GENERATING SIMPLE GROUPS

LÁSZLÓ PYBER AND ENDRE SZABÓ

work in progress, December 14, 2009

We shall use the following notation throughout this note. q is a fixed prime power and r is a power of q, $\mathbb{F}_q \leq \mathbb{F}_r$ are the finite fields with q and r elements and $\overline{\mathbb{F}}_q$ is their algebraic closure.

We shall estimate the size of several finite sets. Besides q, our estimates will depend on two positive parameters: N and ε. N will be used to bound dimensions from above and $\varepsilon > 0$ will control the allowed error in the exponents. N will be a constant, but we may choose ε depending on q.

1. DIMENSION AND COMPLEXITY

We shall use affine algebraic geometry: all occurring sets will be subsets of some affine space $\overline{\mathbb{F}}_q^{\,m}$.

Definition 1. A subset $S \subseteq \overline{\mathbb{F}}_q^{\,m}$ 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 $\overline{\mathbb{F}}_q^{\,m}$, each subset of $\overline{\mathbb{F}}_q^{\,m}$ inherits this topology, called the *Zariski topology*. This is the only topology that we use in this note, so we shall omit the adjective Zariski. The complements of closed subsets are called *open*. For an arbitrary subset $X \subseteq \overline{\mathbb{F}}_q^{\,m}$ we shall denote by $\overline{X}$ the *closure* of X.

Definition 2. For arbitrary subsets $X \subseteq Y \subseteq \overline{\mathbb{F}}_q^{\,m}$ we say that X is *relatively closed* in Y if X is the intersection of a closed set and Y, or equivalently, if $\overline{X} \cap Y = X$.

Definition 3. A subset of $\overline{\mathbb{F}}_q^{\,m}$ is *locally closed* if it is relatively closed in some open set, i.e. if it is the intersection of a closed and an open set. A *constructible set* is the union of finitely many locally closed subsets. The collection of constructible sets is closed for basic set-operations: union, intersection, difference.

Definition 4. A constructible set $X \subseteq \overline{\mathbb{F}}_q^{\,m}$ is called *irreducible* if it has the following property. Whenever we write X as the union of finitely many relatively closed subsets, one of them must be equal to X.

Definition 5. Let $X \subseteq \overline{\mathbb{F}}_q^{\,m}$ be a constructible set. We shall consider chains $X_0 \subsetneq X_1 \subsetneq \dots X_n$ where the X_i are nonempty, irreducible, relatively closed subsets of X. The largest possible length n of such a chain is called the *dimension* of X, denoted by $\dim(X)$.

Definition 6. Let $X \subseteq \overline{\mathbb{F}}_q^{\,m}$ be a constructible set. An *affine* subspace is a translate of a linear subspace. We consider affine subspaces $L \subseteq \overline{\mathbb{F}}_q^{\,m}$ such that $\dim(X) = \dim(L)$ and $X \cap L$ is finite. The *degree* of X, denoted by $\deg(X)$, is the largest possible number of intersection points: $\max_L |X \cap L|$.

Note, that the dimension $\dim(X)$ is an internal property of X, but the degree depends also on the way how X is sitting inside $\overline{\mathbb{F}}_q^{\,m}$ (how much it is curved). E.g. a nonconstant polynomial map $f : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q^{\,m}$ sends a line into a curve (a one dimensional constructible set), the degree of the image curve can be arbitrary (depending on the map). In fact, the degree is just the maximum of the degrees of the coordinate polynomials of f.

Definition 7. Let $X \subseteq \overline{\mathbb{F}}_q^{\,m}$ be a constructible set. Then X can be defined as a Boolean combination of Zariski closed subsets in many different ways. In fact, there is a "simplest" Boolean combination. Let $X_0 = X$. By induction on $i \geq 0$ we define $Y_i = \overline{X_i}$, the closure of X_i in $\overline{\mathbb{F}}_q^{\,m}$, and $X_{i+1} = Y_i \setminus X_i$. Then $\dim(Y_{i+1}) < \dim Y_i$, hence $Y_i = \emptyset$ for $i > m$. So we get a canonical Boolean combination:

$$X = \Big(\Big(\big((Y_0 \setminus Y_1) \cup Y_2 \big) \setminus Y_3 \Big) \cup Y_4 \Big) \setminus Y_5 \dots$$

It is not hard to see that the above decomposition can be rewritten as the union of locally closed sets:

$$X = \big(Y_0 \setminus Y_1\big) \cup \big(Y_2 \setminus Y_3\big) \cup \dots$$

We define the *complexity*

$$\delta(X) = \max\big\{ \dim(X), \deg(Y_0), \deg(Y_1), \deg(Y_2), \dots \big\} .$$

Remark 8. Let X be a constructible set. Then $\dim(X) = 0$ iff X is finite. A finite set X is automatically closed, $X = Y_0$ and all other Y_i is empty, hence $\deg(X) = \delta(X) = |X|$ in this case.

Definition 9. A constructible set $X \subseteq \overline{\mathbb{F}}_q^{\,m}$ is built from closed subsets via set-operations (union,intersection, difference), we use several polynomials to describe the appearing closed sets. There are many different ways to build the same X. We say that X is *defined over* $\mathbb{F}_r$ if there is a way to build it using only polynomials whose coefficients belong to $\mathbb{F}_r$.

Remark 10. Fortunately there is a very simple way to detect definability. Since $\mathbb{F}_r$ is a perfect field, X is defined over $\mathbb{F}_r$ iff all relative automorphisms of the field extension $\overline{\mathbb{F}}_q : \mathbb{F}_r$ carry X into itself. Similarly, a morphism is defined over $\mathbb{F}_r$ iff it commutes with all of these field automorphisms. An easy consequence: if the X of Definition 7 is defined over $\mathbb{F}_r$ then so are all the Y_i.

Definition 11. There is an important variation on the notion of irreducibility. Suppose that a constructible set $X \subseteq \overline{\mathbb{F}}_q^{\,m}$ is defined over $\mathbb{F}_r$. We say that X is $\mathbb{F}_r$-*irreducible* if it has the following property: Whenever we write X as the union of finitely many relatively closed subsets which are defined over $\mathbb{F}_r$, one of them must be equal to X.

Definition 12. Let $X \subseteq \overline{\mathbb{F}}_q^{\,m}$ be a constructible set defined over $\mathbb{F}_r$. Then there is a unique decomposition into a finite union $X = \bigcup_i X_i$ where X_i are relatively closed, $\mathbb{F}_r$-irreducible subsets defined over $\mathbb{F}_r$. These X_i are called the $\mathbb{F}_r$-*irreducible components* of X.

