \subseteq Z$ such that $\dim(Z') > 0$, $\deg(Z') \leq B$ and

$$\mu(\alpha, Z') \geq \mu(\alpha, Z) - \log(B)\,.$$

Moreover, the subset Z' we construct is uniquely determined.

Proof. Assume $K > \Delta^{2N(N+1)^N}$, then

$$\mu(\alpha, Z) \geq \frac{\log(K)}{N} > \log\left(\Delta^{2(N+1)^N}\right). \tag{2}$$

We build by induction a sequence $Z = Z_0 \supset Z_1 \supset Z_2 \supset \cdots \supset Z_I$ of closed subsets such that for all $0 < i \leq I$

$$\begin{gathered} 0 < \dim(Z_i) < \dim(Z_{i-1}), \\ \deg(Z_i) \leq \deg(Z_{i-1})^{N+1} \leq \Delta^{(N+1)^i}, \\ \mu(\alpha, Z_i) \geq \mu(\alpha, Z) - \log\left(\Delta^{i(N+1)^{i-1}}\right). \end{gathered} \tag{3}$$

Since the dimensions are strictly decreasing, such a sequence has length $I+1 \leq N$. Suppose Z_i is already constructed. If Z_i is irreducible we stop the induction, set $Z' = Z_i$, and we are done.

Otherwise, $|\alpha \cap Z_i| > \Delta^{(N+1)^N} > \deg(Z_i)$ by (2) and (3). By Lemma 20 there is an irreducible component $Z_i' \subseteq Z_i$ such that $\dim(Z_i') > 0$ and

$$\mu(\alpha, Z_i') \geq \mu(\alpha, Z_i) - \log\left(\deg(Z_i)\right) \geq \mu(\alpha, Z) - \log\left(\Delta^{(i+1)(N+1)^i}\right). \tag{4}$$

It is possible that there are many choices for Z_i', however we choose one with $\alpha_i = \alpha \cap Z_i'$ lexicographically minimal. Note that α_i is uniquely determined, but Z_i' may not be. (This is the reason why Lemma 21 is more involved than Lemma 20.) Then $\mu(\alpha_i, Z_i') = \mu(\alpha, Z_i')$ and using (2) and (4) we obtain $|\alpha_i| > \deg(Z_i)^{N+1}$. If Z_i' is the only irreducible component containing α_i then it is uniquely determined by the above choice. We stop the induction, set $Z' = Z_i'$ and we are done.

Otherwise, let $T_1, T_2, \ldots$ denote those irreducible components of Z_i which contain α_i and let $Z_{i+1} = \bigcap^j T_j$. This subset is uniquely determined.

Next, we prove that for each closed subset $W \subseteq Z_i$ we have

$$\deg(W \cap Z_{i+1}) \leq \deg(W) \cdot \deg(Z_i)^{\dim(W)}. \tag{5}$$

We prove (5) by induction on $\dim(W)$, the case $\dim(W) = 0$ is obvious. Assume for a moment that W is irreducible. If it is contained in all T_j then $W \cap Z_{i+1} = W$ and (5) holds. On the other hand, if say $W \not\subseteq T_1$ then $W' = W \cap T_1$ has smaller dimension, hence satisfies the analog of (5). But $\deg(W') \leq \deg(W)\deg(T_1) \leq \deg(W)\deg(Z_i)$, so we have

$$\deg(W \cap Z_{i+1}) = \deg(W' \cap Z_{i+1}) \leq$$

$$\leq \deg(W')\deg(Z_i)^{\dim(W)-1} \leq \deg(W)\deg(Z_i)^{\dim(W)}$$

as we promised. For reducible W we simply add up the analogous inequalities for each component of W. So (5) is proved in general.

Applying (5) to $W = Z_i$ we see that $\deg(Z_{i+1}) \leq \deg(Z_i)^{N+1}$. Clearly $\dim(Z_{i+1}) < \dim(Z_i)$ and $\dim(Z_{i+1}) > 0$ by Remark 14. Moreover,

$$\mu(\alpha, Z_{i+1}) = \mu(\alpha_i, Z_{i+1}) > \mu(\alpha_i, Z_i') = \mu(\alpha, Z_i');$$

hence Z_{i+1} satisfies (3). The induction step is complete. However, the induction must stop in at most N steps which proves the lemma. □

Next, we show that the concentration in a closed subset X does not decrease too much when we map X somewhere by a "nice" morphism.

Lemma 22. *Let $Z \subseteq \overline{\mathbb{F}}^m$ be an irreducible closed subset, $\alpha \subset \overline{\mathbb{F}}^m$ be a totally ordered finite set with $\alpha \cap Z \neq \emptyset$, and $f : Z \to \overline{\mathbb{F}}^n$ be a morphism such that $\dim(Z) > \dim\big(\overline{f(Z)}\big) > 0$ and $\dim\big(Z\big) = \dim\big(\overline{f(Z)}\big) + \dim\big(f^{-1}(t)\big)$ for all $t \in f(\alpha \cap Z)$. Then there is a fiber $S = f^{-1}(s)$, $s \in f(\alpha \cap Z)$ such that for all parameters ε (negative, positive or 0) one has*

$$\text{either} \mu\big(f(\alpha \cap Z), \overline{f(Z)}\big) \geq \mu(\alpha, Z) - \varepsilon \dim(S) \tag{6}$$

$$\text{or} \mu\big(\alpha, S\big) \geq \mu(\alpha, Z) + \varepsilon \dim\big(\overline{f(Z)}\big). \tag{7}$$

Moreover, the closed subset S we construct is uniquely determined.

If all nonempty fibers of f have the same dimension then the condition $\dim\big(Z\big) = \dim\big(\overline{f(Z)}\big) + \dim\big(f^{-1}(t)\big)$ is satisfied by Fact 17.(e).

Proof. Let us consider those fibers $f^{-1}(t)$ where the number of points $\big|\alpha \cap f^{-1}(t)\big|$ is maximal, and let $S = f^{-1}(s)$ be the one among them for which the subset $\alpha \cap S \subseteq \alpha$ is lexicographically minimal. Then by assumption we have $0 < \dim(S) = \dim(Z) - \dim\big(\overline{f(Z)}\big) < \dim(Z)$. We have $\big|\alpha \cap Z\big| = \sum_{t \in f(\alpha \cap Z)} \big|\alpha \cap f^{-1}(t)\big|$, hence

$$\big|\alpha \cap Z\big| \leq \big|f(\alpha \cap Z)\big| \cdot \big|\alpha \cap S\big|.$$

We take the logarithm of our inequality and rewrite it in terms of concentrations:

$$\mu(\alpha, Z) \cdot \dim(Z) \leq \mu\big(f(\alpha \cap Z), \overline{f(Z)}\big) \cdot \dim(\overline{f(Z)}) + \mu\big(\alpha, S\big) \cdot \dim(S).$$

We divide both sides by $\dim(Z)$ and we introduce two extra terms involving ε on the right-hand side which cancel each other:

$$\mu(\alpha, Z) \leq \Big[\mu\big(f(\alpha \cap Z), \overline{f(Z)}\big) + \varepsilon \dim(S)\Big] \tfrac{\dim(\overline{f(Z)})}{\dim(Z)} + \Big[\mu\big(\alpha, S\big) - \varepsilon \dim\big(\overline{f(Z)}\big)\Big] \tfrac{\dim(S)}{\dim(Z)}.$$

On the right-hand side we see a weighted arithmetic mean of the two expressions in square brackets. We can certainly bound it it from above with the larger of them, which justifies our statement. □

Finally, we prove a variant of Lemma 22 which is our basic tool for transporting large concentration from one subset to another. The idea is that if the transport fails then we get an even larger concentration somewhere inside the first subset. Lemma 23 is a preliminary version valid for "nice"morphisms, the general result is the Transport Lemma 24.

Lemma 23. *For all parameters $\varepsilon \geq 0$ the following holds. Let $Z \subseteq \overline{\mathbb{F}}^m$ be an irreducible closed subset and $f : Z \to \overline{\mathbb{F}}^n$ be a morphism such that $\deg(Z) \leq \Delta$, $\deg(f) \leq \Delta$, and $\dim\big(\overline{f(Z)}\big) > 0$. Let $\alpha \subseteq Z$ be a totally ordered finite subset such that $\dim\big(Z\big) = \dim\big(\overline{f(Z)}\big) + \dim\big(f^{-1}(t)\big)$ for all $t \in f(\alpha)$. Then either*

$$\mu\big(f(\alpha), \overline{f(Z)}\big) \geq \mu(\alpha, Z) - \log(\Delta + 1) - \varepsilon \cdot \dim(Z) \tag{8}$$

or there is a closed subset $S \subset Z$ such that $\deg(S) \leq \Delta + 1$,
$0 < \dim(S) < \dim(Z)$ and

$$\mu(\alpha, S) \geq \mu(\alpha, Z) - \log(\Delta + 1) + \varepsilon\ . \tag{9}$$

Moreover, the closed subset S we construct is uniquely determined.

Note that the condition $\dim\big(\overline{f(Z)}\big) > 0$ implies that $\dim(Z) > 0$, hence the concentrations appearing in the lemma are defined.

Proof. If $\dim(Z) > \dim\left(\overline{f(Z)}\right)$ then we apply Lemma 22 with parameter ε. We get a fiber $S = f^{-1}(s)$ satisfying (6) or (7). By Fact 17.(c) S is closed and $\deg(S) \le \Delta$. If (6) holds then replacing $\varepsilon \dim(S)$ with $\varepsilon \dim(Z)$ we obtain (8). If (7) holds then replacing $\varepsilon \dim(\overline{f(Z)})$ with ε we obtain (9).

On the other hand, if $\dim(Z) = \dim\left(\overline{f(Z)}\right)$ then all points of α are contained in finite fibers of f, and the number of points in each finite fibe is at most $\deg(f) \le \Delta$ (see Fact 17.(c)). Hence,

$$\mu\Big(f(\alpha), \overline{f(Z)}\Big) = \frac{\log\big|f(\alpha)\big|}{\dim\left(\overline{f(Z)}\right)} \ge \frac{\log\left(\big|\alpha\big|/\Delta\right)}{\dim(Z)} \ge \mu(\alpha, Z) - \log(\Delta)\ . \qquad \square$$

Lemma 24 (Transport)**.** *For all parameters $\varepsilon \ge 0$ and all $\Delta > 0$ there is an integer $B = B_{\mathrm{transport}}(\Delta) \ge 2$ with the following property.*
Let $X \subseteq \overline{\mathbb{F}}^m$ be a closed subset, Z be an irreducible closed subset of X, and $f : X \to \overline{\mathbb{F}}^n$ be a morphism with $\deg(Z) \le \Delta$, $\deg(f) \le \Delta$ and $\dim\left(\overline{f(Z)}\right) > 0$. For each totally ordered finite subset $\alpha \subseteq X$ either

$$\mu\big(f(\alpha), \overline{f(Z)}\big) \ge \mu(\alpha, Z) - \log(B) - \varepsilon \cdot \dim(Z) \tag{10}$$

or there is a closed subset $S \subset Z$ such that $\deg(S) \le B$, $0 < \dim(S) < \dim(Z)$ and

$$\mu(\alpha, S) \ge \mu(\alpha, Z) - \log(B) + \varepsilon\ . \tag{11}$$

Moreover, the closed subset S we construct is uniquely determined.

Proof. To simplify notation we replace α with $\alpha \cap Z$, X with Z, Δ with Δ^2 (see Fact 17.(f)) and f with its restriction to Z, then $\alpha \subseteq Z$. If $\alpha = \emptyset$ then (10) holds automatically since the right hand side is $-\infty$. So we assume $\alpha \ne \emptyset$. This implies that $f(\alpha) \ne \emptyset$, hence the left hand side of (10) is non-negative. If $\mu(\alpha, Z) \le \log(B)$ then inequality (10) obviously holds since the right-hand side is nonpositive. So we assume $\mu(\alpha, Z) > \log(B)$ which implies $\big|\alpha\big| > B$.

We define the subset

$$\alpha' = \left\{ z \in \alpha \;\middle|\; \dim\left(f^{-1}(f(z))\right) = \dim(Z) - \dim\left(\overline{f(Z)}\right) \right\}\ .$$

First we deal with the case $|\alpha'| \ge \big|\alpha\big|/2$. We have

$$\mu(\alpha', Z) = \frac{\log\big|\alpha'\big|}{\dim(Z)} \ge \frac{\log\big|\alpha\big| - \log(2)}{\dim(Z)} \ge \mu(\alpha, Z) - \log(2)\ .$$

Assume that $B \ge 2 + 2\Delta$. We apply Lemma 23 with parameter ε to α' and Z. There are two possibilities. If Lemma 23.(8) holds then

$$\mu\big(f(\alpha), \overline{f(Z)}\big) \ge \mu\big(f(\alpha'), \overline{f(Z)}\big) \ge \mu(\alpha', Z) - \log(1+\Delta) - \varepsilon \cdot \dim(Z) \ge$$
$$\ge \mu(\alpha, Z) - \log(2 + 2\Delta) - \varepsilon \cdot \dim(Z)\ ,$$

which implies (10). If Lemma 23.(9) holds then we obtain a closed subset $S \subset Z$ such that $\deg(S) \le 1 + \Delta$, $0 < \dim(S) < \dim(Z)$ and

$$\mu(\alpha, S) \ge \mu(\alpha', S) \ge \mu(\alpha', Z) - \log(1+\Delta) + \varepsilon \ge$$
$$\ge \mu(\alpha, Z) - \log(2 + 2\Delta) + \varepsilon\ .$$

This implies (11).

In the remaining case we have $\big|\alpha'\big| < \big|\alpha\big|/2$. Setting

$$S = \left\{ z \in Z \;\middle|\; \dim\big(f^{-1}(f(z))\big) > \dim(Z) - \dim\big(\overline{f(Z)}\big) \right\}$$

we have $\big|\alpha \cap S\big| > \frac{1}{2}\big|\alpha\big|$. The irreducibility of Z implies (see Fact 17.(e) and Fact 16.(e)) that S is a closed subset of Z and $\dim(S) < \dim(Z)$, $\deg(S) \le \Delta'$ with a certain bound $\Delta' = \Delta'\big(\dim(Z), \Delta\big)$. We set

$$B = B_{\mathrm{transport}}(\Delta) = \max\big(2 + 2\Delta, 2\Delta'\big) .$$

The subset S has at least $|\alpha \cap S| > |\alpha|/2 \ge B/2 \ge \Delta'$ points, hence $\dim(S) > 0$ (see Remark 14). Therefore, $\mu(\alpha, S)$ is defined and

$$\mu(\alpha, S) = \frac{\log|\alpha \cap S|}{\dim(S)} \ge \frac{\log|\alpha| - \log(2)}{\dim(S)} \ge$$

$$\ge \frac{\dim(Z)}{\dim(S)}\mu(\alpha, Z) - \log(2) \ge \mu(\alpha, Z) - \log(B) + \frac{\mu(\alpha, Z)}{\dim(S)} .$$

We compare now the last term to ε. If $\varepsilon \le \frac{\mu(\alpha,Z)}{\dim(S)}$ then inequality (11) holds. On the other hand, if $\varepsilon > \frac{\mu(\alpha,Z)}{\dim(S)} \ge \frac{\mu(\alpha,Z)}{\dim(Z)}$ then inequality (10) holds, since its right-hand side becomes negative. □

4. Closed subsets and closed subgroups in algebraic groups

In this section we first consider various (Zariski-)closed subgroups of algebraic groups and give estimates on their degrees and other numerical invariants. Then we consider a class of morphisms $\tau_{\underline{g}}$ generalizing the conjugation map. In particular, we give two results, Lemma 32 and Lemma 34, which show that under favorable conditions the images of closed subsets under $\tau_{\underline{g}}$ are nice subsets of positive dimension. These will be used in the proof of the Spreading Theorem 40.

Definition 25. A *linear algebraic group* is a closed subgroup $G \le SL(n, \overline{\mathbb{F}})$. We use this matrix realisation of G to calculate degrees of closed subsets. We will denote by $\mathrm{mult}(G)$ and $\mathrm{inv}(G)$ the degrees of the morphisms $(g, h) \to gh$ and $g \to g^{-1}$.

Proposition 26. *If H is a closed subgroup of a linear algebraic group G then* $\mathrm{mult}(H) \le \deg(H)^2 \cdot \mathrm{mult}(G)$ *and* $\mathrm{inv}(H) \le \deg(H) \cdot \mathrm{inv}(G)$.

Proof. Follows immediately from Fact 17.(f) and Fact 16.(d). □

As usual, $\mathcal{Z}(G)$, $[G, G]$ and G^0 denote the center, the commutator subgroup, and the unit component of the algebraic group G. For any subset $A \subseteq G$ we denote by $\langle A\rangle$, $\mathcal{N}_G(A)$ and $\mathcal{C}_G(A)$ the generated subgroup, the normalizer and the centralizer of A. The subgroup $\mathcal{C}_G(A)^0$ is called the *connected centralizer* of A.

Centralizer subgroups of an algebraic group are defined by linear equations, and normalizers of a closed subset X, can be defined in terms of the equations of X. This proves the following.

Fact 27. *Let G be a linear algebraic group.*

(a) The centralizer $\mathcal{C}_G(X)$ of any subset $X \subseteq G$ is closed and its numerical invariants are bounded: $\deg\big(\mathcal{C}_G(X)\big) \le \deg(G)$, $\mathrm{mult}\big(\mathcal{C}_G(X)\big) \le \mathrm{mult}(G)$, *and* $\mathrm{inv}\big(\mathcal{C}_G(X)\big) \le \mathrm{inv}(G)$. *If X is closed then its normalizer $\mathcal{N}_G(X)$ is also*

closed and its numerical invariants are also bounded: $\deg\left(\mathcal{N}_G(X)\right) \leq \deg(G)\deg(X)^{\dim(G)}$, $\operatorname{mult}\left(\mathcal{N}_G(X)\right) \leq \operatorname{mult}(G)\deg(X)^{\dim(G)}$ *, and* $\operatorname{inv}\left(\mathcal{N}_G(X)\right) \leq \operatorname{inv}(G)\deg(X)^{\dim(G)}$.

(b) Cosets of a closed subgroup $H \leq G$ are also closed, they all have the same degree. Therefore, $\left|G : G^0\right| = \frac{\deg(G)}{\deg(G^0)} \leq \deg(G)$.

Definition 28. Let G be an algebraic group. We denote by $\prod^m G$ the m-fold direct product $G_1 \times G_2 \times \cdots \times G_m$ *with a fixed order of constituents*, where the G_i are identical copies of G. In other words, $\prod^m G$ is the set of all sequences $\underline{g} = (g_1, g_2, \ldots, g_m)$ of elements $g_i \in G$. Throughout the paper we refer to $\prod^m G$ with this fixed order of constituents. Let α be a finite subset of G. Using this fixed order we identify the m-fold product $\prod^m \alpha$ with the corresponding subset of $\prod^m G$. Similarly, if $Y_1, Y_2, \ldots, Y_m$ are closed subsets in G then we identify the product $Y_1 \times Y_2 \times \cdots \times Y_m$ with the corresponding subset of $\prod^m G = G_1 \times G_2 \times \cdots \times G_m$.

Fact 29. *Let G be a linear algebraic group. Suppose that $f : \prod^m G \to \prod^n G$ is a morphism for some integers $m, n > 0$ whose n coordinates are all defined to be product expressions (evaluated in the group G) of length at most k of some fixed group elements, the m variables and their inverses. Then* $\deg\left(\overline{f(G)}\right) \leq \deg(f) \leq \operatorname{inv}(G)^l \operatorname{mult}(G)^{n(k-1)}$ *where $l \leq nk$ denotes the total number of times inverted variables occur in the n expressions (see Fact* 17.(b)*).*

Definition 30. Let G be a linear algebraic group. For all $m > 0$ and for each sequence $\underline{g} = (g_1, g_2, \ldots, g_m)$, $g_i \in G$, we define the morphism $\tau_{\underline{g}} : \prod^m G \to G$ by $\tau_{\underline{g}}(a_1, \ldots, a_m) = (g_1^{-1} a_1 g_1)(g_2^{-1} a_2 g_2) \ldots (g_m^{-1} a_m g_m)$.

Remark 31. Let G be a linear algebraic group and $\underline{g} = (g_1, g_2, \ldots, g_m)$ be any sequence. Suppose that $\dim(G) \leq N$, $\deg(G) \leq \Delta$ and $\operatorname{mult}(G) \leq \Delta$ for certain values N and Δ. Conjugation by g_i is a linear transformation; hence, $\deg(\tau_{\underline{g}}) \leq \operatorname{mult}(G)^{m-1} \leq \Delta^{m-1}$.

In the proof of the Spreading Theorem 40 we will apply the Transport Lemma 24 to various morphisms of the form $\tau_{\underline{g}}$. In the rest of this section we construct the appropriate sequences $\underline{g}$.

As explained in Section 3, we will consider totally ordered sets α to make various subsets and subgroups constructed in our proofs uniquely determined. This will (only) be used through the proof of Lemma 67. There we will consider a linear algebraic group G over $\overline{\mathbb{F}_p}$, a Frobenius map $\sigma : G \to G$, a set α of fixpoints of σ (e.g., a generating set of $SL(n,p)$ inside $SL(n, \overline{\mathbb{F}_p})$). When we apply our lemmas the set α will change but $\langle \alpha \rangle$ will always remain the same (e.g., $SL(n,p)$). We fix a total ordering of $\langle \alpha \rangle$ and make our constructions depend only on this ordering and the input data. (In case the input data involves a product $\prod^m G$, the fixed order of the constituents is also considered part of the input, as we explained in Definition 28.) As a result, in each lemma, if the subsets and subgroups in the hypothesis are σ-invariant then the subsets and subgroups in the conclusion will also be σ-invariant, since σ fixes $\langle \alpha \rangle$ pointwise (hence it fixes the ordering as well).

The following lemma gives a morphism which maps a direct power of a given closed subset Y onto a closed subgroup H.

Lemma 32. *Let $Y \subseteq SL(n, \overline{\mathbb{F}})$ be an irreducible closed subset of positive dimension and $1 \in \alpha \subset SL(n, \overline{\mathbb{F}})$ a finite subset with a total ordering on $\langle \alpha \rangle$. Let $H \leq$*

$SL(n,\overline{\mathbb{F}})$ denote the smallest closed subgroup which is normalized by α and contains $Y^{-1}Y$. Suppose that $\dim(H)\le m$. Then there is a sequence $\underline{g}=(g_1,g_2,\dots,g_{2m})$ of elements $g_i\in\alpha^{m-1}$ such that

$$H=\tau_{\underline{g}}\left(\prod\nolimits^{2m}(Y^{-1}Y)\right)=(g_1^{-1}Y^{-1}Yg_1)(g_2^{-1}Y^{-1}Yg_2)\dots(g_{2m}^{-1}Y^{-1}Yg_{2m})\,.$$

The subgroup H is connected and there is a universal bound $\deg(H)\le\delta\big(m,\deg(\overline{Y^{-1}Y})\big)$. Moreover, H and the sequence $\underline{g}$ we construct are uniquely determined.

Proof. See Lemma 81 in Appendix A. □

Remark 33. Let $G\le SL(n,\overline{\mathbb{F}})$ be any closed subgroup normalized by α which contains Y such that $\deg(Y)\le\Delta$, $\mathrm{mult}(G)\le\Delta$, $\mathrm{inv}(G)\le\Delta$ for some $\Delta>0$. Then one may set $m=\dim(G)$ and one may also use the bound $\deg(\overline{Y^{-1}Y})\le\mathrm{inv}(G)\cdot\mathrm{mult}(G)\cdot\deg(Y)^2\le\Delta^4$ (see Fact 16.(d) and Fact 17.(f)).

