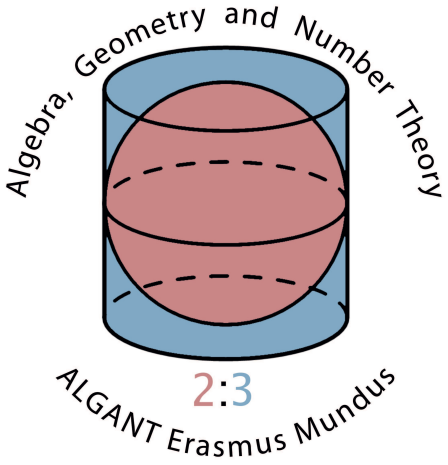
Université de Bordeaux



Diameter of linear groups (after Helfgott)

Oleksandra Gasanova

Advisor: prof. Yuri Bilu

université de BORDEAUX

July, 2015

Contents

1 Introduction

Let G be a finite group. Let $H \subset G$ be a symmetric set of generators of G. By definition, every $x \in G$ can be expressed as a product of elements of H. We would like to know the length of the longest product that might be needed; in other words, we wish to bound from above the diameter $\mathrm{diam}(\Gamma(G,H))$ of the Cayley graph of G with respect to H. (The *Cayley graph* $\Gamma(G,H)$ is the graph (V,E) with the vertex set $V = G$ and the edge set $E = \{(hg, g) : g \in G, h \in H\}$. The *diameter* of a graph $X = (V,E)$ is $\max_{v_1,v_2 \in V} d(v_1,v_2)$, where $d(v_1,v_2)$ is the length of the shortest path between v_1 and v_2 in X).

If G is abelian, the diameter can be very large: if G is cyclic of order $2n+1$, and g is any generator of G, then g^n can not be expressed as a product of length less than n of the elements of $\{g, g^{-1}\}$. However, if G is non-abelian and simple, the diameter is believed to be quite small:

Conjecture 1.1 (Babai, [7]) *For every non-abelian finite simple group G and for any generating set H of G we have*

$$diam(\Gamma(G,H)) \ll (log|G|)^C,$$

where C is some absolute constant and $|G|$ is the number of elements of G.

This conjecture is far from being proved in general. In this paper we will see the proof of this conjecture for $G = SL_2(\mathbf{F}_p)$ (though it's not a simple group, we remark that proving the statement for $G = SL_2(\mathbf{F}_p)$ is equivalent to proving it for $G = PSL_2(\mathbf{F}_p)$ and treating the former group is both slightly more conventional and notationally simpler). The main result of this paper is the following:

Theorem 1.2 (Helfgott) *Let p be a prime number, $H \subset SL_2(\mathbf{F}_p)$ a symmetric generating subset of $SL_2(\mathbf{F}_p)$ containing 1. Then the triple product set $H^{(3)} = H \cdot H \cdot H$ satisfies either $H^{(3)} = SL_2(\mathbf{F}_p)$ or*

$$|H^{(3)}| \geq |H|^{1+\delta},$$

where $\delta = 1/3024$.

The interpretation of this theorem is usually that a subset $H \subset SL_2(F_p)$ "grows" significantly under product, in the sense that

$$\frac{|H^{(3)}|}{|H|} \geq |H|^{\delta},$$

unless it can not grow for relatively obvious reasons: either H is contained in a proper subgroup, or it is already so large that the triple product is all of $SL_2(\mathbf{F}_p)$. Here is a corollary which proves Babai's conjecture for $SL_2(\mathbf{F}_p)$:

Corollary 1.3 (Explicit solution to Babai's conjecture for $SL_2(\mathbf{F}_p)$) *. For any prime number p and any symmetric generating set H of $SL_2(\mathbf{F}_p)$, we have*

$$diam\Gamma(SL_2(\mathbf{F}_p), H) \leq 3(\log |SL_2(\mathbf{F}_p)|)^C$$

with $C = 3323$.