Definition 13. Let $X \subseteq \overline{\mathbb{F}}_q^{\,m}$ and $Y \subseteq \overline{\mathbb{F}}_q^{\,n}$ be constructible sets. A function $f : X \to Y$ is called a *morphism* if its graph $\Gamma_f \subseteq X \times Y \subseteq \overline{\mathbb{F}}_q^{\,m+n}$ is constructible. We say that f *is defined over* $\mathbb{F}_r$ if its graph is defined over $\mathbb{F}_r$. We define an invariant, the *complexity* of f, denoted by $\delta(f)$: it is simply the complexity of its graph.

Constructible sets form a category with the above notion of morphism. Most of our constructible sets and morphism will be defined over $\mathbb{F}_r$, either by assumption, or as a consequence of their construction. As a matter of fact, none of our constructions (e.g. those in Fact 16) leads out from the category of constructible sets defined over $\mathbb{F}_r$. Isomorphic constructible sets have equal dimensions. In contrast, their complexities may not be be equal. The following are well-known:

Fact 14. *Let $X, Y \subseteq \overline{\mathbb{F}}_q^{\,m}$ be constructible sets defined over $\mathbb{F}_r$.*

(a) Any constructible subset of X has dimension at most $\dim(X)$.

(b) The $\mathbb{F}_r$-irreducible components $X_i \leq X$ satisfy

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

$$\deg(X_i) \leq \deg(X) = \sum_j \deg(X_j) ,$$

$$\delta(X_i) \leq \delta(X) \leq \sum_j \delta(X_j) .$$

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

(c) *The sets $X \cup Y$, $X \cap Y$, $X \setminus Y$ and the direct product $X \times Y$ are also constructible, they are defined over $\mathbb{F}_r$ and their complexity is bounded in terms of $\delta(X)$ and $\delta(Y)$.*

(d) *Suppose that X is $\mathbb{F}_r$-irreducible and $Y \subseteq X$. Then Y is dense in X iff any of the following equivalent conditions hold:*

$$\dim(Y) = \dim(X) , \quad \dim(X \setminus Y) < \dim(X) .$$

Moreover, such a Y is also $\mathbb{F}_r$-irreducible.

(e) *A direct product of $\mathbb{F}_r$-irreducible constructible sets is again $\mathbb{F}_r$-irreducible.*

Remark 15. Let X be a constructible set defined over $\mathbb{F}_r$ and let $X' \subseteq X$ an $\mathbb{F}_r$-irreducible component. We apply to X the construction in Definition 7 and obtain a sequence Y_i of closed subsets. It is easy to see that if we apply the same construction to X' then we get the sets $\overline{X'} \cap Y_i$. This implies the complexity estimates of Fact 14.(b).

Fact 16. *Let X and $Y \supseteq T$ be constructible sets and $f : X \to \overline{\mathbb{F}_q}^n$ a morphism, all be defined over $\mathbb{F}_r$. We shall define several subsets of X and $\overline{\mathbb{F}_q}^n$. All of them will be constructible of dimension at most $\dim(X)$, defined over $\mathbb{F}_r$, and their complexity will be bounded from above, and the bounds depend only on $\delta(X)$, $\delta(T)$ and $\delta(f)$.*

(a) *The image set $f(X) \subseteq Y$ is constructible. If X is $\mathbb{F}_r$-irreducible then so is $f(X)$.*

(b) *For each $y \in f(X)$ whose coordinates belong to $\mathbb{F}_r$, the fibre $f^{-1}(y) \subseteq X$ is constructible with complexity $\delta\big(f^{-1}(y)\big) \leq \delta(f)$. The subsets $f^{-1}(T)$ and $X \setminus f^{-1}(T)$ are also constructible. (The condition $y \in \mathbb{F}_r{}^n$ is needed to make $f^{-1}(y)$ be defined over $\mathbb{F}_r$.)*

(c) *The function $y \to \dim\big(f^{-1}(y)\big)$ (for $y \in f(X)$) is upper semi-continuous in the Zariski topology of $f(X)$. In particular, the subsets of $f(X)$ corresponding to any given fibre dimension are constructible.*

(d) *For each $y \in f(X)$ we have*

$$\dim(X) \leq \dim\big(f(X)\big) + \dim\big(f^{-1}(y)\big) .$$

Suppose that X is $\mathbb{F}_r$-irreducible. Then those $y \in f(X)$ with minimal $\dim\big(f^{-1}(y)\big)$ form a dense, $\mathbb{F}_r$-irreducible constructible set $Y_{\min} \subseteq f(X)$ (see (c) *above and Fact 14.*(d)*). In this case*

$$\dim(X) = \dim\big(f(X)\big) + \min_{y \in f(X)} \dim\big(f^{-1}(y)\big) .$$

and $f^{-1}(Y_{\min}) \subseteq X$ is also dense and $\mathbb{F}_r$-irreducible.

Definition 17. For a constructible set X let $X(\mathbb{F}_q)$ denote the set of those points on X whose coordinates belong to $\mathbb{F}_q$.

Remark 18. We shall always use the field $\mathbb{F}_r$ to define our constructible sets. In contrast, we shall use the field $\mathbb{F}_q$ for counting the number of points in certain subsets of $X(\mathbb{F}_q)$ where X is some constructible set.

Remark 19. Note, that for $\dim(X) = 0$ one can give an even easier estimate:

$$\left|X(\mathbb{F}_q)\right| \leq |X| = \delta(X) \ .$$

2. Concentration in general

Definition 20. Let $\alpha \subseteq {\mathbb{F}_q}^m$ be a subset. For each constructible set $X \subseteq {\overline{\mathbb{F}}_q}^m$ of positive dimension we define the *concentration* of α in X as follows:

$$\mu(\alpha, X) \stackrel{\text{def}}{=} \frac{\log_q |\alpha \cap X|}{\dim(X)}$$

When $X \cap \alpha = \emptyset$, then we set $\mu(\alpha, X) = -\infty$.

Corollary 21. *Let $X \subseteq {\overline{\mathbb{F}}_q}^m$ be an infinite constructible set. Then for all finite subsets $\alpha \subset {\mathbb{F}_q}^m$ the concentration $\mu(\alpha, X)$ is nonnegative unless $X \cap \alpha = \emptyset$, and it is bounded from above:*

$$\mu(\alpha, X) \leq \log_q |{\mathbb{F}_q}^m| = m$$

Lemma 22. *Let $Z \subseteq {\overline{\mathbb{F}}_q}^m$ be a constructible set defined over $\mathbb{F}_r$ with $\dim(Z) > 0$ and let $\alpha \subseteq {\mathbb{F}_q}^m$ be any subset. Then there is an $\mathbb{F}_r$-irreducible component $Z' \subseteq Z$ such that $\delta(Z') \leq \delta(Z)$ and at least one of the following holds:*

$$\begin{cases} \dim(Z') = \dim(Z) \quad \textit{and} \\ \mu(\alpha, Z') \geq \mu(\alpha, Z) - \log_q \delta(Z)^2 \end{cases} \tag{1}$$

or

$$\begin{cases} 0 < \dim(Z') < \dim(Z) \quad \textit{and} \\ \mu(\alpha, Z') \geq \left(1 + \frac{1}{\dim(Z)}\right) \mu(\alpha, Z) - \log_q \delta(Z)^2 \end{cases} \tag{2}$$

We note that $\mu(\alpha, Z') \geq \mu(\alpha, Z) - \log_q \delta(Z)^2$ in both cases.