The following lemma yields a morphism $\tau_{\underline{g}}$ which maps a given closed subset Z of some direct power of G onto a subset of G of positive dimension.

Lemma 34. *Let $G\le SL(n,\overline{\mathbb{F}})$ be a linear algebraic group and let $1\in\alpha\subset G$ be a finite subset with a total ordering on $\langle\alpha\rangle$. Suppose that the centralizer $\mathcal{C}_G(\alpha)$ is finite. Then for each integer $m\ge0$ and each irreducible closed subset $Z\subset\prod^m G$ of dimension $\dim(Z)>0$ there is a sequence $\underline{g}=(g_1,g_2,\dots,g_m)\in\prod^m\alpha$ such that $\overline{\tau_{\underline{g}}(Z)}$ has positive dimension. Moreover, the sequence $\underline{g}$ we construct is uniquely determined.*

Proof. See Lemma 83 in Appendix A. □

5. Spreading large concentration in a group

In this section we establish our main technical tool, the Spreading Theorem 40. Roughly speaking, it says the following. Let α be a finite subset in a connected linear algebraic group G such that $\mathcal{C}_G(\alpha)$ is finite. If G has a (Zariski-)closed subset X in which α has much larger concentration than in G then we can find a connected closed subgroup $H\le G$ normalized by α in which a small power of α has similarly large concentration. When G is the simple algebraic group used to define a finite group of Lie type L and α generates L then H turns out to be G itself. After the necessary definitions and a preparatory result (Lemma 38) we will give a detailed outline of the proof of the Spreading Theorem 40.

In the sketch above we considered sets α contained in the group G. To facilitate inductive proofs we actually have to handle the more general situation, when α is contained only in the normalizer of G in $SL(n,\overline{\mathbb{F}})$. This motivates the definitions below.

Definition 35. A *spreading system* $\alpha|G$ consists of a connected closed subgroup $G\le SL(n,\overline{\mathbb{F}})$ with $\dim(G)>0$, a finite symmetric subset $1\in\alpha\subset SL(n,\overline{\mathbb{F}})$ normalizing G such that $\mathcal{C}_G(\alpha)$ is finite, and a total ordering on $\langle\alpha\rangle$.

We say that $\alpha|G$ is (N,Δ,K)-*bounded* for some integers $N>0$, $\Delta>0$, $K>0$ if $\dim(G)\le N$, $\deg(G)\le\Delta$, $\mathrm{mult}(G)\le\Delta$, $\mathrm{inv}(G)\le\Delta$, and $\big|\alpha\cap G\big|\ge K$.

We say that $\alpha|G$ is $(\varepsilon,M,\tilde{\Delta})$-*spreading* for some real $\varepsilon>0$ and integers $M>0$, $\tilde{\Delta}>0$, if there is a connected closed subgroup $H\le G$ normalized by α such that

$\dim(H) > 0$ and

$$\deg(H) \le \tilde{\Delta}\,, \quad \mu\big(\alpha^M, H\big) \ge (1+\varepsilon)\cdot\mu(\alpha, G)\,.$$

We call such an H a *subgroup of spreading*. Note, that $\mathrm{mult}(H)$ and $\mathrm{inv}(H)$ are also bounded in terms of $\tilde{\Delta}$ and Δ by Proposition 26.

Remark 36. Let $\alpha|G$ be a spreading system. We will often use the fact that, if $\alpha^m|G$ is $(\varepsilon, M, \tilde{\Delta})$-spreading for some $m \ge 1$, then $\alpha|G$ is $(\varepsilon', M', \tilde{\Delta}')$-spreading (with the same subgroup of spreading) for all values $\varepsilon' \ge \varepsilon$, $M' \ge mM$ and $\tilde{\Delta}' \ge \tilde{\Delta}$.

Remark 37. For an informal reading of our arguments it may be helpful to assume that N, Δ, K, and $\frac{1}{\varepsilon}$ are bounded from above by some unspecified large function of n.

Suppose that for some $m \ge 0$ we find a closed subset $Z \subseteq \prod^m G$ in which $\prod^m \alpha$ has large concentration. We use the following lemma to find a closed subset of G in which the concentration of a small power of α is almost as large.

Lemma 38 (Back to G)**.** *For all $N > 0$ and $\Delta > 0$ there are integers $B = B_b(N,\Delta) > 0$ and $K = K_b(N,\Delta) \ge 0$ with the following property.*
Let $\alpha|G$ be a spreading system with $\dim(G) \le N$, $\deg(G) \le \Delta$ and $\mathrm{mult}(G) \le \Delta$. Then for all closed subsets $Z \subset \prod^m G$ with $0 < m \le N$, $\dim(Z) > 0$, $\deg(Z) \le \Delta$ and $\big|\prod^m \alpha \cap Z\big| \ge K$ there is a closed subset $Y \subseteq G$ such that $\dim(Y) > 0$, $\deg(Y) \le B$ and

$$\mu\big(\alpha^{3N}, Y\big) \ge \mu\big(\textstyle\prod^m \alpha, Z\big) - \log(B)\,.$$

Moreover, the closed subset Y we construct is uniquely determined.

Proof. We may replace α with $\alpha \cap G$, so we may assume that $\alpha \subseteq G$. Using the total ordering of $\langle\alpha\rangle$ we order $\prod^m \alpha$ lexicographically with respect to the fixed ordering of the constituents of $\prod^m G$ (see Definition 28). We assume $m \ge 2$. Since $\dim(Z) \le N^2$ it is sufficient to prove that our statement holds with appropriate bounds $B_{\mathrm{b}}\big(N, \Delta, \dim(Z)\big)$ and $K_{\mathrm{b}}\big(N, \Delta, \dim(Z)\big)$. We prove this by induction on $\dim(Z)$. If K is large enough then by Lemma 21 there is a (uniquely determined) positive dimensional irreducible closed subset $Z' \subseteq Z$ of degree $\deg(Z') \le B_{\mathrm{irr}}(N^2, \Delta)$ with large concentration:

$$\mu\big(\textstyle\prod^m \alpha, Z'\big) \ge \mu\big(\prod^m \alpha, Z\big) - \log\big(B_{\mathrm{irr}}(N^2,\Delta)\big)\,.$$

This implies immediately that

$$\Big|\textstyle\prod^m \alpha \cap Z'\Big| \ge \dfrac{|\prod^m \alpha \cap Z|^{\dim(Z')/\dim(Z)}}{B_{\mathrm{irr}}(N^2,\Delta)^{\dim(Z')}} \ge \dfrac{K^{1/N^2}}{B_{\mathrm{irr}}(N^2,\Delta)^{N^2}}\,.$$

By the above it is enough to complete the induction step for Z', so from now on we assume that Z is irreducible.

Lemma 34 gives us a (uniquely determined) sequence $\underline{g} = (g_1, g_2, \ldots, g_m) \in \prod^m \alpha$ such that the closed subset $T = \overline{\tau_{\underline{g}}(Z)} \subseteq G$ has positive dimension. We have $\deg(\tau_{\underline{g}}) \le \Delta^{N-1}$ by Remark 31 and $\deg(T) \le \deg(Z)\deg(\tau_{\underline{g}}) \le \Delta^N$ by Fact 17.(f).

We apply Lemma 24 with parameter $\varepsilon = 0$ to the two closed subsets $Z \subseteq X = \prod^m G$, to the morphism $f = \tau_{\underline{g}}$, and to the finite set $\prod^m \alpha$. Note that $\tau_{\underline{g}}\big(\prod^m \alpha\big) \subseteq \alpha^{3N}$. There are two possible outcomes. In case of Lemma 24.(10) the above closed subset $T = \overline{\tau_{\underline{g}}(Z)} \subseteq G$ satisfies

$$\mu\big(\textstyle\prod^m \alpha, Z\big) - \log(B') \le \mu\big(\tau_{\underline{g}}\big(\prod^m \alpha\big), T\big) \le \mu\big(\alpha^{3N}, T\big)\,,$$

where $B' = B_{\text{transport}}(\Delta^N)$. In this case we set $Y = T$, the induction step is complete.

In case of Lemma 24.(11) we obtain a closed subset $S \subset Z \subseteq \prod^m G$ with $0 < \dim(S) < \dim(Z)$, $\deg(S) \le B'$ and $\mu\big(\prod^m \alpha, S\big) \ge \mu\big(\prod^m \alpha, Z\big) - \log(B')$. This implies immediately that

$$\Big|\prod^m \alpha \cap S\Big| \ge \frac{|\prod^m \alpha \cap Z|^{\dim(S)/\dim(Z)}}{(B')^{\dim(S)}} \ge \frac{K^{1/N^2}}{(B')^{N^2}}$$

that is, we can make $\prod^m \alpha \cap S$ sufficiently large by choosing K large enough. We apply the induction hypothesis to this S. We obtain a closed subset $Y \subseteq G$ and a bound $B'' = B_{\text{b}}\big(N, B', \dim(S)\big)$ such that $\dim(Y) > 0$, $\deg(Y) \le B''$ and

$$\mu\big(\alpha^{3N}, Y\big) \ge \mu\big(\prod^m \alpha, S\big) - \log(B'') \ge \mu\big(\prod^m \alpha, Z\big) - \log\big(B'B''\big) .$$

This completes the induction step in this case as well. □

Now we give an outline of the proof of the Spreading Theorem 40 which avoids technicalities. Suppose that α has "large" concentration in a closed subset $X \subseteq G$. We would like to "spread" this large concentration as much as possible, i.e., we are looking for a small power α^M having large concentration in a subgroup H (more precisely, we need a subgroup of spreading H).

We start with $T_0 = X$ and proceed with a simple induction. Lemma 32 gives us a surjective morphism $\tau_{\underline{g}'}$ which maps $Z = \prod^{2\dim(G)}(X^{-1} \times X)$ (the direct product of $2\dim(G)$ copies of the direct product $(X^{-1} \times X)$) onto a subgroup $H \le G$. The concentration of the product set $\prod^{4\dim(G)}\alpha$ is large in Z, and we try to transport it via $\tau_{\underline{g}'}$ into H. Note, that our $\tau_{\underline{g}'}$ maps $\prod^{4\dim(G)}\alpha$ into a small power α^m. According to the Transport Lemma 24 we either succeed and therefore H is a subgroup of spreading,[5] or find a subset $S \subseteq Z$ with significantly larger concentration. This S lives in the direct product $\prod^{4\dim(G)}G$, but Lemma 38 brings it back to G, i.e., we find a subset $T_1 \subseteq G$ such that a small power α^{m_1} has significantly larger concentration in T_1 than α had in T_0 (see Lemma 39).

During the proof of the Spreading Theorem 40 we use Lemma 39 several times. Either at some point we quit the induction with a subgroup of spreading H, or we obtain a sequence of subsets $T_0, T_1, \dots$ with a quickly growing sequence of concentrations $\mu(\alpha^{m_i}, T_i)$. If we let the concentration grow sufficiently large, i.e., $\mu(\alpha^m, T_i) \ge \dim(G)\mu(\alpha, X)$ for some i, then already in T_i there are enough elements to force large concentration in G. Therefore, we either quit the induction with a subgroup of spreading, or in a bounded number of steps we conclude that $\mu(\alpha^{m_i}, G)$ is very large, i.e., G itself is a subgroup of spreading.

Lemma 39 (Try to Spread)**.** *For all $N > 0$, $\Delta > 0$ there are integers $M = M_t(N)$, $B = B_t(N, \Delta) > 0$, and $K = K_t(N, \Delta) > 0$ with the following property.*
Let $\alpha|G$ be an (N, Δ, K)-bounded spreading system and $Y \subset G$ be a closed subset such that $\dim(Y) > 0$, $\deg(Y) \le \Delta$ and $|\alpha \cap Y| \ge K$. For all parameters $\kappa \ge \log(B)$ one of the following holds:
Either there is a connected closed subgroup $H \le G$ normalized by α such that $\dim(H) > 0$, $\deg(H) \le B$ and

$$\mu\big(\alpha^M, H\big) \ge \mu(\alpha, Y) - \kappa \,, \tag{12}$$

[5]This part of the argument is related to what is called "sticking in different directions" in [28].

or there is a closed subset $T \subseteq G$ *with* $\deg(T) \leq B$, $\dim(T) > 0$ *and*

$$\mu\big(\alpha^M, T\big) \geq \mu(\alpha, Y) + \frac{\kappa}{8N^2}\,. \tag{13}$$

Moreover, the H *and* T *we construct are uniquely determined.*

Proof. We may replace α with $\alpha \cap G$, so we may assume that $\alpha \subseteq G$. Using Lemma 21 as in the proof of Lemma 38 we may assume that Y is irreducible.

Apply Lemma 32 to the subset Y, this gives us a (uniquely determined) sequence $\underline{g} = (g_1, g_2, \ldots, g_{2N}) \in \prod^{2N} \alpha^{N-1}$ so that $H = \tau_{\underline{g}}\big(\prod^{2N} Y^{-1}Y\big)$ is a (uniquely determined) connected closed subgroup normalized by α. Moreover, $\dim(H) > 0$ and $\deg(H) \leq \delta(N, \Delta^4)$ by Remark 33. Consider the sequence $\underline{g}' = (g_1, g_1, g_2, g_2, \ldots, g_{2N}, g_{2N})$.

In the product $X = \prod^{4N} G$ we consider the finite subset $\prod^{4N} \alpha$ and the closed subset $Z = \prod^{2N}(Y^{-1} \times Y)$. We order $\prod^{4N} \alpha$ lexicographically with respect to the fixed ordering of the constituents (see Definition 28). Apply Lemma 24 with parameter $\varepsilon = \varepsilon(N, \Delta, \kappa)$ to be specified later to X, Z, and to the morphism $f = \tau_{\underline{g}'}$, and to the finite set $\prod^{4N} \alpha$. Now Z is irreducible (see Fact 16.(f)) with $\dim(Z) \leq 4N^2$, $\deg(Z) = \deg(Y)^{4N} \operatorname{inv}(G)^{2N} \leq \Delta^{6N}$ (see Fact 16.(d) and Fact 17.(f)), and $\deg(f) \leq \Delta^{2N}$ (see Remark 31). The prerequisites of Lemma 24 are satisfied with degree bound Δ^{6N}, hence one of the inequalities 24.(10) or 24.(11) is valid. Moreover, $f(Z) = H$, $\mu\big(\prod^{4N} \alpha, Z\big) = \mu(\alpha, Y)$ and $f\big(\prod^{4N} \alpha\big) \subseteq \alpha^{4N^2}$.

In case of 24.(10), setting $B_{\text{transport}} = B_{\text{transport}}(\Delta^{6N})$, we have

$$\mu\big(\alpha^{4N^2}, H\big) = \mu\big(\alpha^{4N^2}, f(Z)\big) \geq \mu\big(f\big(\textstyle\prod^{4N} \alpha\big), f(Z)\big) \geq$$

$$\geq \mu\big(\textstyle\prod^{4N} \alpha, Z\big) - \log(B_{\text{transport}}) - \varepsilon \cdot \dim(Z) \geq \mu(\alpha, Y) - \kappa$$

and we are done, provided that we choose

$$\varepsilon \leq \frac{\kappa - \log(B_{\text{transport}})}{4N^2}\,. \tag{14}$$

In case of 24.(11) we obtain a closed subset $S \subseteq \prod^{4N} G$ such that $\dim(S) > 0$, $\deg(S) \leq B_{\text{transport}}$ and

$$\mu\big(\textstyle\prod^{4N} \alpha, S\big) \geq \mu\big(\prod^{4N} \alpha, Z\big) - \log(B_{\text{transport}}) + \varepsilon = \mu\big(\alpha, Y\big) - \log(B_{\text{transport}}) + \varepsilon\,.$$

In particular, if we choose $\varepsilon \geq \log(B_{\text{transport}})$ then

$$\big|\textstyle\prod^{4N} \alpha \cap S\big| \geq \big|\alpha \cap Y\big|^{\dim(S)/\dim(Y)} \geq K^{1/\dim(Y)}\,.$$

Hence, if we set K sufficiently large, then $\big|\prod^{4N} \alpha \cap S\big|$ is large enough and we may apply Lemma 38 to the subset $S \subseteq \prod^{4N} G$. We obtain our subset $T \subseteq G$ (denoted there by Y) such that, setting $B_{\text{b}} = B_{\text{b}}\big(4N, \max(\Delta, B_{\text{transport}})\big)$, we have $\dim(T) > 0$, $\deg(T) \leq B_{\text{b}}$ and

$$\mu(\alpha^{12N}, T) \geq \mu\big(\textstyle\prod^{4N} \alpha, S\big) - \log(B_{\text{b}}) \geq,$$

$$\geq \mu\big(\alpha, Y\big) - \log(B_{\text{transport}}) - \log(B_{\text{b}}) + \varepsilon = \mu\big(\alpha, Y\big) + \frac{\kappa}{8N^2},$$

i.e., inequality (13) holds in this case if we set

$$\varepsilon = \frac{\kappa}{8N^2} + \log(B_{\text{transport}}) + \log(B_{\text{b}})\,.$$

It is easy to check that if B, hence κ, is large enough then our ε satisfies inequality (14) and $\varepsilon \geq \log(B_{\text{transport}})$ as required. □

We actually have to prove the Spreading Theorem for closed subsets X contained in some power of the group G.

Theorem 40 (Spreading Theorem)**.** *For all parameters $\frac{1}{3} \geq \varepsilon > 0$ and for all $N > 0$, $\Delta > 0$ there are integers $M = M(N, \varepsilon)$, $K = K(N, \Delta, \varepsilon)$ and $\tilde{\Delta} = \tilde{\Delta}(N, \Delta, \varepsilon)$ with the following property.*
Let $\alpha|G$ be an (N, Δ, K)-bounded spreading system and X be a closed subset in $\prod^m G$ for some $0 < m \leq N$. If $\deg(X) \leq \Delta$, $\dim(X) > 0$ and

$$\mu\left(\prod^m \alpha, X\right) \geq (1 + 3\varepsilon) \cdot \mu(\alpha, G)$$

then $\alpha|G$ is $(\varepsilon, M, \tilde{\Delta})$-spreading. Moreover, the subgroup of spreading we construct is uniquely determined.

Proof. Using Lemma 38 we can easily reduce the theorem to the case $m = 1$, so we assume $X \subseteq G$. Then $\mu(\alpha, X) \geq \mu(\alpha, G) \geq \frac{\log(K)}{N}$.

Using Lemma 39 inductively we build a series of closed subsets $T_i \subseteq G$ such that, with appropriate positive integers $M_i = M_i(N)$, $\Delta_i = \Delta_i(N, \Delta)$,

$$\begin{cases} \dim(T_i) > 0\ , \quad \deg(T_i) \leq \Delta_i\ , \\ \mu\left(\alpha^{M_i}, T_i\right) \geq \left(1 + \frac{\varepsilon}{8N^2}\right)^i \cdot \mu(\alpha, X) \geq \frac{\log(K)}{N}\ . \end{cases} \tag{15}$$

In fact we set $\Delta_0 = \Delta$, $\Delta_i = \max\left(\Delta_{i-1}, B_{\mathrm{t}}(N, \Delta_{i-1})\right)$, $M_i = M_{\mathrm{t}}(N)^i$.

We run the induction until we either find an appropriate subgroup of spreading, or build the subset T_I, where $I = I(N, \varepsilon)$ is the smallest positive integer such that

$$\left(1 + \frac{\varepsilon}{8N^2}\right)^I \geq N\ . \tag{16}$$

We start with $T_0 = X$, this certainly satisfies (15) with $i = 0$. Assume that T_{i-1} is already constructed and $i \leq I$. We apply Lemma 39 to the closed subset $Y = T_{i-1}$ and to the finite set $\alpha^{M_{i-1}}$ with parameter

$$\kappa = \varepsilon \cdot \left(1 + \frac{\varepsilon}{8N^2}\right)^{i-1} \cdot \mu(\alpha, X)\ .$$

Since $\kappa \geq \varepsilon \cdot \mu(\alpha, X) \geq \frac{\varepsilon}{N} \cdot \log(K)$, for large enough K we have $\kappa \geq \log\left(B_{\mathrm{t}}(N, \Delta_{i-1})\right)$. Since $\left|\alpha^{M_{i-1}} \cap T_{i-1}\right| \geq \exp\left(\mu(\alpha^{M_{i-1}}, T_{i-1})\right) \geq K^{1/N}$, for large enough K we have $\left|\alpha^{M_{i-1}} \cap T_{i-1}\right| \geq K_{\mathrm{t}}(N, \Delta_{i-1})$ and the conditions of Lemma 39 hold. Note that with $M = M_I$ we have

$$\left(\alpha^{M_{i-1}}\right)^{M_{\mathrm{t}}(N)} = \alpha^{M_i} \subseteq \alpha^M\ .$$

There are two cases. If inequality 39.(13) holds with a subset T then

$$\mu\left(\alpha^{M_i}, T\right) \geq \mu(\alpha^{M_{i-1}}, T_{i-1}) + \frac{\kappa}{8N^2} \geq \left(1 + \frac{\varepsilon}{8N^2}\right)^{i-1} \cdot \mu(\alpha, X) +$$

$$+ \frac{\varepsilon}{8N^2}\left(1 + \frac{\varepsilon}{8N^2}\right)^{i-1} \cdot \mu(\alpha, X) = \left(1 + \frac{\varepsilon}{8N^2}\right)^i \cdot \mu(\alpha, X)$$

and $\deg(T) \leq B_{\mathrm{t}}(N, \Delta_{i-1}) \leq \Delta_i$, hence $T_i = T$ satisfies (15). On the other hand, if inequality 39.(12) holds with an appropriate subgroup H then $\deg(H) \leq$

$B_{\mathrm{t}}(N, \Delta_{i-1}) \leq \Delta_i$ and

$$\mu\big(\alpha^M, H\big) \geq \mu\big(\alpha^{M_i}, H\big) \geq \mu\big(\alpha^{M_{i-1}}, T_{i-1}\big) - \kappa \geq$$
$$\geq \Big(1 + \frac{\varepsilon}{8N^2}\Big)^{i-1} \cdot \mu(\alpha, X) - \varepsilon \cdot \Big(1 + \frac{\varepsilon}{8N^2}\Big)^{i-1} \cdot \mu(\alpha, X) \geq$$
$$\geq (1-\varepsilon) \cdot \mu(\alpha, X) \geq (1-\varepsilon)(1+3\varepsilon)\mu(\alpha, G) \geq (1+\varepsilon)\mu(\alpha, G)\ .$$

H is an appropriate subgroup of spreading, therefore we stop the induction.

Finally, we consider the case when the induction does not stop during the first I steps and we build T_I. Using the first inequality from Proposition 19 and inequalities (15) and (16) we obtain that

$$\mu(\alpha^M, G) \geq \tfrac{\dim(T_I)}{\dim(G)} \cdot \mu(\alpha^M, T_I) \geq$$
$$\geq \tfrac{1}{N} \cdot \big(1 + \tfrac{\varepsilon}{8N^2}\big)^I \cdot \mu(\alpha, X) \geq \mu(\alpha, X) \geq (1+3\varepsilon)\mu(\alpha, G)\ .$$

In this case G itself is an appropriate subgroup of spreading. □

6. CCC-subgroups

If G is a simple algebraic group then a maximal torus T can be obtained as the connected centralizer of a (regular semisimple) element. A key observation[6] of the proof of Theorem 2 is that, if a subset α of G does not grow and $\alpha \cap T$ contains a regular semisimple element, then for some small M the concentration $\mu\big(\alpha^M, T\big)$ is almost as large as $\mu(\alpha, G)$. Informally speaking T is a full torus. (This corresponds to the case (ii) of the outline of the proof for $SL(n, q)$ in the Introduction, i.e., when α covers a maximal torus.) This key observation is a very special case of the Centralizer Lemma 46 below.