2 Preliminary information

2.1 Notation

1. $|X|$ denotes the cardinality of X.
2. If X and Y are 2 subsets of a group, then $X \cdot Y$ denotes the product set, i.e., $X \cdot Y = \{x \cdot y \mid x \in X, y \in Y\}$.
3. For a subset $H \subset G$ of a group G, we write $H^{(n)}$ for the n-fold product set

$$H^{(n)} = \{x \in G \mid x = h_1 \cdots h_n,\ h_i \in H\}.$$

Note the immediate relations

$$(H^{(n)})^{(m)} = H^{(nm)}, H^{(n+m)} = H^{(n)} \cdot H^{(m)}$$

for $n, m \geq 0$ and $(H^{(n)})^{-1} = H^{(n)}$ is H is symmetric. In addition, if $1 \in H$, we have $H^{(n)} \subset H^{(m)}$ for all $m \geq n$

4. We denote by $trp(H)$ the "tripling constant" of a subset $H \subset G$, defined by

$$trp(H) = \frac{|H^{(3)}|}{|H|}.$$

2.2 Elementary estimates in groups

Lemma 2.1 (Ruzsa) *Let G be a finite group and let $H \subset G$ be a symmetric non-empty subset.*

1. *Denoting*

$$\alpha_n = \frac{|H^{(n)}|}{|H|},$$

for all n≥3 we have

$$\alpha_n \leq \alpha_3^{n-2} = trp(H)^{n-2}.$$

2. *We have $trp(H^{(2)}) \leq trp(H)^4$ and for all $k \geq 3$ we have*

$$trp(H^{(k)}) \leq trp(H)^{3k-3}.$$

Proof:

1. We want to prove this inequality by induction. For $n = 3$ it obviously holds. We assume that it holds for some n and prove it for $n + 1$.

We define the Ruzsa distance between sets:

$$d(A, B) = \log \frac{|A \cdot B^{-1}|}{\sqrt{|A||B|}}.$$

The Ruzsa distance, while not truly a distance function ($d(A, A) \neq 0$ in general), does satisfy the triangle inequality (it can be checked). We use this inequality in the following form:

$$\exp(d(H^{(n-1)}, H^{(2)})) \leq \exp(d(H^{(n-1)}, H^{(1)})) \cdot \exp(d(H^{(1)}, H^{(2)})),$$

which is equivalent to

$$\frac{|H^{(n+1)}|}{\sqrt{|H^{(n-1)}||H^{(2)}|}} \leq \frac{|H^{(3)}|}{\sqrt{|H||H^{(2)}|}} \frac{|H^{(n)}|}{\sqrt{|H^{(n-1)}||H|}},$$

and so

$$|H^{(n+1)}| \geq \frac{|H^{(3)}||H^{(n)}|}{|H|}$$

(recall that all our sets are symmetric and so we can write B instead of B^{-1}). From this inequality we get

$$\alpha_{n+1} = \frac{|H^{n+1}|}{|H|} \leq \frac{|H^{(3)}||H^{(n)}|}{|H|^2} = \alpha_3\alpha_n \leq \alpha_3\alpha_3^{n-2} = \alpha_3^{n-1}.$$

2. We have

$$trp(H^{(k)}) = \frac{\alpha_{3k}}{\alpha_k}.$$

Since $\alpha_k \geq \alpha_3$ for $k \geq 3$, we obtain

$$trp(H^{(k)}) = \frac{\alpha_{3k}}{\alpha_k} \leq \frac{\alpha_{3k}}{\alpha_3} \leq \frac{\alpha_3^{3k-2}}{\alpha_3} = \alpha_3^{3k-3} = trp(H)^{3k-3}$$

(here we used part 1, putting $n = 3k$).

For $k \geq 2$ we have $\alpha_2 \geq 1$ and so we get

$$trp(H^{(2)}) = \frac{\alpha_6}{\alpha_2} \leq \alpha_6 \leq \alpha_3^4 = trp(H)^4$$

(here we used part 1, putting $n = 6$).

□

We first use Ruzsa's lemma to show that Helfgott's theorem holds when $|H|$ is small, in the following sense:

Proposition 2.2 *Let G be a finite group and let H be a symmetric generating set of G containing 1. If $H^{(3)} \neq G$, then we have $|H^{(3)}| \geq 2^{1/2}|H|$.*

