Sum-product estimates over finite fields and growth in $\mathbf{SL}_2(\mathbb{F}_q)$

a semester project by Filippo Candia

under the supervision of

Prof. Philippe Michel and Dr. Ramon Moreira Nunes

EPFL , January 2019

Contents

Chapter 1

Introduction

1.1 Growth

In the English language the word *growth* may be defined as *the process of increasing size*. Mathematically a *process* is essentially a function and, in terms of sets, one may formalize the concept of growth as follows.
Let X be a set, let $f : X \to X$ be a function. A finite set $S \subset X$ *grows* under f if

$$|S| < |f(S) \cup S|,$$

where the absolute value stands for the cardinal of S. In many different areas of mathematics, growth is a highly studied phenomenon. If G is a finite group and S a set of generators, one question that may arise is: *how many elements of* S (counting multiplicity) *do we need, if we want to write all elements of* G *as product of elements in* S? Or, in more technical language, what is the diameter of G with respect to S?
A more sophisticated question would be, given a family of groups $\{G_\alpha\}_{\alpha \in \mathscr{A}}$, how can we bound the diameter of G_α with respect to *any* set of generators, just in term of $|G_\alpha|$? At the end of this document we will be able to answer this question for the family $\left\{\mathrm{SL}_2(\mathbb{F}_p)\right\}_{p \text{ prime}}$.

1.2 Sum-Product and Helfgott's theorems

Beside what we said above, this document is mainly about the proofs of two theorems: the *sum-product estimate* over finite fields and *Helfgott's theorem* (both stated below). Let $q = p^\eta$ be a prime power and let $\mathbb{F}_q$ be the finite field with q elements. For a set $S \subseteq \mathbb{F}_q$ we denote by $2S$ the sum set

$$2S := \{s_1 + s_2 : s_1, s_2 \in S\},$$

and, similarly, we denote by S^2 the product set

$$S^2 := \{s_1 \cdot s_2 : s_1, s_2 \in S\}.$$

The above notation naturally adapts to the case where S lives in an additive or multiplicative group.

Theorem 1.1 (Sum-product theorem over finite fields, [BKT04]). Suppose that $S \subset \mathbb{F}_q$ is a subset such that

$$q^\delta < |S| < q^{1-\delta},$$

for some $\delta > 0$. Then one has a bound of the form

$$\max\{|S^2|, |2S|\} \geqslant c|S|^{1+\varepsilon},$$

where $c > 0$ and $\varepsilon > 0$, depend only on δ.

Theorem 1.2 (Helfgott's theorem, [Hel08]). Let S be a generating subset of $\mathrm{SL}_2(\mathbb{F}_q)$. Then we have that either

$$|S^3| \gg |S|^{1+\delta}$$

holds, either

$$(S \cup S^{-1} \cup \{e\})^k = \mathrm{SL}_2(\mathbb{F}_q)$$

holds, for some absolute constants $\delta > 0$ and $k \geqslant 0$.

Theorem 1.1 above is the first result of its kind, in the sense that nowadays sharper statements are known. In fact, rather than proving the above, we are going to prove two different and stronger versions of the sum-product. One somewhat combinatorial and one using exponential sums (the latter will follow the arguments in [HIS07a]).
The proof of Helfgott's theorem will follow the arguments in [Hel15] (which are essentailly the arguments in [Hel11]).

1.3 Overview of the document

Chapter 2

In the second chapter we establish a first sum-product estimate. This will be done using methods coming from Fourier theory and as well as Weil's bound for Kloosterman sums. Some parts of this chapter will have a somewhat geometrical flavour, since the explicit connection between exponential sums and the sum-product estimates arise from some family of hyperbolas in $\mathbb{F}_q^n$.

Chapter 3

In opposition with Chapter 2, Chapter 3 has mainly a combinatorial flavour. Here we will introduce a standard tool used in additive combinatorics, Rusza's inequality, and we generalize of the classical orbit-stabilizer theorem. We also state two important results in additive combinatorics, Katz-Tao Lemma and the Rusza-Plünnecke inequality, and we will use them to obtain another sum-product estimate.

Chapter 4

In chapter 4 we will give some definitions around the notion of growth. In particular we will define expander graphs and Cayley graphs and we will see how they relate to growth properties. We will also prove a useful result towards the proof of Theorem 1.2.

Chapter 5

In chapter 5 we discuss two techniques to study the growth in linear algebraic groups: the escape principle and the dimensional estimates. Since $\mathrm{SL}_2(\mathbb{F}_q)$ is an algebraic group we will be able to apply these techniques to prove Helfgott's theorem.

Chapter 6

In this short final chapter we will prove Helfgott's Theorem using the results obtained in Chapter 4 and 5. We will also be able to deduce from Helfgott's a bound for the diameter of the family $\{\mathrm{SL}_2(\mathbb{F}_p)\}_{p \text{ prime}}$.

1.4 Notation

Sets

Let $n \in \mathbb{N}$ and S be a subset of some ring, field or group. We will write nS for the set

$$nS := \underbrace{S + \ldots + S}_{n\text{-times}} = \{s_1 + \ldots + s_n : s_i \in S\},$$

and S^n for the set

$$S^n := \underbrace{S \cdot \ldots \cdot S}_{n\text{-times}} = \{s_1 \cdots s_n : s_i \in S\}.$$

To avoid confusion we will denote the Cartesian product, of n copies of a set S, by $S^{\times n}$. For T another subset (living in the same structure of S), we should also write ST for the set

$$ST := \{s \cdot t : s \in S,\ t \in T\}.$$

The absolute value $|S|$ of a finite set S will denote its cardinal and we may refer to it as the *size* of S.
Given a set S, it is standard to denote by $\mathscr{P}(S)$ the set of parts of S, that is, *the set of subsets* of S. We should do the same if needed.

Spaces of functions

The gothic letter $\mathfrak{F}$, will be used to denote spaces of functions. For instance for a finite set S and a field κ, we will denote by $\mathfrak{F}(S,\kappa)$ the κ- vector space over the set of functions of the form $f : S \to \kappa$.

Groups

Given a group G we should denote by e the neutral element.
By character of a group $(G,\cdot)$ we mean a group homomorphism $\chi : (G,\cdot) \to (\mathbb{C}^\times,\cdot)$ and we say that χ is a non-trivial character if $\chi \not\equiv 1$ (that is χ is not the constant map that sends every element of G to $1 \in \mathbb{C}$).
Given a set X and a group G, an *action of G on X* is a map

$$\begin{aligned} \mathcal{O} : G \times X &\longrightarrow X \\ (g,x) &\longmapsto \mathcal{O}_g(x) \end{aligned}$$

such that:

(i) $\mathcal{O}_g(O_h(x)) = \mathcal{O}_{gh}(x)$ for all $g,h \in G$ and for all $x \in X$;

(ii) $\mathcal{O}_e(x) = x$ for all $x \in X$.

It is usual to denote an action of G on X by $G \curvearrowright X$ and to write gx instead of $\mathcal{O}_g(x)$ and we should do so (there will be no need to talk about right or left action). For an element $x \in X$ we denote equivalently by G_x or $\mathrm{Stab}_G(x)$, the *stabilizer* of x, that is the set

$$G_x \coloneqq \{g \in G : gx = x\}.$$

The *orbit* $\mathcal{O}_G(x)$ of an element $x \in X$ is the set

$$\mathcal{O}_G(x) \coloneqq \{gx : g \in G\},$$

For any subset S of G we write $\mathcal{O}_S(x)$ for the S-orbit of x, that we define to be the set

$$\mathcal{O}_S(x) = \{sx : s \in S\}.$$

A group G acts on itself by conjugation. This means that

$$\begin{aligned} G \times G &\longrightarrow G \\ (g,h) &\longmapsto ghg^{-1} \end{aligned}$$

is a group action. In this case, for $h \in G$, we denote $\mathrm{Z}(h)$ the stabilizer of h and we refer to it as the *centralizer* of g. We also write $\mathrm{Cl}(h)$ for the orbit of h and we refer to it as the conjugacy class of h.

Asymptotic notations

Let $f : X \to \mathbb{C}$ and $g : X \to \mathbb{R}$ be two functions. We write $f = O(g)$, or equivalently $f \ll g$, if there exists a constant $C \geqslant 0$ such that

$$|f(x)| = C \cdot g(x) \text{ for all } x \in X.$$

If the constant C depends on some value δ, we may write $f = O_\delta(g)$ or $f \ll_\delta g$, and sometimes we will refer to C as the *implied constant* of $f \ll g$.

Matrices

Let κ be a field. We will write $\mathrm{GL}_2(\kappa)$ for the general linear group over κ, that is the group of matrices

$$\mathrm{GL}_2(\kappa) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \kappa^{\times 4} : ad - bc \neq 0 \right\},$$

and we will write $\mathrm{SL}_2(\kappa)$ for the special linear group over κ, that is the group of matrices

$$\mathrm{GL}_2(\kappa) \coloneqq \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \kappa^{\times 4} : ad - bc = 1 \right\}.$$

Sometimes we will wirte $f = O(g)$ even if $f(x) \leqslant C \cdot g(x)$ holds only for $x \to \infty$.

Affine Algebraic Geometry

The set $\mathrm{SL}_2(\mathbb{C})$ has a natural structure of complex manifold. It is an hyper-surface in $\mathbb{C}^{\times 4}$ and one can perform differential geometry over it. To be able to study $\mathrm{SL}_2(\mathbb{F}_q)$ as a manifold, we need few constructions coming from algebraic geometry. Here, we briefly explain the vocabulary we will use, but we avoid the precise definitions.
Let κ be an algebraically closed field.

- An (affine) algebraic set $\mathscr{X}$ is a subset of $\mathbb{A}^n(\kappa) \coloneqq \kappa^{\times n}$, such that its points correspond to the vanishing set of an ideal of the polynomial ring $R \coloneqq \kappa[X_1, \ldots, X_n]$.

- Let $\mathbb{F}_q^{\mathrm{alg}}$ be the algebraic closure of $\mathbb{F}_q$. Clearly $\mathrm{SL}_2(\mathbb{F}_q^{\mathrm{alg}})$ is an algebraic set.

- An algebraic set $\mathscr{X}$ can be decomposed in a finite unions of smaller algebraic sets, called the irreducible components of $\mathscr{X}$.

- Irreducible algebraic sets are called varieties and they correspond to the vanishing sets of prime ideals. Since the polynomial

$$X_1X_4 - X_2X_3 - 1 \in \mathbb{F}_q[X_1, \ldots, X_n]$$

  is prime, $\mathrm{SL}_2(\mathbb{F}_q^{\mathrm{alg}})$ is an algebraic set.

- To talk concretely, we may avoid the exact definition of *dimension* of an algebraic set. Anyway, we should remark that, more or less intuitively, $\mathrm{SL}_2(\mathbb{F}_q^{\mathrm{alg}})$ has dimension 3 in $(\mathbb{F}_q^{\mathrm{alg}})^{\times 4}$, while the algebraic set

$$\mathscr{X} = \left\{ x \in \mathrm{SL}_2(\mathbb{F}_q^{\mathrm{alg}}) : \mathrm{Trace}(x) = c \right\},$$

  defined for some $c \in \mathbb{F}_q^{\mathrm{alg}}$, has dimension 2 in $(\mathbb{F}_q^{\mathrm{alg}})^{\times 4}$.

- A *regular map* between algebraic sets is essentially a generalization of a smooth map between manifolds.

- Regular maps between affine algebraic sets are a generalization of differentiable maps between manifolds and they are not far from being almost injective. Given a regular map

$$\phi : \mathscr{X} \to \mathscr{Y}$$

  between two algebraic sets, we denote by $\mathscr{X}_{\mathrm{sing}}^{\phi}$ to be the set of points P in $\mathscr{X}$ for which $D_P\phi$ is degenerate (that is the, the differential map $D_P\phi : T_P(\mathscr{X}) \to T_{\phi(P)}(\mathscr{Y})$ is not injective).

- If a matrix group G can be described as an algebraic set we may say that G is a linear algebraic group (although the standard definition of linear algebraic group is far more general).

- Much as in differential geometry we can define tangent planes on algebraic sets and we can differentiate regular maps. For a regular map $\phi : \mathscr{X} \to \mathscr{Y}$ between algebraic sets, we are going to write $D_P\phi : T_P(\mathscr{X}) \to T_{\phi(P)}(\mathscr{Y})$ for the linear map between the tangent planes at $P \in \mathscr{X}$ and $\phi(P) \in \mathscr{Y}$.

- In a linear algebraic group G, a *torus* T is a (linear algebraic) subgroup that is isomorphic to $\kappa^{\times r}$ for some $r \in \mathbb{N}$. If r is maximal we say that T is a *maximal torus* in G.

- A *regular semi-simple* element in the matrix group $\mathrm{GL}_2(\kappa)$ is a diagonalizable element with distinct eigenvalues.

Chapter 2

Sum-Product Theorem over finite fields

2.1 A tiny bit of history

In the 1983 Erdős and Szemerédi proved that there are absolute constants $c > 0$ and $\varepsilon > 0$ such that if $S \subset \mathbb{R}$ is a finite set, then

$$\max\{|2S|, |S^2|\} \geqslant c|S|^{1+\varepsilon},$$

where $2S$ is the *sum set*

$$S + S = \{s_1 + s_2 : s_1, s_2 \in S\},$$

and S^2 is the *product set*

$$S \cdot S = \{s_1 \cdot s_2 : s_1, s_2 \in S\}.$$

Beside proving the above, Erdős and Szemerédi also conjectured that ε can be taken arbitrary closed to 1. Today the problem is still open but lately good lower bounds for ε have been found. A first big result around this conjegture is due to Solymosi that showed in [Sol09] that ε has a lower bound of at least $1/3$. Very recently S. George ameliorated the bound proving that ε is bigger than $1/3 + 5/5277$ ([Sha18]).
Over finite fields the first big result on sum-product estimates is Theorem 1.1, already statetd in the introduction of this document.

Theorem 1.1 (Sum-product theorem over finite fields, [BKT04]). Suppose that $S \subset \mathbb{F}_q$ is a subset such that

$$q^{\delta} < |S| < q^{1-\delta},$$

for some $\delta > 0$. Then one has a bound of the form

$$\max\{|S^2|, |2S|\} \geqslant c|S|^{1+\varepsilon},$$

where $c > 0$ and $\varepsilon > 0$, depend only on δ.

After the publication of [BKT04], no estimates or possible relations between ε and δ were known. Some results in this direction can be found in [HIS07b], in which Hart, Iosevich and Solymosi combined the theory of exponential sums and some basic geometry of finite fields to obtain next theorem.

Theorem 2.1 (Sum-product theorem over finite fields 2, [HIS07b]). Let q be an odd prime power. Let S be a subset of $\mathbb{F}_q$ such that $q^{1/2} \ll |S| \ll q^{7/10}$. Then one has

$$\max(|S^2|, |2S|) \gg \frac{|S|^{3/2}}{q^{1/4}}.$$

We should remark the the lower bound $|S| \gg q^{1/2}$ is there to avoid a trivial statement.
In this chapter, following the arguments in [HIS07b], we give a proof of Theorem 2.1.

2.2 Discrete Fourier Transforms

We start by recalling basic equalities from the theory of discrete Fourier transforms. Let $\psi : (\mathbb{F}_q, +) \to (\mathbb{C}^\times, \times)$ be a non-trivial character of $(\mathbb{F}_q, +)$. We define the Fourier operator

$$\begin{aligned} \widehat{\cdot} : \mathfrak{F}(\mathbb{F}_q^n, \mathbb{C}) &\longrightarrow \mathfrak{F}(\mathbb{F}_q^n, \mathbb{C}) \\ f &\longmapsto \widehat{f}, \end{aligned}$$

which assigns to each f the function $\widehat{f}$

$$\widehat{f}(y) \coloneqq \frac{1}{q^n} \sum_{x \in \mathbb{F}_q} \psi(-y * x) f(x),$$

where $x * y$ denotes the standard scalar product in $\mathbb{F}_q^n$, that is

$$x * y \coloneqq \sum_{i=1}^{n} x_i y_i \in \mathbb{F}_q.$$

We have the following properties.