We also have $T = \mathcal{C}_G(T)^0$. This motivates us to study connected centralizers of connected subgroups, i.e., CCC-subgroups, of arbitrary linear algebraic groups. CCC-subgroups have properties resembling those of maximal tori T. In particular, the duality property in Lemma 44 is a weak extension of the "self-duality" $T = \mathcal{C}_G(T)^0$. The Centralizer Lemma 46 implies that an extension of the above key observation in fact holds for arbitrary CCC-subgroups (see Remark 47).

Definition 41. Let G be an algebraic group and $X \subseteq G$ an irreducible closed subset. A *CC-generator*[7] of X is a $\dim(G)$-tuple $\underline{g} \in \prod^{\dim(G)} X$ such that $\mathcal{C}_G(\underline{g})^0 = \mathcal{C}_G(X)^0$. Let $X^{\mathrm{gen}} \subseteq \prod^{\dim(G)} X$ denote the set of all CC-generators (with respect to G), and let $X^{\mathrm{nongen}} = \big(\prod^{\dim(G)} X\big) \setminus X^{\mathrm{gen}}$ denote the complement.

Lemma 42. *Let G be a connected linear algebraic group and $\emptyset \neq X \subseteq G$ an irreducible closed subset. Then X^{nongen} is a proper closed subset of $\prod^{\dim(G)} X$ whose degree is bounded in terms of* $\dim(G)$, $\deg(G)$, $\mathrm{mult}(G)$, $\mathrm{inv}(G)$, *and* $\deg(X)$.

Proof. See Lemma 86 in Appendix A. □

Definition 43. Let G be an algebraic group. A closed subgroup $A < G$ is a *CCC-subgroup* if $A = \mathcal{C}_G(X)^0$ for some connected closed subgroup X and A is different from $\{1\}$ and G^0.

[6]Results of similar flavor play a crucial role in Helfgott's earlier work (see [27, Proposition 4.1] and [28, Proposition 5.8]), and in the work of Breuillard, Green, and Tao [10, Lemma 4.4].

[7]CC refers to "connected centralizer".

Lemma 44. *Let G be an algebraic group and $A < G$ a CCC-subgroup. Then A has the following duality property:*

$$\mathcal{C}_G\big(\mathcal{C}_G(A)^0\big)^0 = A\ .$$

Moreover, $\deg(A) \le \deg(G)$ *and* $\deg\left(A^{\mathrm{nongen}}\right)$ *is bounded in terms of* $\dim(G)$, $\deg(G)$, $\mathrm{mult}(G)$ *and* $\mathrm{inv}(G)$. *If $B \neq A$ is another CCC-subgroup then $A^{\mathrm{gen}} \cap B^{\mathrm{gen}} = \emptyset$.*

Proof. See Lemma 87 in Appendix A. □

We need the following basic fact.

Proposition 45. *Let $\alpha \subset SL(n, \overline{\mathbb{F}})$ be a symmetric subset and hH a coset of a closed subgroup $H \le SL(n, \overline{\mathbb{F}})$. If $hH \cap \alpha \neq \emptyset$ then*

$$\mu(\alpha^2, hH) \ge \mu(\alpha, H)\ , \quad \mu(\alpha^2, H) \ge \mu(\alpha, hH)\ .$$

□

Lemma 46 (Centralizer Lemma)**.** *For all parameters $\frac{1}{3} > \varepsilon > 0$ and for all $N > 0$, $\Delta > 0$ there are integers $M = M_{\mathrm{c}}(N, \varepsilon)$, $K = K_{\mathrm{c}}(N, \Delta, \varepsilon)$ and $\tilde{\Delta} = \tilde{\Delta}_{\mathrm{c}}(N, \Delta, \varepsilon)$ with the following property.*
Let $\alpha | G$ be an (N, Δ, K)-bounded spreading system and $C = \mathcal{C}_G(b_1, b_2, \dots, b_m)$ the centralizer of $m \le N$ elements $b_i \in \alpha \cap G$. If $0 < \dim(C)$ then either

$$\mu\big(\alpha^M, C^0\big) \ge \Big(1 - \varepsilon \cdot 8N\Big) \cdot \mu(\alpha, G)$$

or $\alpha | G$ is $(\varepsilon, M, \tilde{\Delta})$-spreading. Moreover, in the latter case the subgroup of spreading we construct is uniquely determined.

Proof. Note that $\dim(C^0) = \dim(C) > 0$ and $|C : C^0| \le \deg(C) \le \Delta$ by Fact 27. Combining this with Proposition 45, for some $h \in C$ we have $\mu\big(\alpha^M, C^0\big) \ge \mu(\alpha^{M/2}, hC^0) \ge \mu\big(\alpha^{M/2}, C\big) - \log\big(\Delta\big)$. Assume $K > \Delta^{1/\varepsilon}$. Then we have $\mu(\alpha, G) \ge \frac{1}{\dim(G)} \log(K) > \frac{1}{\varepsilon \cdot N} \log\big(\Delta\big)$.

By the above inequalities it is enough to prove that, for appropriate K, M, $\tilde{\Delta}$, either $\alpha | G$ is $(\varepsilon, M, \tilde{\Delta})$-spreading or

$$\mu\big(\alpha^{M/2}, C\big) \ge \Big(1 - \varepsilon \cdot 7N\Big) \cdot \mu(\alpha, G)\ . \tag{17}$$

If $\dim(C) = \dim(G)$ then $G = C$ and there is nothing to prove. So we assume $\dim(C) < \dim(G)$, and apply Lemma 22 to the subsets $Z = G$, α, and to the function

$$f : G \to \prod^m G\ , \quad f(g) = \big(\ g^{-1}b_1 g,\ g^{-1}b_2 g,\ \dots\ g^{-1}b_m g\ \big) \in \prod^m G$$

with the parameter $\varepsilon' = -7\varepsilon \frac{\mu(\alpha, G)}{\dim(C)}$. The fibers of f are just the right cosets of the subgroup C, which have equal dimension, hence we obtain a coset $S = Ca$ that satisfies one of the inequalities in Lemma 22: either

$$\mu(\alpha, G) \le \mu(\alpha, Ca) + 7\varepsilon \tfrac{\mu(\alpha, G)}{\dim(C)} \big(\dim(G) - \dim(C)\big) \le$$

$$\le \mu(\alpha, Ca) + \varepsilon \cdot 7 \dim(G) \cdot \mu(\alpha, G) \le \mu\big(\alpha^2, C\big) + \varepsilon \cdot 7N \cdot \mu(\alpha, G)$$

(see Proposition 45) and inequality (17) holds in this case, or else

$$\mu(\alpha, G) \le \mu\big(f(\alpha \cap G), \overline{f(G)}\big) - 7\varepsilon \tfrac{\mu(\alpha,G)}{\dim(C)} \dim(C) =$$

$$= \mu\big(f(\alpha \cap G), \overline{f(G)}\big) - 7\varepsilon \cdot \mu(\alpha, G) .$$

We know $f(\alpha \cap G) \subseteq \prod^m \alpha^3$ hence in this latter case we have

$$\mu\big(\prod^m \alpha^3, \overline{f(G)}\big) \ge (1 + 7\varepsilon) \cdot \mu(\alpha, G) .$$

If $\mu(\alpha^3, G) \ge (1 + \varepsilon)\mu(\alpha, G)$ then we are done. Otherwise,

$$(1 + 3\varepsilon)\, \mu(\alpha^3, G) \le (1 + 3\varepsilon)(1 + \varepsilon)\, \mu(\alpha, G) \le$$

$$\le (1 + 7\varepsilon)\mu(\alpha, G) \le \mu\big(\prod^m \alpha^3, \overline{f(G)}\big) .$$

Now $\deg\big(\overline{f(G)}\big) \le \Delta^{3m}$ by Fact 29. We apply the Spreading Theorem 40 with parameter ε to the spreading system $\alpha^3|G$ and $X = \overline{f(G)}$. We obtain that $\alpha^3|G$ is $(\varepsilon, M', \Delta')$-spreading for appropriate M' and Δ' values, hence $\alpha|G$ is $(\varepsilon, 3M', \Delta')$-spreading. □

Remark 47. In particular, Lemma 46 says that, if A is a CCC-subgroup of G and $(b_1, \dots, b_m)$ is a CC-generator of $\mathcal{C}_G(A)^0$ (see Lemma 44) such that all the b_i are contained in α, then either $\alpha|G$ is spreading or $\mu\big(\alpha^M, A\big)$ is almost as large as $\mu(\alpha, G)$. Informally speaking, A is a full CCC-subgroup.

7. Dichotomy

A central idea of the proof of Theorem 2 for $L = SL(n, q)$ (as outlined in the Introduction) is to establish the following fundamental dichotomy. If a generating set α of L does not grow then the intersection of α with any maximal torus of L is either relatively large or relatively small. Here we obtain a similar property of maximal tori A in $SL(n, \overline{\mathbb{F}_q})$: if α does not grow then either $|\alpha \cap A|$ is much smaller than $|\alpha|^{\frac{1}{n+1}}$ or $\big|\alpha^M \cap A\big|$ is almost as large as $|\alpha|^{\frac{1}{n+1}}$ for some small M. This is a special case of the Dichotomy Lemma 50 below. More generally, Lemma 50 implies that CCC-subgroups also satisfy a similar dichotomy.

The following result is closely related to "escape from subvarieties" type results of Helfgott; see [27, Lemma 4.4] and [28, Proposition 4.1].

Lemma 48 (Escape Lemma)**.** *For all parameters $\frac{1}{7N^2} \ge \varepsilon > 0$ and for all $N > 0$, $\Delta > 0$ there are integers $M = M(N, \varepsilon)$, $K = K(N, \Delta, \varepsilon)$ and $\tilde{\Delta} = \tilde{\Delta}(N, \Delta, \varepsilon)$ with the following property.*
Let $\alpha|G$ be an (N, Δ, K)-bounded spreading system and $X \subsetneq Y$ two closed subsets in $\prod^m G$ for some $1 \le m \le N$. Suppose that $\dim(Y) > 0$, Y is irreducible, $\deg(X) \le \Delta$ and

$$\mu\left(\prod^m \alpha, Y\right) \ge (1 - \varepsilon) \cdot \mu(\alpha, G) ,$$

$$\mu\big(\prod^m \alpha,\, Y \setminus X\big) \le (1 - 2\varepsilon) \cdot \mu(\alpha, G) .$$

Then $\alpha|G$ is $(\varepsilon, M, \tilde{\Delta})$-spreading. Moreover, the subgroup of spreading we construct is uniquely determined.

Proof. Assume $K \geq 2^{N/\varepsilon}$. Then $\mu(\alpha, G) \geq \frac{\log(K)}{N} \geq \frac{\log(2)}{\varepsilon}$, hence

$$\log\left(\frac{|\prod^m \alpha \cap Y|}{|\prod^m \alpha \cap (Y \setminus X)|}\right) = \dim(Y)\Big(\mu\big(\prod^m \alpha, Y\big) - \mu\big(\prod^m \alpha, Y \setminus X\big)\Big) \geq$$

$$\geq \dim(Y) \cdot \varepsilon \cdot \mu(\alpha, G) \geq \log(2) .$$

Assume $K \geq (2\Delta+1)^{N/(1-\varepsilon)}$. Then $|\prod^m \alpha \cap X| \geq \frac{1}{2}|\prod^m \alpha \cap Y| \geq \frac{1}{2}|\alpha \cap G|^{(1-\varepsilon)\dim(Y)/\dim(G)} > \Delta$, hence $\dim(X) > 0$ and

$$\mu\left(\prod^m \alpha, X\right) \geq \tfrac{\dim(Y)}{\dim(X)} \mu\left(\prod^m \alpha, Y\right) - \log(2) \geq$$

$$\geq \left(1 + \tfrac{1}{\dim(X)}\right)(1-\varepsilon) \cdot \mu(\alpha, G) - \log(2) \geq (1+7\varepsilon)(1-\varepsilon) \cdot \mu(\alpha, G) - \log(2) \geq$$

$$\geq \big(1+5\varepsilon\big) \cdot \mu(\alpha, G) - \varepsilon \cdot \mu(\alpha, G) > (1+3\varepsilon) \cdot \mu(\alpha, G) .$$

Then we are done by the Spreading Theorem 40. □

Now we prove that if a set α does not grow (or spread), then for any closed subset Z either the intersection of α with Z is relatively small or a small power of α has relatively large intersection with the connected centralizer of Z. We will prove the Dichotomy Lemma 50 by applying this twice.

Lemma 49 (Asymmetric Dichotomy Lemma)**.** *For all parameters $0 < \varepsilon < \frac{1}{56N^3}$ and for all $N > 0$, $\Delta > 0$ there are integers $M = M(N, \varepsilon)$, $K = K(N, \Delta, \varepsilon)$ and $\tilde{\Delta} = \tilde{\Delta}(N, \Delta, \varepsilon)$ with the following property.*
Let $\alpha | G$ be an (N, Δ, K)-bounded spreading system. Then either $\alpha | G$ is $(\varepsilon, M, \tilde{\Delta})$-spreading or, for all irreducible closed subsets $Z \subseteq G$ such that $\dim(Z) > 0$, $\deg(Z) \leq \Delta$ and $\dim\big(\mathcal{C}_G(Z)\big) > 0$, one of the following holds:

$$\mu\left(\alpha, Z\right) < \big(1 - \tfrac{1}{7N^2}\big) \cdot \mu(\alpha, G)$$

or

$$\mu\big(\alpha^M, \mathcal{C}_G(Z)^0\big) \geq \mu\left(\prod^{\dim(G)} \alpha^M,\ \big(\mathcal{C}_G(Z)^0\big)^{\mathrm{gen}}\right) \geq \Big(1 - \varepsilon \cdot 16N\Big) \cdot \mu(\alpha, G) .$$

Moreover, the subgroup of spreading we construct is uniquely determined.

Proof. First, we apply the Escape Lemma 48 with parameter $\varepsilon' = \frac{1}{7N^2}$ to $\alpha | G$ and to the following closed subsets of $\prod^m G$.

$$Y' = \prod^{\dim(G)} Z \quad \supseteq \quad X' = Z^{\mathrm{nongen}}.$$

Note that $\deg(X')$ is bounded in terms of N, Δ (see Lemma 42). If we obtain an appropriate subgroup of spreading then we are done. Otherwise, there are two possibilities. Either

$$\mu(\alpha, Z) = \mu\left(\prod^{\dim(G)} \alpha, Y'\right) < (1-\varepsilon') \cdot \mu(\alpha, G) = \big(1 - \tfrac{1}{7N^2}\big) \cdot \mu(\alpha, G) ,$$

in which case the lemma holds, or else there is at least one $\dim(G)$-tuple $\underline{g} \in \prod^{\dim(G)} \alpha \cap Z^{\mathrm{gen}}$. We select the lexicographically minimal $\underline{g}$ among them, and we apply the Centralizer Lemma 46 with parameter ε to the spreading system $\alpha | G$ and the subgroup $C = \mathcal{C}_G(\underline{g})$. Note that $\mathcal{C}_G(\underline{g})^0 = \mathcal{C}_G(Z)^0 \neq \{1\}$, hence $\dim(C) > 0$, and $\deg(C) \leq \Delta$ by Fact 27. In this case we obtain an appropriate subgroup of spreading, the lemma holds. Otherwise, for an appropriate integer $M'' > 0$ we have

$$\mu\big(\alpha^{M''}, \mathcal{C}_G(Z)^0\big) \geq \big(1 - \varepsilon \cdot 8N\big) \cdot \mu(\alpha, G) . \tag{18}$$

Finally, we apply the Escape Lemma 48 with parameter $\varepsilon''' = \varepsilon \cdot 8N$ to the spreading system $\alpha^{M''}|G$ and the closed subsets

$$Y''' = \prod^{\dim(G)} \mathcal{C}_G(Z)^0 \quad \supseteq \quad X''' = \left(\mathcal{C}_G(Z)^0\right)^{\text{nongen}} .$$

Note, that $\deg(X''')$ is bounded in terms of Δ, N (see Lemma 42). Again, the lemma holds if we obtain an appropriate subgroup of spreading. Otherwise, by (18) and Proposition 19 we have

$$\mu\left(\prod^{\dim(G)} \alpha^{M''},\ \left(\mathcal{C}_G(Z)^0\right)^{\text{gen}}\right) > (1 - 2\varepsilon''') \cdot \mu(\alpha, G) = \Big(1 - \varepsilon \cdot 16N\Big)\mu(\alpha, G) .$$

Assume $M \geq M''$. The lemma follows from the following calculation using Proposition 19:

$$\mu\big(\alpha^M, \mathcal{C}_G(Z)^0\big) = \mu\big(\prod^{\dim(G)} \alpha^M, Y'''\big) \geq$$

$$\geq \mu\big(\prod^{\dim(G)} \alpha^M, (Y''' \setminus X''')\big) = \mu\left(\prod^{\dim(G)} \alpha^M,\ \left(\mathcal{C}_G(Z)^0\right)^{\text{gen}}\right) .$$

□

The connected centralizer of the connected centralizer of a CCC-subgroup A is A itself (see Lemma 44). Hence, applying the previous lemma twice, we obtain the following.

Lemma 50 (Dichotomy Lemma)**.** *For all parameters $0 < \varepsilon < \frac{1}{119N^3}$ and for all $N > 0$, $\Delta > 0$ there are integers $M = M(N, \varepsilon)$, $K = K(N, \Delta, \varepsilon)$ and $\tilde{\Delta} = \tilde{\Delta}(N, \Delta, \varepsilon)$ with the following property.*
Let $\alpha|G$ be an (N, Δ, K)-bounded spreading system. Then either $\alpha|G$ is $(\varepsilon, M, \tilde{\Delta})$-spreading or, for all CCC-subgroups $A < G$, one of the following holds:

$$\mu(\alpha, A) < \left(1 - \tfrac{1}{7N^2}\right) \cdot \mu(\alpha, G)$$

or else

$$\mu\big(\alpha^M, A\big) \geq \mu\left(\prod^{\dim(G)} \alpha^M,\ A^{\text{gen}}\right) \geq \Big(1 - \varepsilon \cdot 16N\Big) \cdot \mu(\alpha, G) .$$

Moreover, the subgroup of spreading we construct is uniquely determined.

Proof. We apply the Asymmetric Dichotomy Lemma 49 with parameter ε to $\alpha|G$ and the irreducible subset $Z' = A$. Note that $\dim(A) > 0$, $\dim\left(\mathcal{C}_G(A)\right) > 0$ and $\deg(A) \leq \Delta$ by Definition 43 and Lemma 44. If we obtain an appropriate subgroup of spreading or if

$$\mu(\alpha, A) < \left(1 - \tfrac{1}{7N^2}\right) \cdot \mu(\alpha, G)$$

then the lemma holds. Otherwise, or an appropriate M' , we have

$$\mu\big(\alpha^{M'}, \mathcal{C}_G(A)^0\big) \geq \Big(1 - \varepsilon \cdot 16N\Big) \cdot \mu(\alpha, G) . \tag{19}$$

We apply again the Asymmetric Dichotomy Lemma 49 with parameter ε to $\alpha^{M'}|G$ and $Z'' = \mathcal{C}_G(A)^0$. If we obtain an appropriate subgroup of spreading then we are done. Otherwise, $\alpha^{M'}|G$ and Z'' must satisfy one of the two inequalities of that lemma. The first one is $\mu\left(\alpha^{M'}, \mathcal{C}_G(A)^0\right) < \left(1 - \frac{1}{7N^2}\right) \cdot \mu(\alpha^{M'}, G)$. But $(1 - \frac{1}{7N^2})(1 + \varepsilon) < 1 - \varepsilon 16N$, hence using (19) we see that $\mu(\alpha^{M'}, G) \geq (1 + \varepsilon)\mu(\alpha, G)$. So G is an appropriate subgroup of spreading and we are done in this case. The

other inequality is

$$\mu\left(\left(\alpha^{M'}\right)^{M'},\, \mathcal{C}_G\big(\mathcal{C}_G(A)^0\big)^0\right) \geq$$

$$\geq \mu\left(\prod^{\dim(G)}\alpha^{M'\cdot M'},\, \left(\mathcal{C}_G\big(\mathcal{C}_G(A)^0\big)^0\right)^{\mathrm{gen}}\right) \geq \Big(1-\varepsilon\cdot 16N\Big)\mu(\alpha,G)\,,$$

and we are done since $\mathcal{C}_G\big(\mathcal{C}_G(A)^0\big)^0 = A$ by Lemma 44. □

8. Finding and using full CCC-subgroups

The starting point for the proof of Theorem 2 for $SL(n,q)$ (as outlined in the Introduction) is to find at least one full maximal torus. In this section we first show that, more generally, if G is a non-nilpotent algebraic group and $\alpha|G$ is a spreading system which does not spread then we can find a CCC-subgroup A which is full in a similar sense (see Theorem 52).

Furthermore, if our G is a simple algebraic group then $A = T$ is a full maximal torus of G. Using this we can show that if α does not grow then α itself must be "very large" compared to $\langle\alpha\rangle$.[8] We actually obtain a similar result for non-normal CCC-subgroups of arbitrary connected linear algebraic groups G (see Theorem 54.(b)). The proof of this result corresponds to the part of the argument for $SL(n,q)$ where we try to grow our set by conjugating full tori.

We also prove an analogous result for the case when $\langle\alpha\rangle$ is not finite (see Theorem 54.(a)). This will be used in the proof of Theorem 6.

The next lemma extends the fact that in a simple algebraic group almost all elements are regular semisimple.

Lemma 51. *Let G be a non-abelian connected linear algebraic group and $\mathcal{S} \subseteq G$ the closure of the set of those elements $g \in G$ whose centralizer is either the whole of G or does not contain any maximal torus. Then* $\dim(\mathcal{S}) < \dim(G)$ *and* $\deg(\mathcal{S})$ *is bounded in terms of* $\dim(G)$, $\deg(G)$.