Proof: $H^{(3)} \neq G \Rightarrow H^{(3)} \neq H^{(2)}$ (otherwise, if $H^{(3)} = H^{(2)}$ then we have $G \neq H^{(3)} = H^{(4)} = H^{(5)} = \ldots$ which is a contradiction since H is a generating set of G). We fix some $x \in H^{(3)} - H^{(2)}$ and consider the injective map

$$i : \begin{cases} H \to G \\ h \mapsto hx \end{cases}.$$

The image of this map is contained in $H^{(4)}$ and it's disjoint with H (otherwise, if they intersect, $h_1x = h_2$, $h_1, h_2 \in H \Rightarrow x = h_1^{-1}h_2 \in H^{(2)}$. Hence $H^{(4)}$, which contains both H and the image of i, satisfies $|H^{(4)}| \geq 2|H|$ Hence, by Ruzsa's Theorem ($n = 4$) we obtain

$$(trp(H))^{4-2} \geq \alpha_4 = \frac{|H^{(4)}|}{|H|} \Rightarrow trp(H) \geq \left(\frac{|H^{(4)}|}{|H|}\right)^{1/2} \geq 2^{1/2}.$$

□

Theorem 2.3 (the orbit-stabilizer theorem) *Let G be a finite group acting on a non-empty finite set X. Fix some $x \in X$ and let $K \subset G$ be the stabilizer of x in G. For any non-empty symmetric subset $H \subset G$ we have*

$$|K \cap H^{(2)}| \geq \frac{|H|}{|H \cdot x|},$$

where $H \cdot x = \{h \cdot x \mid h \in H\}$.

Note that since H is symmetric, $1 \in K \cap H^{(2)}$.

Proof: Consider the orbit map, but restricted to H :

$$\phi : \left\{ \begin{array}{c} H \to X \\ h \mapsto h \cdot x \end{array} \right. .$$

Using the fibers of this map to count the number of elements in H, we get

$$|H| = \sum_{y \in \phi(H)} |\phi^{-1}(y)|.$$

But the image of ϕ is $\phi(H) = H \cdot x$ and we have

$$|\phi^{-1}(y)| \leq |K \cap H^{(2)}|$$

for all y (indeed, if $y = \phi(h_0), h_0 \in H$, then all elements $h \in H$ with $\phi(h) = y$ satisfy $h_0^{-1}h \in K \cap H^{(2)}$). Therefore we get

$$|H| \leq |H \cdot x||K \cap H^{(2)}|,$$

as claimed □

Theorem 2.4 *Let G be a finite group, $K \subset G$ its subgroup, $H \subset G$ an arbitrary symmetric subset. For any $n \geq 1$ we have:*

$$\frac{|H^{(n+1)}|}{|H|} \geq \frac{|H^{(n)} \cap K|}{|H^{(2)} \cap K|}.$$

Proof: Let $X \subset G/K$ be the set of cosets of K intersecting H:

$$X = \{xK \in G/K \mid xK \cap H \neq \emptyset\}.$$

We can estimate the size of this set from below by splitting H into its intersections with cosets of K: we have

$$|H| = \sum_{xK \in X} |H \cap xK|.$$

But for any $xK \in X$ fixing some $g_0 \in xK \cap H$ we have $g^{-1}g_0 \in K \cap H^{(2)}$ if $g \in xK \cap H$, hence

$$|xK \cap H| \leq |K \cap H^{(2)}|,$$

so that from the above splitting we will get:

$$|H| = \sum_{xK \in X} |H \cap xK| \leq \sum_{xK \in X} |K \cap H^{(2)}| = |K \cap H^{(2)}||X|,$$

and so we have the lower bound

$$|X| \geq \frac{|H|}{|K \cap H^{(2)}|}.$$

Now take once more some $xK \in X$ and fix an element $xk = h \in xK \cap H$. Then all the elements xkg are distinct for $g \in G$ and they are in $xK \cap H^{(n+1)}$ if $g \in K \cap H^{(n)}$, so that

$$|xK \cap H^{(n+1)}| \geq |K \cap H^{(n)}|$$

for any $xK \in X$ and (cosets being disjoint)

$$|H^{(n+1)}| \geq |X||K \cap H^{(n)}| \geq \frac{|H|}{|K \cap H^{(2)}|}|K \cap H^{(n)}|,$$

which is the result we need. □

Theorem 2.5 *For a prime $p \geq 3$, if a subset $H \subset SL_2(\mathbf{F}_p)$ satisfies*

$$|H| \geq 2|SL_2(\mathbf{F}_p)|^{8/9},$$

we have $H^{(3)} = SL_2(\mathbf{F}_p)$.

The proof of this theorem can be found in [2, §4.5].