Lemma 2.2.1 (Inversion). For all $x \in \mathbb{F}_q^n$ and for all maps $f \in \mathfrak{F}(\mathbb{F}_q^n, \mathbb{C})$, we have

$$f(y) = \sum_{x \in \mathbb{F}_q^n} \psi(x * y) \widehat{f}(x).$$

Proof. We have,

$$\sum_{x \in \mathbb{F}_q^n} \psi(x * y) = \sum_{x_1} \cdots \sum_{x_n} \prod_{i=1}^{n} \psi(x_i y_i) = \begin{cases} 0 & \text{if } y \neq 0; \\ q^n & \text{if } y = 0. \end{cases}$$

Thus,

$$\frac{1}{q^n} \sum_{x \in \mathbb{F}_q^n} \sum_{z \in \mathbb{F}_q^n} \psi(x * y) \psi(-z * x) f(z) = f(y).$$

□

Lemma 2.2.2 (Parseval).

$$\sum_{x \in \mathbb{F}_q^n} \left| \widehat{f}(x) \right|^2 = \frac{1}{q^n} \sum_{x \in \mathbb{F}_q^n} |f(x)|^2 .$$

Proof. By simple computation one verifies that,

$$\begin{aligned} \sum_{x \in \mathbb{F}_q^n} |\widehat{f}(x)|^2 &= \sum_{x \in \mathbb{F}_q^n} \widehat{f}(x) \overline{\widehat{f}(x)} \\ &= \sum_{x \in \mathbb{F}_q^n} \frac{1}{q^{2n}} \sum_{y_1, y_2 \in \mathbb{F}_q^n} f(y_1) \overline{f(y_2)} \psi(x * (y_1 - y_2)) \\ &= \frac{1}{q^n} \sum_{y \in \mathbb{F}_q^n} f(y) \overline{f(y)} = \frac{1}{q^n} \sum_{y \in \mathbb{F}_q^n} |f(y)|^2. \end{aligned}$$

□

Since we are approaching a counting problem we are interested in characteristic functions. Let S be a subset of $\mathbb{F}_q^n$ and s be its characteristic function. We remark that

$$\begin{aligned} \widehat{s}(y) &= \frac{1}{q^n} \sum_{x \in \mathbb{F}_q^n} \psi(-y * x) s(x), \\ &= \frac{1}{q^n} \sum_{x \in S} \psi(-y * x), \end{aligned}$$

so that $\widehat{s}(0) = |S|/q^n$. In particular for all y in $\mathbb{F}_q^n$

$$|\widehat{s}(y)| \leqslant \frac{|S|}{q^n}$$

We also remark that for any $\gamma : \mathbb{F}_q^n \to \mathbb{F}_q$, if $S = \left\{x \in \mathbb{F}_q^n : \gamma(x) = 0\right\}$, we have

$$|S| = \sum_{x\in S} 1 = \sum_{x\in\mathbb{F}_q^n} \frac{1}{q} \sum_{t\in\mathbb{F}_q} \psi(t\gamma(x)).$$

2.3 Hyperbolas in $\mathbb{F}_q^n$

In this section we see how to count points on hyperbolas in $\mathbb{F}_q^n$. We begin with some definitions/notations. Let $c \in \mathbb{F}_q^\times$. The *c-hyperbola* (of dimension n) will be the set

$$H_c := \left\{ x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n : \prod_{i=1}^n x_i = c \right\}.$$

For any map $\phi : X \to \mathbb{F}_q^n$ and any subset $Y \subseteq X$, we define the *pre-(c-)hyperbola* (of dimension n) $H_c^\phi(Y)$, to be the set

$$H_c^\phi(Y) := \{y \in Y : \phi(y) \in H_c\}.$$

If $\phi = \mathrm{id}$ and $S \subset \mathbb{F}_q^n$, we simply write $H_c(S)$, while if $S, S' \subset \mathbb{F}_q^n$, we will denote by $H_c^\pm(S \times S')$ the set

$$\left\{(s, s') \in S_1 \times S_2 : (s \pm s') \in H_c\right\}.$$

Clearly if $S \subset S'$ one has $|H_c(S)| \leqslant |H_c(S')|$. As a consequence one sees that

$$|H_c| = q^{n-1} + O(q^{n-2}). \tag{2.1}$$

We present an unnecessarily long proof of (2.1) in the paragraph below, which is fun, but somehow really unnecessary.

Lines and roots

Let P be a polynomial in $\mathbb{F}_q[X_1, \ldots, X_n]$ and write $\tilde{x}$ for the image of $x = (x_1, \ldots, x_n)$ under the map $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{n-1})$.
If we suppose that for all $\tilde{x} \in \mathbb{F}_q^{n-1}$,

$$P(\tilde{x}, \cdot) : z \longmapsto P(x_1, \ldots, x_{n-1}, z)$$

defines a bijection or a zero map, then

$$\sum_{z\in\mathbb{F}_q} \psi(P(x_1, \ldots, x_{n-1}, z)) = \begin{cases} q \text{ if } (x_1, \ldots, x_{n-1}, \mathbb{F}_q) \subset \mathrm{roots}(P); \\ 0 \text{ otherwise}, \end{cases}$$

where ψ is again a non-trivial character of $(\mathbb{F}_q, +)$. It is not hard to see that next statement holds.

Proposition. Let $P \in \mathbb{F}_q[X_1, \ldots, X_n]$ be such that $P(\tilde{x}, \cdot)$ is either a bijection, either the zero map. For $\tilde{x} \in \mathbb{F}_q^{n-1}$, let also $l_{\tilde{x}} = \{\tilde{x}\} \times \mathbb{F}_q$. Then

$$\sum_{x_1} \cdots \sum_{x_n} \psi(P(x_1, \ldots, x_n)) = \sum_{l_{\tilde{x}} \subset \mathrm{roots}(P)} q.$$

Example 1. Consider $P(x, y) = xy$. We have that $l_0 \in \mathrm{roots}(P)$ and $l_x \notin \mathrm{roots}(P)$ for all $x \neq 0$. Thus $\sum_{(x,y)\in\mathbb{F}_q^2} \psi(xy) = q$

Example 2. Consider $P(x) = \prod_{i=1}^n x_i$. We have that $l_{\tilde{x}} \in \mathrm{roots}(P)$ if and only if $\tilde{x}_i = 0$ for at least one i. It is not hard to see that in this situation:

$$\sum_{x\in\mathbb{F}_q^n} \psi(P(x)) = q^n - q(q-1)^{n-1}. \tag{2.2}$$

Indeed one can simply count the lines in the set of roots. Let

$$E = \left\{ \tilde{x} \in \mathbb{F}_q^{n-1} : \tilde{x} \text{ has exactly } k \text{ entries equal to } 0 \right\},$$

then $|\{l_{\tilde{x}} : \tilde{x} \in E\}| = \binom{n-1}{k}(q-1)^{n-1-k}$ and

$$\sum_{k=1}^{n-1} \binom{n-1}{k}(q-1)^{n-1-k} = q^{n-1} - (q-1)^{n-1}.$$

Form (2.2) we easily deduce (2.1):

$$\begin{aligned} |H_c| &= q^{-1} \sum_{t\in\mathbb{F}_q} \sum_{x\in\mathbb{F}_q^n} \psi(t(P(x)-c)) \\ &= q^{n-1} + q^{-1} \sum_{t\in\mathbb{F}_q^\times} \psi(-tc) \sum_{x\in\mathbb{F}_q^n} \psi(tP(x)) \\ &= q^{n-1} + q^{-1}(q^{n-1} - (q-1)^{n-1}) \sum_{t\in\mathbb{F}_q^\times} \psi(-tc) \\ &= q^{n-1} + O(q^{n-2}). \end{aligned}$$

2.4 Kloosterman sums

We say that $S \subset \mathbb{F}_q^n$ is a *box* whenever S is equal to $S_1 \times \cdots \times S_n$ for a collection of subsets $\{S_i\}_{i=1}^n$ of $\mathbb{F}_q$. The key statement we use to prove Theorem 2.1 is the following theorem. We will need it only in the case $\mathbb{F}_q^n = \mathbb{F}_q^2$, but since it holds for all $n \geqslant 1$, we state it and prove it in its full generality.

Theorem 2.2. For all boxes $A, B \subset \mathbb{F}_q^n$,

$$|H_c^-(A\times B)| = O\left(|A|\cdot|B|\cdot q^{-1} + q^{(n-1)/2}\cdot(|A|\cdot|B|)^{1/2}\right). \tag{2.3}$$

We recall that $H_c^-(A\times B)$ was defined to be the set $\{(a,b)\in A\times B : a-b\in H_c\}$.

We prove Theorem 2.2 for the case $n=2$ in the next section, while, in this one, we spend few lines talking about exponential sums. Let us begin by saying that the proof of Theorem 2.2 relies on the following bound, that is a particular case of a more general statement proved by Deligne.

Theorem 2.3 (Deligne bound for hyper-Kloosterman sums, [Del74]). For all centred hyperbolas H_c of dimension $n \geqslant 1$ and for all $t \in (\mathbb{F}_q^\times)^n$, we have

$$\left| \sum_{x\in H_c^n} \psi(t*x) \right| \ll q^{(n-1)/2}. \tag{2.4}$$

The sum on the left-hand-side of (2.4), is a multi-dimensional version of the sum

$$\mathrm{K}_2(a,q) := \sum_{x\in\mathbb{F}_q^\times} e_q\left(x + \frac{a}{x}\right), \tag{2.5}$$

(where $e_q(z) := \exp(2\pi i z/q)$ is a character of $(\mathbb{F}_q,+)$ and where $a\in\mathbb{F}_q^\times$), known as *Kloosterman sum*. Kloosterman sums were intruduced by the homonym in [K$^+$26]. The bound

$$|\mathrm{Kl}_2(a,q)| \geqslant 2q^{(n-1)/2},$$

which coincide with Theorem 2.3 for the case $n=2$, was already known before [Del74], and is due to Weil (see [Wei48]). Before Weil, a weaker bound was known: Kloosterman himself proved that

$$|\mathrm{Kl}_2(a,q)| \leqslant 2q^{2/3}.$$

The latter can be proved avoiding abstract and sophisticated tools (tools that are un-avoidable, so to say, in the proof of 2.4) and therefore we have decided to prove it in here before moving on to next section.

Theorem 2.4 (Kloosterman). Let q be a prime. We have that

$$\mathrm{Kl}_2(a,q) \leqslant 2q^{3/4}. \tag{2.6}$$

We remark that $\mathrm{Kl}_2(a,q)$ is a real number (it is equal to its conjugate).

Proof. We are going to explicitly compute

$$M_4(q) := \sum_{a\in\mathbb{F}_q^\times} |\mathrm{Kl}_2(a,q)|^4.$$

The result will follow from the trivial inequality $\mathrm{Kl}_2(a,q) \leqslant M_4(q)^{1/4}$. Notice that for all $b \in \mathbb{F}_q^\times$,

$$\sum_{a\in\mathbb{F}_q^\times} \mathrm{Kl}_2(ab,q) = \sum_{a\in\mathbb{F}_q^\times} \mathrm{Kl}_2(a,q).$$

We have

$$\begin{aligned}
M_4(q) &= \frac{1}{q-1}\sum_{a,b\in\mathbb{F}_q^\times} \mathrm{Kl}_2(ab,q)^4 \\
&= \frac{1}{q-1}\sum_{a,b}\left(\sum_{x\in\mathbb{F}_q^\times} e_q\left(x+\frac{ab}{x}\right)\right)^4 \\
&= \frac{1}{q-1}\sum_{a,b}\left(\sum_{x_{1,2,3,4}\in\mathbb{F}_q^\times} e_q\left(x_1+x_2-x_3-x_4+\frac{ab}{x_1}+\frac{ab}{x_2}-\frac{ab}{x_3}-\frac{ab}{x_4}\right)\right) \\
&= \frac{1}{q-1}\sum_{\substack{x_i\in\mathbb{F}_q^\times\\ 1\leq i\leq 4}}\sum_{a,b\in\mathbb{F}_q^\times} e_q\left(x_1+x_2-x_3-x_4+\frac{ab}{x_1}+\frac{ab}{x_2}-\frac{ab}{x_3}-\frac{ab}{x_4}\right).
\end{aligned}$$

With the change of variable $x_i \leftrightarrow ax_i$ we can replace the main addendum:

$$\begin{aligned}
&\frac{1}{q-1}\sum_{\substack{x_i\in\mathbb{F}_q^\times\\ 1\leq i\leq 4}}\sum_{a,b\in\mathbb{F}_q^\times} e_q\left(a(x_1+x_2-x_3-x_4)+b\left(\frac{1}{x_1}+\frac{1}{x_2}-\frac{1}{x_3}-\frac{1}{x_4}\right)\right) \\
&\quad= \frac{1}{q-1}\sum_{\substack{x_i\in\mathbb{F}_q^\times\\ 1\leq i\leq 4}}\sum_{a,b\in\mathbb{F}_q^\times} e_q\big(a(x_1+x_2-x_3-x_4)\big)\cdot e_q\left(b\left(\frac{1}{x_1}+\frac{1}{x_2}-\frac{1}{x_3}-\frac{1}{x_4}\right)\right) \\
&\quad= \frac{1}{q-1}\sum_{\substack{x_i\in\mathbb{F}_q^\times\\ 1\leq i\leq 4}}\left[\sum_{a\in\mathbb{F}_q^\times} e_q\big(a(x_1+x_2-x_3-x_4)\big)\cdot\sum_{b\in\mathbb{F}_q^\times} e_q\left(b\left(\frac{1}{x_1}+\frac{1}{x_2}-\frac{1}{x_3}-\frac{1}{x_4}\right)\right)\right].
\end{aligned}$$

To simplify the notation let $\alpha = x_1+x_2-x_3-x_4$ and $\beta = \frac{1}{x_1}+\frac{1}{x_2}-\frac{1}{x_3}-\frac{1}{x_4}$. Since (for $y\in\mathbb{F}_q^\times$)

$$1+\sum_{a\in\mathbb{F}_q^\times} e_q(ay) = \sum_{a\in\mathbb{F}_q} e_q(ay) = q\cdot\delta_{y=0}$$

We can then express $M_4(q)$ as

$$M_4(q) = \frac{1}{q-1}\sum_{\dots}(q\cdot\delta_{X=0}-1)(q\cdot\delta_{\frac{1}{X}=0}-1),$$

or more explicitly

$$M_4(q) = \frac{1}{q-1}\left[q^2\sum_{\substack{\alpha=0\\ \beta=0}} 1 + \sum_{\substack{x_i\in\mathbb{F}_q^\times\\ 1\leq i\leq 4}} 1 - q\sum_{\substack{x_i\in\mathbb{F}_q^\times\\ 1\leq i\leq 4}}\delta_\star - q\sum_{\substack{x_i\in\mathbb{F}_q^\times\\ 1\leq i\leq 4}}\delta_{\frac{1}{\star}}\right].$$

The second sum gives $(q-1)^4$, the third and the fourth are equal and to understand them one just have to understand the size of the set

$$T = \left\{ (x_1, x_2, x_3, x_4) \in \bigoplus^4 \mathbb{F}_q^\times : \sum_i x_i = 0 \right\},$$

which is simply $|T| = (q-1)^3$. The only thing left is to understand the first sum

$$\sum_{\substack{\alpha=0 \\ \beta=0}} 1 = \# \left\{ \vec{x} \in \bigoplus^4 \mathbb{F}_q^\times : (x_1 + x_2) - (x_3 + x_4) = \left(\frac{1}{x_1} + \frac{1}{x_2}\right) - \left(\frac{1}{x_3} + \frac{1}{x_4}\right) = 0 \right\}.$$

If $u = (x_1 + x_2) = (x_3 + x_4)$ and $v = \left(\frac{1}{x_1} + \frac{1}{x_2}\right) = \left(\frac{1}{x_3} + \frac{1}{x_4}\right)$ and if we define

$$N(u, v) = \# \left\{ (x, y) \in \bigoplus^2 \mathbb{F}_q^\times : \substack{x+y=u \\ 1/x+1/y=v} \right\}$$

The sum becomes just:

$$\sum_{\substack{\alpha=0 \\ \beta=0}} 1 = \sum_{u,v \in \mathbb{F}_q} N(u, v)^2$$

If this is not clear, we can see this just partitioning the set:

$$\begin{aligned}
&\left\{ \vec{x} \in \bigoplus^4 \mathbb{F}_q^\times : (x_1 + x_2) - (x_3 + x_4) = \left(\frac{1}{x_1} + \frac{1}{x_2}\right) - \left(\frac{1}{x_3} + \frac{1}{x_4}\right) = 0 \right\} = \\
&= \bigsqcup_{v \in \mathbb{F}_q} \left\{ \vec{x} \in \bigoplus^4 \mathbb{F}_q^\times : (x_1 + x_2) - (x_3 + x_4) = \left(\frac{1}{x_1} + \frac{1}{x_2}\right) - \left(\frac{1}{x_3} + \frac{1}{x_4}\right) = 0, x_1 + x_2 = v \right\} \\
&= \bigsqcup_{v,u \in \mathbb{F}_q} \left\{ \vec{x} \in \bigoplus^4 \mathbb{F}_q^\times : (x_1 + x_2) - (x_3 + x_4) = \left(\frac{1}{x_1} + \frac{1}{x_2}\right) - \left(\frac{1}{x_3} + \frac{1}{x_4}\right) = 0, \substack{x_1+x_2=u \\ 1/x_1+1/x_2=v} \right\},
\end{aligned}$$

and the size of each one of these parts is precisely $N(u, v)^2$ since we have $N(x, y)$ possibilities for x_1, x_2 and $N(u, v)$ for x_3, x_4.
Hopefully everything until now is clear and we are left to compute

$$\sum_{u,v \in \mathbb{F}_q^\times} N(u, v)^2.$$

To do this we consider two cases.