Proof. Let $A \leq G$ be a Cartan subgroup. (See [15, Sections 7.1 and 7.2] for the basic properties of Cartan subgroups that we use.) Then $A = \mathcal{C}_G(T)$ for some maximal torus $T \leq G$. For each $g \in A$ we have $T \leq \mathcal{C}_G(g)$. All Cartan subgroups are conjugates of A, hence their union, denoted by $\mathcal{R}$, is the image of the conjugation map $f : A \times G \to G$, $f(a,g) = g^{-1}ag$. It is well known that $\mathcal{R}$ contains an open subset U of G and by definition $\overline{G\setminus\mathcal{R}} \subseteq G \setminus U$, so $\dim\left(\overline{G\setminus\mathcal{R}}\right) < \dim(G)$ (see Fact 16.(e)). Moreover, $\deg\left(\overline{G\setminus\mathcal{R}}\right)$ is bounded in terms of $\dim(G)$ and $\deg(G)$ (see Fact 17.(d)). We also know that $\deg\big(\mathcal{Z}(G)\big) \leq \deg(G)$ (see Fact 27). Hence, $\mathcal{S} = \left(\overline{G\setminus\mathcal{R}}\right) \cup \mathcal{Z}(G)$ also has bounded degree. □

Theorem 52 (Finding full CCC-subgroups)**.** *For all parameters $0 < \varepsilon \leq \frac{1}{56N^3}$ and for all $N > 0$, $\Delta > 0$ there are integers $M = M(N,\varepsilon)$, $K = K(N,\Delta,\varepsilon)$ and $\tilde{\Delta} = \tilde{\Delta}(N,\Delta,\varepsilon)$ with the following property.*
Let $\alpha|G$ be an (N,Δ,K)-bounded spreading system such that G is non-nilpotent. Then either it is $(\varepsilon, M, \tilde{\Delta})$-spreading, or there is a non-normal CCC-subgroup $A \leq G$ which contains exactly one maximal torus of G and satisfies

$$\mu\big(\alpha^M, A\big) > (1-\varepsilon\cdot 17N)\mu(\alpha^M, G)\,. \tag{20}$$

[8] This may be viewed as an abstract version of Theorem 2.

Moreover, the subgroup A and the subgroup of spreading, whichever we construct, are uniquely determined.

Proof. Recall from the Centralizer Lemma 46 the constant $M_c = M_c(N, \varepsilon)$.

We set $g_0 = 1 \in G$, $G_0 = G$, and define by induction on i the elements $g_i \in \alpha^{(M_c)^{i-1}} \cap G$ in such a way that the connected subgroups

$$G_i = \mathcal{C}_G(g_0, g_1, g_2, \ldots, g_i)^0 = \mathcal{C}_{G_{i-1}}(g_i)^0$$

satisfy

$$\mu\left(\alpha^{(M_c)^i}, G_i\right) \geq \Big(1 - \varepsilon \cdot 8N\Big)\mu(\alpha, G)\ , \tag{21}$$

all G_i contain some maximal torus of G and they form a strictly decreasing series of subgroups (necessarily of length at most N).

Suppose that such a G_i is already defined for some $i \geq 0$. If it is abelian then we stop the induction. Otherwise, we apply Lemma 51 to the group G_i and obtain a subset $\mathcal{S}_i \subsetneq G_i$. Then $\deg(\mathcal{S}_i)$ is bounded in terms of N and Δ, and $\deg(G_i) \leq \Delta$ by Fact 27. We apply the Escape Lemma 48 with parameter $\varepsilon' = \varepsilon \cdot 8N$ to $\alpha^{(M_c)^i}|G$ and the subsets $X = \mathcal{S}_i$ and $Y = G_i$ of G. If we obtain an appropriate subgroup of spreading then we are done. Otherwise, since (21) holds, we find at least one element

$$g_{i+1} \in \alpha^{(M_c)^i} \cap \left(G_i \setminus \mathcal{S}_i\right)\ .$$

We select the g_{i+1} which is minimal in the total order of $\langle\alpha\rangle$. According to the definition of $\mathcal{S}_i$, the subgroup $G_{i+1} = \left(G_i \cap \mathcal{C}_G(g_{i+1})\right)^0$ contains a maximal torus of G_i, which is also a maximal torus in G, and G_{i+1} is strictly smaller than G_i. We apply the Centralizer Lemma 46 with parameter ε to $\alpha^{(M_c)^i}|G$ and the subgroup $\mathcal{C}_G(g_0, \ldots, g_{i+1})$. If we obtain an appropriate subgroup of spreading then we are done. Otherwise, G_{i+1} satisfies (21), as shown by the following calculation:

$$\mu\left(\alpha^{(M_c)^i M_c}, G_{i+1}\right) \geq \Big(1 - \varepsilon \cdot 8N\Big) \cdot \mu(\alpha^{(M_c)^i}, G) \geq \Big(1 - \varepsilon \cdot 8N\Big)\mu(\alpha, G).$$

Since $\dim(G_i)$ decreases in each step, the induction must stop, and for some $I \leq N$ we arrive at a connected abelian subgroup G_I which contains a maximal torus T and satisfies inequality (21).

We set $A = \mathcal{C}_G(G_I)^0$. On the one hand, T commutes with G_I, hence $T \leq A$. On the other hand $A = \mathcal{C}_G(G_I)^0 \leq \mathcal{C}_G(T)$, and the latter one is a Cartan subgroup, which has a unique maximal torus. Therefore, T is the only maximal torus in A. But G is non-nilpotent, so it has several (conjugate) maximal tori. Therefore A is a non-normal CCC-subgroup. We apply the Asymmetric Dichotomy Lemma 49 with parameter ε to $\alpha^{(M_c)^N}|G$ and the subset $Z = G_I$. If we obtain an appropriate subgroup of spreading then we are done. Otherwise, since G_I satisfies (21) and $\varepsilon \cdot 8N \leq \frac{1}{7N^2}$, for an appropriate integer M we obtain that

$$\mu(\alpha^M, A) \geq (1 - \varepsilon \cdot 16N)\, \mu(\alpha, G) > (1 - \varepsilon \cdot 17N)\, (1 + \varepsilon)\, \mu(\alpha, G)\ .$$

If $\mu(\alpha^M, G) \leq (1 + \varepsilon)\, \mu(\alpha, G)$ then (20) holds. Otherwise G itself is an appropriate subgroup of spreading and we are done again. □

The following useful lemma shows that growth in a subgroup of G implies growth in G itself. See [28, Section 7] for similar results.

Lemma 53. *Let $A \le G \le SL(n,\overline{\mathbb{F}})$ be closed subgroups and $1 \in \alpha \subset SL(n,\overline{\mathbb{F}})$ a finite subset. Then for all integers $k > 0$ one has*

$$\mu\big(\alpha^{k+1},G\big) \ge \mu\big(\alpha,G\big) + \tfrac{\dim(A)}{\dim(G)}\Big[\mu\big(\alpha^k,A\big) - \mu\big(\alpha^{-1}\alpha,A\big)\Big]$$

or equivalently $\dfrac{\left|\alpha^{k+1}\cap G\right|}{\left|\alpha\cap G\right|} \ge \dfrac{\left|\alpha^k\cap A\right|}{\left|\alpha^{-1}\alpha\cap A\right|}$.

Proof. The two inequalities are clearly equivalent, we will prove the latter form. We will look at the multiplication map

$$(\alpha\cap G)\times\big(\alpha^k\cap A\big) \xrightarrow{\ \phi\ } (\alpha\cap G)\cdot\big(\alpha^k\cap A\big) \subseteq \big(\alpha^{k+1}\cap G\big).$$

On the left-hand side we have $|\alpha\cap G|\cdot\left|\alpha^k\cap A\right|$ elements; on the right-hand side there are $\left|\alpha^{k+1}\cap G\right|$ elements. Therefore, it is enough to prove that $\left|\phi^{-1}(g)\right| \le \left|\alpha^{-1}\alpha\cap A\right|$ for all $g\in\alpha^{k+1}\cap G$, and this follows from the calculation below:

$$\phi^{-1}(g) \subseteq \big\{(a,a^{-1}g)\ \big|\ a\in\alpha,\ a^{-1}g\in A\big\} \subseteq \big\{(a,a^{-1}g)\ \big|\ a\in\alpha\cap gA\big\}\ ,$$

hence $\left|\phi^{-1}(g)\right| \le \left|\alpha\cap gA\right| \le \left|(\alpha\cap gA)^{-1}(\alpha\cap gA)\right| \le \left|\alpha^{-1}\alpha\cap A\right|$. □

It is crucial in the proofs of our main theorems to find sufficiently many $\langle\alpha\rangle$-conjugates of a CCC-subgroup $A\le G$. Accordingly, conditions (a) and (b) of the lemma below express the fact that the number of conjugates, $\left|\langle\alpha\rangle : \mathcal{N}_{\langle\alpha\rangle}(A)\right|$, is relatively large compared to $|\alpha|$.

Theorem 54 (Using full CCC-subgroups)**.** *For all parameters $\frac{1}{119N^3} > \varepsilon > 0$ and for all $N>0$, $\Delta>0$ there are integers $M = M(N,\varepsilon)$, $K = K(N,\Delta,\varepsilon)$ and $\tilde\Delta = \tilde\Delta(N,\Delta,\varepsilon)$ with the following property.*
Let $\alpha|G$ be an (N,Δ,K)-bounded spreading system and $A<G$ a CCC-subgroup such that

$$\mu(\alpha,A) > \big(1-\tfrac{1}{7N^2}\big)\cdot\mu(\alpha,G)\ .$$

Suppose that at least one of the following holds:

(a) $\left|\langle\alpha\rangle : \mathcal{N}_{\langle\alpha\rangle}(A)\right| \ge \left|\alpha\right|^{2N}$,

(b) $\alpha\subset G$, *A is not normal in G and*

$$\mu(\alpha,G) = \frac{\log|\alpha|}{\dim(G)} \le \Big(1-\varepsilon\cdot 64N^3\Big)\cdot\frac{\log\left|\langle\alpha\rangle : \mathcal{N}_{\langle\alpha\rangle}(A)\right|}{\dim(G)-\dim\big(\mathcal{N}_G(A)\big)}\ .$$

Then $\alpha|G$ is $(\varepsilon,M,\tilde\Delta)$-spreading. Moreover, the subgroup of spreading we construct is uniquely determined.

Proof. By Lemma 44 the conjugate subsets $h^{-1}A^{\mathrm{gen}}h$ for various h normalising G are pairwise disjoint or coincide. They are all contained in $\prod^{\dim(G)}G$ which has dimension $\dim(G)^2\le N^2$.

In case (b) we consider the following set:

$$X = \bigcup\Big\{h^{-1}A^{\mathrm{gen}}h\ \Big|\ h\in G\Big\} \subseteq \prod^{\dim(G)}G\ .$$

Then $\dim\big(\overline{X}\big) \le N^2$. Consider the conjugation map $\phi : G\times\overline{A^{\mathrm{gen}}} \to \prod^{\dim(G)}G$

defined as $\phi(h,\underline{a}) = h^{-1}\underline{a}h$ (note that $\overline{A^{\rm gen}} = \prod^{\dim(G)} A$). By definition $X = \phi\big(G \times A^{\rm gen}\big)$ hence $\overline{X} = \overline{\mathrm{im}(\phi)}$ and $\deg(\overline{X})$ is bounded in terms of N and Δ (see Fact 17.(f)). Consider any pair $(h_0, \underline{a_0}) \in G \times A^{\rm gen}$ and its image $x = h_0^{-1}\underline{a_0}h_0 \in X$. The corresponding fiber is

$$\phi^{-1}(x) = \left\{ (nh_0, n\underline{a}_0 n^{-1}) \,\middle|\, n \in \mathcal{N}_G(A) \right\} ,$$

which is isomorphic (in the sense of Definition 15) to $\mathcal{N}_G(A)$. In particular, $G \times A^{\rm gen}$ (which is open and dense in the domain of ϕ) is the union of fibers of dimension $\dim\big(\mathcal{N}_G(A)\big)$. Therefore,

$$\dim(\overline{X}) = \dim\left(A^{\rm gen}\right) + \Big[\dim(G) - \dim\left(\mathcal{N}_G(A)\right)\Big] > \dim\left(A^{\rm gen}\right)$$

(apply Fact 17.(e) to the irreducible subset $G \times \overline{A^{\rm gen}}$).

We consider in both cases all the conjugate subgroups

$$\mathcal{A} = \left\{ t^{-1}At \;\middle|\; t \in \langle\alpha\rangle \right\} ;$$

they are all CCC-subgroups of G since α normalizes G.

In case (a) we have $\log\big|\mathcal{A}\big| \geq 2N \log|\alpha|$ by assumption. In case (b), with the shorthand notation $\varepsilon'' = \varepsilon \cdot 16N$, we obtain

$$\begin{aligned}
\log\big|\mathcal{A}\big| = \log\Big|\langle\alpha\rangle : \mathcal{N}_{\langle\alpha\rangle}(A)\Big| \geq \Big[\dim(G) - \dim\left(\mathcal{N}_G(A)\right)\Big] \cdot \tfrac{1}{1-\varepsilon\cdot 64N^3} \cdot \mu(\alpha, G) = \\
= \big[\dim(\overline{X}) - \dim(A^{\rm gen})\big] \cdot \tfrac{1}{1-\varepsilon\cdot 64N^3} \cdot \mu(\alpha, G) > \\
> \big[\dim(\overline{X}) - \dim(A^{\rm gen})\big] \cdot \big(1 + \varepsilon'' \cdot 4\dim(\overline{X})\big) \cdot \mu(\alpha, G) .
\end{aligned}$$

Suppose first that for all $B \in \mathcal{A}$

$$\mu\big(\alpha^2, B\big) \geq \big(1 - \tfrac{1}{7N^2}\big)\, \mu(\alpha, G) . \tag{22}$$

We apply the Dichotomy Lemma 50 with parameter ε to $\alpha^2|G$ and to each $B \in \mathcal{A}$. If we obtain a subgroup of spreading then we are done. Otherwise, for an appropriate integer $M' = M'(N, \varepsilon)$,

$$\mu\Big(\prod^{\dim(G)} \alpha^{2M'}, B^{\rm gen}\Big) \geq \Big(1 - \varepsilon \cdot 16N\Big)\mu(\alpha^2, G) \geq (1 - \varepsilon'')\mu(\alpha, G)$$

for all $B \in \mathcal{A}$. Hence, $\prod^{\dim(G)} \alpha^{2M'}$ intersects each $B^{\rm gen}$. By Lemma 44 the subsets $B^{\rm gen}$ are pairwise disjoint. In case (b) we obtain

$$\begin{aligned}
\mu\left(\prod^{\dim(G)} \alpha^{2M'}, \overline{X}\right) = \tfrac{1}{\dim(\overline{X})} \log\left|\prod^{\dim(G)} \alpha^{2M'} \cap \overline{X}\right| \geq \\
\geq \tfrac{1}{\dim(\overline{X})} \log\left(\sum_{B\in\mathcal{A}} \left|\prod^{\dim(G)} \alpha^{2M'} \cap B^{\rm gen}\right|\right) \geq \\
\geq \tfrac{1}{\dim(\overline{X})} \left[\log\big|\mathcal{A}\big| + \log\left(\min_{B\in\mathcal{A}} \left|\prod^{\dim(G)} \alpha^{2M'} \cap B^{\rm gen}\right|\right)\right] = \\
\geq \tfrac{1}{\dim(\overline{X})} \left[\log\big|\mathcal{A}\big| + \dim(A^{\rm gen}) \cdot \min_{B\in\mathcal{A}} \left(\mu\left(\prod^{\dim(G)} \alpha^{2M'}, B^{\rm gen}\right)\right)\right] \geq \\
\geq \tfrac{1}{\dim(\overline{X})} \Big[\log\big|\mathcal{A}\big| + \dim(A^{\rm gen}) \cdot (1 - \varepsilon'')\, \mu(\alpha, G)\Big] \geq \\
\geq \tfrac{1}{\dim(\overline{X})} \Big[\big[\dim(\overline{X}) - \dim(A^{\rm gen})\big] \cdot \big(1 + \varepsilon'' \cdot 4\dim(\overline{X})\big)\mu(\alpha, G) + \\
+ \dim(A^{\rm gen}) \cdot (1 - \varepsilon'')\, \mu(\alpha, G)\Big] =
\end{aligned}$$

$$= \Big[1 + 4\varepsilon''\big(\dim(\overline{X}) - \dim(A^{\mathrm{gen}})\big) - \varepsilon''\tfrac{\dim(A^{\mathrm{gen}})}{\dim(\overline{X})}\Big]\,\mu(\alpha, G) >$$

$$> \big(1 + 3\varepsilon''\big)\cdot\mu(\alpha, G)\ .$$

In case (a) a similar, but much shorter, calculation shows that

$$\mu\left(\prod^{\dim(G)}\alpha^{2M'}, \prod^{\dim(G)} G\right) \geq \tfrac{\log|\mathcal{A}|}{\dim(G)^2} \geq \tfrac{2\log|\alpha|}{\dim(G)} \geq (1 + 3\varepsilon'')\mu(\alpha, G)\ .$$

Next, we apply the Spreading Theorem 40 with parameter ε'' to $\alpha^{2M'}|G$, and in case (a) to the subset $Z'' = \prod^{\dim(G)} G$, in case (b) to the subset $Z'' = \overline{X}$. We get an appropriate subgroup of spreading, we are done.

Finally, we assume that condition (22) fails for some member of $\mathcal{A}$. As A itself satisfies (22), there must be at least one subgroup $B_0 \in \mathcal{A}$ and an element $b \in \alpha$ such that B_0 satisfies (22) but $b^{-1}B_0 b$ doesn't:

$$\mu\big(\alpha^2, b^{-1}B_0 b\big) < \big(1 - \tfrac{1}{7N^2}\big)\,\mu(\alpha, G)\ . \tag{23}$$

Conjugation with b transforms (22) into

$$\mu\big(\alpha^4, b^{-1}B_0 b\big) \geq \mu\big(b^{-1}\alpha^2 b, b^{-1}B_0 b\big) = \mu\big(\alpha^2, B_0\big) > \big(1 - \tfrac{1}{7N^2}\big)\ \mu(\alpha, G)\ .$$

Again, we apply the Dichotomy Lemma 50 with parameter ε to $\alpha^4|G$ and the CCC-subgroup $b^{-1}B_0 b$. Either we obtain an appropriate subgroup of spreading, and the lemma holds in this case, or

$$\mu\big(\alpha^{4M'}, b^{-1}B_0 b\big) \geq \big(1 - \varepsilon\cdot 16N\big)\mu(\alpha, G)\ .$$

Now we compare this to inequality (23) and apply Lemma 53 with $k = 4M'$ to the subgroup $b^{-1}B_0 b$. We obtain that

$$\mu\big(\alpha^{4M'+1}, G\big) \geq \mu(\alpha, G) + \tfrac{\dim(b^{-1}B_0 b)}{\dim(G)}\,\big[\tfrac{1}{7N^2} - \varepsilon\cdot 16N\big]\,\mu(\alpha, G) \geq$$

$$\geq \mu(\alpha, G) + \tfrac{1}{N}\,\big[\tfrac{1}{7N^2} - \varepsilon\cdot 16N\big]\,\mu(\alpha, G) =$$

$$= \big[1 + \tfrac{1}{7N^3} - 16\varepsilon\big]\,\mu(\alpha, G) \geq (1 + \varepsilon)\,\mu(\alpha, G)\ ,$$

hence G itself is an appropriate subgroup of spreading for $\alpha|G$. □

9. The proof of Theorem 6

Combining our general results on algebraic groups, Theorem 52 and Theorem 54, we first prove a kind of "spreading lemma" (Lemma 58) for spreading systems $\alpha|G$ with $\langle\alpha\rangle \cap G$ not virtually nilpotent. Using this we show that, if α is a large non-growing subset of $SL(n, \overline{\mathbb{F}})$, $\overline{\mathbb{F}}$ an algebraically closed field (of any characteristic), then $\langle\alpha\rangle \cap H$ is virtually nilpotent for an appropriate closed subgroup H (see Lemma 59). Theorem 6 will follow by an inductive argument.

We need a few basic results.

Proposition 55 (Freiman [20], [21])**.** *Let α be a finite subset of a group G. If $|\alpha\cdot\alpha| < \frac{3}{2}|\alpha|$, then $S := \alpha\cdot\alpha^{-1}$ is a finite group of order $|\alpha\cdot\alpha|$, and $\alpha \subset S\cdot x = x\cdot S$ for some x in the normalizer of S.*

For the following useful result of Helfgott see [27, proof of Lemma 2.2] (see also [53]). A similar result follows from an old argument of Ruzsa and Turjányi [52] who considered the case of abelian groups.

Proposition 56 (Helfgott)**.** *Let α be a finite subset of a group. Then:*

a) $$\frac{\left|\left(\alpha \cup \alpha^{-1} \cup \{1\}\right)^3\right|}{|\alpha|} \leq \left(3\frac{\left|\alpha^3\right|}{|\alpha|}\right)^3$$

b) If $1 \in \alpha = \alpha^{-1}$ (i.e., α is symmetric) and $m \geq 2$ then

$$\frac{\left|\alpha^m\right|}{|\alpha|} \leq \left(\frac{\left|\alpha^3\right|}{|\alpha|}\right)^{m-2}$$

Proposition 57. *Let $1 \in \alpha = \alpha^{-1}$ be a finite subset of a group G, $\tilde{G} = G/N$ a quotient of G and $\tilde{\alpha} = \alpha N/N$. Then $\left(|\alpha^3|/|\alpha|\right)^2 \geq |\tilde{\alpha}^3|/|\tilde{\alpha}|$.*

Proof. There is a coset gN of N such that $|\alpha \cap gN| \geq |\alpha|/|\tilde{\alpha}|$ and $g \in \alpha$. Let $\{g_i\}$ be a system of representatives of the cosets in $\tilde{\alpha}^3$ with $g_i \in \alpha^3$. Then the sets $g_i(\alpha \cap gN)$ are disjoint subsets of α^4 hence $\left|\alpha^4\right| \geq \left|\tilde{\alpha}^3\right||\alpha|/|\tilde{\alpha}|$. Our statement follows then from Proposition 56.(b). □

Lemma 58. *For all parameters $\frac{1}{119N^3} > \varepsilon > 0$ and for all $N > 0$, $\Delta > 0$ there are integers $M = M_\infty(N, \varepsilon) > 0$, $K = K_\infty(N, \Delta, \varepsilon) > 0$, and $\tilde{\Delta} = \tilde{\Delta}_\infty(N, \Delta, \varepsilon) > 0$ with the following property.*
Let $\alpha|G$ be an (N, Δ, K)-bounded spreading system. Then either $\langle\alpha\rangle \cap G$ is virtually nilpotent or $\alpha|G$ is $(\varepsilon, M, \tilde{\Delta})$-spreading.

Proof. Assume that G is non-nilpotent. Using Theorem 52, either we obtain an appropriate subgroup of spreading, or we obtain a non-normal CCC-subgroup $A \leq G$ containing a single maximal torus T, and an integer M' such that

$$\mu\left(\alpha^{M'}, A\right) > (1 - \varepsilon \cdot 17N)\, \mu(\alpha^{M'}, G) > \left(1 - \tfrac{1}{7N^2}\right) \mu(\alpha^{M'}, G)\ .$$

If A has infinitely many $\langle\alpha\rangle$-conjugates then, for appropriate M'' and $\tilde{\Delta}''$, $\alpha^{M'}|G$ is $(\varepsilon, M'', \tilde{\Delta}'')$-spreading by Theorem 54 and we are done. Otherwise, A has finitely many $\langle\alpha\rangle$-conjugates. Then T has finitely many $\langle\alpha\rangle$-conjugates, hence $\langle\alpha\rangle \cap \mathcal{N}_G(T)$ has finite index in $\langle\alpha\rangle \cap G$.

Now $\mathcal{C}_G(T)$ is a Cartan subgroup, so it is nilpotent and has finite index in its normalizer. But $\mathcal{N}_G(T) = \mathcal{N}_G\left(\mathcal{C}_G(T)\right)$ hence $\mathcal{N}_G(T)$, and therefore $\langle\alpha\rangle \cap G$, is virtually nilpotent □

In the proof of the next lemma we apply Lemma 58, then apply it to the subgroup of spreading, then apply it again to the new subgroup of spreading, and so on, until we arrive at a subgroup of positive dimension whose intersection with $\langle\alpha\rangle$ is virtually nilpotent.