2.3 Tori, semisimple elements, involved sets

Definition: Fix a prime number p and let $G = SL_2(\mathbf{F}_p), \mathbf{G} = SL_2(\bar{\mathbf{F}}_p)$

1. A *semisimple* element $g \in \mathbf{G}$ is an element which is diagonalizable (in some basis). A *regular* semisimple element is a semisimple element with distinct eigenvalues. For any subset $H \subset \mathbf{G}$, we write H_{reg} for the set of the regular semisimple elements in H.
2. A *maximal torus* in $\mathbf{G}$ is a subgroup of $\mathbf{G}$ which is a conjugate of the subgroup
$$D = \left\{ \begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix} \mid d \in \bar{\mathbf{F}}_p^{\times} \right\}.$$
of diagonal matrices. Equivalently, a maximal torus in $\mathbf{G}$ is the centralizer of a regular semisimple element.
3. Let $p > 3$. A *maximal torus* T in G is a subgroup of the form $T = \mathbf{T} \cap G$, where $\mathbf{T}$ is a maximal torus in $\mathbf{G}$ such that $\mathbf{T} \cap G \neq \{\pm 1\}$ Equivalently, a maximal torus in G is a maximal commutative subgroup in G which becomes diagonalizable over some field extension (actually, it's equivalent to require diagonalizability over a quadratic extension).

There are 2 conjugacy classes of maximal tori in $G = SL_2(\mathbf{F}_p)$. The first class consists of those tori which are already diagonalizable over $\mathbf{F}_p$ or equivalently, those are the tori that are conjugated to the standard diagonal torus

$$A = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbf{F}_p^{\times} \right\}.$$

A maximal torus in this class is called a split torus. The second class consists of those maximal tori which are not diagonalizable over $\mathbf{F}_p$. These tori are not conjugated to A. A maximal torus in this class is called a non-split torus.

Properties:

1. A split maximal torus in G is a cyclic group with $p-1$ elements, while a non-split maximal torus is a cyclic group with $p+1$ elements.
2. A regular semisimple element $x \in \mathbf{G}$ is contained in a unigue maximal torus $\mathbf{T}$, namely its centralizer $\mathbf{T} = C_{\mathbf{G}}(x)$. In particular, if $\mathbf{T} \neq \mathbf{S}$ are 2 maximal tori, we have
$$\mathbf{T}_{reg} \cap \mathbf{S}_{reg} = \emptyset$$
3. If $\mathbf{T} \subset \mathbf{G}$ is a maximal torus, we have
$$|\mathbf{T} - \mathbf{T}_{reg}| = 2$$
4. For any maximal torus $\mathbf{T}$, its normalizer $N_{\mathbf{G}}(\mathbf{T})$ contains $\mathbf{T}$ as a subgroup of index 2. Similarly, for any maximal torus $T \in G$, its normalizer $N_G(T)$ contains T as a subgroup of index 2 and in particular
$$2(p-1) \leq |N_G(T)| \leq 2(p+1)$$
5. The conjugacy class $\mathbf{Cl}(g)$ of a regular semisimple element $g \in \mathbf{G}$ is the set of all $x \in \mathbf{G}$ such that $tr(x) = tr(g)$. The set of elements in $\mathbf{G}$ which are not regular semisimple is the set of all $x \in \mathbf{G}$ such that $tr(x)^2 = 4$

Remark: For general facts about finite groups of Lie type, one may look at [4] or [6] and for conjugacy classes of $SL_2(\mathbf{F}_p)$ one may look at [5].

Definition: Let p be a prime number, $H \subset SL_2(\mathbf{F}_p)$, and $\mathbf{T} \subset SL_2(\bar{\mathbf{F}}_p)$ a maximal torus. Then $\mathbf{T}$ is *involved* with H (or H is involved with $\mathbf{T}$) if and only if H contains a regular semisimple element of $\mathbf{T}$ with non-zero trace, i.e., $H \cap \mathbf{T}_{sreg} \neq \emptyset$, where the subscript "sreg" means regular semisimple elements with non-zero trace.

Two important tools in the proof of our growth theorem are estimates for escape from subvarieties and estimates for non-concentration in subvarieties. In the next section we state and prove the special cases that we need for our main result.