a. if $v = 0$ the condition becomes $y = -x$ and therefore $N(u, v) = 0$ unless $u = 0$

$$N(u, 0) = \begin{cases} 0 & \text{if } u \neq 0 \\ q-1 & \text{if } u = 0 \end{cases}.$$

b. if $v \neq 0$ each couple (x, y) must satisfy $xy = \frac{x+y}{1/x+1/y} = \frac{u}{v}$. Also each couple (x, y) satisfies $x + y = u$ and therefore x and y have to be roots of

$$P(X) = X^2 - uX + \frac{u}{v} = 0.$$

In this case (χ_2 is the Legandre symbol):

$$\begin{aligned}
N(u, v) &= 1 + \chi_2(u^2 - 4\frac{u}{v}) = \begin{cases} 0 & \text{if } u^2 - 4\frac{u}{v} \text{ is a square mod } q \\ 2 & \text{if } u^2 - 4\frac{u}{v} \text{ is a square mod } q \end{cases} \\
&= 1 + \chi_2\left(1 - \frac{4}{uv}\right) = N(1, uv).
\end{aligned}$$

Finally

$$\sum_{u,v\in\mathbb{F}_q} N(u,v)^2 = \sum_{u,v\in\mathbb{F}_q^\times} N(1,uv)^2 = \sum_{u\in\mathbb{F}_q^\times}\sum_{v\in\mathbb{F}_q^\times} N(1,v)^2$$

$$= (q-1)\sum_{v\in\mathbb{F}_q^\times}\left(1+\chi_2(1-\frac{4}{v})\right)^2 \qquad \left[\omega = 1-\frac{4}{v}\in\mathbb{F}_q\setminus\{1\}\right]$$

$$= (q-1)\sum_{\omega\in\mathbb{F}_q\setminus\{1\}} 1+\chi_2(\omega)^2+2\chi_2(\omega)$$

$$= (q-1)[(q-1)+(q-2)-2] = (q-1)(2q-5).$$

Combining all together we obtain (2.6). □

2.5 Proof of Theorem 2.2 and Theorem 2.1

Proof of Theorem 2.2

We start by computing $|H_c^-(A\times B)|$ using the Fourier inversion: we have

$$|H_c^-(A\times B)| = \sum_{x,y\in\mathbb{F}_q^2} a(x)\cdot b(y)\cdot h(x-y)$$

$$= \sum_{x,y,t\in\mathbb{F}_q^2} a(x)\cdot b(y)\cdot \psi(t(x-y))\cdot \widehat{h}(t)$$

$$= \sum_{t\in\mathbb{F}_q^2} q^4\cdot \widehat{a}(-t)\cdot\widehat{b}(t)\cdot\widehat{h}(t)$$

$$\leqslant q^4\cdot|A|\cdot|B|\cdot|\widehat{h}(0)| + \sum_{t\in\mathbb{F}_q^2\setminus(0,0)} q^4\cdot\widehat{a}(-t)\cdot\widehat{b}(t)\cdot\widehat{h}(t)$$

$$=: \Sigma_1+\Sigma_2$$

Then, by Cauchy-Schwartz

$$\Sigma_2 \leqslant \left(\sum_{t\in\mathbb{F}_q^2}(\widehat{a}(t))^2\right)^{1/2}\cdot\left(\sum_{t\in\mathbb{F}_q^2}(\widehat{b}(t))^2\right)^{1/2}\cdot \sup_{t\neq(0,0)}\left\{|\widehat{h}(t)| : t\in\mathbb{F}_q^2\right\}.$$

and applying Perseval identity and Weil's bound we deduce that

$$\Sigma_2 \ll q^{1/2}\cdot|A|^{1/2}\cdot|B|^{1/2}.$$

Applying (2.1) to Σ_1 we obtain

$$\Sigma_1 \ll |A|\cdot|B|\cdot q^{-1}.$$

We have proved Theorem 2.2 for the case $n=2$.

Proof of Theorem 2.1

On view of using Theorem 2.2, we should build a pre-hyperbola (of dimension 2) containing informations about both $2S$ and S^2. Recover S^2 from an hyperbola is trivial, since the set S^2 and the family $\{H_c(S^{\times 2})\}_{c\in\mathbb{F}_q^\times}$ are essentially the same thing. But how can we find some informations about $2S$ inside an hyperbola? The answer lies in the pre-hyperbolas of the shape

$$H_\star := H_c^-((2S)^{\times 2}\times S^{\times 2})$$

$$= \left\{((x_1,x_2);(y_1,y_2))\in(2S)^{\times 2}\times S^{\times 2} : (x_1-y_1)\cdot(x_2-y_2)=c\right\}.$$

Notice that by Theorem 2.2 these have all cardinal less than or equal to

$$C\left(|2S|^2\cdot|S|^2\cdot q^{-1}+q^{1/2}\cdot(|2S|\cdot|S|)\right)$$

for a positive constant C. Furthermore, since $H_\star$ admits the decomposition below, $H_\star$ contains $|S|^2$ copies of $H_c(S^{\times 2})$:

$$H_\star \simeq \bigsqcup_{(s_1,s_2)\in S^{\times 2}} H_c((S+S)^{\times 2}-(s_1,s_2)) \supset \bigsqcup_{(s_1,s_2)\in S^{\times 2}} H_c(S^{\times 2}),$$

and thus by pigeon-hole we have the lower bound

$$|H_\star| \geqslant \left(\sum_{x \in S^{\times 2}} \frac{|S|^2}{|S^2|} \right) = \frac{|S|^4}{|S^2|}.$$

for at least one value of $c \in \mathbb{F}_p^\times$. Indeed $S^{\times 2} = \bigsqcup_{c \in S^2} H_c(S^{\times 2})$ and by pigeon-hole there is $c \in \mathbb{F}_q^\times$ such that $H_c(S^{\times 2}) \geqslant |S|^2 \cdot |S^2|^{-1})$. We are at the main checkpoint of the proof:

$$\begin{aligned} \frac{|S|^4}{|S^2|} \leqslant |H_\star| &\ll |2S|^2 \cdot |S|^2 \cdot q^{-1} + q^{1/2}|2S| \cdot |S| \\ \Rightarrow \qquad |S|^3 &\ll |2S|^2 \cdot |S^2| \cdot |S| \cdot q^{-1} + q^{1/2} \cdot |2S| \cdot |S^2|. \end{aligned}$$

We now prove the final estimate. Let $M = \max\{|2S|, |S^2|\}$. The inequality

$$|S|^3 \ll |2S|^2 \cdot |S^2| \cdot |S| \cdot q^{-1} + q^{1/2} \cdot |2S| \cdot |S^2|$$

implies either $|S|^3 \ll q^{1/2}M^2$, either $|S|^3 \ll q^{-1}M^3|S|$. In the first case we get $M \gg q^{-1/4}|S|^{3/2}$ without any assumption on $|S|$. In the second case we get

$$M \gg q^{1/3}|S|^{2/3} \gg q^{-1/4}|S|^{3/2},$$

where the second inequality follows from $q^{7/10} \gg |S|$. □

Before moving to next chapter we remark that the use of (2.6) in the proof of Theorem 2.1 would have lead to the weaker bound

$$|S|^3 \leqslant C\left(|2S|^2 \cdot |S^2| \cdot |S| \cdot q^{-1} + q^{3/4} \cdot (|2S| \cdot |S^2|)\right),$$

and thus to the estimate

$$\max\{|2S|, |S^2|\} \gg \frac{|S|^{3/2}}{q^{3/8}},$$

provided that $|S| \ll q^{17/20}$.

Chapter 3

Combinatorial tools

In this chapter we consider finite subsets of groups and fields and we study their growth properties from a combinatorial point of view. In particular we give some inequalities that allow us to manipulate them controlling their size. The letters S, T, X, Y, Z will usually denotes sets.
Notice that if two subsets S and T live in a non-abelian group, the cardinals $|ST|$ and $|TS|$ will not be necessarily equal. We should also remark that there is no reason to believe that $|SS^{-1}|$ and $|S^2|$ coincide.

3.1 Ruzsa inequality

Lemma 3.1.1 (Ruzsa's Triangle Inequality). If X, Y, Z are three finite subsets of a group G, we have

$$|XZ| \cdot |Y| \leqslant |XY| \cdot |Y^{-1}Z|. \tag{3.1}$$

Proof. It is enough to construct a subset of $XY \times Y^{-1}$ of size $|XZ| \cdot |Y|$. The map

$$\begin{aligned} \pi : X \times Z &\longrightarrow XZ \\ (x, z) &\longmapsto xz, \end{aligned}$$

is surjective. Thus there are two subsets $X_0 \subset X$ and $Z_0 \subset Z$ such that $\pi|_{X_0 \times Z_0}$ is bijective. Notice that for all $y_1, y_2 \in Y$ distinct, we have

$$W := (X_0 y_1 \times y_1^{-1} Z_0) \cap (X_0 y_2 \times y_2^{-1} Z_0) = \emptyset.$$

Indeed $(xy_1, y_1^{-1}z) = (\tilde{x}y_1, y_1^{-1}\tilde{z})$ would imply $xz = \tilde{x}\tilde{z}$, which contradicts the assumption $\pi|_{X_0 \times Z_0}$ is bijective. Hence the union

$$\bigcup_{y \in Y} (X_0 y \times y^{-1} Z_0)$$

is actually disjoint and defines a subset of $XY \times Y^{-1}Z$ of size $|X_0||Y_0||Y| = |XZ||Y|$ (recall $\pi|_{X_0 \times Z_0}$ is bijective). □

Inequality (3.1) has to be understood as a triangle inequality for sets. Indeed if we rearrange,

$$|XZ| \leqslant \frac{|XY|}{|Y|^{1/2}} \cdot \frac{|Y^{-1}Z|}{|Y|^{1/2}},$$

divide by $|X|^{1/2}|Z|^{1/2}$,

$$\frac{|XZ|}{|X|^{1/2}|Z|^{1/2}} \leqslant \frac{|XY|}{|Y|^{1/2}|X|^{1/2}} \cdot \frac{|Y^{-1}Z|}{|Y|^{1/2}|Z|^{1/2}}$$

and take the logarithm

$$\log\left(\frac{|XZ|}{|X|^{1/2}|Z|^{1/2}}\right) \leqslant \log\left(\frac{|XY|}{|Y|^{1/2}|X|^{1/2}}\right) + \log\left(\frac{|Y^{-1}Z|}{|Y|^{1/2}|Z|^{1/2}}\right) \tag{3.2}$$

we obtain a triangle inequality for the (almost) distance function

$$\mathrm{d}(S, T) := \log\left(\frac{|ST^{-1}|}{|S|^{1/2}|T|^{1/2}}\right).$$

The function d above is not a distance because the equality $\mathrm{d}(X, Y) = 0$ do not implies $X = Y$, but only that X and Y are both cosets of a subgroup of G ([TV06],Proposition 2.7).
From Lemma 3.1.1 one can deduce the following two inequalities.

Corollary 3.1.1. Let S be a finite subset of a (not necessarily abelian) group G. We have

$$\frac{|\left(S\cup S^{-1}\cup\{e\}\right)^3|}{|S|}\leqslant 14\left(\frac{|S^3|}{|S|}\right)^3. \tag{3.3}$$

Assuming $S=S^{-1}$, one also has

$$\frac{|S^k|}{|S|}\leqslant\left(\frac{|S^3|}{|S|}\right)^{k-2}. \tag{3.4}$$

The inequalities (3.3) and (3.4) are useful (as we will see in some proofs) in many different ways. Essentially, they allow to suppose that $S=S\cup S^{-1}\cup\{e\}$.

Proof.

(3.3): Using Rusza inequality we obtain

$$|SS^{-1}S|\cdot|S|\leqslant|SS^{-2}|\cdot|S^2|,$$
$$|SS^{-2}|\cdot|S|\leqslant|S^2|\cdot|S^3|,$$
$$|S^{-1}S^2|\cdot|S|\leqslant|S^2|\cdot|S^3|,$$

and thus we have

$$|SS^{-1}S|\cdot|S|\leqslant\frac{|S^3|\cdot|S^2|^2}{|S|}\leqslant\frac{|S^3|^3}{|S|},$$

which gives

$$\frac{|SS^{-1}S|}{|S|}\leqslant\left(\frac{|S^3|}{|S|}\right)^3.$$

We have the same bound for $|SS^{-2}|$ and $|S^{-1}S^2|$, since

$$\frac{|S^{-1}S^2|}{|S|},\frac{|SS^{-2}|}{|S|}\leqslant\frac{|S^3||S^2|}{|S|^2}\leqslant\left(\frac{|S^3|}{|S|}\right)^2\left(\frac{|S^3|}{|S|}|\right)^3.$$

Now, from the identities

$$|S^3|=|S^{-3}|,$$
$$|SS^{-1}S|=|S^{-1}SS^{-1}|,$$
$$|S^2S^{-1}|=|SS^{-2}|,$$
$$|S^{-2}S|=|S^{-1}S^2|,$$

we deduce

$$\frac{|(S\cup S^{-1})^3|}{|S|}\ll\left(\frac{|S^3|}{|S|}\right)^3.$$

with implied constants $C=8$. Furthermore

$$\frac{|(S\cup S^{-1})|}{|S|}\leq\frac{|(S\cup S^{-1})^2|}{|S|}\leq\frac{|(S\cup S^{-1})^3|}{|S|}\ll\left(\frac{|S^3|}{|S|}\right)^3.$$

Since

$$(S\cup S^{-1}\cup\{e\})^3=\{e\}\cup(S\cup S^{-1})\cup(S\cup S^{-1})^2\cup(S\cup S^{-1})^3$$

and

$$(S\cup S^{-1})^2=S^2\cup S^{-2}\cup SS^{-1}\cup S^{-1}S$$

we have proved the first statement.

(3.4): Rusza inequality gives

$$|S^4|\cdot|S|\leqslant|S^3|^2,$$

that implies the statement for $k=4$. Suppose the statement is true for all $k<n$. Then

$$|S^n|\cdot|S|\leqslant|S^{\lfloor n/2\rfloor+1}|\cdot|S^{\lceil n/2\rceil+1}|$$

and induction gives

$$\frac{|S^n|}{|S|}\leqslant\left(\frac{|S^3|}{|S|}\right)^{\lfloor n/2\rfloor-1}\cdot\left(\frac{|S^3|}{|S|}\right)^{\lceil n/2\rceil-1}=\left(\frac{|S^3|}{|S|}\right)^{n-2},$$

which proves the second statement.

□

3.2 Orbit-Stabilizer

Let $G \curvearrowright X$ be a group action. The next Lemma is a generalization of the classic orbit stabilizer theorem. It allows to control lower bounds of $|SS^{-1} \cap G_x|$ with upper bounds of $\mathscr{O}_S(x)$. It will play an important role in the proof of Helfgott's Theorem (Theorem 1.2).

Lemma 3.2.1 (Orbit-Stabilizer). Let G be a finite group and let $S \subset G$ be a non empty subset. Let also S' be another subset of G. We have the two inequalities

$$|\mathscr{O}_S(x)| \cdot |SS^{-1} \cap G_x| \geqslant |S|, \tag{3.5}$$

$$|SS'| \geqslant |S \cap G_x| \cdot |\mathscr{O}_{S'}(x)|. \tag{3.6}$$

Proof. To prove (3.5) we construct an injective map from S to $S^{-1}S \cap G_x$. To do this we consider the map

$$\xi : s \mapsto sx,$$

and for each $s \in S$ we chose an element $\sigma(s) \in \xi^{-1}(sx)$ in a way such that, whenever $s_1 x = s_2 x$ holds, $\sigma(s_1) = \sigma(s_2)$ holds too. Since $s_1 x = s_2 x$ implies that

$$s_2^{-1} s_1 \in S^{-1}S \cap G_x,$$

we see that, for all $s_0 \in S$, we can inject $\xi^{-1}(s_0 x)$ in $SS^{-1} \cap G_x$ with the map

$$\pi : s \mapsto s^{-1}\sigma(s).$$

But then the map

$$s \longmapsto (\xi(s), \pi(s))$$

is injective: indeed $\xi(s_1) = \xi(s_2)$ implies $\sigma(s_1) = \sigma(s_2)$ and thus if $\pi(s_1) = \pi(s_2)$ we have $s_1 = s_2$. This proves (3.5).