Lemma 59. *Let $G \leq SL(n, \overline{\mathbb{F}})$ be a closed subgroup and $\alpha \subseteq G$ a finite subset such that $\dim(G) \geq 1$, $\deg(G) \leq \Delta$ and $\left|\alpha^3\right| \leq \mathcal{K}|\alpha|$ for some $\mathcal{K}$. Then either $|\alpha| \leq \mathcal{K}^m$ for some integer $m = m_{\mathrm{nilp}}(n, \Delta)$, or one can find a connected closed subgroup $H \leq G$ normalized by α such that $\dim(H) \geq 1$, $\deg(H)$ is bounded in terms of n and Δ, and $\langle\alpha\rangle \cap H$ is virtually nilpotent.*

Proof. By Proposition 56.(a) and Proposition 55 we may suppose that $1 \in \alpha = \alpha^{-1}$ and $\mathcal{K} \geq \frac{3}{2}$. If $\mathcal{C}_G(\alpha)$ is infinite then we take $H = \mathcal{C}_G(\alpha)^0$ (see Fact 27). So we assume that $\mathcal{C}_G(\alpha)$ is finite. We totally order the subgroup $\langle\alpha\rangle$, this turns $\alpha|G$ into a spreading system. It is clear that $\dim(G) \leq n^2$. Assume also that $|\alpha| > \mathcal{K}^m$.

During the proof we encounter several lower bounds for m, we assume that our m satisfies them all. Similarly, we will establish several alternative upper bounds on $\deg(H)$.

By assumption $|G : G^0| \leq \Delta$, hence $|\alpha^2 \cap G^0| \geq \frac{|\alpha|}{\Delta}$. We set $\varepsilon = \frac{1}{120n^6}$, $G_0 = G^0$, and construct by induction a sequence of connected closed subgroups $G_0 > G_1 > G_2 > \dots$ normalized by α and corresponding constants e_i, $\tilde{\Delta}_i$ such that

$$\dim(G_i) \geq 1\,, \quad \deg(G_i) \leq \tilde{\Delta}_i\,, \quad \left|\alpha^{e_i} \cap G_i\right| \geq \left(\tfrac{|\alpha|}{\Delta}\right)^{\dim(G_i)/n^2}\,. \tag{24}$$

It will be clear from the construction that all of the appearing constants (i.e., e_i, K_i, $\tilde{\Delta}_i$, Δ_i and M, see below) depend only on n and Δ since ε depends on n. We already defined G_0, our statement holds with $\tilde{\Delta}_0 = \Delta$ and $e_0 = 2$. Suppose that G_i, $\tilde{\Delta}_i$ and e_i are already constructed for some $i \geq 0$. We assume that $\langle\alpha\rangle \cap G_i$ is not virtually nilpotent, since otherwise the lemma holds with $H = G_i$. According to Proposition 26 the numerical invariants $\deg(G_i)$, $\mathrm{mult}(G_i)$ and $\mathrm{inv}(G_i)$ are bounded from above by a certain constant $\Delta_i = \Delta_i(n^2, \tilde{\Delta}_i)$. Recall from Lemma 58 the constants $M = M_\infty(n^2, \varepsilon)$, $K_{i+1} = K_\infty(n^2, \Delta_i, \varepsilon)$ and $\tilde{\Delta}_{i+1} = \tilde{\Delta}_\infty(n^2, \Delta_i, \varepsilon)$. We assume that m is large enough so that $|\alpha| > \mathcal{K}^m > \left(\frac{3}{2}\right)^m > (K_{i+1})^{n^2}\Delta$. Then, by (24), $\alpha^{e_i}|G_i$ is an (n^2, Δ_i, K_{i+1})-bounded spreading system. The same is true for $\alpha^e|G_i$ for all $e \geq e_i$, hence according to Lemma 58 they are all $(\varepsilon, M, \tilde{\Delta}_{i+1})$-spreading.

Consider the spreading systems $\alpha^{e_i M^j}|G_i$ for $j = 0, 1, 2, \dots J-1$, where $J = 2\frac{n^2}{\varepsilon} = 240n^8$.

We claim that there is a value $j < J$ such that the corresponding subgroup of spreading (obtained above using Lemma 58) is a proper subgroup of G_i. Otherwise, for each j, G_i itself is the corresponding subgroup of spreading, i.e., $\mu\big(\alpha^{e_i M^{j+1}}, G_i\big) \geq (1+\varepsilon)\mu\big(\alpha^{e_i M^j}, G_i\big)$. This implies $\mu\big(\alpha^{e_i M^J}, G_i\big) \geq (1+\varepsilon)^J \mu(\alpha, G_i)$, and using (24) we obtain

$$\left|\alpha^{e_i M^J} \cap G_i\right| \geq \left|\alpha^{e_i} \cap G_i\right|^{(1+\varepsilon)^J} > \left(\tfrac{|\alpha|}{\Delta}\right)^{J\varepsilon/n^2} = \left(\tfrac{|\alpha|}{\Delta}\right)^2 \geq |\alpha|\tfrac{\mathcal{K}^m}{\Delta^2}\,.$$

On the other hand, by Proposition 56.(b) we have $\left|\alpha^{e_i M^J}\right| \leq |\alpha|\mathcal{K}^{e_i M^J - 2}$. We rule this case out by choosing, say, $m \geq e_i M^J + \Delta^2$.

Let $j_0 < J$ be the smallest value such that the above claim holds. Let G_{i+1} be the subgroup of spreading corresponding to j_0 and set $e_{i+1} = e_i M^J$. We have $\mu\big(\alpha^{e_i M^{j_0+1}}, G_{i+1}\big) \geq (1+\varepsilon)\mu\big(\alpha^{e_i M^{j_0}}, G_i\big)$, hence

$$\left|\alpha^{e_{i+1}} \cap G_{i+1}\right| \geq \left|\alpha^{e_i M^{j_0+1}} \cap G_{i+1}\right| \geq \left|\alpha^{e_i M^{j_0}} \cap G_i\right|^{\frac{\dim(G_{i+1})}{\dim(G_i)}} \geq$$

$$\geq \left|\alpha^{e_i} \cap G_i\right|^{\frac{\dim(G_{i+1})}{\dim(G_i)}} \geq \left(\tfrac{|\alpha|}{\Delta}\right)^{\frac{\dim(G_i)}{n^2}\,\frac{\dim(G_{i+1})}{\dim(G_i)}} \geq \left(\tfrac{|\alpha|}{\Delta}\right)^{\frac{\dim(G_{i+1})}{n^2}}\,,$$

the induction step is complete. The dimensions $\dim(G_i)$ strictly decrease as i grows, hence the induction must stop in at most n^2 steps. But the only way it can stop is to produce the required subgroup H. □

We prove Theorem 6 by iterating Lemma 59. For the iteration we need the following (more explicit) version of Chevalley's theorem on quotients of algebraic groups (see [33, Theorem 11.5]).

Proposition 60. *Let H be a closed subgroup of $SL(n,\overline{\mathbb{F}})$. For some $n'=n'\big(n,\deg(H)\big)$ there is a homomorphism $\mathcal{N}_{SL(n,\overline{\mathbb{F}})}(H)\to SL(n',\overline{\mathbb{F}})$ of degree bounded in terms of n and $\deg(H)$ whose kernel is H.*

Proof. See Proposition 90 in Appendix A. □

Now we prove Theorem 6. In the proof we need an auxiliary subgroup G in order to do induction on $\dim(G)$. The important case is $G=SL(n,\overline{\mathbb{F}})$, $\deg(G)=1$.

Theorem 61. *Let $G\le SL(n,\overline{\mathbb{F}})$ be a closed subgroup and $\alpha\subseteq G$ a finite subset such that $\big|\alpha^3\big|\le\mathcal{K}|\alpha|$ for some $\mathcal{K}$. Then there is a virtually soluble normal subgroup $\Gamma\lhd\langle\alpha\rangle$ and a bound $m=m\big(n,\deg(G)\big)$ such that the subset α can be covered by $\mathcal{K}^m$ cosets of Γ.*

Proof. By Proposition 56.(a) and Proposition 55 we may suppose that $1\in\alpha=\alpha^{-1}$ and $\mathcal{K}\ge\frac{3}{2}$. We prove the theorem by induction on $\dim(G)$. If $\dim(G)=0$ then $|\alpha|\le\deg(G)$ and we are done. We will apply Lemma 59, assume that $m\ge m_{\mathrm{nilp}}\big(n,\deg(G)\big)$. If $|\alpha|\le\mathcal{K}^m$ then we are done. Otherwise , we obtain a closed subgroup H normalized by α such that $\langle\alpha\rangle\cap H$ is virtually nilpotent, $\dim(H)\ge1$, and $\deg(H)$ is bounded in terms of n and $\deg(G)$.

Consider the algebraic group $\overline{G}=\mathcal{N}_G(H)/H$, let $\overline{\alpha}\subseteq\overline{G}$ denote the image of α. By Proposition 57 we have $|\overline{\alpha}^3|\le\mathcal{K}^2|\overline{\alpha}|$. By Proposition 60 and Fact 17.(f) there is an embedding $\overline{G}\le SL(n',\overline{\mathbb{F}})$ where n' and $\deg(\overline{G})$ are bounded in terms of n and $\deg(G)$. Clearly $\dim(\overline{G})<\dim(G)$, so by the induction hypothesis we obtain a virtually soluble normal subgroup $\overline{\Gamma}\lhd\langle\overline{\alpha}\rangle$ such that $\overline{\alpha}$ is covered by $\mathcal{K}^{2m(n',\deg(\overline{G}))}$ cosets of $\overline{\Gamma}$. We define Γ to be the preimage of $\overline{\Gamma}$ in $\langle\alpha\rangle$. Then Γ is virtually soluble since the class of virtually soluble groups is closed under extensions (see, e.g., [36]). The induction step is complete. □

10. The proof of Theorem 2

Simple groups of Lie type can be treated as very large subgroups of fixpoint groups G^σ of Frobenius maps of simple algebraic groups G (see [37, §5.4] for details). Combining our general results on algebraic groups, Theorem 52 and Theorem 54, with Hrushovski's twisted Lang-Weil estimates we obtain a general lemma (Lemma 67) concerning growth of subsets in fixpoint groups of Frobenius maps. Theorem 2 will follow easily. Another application of Lemma 67, for not necessarily simple groups, will be the proof of Theorem 5 in Section 11.

To prove Theorem 2 we also need some finite group-theoretic results.

Proposition 62 (Olson [47])**.** *Let $1\in\alpha$ be a generating set of a finite group G and β a nonempty subset of G. Then $|\alpha\beta|\ge\min\big(|\beta|+|\alpha|/2,|G|\big)$. In particular, if $\alpha^3\ne L$ then $|\alpha^3|\ge2|\alpha|$.*

A result of Gowers [25] implies the following.

Proposition 63 (Nikolov, Pyber [45])**.** *Let G be a finite group and let k denote the minimal degree of a complex representation. If α is a subset of G such that $|\alpha|>|G|/\sqrt[3]{k}$ then $\alpha^3=G$.*

A Frobenius map $\sigma:G\to G$ has a power σ^k which is a standard Frobenius map $Frob_q$, i.e., the q-th power map. We set $q_\sigma=\sqrt[k]{q}$.

Proposition 64. *Let G be a simple algebraic group and $\sigma : G \to G$ a Frobenius map. If L is the simple group of Lie type obtained as a composition factor of G^σ then the minimal degree of a complex representation of L is at least $\frac{q_\sigma - 1}{2}$. If $q_\sigma \geq 20$ and $\alpha \subseteq L$ is a subset of size at least $q_\sigma^{\dim(G)-\frac{1}{4}}$ then $\alpha^3 = L$.*

Proof. The first statement is an obvious consequence of the Landazuri-Seitz lower bounds ([40] cf. [37, Table 5.3A]). If $q_\sigma \geq 4$ then $|L| \leq q_\sigma^{\dim(G)}$ (see [13]). The second statement follows from Proposition 63. □

We will use the powerful twisted Lang-Weil estimates (see [30, Theorem 1.1] and the discussion afterward).

Proposition 65 (Hrushovski)**.** *Let G be a connected linear algebraic group and $\sigma : G \to G$ a Frobenius map. Then there is a constant $C = C\big(\dim(G), \deg(G)\big)$ such that $|G^\sigma|$ is approximately $q_\sigma^{\dim(G)}$ with error*

$$\Big||G^\sigma| - q_\sigma^{\dim(G)}\Big| \leq C \cdot q_\sigma^{\dim(G)-\frac{1}{2}} .$$

In the following corollary, besides various technical estimates, we establish that the finite group G^σ (if it is large enough) reflects the group-theoretic properties of G.

Corollary 66. *Let G be a connected linear algebraic group, $\sigma : G \to G$ a Frobenius map and α a subset of G^σ. Suppose that $\dim(G) \leq N$, $\deg(G) \leq \Delta$, $\big|G^\sigma : \langle\alpha\rangle\big| \leq I$. There is an integer K which depends on N, Δ, and I such that if $|\alpha| \geq K$ then the following holds.*

(a) Let $A < G$ be a proper σ-invariant closed subgroup of degree $\deg(A) \leq \Delta$. Then $\langle\alpha\rangle \cap A \neq \langle\alpha\rangle$ and

$$\Big|\langle\alpha\rangle : \langle\alpha\rangle \cap A\Big| > \frac{1}{4I\Delta}\Big|\langle\alpha\rangle\Big|^{1-\dim(A)/\dim(G)}$$

(b) If A is not normal in G then α does not normalize A and

$$\Big|\langle\alpha\rangle : \mathcal{N}_{\langle\alpha\rangle}(A)\Big| > \tfrac{1}{c}\, q_\sigma^{\dim(G)-\dim(\mathcal{N}_G(A))}$$

for some positive integer c which depends on N, Δ and I.

(c) $\mathcal{C}_G(\alpha) = \mathcal{Z}(G)$.

Proof. By Proposition 65 we have $K \leq |\alpha| \leq |G^\sigma| \leq (1+C)q_\sigma^N$, hence by choosing K large enough one can force q_σ to be arbitrary large.

By Proposition 65 for large enough q_σ we have $|G^\sigma| \geq \frac{1}{2}\, q_\sigma^{\dim(G)}$, i.e., $q_\sigma \leq \big(2|G^\sigma|\big)^{\frac{1}{\dim(G)}}$. On the other hand, $\big|(A^0)^\sigma\big| \leq 2\, q_\sigma^{\dim(A)} \leq 2\big(2|G^\sigma|\big)^{\frac{\dim(A)}{\dim(G)}} \leq 4\big|G^\sigma\big|^{\frac{\dim(A)}{\dim(G)}}$. Since $\big|A^\sigma\big| \leq \Delta\big|(A^0)^\sigma\big|$ this implies

$$\Big|G^\sigma : A^\sigma\Big| > \frac{1}{4\Delta}\Big|G^\sigma\Big|^{1-\dim(A)/\dim(G)} .$$

Using $A^\sigma = A \cap G^\sigma$ and $\big|G^\sigma : \langle\alpha\rangle\big| \leq I$ we obtain the inequality in (a). In particular, if K (hence q_σ) is large enough then $\langle\alpha\rangle \cap A \neq \langle\alpha\rangle$.

Suppose now that A is not normal in G. By Fact 27 there is an upper bound $\Delta' = \Delta'(N, \Delta) \geq \deg\big(\mathcal{N}_G(A)\big)$. If K is large enough then we may apply (a) to the proper subgroup $\mathcal{N}_G(A) < G$. We obtain that $\langle\alpha\rangle \neq \langle\alpha\rangle \cap \mathcal{N}_G(A) = \mathcal{N}_{\langle\alpha\rangle}(A)$, i.e.,

α does not normalize A. Using $\big|\langle\alpha\rangle\big| \geq \frac{1}{I}\big|G^\sigma\big| \geq \frac{1}{2I}q_\sigma^{\dim(G)}$ we find that (a) implies the inequality in (b).

If (c) does not hold then let $g \in \mathcal{C}_G(\alpha)$ be such that $g \notin \mathcal{Z}(G)$. Clearly all elements of the $\langle\sigma\rangle$-orbit $g^{\langle\sigma\rangle}$ commute with the elements of α, hence $\langle\alpha\rangle \leq \mathcal{C}_G(g^{\langle\sigma\rangle})$. Since $\mathcal{C}_G(g^{\langle\sigma\rangle})$ is a proper σ-invariant closed subgroup of degree at most Δ, part (a) implies that $\langle\alpha\rangle \cap \mathcal{C}_G\big(g^{\langle\sigma\rangle}\big) \neq \langle\alpha\rangle$, a contradiction. Therefore ,$\mathcal{C}_G(\alpha) = \mathcal{Z}(G)$ as required. □

We now prove a general lemma concerning growth of subsets in finite linear groups. Theorem 2 is essentially a special case of this.

Lemma 67. *Let G be a connected linear algebraic group over $\overline{\mathbb{F}_p}$. Let $\sigma : G \to G$ be a Frobenius map and $1 \in \alpha \subseteq G^\sigma$ a finite symmetric subset. Suppose that $\mathcal{Z}(G)$ is finite, $\dim(G) \leq N$, $\deg(G) \leq \Delta$, $\mathrm{mult}(G) \leq \Delta$, $\mathrm{inv}(G) \leq \Delta$, and $\big|G^\sigma : \langle\alpha\rangle\big| \leq I$. There is a bound $K = K(N, \Delta, I)$ such that the following holds. If*

$$K \leq |\alpha| \leq q_\sigma^{\dim(G)-\frac{1}{4}}$$

then there is a σ-invariant connected closed normal subgroup $H \triangleleft G$ such that $\dim(H) > 0$,

$$|\alpha^M \cap H| \geq |\alpha|^{(1+\delta)\dim(H)/\dim(G)},$$

where $\delta = \frac{1}{1024N^4}$, the exponent M depends only on N, and $\deg(H)$ is less then $\tilde{\Delta} = \tilde{\Delta}(N, \Delta)$.

Proof. If K is large enough then Corollary 66.(c) yields $\mathcal{C}_G(\alpha) = \mathcal{Z}(G)$, which is finite. We totally order $\langle\alpha\rangle$, this turns $\alpha|G$ into an (N, Δ, K)-bounded spreading system.

The subgroup H we construct will be uniquely determined hence, as it is explained in Section 4 before Lemma 32, it will be σ-invariant. By Corollary 66.(b) the rest of the conclusion of the theorem can be rewritten as follows: H is normalized by α, $\deg(H) \leq \tilde{\Delta}$, $\dim(H) > 0$ and

$$\mu(\alpha^M, H) \geq (1+\delta)\mu(\alpha, G)\ ,$$

i.e., we need to prove that $\alpha|G$ is $(\delta, M, \tilde{\Delta})$-spreading.

If G were nilpotent then $\mathcal{Z}(G)$ would have positive dimension. By assumption $\mathcal{Z}(G)$ is finite, hence G is not nilpotent. We apply Theorem 52 with parameter $\varepsilon = \delta$ to $\alpha|G$. In case we obtain a subgroup of spreading, the theorem holds. Otherwise, we find a CCC-subgroup $A \leq G$ which is not normal in G and, for an appropriate integer M', satisfies

$$\mu\big(\alpha^{M'}, A\big) > (1 - \delta \cdot 17N)\,\mu(\alpha^{M'}, G) > \big(1 - \tfrac{1}{7N^2}\big)\,\mu(\alpha^{M'}, G)\ .$$

We know from Lemma 44 that $\deg(A) \leq \deg(G)$. By assumption

$$\mu(\alpha, G) \leq \log(q_\sigma)\big(1 - \tfrac{1}{4N}\big)\ .$$

If $\mu(\alpha^{M'}, G) \geq \log(q_\sigma)\big(1 - \frac{1}{8N}\big)$ then the lemma holds with $G = H$. Otherwise,

$$\mu(\alpha^{M'}, G) < \log(q_\sigma)\big(1 - \tfrac{1}{8N}\big) \leq \big(\log(q_\sigma) - \log(c)\big)\big(1 - \tfrac{1}{16N}\big)$$

if K (hence q_σ) is large enough, where c as in Corollary 66.(b). Therefore, taking logarithms in Corollary 66.(b), we obtain

$$\mu(\alpha^{M'}, G) \leq \Big(1 - \tfrac{1}{16N}\Big)\frac{\log\big|\langle\alpha\rangle:\langle\alpha\rangle\cap A\big|}{\dim(G) - \dim\big(\mathcal{N}_G(A)\big)} \leq \Big(1 - \delta \cdot 64N^3\Big)\frac{\log\big|\langle\alpha\rangle:\langle\alpha\rangle\cap A\big|}{\dim(G) - \dim\big(\mathcal{N}_G(A)\big)}$$

Applying Theorem 54 with $\varepsilon = \delta$ to $\alpha^{M'}|G$ we obtain a subgroup of spreading as required. □

We now prove our main result, Theorem 2.

Theorem 68. *Let L be a finite simple group of Lie type of Lie rank at most r and $\alpha \subset L$ a generating set. Then either $\alpha^3 = L$ or*

$$|\alpha^3| \geq |\alpha|^{1+\varepsilon}$$

where ε depends only on r.

Proof. There is a simple adjoint algebraic group G and a Frobenius map $\sigma : G \to G$ such that $L \leq G^\sigma$, and there are universal bounds $I(r)$, $N(r)$ and $\Delta(r)$ such that

$$\left|G^\sigma : L\right| \leq I(r)\,, \quad \dim(G) \leq N(r)\,,$$

$$\deg(G) \leq \Delta(r)\,, \quad \mathrm{mult}(G) \leq \Delta(r)\,, \quad \mathrm{inv}(G) \leq \Delta(r)\,.$$

By Proposition 56.(a) we may assume that $\alpha = \alpha^{-1}$ is symmetric with $1 \in \alpha$. We may also suppose that $q_\sigma \geq 20$. If $|\alpha| \geq q_\sigma^{\dim(G)-\frac{1}{4}}$ then $\alpha^3 = L$ by Proposition 64. Assume otherwise.

Since G is simple, Lemma 67 implies that

$$\left|\alpha^M \cap G\right| \geq |\alpha|^{1+\delta}$$

for some M and δ if $|\alpha| \geq K$ where M, δ, and K depend only on r. Hence, for $|\alpha| \geq K$ our statement follows using Proposition 56.(b).

Proposition 62 yields $\left|\alpha^3\right| \geq 2|\alpha|$, hence for $|\alpha| \leq K$ our statement holds with $\varepsilon = \frac{\log 2}{\log K}$. □

Remark 69. In the proof of Theorem 2 one can avoid using Proposition 65. We know explicitly the number of elements in all finite simple groups of Lie type and also in their maximal tori (see, e.g., [12]). When G is a connected adjoint simple algebraic group, one can show directly that $(G^\sigma)'$ does not normalize any proper connected closed subgroups of positive dimension and small degree. This also implies that $\mathcal{C}_G\big((G^\sigma)'\big)$ is finite which is all we need for the proofs of Theorem 4 and Theorem 2. See Proposition 91 in Appendix B for a more general result communicated to us by Martin Liebeck. This can be used to complete the above sketch.

11. The proof of Theorem 5

In this section we prove various results for p-generated subgroups of $SL(n, \mathbb{F}_p)$, i.e., subgroups generated by elements of order p. These finite groups can be obtained roughly as fixpoint groups of Frobenius maps of linear algebraic groups. For perfect p-generated groups we first prove a growth result (Lemma 73). The proof of this lemma relies on our algebraic group machinery via Lemma 67. Theorem 5 will follow quickly from Lemma 73 and Theorem 4.