3 The first main tool: Escape theorem

Theorem 3.1 (Escape) *Let $p \geq 7$ be a prime number and let $H \subset SL_2(\mathbf{F}_p)$ be a symmetric generating set with $1 \in H$. Then $(H^{(3)})_{sreg} \neq \emptyset$, i.e., the three-fold product set $H^{(3)}$ contains a regular semisimple element x with non-zero trace. In particular, there exists a torus $\mathbf{T} = \mathbf{C}_{\mathbf{G}}(x)$ involved with $H^{(3)}$.*

Proof: Let N be the set of elements in $SL_2(\mathbf{F}_p)$ that are not regular semisimple. This is the union of the 2 central elements ± 1 and 4 conjugacy classes of

$$u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, v = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, u' = \begin{pmatrix} 1 & \epsilon \\ 0 & 1 \end{pmatrix}, v' = \begin{pmatrix} -1 & \epsilon \\ 0 & -1 \end{pmatrix},$$

where $\epsilon \in \mathbf{F}_p^{\times}$ is a fixed non-square. This set is invariant under $SL_2(\mathbf{F}_p)$ - conjugation and is the set of all matrices with trace equal to ± 2. Elements with trace 0 are conjugates of

$$g_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Next we note that if this theorem holds/fails for H, then it also holds/fails for all conjugates of H, so we can "normalize" at least 1 element to a specific representative of its conjugacy class. Now we assume that $(H^{(3)})_{sreg}$ is empty and $p \geq 7$ and derive a contradiction. We distinguish 2 cases:

Case 1: Assume that H contains at least 1 element with trace ± 2 which is not ± 1. The observation above shows that we can assume that one of u, v, u', v' is in H. Suppose $u \in H$. Since H is a symmetric generating set, it must contain some element

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

with $c \neq 0$, since otherwise all elements of H would be upper-triangular and H will not be a generating set. Then $H^{(3)}$ contains

$$ug, u^2g, u^{-1}g, u^{-2}g,$$

which have traces, respectively, equal to

$$tr(g) + c, tr(g) + 2c, tr(g) - c, tr(g) - 2c.$$

Since $c \neq 0$ and p is not 2 or 3, these traces are distinct and since there are 4 of them, at least one is not in {-2, 0, 2}. A similar argument holds if $v \in H$ or $u' \in H$ or $v' \in H$.

Case 2: In this case all elements of H except ± 1 have trace 0. We split our proof into 2 subcases depending on properties of $\mathbf{F}_p$.

Subcase 2.1: -1 is not a square in $\mathbf{F}_p$. Conjugating again, we can assume that $g_0 \in H$. Since H generates $SL_2(\mathbf{F}_p)$, there exists $g \in H$ such that $g \neq \pm 1, \pm g_0$. If

$$g = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in H$$

is such an element, then we have $a \neq 0$, since otherwise $b = -c^{-1}$ and the trace of

$$g_0 g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -c^{-1} \\ c & 0 \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & c^{-1} \end{pmatrix}$$

is $c + c^{-1}$ which is not in {-2, 0, 2} ($c + c^{-1} = 2 \Leftrightarrow c = 1, c + c^{-1} = -2 \Leftrightarrow c = -1$, in these 2 cases $g = \pm g_0$; $c + c^{-1} = 0 \Leftrightarrow c^2 + 1 = 0$ - no solutions since -1 is not a square), so $H^{(2)}_{sreg} \neq \emptyset$, contrary to the

assumption. Moreover, we can find g as above with $b \neq c$, otherwise all matrices in H (except g_0) would have the form

$$\begin{pmatrix} a & b \\ b & -a \end{pmatrix},$$

and all matrices of this type belong to the normalizer of a non-split maximal torus. Indeed, if we take a torus T which contains g_0 and conjugate it by the matrix

$$\begin{pmatrix} a & b \\ b & -a \end{pmatrix}$$

(all matrices have determinant 1, of course), we'll get

$$\begin{pmatrix} a & b \\ b & -a \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -a & -b \\ -b & a \end{pmatrix} = \begin{pmatrix} ba - ab & a^2 + b^2 \\ -(b^2 + a^2) & ba - ab \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and the resulting matrix is just the inverse of the initial one (in particular, it also belongs to T). Obviously, g_0 also belongs to the normalizer of this torus. Therefore, H will belong to this subgroup and so it will not be a generating set. It means, we can find g as above (with $a \neq 0, b \neq c$). We have

$$g_0 g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \begin{pmatrix} c & -a \\ -a & -b \end{pmatrix} \in H^{(2)}$$

with nonzero trace $t = c - b$. If $t = 2$, i.e., $c = b + 2$, the condition $\det(g_0 g) = 1$ implies

$$-2b - b^2 - a^2 = 1,$$

or $(b+1)^2 = -a^2$. Similarly, if $t = -2$, we get $(b-1)^2 = -a^2$. Since $a \neq 0$, it follows in both cases that -1 is a square in $\mathbf{F}_p$, which is a contradiction