To see that (3.6) also holds we construct another injection. We start by defining a *choice* map

$$c : \mathscr{O}_{S'}(x) \longmapsto S'$$

that assigns to each $y \in \mathscr{O}_{S'}(x)$ and element $c_y \in S'$ such that $c_y x = y$. The choice is clearly injective. Then we claim that the map

$$\begin{aligned} \mathscr{O}_{S'}(x) \times S \cap G_x &\longrightarrow S'S \\ (y, s) &\longmapsto c_y s \end{aligned}$$

is also injective. Indeed if we have $c_y s = c_z r$, for some $y, z \in \mathscr{O}_{S'}(x)$ and $s, r \in S \cap G_x$, we also have $c_y s x = c_z r x$, which gives $c_y x = c_z x$, hence $y = z$ and $c_y = c_z$ and $s = r$. We have proved (3.6). □

Corollary 3.2.1 (Classic Orbit-Stabilizer). If H is a subgroup of G, then

$$|H = |\mathscr{O}_H(x)| \cdot |H_x|.$$

Proof. Apply Theorem 3.2.1 to $H = S = S'$, so that

$$|S| \geqslant |S \cap G_x| \cdot |\mathscr{O}_S(x)| \geqslant |S|$$

□

3.3 Another sum-product estimate

Katz-Tao Lemma and Rusza-Plünnecke inequality

In this paragraph we state two important results in additive combinatorics. These are somewhat strong results and after a small number of simple lemmas they will lead us to another proof of the sum-product theorem. The first is Katz-Tao lemma.

Theorem 3.1 (Katz-Tao, [TV06], Lemma 2.53). Let R be a commutative ring, $R^\times$ the biggest multiplicative group in R (the *unities*). Let S be a finite subset of $R^\times$ such that

$$\max\left\{|2S|, |S^2|\right\} \leqslant K|S|.$$

Then there is a subset $S_0 \subseteq S$ such that $|S_0| + 1 \geqslant |S|/2K$ and

$$|S_0^2 - S_0^2| \ll K^{O(1)}|S_0|.$$

The second important result is a corollary of the following theorem (which is itself an easy consequence of Plünnecke theorem, [TV06],Theorem 6.27).

Theorem 3.2 (Plünnecke inequality, [TV06] Corollary 6.28). Let S and T be two finite sets of an abelian group G. Suppose that $|ST| \leqslant K|S|$. Then for all integers $l > 0$ there is a subset $S_0 \subset S$ such that

$$|S_0 T^l| \leqslant K^l |S_0|.$$

Corollary 3.3.1 (Ruzsa-Plünnecke inequality). Same hypothesis as above. We have that for all integers $n, m \geqslant 1$

$$|T^n T^{-m}| \leqslant K^{n+m}|S|$$

Proof. We have that G is abelian. Thus, using Ruzsa inequality and previous theorem, we have

$$\begin{aligned} |T^n T^{-m}| \cdot |S_0| &\leqslant |T^n S_0| \cdot |S_0^{-1} T^{-m}| \\ &= |S_0 T^n| \cdot |S_0 T^m| \\ &\leqslant K^{n+m}|S_0|^2 \\ &\leqslant K^{n+m}|S_0| \cdot |S|. \end{aligned}$$

□

Another sum-product over finite fields

If we assume Theorem 3.1 and Theorem 3.2 we easily obtain a sum product estimate sharper then the one in Theorem 1.1. We cut the proof in four lemmas and one proposition for simplicity.

Lemma 3.3.1. Let S and T be two subset of $\mathbb{F}_q$, with q odd. There is $\xi \in \mathbb{F}_q^\times$ such that

$$|S + \xi T| \geqslant \min\left\{\frac{|S||T|}{2}, \frac{q}{10}\right\}. \tag{3.7}$$

Proof. To simplify the reading we cut the proof in three parts. In (i) we bound $|S+\xi T|$ below, in (ii) we suppose $|S||T| \leqslant q/2$ and we deduce $|S + \xi T| \geqslant |S||T_0|/2$, while in (iii) we show that if $|S||T| \leqslant q/2$, then $|S + \xi T| \geqslant q/10$.

(i) The inclusion-exclusion formula tells us that, for a family of finite sets $\{X_i\}_{i=1}^n$, the cardinal of $\left|\bigcup_{i=1}^n X_i\right|$ is given by

$$\left|\bigcup_{i=1}^n X_i\right| = \sum_{i=1}^n |X_i| - \sum_{1\leqslant i<j\leqslant n} |X_i \cap X_j| + \sum_{1\leqslant i<j<k\leqslant n} |X_i \cap X_j \cap X_k| + \ldots + (-1)^{n-1}\left|\bigcap_i^n X_i\right|.$$

In particular one has

$$\left|\bigcup_{i=1}^n X_i\right| \geqslant \sum_{i=1}^n |X_i| - \sum_{1\leqslant i<j\leqslant n} |X_i \cap X_j|. \tag{3.8}$$

Let $\xi \in \mathbb{F}_q^\times$. We apply (3.8) to the family $\{s + \xi T\}_{s\in S}$ and we get

$$\begin{aligned} |S + \xi T| = \left|\bigcup_{s\in S}(s + \xi T)\right| &\geqslant \sum_{s\in S}|s + \xi T| - \frac{1}{2}\sum_{s_1\neq s_2}|(s_1 + \xi T) \cap (s_2 + \xi T)| \\ &= |S||T| + \xi T| - \frac{1}{2}\sum_{s_1\neq s_2}|(s_1 + \xi T) \cap (s_2 + \xi T)| \\ &= |S||T| - \frac{1}{2}\sum_{s_1\neq s_2}\sum_{t_1\neq t_2} 1_{\xi = \frac{s_1 - s_2}{t_2 - t_1}}(\xi). \end{aligned}$$

(ii) Suppose $|S||T| \leqslant q/2$. By averaging over all $\xi \in \mathbb{F}_q^\times$ we get

$$\begin{aligned}\frac{1}{q-1}\sum_{\xi\in\mathbb{F}_q^\times}|S+\xi T| &\geqslant |S||T| - \frac{1}{2}\frac{|S||T|(|S|-1)(|T|-1)}{q-1}\\ &\geqslant |S||T| - \frac{1}{2}\frac{|S|^2|T|^2}{q-1} \geqslant |S||T| - \frac{1}{2}\frac{|S|^2|T|^2}{2(|S||T|-1)}\\ &\geqslant |S||T| - \frac{1}{2}|S||T|,\end{aligned}$$

and (3.7) follows applying the pigeon-hole principle.

(iii) If $|S|\cdot|T| > q/2$, we consider the set $T_0 = T\setminus\{t_1,\dots,t_m\}$, where $m\in\mathbb{N}$ is minimal such that $|S|\cdot|T_0| = |S|(|T|-m) \leqslant q/2$. By the previous reasoning, we have

$$|S+\xi T| \geqslant |S+\xi T_0| \geqslant \min\left\{\frac{1}{2}|S||T_0|, \frac{q}{10}\right\}.$$

If $|S||T_0|/2 \geqslant q/10$, we are done, therefore suppose $|S||T_0| < q/5$. Since $|S||T_0| = |S||T| - m|S|$ and m is minimal such that $|S||T_0| \leqslant q/2$, we deduce that $|S||T_0| + |S| > q/2$ and in particular we see that

$$S > q/2 - |S||T_0| > \frac{q}{2} - \frac{q}{5}.$$

This proves (), since we have

$$|S+\xi T| > |S| > \frac{q}{2} - \frac{q}{5} = \frac{3q}{10} > \frac{q}{10} = \min\left\{\frac{|S||T|}{2}, \frac{q}{10}\right\}.$$

□

Let S, T be two subsets of $\mathbb{F}_p$. We introduce the notation

$$\mathbb{Q}(S,T) = \frac{S-S}{T-T\setminus\{0\}}.$$

Lemma 3.3.2. Let ξ be in $\mathbb{F}_p$. We have that $\xi\in\mathbb{Q}(S,T)$ if and only if $|S+\xi T| < |S||T|$.

Proof. The inequality $|S+\xi T| < |S||T|$ means that all maps from $S\times T$ to $|S+\xi T|$ are non injective. Thus if $|S+\xi T| < |S||T|$, the map

$$\phi : (s,t) \longmapsto s+\xi t,$$

has a non trivial collision (i.e. there is $(s_1,t_1)\neq(s_2,t_2)$ such that $\phi(s_1,t_1) = \phi(s_2,t_2)$). Since

$$[t_1 = t_2 \text{ and } \phi(t_1,s_1) = \phi(s_2,t_2)] \Rightarrow [s_1 = s_2],$$

we have $\xi\in\mathbb{Q}(S,T)$.
Conversely we it is easy to see that if $\xi\in\mathbb{Q}(S,T)$, the map ϕ defined above has a non trivial collision. □

Next lemma can be seen as a consequence of the following fact. Let G be a group acting on a set X. This induces an action on $\mathscr{P}(X)$. Suppose G is cyclic and generated by g_0. If g_0 fixes some point, the same point is fixed by the whole group. Let $S\in\mathscr{P}(X)$, $S\notin\{\emptyset, X\}$ and suppose $g_0 S = S$. Since $gX = X$, we see that $g_0(X\setminus S) = (X\setminus S)$, hence that $G\curvearrowright X$ it is not transitive!

Lemma 3.3.3. If S, T are two non-empty subsets of $\mathbb{F}_q$ with $|T| > 1$ and $\mathbb{Q}(S,T)\neq\mathbb{F}_q$. Then

$$|2ST - 2ST + S^2 - T^2| \geqslant |X||Y| \tag{3.9}$$

Proof. Consider the set of elements $X := \{\xi+1 : \xi\in\mathbb{Q}(S,T)\}$. The action $(\mathbb{F}_q,+)\cap\mathbb{F}_q$ is transitive. As a consequence of what we said above, we have that $X\cap\mathbb{Q}(S,T)\subsetneq X$, hence there is an element $\xi\in\mathbb{Q}(S,T)$ such that $\xi+1\notin\mathbb{Q}(S,T)$. Be the previous lemma we have

$$|S+(\xi+1)T| \geqslant |S||T|.$$

which is actually an equality (recall the trivial estimate $|S+\xi T|\leqslant|S||\xi T| = |S||T|$).Finally write ξ as $(s_1-s_2)/(t_1-t_2)$ with $s_1,s_2\in S$ and $t_1,t_2\in T$. We have

$$S+(\xi+1)T \overset{\text{bijection}}{\longleftrightarrow} (t_1-t_2)S + (s_1-s_2+(t_1-t_2))T) \subseteq TS - TS + ST - ST + T^2 - T^2,$$

which proves the statement. □

Lemma 3.3.4. If $\xi \in \mathbb{Q}(S,T)$, we have

$$|2ST - 2ST| \geqslant |S + \xi T|. \tag{3.10}$$

Proof. Let $\xi = (s_1 - s_2)/(t_1 - t_2) \in \mathbb{Q}(S,T)$. Then

$$|S + \xi T| = |(t_1 - t_2)S + (s_1 - s_2)T| \leqslant |TS - TS + ST - ST|.$$

□

Proposition 3.3.1. For all $S, T \subset \mathbb{F}_q$ such that $|T| > 1$, we have

$$|2ST - 2ST + T^2 - T^2| \gg \frac{1}{2}\min(|S||T|, q-1). \tag{3.11}$$

Proof. We combine the four lemmas above. If $\mathbb{Q}(S,T) \neq \mathbb{F}_q$, (3.9) implies (3.11). If $\mathbb{Q}(S,T) = \mathbb{F}_q$, we deduce from (3.7) and (3.10) that

$$|2ST - 2ST + T^2 - T^2| \geqslant \min\left\{\frac{|S||T|}{2}, \frac{q}{10}\right\}.$$

Since $q/10 \gg (q-1)/2$, (3.11) follows. □

Theorem 3.3 (Sum-product, third version.). Let S be a subset of $\mathbb{F}_q$ such that $|S| < q^{1-\delta}$ for some $\delta > 0$. Then either $|2S| \gg |S|^{1+\varepsilon}$, either $|S^2| \gg |S|^{1+\varepsilon}$, where $\varepsilon > 0$ and the implied constants depend only on δ.

Theorem 3.3 is stronger than Theorem 1.1 in the sense that $|S|$ has no lower bounds to respect.

Proof. If $|S|$ is smaller than a constant the result is trivial, so suppose that is not. Ab absurdo, suppose that for all $\varepsilon > 0$ the theorem does not hold (say for implied constants equal to 1). Then we can apply Katz-Tao lemma and we obtain that there is a subset S_0 of S, such that $|S_0| + 1 \geqslant |S|^{1-\varepsilon}/2$ and such that

$$|S_0^2 - S_0^2| \ll |S|^{1+O(\varepsilon)}. \tag{3.12}$$

At the same time, thanks to (3.11), we have

$$|3S_0^2 - 3S_0^2| \gg |S_0|^{1+\delta}.$$

Thus applying (the inverse of) Corollary 3.3.1 we see that

$$|S_0^2 - s_0^2| \gg |S_0|^{1+\delta/6} \gg |S|^{(1-\varepsilon)(1+\delta/6)} = |S|^{1-\varepsilon+\frac{\delta}{6}-\frac{\delta\varepsilon}{6}}. \tag{3.13}$$

If $|S|$ is bigger than a constant and $|\varepsilon|$ is small enough, (3.13) contradicts (3.12). □

Chapter 4

Expanders and Cayley Graphs

In this chapter we link the notion of growth in a group with the notion of *expander* graphs. We will also be able to prove that, if S is a symmetric subset of $\mathrm{SL}_2(\mathbb{F}_q)$ such that $|S| \geqslant 2|G|^{8/9}$, then every element of G can be written as $s_1 s_2 s_3$ for some $s_1, s_2, s_3 \in S$.

4.1 Basic definitions

We recall that a graph $\mathfrak{G} = (V, E)$ is a set $\mathfrak{G}(V)$ of *vertexes* together with a subset $\mathfrak{G}(E)$ of $V \times V$ called the *edges* of $\mathfrak{G}$. If for all couples (v, w) in E, the couple (w, v) is also in E, then we say $\mathfrak{G}$ is undirected. Couples of the form (v, v) are usually called *loops*. A *walk* γ from v to w (for $v, w \in V$) is a finite sequence of vertexes

$$v = \gamma_0, \gamma_1, \ldots, \gamma_{n-1} = w$$

such that $(\gamma, \gamma + 1) \in E$ for all i in $\mathbb{Z}/n\mathbb{Z}$. We say that a walk γ has length l and we write $|\gamma| = n$ when γ is a sequence of n vertexes. We say that a walk is a *path* if all vertex in the sequence are pairwise distinct. Using this notion there is a natural metric d that we can associate to $\mathfrak{G}$ and that is the one given by

$$d(v, w) \coloneqq \min\{|\gamma| : \gamma \text{ is a path between } v \text{ and } w\}.$$

This allows us to define the distance between a vertex v and a subset S of $\mathfrak{G}$: we let

$$d(x, S) \coloneqq \min_{s \in S} d(x, s).$$

We define the *diameter* of a graph to be the maximal distance between any two elements. Given a subset S of $\mathfrak{G}$, we define the boundary of S to be

$$\partial S \coloneqq \{v \in \mathfrak{G}(V) \setminus S : d(v, S) = 1\}.$$

The degree of a vertex v is the number $|\partial\{v\}|$, that corresponds to the number of *neighbourhoods* of v. We say that $\mathfrak{G}$ is *regular* if $|\partial\{v\}|$ is constant when v varies and we say that $\mathfrak{G}$ is k regular if $|\partial\{v\}| = k$ for all v. A graph $\mathfrak{G}$ is called *simple* if it is undirected and has no loop. We say that a graph is *connected* if for every couple of vertex (v, w) there is a path linking them. A *connected component* of a graph $\mathfrak{G}$ is a maximal connected sub-graph. Hence the connected components of a graph $\mathfrak{G}$ give a disjoint decomposition of $\mathfrak{G}$.

4.2 Expanders

Vertex Expander

We define now the notion of expander graph. Consider a k-regular graph $\mathfrak{G}$ with n vertexes.

Definiton 4.1. The graph $\mathfrak{G}$ is a *(vertex) c-expander* if for all subsets S of $\mathfrak{G}(V)$ such that $|S| \leqslant n/2$, we have that

$$|\partial S| \geqslant c|S|. \tag{4.1}$$

We remark, in the next lemma, that the notion of c-expander graph refines the notion of connected graph.