We will use the following special case of a deep result of Nikolov and Segal ([46, Theorem 1.7]).

Proposition 70. *Let P be a finite perfect group generated by d elements. Then every element of G is the product of $g(d)$ commutators where $g(d) = 12d^3 + \mathcal{O}(d^2)$ depends only on d.*

Next, we will describe more precisely the Nori correspondence between p-generated subgroups of $SL(n,\mathbb{F}_p)$ and certain closed subgroups of $SL(n,\overline{\mathbb{F}_p})$ and some other useful facts about perfect p-generated subgroups. As usual, we denote by $Frob_p$ the automorphism $SL(n,\overline{\mathbb{F}_p}) \to SL(n,\overline{\mathbb{F}_p})$ which raises each matrix entry to p-th power.

Proposition 71. *Let $P \leq SL(n,\mathbb{F}_p)$ be a p-generated subgroup. Then there are bounds $I = I_{\exp}(n)$, $\Delta = \Delta_{\exp}(n)$ and $K = K_{\exp}(n)$ with the following properties.*

(a) There is a $Frob_p$-invariant connected closed subgroup $G \leq SL(n,\overline{\mathbb{F}_p})$ such that $\dim(G) \leq n^2$, $\deg(G) \leq \Delta$, $\mathrm{mult}(G) \leq \Delta$, $\mathrm{inv}(G) \leq \Delta$, and P is a subgroup of $G(\mathbb{F}_p)$ of index at most I.

(b) If P is perfect then the degree of any complex representation is at least $(p-1)/2$.

(c) If moreover $|P| \geq K$ and $\alpha \subseteq P$ is a subset of size $|\alpha| \geq p^{\dim(G)-\frac{1}{4}}$ then $\alpha^3 = P$.

Proof. We first prove (a). By a result of Nori [44] there is a constant $I = I_{\exp}(n)$ such that there is a $Frob_p$-invariant connected closed subgroup $G \leq SL(n,\overline{\mathbb{F}_p})$ with $P \leq G(\mathbb{F}_p)$ of index $\big|G(\mathbb{F}_p) : P\big| \leq I$. Clearly, $\dim(G) \leq n^2$. By [39, Proposition 3] there is an upper bound $\Delta_{\exp}(n) \geq \deg(G)$ (which can also be proved easily from [44] using the degree of the exponential map). By Proposition 26 we may assume that $\Delta_{\exp}(n)$ is also an upper bound for $\mathrm{mult}(G)$ and $\mathrm{inv}(G)$. Let $\sigma : G \to G$ denote the restriction to G of the automorphism $Frob_p$, then $G(\mathbb{F}_p) = G^\sigma$.

Assume now that P is perfect. Let $\phi : P \to GL(k,\mathbb{C})$ be a nontrivial complex representation. If $k < \frac{p-1}{2}$ then by well-known results of Brauer and Feit-Thompson (see, e.g., [35, Theorem 14.11] and the remark after its proof) $\phi(P)$ has a normal Sylow-p subgroup. This is impossible since $\phi(P)$ is also a perfect p-generated group. This proves (b).

If K is large enough then $p \geq K^{1/n^2}$ is large as well, hence by Proposition 65 we have $|P| \leq 2p^{\dim(G)}$ and $\alpha^3 = P$ by Proposition 63. □

We need the following more precise version of Proposition 60.

Proposition 72. *Let H be a closed subgroup of $SL(n,\overline{\mathbb{F}})$. For some $n' = n'\big(n, \deg(H)\big)$ there is a homomorphism $\mathcal{N}_{SL(n,\overline{\mathbb{F}})}(H) \to SL(n',\overline{\mathbb{F}})$ of degree bounded in terms of n and $\deg(H)$ whose kernel is H. Moreover, if $\overline{\mathbb{F}}$ has characteristic p and H is $Frob_p$-invariant for some p-power q then the homomorphism we construct is $Frob_p$-equivariant.*

Proof. See Proposition 90 in Appendix A. □

The next lemma follows by an induction argument based on Lemma 67.

Lemma 73. *Let $P \leq SL(n,\mathbb{F}_p)$ be a perfect p-generated subgroup. Let $1 \in \alpha \subseteq P$ be a symmetric generating set which projects onto each simple quotient of P. Then:*

(a) either $\alpha^3 = P$ or $|\alpha^3| \geq |\alpha|^{1+\varepsilon}$ where ε depends on n, or

(b) the diameter of the Cayley graph of P with respect to α is at most $d(n)$ where $d(n)$ depends on n.

Proof. Let l be the smallest integer such that $|P| \leq p^{l/2}$, note that $l \leq 2n^2$. We prove (a) by induction on l. For $l = 0$ it is clear. We assume that $l > 0$ and the

statement holds for all groups of order at most $p^{(l-1)/2}$ and for all matrix sizes n with an ε-value $0 < \varepsilon'(n,l)$.

Our argument will yield a positive integer $K = K(n)$ such that the induction step goes through if $|\alpha| \geq K$. If $|\alpha| \leq K$ and $\alpha^3 \neq P$ then $|\alpha^3| \geq 2|\alpha|$ by Proposition 62 and (a) holds in this case with any $\varepsilon \geq \log(2)/\log(K)$. If $|\alpha| > p^{\dim(G)-1/4}$ then $\alpha^3 = P$ by Proposition 71.(c). So we assume

$$K < |\alpha| \leq p^{\dim(G)-\frac{1}{4}} .$$

We apply Proposition 71 to P and obtain the $Frob_p$-invariant connected closed subgroup $G \leq SL(n, \overline{\mathbb{F}_p})$ for which $\deg(G)$, $\mathrm{mult}(G)$ and $\mathrm{inv}(G)$ are at most $\Delta_{\exp}(n)$, $\dim(G) \leq n^2$, and $\big|G(\mathbb{F}_p) : P\big| \leq I_{\exp}(n)$.

During the induction step we will consider a $Frob_p$-invariant connected closed proper normal subgroup H of G such that $\deg(H) \leq \Delta^*$ for some positive integer $\Delta^* = \Delta^*(n)$ to be defined later. (H will be given by an application of Lemma 67 or it will be $\mathcal{Z}(G)^0$.)

Let H be such a normal subgroup. Then by Corollary 66.(a), for sufficiently large K, $\alpha \not\subseteq H$. By Proposition 72 there is a $Frob_p$-equivariant homomorphism $G \to SL(n', \overline{\mathbb{F}_p})$ for some common $n' = n'\big(\dim(G), \Delta^*\big)$ whose kernel is H. The elements of α are fixpoints of $Frob_p$, so by the equivariance their images are also fixpoints of $Frob_p$, i.e., the image set α_H of α generates a subgroup of $SL(n', \mathbb{F}_p)$ isomorphic to $P/(H \cap P)$. This subgroup is again perfect, p-generated and α_H projects onto each of its simple quotients. In particular $\big|\alpha_H\big| \geq p \geq |\alpha|^{1/n^2}$. We know from Proposition 65 that if K is large enough then $|H \cap P| \geq \big|H(\mathbb{F}_p)\big|/I_{\exp}(n) > \sqrt{p}$ so $\big|P/(H \cap P)\big| < |P|/\sqrt{p} \leq p^{(l-1)/2}$ and the induction hypothesis holds for α_H and $P/(H \cap P)$ with the ε-value $\varepsilon' = \varepsilon'\big(n', l\big)$.

Suppose that we find such an H with $\big|\alpha_H^3\big| \geq \big|\alpha_H\big|^{1+\varepsilon'}$. Then

$$\big|\alpha^5\big| \geq \big|\alpha_H^3\big| \cdot \big|\alpha^2 \cap H\big| \geq \big|\alpha_H\big|^{1+\varepsilon'} \cdot \big|\alpha^2 \cap H\big| \geq \big|\alpha\big| \cdot \big|\alpha_H\big|^{\varepsilon'} \geq \big|\alpha\big|^{1+\varepsilon'/n^2}$$

and by Proposition 56.(b) the induction step is complete. So we may assume that for all such H we have $\alpha_H^3 = P/(H \cap P)$.

Suppose next that $\mathcal{Z}(G)$ is finite. We apply Lemma 67 with parameters $N = \dim(G)$, $\Delta = \Delta_{\exp}(n)$ and $I = I_{\exp}(n)$ to the subset $\alpha \subset G^{Frob_p}$. We obtain a $Frob_p$-invariant connected closed normal subgroup $H \lhd G$ of degree bounded by $\tilde{\Delta} = \tilde{\Delta}(n)$ such that $\dim(H) > 0$ and

$$\big|\alpha^M \cap H\big| \geq \big|\alpha\big|^{(1+\delta)\dim(H)/\dim(G)}$$

where M and δ depend only on n. We set $\Delta^* = \max\big(\deg(G), \tilde{\Delta}\big)$.

If $H = G$ then $\big|\alpha^M\big| \geq \big|\alpha\big|^{1+\delta}$.

Otherwise, H is a proper normal subgroup, and by the above argument we have $\alpha_H^3 = P/(H \cap P)$. It follows from Corollary 66.(a) that if K is sufficiently large then we have, say,

$$\big|\alpha_H^3\big| = \big|P/(H \cap P)\big| \geq \big|P\big|^{1-\dim(H)/\dim(G)-\delta/(2n^2)} \geq \big|\alpha\big|^{1-\dim(H)/\dim(G)-\delta/(2n^2)} .$$

Therefore,

$$\big|\alpha^{3+M}\big| \geq \big|\alpha_H^3\big| \cdot \big|\alpha^M \cap H\big| \geq \big|\alpha\big|^{1-\frac{\dim(H)}{\dim(G)}-\frac{\delta}{2n^2}} \cdot \big|\alpha\big|^{(1+\delta)\frac{\dim(H)}{\dim(G)}} \geq \big|\alpha\big|^{1+\frac{\delta}{2n^2}} .$$

By Proposition 56.(b) the induction step is complete in this case.

Finally, if $\mathcal{Z}(G)$ is infinite then we consider the normal subgroup $H = \mathcal{Z}(G)^0$, which has degree at most $\deg(G) \leq \Delta^*$. By assumption $\alpha_H^3 = P/(H \cap P)$ hence α^3 intersects every $(H \cap P)$-coset in P. Hence every commutator element of P is in fact the commutator of two elements in α^3. It is well-known that P is generated by at most n^2 elements (see [51]) hence by Proposition 70 each element of P is the product of Cn^6 commutators for some constant C. By assumption $|\alpha| \leq p^{\dim(G)-1/4}$. If K is large enough then $|P| \geq p^{\dim(G)-1/8}$ by Proposition 65. Therefore,

$$\left|\alpha^{3\cdot 4\cdot Cn^6}\right| = |P| > |\alpha|^{1+1/8\dim(G)}$$

and by Proposition 56.(b) the induction step is complete in this case too. This proves (a).

Let us apply (a) successively to $\alpha, \alpha^3, \alpha^9, \ldots$. We obtain by induction that either $\alpha^{3^i} = P$ or $\left|\alpha^{3^i}\right| \geq |\alpha|^{(1+\varepsilon)^i}$ for all i. Since by assumption $|\alpha| \geq p$ and $|P| < p^{n^2}$, part (b) follows. □

Now we prove Theorem 5.

Theorem 74. *Let $P \leq SL(n, \mathbb{F}_p)$ be a perfect p-generated subgroup. Then the diameter of the Cayley graph of P with respect to any symmetric generating set is at most $\left(\log|P|\right)^{M(n)}$ where $M(n)$ depends only on n.*

Proof. The Lie rank of any simple quotient L of P is at most n (see [19] and [37, Proposition 5.2.12]). By Theorem 4 the subset α^m projects onto each such quotient L for some $m \leq \left(\log|P|\right)^{c(n)}$. Applying Lemma 73 to α^m our statement follows. □

Example 75. Let G be the commutator subgroup of the permutational wreath product $W = C_{q-1} \operatorname{wr} A_5$, where q is a power of 2. The structure of such wreath products W is described in [17, Chapter A, 18.4 (c) and (d)]. G is perfect since it is generated by its A_5 subgroups. Moreover, G has an abelian normal subgroup of index 60 and order $(q-1)^4$. By a result of Annexstein and Baumslag [1, Theorem 5], if a group H has an abelian subgroup of index r then a connected Cayley graph of degree k has diameter at least $\left(|H|/r\right)^{1/2kr}$. We see that G has connected Cayley graphs of diameter at least $|G|^c$ for some absolute constant $c > 0$. Clearly, G is a 2-generated subgroup of $SL(5, \mathbb{F}_q)$. This example shows that Theorem 5 does not hold for subgroups of $SL(n, \mathbb{F}_q)$, q a prime power.

Remark 76. It is likely that the following holds: If P is a p-generated subgroup of $SL(n, \mathbb{F}_q)$, q a power of p, such that the minimal degree of a complex representation is large enough compared to n, then Cayley graphs of P have diameter at most $\left(\log|P|\right)^{c(n)}$.
This would imply Theorem 4.

12. Dependence of the growth on rank: an example

In this section we give some examples which show that the constant $\varepsilon(r)$ for which Theorem 68 holds must be less than $\frac{C}{r}$.

Example 77. Consider the group $SL(n, q)$ where $n \geq 3$ (which has Lie rank $r = n-1$). Let H be the subgroup of all diagonal matrices, this has order $(q-1)^{n-1}$.

If N denotes the subgroup of all monomial matrices then $N/H \simeq S_n$ Choose an element s of N projecting onto an n-cycle of N/H. If $e_1, \dots, e_n$ is the standard basis of $(\mathbb{F}_q)^n$, consider the subgroup $L_{1,2} \simeq SL(2,q)$ which fixes $e_3, \dots, e_n$. In [2, Theorem 3.1] a 3-element generating set $\{a, b, c\}$ of $L_{1,2}$ is chosen. As shown in [2] s, a, b and c generate $SL(n,q)$. Now s normalizes the diagonal subgroup H and it is clear that a, b and c normalize a subgroup H_0 of index $(q-1)^2$ in H (the group of diagonal matrices fixing e_1 and e_2). The set $A = H \cup \{a, b, c, s\}$ generates $SL(n,q)$.

We claim that $\left|A^3\right| \le |H|\big(3(q-1)^2 + 58\big) + 64$.

It is easy to see that $\left|A^3\right| \le \left|H\{a,b,c,s\}H\right| + 57|H| + 64$. Since s normalizes H we have $\left|HsH\right| = |H|$. Since a (resp. b and c) normalizes H_0 we have $\left|HaH\right| \le |H|(q-1)^2$ (and analogous inequalities hold for b and c) which implies the claim.

Setting $q = 3$ we obtain the generating set with $\left|A^3\right| \le 100|A|$ mentioned in the introduction.

Clearly, there are many ways in which the above construction can be extended. For example the full diagonal subgroup H can be replaced by its characteristic subgroups isomorphic to C_t^{n-1} where t divides $q-1$. This way, e.g., we can construct large families of generating sets of constant growth whenever q is odd.

It would be most interesting to find some essentially different families of examples of large generating sets of $SL(n,q)$ with constant growth.

Appendix A

Basic degree estimates

Lemma 78 (= First part of Fact 16.(g))**.** *Let $X \subseteq \overline{\mathbb{F}}^m$ be the common zero locus of degree d polynomials. Then it is the common zero locus of at most $(d+1)^m$ of them, and $\deg(X) \le d^m$.*

Proof. Let $\mathcal{Y}$ denote the collection of the zero sets of the given polynomials. We construct by induction a finite sequence of closed subsets $X_0 \supset X_1 \supset X_2 \supset \cdots \supset X_I = X$. We start with $X_0 = \mathbb{F}^m$. If X_i is already constructed then we look for a member $Y_i \in \mathcal{Y}$ which does not contain X_i. If we find one then we set $X_{i+1} = X_i \cap Y_i$, otherwise $X_i = \bigcap \mathcal{Y} = X$, so we set $I = i$ and stop the induction.

In order to bound $\deg(X_i)$ and I we need two invariants. For closed subsets $Z \subseteq \mathbb{F}^m$ with irreducible decomposition $Z = \bigcup_j Z_j$ we define

$$\delta(Z) = \sum\nolimits_j \deg(Z_j) d^{\dim(Z_j)}\,, \quad \delta'(Z) = \sum\nolimits_j \deg(Z_j)(d+1)^{\dim(Z_j)}\,.$$

By Fact 16.(d) we have $\delta(Z \cap Y) \le \delta(Z)$ and $\delta'(Z \cap Y) < \delta'(Z)$ for all $Y \in \mathcal{Y}$. Therefore $\deg(X) \le \delta(X) \le \delta(X_0) = d^m$. Moreover, $\delta'(X_i)$ is strictly decreasing and positive, hence $I \le \delta'(X_0) = (d+1)^m$. □

Lemma 79 (= Fact 17.(a))**.** *Let $X \subseteq \overline{\mathbb{F}}^m$ be a closed subset and let $f : X \to \overline{\mathbb{F}}^m$ be a morphism. We define the function $\Phi(d) = (d+2)^{(d+1)^{\dim(X)+\deg(f)}2^d}$ and set $D = \Phi\big(\Phi\big(\dots\Phi\big(\deg(f)\big)\big)\dots\big)^{\dim(X)+\deg(f)}$ where the function Φ is iterated $\dim(X)+\deg(f)-1$ times. Then there is a partition of $\overline{f(X)}$ into at most D locally closed subsets Y_i of degree at most D such that the closure of each Y_i is the union of partition classes and either $f^{-1}(Y_i) = \emptyset$ or $\dim\big(f^{-1}(y)\big) = \dim(X) - \dim(Y_i)$ for all $y \in Y_i$.*

Sketch of the proof. Let $\Gamma_f \subseteq \overline{\mathbb{F}}^m \times \overline{\mathbb{F}}^n$ be the graph of f, and $\pi : \overline{\mathbb{F}}^m \times \overline{\mathbb{F}}^n \to \overline{\mathbb{F}}^n$ the linear projection to the second factor. Then Γ_f is isomorphic to X, hence it is enough to find an analogous partition of $\overline{\pi(\Gamma_f)} = \overline{f(X)}$ with respect to π and Γ_f (with the same bound D defined in terms of $\deg(f)$ and $\dim(X)$).

Let L denote the linear span of Γ_f and set $\tilde{\pi} = \pi\big|_L$. Using [26, Ex. I.7.7] one can easily show that $\dim(L) \leq \dim(\Gamma_f) + \deg(\Gamma_f) - 1 = \dim(X) + \deg(f) - 1$. We need to find a partition of $\overline{\tilde{\pi}(\Gamma_f)} = \overline{f(X)}$ as in the statement lemma with respect to $\tilde{\pi}$ and Γ_f (with the same bound D). We factor $\tilde{\pi}$ into $\dim(L) - \dim\big(\tilde{\pi}(L)\big) \leq \dim(X) + \deg(f) - 1$ consecutive linear projections $\tilde{\pi}_j$, each with one-dimensional fibers. Our strategy is the following. First we partition $\overline{\tilde{\pi}_1(\Gamma_f)}$ via the next Claim 80. Then for each partition class $C \subseteq \overline{\tilde{\pi}_1(\Gamma_f)}$ we apply again Claim 80, and partition the closed image $\tilde{\pi}_2(\overline{C})$ We obtain various partitions on partially overlapping subsets of $\tilde{\pi}_2\big(\tilde{\pi}_1(\Gamma_f)\big)$. Let us consider the common refinement of them, it is a partition of $\tilde{\pi}_2\big(\tilde{\pi}_1(\Gamma_f)\big)$ into locally closed subsets. We iterate this procedure, and obtain partitions of $\tilde{\pi}_j \circ \cdots \circ \tilde{\pi}_1(\Gamma_f)$ for each j. (Note that k in these applications of Claim 80 is always at most $\dim(X) + \deg(f) - 2$.) In the last step we obtain a partition of $\overline{\tilde{\pi}(\Gamma_f)} = \overline{f(X)}$ as required. □

Claim 80. *Let $Z \subseteq \overline{\mathbb{F}}^k$ be a locally closed subset and Γ be the common zero locus inside $\overline{\mathbb{F}} \times Z$ of some polynomials of degree at most d.*

(a) Then Z has a partition into at most $(d+2)^{(d+1)^{k+2}-1}$ locally closed subsets Z_i and there are corresponding $(k+1)$-variate polynomials P_i of degree at most $d^{(d+1)^{k+1}2^d}$ such that

$$\Gamma \cap \big(\overline{\mathbb{F}} \times Z_i\big) = \Big\{(t, \underline{z}) \in \overline{\mathbb{F}} \times Z_i \;\Big|\; P_i(t, \underline{z}) = 0\Big\}$$

for all i, and the closures $\overline{Z_i}$ are defined via equations of degree at most $d^{(d+1)^{k+1}2^d}$ plus the equations of $\overline{Z}$.

(b) The three loci of those points $\underline{z} \in Z_i$ for which the set $\Gamma \cap \big(\overline{\mathbb{F}} \times \{\underline{z}\}\big)$ is empty, finite, or one dimensional are locally closed subsets defined inside Z via equations of degree at most $d^{(d+1)^{k+1}2^d}$, and the total number of these subsets is at most $(d+2)^{(d+1)^{k+2}}$.

(c) Moreover, one may require both partitions to have the following additional property: the closure in Z of each partition class is the union of partition classes.

Sketch of proof. The statement follows from standard elimination theory, here we explain how to keep track of the degrees. It will turn out that the polynomials P_i in (a) will have t-degree at most d. So it is natural to consider $\mathcal{X}_d$, the collection of all locally closed subsets of the form

$$X_{V,Q} = \Big\{(t, \underline{z}) \in \overline{\mathbb{F}} \times V \;\Big|\; Q(t, \underline{z}) = 0\Big\} \subseteq \overline{\mathbb{F}} \times Z$$

where $V \subseteq Z$ is a locally closed subset and $Q(t, \underline{z})$ is a polynomial of the variables $t \in \overline{\mathbb{F}}$ and $\underline{z} \in \overline{\mathbb{F}}^k$ whose t-degree is at most d. The intersection of two such sets can be written as the disjoint union of a number of other members of $\mathcal{X}_d$. To see this, we use the Euclidean algorithm in the t-variable for the defining polynomials (treating $\underline{z}$ as a fixed parameter), and partition the set of possible $\underline{z}$-values according to how the algorithm runs (i.e., how many steps we need to conclude and what are the

degrees of the divisors). Part (a) follows since Γ is the intersection of a bounded number of members from $\mathcal{X}_d$.

Next, we give a more detailed sketch of the proof. The upper bounds and part (c) follow immediately from our construction, we leave them to the reader. Γ can be defined as the common zero locus inside $\overline{\mathbb{F}} \times Z$ of at most $(d+1)^{k+1}$ polynomials of degree at most d (see Fact 16.(g)). We prove (a) via induction on the number of defining polynomials. If $\Gamma = \overline{\mathbb{F}} \times Z$ then there is nothing to prove. Otherwise, let g be one of the nonzero defining polynomials of Γ and $\Gamma' \subseteq \overline{\mathbb{F}} \times Z$ the common zero locus of the other defining polynomials. Applying the induction hypothesis to Γ' gives us a partition $\bigcup_j Z'_j = Z$ and corresponding polynomials P'_j. Our goal is to refine this partition, i.e., find partitions $Z'_j = \bigcup_i Z'_{ji}$ and find appropriate polynomials P'_{ji}. We will find the Z'_{ji} one by one with the following algorithm.