Proof. The condition $\delta(Z') \leq \delta(Z)$ is automatic (see Fact 14.(b)). If the right hand side of (1) is non-positive than we can simply take for Z' any $\dim(Z)$-dimensional $\mathbb{F}_r$-irreducible component of Z (see Fact 14.(b)) So we shall assume $\mu(\alpha, Z) > \log_q \delta(Z)^2$, which implies that

$$\left|\alpha \cap Z\right| > \delta(Z)^2 \ .$$

We decompose Z into $\mathbb{F}_r$-irreducible components. There are at most $\delta(Z)$ components. Hence there is a component $Z' \subseteq Z$ with

$$\big|\alpha \cap Z'\big| \geq \frac{|\alpha \cap Z|}{\delta(Z)} \,. \tag{3}$$

Since $\delta(Z') \leq \delta(Z)$ we obtain

$$\big|Z'\big| \geq |Z' \cap \alpha| > \delta(Z)^2/\delta(Z) \geq \delta(Z') \,,$$

hence $\dim(Z') > 0$ (see Remark 19). We take logarithm of the inequality (3), divide the two sides by $\dim(Z')$ and rewrite it in terms of the concentrations. We get an estimate even better than we promised:

$$\mu(\alpha, Z') \geq \frac{\dim(Z)}{\dim(Z')}\mu(\alpha, Z) - \frac{\log_q \delta(Z)}{\dim(Z')} \geq$$

$$\geq \left(1 + \frac{\dim(Z) - \dim(Z')}{\dim(Z')}\right)\mu(\alpha, Z) - \log_q \delta(Z) \,.$$

Note that $0 < \dim(Z') \leq \dim(Z)$ (see Fact 14.(a)), hence our last inequality implies either (1) or (2). □

Lemma 23. *For each $d > 0$ there is a bound $B_2 = B_2(d)$ with the following property. Let $Z \subseteq X$ be constructible sets and $f : X \to \overline{\mathbb{F}}_q^{\,m}$ be a morphism with $\delta(Z) \leq d$, $\delta(f) \leq d$ and $\dim\big(f(Z)\big) > 0$. Suppose, that X, Z and f are defined over $\mathbb{F}_r$ and Z is $\mathbb{F}_r$-irreducible. Then for all finite subsets $\alpha \subseteq X(\mathbb{F}_q)$ and for all values $\varepsilon \geq 0$ either*

$$\mu\big(f(\alpha), f(Z)\big) \geq \mu(\alpha, Z) - \log_q B_2 - \varepsilon \cdot \dim(Z) \tag{4}$$

or there is a constructible subset $S \subset Z$ defined over $\mathbb{F}_r$ such that $\delta(S) \leq B_2$, $0 < \dim(S) < \dim(Z)$ and

$$\mu(\alpha, S) \geq \mu(\alpha, Z) - \log_q B_2 + \varepsilon \,. \tag{5}$$

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

Proof. If $Z \cap \alpha = \emptyset$ then (4) holds automatically since the left hand side is $-\infty$. So we shall assume $Z \cap \alpha \neq \emptyset$. This implies that $f(\alpha) \cap f(Z) \neq \emptyset$ hence the left hand side of (4) is nonnegative.

First we prove the lemma with some bound B_2' in the special case when all fibres of f have the same dimension, i.e.

$$\dim\big(f^{-1}(t)\big) = \dim(Z) - \dim\big(f(Z)\big) \tag{6}$$

for all $t \in f(Z)$ (see Fact 16.(d)). In this case we get:

$$\big|\alpha \cap Z\big| = \sum_{t \in f(Z)} \big|\alpha \cap f^{-1}(t)\big| \leq \big|f(\alpha) \cap f(Z)\big| \cdot \max_{t \in f(Z)} \big|\alpha \cap f^{-1}(t)\big|$$

We shall fix a value $t \in f(Z)$ where $\big|\alpha \cap f^{-1}(t)\big|$ is maximal, and define $S = f^{-1}(t)$. Since $Z \cap \alpha \neq \emptyset$, our t must lie in $f(\alpha)$, hence its coordinates belong to $\mathbb{F}_q \leq \mathbb{F}_r$. This ensures us that S is constructible and defined over $\mathbb{F}_r$ (see Fact 16.(b)). The equation (6) implies that $\dim(S) = \dim(Z) - \dim\big(f(Z)\big) < \dim(Z)$. We distinguish two possibilities. If $\dim(S) > 0$, then we rewrite the previous inequality with the new notation:

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

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

$$\mu(\alpha, Z) \cdot \dim(Z) \leq \mu\big(f(\alpha), f(Z)\big) \cdot \dim(f(Z)) + \mu\big(\alpha, S\big) \cdot \dim(S)$$

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

$$\mu(\alpha, Z) \leq$$

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

We recall (6), i.e. that $\dim(Z) = \dim(f(Z)) + \dim(S)$. Therefore we see a weighted arithmetic mean on the right hand side. Either

$$\mu(\alpha, Z) \leq \mu\big(f(\alpha), f(Z)\big) + \varepsilon \dim(S) \leq \mu\big(f(\alpha), f(Z)\big) + \varepsilon \dim(Z)$$

or

$$\mu(\alpha, Z) \leq \mu\big(\alpha, S\big) - \varepsilon \dim(f(Z)) \leq \mu\big(\alpha, S\big) - \varepsilon \,,$$

hence either (4) or (5) holds even without the error term $\log_q B_2$. The special case of the lemma is proven for the case $\dim(S) > 0$. On the other hand, if $\dim(S) = 0$ then all fibres of f are finite, and the number of points in each fibre is at most $\delta(f) \leq d$ (see Fact 16.(b)). Hence

$$\mu\Big(f(\alpha), f(Z)\Big) \geq \frac{\log_q \big|f(\alpha \cap Z)\big|}{\dim\big(f(Z)\big)} \geq \frac{\log_q \Big(\big|\alpha \cap Z\big| / \delta(f)\Big)}{\dim(Z)} \geq$$

$$\geq \frac{\log_q \big|\alpha \cap Z\big| - \log_q d}{\dim(Z)} \geq \mu(\alpha, Z) - \log_q d \,,$$

hence (4) holds for any $B_2 \geq d$. The special case of the lemma is proven with the bound $B_2' = \max(2, d)$.