Lemma 4.2.1. A k-regular graph $\mathfrak{G}$ with n vertexes is a c-expander for some $c > 0$ if and only if $\mathfrak{G}$ is connected.

Proof. Suppose $\mathfrak{G}$ is not connected. Let S be a connected component. Then $\partial(S) = \emptyset$ and thus $\mathfrak{G}$ is not an expender for every $c > 0$.
Suppose $\mathfrak{G}$ is connected. Since $|\mathfrak{G}| = n < \infty$, there is a finite number of subsets $S \subseteq \mathfrak{G}(V)$. Defining

$$c(\mathfrak{G}) \coloneqq \min_{\substack{S \text{ subset} \\ |S| \leqslant n/2}} \frac{|\partial S|}{|S|},$$

we see that $\mathfrak{G}$ is a $c(\mathfrak{G})$ expander. The value $c(\mathfrak{G})$ is usually called the *Cheeger constant* of $\mathfrak{G}$ and is strictly positive whenever $\mathfrak{G}$ is connected. Indeed connected implies that for all $S \notin \{\emptyset, \mathfrak{G}(V)\}$,

$$\partial S \neq \emptyset.$$

□

We have just seen that, for a c-expander $\mathfrak{G}$, the Cheeger constant gives a lower bound for c. Although one can and should aim for better values of c, since the smaller c is, the more interesting $\mathfrak{G}$ is.

Definiton 4.2. Let $\{\mathfrak{G}_i\}_{i=1}^{\infty}$ be a sequence of graphs such that $\lim_{i\to\infty} |\mathfrak{G}_i(V)| = \infty$. We say that $\{\mathfrak{G}_i\}_{i=1}^{\infty}$ is a *c-expander family* if each graph in the sequence is a c expander.

An equivalent definition of expander graphs and families can be stated in terms of spectral gap of the adjacency matrix.

Spectral Expanders

Before stating the definition of a spectral expander we recall the definition and some basic features of the adjacency operator. First of all, consider the vector space $\mathfrak{F} = \mathfrak{F}(G, \mathbb{C})$. Its canonical basis is given by $\{\beta_v : v \in \mathfrak{G}(V)\}$ where β_v is defined as

$$\beta_v : x \longmapsto \beta_v(x) = \begin{cases} 1 \text{ if } v = x; \\ 0 \text{ otherwise .} \end{cases}$$

We remark that we can naturally rig the space $\mathfrak{F}$ with the standard scalar product: given $f_1,\ f_2 \in \mathfrak{F}$, we define

$$\langle f_1, f_2 \rangle \coloneqq \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

The (normalized) *adjacency matrix* of a k-regular graph $\mathfrak{G}$ is the matrix $\Gamma = \Gamma_{\mathfrak{G}}$ whose entries are given by

$$\Gamma_{v,w} = \begin{cases} 1/k \text{ if } (v,w) \in E, \\ 0 \text{ otherwise .} \end{cases}$$

Clearly Γ defines a linear operator on $\mathfrak{F}$ and when G is an undirected graph, Γ is symmetric. Explicitly we have that for $f \in \mathfrak{F}$, $\Gamma(f)$ is given by

$$\Gamma(f)(v) = \sum_{w \in \mathfrak{G}(V)} \Gamma_{v,w} \cdot f(w) = \frac{1}{k} \sum_{(v,w) \in E} f(w), \tag{4.2}$$

from which we see that $\Gamma(f)(v)$ can be interpreted as the average of f around v. Because of its symmetry, all eigenvalues of Γ are real and it is not hard to see that they all lie in $[-1, 1]$ and that the maximal eigenvalue 1 corresponds to the constant functions.

Definiton 4.3. We say that a k-regular graph $\mathfrak{G}$ is a (spectral) ε- expander if

$$\max_{\lambda \in \mathrm{Spec}(\Gamma) \setminus \{1\}} |1 - \lambda| \geqslant \varepsilon.$$

The two following theorems explain how spectral expanders and vertex expanders are related.

Theorem 4.1 ([V$^+$12], Theorem 4.6). Let $\mathfrak{G}$ be a spectral ε- expander. Then $\mathfrak{G}$ is a vertex c-expander for $c = 1 + \varepsilon$.

Theorem 4.2 ([V$^+$12], Theorem 4.9). Let $\mathfrak{G}$ be a k regular vertex c-expander. Then $\mathfrak{G}$ is a spectral ε-expander for

$$\varepsilon \gg \frac{c-1}{k}.$$

Before linking this to the notion of growth in groups we remark one last feature of the adjacency matrix.

Lemma 4.2.2. Consider the *unnormalized* adjacency matrix Γ^{un} of a graph $\mathfrak{G}$, that is

$$\Gamma^{\mathsf{un}}_{v,w} = \begin{cases} 1 \text{ if } (v,w) \in E \\ 0 \text{ otherwise .} \end{cases}$$

Then one has that $(\Gamma^{\mathsf{un}})^n_{v,w} = (\Gamma^{\mathsf{un}} \circ \ldots \circ \Gamma^{\mathsf{un}})_{v,w}$ is precisely the number of different walks of length n from v to w.

Proof. We write Γ instead of Γ^{un}. Let $\{1,\ldots,r\}$ denote the elements of $\mathfrak{G}$. For $\Gamma = \Gamma^1$ the statement is trivial. We prove the general case by induction. Suppose that $\Gamma^{n-1}_{i,j}$ is indeed the number of walks of length $n-1$ from i to j for all couples $(i,j) \in V(\mathfrak{G}) \times V(\mathfrak{G})$. Then by definition

$$\Gamma^n_{i,j} = \sum_{k=1}^{r:=|\mathfrak{G}|} \Gamma^{n-1}_{i,k} \cdot \Gamma_{k,j}.$$

We should prove that the right-hand-side coincide with the number of walks of length n from i to j. This is immediate since by induction we have

$$\Gamma^{n-1}_{i,k} \cdot \Gamma_{k,j} = |\{(i,j)\text{-walks of legnth } n \text{ such that at step } n-1 \text{ we are on } k\}|.$$

□

4.3 Cayley Graphs

The notion of growth on a group can be related to the notion of expansion on a graph via the definition of a Cayley graph.

Definiton 4.4. Let G be a finite group and S be a subset generating G. The Cayley graph of the couple (G,S) is the graph

$$\mathrm{Cay}(G,S) := \begin{cases} V = G, \\ E = \{(g, sg) : s \in S,\ g \in G\}. \end{cases}$$

Then to say that $\mathrm{Cay}(G,S)$ is a ε-expander is the same as saying that, for all subsets $S_0 \subseteq G$ such that $|S_0| \leqslant |G|/2$, one has

$$|S \cup S_0 S| \geqslant (1+\varepsilon)|S|,$$

or, more informally, that for every small set S_0 in G, the orbit $\mathscr{O}_{S_0 \cup \{e\}}(S)$ is noticeably bigger than S.
Before building up the proof of the main result of this chapter (namely Theorem 4.4 below) we remark and verify few simple facts about Cayley graphs.
We should notice for example that $\mathrm{Cay}(G,S)$ is indeed a graph, in the sense that is not a multi-graph, i.e. if there is an edge linking to vertexes, the edge is unique. Also, a Cayley graph has no loops if and only if $1 \notin S$. To achieve the "undirectedness" of a Cayley graph we need to suppose that $S = S^{-1}$. A Cayley graph is connected since all element g admits a path towards 1_G: indeed since S is a set of generators, g can be written as $s_1 \cdots s_l$ for some $l > 0$ and we have the path

$$(1_G, s_l),\ (s_l, s_{l-1}s_l),\ \ldots, (s_1^{-1}g, g).$$

Furthermore a Cayley graph is cleary $|S|$-regular. Notice that the diameter of a Cayley graph coincide to the diameter of the group mentioned in the introduction. There is a classic result of Babai that correlates the diameter of $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(G, S \cup S^{-1})$.

Theorem 4.3 ([Bab06], Theorem 1.4). Let G be a group and S be a set of generators of G. Let d the diameter of G for S, and let d_* be the diameter of G for $S \cup S^{-1}$. Then

$$d \leqslant d_*^2 (\log|G|)^3.$$

Adjacency matrix of a Cayley graph

Let Γ be the normalized adjacency matrix of $\mathrm{Cay}(G,S)$. In the specific case $\mathfrak{G} = \mathrm{Cay}(G,S)$, (4.2) becomes

$$\Gamma(f)(g) = \sum_{h\in G} \Gamma_{g,h} \cdot f(h) = \frac{1}{|S|} \sum_{h\in Sg} f(h) = \frac{1}{|S|} \sum_{s\in S} f(sg).$$

Suppose $S = S^{-1}$. To explicitly see that Γ is indeed symmetric we can simply compute.

$$\begin{aligned}
\langle \Gamma(f_1, f_2)\rangle =& \frac{1}{|S|} \sum_{g\in G}\sum_{s\in S} f_1(sg) f_2(g) \\
=& \frac{1}{|S|} \sum_{s\in S}\sum_{g\in G} f_1(sg) f_2(g) \\
=& \frac{1}{|S|} \sum_{s\in S}\sum_{g\in G} f_1(g) f_2(s^{-1}g) \\
=& \frac{1}{|S|} \sum_{s\in S}\sum_{g\in G} f_1(g) f_2(sg) = \langle f_1, \Gamma(f_2)\rangle .
\end{aligned}$$

Lemma 4.3.1. Let G be any group and S be a symmetric subset of G. Then if $x \notin S^3$ we have that

$$\langle \Gamma(1_S), 1_{xS^{-1}}\rangle = 0.$$

Proof. First we remark that for any subset $T \subseteq G$

$$\Gamma(1_T)(g) = \frac{|Sg \cap T|}{|T|}.$$

Then we see we have

$$\langle \Gamma(1_S), 1_{xS^{-1}}\rangle = \sum_{g\in G} \Gamma(1_S)(g) \cdot 1_{xS^{-1}} = \frac{1}{|S|} \cdot \sum_{g\in xS^{-1}} |Sg \cap S|.$$

We need to prove that $|Sg \cap S| = 0$ for every $g \in xS^{-1}$. If $x^{\sim} \in SxS^{-1} \cap S$, we would have $x \in S^{-1}x^{\sim}S \subset S^{-1}SS = SSS$ by hypothesis. But, also by hypothesis, $x \notin S^3$, hence $Sg \cap S = \emptyset$ for all $g \in x^{-1}S$. □

4.4 A lower bound for generating $\mathrm{SL}_2(\mathbb{F}_q)$

Theorem 4.4. Let q be a prime power and S a subset of $G = \mathrm{SL}_2(\mathbb{F}_q)$. Suppose $S = S^{-1}$ and $|S| \geqslant |G|^{8/9}$. Then

$$S^3 = G.$$

To proof of the above rely on a non trivial upper bound of the eigenvalues of Γ (Propositon 4.4.1 below).
The multiplicity of an eigenvalue λ of Γ (since Γ is diagonalizable) is given by the dimension of corresponding eigenspace λ, which in particular is a subvector space of $\mathfrak{F}$ with the property of being stable under multiplication by Γ. Because we are working with a group G (and not just a simple set of vertex) the vector space $\mathfrak{F}$ has a more richer structure.
Indeed we can make the group G act on $\mathfrak{F}$: for $h \in G$ and $f \in \mathfrak{F}(G,\mathbb{C})$ we define $hf \in \mathfrak{F}(G,\mathscr{X})$ to be the map $x \mapsto f(xh)$.
For λ an eignevalue, denote by $\mathfrak{F}_\lambda$ the corresponding eigenspace and consider some $f \in \mathfrak{F}_\lambda$. For all h and x in G we have that

$$\Gamma(hf)(x) = \frac{1}{|S|} \sum_{s\in S} f(sxh) = \Gamma(f)(xh) = h\Gamma(f)(x) = \lambda \cdot hf(x),$$

and thus $\mathfrak{F}_\lambda$ is G-invariant. Equivalently, there is a natural $\kappa[G]$-module structure on each eigenspace, which means that for each eigenspace of Γ we can associate a representation.
The dimension of a representation (i.e. the dimension of its associated eigenspace) can be bounded by looking at the character table of G. Of course the computation of some character tables may be non trivial, but for well studied groups (as $\mathrm{SL}_2(\mathbb{F}_q)$) these can be easily find in the literature.

Lemma 4.4.1 (Character table of $\mathrm{SL}_2(\mathbb{F}_q)$, [FH13]). Every non trivial representaion of $\mathrm{SL}_2(\mathbb{F}_q)$ has dimension at least $(q-1)/2$.

Proposition 4.4.1. Let $S = S^{-1}$ be a symmetric subset of $\mathrm{SL}_2(\mathbb{F}_q)$. Let Γ the adjacency matrix of $\mathrm{Cay}(\mathrm{SL}_2(\mathbb{F}_q), S)$. For all eigenvalues $\lambda \neq 1$ of Γ we have the bound

$$|\lambda| \leqslant \sqrt{\frac{2|\mathrm{SL}_2(\mathbb{F}_q)|}{|S|(q-1)}}.$$

Proof. By Lemma 4.4.1, $\dim_{\mathbb{C}}(\mathfrak{F}_\lambda)$ is at least $(q-1)/2$ for each eigenvalue λ. This shows that for all $m \in \mathbb{N}_{>0}$

$$\mathrm{Tr}(\Gamma^{2m}) = \sum_{i=1}^{r} \dim_{\mathbb{C}}(\mathfrak{F}_{\lambda_i}) \cdot \lambda_i^{2m} \geqslant \lambda_i^{2m} \cdot \frac{q-1}{2}.$$

Since $\lambda_i \leqslant 1$, the sharpest way to use the inequality above is to set $m = 1$.

$$\mathrm{Tr}(\Gamma^2) = \sum_i \lambda_i^2 \geqslant \lambda_i^2 \cdot \frac{q-1}{2},$$

for all i. On the other hand, the trace of Γ^2 can also be computed with Lemma 4.2.2, so that we obtain

$$\mathrm{Tr}(\Gamma^2) = \frac{|\mathrm{SL}_2(\mathbb{F}_q)|}{|S|}.$$

□

Proof of Theorem 4.4

Ab absurdo, let $x \notin S^3$. We show that $\langle \Gamma(1_S), 1_{x^{-1}S} \rangle > 0$ (which contradicts Lemma 4.3.1).
Let f_i (resp. λ_i) denote the eigenvectors (resp. eigenvalues) of Γ. Suppose without loss of generality that they have norm l_2 equal to 1. Notice that this implies that $f_0 \equiv |G|^{-1/2}$ (here f_0 denotes the eigenvector corresponding to the constant functions).
We have

$$\begin{aligned}
\langle \Gamma(1_S), 1_{x^{-1}S} \rangle &= \sum_i \lambda_i \cdot \langle 1_S, f_i \rangle \cdot \langle f_i, 1_{x^{-1}S} \rangle \\
&= \langle 1_S, f_0 \rangle \langle f_0, 1_{x^{-1}S} \rangle + \sum_{i>0} \lambda_i \cdot \langle 1_s, f_i \rangle \cdot \langle f_i, 1_{x^{-1}S} \rangle \\
&=: \frac{|S|^2}{|G|} + \xi,
\end{aligned}$$

and we want to show

$$|S|^2 > |G| \cdot |\xi| \tag{4.3}$$

Using Cauchy Schwartz we can bound ξ above:

$$|\xi|^2 \leqslant \frac{2|G|}{|S| \cdot (q-1)} \cdot |S|^2. \tag{4.4}$$

Thus, squaring (4.3) and replacing ξ by the right-hand-side of (4.4), we see we should show

$$|S|^4 > |G|^2 \cdot |S|^2 \cdot \frac{2|G|}{|S| \cdot (q-1)},$$

that we rearrange in

$$|S| > |G| \cdot \left(\frac{2}{(q-1)}\right)^{1/3}. \tag{4.5}$$

We are left to see that the contidion $|S| \geqslant 2|G|^{8/9}$ implies (4.5). To do this we compute the logarithm in base $|G|$ of the right-hand-side of (4.5). Recall that $|G| = q \cdot (q^2-1)$. We have

$$\log_{|G|}\left(\frac{|G|}{(q-1)^{1/3}}\right) = 1 - \frac{1}{3} \cdot \log_{(q+1)q(q-1)}(q+1) > 1 - \frac{1}{3} \cdot \frac{1}{3} = \frac{8}{9}$$

and therefore if $|S| \geqslant 2|G|^{8/9}$, (4.5) is satisfied. □

Chapter 5

Escape principle and Dimensional Estimates

5.1 Technical Lemmas for this and next chapter

Lemma 5.1.1. The centralizer of a regular semi-simple element is a maximal tori.