Subcase 2.2: $-1 = z^2$ is a square in $\mathbf{F}_p$. Then we can diagonalize g_0 over $\mathbf{F}_p$ and conjugating again, assume that H contains

$$g_0' = \begin{pmatrix} z & 0 \\ 0 & -z \end{pmatrix}$$

Also H contains other matrices of type

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

We distinguish 2 different types of matrices: if $a = 0$, then we have matrices of type

$$\begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix}$$

(let's call them "quasi-diagonal"); if we have a matrix

$$g' = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$$

with $a \neq 0$, we will have that the trace of

$$g_0' g' = \begin{pmatrix} z & 0 \\ 0 & -z \end{pmatrix} \begin{pmatrix} a & b \\ c & -a \end{pmatrix} = \begin{pmatrix} za & zb \\ -zc & za \end{pmatrix} \in H^{(2)}$$

is $2za$ which should be ± 2 (otherwise we are done), therefore $za = \pm 1$ which implies $-a^2 = 1$, (so $a = \pm z$) and since $1 = \det(g') = -a^2 - bc = 1 - bc$, we get that $bc = 0$ for all matrices of this type (and g_0' also belongs to this type). Clearly, H contains matrices of type 2 except $\pm g_0'$, otherwise H would contain only diagonal

(and, perhaps, quasi-diagonal) matrices and thus will not be a generating set. Now we distinguish 2 cases. First case is if H contains a quasi-diagonal matrix

$$h = \begin{pmatrix} 0 & -d^{-1} \\ d & 0 \end{pmatrix}$$

and, as we have just figured out, H must contain a matrix of type 2 which is not $\pm g_0'$ (let it be $h' = \begin{pmatrix} \pm z & b \\ 0 & \mp z \end{pmatrix}$ with $b \neq 0$, for a lower triangular matrix the proof is similar). Then we will have:

$$h'h = \begin{pmatrix} \pm z & b \\ 0 & \mp z \end{pmatrix} \begin{pmatrix} 0 & -d^{-1} \\ d & 0 \end{pmatrix} = \begin{pmatrix} bd & \mp zd^{-1} \\ \mp zd & 0 \end{pmatrix},$$

$$g_0'h'h = \begin{pmatrix} z & 0 \\ 0 & -z \end{pmatrix} \begin{pmatrix} bd & \mp zd^{-1} \\ \mp zd & 0 \end{pmatrix} = \begin{pmatrix} zbd & \pm d^{-1} \\ \mp d & 0 \end{pmatrix},$$

$tr(h'h) = bd$, $tr(g_0'h'h) = zbd$. The traces of these matrices are both non-zero; if $tr(h'h)^2 = tr(g_0'h'h)^2 = 4$ it means that $z = \pm 1$ which is a contradiction since z is a square root of -1 and $p \neq 2$. Now assume that H doesn't contain quasi-diagonal matrices. So all matrices in H are of type 2. Then for all matrices in H we have $bc = 0$. If all matrices in H satisfy $b = 0$, then H would be contained in the subgroup of upper triangular matrices. So there exists a matrix in $x \in H$ with $b \neq 0$, hence $c = 0$

$$x = \begin{pmatrix} a & b \\ 0 & -a \end{pmatrix}$$

(Note that $a = z$ or $a = -z$, but we can always choose a matrix with $a = z$ (otherwise, if $a = -z$ we just replace x with x^{-1} which is also in H since H is symmetric). So, in H we have a matrix

$$x = \begin{pmatrix} z & b \\ 0 & -z \end{pmatrix}$$

with $b \neq 0$. Similarly, H contains a matrix

$$y = \begin{pmatrix} z & 0 \\ c & -z \end{pmatrix}$$

with $c \neq 0$. Then we have:

$$xy = \begin{pmatrix} z & b \\ 0 & -z \end{pmatrix} \begin{pmatrix} z & 0 \\ c & -z \end{pmatrix} = \begin{pmatrix} -1 + bc & -bz \\ -cz & -1 \end{pmatrix},$$

$$g_0'xy = \begin{pmatrix} z & 0 \\ 0 & -z \end{pmatrix} \begin{pmatrix} -1 + bc & -bz \\ -cz & -1 \end{pmatrix} = \begin{pmatrix} -z + bcz & b \\ -c & z \end{pmatrix}$$