Next we prove the lemma in full generality with a slightly larger bound $B_2 = B_2(d, B_2')$. If $\mu(\alpha, Z) \leq \log_q B_2$ then the inequality (4) is automatic since the right hand side is nonpositive and the left hand side is nonnegative. So we shall assume $\mu(\alpha, Z) > \log_q B_2$ which implies

$$\big|\alpha \cap Z\big| > B_2 \,. \tag{7}$$

We define the following subset:

$$T = \left\{ t \in f(Z) \;\middle|\; \dim\left(f^{-1}(t)\right) = \dim(Z) - \dim\left(f(Z)\right) \right\} .$$

It follows from Fact 16.(b) and (c) that T and $Z' = f^{-1}(T)$ are constructible sets defined over $\mathbb{F}_r$ and their complexity is bounded in terms of d. Moreover, the irreducibility of Z implies that $f(Z)$ is irreducible (see Fact 16.(a)), and $T \subseteq f(Z)$ and $Z' \subseteq Z$ are both $\mathbb{F}_r$-irreducible dense subsets (see Fact 16.(d)). In particular, $\dim(Z) = \dim(Z')$ and $\dim\left(f(Z')\right) = \dim(T) = \dim\left(f(Z)\right) \geq 1$ (see Fact 14.(d)). First we deal with the case $|Z' \cap \alpha| \geq \left|Z \cap \alpha\right|/2$. Then

$$\mu(Z', \alpha) = \frac{\log_q \left|\alpha \cap Z'\right|}{\dim(Z')} \geq \frac{\log_q \left|\alpha \cap Z\right| - \log_q 2}{\dim(Z)} \geq \mu(Z, \alpha) - \log_q 2 \, .$$

We can apply the lemma to Z' (which we established at the beginning), hence we get either

$$\mu\big(f(\alpha), f(Z)\big) \geq \mu\big(f(\alpha), f(Z')\big) \geq \mu(\alpha, Z') - \log_q B_2' - \varepsilon \cdot \dim(Z') \geq$$

$$\geq \mu(\alpha, Z) - \log_q 2 - \log_q B_2' - \varepsilon \cdot \dim(Z') = \mu(\alpha, Z) - \log_q(2B_2') - \varepsilon \cdot \dim(Z)$$

or there is an $S \subset Z'$ defined over $\mathbb{F}_r$ such that $\delta(S) \leq B_2'$, $0 < \dim(S) < \dim(Z') = \dim(Z)$ and

$$\mu(\alpha, S) \geq \mu(\alpha, Z') - \log_q B_2' + \varepsilon \geq \mu(\alpha, Z) - \log_q 2 - \log_q B_2' + \varepsilon =$$

$$= \mu(\alpha, Z) - \log_q(2B_2') + \varepsilon \, .$$

hence the lemma holds in this case. In the remaining case we have $\left|Z' \cap \alpha\right| < \left|Z \cap \alpha\right|/2$. Now we set $S = Z \setminus Z'$. Then $\delta(S)$ is bounded (see Fact 16.(b)), $\dim(S) < \dim(Z)$ by the density (see Fact 14.(d)). By the inequality (7) the set S has at least $|S \cap \alpha| \geq |\alpha \cap Z|/2 \geq B_2/2$ points. If we choose $B_2 > \delta(S)$ then $\dim(S) > 0$ (see Remark 19), hence $\mu(\alpha, S)$ is defined and we can write:

$$\mu(\alpha, S) = \frac{\log_q |S \cap \alpha|}{\dim(S)} \geq \frac{\log_q |Z \cap \alpha| - \log_q 2}{\dim(S)} \geq$$

$$\geq \frac{\dim(Z)}{\dim(S)} \mu(\alpha, Z) - \frac{\log_q 2}{\dim(S)} \geq \mu(\alpha, Z) - \log_q 2 + \frac{\mu(\alpha, Z)}{\dim(S)} \geq$$

$$\geq \mu(\alpha, Z) - \log_q 2 + \frac{\mu(\alpha, Z)}{\dim(Z)} \, .$$

We compare now the last term to ε. If $\varepsilon \leq \frac{\mu(\alpha, Z)}{\dim(Z)}$ then we can replace the last term with ε which proves the inequality (5) for any $B_2 \geq 2$ in this case. On the other hand, for larger ε, i.e. when $\varepsilon > \frac{\mu(\alpha, Z)}{\dim(Z)}$, the

inequality (4) holds, since its right hand side becomes negative. We proved the lemma in all cases. □

3. Constructible sets in groups

Definition 24. $G \leq GL(N, \overline{\mathbb{F}}_q)$ will denote a closed subgroup of the general linear group defined over $\mathbb{F}_r$. For simplicity, we shall say that "G is a linear algebraic group over $\mathbb{F}_r$". We use this matrix realisation of G to calculate complexities of constructible subsets. We shall use the notation

$$\operatorname{repdim}(G) = N^2$$

As usual, $\langle A \rangle$, $\mathcal{N}_G(A)$ and $\mathcal{C}_G(A)$ will denote the generated subgroup, the normaliser and the centraliser of a subset $A \subseteq G$. We shall often use products of several elements and subsets in the usual sense. In order to distinguish from this kind of product, the n-fold direct product of a subset $\alpha \subseteq G$ is denoted by $\prod^n \alpha \subseteq G^n$. For each sequence $\underline{g} = (g_1, g_2, \dots g_n) \in G^n$ we define the morphism

$$\tau_{\underline{g}} : G^{n+1} \to G \qquad : \qquad \tau_{\underline{g}}(a_0, a_1, \dots a_n) = a_0 g_1 a_1 g_2 a_2 \dots g_n a_n$$

We denote by $\Delta(G)$ the largest of the complexities of the variety G and of the maps $\tau_{(h)}$ for all $h \in G$. Then the complexity of the more general $\tau_{\underline{g}}$ can be bounded from above in terms of $\Delta(G)$ and the length of the sequence $\underline{g}$. Closed subgroups of G can be very complicated. In contrast, cosets of normaliser or centraliser subgroups are defined by linear equations, hence they are automatically closed and their complexity is at most $\Delta(G)$. The subset $G(\mathbb{F}_q)$ is a finite subgroup.

Fact 25. *Let G be a linear algebraic group and $X \leq G$ a constructible subset. Then the generated subgroup $\langle X \rangle \leq G$ is a closed subgroup. If X is irreducible then $\langle X \rangle$ is connected. It follows from Corollary 21 that for all finite sets $\alpha \subseteq G(\mathbb{F}_q)$ we have*

$$\mu(\alpha, X) \leq \operatorname{repdim}(G) \ .$$

Lemma 26. *Let G be a linear algebraic group and $A, B \subseteq G$ nonempty constructible sets. Suppose that $\dim(A) = \dim(AgB)$ for some element $g \in G$. Then there are connected closed subgroups $K \leq H \leq G$ of dimension $\dim(B) \leq \dim(K) \leq \dim(H) \leq \dim(A)$ such that*

$$\left\{ m \in G \;\middle|\; \dim(AmB) = \dim(A) \right\} \subseteq g \left\{ n \in G \;\middle|\; nKn^{-1} \leq H \right\} \ . \tag{8}$$

In particular, if $\dim(A) = \dim(B)$ then $K = H$ and on the right hand side we see a coset of the normaliser $\mathcal{N}_G(H)$.