Proof. A regular semi-simple element is conjugated to a diagonal matrix. Similar elements have isomorphic centralizers. □

Lemma 5.1.2. The intersection of two maximal tori in $\mathrm{SL}_2(\mathbb{F}_q)$ is contained in $\{\pm \mathrm{id}_2\}$, where $\mathrm{id}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Proof. Let τ be the set of maximal tori of $G = \mathrm{SL}_\kappa(\mathbb{F}_q)$. Then $G \curvearrowright \tau$ via conjugation.

Let T be the canonical maximal tori of G (that is, the subgroup of G of diagonal matrices). Then if $\xi \in \mathrm{Stab}_G(T)$ stabilize T, we have that $\xi t \xi^{-1}$ is a diagonal matrix for all t in T.

$$\xi t \xi^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad\lambda_1 - bc\lambda_2 & ab(\lambda_2 - \lambda_1) \\ cd(\lambda_1 - \lambda_2) & ad\lambda_2 - bc\lambda_1 \end{pmatrix} \tag{5.1}$$

But if $\xi t \xi^{-1}$ is a diagonal matrix, we see in 5.1 that exactly one of the following things will happen:

(i) t has a unique eigenvalue and $\xi t \xi^{-1} = \pm \mathrm{id}_2$.

(ii) Both a and d are 0, and $bc = -1$. In G there are exactly $|T|$ matrices like this.

(iii) Both b and c are 0, and $ad = 1$. In G there are exactly $|T|$ matrices like this.

Thus the stabilizer of T is the subgroup of diagonal and anti-diagonal matrices in G and $|\mathrm{Stab}_G(T)| = 2|T|$. This shows that (using the classical orbit-stabilizer)

$$|\mathscr{O}_G(T)| = \frac{|G|}{|\mathrm{Stab}_G(T)|} = \frac{|G|}{2|T|}. \tag{5.2}$$

We also see that if $x \in \xi T \xi^{-1} \cap \theta T \theta^{-1}$ then $x' \in T$ with

$$x' = \sigma^{-1} \xi x \xi^{-1} \sigma$$

and thus either $\sigma T \sigma^{-1} = \xi T \xi^{-1}$, either $x = \{\pm \mathrm{id}\}$. □

Lemma 5.1.3. Let g be a regular semi-simple element in $\mathrm{SL}_2(\kappa)$. Then $\mathrm{Cl}(g)$ is an irreducible closed subvariety of G of dimension 2.

Proof. Let $c = \mathrm{Tr}(g)$. For two matrices x and y, we are going to write $x \sim_\kappa y$ to say that x and y are similar over κ. We prove that

$$\mathrm{Cl}(g) = \mathscr{X} := \{x \in G : \mathrm{Tr}(x) = c\}.$$

If two matrices are similar over κ^{alg}, then they are similar over κ (this is a consequence of the structure theorem for finitely generated modules over a principal ideal domain, and is a standard fact, see for

example [BML98], Section X.1.8, *The Calculation of Invariant Factors*). By the uniqueness of the Jordan normal form, for every $\sigma \in \mathrm{Cl}(g)$, we have

$$\mathrm{Cl}(g) = \left\{ \sigma \in \mathrm{SL}_2(\kappa) : \sigma \sim_{\kappa^{\mathrm{alg}}} \begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix} \right\}$$

for some $\lambda \in \kappa^{\mathrm{alg}} \setminus \{\pm 1\}$ such that $\lambda + 1/\lambda = c$. Since the equation

$$\lambda^2 - \lambda c + 1 = 0$$

and the equation

$$\lambda^2 - \lambda c' + 1 = 0$$

have no common solution for $c' \neq c$, we deduce that $\mathscr{X} \subseteq \mathrm{Cl}(g)$. The other inclusion being clear, we have finished the proof (the fact that $\mathscr{X}$ is closed irreducible and of dimension 1 is clear). □

Lemma 5.1.4. Consider an element $g \in \mathrm{SL}_2(\kappa)$ a regular semi-simple element. Let $\mathscr{X} = \mathrm{Cl}(g)$. Then if $h\mathscr{X} = \mathscr{X}$ for some $h \in G$, we have $h \in \{\pm \mathrm{id}_2\}$.

Proof. By previous proposition we have that $\mathscr{X}$ is the variety

$$\mathscr{X} = \{\sigma \in G : \mathrm{Tr}(\sigma) = t\}$$

where $t = \mathrm{Tr}(g) \neq \pm 2$. Since $\sigma \in \mathscr{X}$ has trace t we have that σ has the shape

$$\sigma = \begin{pmatrix} A & x \\ y & t - A \end{pmatrix}$$

with $A \in \kappa$ and $x, y \in \kappa$ such that $xy = A(t-A) - 1$. Thus

$$\mathscr{Y} = \left\{ \sigma = \begin{pmatrix} \sigma_0 & \sigma_0(t-\sigma_0) - 1 \\ 1 & t - \sigma_0 \end{pmatrix} : \sigma_0 \in \kappa \right\}$$

is a sub variety of $\mathscr{X}$ and if $h\mathscr{X} = \mathscr{X}$, we see that $h\mathscr{Y} \subseteq \mathscr{X}$. Let $h = \begin{pmatrix} h_1 & h_2 \\ h_3 & h_4 \end{pmatrix}$. We have that for $\sigma \in \mathscr{Y}$,

$$h\sigma = \begin{pmatrix} h_1 \cdot \sigma_0 + h_2 & * \\ * & h_3 \cdot (\sigma_0 \cdot (t - \sigma_0) - 1) + h_4 \cdot (t - \sigma_0) \end{pmatrix}$$

and since $\mathrm{Tr}(hg) = t$ by hypothesis we have that h is a point on the hyperplane $H(\sigma_0)$ that we define as the vanishing set of the polynomial

$$P_{\sigma_0} = \sigma_0 \cdot X_1 + X_2 + (\sigma_0(t - \sigma_0) - 1) \cdot X_3 + (t - \sigma_0) \cdot X_4 - t \in \kappa[X_1, \ldots, X_4].$$

Since this has to be true for all $\sigma_0 \in \kappa$, we have in particular that

$$h \in H(\sigma_0) \Rightarrow h \in H(\sigma_0 + 1) \cap H(\sigma_0)$$

for all $\sigma_0 \in \kappa$ (the big right arrow clearly stands for "implies"). But the hyperplane $H(\sigma_0 + 1)$ is the vanishing set of the polynomial

$$P_{\sigma_0 + 1} = P_{\sigma_0} + X_1 + X_3(t - (2\sigma_0 + 1)) - X_4$$

and thus h has to be contained in the vanishing set of the family of polynomials

$$A = \left\{ X_1 + X_3(t - (2\sigma_0 + 1)) - X_4 : \sigma_0 \in \kappa \right\}.$$

By repeating the same argument on

$$\mathscr{Y}' = \left\{ \sigma = \begin{pmatrix} \sigma_0 & 1 \\ \sigma_0(t - \sigma_0) - 1 & t - \sigma_0 \end{pmatrix} : \sigma_0 \in \kappa \right\}$$

we deduce that h has also to be contained in the vanishing set of the family of polynomials

$$B = \left\{ X_1 + X_2(t - (2\sigma_0 + 1)) - X_4 : \sigma_0 \in \kappa \right\}.$$

By simple computations (one has just to realize that multiplication by $t - (2\sigma_0 + 1)$ is a bijection of κ for almost every value of σ_0) one realize that the ideal $I \in \kappa[X_1, \ldots, X_4]$ generated by the polynomials in $A \cup B$ is actually generated just by $P_1 = X_1 - X_4$, $P_2 = X_2$, $P_3 = X_3$. Thus since $h \in \mathrm{SL}_2(\kappa)$, we see that $h = \pm \mathrm{id}_2$. □

5.2 Escape principle

Let G be a group generated by a set S. Suppose G acts on the affine space $\mathbb{A}^n$. Intuitively speaking the *escape principle* describes how a point $x_0 \in \mathbb{A}^n$ moves under the action of G. A bit more precisely it describes how *fast* and *often* x_0 can escape from an algebraic set $\mathscr{X}$. We should explain what we mean by *fast* and *often*. Suppose there are m elements in S^k such that $gx_0 \notin \mathscr{X}$ for all $g \in S_k$. We say that x_0 can escape fast in the sense that k is small, and we say that x_0 escape often when m is big.

To properly state the escape principle, we introduce the following notion. For $\mathscr{X}$ an algebraic set we define a *chain of proper sub-algebraic sets* to be a sequence

$$\mathscr{X} = \mathscr{X}_N \supsetneq \mathscr{X}_{N-1} \supsetneq \ldots \supset \mathscr{X}_1 = \{x\}.$$

We say that N is the *chain number* of $\mathscr{X}$ if N is maximal.

Theorem 5.1. Let G be a group acting on $\mathbb{A}^n(\kappa)$. Let $\mathscr{X}$ be a proper sub algebraic set and suppose that the orbit of some element x_0 is not contained in $\mathscr{X}$, hence

$$\mathscr{O}_G(x_0) \nsubseteq \mathscr{X},$$

for some $x_0 \in \mathbb{A}^n$. Suppose $S = S \cup S^{-1} \cup \{e\}$ is a set of generators for G. If $\mathscr{X}$ has chain number equal to N, there are at least

$$m = \max\{1, |S|/2^N\}$$

elements $g_1, \ldots, g_m$ in S^k, $k = 1 + 2N$, such that $g_i x_0 \notin \mathscr{X}$.

Proof. First of all, if $\mathscr{O}_S(x_0)$ is disjoint from $\mathscr{X}$, we have that $gx_0 \notin \mathscr{X}$ for all $g \in S$ and there is nothing to prove. We should suppose that $\mathscr{O}_S(x_0)$ intersects $\mathscr{X}$ non trivially.
Consider first the case $\mathscr{X} = \{x\}$ for some x in $\mathscr{O}_G(x)$. Clearly $\mathscr{X}$ has chain number equal to 1. We have

$$S = S_x \sqcup S \setminus S_x$$

where S_x denotes the stabilizers of x in S, that is $S \cap G_x$. Notice that $S \setminus S_x$ is non empty by hypothesis. Let $g \in S \setminus S_x$. If

$$|S_x| > |S|/2$$

holds, then

$$|SS_x| \geqslant |gS_x| > |S/2|,$$

holds too. Hence either $|S \setminus S_x| > |S|/2$ holds, either $|gS_x| > |S|/2$ holds.
If we let $h \in S$ be such that $hx_0 = x$, we get that either $|(S \setminus S_x)h| > |S|/2$, either $|gS_xh| > |S/2|$ holds, which shows that there are at least $|S|/2$ elements in S^3 such that $gx_0 \notin \mathscr{X}$. This proves the theorem for $\mathscr{X} = \{x\}$.

Now, we show how the values m and k changes when we increase the chain number. Suppose that for all proper sub-algebraic-sets $\mathscr{X}' \subsetneq \mathscr{X}$ we have that there are at least $m = \max\{1, |S|/l\}$ elements $g_1, \ldots, g_m$ in S^k such that $g_i x_0 \notin \mathscr{X}'$ for all $i \in \{1, \ldots, m\}$ (where l and k depend only on the chain number of $\mathscr{X}'$). Our goal should be to understand how we can make x_0 reach one of these sub-algebraic-set. If we are able to explicitly do this we should also be able to deduce the full statement by induction. We recall we have supposed that $\mathscr{O}_S(x_0) \cap \mathscr{X} \neq \emptyset$, otherwise the statement is trivial.

First we we consider an element $g_* \in S$ such that $g_*\mathscr{X} \neq \mathscr{X}$. We may assume that such an element exists, because otherwise the hypothesis $\mathscr{O}_G(x_0) \nsubseteq \mathscr{X}$, together with the assumption $g\mathscr{X} = \mathscr{X}$ for all $g \in S$, would imply that $gx_0 \notin \mathscr{X}$ for all $g \in S$ (hence the theorem would be trivial).

We have found an element $g_* \in S$ such that $g_*^{-1}\mathscr{X} \cap \mathscr{X} \nsubseteq \mathscr{X}$. Now we may look for an element $x' \in g_*^{-1}\mathscr{X} \cap \mathscr{X} \cap \mathscr{O}_S(x_0)$. Suppose by absurd that for all $x' \in \mathscr{O}_S(x_0)$, we have $x' \notin g_*^{-1}\mathscr{X} \cap \mathscr{X}$. We also have

$$g_*x' \notin \mathscr{X} \cap g\mathscr{X},$$

and since $g_*x' \in g\mathscr{X}$, we deduce

$$g_*x' \notin \mathscr{X},$$

This is a non-standard definition, made up only for the purpose of this section.

hence $\mathcal{O}_S(x_0) \cap \mathcal{X} = \emptyset$. By hypothesis this is not the case.

We have found an element g_* and an element x' such that $x' \in g_*^{-1}\mathcal{X} \cap \mathcal{X} \subsetneq \mathcal{X}$. Let $h \in S$ be such that $hx_0 = x'$. By our induction hypothesis there are at least m elements $g_1 \dots, g_m \in S^k$ such that $g_i h x_0 \notin g_*^{-1}\mathcal{X} \cap \mathcal{X}$ for all i. Hence for each i, either $g_i h x_0 \notin \mathcal{X}$, either $g_* g_i h x_0 \notin \mathcal{X}$, which means that there are at least $m/2$ elements in $g \in S^{k+2}$,of shape either $g_i h$ either $g_* g_i h$, such that $g x_0 \notin \mathcal{X}$. This means that when we increase the chain number by 1 we get: $l \rightsquigarrow l/2$ and $k \rightsquigarrow k+2$. This implies the theorem since we have found $m = \max\{1, |S|/2l\}$ elements in S^{k+2} that make x_0 escape. □

A soft application of the escape principle

The escape principle above can be used in the following situation. *Non generic* points are usually defined by a *closed* equation and they often define an algebraic set. For instance, let G be an algebraic group and consider a set of generators S. The escape principle tells us that we can find *enough* generic points in S^k, where k is a positive integer that depends only on the algebraic set defined by the non-generic points.
A concrete example may be the following. The regular semi-simple elements in $\mathrm{SL}_2(\mathbb{F}_q)$ (q odd) are precisely the elements whose trace is different from ± 2, i.e. those elements outside the algebraic set of dimension 2 defined by

$$\left\{\sigma \in \mathrm{SL}_2(\mathbb{F}_q) : \mathrm{Tr}(\sigma) = 2\right\} \cup \left\{\sigma \in \mathrm{SL}_2(\mathbb{F}_q) : \mathrm{Tr}(\sigma) = -2\right\}.$$

If S generates $\mathrm{SL}_2(\mathbb{F}_q)$, and $S \subseteq \mathcal{X}$, then, by the escape principle, there are regular semi-simple elements in S^2.

5.3 Dimensional estimates

The ideas behind the arguments in this section are (at least conceptually) the main ingredients used by Pyber and Szabó in the proof of the following theorem.

Theorem 5.2 ([PS14], Theorem 24). Let $\varepsilon > 0$ be a fixed constant. Let G be an algebraic group defined over $\mathbb{F}_q$. Suppose that $\mathrm{Z}(G(\mathbb{F}_q))$ is finite and that $G(\mathbb{F}_q)$ do not normalize any proper subgroup of G of positive dimension as well as positive codimension in $G(\mathbb{F}_q)$.
Let S be a generating subset of $G(\mathbb{F}_q)$, with $e \in S$ and let $\mathcal{X}$ be a variety of positive dimension. Then

$$|S^k| \geqslant |\mathcal{X}_0 \cap S|^{(1+\varepsilon)\frac{\dim(\mathcal{X})}{\dim(G)}},$$

where $k \in \mathbb{N}_{>0}$ depends only on ε and $\dim(G)$.

Almost Injectivity

We start by remarking some very simple facts. Let $f : X \to Y$ be an injective map between sets. This is equivalent to say that

$$|f^{-1}(y)| = 1 \text{ for all } y \in Y. \tag{5.3}$$

In particular, if f is injective one has $|f(X)| = |X|$. If we relax condition (5.3) and we replace it with

$$|f^{-1}(y)| \ll 1 \text{ for all } y \in Y. \tag{5.4}$$

instead of $|f(X)| = |X|$ we get

$$|f(X)| \ll O(|X|). \tag{5.5}$$

A function that satisfies (5.5) may be called *almost injective*.
A simple example of almost injective maps is given by any non-constant holomorphic map between Riemann surfaces.