The portion of Γ that lies inside $\overline{\mathbb{F}} \times Z'_j$ is defined by the equations $P'_j(t, \underline{z}) = g(t, \underline{z}) = 0$ (besides the equations and inequalities defining Z'_j). We consider g and P'_j as polynomials in the variable t whose coefficients are polynomial functions of the parameter $\underline{z}$. Note that g and P'_j as well as all the polynomials P'_{ji} we construct below have t-degrees at most d. Our plan is to find the gcd of g and P'_j with respect to the variable t for all values of $\underline{z}$ simultaneously. In order to do so we try to run Euclid's algorithm simultaneously for all $\underline{z}$. There are two obstacles we have to overcome. First, for different values of $\underline{z}$ the algorithm needs a different number of steps to complete. Second, to do a polynomial division uniformly for several values of $\underline{z}$ we have to make sure that the degree of the divisor do not vary with $\underline{z}$ (i.e., we can talk about the leading coefficient). So before each polynomial division we construct also a partition of Z'_j, always refining the partition obtained in the previous step, so that the upcoming division can be done uniformly for values $\underline{z}$ lying in the same partition class.

To begin with, let Z'_{j0} and Z'_{j1} denote the loci of those $\underline{z} \in Z'_j$ where all coefficients of g or P'_j respectively vanish. We set $P'_{j0} = P'_j$ and $P'_{j1} = g$. Similarly, for each pair of integers $0 \leq a, b \leq d$ we consider the locus of those $\underline{z} \in Z'_j$ where the t-degrees of g and P'_j are just a and b. This is a partition of Z'_j into locally closed subsets, each defined via the vanishing or non-vanishing of a number of coefficients. For parameter values $\underline{z}$ lying in Z'_{j0} or Z'_{j1} the algorithm stops right away with gcd equal to P'_{j0} or P'_{j1}. On the other hand, for any other partition class $\tilde{Z} \subseteq Z'_j$ we can do the first polynomial division uniformly for all $\underline{z} \in \tilde{Z}$.

During the algorithm we do similar subdivisions again and again. Suppose that we completed a number of polynomial divisions and constructed the partition corresponding to the last completed division. Let $\tilde{Z}$ be a class of that partition and suppose that the algorithm is still running for $\underline{z} \in \tilde{Z}$ and $\tilde{g}$ and $\tilde{r}$ are the divisor and the remainder of the last completed polynomial division for all values $\underline{z} \in \tilde{Z}$. We consider the locus of those $\underline{z} \in \tilde{Z}$ where all coefficients of $\tilde{r}$ vanish (here $\tilde{g}$ does not vanishes). This will be our next Z'_{ji} (whatever i follows now). For $\underline{z} \in Z'_{ji}$ Euclid's algorithm stops at this stage, and we set $P'_{ji} = \tilde{g}$, the gcd we obtain. As before, we partition $\tilde{Z} \setminus Z'_{ji}$ according to the t-degree of $\tilde{r}$ (here the t-degree of $\tilde{g}$ is unimportant). Then we can do the polynomial division $\tilde{g} : \tilde{r}$ uniformly for values $\underline{z}$ lying in the same partition class. This way we obtain our new remainders (one for each partition class), and Euclid's algorithm continues.

It is clear that for each $\underline{z} \in Z'_j$ the gcd is found in at most $\deg(g)+1 \le d+1$ steps, hence we obtain the promised partition $Z'_j = \cup_i Z'_{ji}$. The induction step is complete.

Part (b) follows from part (a). Indeed, the portion of Γ that lies inside $\overline{\mathbb{F}} \times Z_i$ is defined by the equation $P_i(t,\underline{z}) = 0$ (besides the equations of Z_i). For each $\underline{z} \in Z_i$ the set $\Gamma \cap \left(\overline{\mathbb{F}} \times \{\underline{z}\}\right)$ is empty, finite, or one-dimensional precisely if $P_i(t,\underline{z})$ is nonzero constant, non-constant, or zero, respectively. Hence, the three loci in (b) can be defined via the vanishing or non-vanishing of a number of t-coefficients of $P_i(t,\underline{z})$ (which are themselves polynomials of $\underline{z}$). □

Closed subsets and closed subgroups in algebraic groups

Here we will give the proofs of two results from Section 4, and an auxiliary result, Lemma 82, needed for the proof of Lemma 83.

Lemma 81 (= Lemma 32)**.** *Let $Y \subseteq SL(n,\overline{\mathbb{F}})$ be an irreducible closed subset of positive dimension and $1 \in \alpha \subset SL(n,\overline{\mathbb{F}})$ a finite subset with a total ordering on $\langle\alpha\rangle$. Let $H \le SL(n,\overline{\mathbb{F}})$ denote the smallest closed subgroup which is normalized by α and contains $Y^{-1}Y$. Suppose that $\dim(H) \le m$. Then there is a sequence $\underline{g} = (g_1, g_2, \dots, g_{2m})$ of elements $g_i \in \alpha^{m-1}$ such that*

$$H = \tau_{\underline{g}}\left(\prod^{2m}(Y^{-1}Y)\right) = (g_1^{-1}Y^{-1}Yg_1)(g_2^{-1}Y^{-1}Yg_2)\dots(g_{2m}^{-1}Y^{-1}Yg_{2m})\,.$$

The subgroup H is connected and there is a universal bound $\deg(H) \le \delta\big(m, \deg(\overline{Y^{-1}Y})\big)$. Moreover, H and the sequence $\underline{g}$ we construct are uniquely determined.

Proof. We set $g_1 = 1$. We will define $g_i \in \alpha^{i-1}$ by induction and consider the product sets

$$Z_i = (g_1^{-1}Y^{-1}Yg_1)(g_2^{-1}Y^{-1}Yg_2)\dots(g_i^{-1}Y^{-1}Yg_i) \subseteq H\,.$$

Suppose that $g_1, g_2, \dots, g_i$ are already defined. We set $g_{i+1} \in \alpha^i$ to be the first element such that $\dim\left(\overline{Z_i}\right) < \dim\left(\overline{Z_i \cdot (g_{i+1}^{-1}Y^{-1}Yg_{i+1})}\right)$, if there is any. Since the dimension of $\overline{Z_i}$ is strictly increasing, eventually we must arrive to an index $i \le m$ so that g_{i+1} does not exist. But then for all $g \in \alpha^i$ the closed subsets $\overline{Z_i} \subseteq \overline{Z_i \cdot (g^{-1}Y^{-1}Yg)}$ are irreducible (see Fact 17.(b)) of the same dimension, hence they are equal. This implies that $\overline{Z_i}^2 \subseteq \overline{Z_i}$ and $g^{-1}\overline{Z_i}g \subseteq \overline{Z_i}$ for all $g \in \alpha$, hence $\overline{Z_i}$ is a closed connected subgroup normalized by α, i.e., $\overline{Z_i} = H$. By Fact 17.(b) the product Z_i contains a dense open subset of H, hence $H = Z_i^2$ by [33, Lemma on page 54]. Setting $g_{i+j} = g_j$ for $1 \le j \le i$ and $g_{2i+1} = \dots g_{2m} = 1$ we obtain our statement. □

Lemma 82. *Let $G \le SL(n,\overline{\mathbb{F}})$ be a closed subgroup, $Z \subseteq G \times G$ an irreducible closed subset and $(a,b) \in Z$. Suppose that $\overline{\tau_{(1,1)}(Z)}$ has dimension 0, i.e., it is a finite set. Then there is an irreducible closed subset $A \subseteq G$ such that*

$$Z = \left\{(ah, h^{-1}b) \;\middle|\; h \in A\right\} \tag{25}$$

and

$$\left\{c \in SL(n,\overline{\mathbb{F}}) \;\middle|\; \dim\left(\overline{\tau_{(c,1)}(Z)}\right) = 0\right\} = \mathcal{C}_{SL(n,\overline{\mathbb{F}})}(A)\,.$$

Proof. By assumption $\tau_{(1,1)}(Z)$ is finite and its closure is irreducible (see Fact 17.(b)), hence it is the single point $ab \in G$. Let $\mathrm{pr}_1 : G \times G \to G$ denote the projection on the first factor. We set $A = a^{-1}\,\mathrm{pr}_1(Z)$.

We will prove later, that it is in fact closed. Anyway, $\overline{A}$ is irreducible (see Fact 17.(b)) and by definition $1 = a^{-1}a \in A$. Then each point of Z has the form (ah, β) with some $h \in A$ and $\beta \in G$, and for all $h \in A$ there must exist at least one such point. But then $ab = \tau_{(1,1)}(ah, \beta) = ah\beta$ hence $\beta = h^{-1}b$. This proves equation (25). The subset Z is closed, hence A is closed by equation (25). Now

$$\tau_{(c,1)}(Z) = \Big\{c^{-1}(ah)c(h^{-1}b) \;\Big|\; h \in A\Big\} = c^{-1}a\Big\{hch^{-1} \;\Big|\; h \in A\Big\}b$$

for all $c \in SL(n, \overline{\mathbb{F}})$. This has dimension 0 iff the set $\big\{hch^{-1}\big|h \in A\big\}$ is finite. But A is irreducible, hence its closed image $\overline{\big\{hch^{-1}\big|h \in A\big\}}$ is also irreducible (see Fact 17.(b)), so it is finite iff it is a single point (see Remark 14), i.e., iff hch^{-1} is independent of $h \in A$. But $1 \in A$, hence this last condition is equivalent to $hch^{-1} = c$ for all $h \in A$, which simply means that c commutes with all $h \in A$. □

Lemma 83 (= Lemma 34)**.** *Let $G \leq SL(n, \overline{\mathbb{F}})$ be a linear algebraic group and let $1 \in \alpha \subset G$ be a finite subset with a total ordering on $\langle\alpha\rangle$. Suppose that the centralizer $\mathcal{C}_G(\alpha)$ is finite. Then for each integer $m \geq 0$ and each irreducible closed subset $Z \subset \prod^m G$ of dimension $\dim(Z) > 0$ there is a sequence $\underline{g} = (g_1, g_2, \ldots, g_m) \in \prod^m \alpha$ such that $\overline{\tau_{\underline{g}}(Z)}$ has positive dimension. Moreover, the sequence $\underline{g}$ we construct is uniquely determined.*

Proof. We will prove the theorem by induction on m. For $m = 1$ the statement is obvious. So let $m \geq 2$ and we assume that the corollary holds whenever the number of factors is smaller than m. We define several morphisms. For all $g \in G$ let

$$\sigma_g : \textstyle\prod^m G \to \prod^{m-1} G\,, \qquad \sigma_g(a_1, \ldots, a_m) = \big(g^{-1}a_1 g a_2, a_3, \ldots, a_m\big)$$

and let

$$\pi : \textstyle\prod^m G \to \prod^{m-2} G\,, \qquad \pi(a_1, \ldots, a_m) = (a_3, a_4, \ldots, a_m)\,,$$
$$\rho : \textstyle\prod^{m-1} G \to \prod^{m-2} G\,, \qquad \rho(a_2, \ldots, a_m) = (a_3, a_4, \ldots, a_m)\,.$$

For $m = 2$ we use the convention that $\prod^0 G$ is a single point. Note, that these morphisms manipulate only the first two coordinates. In particular $\rho\big(\sigma_g(x)\big) = \pi(x)$ for all $x \in \prod^m G$.

Our goal is to find an element $g \in \alpha$ such that

$$\dim\big(\overline{\sigma_g(Z)}\big) > 0\,. \tag{26}$$

Then we choose the smallest such g (in the total order of $\langle\alpha\rangle$) and use the induction hypotheses for $\overline{\sigma_g(Z)} \subseteq \prod^{m-1} G$. This proves the lemma for Z as well.

We distinguish two cases. Suppose first that for all $z \in \prod^{m-2} G$ the subset $Z \cap \pi^{-1}(z)$ is finite (i.e., 0 dimensional). Then $\dim(Z) = \dim\big(\overline{\pi(Z)}\big)$ is positive (see Fact 17.(e)). But for arbitrary g we have

$$\dim(Z) \geq \dim\big(\overline{\sigma_g(Z)}\big) \geq \dim\Big(\overline{\rho\big(\sigma_g(Z)\big)}\Big) = \dim\big(\overline{\pi(Z)}\big)$$

hence all these dimensions are equal. Hence (26) is achieved.

Suppose next that there is a point $z \in \prod^{m-2} G$ such that $Z \cap \pi^{-1}(z)$ has an irreducible component Z' with positive dimension. For simplicity we will identify

the subset $\pi^{-1}(z) = \prod^2 G \times \{z\} \subset \prod^m G$ with $\prod^2 G$ and also $\rho^{-1}(z) = G \times \{z\} \subset \prod^{m-1} G$ with G. With these identifications we have

$$\sigma_g(x) = \tau_{(g,1)}(x) \qquad \text{for all } x \in \prod^2 G \text{ and all } g \in \alpha\ .$$

If $\overline{\sigma_1(Z')} = \overline{\tau_{(1,1)}(Z')}$ has positive dimension then (26) holds with $g = 1$ since $\dim\left(\overline{\sigma_1(Z)}\right) \geq \dim\left(\overline{\sigma_1(Z')}\right)$. Otherwise we apply Lemma 82 to our Z' and get an infinite subset $A \leq G$. By assumption α does not centralize A, hence there is an element $g \in \alpha$ which does not commute with A, i.e., $g \notin \mathcal{C}_G(A) \cdot 1$. Now $\overline{\tau_{(g,1)}(Z')} = \overline{\sigma_g(Z')}$ has positive dimension. But then the potentially larger set $\overline{\sigma_g(Z)} \supseteq \overline{\sigma_g(Z')}$ has positive dimension as well. In all cases we proved (26), hence the lemma holds. □

CCC-subgroups

Here we prove two results from Section 6 and some auxiliary results.

Lemma 84. *Let G be an algebraic group and $X \subseteq G$ an irreducible closed subset. Then X has a CC-generator, i.e., $X^{\text{gen}} \neq \emptyset$.*

Proof. We consider sequences $\underline{a} = a_1, a_2, \ldots, a_m$, $a_i \in X$ such that

$$G > \mathcal{C}_G(a_1)^0 > \mathcal{C}_G(a_1, a_2)^0 > \mathcal{C}_G(a_1, a_2, a_3)^0 > \ldots$$

is a strictly decreasing chain of subgroups. The dimension is strictly decreasing in such a chain, hence the length of $\underline{a}$ is $m \leq \dim(G)$. Therefore, one of them, say $\underline{a}_{\max}$, is maximal, i.e., it cannot be extended. But then $\mathcal{C}_G(X)^0 = \mathcal{C}_G(\underline{a}_{\max})^0$ and we can build a CC-generator from $\underline{a}_{\max}$ by adding to it $\dim(G) - m$ arbitrary elements of X. □

Proposition 85. *Let G be a connected linear algebraic group, X an irreducible closed subset and $G \times X \to X$ a morphism which is a group action. For points $x \in X$ let G_x denote the stabiliser subgroup of x. These are closed subgroups and for each integer d the subset $\{x \in X \mid \dim(G_x) > d\}$ is closed in X. In particular, for each d the points $\underline{g} \in \prod^{\dim(G)} G$ with $\dim\left(\mathcal{C}_G(\underline{g})\right) > d$ form a closed subset in $\prod^{\dim(G)} G$.*

Proof. For the first half of the proposition (about stabilizer subgroups) we refer to [34, Proposition in 1.4]. If we apply this to the conjugation map $G \times \prod^{\dim(G)} G \to \prod^{\dim(G)} G\ ,\quad (h, \underline{g}) \to h^{-1}\underline{g}h$, then we obtain the second half (about centralizer subgroups). □

Lemma 86 (= Lemma 42)**.** *Let G be a connected linear algebraic group and $\emptyset \neq X \subseteq G$ an irreducible closed subset. Then X^{nongen} is a proper closed subset of $\prod^{\dim(G)} X$ whose degree is bounded in terms of* $\dim(G)$, $\deg(G)$, $\text{mult}(G)$, $\text{inv}(G)$, *and* $\deg(X)$.

Proof. First of all, $X^{\text{nongen}} = \left\{\underline{g} \,\middle|\, \dim(\mathcal{C}_G(\underline{g})) > \dim(A)\right\}$ is closed by Proposition 85. Let us consider the conjugation map

$$f : G \times \prod^{\dim(G)} X \to \prod^{\dim(G)} G \times \prod^{\dim(G)} X\ ,\quad f(h, \underline{g}) = \left(h^{-1}\underline{g}h, \underline{g}\right)\ .$$

Let Y denote the diagonal subset

$$Y = \left\{(\underline{g}, \underline{g}) \,\middle|\, \underline{g} \in \prod^{\dim(G)} X\right\} \subset \prod^{\dim(G)} G \times \prod^{\dim(G)} X$$

and let $\tilde{f}$ denote the restriction of f to $f^{-1}(Y)$ composed with the second projection $Y \to \prod^{\dim(G)} X$.

The nonempty fibers of f can be easily identified with cosets of appropriate centralizer subgroups. Namely, if $f^{-1}(\underline{g}', \underline{g}) \neq \emptyset$ then $\underline{g}' = h^{-1}\underline{g}h$ for some element $h \in G$ and $f^{-1}(\underline{g}', \underline{g}) = \mathcal{C}_G(\underline{g})h \times \{\underline{g}\}$. All of the involved centralizers contain the subgroup $A = \mathcal{C}_G(X)^0$ and by Lemma 84 at least one of them has dimension $\dim(A)$. For $\underline{g} \in \prod^{\dim(G)} X$ we have $\underline{g} \in X^{\mathrm{nongen}}$ iff $\dim\left(f^{-1}(\underline{g}, \underline{g})\right) > \dim(A)$. By Fact 17.(e) the subset

$$Z = \left\{ t \;\middle|\; \dim\left(f^{-1}\big(f(t)\big)\right) > \dim(A) \right\} \subseteq G \times \prod^{\dim(G)} X$$

is a closed subset and $\deg(Z)$ is bounded in terms of $\dim(G)$, $\deg(G)$, $\mathrm{mult}(G)$, $\mathrm{inv}(G)$, and $\deg(X)$. By the above $\tilde{f}\big(Z \cap f^{-1}(Y)\big) = X^{\mathrm{nongen}} = \overline{X^{\mathrm{nongen}}}$. By Fact 17.(f) and Fact 16.(d) we see that $\deg(X^{\mathrm{nongen}}) = \deg\left(\overline{f(Z)} \cap Y\right) \leq \deg(f) \cdot \deg(Z) \cdot \deg(Y)$ which is bounded in terms of $\dim(G)$, $\deg(G)$, $\mathrm{mult}(G)$, $\mathrm{inv}(G)$, and $\deg(X)$. □

Lemma 87 (= Lemma 44)**.** *Let G be an algebraic group and $A < G$ a CCC-subgroup. Then $\mathcal{C}_G\big(\mathcal{C}_G(A)^0\big)^0 = A$, $\deg(A) \leq \deg(G)$ and $\deg\left(A^{\mathrm{nongen}}\right)$ is bounded in terms of $\dim(G)$, $\deg(G)$, $\mathrm{mult}(G)$ and $\mathrm{inv}(G)$. If $B < G$ is another CCC-subgroup with $A \neq B$ then $A^{\mathrm{gen}} \cap B^{\mathrm{gen}} = \emptyset$.*

Proof. Let $X \leq G$ be a connected closed subgroup such that $A = \mathcal{C}_G(X)^0$. Then $X \subseteq \mathcal{C}_G(A)^0$, A is connected and commutes with $\mathcal{C}_G(A)^0$, hence $A = \mathcal{C}_G(X)^0 \supseteq \mathcal{C}_G\big(\mathcal{C}_G(A)^0\big)^0 \supseteq A$.

Now $\deg(A) \leq \deg(G)$ by Fact 27 and then Lemma 86 implies that $\deg\left(A^{\mathrm{nongen}}\right)$ is bounded in terms of $\dim(G)$, $\deg(G)$, $\mathrm{mult}(G)$ and $\mathrm{inv}(G)$. Finally if $\underline{g} \in A^{\mathrm{gen}}$ then $\mathcal{C}_G\big(\mathcal{C}_G(\underline{g})^0\big)^0 = A \neq B$ hence $\underline{g} \notin B^{\mathrm{gen}}$. This proves that $A^{\mathrm{gen}} \cap B^{\mathrm{gen}} = \emptyset$. □

Chevalley embedding with bounds

In this section we prove an effective version of Chevalley's theorem on quotients of algebraic groups.

The following result is proved by Mumford in [43, Introduction]. See [4, Proposition 8] for a precise formulation in the form we need.

Proposition 88. *Let X be a smooth equidimensional closed subset (called variety in [4]) of the affine space $\overline{\mathbb{F}}^N$. Then the ideal of X in $\overline{\mathbb{F}}[x_1, \ldots, x_N]$, is generated by polynomials of degree at most $\deg(X)$.*

Remark 89. Equidimensional means that all irreducible components of X have the same dimension; see [33, Section 5.3] for a definition of smoothness. Algebraic groups are smooth and equidimensional.

Proposition 90 (= Proposition 60 and Proposition 72)**.** *Let H be a closed subgroup of $SL(n, \overline{\mathbb{F}})$. For some $n' = n'\big(n, \deg(H)\big)$ there is a homomorphism $\mathcal{N}_{SL(n,\overline{\mathbb{F}})}(H) \to SL(n', \overline{\mathbb{F}})$ of degree bounded in terms of n and $\deg(H)$ whose kernel is H. Moreover, if $\overline{\mathbb{F}}$ has characteristic p and H is $Frob_p$-invariant for some p-power q then the homomorphism we construct is $Frob_p$-equivariant.*

This proposition is an effective version of [33, Theorem 11.5]. A standard (and straightforward) way to prove it is to adapt the proof in [33] to families of subgroups. (See [49, pages 56–59] for a very detailed explanation of this method.) Here we follow a more direct approach using Proposition 88, which gives better bounds on the degrees.

Sketch of proof. The proof of [33, Theorem 11.5] relies on [33, Theorem 11.2]. Set $G = SL(n, \overline{\mathbb{F}})$ and consider its coordinate ring $K[G]$ (see [33, Section 1.5]). Let I denote the ideal in $K[G]$ vanishing on H.

For the proof of [33, Theorem 11.2] we need a finite dimensional subspace $W \leq K[G]$ invariant under right translations by all $g \in G$ which contains a generating set of I. Below we give a direct construction for such a subspace.

Consider $\overline{\mathbb{F}}^{n^2}$, the space of n-by-n matrices, denote by $x_{1,1}, \ldots, x_{n,n}$ the coordinates. The group G is a closed subset in $\overline{\mathbb{F}}^{n^2}$, the ideal of G is $\big(\det(x_{i,j}) - 1\big)$, so its coordinate ring $K[G]$ is the factor-ring $\overline{\mathbb{F}}[x_{1,1}, \ldots, x_{n,n}]/\big(\det(x_{i,j}) - 1\big)$. We represent the elements of $K[G]$ by polynomials.