Remark 27. In fact for $\dim(A) = \dim(B)$, with a little extra work, one can prove equality in (8), but we do not need this.

Proof. Let $A' \subseteq \overline{A}$ and $B' \subseteq \overline{B}$ be irreducible components such that $\dim(A') = \dim(A)$ and $\dim(B') = \dim(B)$. We shall define

$$H = \left\{ h \in G \;\middle|\; A'gh = A'g \right\},$$

it is certainly a closed subgroup. Let us pick elements $a \in A'g$ and $b \in B'$. Then $1 \in a^{-1}A'g$ and $1 \in B'b^{-1}$. On the one hand

$$H \subseteq a^{-1}A'gH = a^{-1}A'g$$

implies that $\dim(H) \leq \dim(A)$. On the other hand we may consider the following constructible subsets:

$$A'g \subseteq (A'g) \cdot (B'b^{-1}) \subseteq \overline{A'}g\overline{B'}b^{-1} \subseteq (\overline{A'gB'}) \cdot b^{-1} .$$

The first one and the last one are is irreducible closed sets of dimension $\dim(A)$ (see Fact 14.(e) and Fact 16. (a)), hence all of these sets are equal. But then $A'g = (A'g) \cdot (B'b^{-1})$, therefore

$$B'b^{-1} \subseteq H$$

Let K denote the closed subgroup generated by $B'b^{-1}$, it is connected because B' is irreducible, and the above formula shows that $K \leq H$. The dimension requirements are also satisfied:

$$\dim(B) = \dim(B'b^{-1}) \leq \dim(K) \leq \dim(H) \leq \dim(A) .$$

Suppose now, that $\dim\left(A(gn)B\right) = \dim(A)$ for certain $\tilde{n} \in G$. We can repeat the whole argument for $\tilde{n}B'$ and $\tilde{n}b$ in the role of B' and b, then $\tilde{n}Bb^{-1}\tilde{n}^{-1} \subseteq \tilde{n}K\tilde{n}^{-1}$ will play the role of $B'b^{-1} \subseteq K$ but the definition of H remains unaffected. Hence the closed subgroup $\tilde{n}K\tilde{n}^{-1}$ is also in H. Therefore

$$\tilde{n} \in \left\{ n \in G \;\middle|\; nKn^{-1} \leq H \right\}$$

as we promised in (8). Finally, if $\dim(A) = \dim(B)$ then we have two connected closed subgroups $K \leq H$ of equal dimension, hence they are equal. □

Corollary 28. *Let G be a linear algebraic group over $\mathbb{F}_r$ and let $1 \in \alpha \subseteq G(\mathbb{F}_q)$ be a generating set. Suppose that $G(\mathbb{F}_q)$ does not normalise any closed subgroup $H < G$ with $0 < \dim(H) < \dim(G)$. Then for each infinite constructible subset $Y \subset G$ and for all integers $n \geq 2^{\dim(G)-\dim(Y)} - 1$ there is a sequence $\underline{g} = (g_1, g_2, \ldots g_n) \subseteq \prod^n \alpha$ of generators such that the product set*

$$\tau_{\underline{g}}\left(\prod^{n+1} Y\right) = Y g_1 Y g_2 Y \ldots g_n Y$$

has dimension $\dim(G)$.

Proof. If $A, B \subseteq G$ are constructible sets and $b \in B$ then $\dim(AB) \geq \dim(Ab) = \dim(A)$. Hence if a sequence $\underline{g}$ satisfies the lemma, then so do those sequences which contain $\underline{g}$ as a subsequence. So we may assume $n = 2^{\dim(G)-\dim(Y)} - 1$. We shall prove by downward induction on $\dim(Y)$. If $\dim(Y) = \dim(G)$ then $n = 0$ and $\tau_{\underline{g}}$ is just the inclusion $Y \hookrightarrow G$ so there is nothing to prove. Let us assume that $\dim(Y) < \dim(G)$ and the lemma holds for subsets of larger dimension.

Our first goal is to find an element $g \in \alpha$ such that $\dim(YgY) > \dim(Y)$. Let us start with $g = 1 \in \alpha$. If $\dim(YgY) > \dim(Y)$ then we keep this g, otherwise we are going to replace it with a better one. Let us apply Lemma 26 to $A = B = Y$, we get a closed subgroup H. Since $\dim(Y) = \dim(H) < \dim(G)$, our conditions imply that $G(\mathbb{F}_q) \not\subseteq \mathcal{N}_G(H)$. Therefore $\alpha \not\subseteq \mathcal{N}_G(H)$ and there is an element $g' \in \alpha$ such that $g' \notin 1 \cdot \mathcal{N}_G(H)$. We replace g with this g', this way we achieve that $\dim(YgY) > \dim(Y)$ in all cases.

Now we can apply the induction hypotheses to the set YgY, hence get a sequence $(h_1, h_2, \dots h_m) \subseteq \prod^m \alpha$ with $m = 2^{\dim(G)-\dim(Y)-1} - 1$ such that the product set

$$(YgY)h_1(YgY)h_2 \dots h_m(YgY)$$

has dimension $\dim(G)$. This is a product of the required form, the corollary is proved. □

Lemma 29. *Let G be a linear algebraic group and $Z \subseteq G \times G$ a nonempty constructible set. Suppose that $\tau_{(g)}(Z)$ has dimension 0 for some element $g \in G$, i.e. it is a finite set. Then there is a constructible subset $A \subseteq G$ such that* $\dim(A) = \dim(Z)$ *and*

$$\left\{ c \in G \;\middle|\; \dim\Big(\tau_{(c)}\big(Z\big)\Big) = 0 \right\} = \mathcal{C}_G\big(A\big)g \tag{9}$$