Lemma 5.3.1 (Almost Injectivity Lemma). Let $\mathcal{X}$ and $\mathcal{Y}$ be two affine varieties and let $\phi : \mathcal{X} \to \mathcal{Y}$ be a regular map. Suppose $\mathcal{X}_0$ is sub-variety of $\mathcal{X}$ such that $\mathcal{X}_0 \supseteq \mathcal{X}_{\mathrm{sing}}^{\phi}$. Then $\phi\,|_{\mathcal{X}\setminus\mathcal{X}_0}$ is almost injective. In particular, for all subsets $S \subset \mathcal{X} \setminus \mathcal{X}_0$,

$$|S| \ll |\phi(S)|.$$

Proof. Because $\mathcal{X}_{\mathrm{sing}}^{\phi} \subseteq \mathcal{X}_0$, one easily deduce that if $y \in \mathrm{Im}(\phi|_{\mathcal{X}\setminus\mathcal{X}_0})$, $\phi^{-1}(y)$ is a finite set and its size can be bounded by a constant that depends only on the degree of $\mathcal{X}$ and ϕ. □

Intersection with varieties of dimension one

In this section we study the intersection properties of a set of generators of $\mathrm{SL}_2(\mathbb{F}_q)$. Since we are avoiding any kind of assumption on S, the following arguments, are based merely on some (light) properties of SL_2: the dimension and the (almost) simplicity[†].

Proposition 5.3.1. Let $\mathscr{X}_0$ be a variety living in some larger (algebraic) set Ω, and such that $\dim(\mathscr{X}_0) = 1$. We define $\mathscr{X} = \mathscr{X}_o^{\times n}$ and we let $\phi : \mathscr{X} \to \Omega$ be a regular map of such that $\mathscr{X}_{\mathrm{sing}}^{\phi}$ has positive codimension in $\mathscr{X}$. Suppose S is a subset of Ω such that $\phi(S^{\times n}) \subset S^k$ for some $k \geqslant 1$. Then one has

$$|S \cap \mathscr{X}_0| \ll \sqrt[n]{|S|^{n-1} + |S^k|}, \tag{5.6}$$

where the implicit constant depends only on degree of ϕ and the degree of $\mathscr{X}$.

Proof. To simplify the reading we cut the proof in two parts. In (i) we prove the statement for the particular case $n = 2$, while in (ii) we deduce the general statement.

(i) We have $|S^{\times 2} \cap \mathscr{X}| = |S^{\times 2} \cap \mathscr{X}_{\mathrm{sing}}^{\phi}| + |S \cap (\mathscr{X} \setminus \mathscr{X}_{\mathrm{sing}}^{\phi})|$. By almost injectivity we also have

$$|S^2 \cap \mathscr{X} \setminus \mathscr{X}_{\mathrm{sing}}^{\phi}| \ll |\mathrm{Im}(\phi\,|_{S^2 \cap \mathscr{X} \setminus \mathscr{X}_{\mathrm{sing}}^{\phi}})| \leqslant |S^k|.$$

To bound $|S^{\times}2 \cap \mathscr{X}_{\mathrm{sing}}^{\phi}|$ consider the projection $\pi : \mathscr{X}_{\mathrm{sing}}^{\phi} \to \mathscr{X}_0$ that maps (x_1, x_2) to x_1. Then we decompose $\mathscr{X}_{\mathrm{sing}}^{\phi}$ in *nice points* and *bad points*. That is

$$\mathscr{X}_{\mathrm{sing}}^{\phi} = \left(\bigsqcup_{\substack{y \text{ s.t.} \\ \dim(\pi^{-1}(y))=0}} \pi^{-1}(y) \right) \sqcup \left(\bigsqcup_{\substack{y \text{ s.t.} \\ \dim(\pi^{-1}(y))=1}} \pi^{-1}(y) \right).$$

We abbreviate the decomposition above writing $\mathscr{X}_{\mathrm{sing}}^{\phi} = \mathscr{Z}_g \sqcup \mathscr{Z}_b$.
Clearly when restricted to $\mathscr{Z}_g$, the projection π becomes almost injective.
On the other hand $\mathscr{Z}_b$ contains only a finite number of points: if the contrary were true, $\mathscr{X}_{\mathrm{sing}}^{\phi}$ would contain an infinite number of disjoint components of dimension 1, which is impossible ($\mathscr{X}_{\mathrm{sing}}^{\phi}$ has positive codimension).
Thus we have $|\mathscr{Z}_g \cap S^{\times 2}| \ll |\pi(\mathscr{Z}_g \cap S^{\times 2})| \leqslant |S|$ and $|\mathscr{Z}_b \cap S^{\times 2}| \ll 1$ where both implied constants depend only on $\mathscr{X}_{\mathrm{sing}}^{\phi}$. Combining all together we obtain

$$|\mathscr{X}_0 \cap S|^2 = |\mathscr{X} \cap S^{\times 2}| \ll |S^k| + |S| + 1,$$

which proves the statement for $n = 2$.

(ii) To obtain the general statement one can for example define $n-1$ projections

$$\mathscr{X}_{\mathrm{sing}}^{\phi} \xrightarrow{\pi_1} \mathscr{X}_0^{n-1} \xrightarrow{\pi_2} \mathscr{X}_0^{n-2} \xrightarrow{\pi_3} \cdots \xrightarrow{\pi_{n-1}} \mathscr{X}_0,$$

$$\pi_i : (x_1, \ldots, x_{n-i+1}) \longmapsto (x_1, \ldots, x_{n-i}),$$

and, at each application of π_i, separate bad and good points (of the new image) and apply π_{i-1} to bad points. More concretely: start at $\mathscr{X}_{\mathrm{sing}}^{\phi}$ and separate it in $\mathscr{Z}_g^{(1)}$ and $\mathscr{Z}_b^{(1)}$ (as before) then apply π_2 to $\pi_1(\mathscr{Z}_b^{(1)})$ and repeat, so that at each step one separate $\pi_i(\mathscr{Z}_b^{(i)})$ in

$$\mathscr{Z}_g^{(i+1)} \sqcup \mathscr{Z}_b^{(i+1)} := \left(\bigsqcup_{\substack{y \text{ s.t.} \\ \dim(\pi_{i+1}^{-1}(y))=0}} \pi_{i+1}^{-1}(y) \right) \sqcup \left(\bigsqcup_{\substack{y \text{ s.t.} \\ \dim(\pi_{i+1}^{-1}(y))>0}} \pi_{i+1}^{-1}(y) \right).$$

At the end of this long decomposition, by almost injectivity we obtain that for all $i \in \{1, \ldots, n-1\}$

$$|\mathscr{Z}_g^{(i)} \cap S^{\times(n-i+1)}| \ll |S|^{n-i}.$$

[†]Here, almost simple, means that it does not contain any proper connected normal algebraic subgroup.

By dimensional reasons (recall, again, that $\mathscr{X}_{\text{sing}}^{\phi}$ has positive codimension in $\mathscr{X}$) we obtain as well that for all $i \in \{n-1, \dots, 1\}$

$$|\mathscr{Z}_g^{(i)} \cap S^{\times n-i+1}| \ll |S|^{n-(i+1)}.$$

We have shown that

$$|\mathscr{X}_0 \cap S|^n = |\mathscr{X} \cap S^{\times n}| \ll \sqrt[n]{|S|^{n-1} + |S^k|}.$$

□

Intersection with conjugacy classes

In this paragraph we prove Theorem 5.2 in the particular case $G = \mathrm{SL}_2(\mathbb{F}_q)$ and $\mathscr{X} = \mathrm{Cl}(g)$, for g regular and semi-simple.

Proposition 5.3.2. Let $g \in \mathrm{SL}_{\mathbb{F}_q}(\kappa)$ be a regular semi-simple element. Let S be a generating subset of $\mathrm{SL}_2(\mathbb{F}_q)$ such that $S = S \cup S^{-1} \cup \{e\}$. Then

$$|S \cap \mathrm{Cl}(g)| \ll |S^k|^{2/3}$$

where k is absolute.

Proof. By Lemma 5.1.3, $\mathrm{Cl}(g)$ is a closed variety of dimension 2. We start by considering the map

$$\pi : \mathrm{Cl}(g) \times \mathrm{Cl}(g) \longrightarrow G$$

defined by $\pi(x, y) = xy$. Let $h \in G$ and consider the pre-image $\pi^{-1}(h)$, given by the set

$$\left\{(x, x^{-1}h) \in \mathrm{Cl(g)} \times \mathrm{Cl(g)} : x^{-1}h \in \mathrm{Cl(g)}\right\}.$$

The condition $x^{-1}h \in \mathrm{Cl}(g)$ is equivalent to $x^{-1} \in \mathrm{Cl}(g)h^{-1}$ which is again equivalent to $x \in h\mathrm{Cl}(g)$. Thus we can see that we have an isomorphism (of varieties)

$$\pi^{-1}(h) \simeq h\mathrm{Cl}(g) \cap \mathrm{Cl}(g).$$

In particular we have $\dim(\pi^{-1}(h)) = \dim(h\mathrm{Cl}(g) \cap \mathrm{Cl}(g)) \leqslant 2$. We have $\dim(h\mathrm{Cl}(g) \cap \mathrm{Cl}(g)) = 2$ if and only if,

$$h\mathrm{Cl}(g) = \mathrm{Cl}(g),$$

hence if and only if $h = \pm\mathrm{id}$ (see Lemma 5.1.4).
Let $\varpi = \pi|_{(S\cap\mathrm{Cl}(g))\times(S\cap\mathrm{Cl}(g)\setminus\{\pm\mathrm{id}\})}$. By the usual identity

$$\mathrm{Dom}(\varpi) = \bigsqcup_{h\in\mathrm{Im}(\varpi)} \varpi^{-1}(h)$$

one deduce

$$|\varpi^{-1}(h_0)| \cdot |\mathrm{Im}(\varpi)| \geqslant |S \cap \mathrm{Cl}(g)| \cdot |S \cap \mathrm{Cl}(g) \setminus \{e\}| = |S \cap \mathrm{Cl}(g)|^2 - 2|S \cap \mathrm{Cl}(g)| \tag{5.7}$$

where h_0 is such that $|\varpi^{-1}(h_0)| = |S \cap h_0\mathrm{Cl}(g) \cap \mathrm{Cl}(g)|$ is maximal. Solving the inequality for $|S\cap\mathrm{Cl}(g)|^2$ (and remarking that $\mathrm{Im}(\varpi) \subseteq |S^2|$) one obtains,

$$|S \cap \mathrm{Cl}(g)| \leqslant 2 + \sqrt{\varpi^{-1}(0) \cdot |S^2|}. \tag{5.8}$$

If $\dim(\pi^{-1}(h_0)) = 0$, by (5.8), we are done. We can assume $\dim(\pi^{-1}(h_0)) = 1$.
Let $\mathscr{Z}$ be an irreducible component of $\pi^{-1}(h)$ with $\dim(\mathscr{Z}) = 1$ and consider the map

$$\begin{aligned} \phi_{(\xi_1,\xi_2)} : \mathscr{Z} \times \mathscr{Z} \times \mathscr{Z} &\longrightarrow G \\ (z_1, z_2, z_3) &\longmapsto x \cdot \xi_1 y \xi_1^{-1} \cdot \xi_2 z \xi_2^{-1} \end{aligned}$$

Claim: *there exists a positive integer k such that there is at least a point $(\xi_1, \xi_2) \in G \times G$ and a point $P = (x_*, x_*, x_*) \in \mathscr{Z}^{\times 3}$ such that $D_P\phi_{(\xi_1,\xi_2)}$ is non degenerate. Furthermore the set of points (ξ_1, ξ_2) such that $D_P\phi_{\xi_1,\xi_2}$ is degenerate form an algebraic set in $G \times G$.*

Assume the claim. By the escape principle we may suppose that $(\xi_1, \xi_2) \in S^k \times S^k$ for some positive integer k that depends only on the chain number of $\mathscr{Z}$ (and hence on the chain number of $\mathscr{X}$, but it does not depend on g). Notice that since $\xi_1, \xi_2 \in S^k$, $\mathrm{Im}(\phi\mid_{S^{\times 3}}) \subseteq S^{3k+3}$. We apply Proposition 5.3.1 and we obtain that

$$|S \cap \mathscr{Z}| \ll |S^{k'}|^{1/3}, \tag{5.9}$$

with $k' = 3k+3$. We combine (5.9) with (5.8) we are done, since

$$|S \cap \mathrm{Cl}(g)| \ll 2 + \sqrt{|S^{k'}|^{1/3} \cdot |S^2|} \ll \sqrt{|S^{k'}|^{1/3} \cdot |S^{k'}|} = |S^{k'}|^{2/3}.$$

□

Of course the prove is not exactly complete since we still have to discuss the claim. We sketch a proof of the claim in next paragraph. This will implicitly involve some technical facts beyond the scope of the document and therefore it may be skipped.

Almost simplicity and non degeneracy

In order to explain in detail why the claim in the proof of Proposition 5.3.2 holds, we need to be able to compute differentials of regular maps between algebraic groups explicitly. Since this is a bit out of of the scope of this document we will not introduce the theory and the precise definitions necessary to do differentiate, but we merely introduce the concepts behind it. First of all linear algebraic groups are regular. This means that for all linear algebraic groups G and for all $x \in G$, the tangent $T_x(G)$ has the same dimension of G. Furthermore all tangent space of a group G can be rigged with a natural structure of Lie algebra. One usually denote $\mathrm{Lie}(G)$ the the tangent space at $e \in G$. From a Lie algebra point of view there is really nothing special about $T_e(G)$, since all tangent spaces (and their Lie algebra structure) are isomorphic. We have:

Proposition 5.3.3 ([Bou72], Chapter 3, Section 9.8, Proposition 27). If G is a Lie group with no proper normal connected subgroup, then $\mathrm{Lie}(G)$ is simple, that is $\mathrm{Lie}(G)$ has no proper ideals.

From which we deduce:

Proposition 5.3.4. Let G be an *almost simple* algebraic group over an algebraically closed field. Let $\mathscr{X}_0 \subset G$ be a variety of dimension 1 and let $\mathscr{X} = \mathscr{X}_0^{\times n}$. For each $\xi = (\xi_1, \dots, \xi_n) \in G^{\times n}$, define ϕ_ξ to be the map

$$\begin{aligned} \phi_\xi : \mathscr{X} &\longrightarrow G \\ (x_0, x_1, \dots, x_{n-1}) &\longmapsto x_0 \cdot \xi_1 x_1 \xi_1^{-1} \cdot \xi_2 x \xi_2^{-1} \cdot \ldots \cdot \xi_n x_n \xi_n^{-1}. \end{aligned}$$

Then

$$\left\{ \xi \in G^{\times n} : \dim(\mathscr{X}_{\mathrm{sing}}^{\phi_\xi}) = n \right\} \subset G^{\times n}$$

is an algebraic set of positive codimension.

We remark that this is still not enough to prove the claim because, for our purposes, we would need the same result over the finite field $\mathbb{F}_q$.

Sketch of the proof of Proposition 5.3.4. Let $\phi = \phi_\xi$ and for a point P in G, let $\mathrm{Lie}_P(G) = T_P(G)$. One can show that the differential $D_P\phi$ at a given point $P = (x_*, \dots, x_*)$ is given by

$$\begin{aligned} D_P\phi : \bigoplus_{i=1}^{n} T_{x_*}(\mathscr{X}_0) &\longrightarrow \mathrm{Lie}_{\phi(P)}(G) \\ (v_1, \dots, v_n) &\longmapsto v_0 + \xi_1 v_1 \xi_1^{-1} + \ldots + \xi_{n-1} v_{n-1} \xi_{n-1}^{-1}. \end{aligned}$$

The image of $D_P\phi$ can be decomposed in the sum

$$\mathrm{Im}(D_P\phi) = T_{x_*}(\mathscr{X}_0) + \xi_1 T_{x_*}(\mathscr{X}_0)\xi_1^{-1} + \ldots + \xi_{n-1} T_{x_*}(\mathscr{X}_0)\xi_{n-1}^{-1}, \tag{5.10}$$

and we have that $D_P(\phi)$ is not degenerate if and only if the sum above is a direct sum.
Since the tangent spaces in the sum are one dimensional, to say that two tangent spaces are in direct sum is the same as saying that they are different. If for all $\xi \in G(\kappa^{\mathrm{alg}})$,

$$T_{x_*}(\mathscr{X}_0) = \xi T_{x_*}(\mathscr{X}_0)\xi^{-1},$$

holds, one can show that $T_{x_*}(\mathscr{X}_0)$ is stable under the Lie bracket. This would imply that $T_{x_*}(\mathscr{X}_0)$ is a proper ideal of $\mathrm{Lie}_{\phi(P)}(G) \simeq \mathrm{Lie}(G)$, which contradicts Proposition 5.3.3. Hence there is at least one element $\xi_1 \in G$ such that

$$T_{x_*}(\mathscr{X}_0) + \xi_1 T_{x_*}(\mathscr{X}_0)\xi_1 = T_{x_*}(\mathscr{X}_0) \oplus \xi_1 T_{x_*}(\mathscr{X}_0)\xi_1.$$

If we iterate the argument we eventually deduce that the sum (5.10) is indeed direct. □

As mentioned few lines above this is not enough to obtain the claim we want to prove, since a priori the algebraic set

$$\left\{\xi \in G^{\times n} : \dim(\mathscr{X}_{\mathrm{sing}}^{\phi_\xi}) = n\right\} \subset G^{\times n}$$

could contain $G(\mathbb{F}_q)^{\times n}$ for some power of prime q (here $G(\mathbb{F}_q)$ denotes the points of G with coordinates in $\mathbb{F}_q$). We can avoid these kinds of problems, provided that the characteristic of the field is large enough.