Consider the *right multiplication* action of G on $\overline{\mathbb{F}}^{n^2}$, the space of n-by-n matrices, defined by the formula $(g, m) \to mg^{-1}$. As in [33, Section 8.5], this induces a linear representation $\tilde{\rho}$ of G on the polynomial ring $\overline{\mathbb{F}}[x_{1,1}, \ldots, x_{n,n}]$. Explicitly, for matrices $g = (g_{i,j}) \in G$ and for polynomials f we have

$$\big(\tilde{\rho}_g f\big)(x_{1,1}, \ldots, x_{n,n}) = f\big((x_{i,j}) \cdot g\big) = f\Big(\big(\textstyle\sum_j x_{1,j} g_{j,1}\big), \ldots, \big(\sum_j x_{n,j} g_{j,n}\big)\Big) .$$

Here we substitute linear expressions of the $x_{i,n}$ variables into f, hence $\tilde{\rho}_g$ preserves the degree of the polynomial. As a special case we have

$$\tilde{\rho}_g \det(x_{i,j}) = \det\big((x_{i,j}) \cdot g\big) = \det(x_{i,j}) \cdot \det(g) = \det(x_{i,j}) ,$$

hence $\tilde{\rho}$ descends to a G-action ρ on $K[G]$. This ρ is called the *right translation action* of G, see [33, 8.5].

For $l \geq 0$ let $P_l \leq \overline{\mathbb{F}}[x_{1,1}, \ldots, x_{n,n}]$ denote the subspace of polynomials of degree at most l. Since $\tilde{\rho}$ is degree-preserving we can restrict it to a representation $\tilde{\rho}|_{P_l} : G \to GL(P_l)$. As a basis of P_l we use the monomials, the coordinates of a polynomial f are simply its coefficients f_J for multi-indices J. Expanding the above formula we find that the coefficients of $\tilde{\rho}_g f$ (as a polynomial of the $x_{i,j}$) are polynomial expressions of the variables f_J and $g_{i,j}$. More precisely, they are sums of products of a single coefficient of f and at most l of the $g_{i,j}$. That is, these coefficients are linear in the f_J variables and have degree at most l in the $g_{i,j}$ variables. Hence, $\tilde{\rho}|_{P_l}$ can be given by a $\dim(P_l)$-by-$\dim(P_l)$ matrix $\mathcal{M}_{\tilde{\rho}|_{P_l}}$ whose entries are polynomials of degree at most l in the variables $g_{j,k}$.

Our H is a closed subset both in G and in $\overline{\mathbb{F}}^n$. Let $\tilde{I}$ and I denote the ideal of H in $\overline{\mathbb{F}}[x_{1,1}, \ldots, x_{n,n}]$ and in $K[G]$. Clearly, I is the projection of $\tilde{I}$ into $K[G]$. Being an algebraic group, H must be smooth and equidimensional. By Proposition 88 the ideal $\tilde{I}$ is generated by polynomials of degree at most $\deg(H)$.

Let $W \leq K[G]$ denote the vectorspace of those elements which can be represented by polynomials of degree at most $\deg(H)$, i.e., the projection of $P_{\deg(H)}$. By the

previous argument $I \cap W$ generates the ideal I. Since $\tilde{\rho}$ preserves the degrees, $\rho_g W = W$ for all $g \in G$ as required.

Next we borrow two constructions from [33]. First, we follow the proof of [33, Theorem 11.2]. As in that proof, our W is a finite-dimensional subspace of $K[G]$ which is ρ_g-invariant for all $g \in G$ and contains a generating set of I. As in that proof, we set $M = I \cap W$, $d = \dim(M)$, $V = \bigwedge^d W$, and $L = \bigwedge^d M$. Let $\rho|_W : G \to GL(W)$ be the restriction of ρ to the invariant subspace W. In [33, Theorem 11.2] the representation $\phi : G \to GL(V)$ is the d-th exterior power of $\rho|_W$. The proof of [33, Theorem 11.2] shows that L is a one-dimensional subspace of V such that $H = \big\{g \in G \big| \phi(g)L = L\big\}$.

Since $d \leq \dim(W) \leq \dim(P_{\deg(H)})$ and $\dim(V) \leq \dim(W)^d \leq \dim(P_{\deg(H)})^{\dim(P_{\deg(H)})}$, all these dimensions are bounded in terms of n and $\deg(H)$. The matrix $\mathcal{M}_\rho$ of the representation ρ is, in an appropriate basis, the submatrix of the above matrix $\mathcal{M}_{\tilde{\rho}|_{P_{\dim(W)}}}$ corresponding to the factor-space W. So its entries are polynomials of degree $\deg(H)$ in the $g_{i,j}$ variables. The matrix of ϕ is $\mathcal{M}_\phi = \bigwedge^d \mathcal{M}_\rho$, so its entries are polynomials of degree at most $\deg(H)^d$.

Next, we follow the proof of [33, Theorem 11.5] for the group $G_0 = \mathcal{N}_G(H)$, and the normal subgroup $N = H$. One starts with the above representation ϕ, restricts its domain to G_0, and finds an appropriate G_0-invariant subspace $V_0 \leq V$ to obtain a representation $\phi_0 : G_0 \to GL(V_0)$. After composing ϕ_0 with the adjoint representation $\mathrm{Ad} : GL(V_0) \to GL\big(\mathrm{End}(V_0)\big)$, one finds an appropriate G_0-invariant subspace $W_0 \leq \mathrm{End}(V_0)$ (called W in [33]) to obtain a representation $\psi : G_0 \to GL(W_0)$. It is proved in [33] that $\ker(\psi) = N$.

Clearly $\dim(V_0) \leq \dim(V)$ and $\dim(W_0) \leq \dim\big(\mathrm{End}(V_0)\big) \leq \dim(V)^2$. The matrix $\mathcal{M}_{\phi_0}$ of ϕ_0, in an appropriate basis, is a submatrix of $\mathcal{M}_\phi$, with the same kind of polynomial entries. The matrix of Ad is a $\dim(V_0)^2$-by-$\dim(V_0)^2$ matrix $\mathcal{M}_{\mathrm{Ad}}$ whose entries are rational functions of the $\nu_{i,j}$ with numerators and denominators having degree at most $\dim(V_0)$. One obtains the matrix of the composed representation $\mathrm{Ad} \circ \phi$ by substituting in $\mathcal{M}_{\mathrm{Ad}}$ the variables $\nu_{i,j}$ with the corresponding entries in $\mathcal{M}_{\phi_0}$. Hence, the entries of $\mathcal{M}_{\mathrm{Ad}\circ\phi_0}$ are rational functions of the $g_{i,j}$, the degrees of their numerators and denominators are at most $\dim(V)\deg(H)^d$. The matrix $\mathcal{M}_\psi$ of ψ, in an appropriate basis, is the submatrix of $\mathcal{M}_{\mathrm{Ad}\circ\phi}$ corresponding to the subspace W_0, hence it has the same kind of entries.

Our ψ is a representation in $GL(W_0)$, now we turn it into a representation in $SL(n', \overline{\mathbb{F}})$ where $n' = \dim(W_0) + 1$. To each $m \in GL(W_0)$ we assign the block-diagonal matrix with blocks m and $\frac{1}{\det(m)}$. This defines an embedding $\iota : GL(W_0) \hookrightarrow SL(n', \overline{\mathbb{F}})$. The composition $\iota \circ \psi$ is a representation $\mathcal{N}_G(H) = G_0 \to SL(n', \overline{\mathbb{F}})$. The entries of its matrix $\mathcal{M}_{\iota\circ\psi}$ are rational functions of the $g_{i,j}$, the degrees of their numerator and denominator are bounded in terms of n and $\deg(H)$. It follows that the degree of the morphism $\iota\circ\psi$ is bounded in terms of n and $\deg(H)$.

If the automorphism $Frob_p$ maps H into itself then it transforms W, M, V, L and V_0 into itself, hence it acts on $\mathrm{End}(V_0)$. It follows easily from the proof of [33, Theorem 11.5] that $Frob_p$ maps the subspace $W_0 \leq \mathrm{End}(V_0)$ into itself. Moreover, the morphisms $\tilde{\rho}$, $\tilde{\rho}|_{P_l}$, Ad, and ι (which are defined independently of H) are visibly $Frob_p$-equivariant. Therefore ρ, ϕ, ϕ_0, ψ, and $\iota \circ \psi$ must also be $Frob_p$-equivariant. The representation $\iota\circ\psi$ satisfies all requirements of the proposition. □

Appendix B

A property of the group of fixpoints of Frobenius maps of simple algebraic groups

The following result was communicated to us by Martin Liebeck. Let G be a connected adjoint simple algebraic group over an algebraically closed field $\mathbb{F}$ of characteristic p, and σ a Frobenius map of G. Let $G(q) = (G^\sigma)'$ and assume $G(q)$ is simple.

Proposition 91. *There is no proper connected closed subgroup of G which contains $G(q)$.*

Proof. Suppose for a contradiction that $G(q) < H < G$, where H is connected and closed.

First, we consider the action of $G(q)$ on the adjoint module $L(G)$. The G-composition factors of $L(G)$ are well-known, and can be found in [41, 1.10]. With the exception of $G = B_n, C_n, D_n, F_4$ with $p = 2$ and G_2 with $p = 3$, G is either irreducible on $L(G)$, or has two composition factors, one of which is trivial. In any case, each composition factor is either a restricted $\mathbb{F}G$-module, or a field twist of one. It follows that $G(q)$ is irreducible on every G-composition factor of $L(G)$. Therefore, H is also irreducible on every G-composition factor of $L(G)$, and hence H must be a semisimple group.

For the moment, exclude the exceptions $B_n, \dots G_2$ in the above paragraph. Clearly $G(q)$ fixes $L(H) \subset L(G)$, so it follows that $L(H)$ must be a composition factor of co-dimension 1 in $L(G)$. If U_H is a maximal connected unipotent subgroup of H, then a standard result tells us that $\dim H = 2\dim U_H + \mathrm{rank}(H)$. Since $\dim H = \dim G - 1$, it follows that U_H is also a maximal unipotent subgroup of G, and $\mathrm{rank}(H) = \mathrm{rank}(G) - 1$. So the root system of H has the same number of roots as that of G, and H has rank 1 less than G. An easy check of root systems shows that this is impossible.

It remains to handle the exceptional cases $G = B_n, C_n, D_n, F_4$ ($p = 2$) and G_2 ($p = 3$). Consider G_2 and F_4, and let H_0 be a simple factor of H which contains an isomorphic copy of $G(q)$. Then H_0 is of rank at most 2 (resp. 4), and the smallest projective representation of H_0 has dimension at least that of $G(q)$, which is 7 (resp. 26). This is clearly impossible.

Next let $G = D_n$. Here the G-composition factors of $L(G)$ are of high weights $\lambda_2, 0$ (n odd) or $\lambda_2, 0^2$ (n even). We have already dealt with the case where $\dim H = \dim G - 1$, so we may assume n is even and $\dim H = \dim G - 2$. Then either $\dim U_H = \dim U_G$, $\mathrm{rank}(H) = \mathrm{rank}(G) - 2$, or $\dim U_H = \dim U_G - 1$, $\mathrm{rank}(H) = \mathrm{rank}(G)$. An inspection of root systems shows that neither of these is possible.

Now let $G = C_n$, and let V be the natural $2n$-dimensional G-module. As $G(q)$ cannot act nontrivially on a module of dimension less than $2n$, it must act tensor indecomposably on V, and hence so does H. Therefore, H is simple. The possibilities for $G(q)$ are $C_n(q)$ and $Sz(q)$ (the latter just for $n = 2$). In the former case $G(q)$ has an elementary abelian subgroup $R = r^n$, where r is a prime dividing $q+1$. Note that r is odd as $p = 2$. Also, $\mathrm{rank}(H) \leq \mathrm{rank}(G) = n$. An elementary argument (see [14, Section 2]) shows that the abelian r-rank of H is equal to $\mathrm{rank}(H)$, and hence $\mathrm{rank}(H) = n$. The only possibility is that $H = D_n$. But $G(q) = C_n(q)$ does not lie in D_n as it does not fix a quadratic form on V. If $G(q) = Sz(q)$ then

H cannot have rank 2 (as C_2 has no connected simple proper subgroup of rank 2), so $H = A_1$; but $Sz(q) \not\leq A_1$, a contradiction.

Finally, if $G = B_n$ then there is a morphism from G to C_n which is an isomorphism of abstract groups, and applying this morphism to $G(q)$ and H, we reduce to the C_n case. This completes the proof. □

Acknowledgments

The authors are particularly indebted to Martin Liebeck who proved Proposition 91. The authors also thank Nick Gill, Bob Guralnick, Gergely Harcos, Andrei Jaikin-Zapirain, Attila Maróti, Nikolay Nikolov, Lajos Rónyai, and Tamás Szamuely for various remarks on earlier drafts of this article. The authors thank the referees, whose criticism helped to greatly improve the exposition of this article.

References

[1] Fred Annexstein and Marc Baumslag, *On the diameter and bisector size of Cayley graphs*, Math. Systems Theory **26** (1993), no. 3, 271–291, DOI 10.1007/BF01371728. MR1209998 (94c:05036)

[2] L. Babai, W. M. Kantor, and A. Lubotsky, *Small-diameter Cayley graphs for finite simple groups*, Eur. J. Combin. **10** (1989), no. 6, 507–522, DOI 10.1016/S0195-6698(89)80067-8. MR1022771 (91a:20038)

[3] László Babai and Ákos Seress, *On the diameter of permutation groups*, Eur. J. Combin. **13** (1992), no. 4, 231–243, DOI 10.1016/S0195-6698(05)80029-0. MR1179520 (93h:20001)

[4] Cristina Blanco, Gabriela Jeronimo, and Pablo Solernó, *Computing generators of the ideal of a smooth affine algebraic variety*, J. Symbolic Comput. **38** (2004), no. 1, 843–872, DOI 10.1016/j.jsc.2004.02.002. MR2094559 (2006c:14085)

[5] Jean Bourgain and Alex Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. Math. (2) **167** (2008), no. 2, 625–642, DOI 10.4007/annals.2008.167.625. MR2415383 (2010b:20070)

[6] Jean Bourgain and Alex Gamburd, *Expansion and random walks in* $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$. *II*, J. Eur. Math. Soc. (JEMS) **11** (2009), no. 5, 1057–1103, DOI 10.4171/JEMS/175. With an appendix by Bourgain. MR2538500 (2011a:60021)

[7] Jean Bourgain, Alex Gamburd, and Peter Sarnak, *Affine linear sieve, expanders, and sum-product*, Invent. Math. **179** (2010), no. 3, 559–644, DOI 10.1007/s00222-009-0225-3. MR2587341 (2011d:11018)

[8] J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), no. 1, 27–57, DOI 10.1007/s00039-004-0451-1. MR2053599 (2005d:11028)

[9] Emmanuel Breuillard, Ben Green, and Terence Tao, *Linear approximate groups*, Electron. Res. Announc. Math. Sci. **17** (2010), 57–67, DOI 10.3934/era.2010.17.57. MR2718104 (2011g:11018)

[10] Emmanuel Breuillard, Ben Green, and Terence Tao, *Approximate subgroups of linear groups*, Geom. Funct. Anal. **21** (2011), no. 4, 774–819, DOI 10.1007/s00039-011-0122-y. MR2827010

[11] Emmanuel Breuillard and Ben Green, *Approximate groups, II: The solvable linear case*, Q. J. Math. **62** (2011), no. 3, 513–521, DOI 10.1093/qmath/haq011. MR2825469

[12] Roger W. Carter, *Simple groups of Lie type*, Pure and Applied Mathematics, Vol. 28, John Wiley & Sons, London-New York-Sydney, 1972. MR0407163 (53 #10946)

[13] Roger W. Carter, *Finite groups of Lie type*, Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York, 1985. Conjugacy classes and complex characters; A Wiley-Interscience Publication. MR794307 (87d:20060)

[14] Arjeh M. Cohen and Gary M. Seitz, *The r-rank of the groups of exceptional Lie type*, Nederl. Akad. Wetensch. Indag. Math. **49** (1987), no. 3, 251–259. MR914084 (88k:20062)

[15] Claude Chevalley, *Classification des groupes algébriques semi-simples* (French), Springer-Verlag, Berlin, 2005. Collected works. Vol. 3; Edited and with a preface by P. Cartier; With the collaboration of Cartier, A. Grothendieck, and M. Lazard. MR2124841 (2006b:20068)

[16] Oren Dinai, *Growth in* SL_2 *over finite fields*, J. Group Theory **14** (2011), no. 2, 273–297, DOI 10.1515/JGT.2010.056. MR2788087 (2012c:20134)
[17] Klaus Doerk and Trevor Hawkes, *Finite soluble groups*, de Gruyter Expositions in Mathematics, vol. 4, Walter de Gruyter & Co., Berlin, 1992. MR1169099 (93k:20033)
[18] György Elekes and Zoltán Király, *On the combinatorics of projective mappings*, J. Algebraic Combin. **14** (2001), no. 3, 183–197, DOI 10.1023/A:1012799318591. MR1869409 (2003e:52034)
[19] Walter Feit and Jacques Tits, *Projective representations of minimum degree of group extensions*, Canad. J. Math. **30** (1978), no. 5, 1092–1102. MR0498824 (58 #16861)
[20] G. A. Freĭman, *Groups and the inverse problems of additive number theory* (Russian), Number-theoretic studies in the Markov spectrum and in the structural theory of set addition (Russian), Kalinin. Gos. Univ., Moscow, 1973, pp. 175–183. MR0435006 (55 #7968)
[21] Gregory A. Freiman, *On finite subsets of nonabelian groups with small doubling*, Proc. Amer. Math. Soc. **140** (2012), no. 9, 2997–3002, DOI 10.1090/S0002-9939-2012-11156-6. MR2917072
[22] William Fulton, *Intersection theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 2, Springer-Verlag, Berlin, 1984. MR732620 (85k:14004)
[23] Nick Gill and Harald Andrés Helfgott, *Growth of small generating sets in* $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$, Int. Math. Res. Not. IMRN **18** (2011), 4226–4251. MR2836020
[24] Alireza Salehi Golsefidy and Peter Sarnak, *The affine sieve*, J. Amer. Math. Soc. **26** (2013), no. 4, 1085–1105, DOI 10.1090/S0894-0347-2013-00764-X. MR3073885
[25] W. T. Gowers, *Quasirandom groups*, Combin. Probab. Comput. **17** (2008), no. 3, 363–387, DOI 10.1017/S0963548307008826. MR2410393 (2009f:20105)
[26] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. MR0463157 (57 #3116)
[27] H. A. Helfgott, *Growth and generation in* $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, Ann. Math. (2) **167** (2008), no. 2, 601–623, DOI 10.4007/annals.2008.167.601. MR2415382 (2009i:20094)
[28] H. A. Helfgott, *Growth in* $\mathrm{SL}_3(\mathbb{Z}/p\mathbb{Z})$, J. Eur. Math. Soc. (JEMS) **13** (2011), no. 3, 761–851, DOI 10.4171/JEMS/267. MR2781932
[29] H. A. Helfgott, *Growth in groups: ideas and perspectives*, preprint, arXiv:1303.0239
[30] E. Hrushovski, *The elementary theory of the Frobenius automorphisms*. preprint, arXiv:math.LO/0406514
[31] Ehud Hrushovski, *Stable group theory and approximate subgroups*, J. Amer. Math. Soc. **25** (2012), no. 1, 189–243, DOI 10.1090/S0894-0347-2011-00708-X. MR2833482 (2012h:03104)
[32] E. Hrushovski and A. Pillay, *Definable subgroups of algebraic groups over finite fields*, J. Reine Angew. Math. **462** (1995), 69–91. MR1329903 (97f:20059)
[33] James E. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics, NO. 21, Springer-Verlag, New York-Heidelberg, 1975. MR0396773 (53 #633)
[34] James E. Humphreys, *Conjugacy classes in semisimple algebraic groups*, Mathematical Surveys and Monographs, vol. 43, American Mathematical Society, Providence, RI, 1995. MR1343976 (97i:20057)
[35] I. Martin Isaacs, *Character theory of finite groups*, AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. MR2270898
[36] E. I. Khukhro, Ant. A. Klyachko, N. Yu. Makarenko, and Yu. B. Melnikova, *Automorphism invariance and identities*, Bull. Lond. Math. Soc. **41** (2009), no. 5, 804–816, DOI 10.1112/blms/bdp056. MR2557461 (2010k:20050)
[37] Peter Kleidman and Martin Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990. MR1057341 (91g:20001)
[38] Jordan S. Ellenberg, Chris Hall, and Emmanuel Kowalski, *Expander graphs, gonality, and variation of Galois representations*, Duke Math. J. **161** (2012), no. 7, 1233–1275, DOI 10.1215/00127094-1593272. MR2922374
[39] Michael Larsen, *Exponential generation and largeness for compact p-adic Lie groups*, Algebra Number Theory **4** (2010), no. 8, 1029–1038, DOI 10.2140/ant.2010.4.1029. MR2832632
[40] Vicente Landazuri and Gary M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443. MR0360852 (50 #13299)

[41] Martin W. Liebeck and Gary M. Seitz, *On the subgroup structure of exceptional groups of Lie type*, Trans. Amer. Math. Soc. **350** (1998), no. 9, 3409–3482, DOI 10.1090/S0002-9947-98-02121-7. MR1458329 (99j:20055)

[42] Alexander Lubotzky, *Expander graphs in pure and applied mathematics*, Bull. Amer. Math. Soc. (N.S.) **49** (2012), no. 1, 113–162, DOI 10.1090/S0273-0979-2011-01359-3. MR2869010 (2012m:05003)

[43] David Mumford, *Varieties defined by quadratic equations*, Questions on Algebraic Varieties (C.I.M.E., III Ciclo, Varenna, 1969), Edizioni Cremonese, Rome, 1970, pp. 29–100. MR0282975 (44 #209)

[44] Madhav V. Nori, *On subgroups of* $\mathrm{GL}_n(\mathbf{F}_p)$, Invent. Math. **88** (1987), no. 2, 257–275, DOI 10.1007/BF01388909. MR880952 (88d:20068)

[45] N. Nikolov and L. Pyber, *Product decompositions of quasirandom groups and a Jordan type theorem*, J. Eur. Math. Soc. (JEMS) **13** (2011), no. 4, 1063–1077, DOI 10.4171/JEMS/275. MR2800484 (2012h:20054)

[46] Nikolay Nikolov and Dan Segal, *On finitely generated profinite groups. I. Strong completeness and uniform bounds*, Ann. Math. (2) **165** (2007), no. 1, 171–238, DOI 10.4007/annals.2007.165.171. MR2276769 (2008f:20052)

[47] John E. Olson, *On the sum of two sets in a group*, J. Number Theory **18** (1984), no. 1, 110–120, DOI 10.1016/0022-314X(84)90047-7. MR734442 (85j:20021)

[48] L. Pyber, E. Szabó, Growth in finite simple groups of Lie type. announcement: arXiv:1001.4556

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

[50] L. Pyber, E. Szabó, *Growth in linear groups*, in preparation

[51] László Pyber, *Asymptotic results for permutation groups*, Groups and computation (New Brunswick, NJ, 1991), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, RI, 1993, pp. 197–219. MR1235804 (94g:20003)

[52] I. Z. Ruzsa and S. Turjányi, *A note on additive bases of integers*, Publ. Math. Debrecen **32** (1985), no. 1-2, 101–104. MR810596 (87a:11014)

[53] Terence Tao, *Product set estimates for non-commutative groups*, Combinatorica **28** (2008), no. 5, 547–594, DOI 10.1007/s00493-008-2271-7. MR2501249 (2010b:11017)

[54] Péter P. Varjú, *Expansion in* $SL_d(\mathcal{O}_K/I)$*, I square-free*, J. Eur. Math. Soc. (JEMS) **14** (2012), no. 1, 273–305, DOI 10.4171/JEMS/302. MR2862040

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

E-mail address: pyber.laszlo@renyi.mta.hu

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

E-mail address: szabo.endre@renyi.mta.hu