Proof. Let $Z = \bigcup_i Z_i$ be the decomposition of Z into irreducible components. By assumption $\tau_{(g)}(Z_i)$ is finite and irreducible (see Fact 16.(a)), hence it is a single point $z_i \in G$. Let $\mathrm{pr}_1 : G \times G$ denote the projection on the first factor. We choose an element $a_i \in \mathrm{pr}_1(Z_i)$, and set $A_i = a_i^{-1} \mathrm{pr}_1(Z_i)$, $b_i = a_i^{-1} z_i$. This A_i is irreducible and by definition $1 \in A_i$. Then each point of Z_i has the form $(a_i h, \beta)$ with some $h \in A_i$ and $\beta \in G$, and for all $h \in A_i$ must exists at least one such point. But then

$$z_i = \tau_{(g)}(a_i h, \beta) = a_i h g \beta$$

hence

$$\beta = g^{-1} h^{-1} a_i^{-1} z_i = g^{-1} h^{-1} b_i$$

is the only possible choice for β. Therefore

$$Z_i = \Big\{ \big(a_i h, g^{-1} h b_i\big) \;\Big|\; h \in A_i \Big\}$$

and the map

$$A_i \to Z_i \ , \quad h \to \big(a_i h, g^{-1} h b_i\big)$$

is a one-to-one morphism. In particular $\dim(Z_i) = \dim(A_i)$. Hence

$$\tau_{(c)}(Z) = \bigcup_i \Big\{ (a_i h) c (g^{-1} h^{-1} b_i) \;\Big|\; h \in A_i \Big\} =$$

$$= \bigcup_i a_i \Big\{ h(cg^{-1})h^{-1}) \;\Big|\; h \in A_i \Big\} b_i$$

for all $c \in G$. This has dimension 0 iff the $\big\{ h(cg^{-1})h^{-1} \big| h \in A_i \big\}$ is finite for all i. But A_i is irreducible, hence its image $\big\{ h(cg^{-1})h^{-1} \big| h \in A_i \big\}$ is also irreducible (see Fact 16.(a)), so it is finite iff it is a single point, i.e. iff $h(cg^{-1})h^{-1}$ is independent of $h \in A_i$. But $1 \in A_i$, hence this last condition is equivalent to $h(cg^{-1})h^{-1} = cg^{-1}$ for all $h \in A_i$, which simply means that cg^{-1} commutes with all $h \in A_i$ for all i, i.e. $cg^{-1} \in \mathcal{C}_G(\cup_i A_i)$. This proves the lemma for $A = \cup_i A_i$, since

$$\dim(A) = \max_i \big(\dim(A_i) \big) = \max_i \big(\dim(Z_i) \big) = \dim(Z) \ .$$

□

Corollary 30. *Let G be a linear algebraic group over $\mathbb{F}_r$ and let $1 \in \alpha \subseteq G(\mathbb{F}_q)$ be a generating set. Suppose that the centraliser of $G(\mathbb{F}_q)$ in G is finite. Then for each infinite constructible subset $Z \subset G^{n+1}$ (with $n \geq 0$) there is a sequence $\underline{g} = (g_1, g_2, \dots g_n) \in \prod^n \alpha$ of generators such that image set $\tau_{\underline{g}}(Z)$ has positive dimension.*

Proof. We shall prove the theorem by induction on n. For $n = 0$ the statement is obvious. So let $n \geq 1$ and we assume that the corollary holds for smaller number of factors. We define several morphisms. For all $g \in G$ let

$$\sigma_g : G^{n+1} \to G^n \ , \qquad \sigma_g(a_0, a_1, \dots a_n) = (a_0 g a_1, a_2, a_3, \dots a_n)$$

and let

$$\pi : G^{n+1} \to G^{n-1} \ , \qquad \pi(a_0, a_1, \dots a_n) = (a_2, a_3, \dots a_n) \ ,$$

$$\rho : G^n \to G^{n-1} \ , \qquad \rho(a_1, \dots a_n) = (a_2, a_3, \dots a_n) \ .$$

For $n = 1$ we use the convention that G^0 a single point. Note, that these morphisms manipulate only the first two coordinates. In particular

$$\rho\big(\sigma_g(x)\big) = \pi(x) \qquad \text{for all } x \in G^{n+1} \ .$$

Our goal is to find a generator $g \in \alpha$ such that

$$\dim\big(\sigma_g(Z)\big) > 0\ . \tag{10}$$

Then we can use the induction hypotheses for $\sigma_g(Z) \subseteq G^n$, and this proves the corollary for Z as well.

We distinguish two cases. Suppose first that for all $z \in G^{n-1}$ the subset $Z \cap \pi^{-1}(z)$ is finite (i.e. 0 dimensional). Then $\dim(Z) = \dim \pi(Z)$ is positive (see Fact 16.(d)). But

$$\dim(Z) \geq \dim\big(\sigma_g(Z)\big) \geq \dim\big(\rho\big(\sigma_g(Z)\big)\big) = \dim\big(\pi(Z)\big)$$

hence all these dimensions are equal. Hence (10) is achieved, the corollary holds in this case.

Suppose next that there is a point $z \in G^{n-1}$ such that $Z' = Z \cap \pi^{-1}(z)$ has positive dimension. For simplicity we shall identify the subset $\pi^{-1}(z) = G^2 \times \{z\} \subset G^{n+1}$ with G^2 and also $\rho^{-1}(z) = G \times \{z\} \subset G^n$ with G. With these identification we have

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

Let us start with $g = 1 \in \alpha$. If $\sigma_1(Z') = \tau_{(1)}(Z')$ has positive dimension then we keep this g, otherwise we are going to replace it with a better one. We apply Lemma 29 to our Z' and the "bad" $g = 1$, and get an infinite subset $A \leq G$. Then A does not centralise $G(\mathbb{F}_q)$, hence there is a generator $g' \in \alpha$ which does not commute with A, i.e. $g' \notin \mathcal{C}_G(A) \cdot 1$. We replace g by this g', then $\tau_{(g)}(Z') = \sigma_g(Z')$ has positive dimension in this case as well. But then the larger set $\sigma_g(Z) \supseteq \sigma_z(Z')$ has positive dimension as well. In all cases we proved (10), hence the corollary is true. □

Question 31. *Let $Z \subseteq G \times G$ a constructible set, $\mathrm{pr}_2(Z) \subseteq G$ denote its projection on the second factor. Then*

$$\dim\big(\tau_{(g)}(Z)\big) \geq \dim(Z) - \dim\big(\mathrm{pr}_2(Z)\big)\ .$$

What can we say if it is an equality and Z is irreducible?