Lemma 5.3.2. Let G be an algebraic group over $\mathbb{F}_p^{\mathrm{alg}}$ whose equations are defined over $\mathbb{F}_p[X_1, \dots, X_n]$. Let $\mathscr{X} \subsetneq G$ be a proper sub variety of G (the equations defining $\mathscr{X}$ may not be defined in $\mathbb{F}_p[X_1, \dots, X_n]$). Then if p is large enough,

$$\mathscr{X}(\mathbb{F}_p) \subsetneq G(\mathbb{F}_p),$$

where $\mathscr{X}(\mathbb{F}_p)$ and $G(\mathbb{F}_p)$ are the set of points in $\mathscr{X}$ and G whose coordinates are in $\mathbb{F}_p$.

Again, since it is out of the scope of this document we will not introduce the projective space, although we use it in the proof of Lemma. The reader may skip this proof. We sketch it for the sake of completeness.

Proof. Denote by $\overline{G}$ the projective closure of G in $\mathbb{P}^n(\mathbb{F}_p^{\mathrm{alg}})$ and by G_∞ the intersection of $\overline{G}$ with the hyperplane at infinity that we denote by H_∞. Notice $\dim(G_\infty) < \dim(G)$. By the Lang-Weil's bound (see theorem below[‡]) we have

$$\overline{G}(\mathbb{F}_p) - p^{\dim(G)} = O(p^{\dim(G)-1/2})$$

as well as

$$G_\infty(\mathbb{F}_p) - p^{\dim(G_\infty)} = O(p^{\dim(G_\infty)-1/2}).$$

Same holds for $\overline{\mathscr{X}}$ and $\mathscr{X}_\infty$ (defined similarly) and we obtain

$$|G(\mathbb{F}_p) \setminus \mathscr{X}(\mathbb{F}_p)| = |G(\mathbb{F}_p)| - |\mathscr{X}(\mathbb{F}_p)| \gg p^{\dim(G)} - O(p^{\dim(G)-1}),$$

where the two implied constants depend on the degree and dimension of G and $\mathscr{X}$ (and n), but not on p. Thus if p is large enough, the right hand side of the inequality is positive. We remark that exactly the same argument works for $\mathbb{F}_q$, where q a power of p. □

Theorem 5.3 (Lang-Weil, [LW54]). Let $\mathscr{X}$ be a variety in $\mathbb{P}^n$ of degree d and dimension r. Let N be the number of points of $\mathscr{X}(\mathbb{F}_q)$. Then there exists a constant c such that

$$|N - q^r| \leqslant (d-1)(d-2)q^{r-1/2} + cq^{r-1},$$

where c depends only on n, d, r.

Intersection with a centralizer

By the means of the generalized orbit-stabilizer theorem, we can use Proposition 5.3.1 to obtain an upper bound for the intersection of S with $\mathrm{Z}(g)$.

Corollary 5.3.1. Let $g \in \mathrm{SL}_2(\kappa)$ be a regular semi-simple element. Let S be a generating subset of $\mathrm{SL}_2(\kappa)$ such that $S = S \cup S^{-1} \cup \{e\}$. Suppose that $|S^3| < |S|^{1+\delta}$. Then

$$|S^2 \cap \mathrm{Z}(g)| \gg |S|^{1/3-O(\delta)}$$

where $\mathrm{Z}(g)$ is the centralizer of g and k is absolute.

[‡]We could have avoided the use of the Lang-Weil's bound by stating in its full generality Deligne's bound (Theorem 2.3). Although this would have overkilled our needs.

Proof. When $G = \mathrm{SL}_2(\kappa)$ acts on G via conjugation, the stabilizer of an element g is the centralizer g. Let g be regular and semi-simple. By Theorem 3.2.1 and Proposition 5.3.2 we have

$$|S^2 \cap \mathrm{Z}(g)| \geqslant \frac{|S|}{|\mathscr{O}_S(x)|} = \frac{|S|}{|S \cap \mathrm{Cl(g)}|} \gg \frac{|S|}{|S^k|^{2/3}}.$$

By hypothesis we have $|S^3| < |S|^{1+\delta}$ and thus, using (3.4), we obtain

$$|S^k| \leqslant |S^3|^{k-2} \cdot |S|^{k-1} \leqslant |S|^{2k-3+(k-2)\delta} = |S|^{O(\delta)},$$

which concludes the proof. □

Chapter 6

Proof of Helfgott's Theorem

We recall Helfgott's Theorem.

Theorem 1.2 (Helfgott's theorem, [Hel08]). Let S be a generating subset of $\mathrm{SL}_2(\mathbb{F}_q)$. Then we have that either

$$|S^3| \gg |S|^{1+\delta}$$

holds, either

$$(S \cup S^{-1} \cup \{e\})^k = \mathrm{SL}_2(\mathbb{F}_q)$$

holds, for some absolute constants $\delta > 0$ and $k \geqslant 0$.

6.1 Proof of the Helfgott's Theorem

It is finally time to prove Theorem 1.2. We are going to use the results proved in the last two chapters.

Reduction to the case $S = \overline{S}$

Suppose that the theorem holds, for k and δ absolute, for sets of the form $S = S \cup S^{-1} \cup \{e\}$. We want to show that there is an absolute constant k' such that $|S^3| < |S|^{1+\delta}$ implies $S^{k'} = G$. To see this we use (3.3) and $|S^3| < |S|^{1+\delta}$ to obtain

$$|(S \cup S^{-1} \cup \{e\})^3| \ll |S|^{1+3\delta}$$

with absolute implied constant. Then letting $k = 3k_0 + r$ (with $0 < r < 3$) we see that

$$|G| = |S \cup S^{-1} \cup \{e\}^k| \leqslant |S|^{k_0(1+3\delta+\log_2(c))+r},$$

and thus $k' = \lceil k_0(1 + 3\delta + \log_2(c)) + r \rceil$ does the job. This shows we can assume $S = \overline{S}$.

Pivoting

We will show that if

$$|S^3| < |S|^{1+\delta}, \tag{6.1}$$

then S generates G (for $\delta > 0$ small enough). For this let

$$\begin{aligned} \pi_\xi : S \times \mathscr{X} &\longrightarrow G \\ (s, x) &\longmapsto s\xi x \xi^{-1}, \end{aligned}$$

where $\mathscr{X} = \mathrm{Z}(g_0)$ is the centralizer of some regular semi-simple element (and therefore a maximal torus). We can find such g_0 in S^2 using the escape proposition with "G" $= \langle S \rangle$ and "$\mathscr{X}$" $= \{\pm \mathrm{id}\}$.
We have three possible cases.

(A) There is ξ in S such that $\ker(\pi_\xi) \subseteq \{\pm \mathbf{id}\}$

We show that this case, if $\delta > 0$ is small enough, cannot happen. Suppose that $\ker(\pi_\xi) \subseteq \{\pm \mathrm{id}\}$ for some $\xi \in S$. Then we have

$$|S^5| \geq |\pi_\xi(S \times (S^2 \cap \mathscr{X}))| \geq \frac{1}{4}|S| \cdot |S^2 \cap \mathscr{X}| \gg |S|^{4/3-O(\delta)}, \tag{6.2}$$

where the factor $1/4$ is due to the fact that $\pi_\xi(\pm x, \pm y) = \pi_\xi(\mp x, \pm y)$ for all x, y in the domain. But if δ is small enough, this is not possible since by (3.3) we have $|S^5| \leqslant |S^3|^3/|S|^2$ and hence, using (6.1),

$$|S^5| < |S|^{1+3\delta},$$

which is clearly in contradiction with (6.2).

(B) For any ξ in G, $\ker(\pi_\xi) \supsetneq \{\pm \mathbf{id}\}$

In this case we have that for all ξ there are $s_1, s_2 \in S$ and $x_1, x_2 \in \mathscr{X}$ such that both $(s_1, t_1) \neq (s_2, t_2)$ and $\pi_\xi(s_1, t_1) = \pm\pi_\xi(s_2, t_2)$ hold. This translates in

$$s_2^{-1}s_1 = \xi t_2 t_1^{-1} \xi^{-1}$$

and in particular it means that for all $\xi \in \mathrm{SL}_2(\mathbb{F}_q)$

$$S^2 \cap \xi T \xi^{-1} \supsetneq \{\pm \mathrm{id}_2\}.$$

Let $g \neq \pm \mathrm{id}_2$ be an element of $S^2 \cap \xi T \xi^{-1}$. We have that $\mathrm{Z}(g) = \xi T \xi^{-}1$ and thus, by **Corollary** 5.3.1,

$$|S^2 \cap \xi T \xi^{-1}| \gg |S|^{1/3-O(\delta)}.$$

We have seen in Lemma 5.1.2 that the intersection of two maximal tori in $\mathrm{SL}_2(\mathbb{F}_q)$ is at most $\{\pm \mathrm{id}\}$ and since there are at least $|G|/2|T|$ maximal tori (recall (5.2)), we have

$$|S^2| \geqslant \frac{|G|}{2|T|}|S^2 \cap \xi T \xi^{-1}| \gg q^2|S|^{1/3-O(\delta)}. \tag{6.3}$$

We are assuming that ($|S^2| \leqslant$) $|S^3| < |S|^{1+\delta}$, hence (6.3) tells us that

$$|S|^{O(\delta)} \gg q^3 \tag{6.4}$$

Since $|G| = q^2(q-1) = O(q^3)$ we can find δ small enough such that (6.4) implies $|S| \geqslant 2|G|^{8/9}$ and by Theorem 4.4 we deduce that S generates G.

(C) There is ξ in $G \setminus S$ such that $\ker(\pi_\xi) \subseteq \{\pm \mathbf{id}\}$

Let ξ be such that $\ker(\pi_\xi) \subseteq \{\pm \mathrm{id}\}$. Since S generates G, we can chose ξ such that $\xi = s_0 g$ with $s_0 \in S$ and $g \in G$, with π_g not injective. As before we obtain

$$|S^2 \cap gTg^{-1}| \gg |S|^{1/3-O(\delta)}.$$

But then $T' := g^{-1}(S^2 \cap gTg^{-1})g \subset T$ and by injectivity of π_ξ we obtain

$$|\pi_\xi(S \times T')| \geqslant \frac{1}{4}|S| \cdot |T'| = \frac{1}{4} \cdot |S| \cdot |S^2 \cap gTg^{-1}| \gg |S|^{4/3-O(\delta)}.$$

Let $(s, t) \in S \times T'$, so that

$$(s, t) = (s, g^{-1}s_1 s_2 g)$$

for some $s_1, s_2 \in S$. Then $\pi_\xi(s, t) = ss_0 s_1 s_2 s_0^{-1} \in S^5$ and we conclude like in the first case. □

6.2 Diameter of $\mathrm{SL}_2(\mathbb{F}_q)$

To conclude, we propose an quick application of Helfgott's Theorem.

Corollary 6.2.1. The diameter of $\mathrm{SL}_2(\mathbb{F}_q)$ with respect to any set of generators is $\log(|\mathrm{SL}_2(\mathbb{F}_q)|)^{O(1)}$.

Proof. By Helfgott's theorem we either have

$$\begin{aligned}|S^{3^m}| &\geqslant |S^{3^{m-1}}|^{1+\delta} \\ &\geqslant |S^{3^{m-1}}|^{(1+\delta)^2} \geqslant \ldots \geqslant |S|^{(1+\delta)^m},\end{aligned}$$

either $(S^{3^{m-1}} \cup S^{-3^{m-1}} \cup \{e\})^k = G$. Hence if we choose m to be

$$m = \lfloor \log_{(1+\delta)}(\log_{|S|}|G|)\rfloor + 1 = \lfloor \frac{\log\left(\frac{\log|G|}{\log|S|}\right)}{\log(1+\delta)}\rfloor + 1$$

we have $(S^{3^{m-1}} \cup S^{-3^{m-1}} \cup \{e\})^k = G$, which means that the diameter of $(S^{3^{m-1}} \cup S^{-3^{m-1}} \cup \{e\})$ is smaller than k. Clearly we have

$$(S^{3^{m-1}} \cup S^{-3^{m-1}} \cup \{e\}) \subseteq (S \cup S^{-1} \cup \{e\})^{3^{m-1}},$$

and we see that the diameter of $S \cup S^{-1}$ is smaller than $O\left(k\left(\frac{\log|G|}{\log|S|}\right)^{O(1/\log\delta)}\right) = O\left(\log(|G|)^{O(1/\log\delta)}\right)$. By Theorem 4.3 we obtain that the diameter of S is at most $O\left(\log(|G|)^{O(2/\log\delta)+3}\right)$, δ absolute. □

Bibliography

[Bab06] László Babai. On the diameter of eulerian orientations of graphs. In *Proceedings of the seventeenth annual ACM-SIAM symposium on Discrete algorithm*, pages 822–831. Society for Industrial and Applied Mathematics, 2006.

[BKT04] J. Bourgain, N. Katz, and T. Tao. A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.*, 14(1):27–57, 2004.

[BML98] Garrett Birkhoff and Saunders Mac Lane. *A survey of modern algebra*. AK Peters/CRC Press, 1998.

[Bou72] N. Bourbaki. *Éléments de mathématique. Fasc. XXXVII. Groupes et algèbres de Lie. Chapitre II: Algèbres de Lie libres. Chapitre III: Groupes de Lie*. Hermann, Paris, 1972. Actualités Scientifiques et Industrielles, No. 1349.

[Del74] Pierre Deligne. La conjecture de weil. i. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 43(1):273–307, 1974.

[FH13] William Fulton and Joe Harris. *Representation theory: a first course*, volume 129. Springer Science & Business Media, 2013.

[Hel08] H. A. Helfgott. Growth and generation in $SL_2(Z/pZ)$. *Ann. of Math. (2)*, 167(2):601–623, 2008.

[Hel11] H. A. Helfgott. Growth in $SL_3(\mathbb{Z}/p\mathbb{Z})$. *J. Eur. Math. Soc. (JEMS)*, 13(3):761–851, 2011.

[Hel15] Harald A. Helfgott. Growth in groups: ideas and perspectives. *Bull. Amer. Math. Soc. (N.S.)*, 52(3):357–413, 2015.

[HIS07a] Derrick Hart, Alex Iosevich, and Jozsef Solymosi. Sum-product estimates in finite fields via Kloosterman sums. *Int. Math. Res. Not. IMRN*, (5):Art. ID rnm007, 14, 2007.

[HIS07b] Derrick Hart, Alex Iosevich, and Jozsef Solymosi. Sum-product estimates in finite fields via kloosterman sums. *International Mathematics Research Notices*, 2007(9):rnm007–rnm007, 2007.

[K+26] HD Kloosterman et al. On the representation of numbers in the form ax2+ by2+ cz2+ dt2. *Acta mathematica*, 49(3-4):407–464, 1926.

[LW54] Serge Lang and André Weil. Number of points of varieties in finite fields. *Amer. J. Math.*, 76:819–827, 1954.

[PS14] László Pyber and Endre Szabó. Growth in linear groups. *Thin groups and superstrong approximation*, 61:253–268, 2014.

[Sha18] George Shakan. On higher energy decompositions and the sum-product phenomenon. *arXiv preprint arXiv:1803.04637*, 2018.

[Sol09] József Solymosi. Bounding multiplicative energy by the sumset. *Adv. Math.*, 222(2):402–408, 2009.

[TV06] Terence Tao and Van Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

[V+12] Salil P Vadhan et al. Pseudorandomness. *Foundations and Trends® in Theoretical Computer Science*, 7(1–3):1–336, 2012.

[Wei48] André Weil. On some exponential sums. *Proc. Nat. Acad. Sci. U. S. A.*, 34:204–207, 1948.