4. spreading large concentration in a group

Lemma 32. *For all $d > 0$ and $n > 0$ there is a bound $K_2 = K_2(n, d)$ with the following property. Let G be a linear algebraic group over $\mathbb{F}_r$ with $\Delta(G) \leq d$ and $1 \in \alpha \subseteq G(\mathbb{F}_q)$ a generating set. Suppose that the centraliser of $G(\mathbb{F}_q)$ in G is finite. Then for all constructible subset $Z \subset G^{n+1}$ defined over $\mathbb{F}_r$ such that $\dim(Z) > 0$ and $\delta(Z) \leq d$ there is a constructible subset $Y \subseteq G$ defined over $\mathbb{F}_r$ with $\dim(Y) > 0$, $\delta(Y) \leq K_2$ and*

$$\mu\big(\alpha^{2n+1}, Y\big) \geq \mu\big(\textstyle\prod^{n+1}\alpha, Z\big) - \log_q K_2\ .$$

Proof. We prove the lemma by induction on $\dim(Z)$ so we assume it holds in dimensions smaller than $\dim(Z)$ with some bound $K_2'(n,d)$. By Lemma 22 there is an $\mathbb{F}_r$-irreducible component $Z' \subseteq Z$ with large concentration:

$$\mu(\prod^{n+1}\alpha, Z') \geq \mu(\prod^{n+1}\alpha, Z) - \log_q \delta(Z)^2 \ .$$

We may simply replace Z with this component, so from now on Z is $\mathbb{F}_r$-irreducible. Corollary 30 gives us a sequence $\underline{g} = (g_1, g_2, \dots g_n) \in \prod^{n+1}\alpha$ such that $\tau_{\underline{g}}(Z)$ has positive dimension. It is clear, that $\delta(\tau_{\underline{g}})$ has an upper bound depending only on $\Delta(G) \leq d$ and n, let $D = D(d,n)$ denote larger of this bound and d.

We use Lemma 23. for the two constructible sets $Z \subseteq X = G^{n+1}$, the morphism $f = \tau_{\underline{g}}$, the finite set $\prod^{n+1}\alpha$ (denoted by α in Lemma 23.) and $\varepsilon = 0$. We note, that $f\big(\prod^{n+1}\alpha\big) \subseteq \alpha^{2n+1}$. There are two possible outcomes. In case of Lemma 23.(4) we have a constructible subset $T \subseteq G$ with $\dim(T) > 0$, $\delta(T) \leq B_2(D)$ and

$$\mu\big(\prod^{n+1}\alpha, Z\big) - \log_q B_2(D) \leq \mu\big(f\big(\prod^{n+1}\alpha\big), T\big) \leq \mu\big(\alpha^{2n+1}, T\big)$$

hence the lemma holds now with $Y = T$ and any $K_2 \geq B_2(D)$. In case of Lemma 23.(5) we have a constructible subset $S \subseteq Z \subseteq G^{n+1}$ with $0 < \dim(S) < \dim(Z)$, $\delta(S) \leq B_2(D)$ and

$$\mu(\prod^{n+1}\alpha, S) \geq \mu(\prod^{n+1}\alpha, Z) - \log_q B_2(D) \ .$$

We set $K_2'' = K_2'\big(n, B_2(D)\big)$ and apply the induction hypothesis to this S. This gives us a constructible set $Y \subseteq G$ such that $\dim(Y) > 0$, $\delta(Y) \leq K_2''$ and

$$\mu(\alpha^{2n+1}, Y) \geq \mu(\prod^{n+1}\alpha, S) - \log_q K_2'' \geq$$

$$\geq \mu(\prod^{n+1}\alpha, Z) - \log_q \big(B_2(D)K_2''\big) \ ,$$

the lemma holds again with the bound $K_2 = B_2(D)K_2''$. □

Lemma 33. *For all values $d > 0$, $N > 0$ and $0 < \kappa < 1$ there are constants $K_1 = K_1(N,d,\kappa) > 0$ and $\lambda = \lambda(N,\kappa) > 1$ with the following property. Let G be a linear algebraic group over $\mathbb{F}_r$ with $\dim(G) \leq \log_2 N$, $\Delta(G) \leq d$ and $1 \in \alpha \subseteq G(\mathbb{F}_q)$ be a generating set. Suppose that $G(\mathbb{F}_q)$ does not normalise any closed subgroup $H < G$ with $0 < \dim(H) < \dim(G)$ and the centraliser of $G(\mathbb{F}_q)$ in G is finite. Then for all constructible subsets $Y \subset G$ defined over $\mathbb{F}_r$ such that $\dim(Y) > 0$, $\delta(Y) \leq d$ and*

$$\mu(\alpha, Y) \geq \log_q K_1 \tag{11}$$

there is a constructible set $T \subseteq G$ defined over $\mathbb{F}_r$ such that $\delta(T) \leq K_1$ and at least one of the following holds:

$$\dim(T) = \dim(G) \quad \textit{and} \quad \mu\big(\alpha^{2N-1}, T\big) \geq \kappa \cdot \mu(\alpha, Y) \tag{12}$$

or

$$\dim(G) > \dim(T) > 0 \quad \textit{and} \quad \mu\big(\alpha^{2N-1}, T\big) \geq \lambda \cdot \mu(\alpha, Y)\ . \tag{13}$$

Proof. By using Lemma 22, as in the proof of Lemma 32, we may assume that Y is $\mathbb{F}_r$-irreducible. We apply Corollary 28. for $n = N-1$ and the subset Y, this gives us a sequence $\underline{g} = (g_1, g_2, \dots g_n) \in \prod^n \alpha$ of generators such that the image set $\tau_{\underline{g}}(\prod^N Y) \subseteq G$ has dimension $\dim(G)$. Next we apply Lemma 23. to the subsets $X = G^N$ and $Z = \prod^N Y$, the morphism $f = \tau_{\underline{g}}$, the finite set $\prod^N \alpha$ (denoted by α in Lemma 23.) and we set

$$\varepsilon = (1-\kappa) \cdot \frac{\mu(\alpha, Y)}{N \dim(G)}\ .$$

Since Y is $\mathbb{F}_r$-irreducible, Z is also $\mathbb{F}_r$-irreducible (see Fact 16.(e)). In this setup $\delta(Z) = \delta(Y)^N \leq d^N$ and $\delta(f) \leq \Delta(G)^{N-1} \leq d^N$. Therefore the prerequisites of the Lemma 23 are satisfied with the bound d^N (which is denoted there by d) hence the inequalities 23.(4) and 23.(5) are valid with $B_2 = B_2(d^N)$. We define

$$K_1 = B_2^{2N \dim(G)/(1-\kappa)} \geq B_2$$

then the error term of 23.(4) and 23.(5) can be written, using (11), as

$$\log_q B_2 = \frac{1-\kappa}{2N \dim(G)} \cdot \log_q K_1 \leq \frac{1-\kappa}{2N \dim(G)} \cdot \mu(\alpha, Y) = \varepsilon/2$$

Moreover, $\mu\big(\prod^N \alpha, Z\big) = \mu(\alpha, Y)$ and $f\big(\prod^N \alpha\big) \subseteq \alpha^{2N-1}$. In Lemma 23 there are two possible scenarios. I case of 23.(4) we define $T = f(Z)$, then $\dim\big(f(Z)\big) = \dim(G)$ by the definition of $f = \tau_{\underline{g}}$ and we have

$$\mu\big(\alpha^{2N-1}, T\big) \geq \mu\big(f\big(\textstyle\prod^N \alpha\big), f(Z)\big) \geq$$

$$\geq \mu\big(\textstyle\prod^N \alpha, Z\big) - \log_q B_2 - \varepsilon \cdot \dim(Z) \geq \mu(\alpha, Y) - \varepsilon/2 - \varepsilon \cdot \big(N \dim(G) - N\big) \geq$$

$$\geq \mu(\alpha, Y) - \varepsilon \cdot N \dim(G) = \kappa \cdot \mu(\alpha, Y)$$

which is nothing but the inequality (12). In case of 23.(5) we have a subset $S \subseteq G^N$ with $\dim(S) > 0$, $\delta(S) \leq B_2$.

$$\mu\big(\textstyle\prod^N \alpha, S\big) \geq \mu\big(\prod^N \alpha, Z\big) - \log_q B_2 + \varepsilon \geq$$

$$\geq \mu(\alpha, Y) + \varepsilon/2 = \left(1 + \frac{1-\kappa}{2N \dim(G)}\right) \cdot \mu(\alpha, Y)\ .$$

We combine this with (11):

$$\mu\big(\textstyle\prod^N \alpha, S\big) \geq \left(1 + \dfrac{1-\kappa}{4N\dim(G)}\right) \cdot \mu(\alpha, Y) + \dfrac{1-\kappa}{4N\dim(G)} \log_q K_1 \ .$$

We apply Lemma 32. to $Z = S$, $n = N-1$, and for the value denoted by d in the lemma we set $D = \max(d^N, B_2)$. Then in the inequalities we have to use $K_2 = K_2(D)$. The Lemma 32. gives us a subset $T \subseteq G$ (denoted by Y in that lemma) with $\dim(T) > 0$, $\delta(T) \leq K_2$

$$\mu(\alpha^{2N-1}, T) \geq \mu\big(\textstyle\prod^N \alpha, S\big) - \log_q K_2 \geq$$

$$\geq \left(1 + \dfrac{1-\kappa}{4N\dim(G)}\right) \cdot \mu(\alpha, Y) + \left[\dfrac{1-\kappa}{4N\dim(G)} \log_q K_1 - \log_q K_2\right] \ .$$

We collected the two error terms in the square bracket, we wish to make it positive (which allows to omit it). If we choose sufficiently large K_1 then the positive term will overcome the other one, hence (13) holds with any

$$\lambda \leq \left(1 + \dfrac{1-\kappa}{4N\dim(G)}\right) \ .$$

□

Theorem 34. *For all values $d > 0$, $n > 0$ and $0 < \kappa < 1$ there are bounds $M = M(n, \kappa)$ and $K_3 = K_3(n, d, \kappa) > 0$ with the following property. Let G be a linear algebraic group over $\mathbb{F}_r$ with $\dim(G) \leq n$ and $\Delta(G) \leq d$. Suppose that $G(\mathbb{F}_q)$ does not normalise any closed subgroup $H < G$ with $0 < \dim(H) < \dim(G)$ and the centraliser of $G(\mathbb{F}_q)$ in G is finite. If $1 \in \alpha \subseteq G(\mathbb{F}_q)$ is a generating set and $X \subset G$ is an infinite constructible subset defined over $\mathbb{F}_r$ such that*

$$\delta(X) \leq d \quad \textit{and} \quad \mu(\alpha, X) > \log_q K_3$$

then

$$\mu\big(\alpha^M, G\big) \geq \kappa \cdot \mu(\alpha, X) \ .$$

Note, that the conditions imply that $X \cap \alpha \subseteq G(\mathbb{F}_q)$ is large, hence q must also be large.

Proof of Theorem 34. With an induction on $i \geq 0$ we shall define integers M_i, real numbers $d_i > 0$ and constructible subsets $T_i \subseteq G$ such that such that $\dim(T_i) > 0$,

$$\delta(T_i) \leq d_i \qquad \text{and} \qquad \mu\big(\alpha^{M_i}, T_i\big) \geq \lambda^i \cdot \mu(\alpha, X) \tag{14}$$

for some fixed $\lambda > 1$. Let I be the smallest integer such that $\lambda^I > \dim(G)$, and let $M = M_I$. We shall run the induction for at most I steps. We start with $M_0 = 1$, $d_0 = d$ and $T_0 = X$. In the i-th step, for $i \leq I$, we shall use Lemma 33. with the values $d = d_{i-1}$, $N = 2^n$ and

our κ. We always get the same $\lambda = \lambda(N, \kappa) > 1$, this is the λ we use in (14). We define $d_i = K_1(d_{i-1}, \kappa)$, $M_i = (2N-1)M_{i-1} = (2N-1)^i$. We apply this Lemma 33. to the generating set $\alpha^{M_{i-1}}$ and to the constructible set $Y = T_{i-1}$, we get a new constructible set T. On the one hand, if this T satisfies (12) then we stop the induction. Now $i \leq I$, so $M \geq M_i$ and

$$\mu\big(\alpha^M, G\big) \geq \mu\big(\alpha^{M_i}, T\big) \geq \kappa \cdot \mu\big(\alpha^{M_{i-1}}, T_{i-1}\big) \geq$$
$$\geq \kappa\lambda^{i-1} \cdot \mu(\alpha, X) \geq \kappa \cdot \mu(\alpha, X) \; .$$

This proves the Theorem in this case. On the other hand, if T satisfies (13), then we define $T_{i+1} = T$, which satisfies (14). If $i < I$ then we go on with the induction, if $i = I$ the we stop, and use (14) for $i = I$ to prove the theorem:

$$\mu\big(\alpha^M, G\big) \geq \frac{\dim(T_I)}{\dim(G)} \cdot \mu\big(\alpha^M, T_I\big) \geq$$
$$\geq \frac{1}{\dim(G)} \cdot \lambda^I \cdot \mu\big(\alpha, X\big) \geq \mu\big(\alpha, X\big) \; .$$

□

We can reformulate Theorem 34. using the number of generators instead of the concentrations:

Corollary 35. *For all values $d > 0$, $n > 0$ and $0 < \kappa < 1$ the bounds $K_3 = K_3(n, d, \kappa)$ and $M = M(n, \kappa)$ of Theorem 34. has the following property. Let G be a linear algebraic group over $\mathbb{F}_r$ with $\dim(G) \leq n$ and $\Delta(G) \leq d$. Suppose that $G(\mathbb{F}_q)$ does not normalise any closed subgroup $H < G$ with $0 < \dim(H) < \dim(G)$ and the centraliser of $G(\mathbb{F}_q)$ in G is finite. If $1 \in \alpha \subseteq G(\mathbb{F}_q)$ is a generating set and $X \subset G$ is an infinite constructible subset defined over $\mathbb{F}_r$ such that*

$$\delta(X) \leq d \quad \textit{and} \quad \big|\alpha \cap X\big| > K_3^{\dim(X)}$$

then

$$\big|\alpha^M\big| \geq \big|\alpha \cap X\big|^{\kappa \cdot \dim(G)/\dim(X)} \; .$$

□