The traces of these matrices are $bc-2$ and bcz, respectively. The interesting cases are when $bc-2 \in \{0, 2, -2\}$, i.e, when $bc \in \{0, 2, 4\}$. Obviously, $bc = 0$ is impossible. If $bc = 2$, then $bcz = 2z \notin \{0, 2, -2\}$ (again, since $p \neq 2$), if $bc = 4$, then $bcz = 4z \notin \{0, 2, -2\}$ (this is possible only if $2z \in \{0, 1, -1\}$, so, $4z^2 = -4 \in \{0, 1\}$, i.e., either $-4 = 0$ ($p = 2$) or $-4 = 1$ ($p = 5$)). Again we have obtained a contradiction which completes the proof of the theorem. $\square$

4 The second main tool: Non-concentration inequality

4.1 Preparation lemmas

The main idea that we will use here is the following: we would like to estimate from above the cardinality of $\mathbf{Cl}(g) \cap H$. We will use the following technique: we will define a map from $(\mathbf{Cl}(g))^3$ to $\mathbf{G}^2$ and then restrict it to $(\mathbf{Cl}(g) \cap H)^3$. Then the cardinality of $(\mathbf{Cl}(g) \cap H)^3$ (and thus, of $\mathbf{Cl}(g) \cap H$) can be estimated from above using the fibers of this map. We will start with the following lemma:

Lemma 4.1 *Let k be any field, $G = SL_2(k)$. Let $C \subset G$ be a conjugacy class, and define*

$$\phi : \begin{cases} C^3 \to G^2 \\ (x_1, x_2, x_3) \mapsto (x_1 x_2, x_1 x_3) \end{cases} .$$

Then for any $(y_1, y_2) \in G \times G$, we have a bijection

$$\begin{cases} C \cap y_1 C^{-1} \cap y_2 C^{-1} \to \phi^{-1}(y_1, y_2) \\ x_1 \mapsto (x_1, x_1^{-1} y_1, x_1^{-1} y_2) \end{cases} .$$

In particular, if $k = \bar{\mathbf{F}}_p$ and C is a regular semisimple conjugacy class, we have a bijection

$$\phi^{-1}(y_1, y_2) \to C \cap y_1 C \cap y_2 C.$$

Proof: Take an element in $\phi^{-1}(y_1, y_2)$. It's a triple in C^3. From this triple we can uniquely determine x_1 and vice versa, given x_1 we can uniquely determine the whole triple in the fiber ($x_2 = x_1^{-1} y_1$, $x_3 = x_1^{-1} y_2$). Therefore, elements of the fiber (triples) are in 1 to 1 correspondence with all the proper x_1's. What are the proper x_1's? The triple should belong to C^3 which is equivalent to this condition:

$$x_1 \in C,\ x_1^{-1} y_1 \in C,\ x_1^{-1} y_2 \in C \Leftrightarrow x_1 \in C \cap y_1 C^{-1} \cap y_2 C^{-1},$$

which proves the first part. For the second part, simply notice that if C is a regular semisimple conjugacy class, say, that of g, then $C = C^{-1}$ because g^{-1} has the same characteristic polynomial as g, hence is conjugate to g. □

Now we have seen that for $k = \bar{\mathbf{F}}_p$ the fibers of this map are in bijection with sets of type $C \cap y_1 C \cap y_2 C$. Therefore, we would like to know something about them. The main question is: how big are they? The next theorem gives us the answer to this question.

Theorem 4.2 (Pink) *Let K be an algebraically closed field with $char(K) \neq 2$, $g \in SL_2(K)$ a regular semisimple element with nonzero trace and C is the conjugacy class of g. For $y_1, y_2 \in SL_2(K)$ the intersection $X = C \cap y_1 C \cap y_2 C$ is finite and contains at most 2 elements unless one of the following holds:*

1. *We have $y_1 = 1$ or $y_2 = 1$ or $y_1 = y_2$;*
2. *There exists $x \in SL_2(K)$ such that*

$$y_1 = x \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} x^{-1}$$

and we have several (classes of) possibilities for y_2:

$$y_2 = x \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} x^{-1},$$

$$y_2 = x \begin{pmatrix} \alpha^2 & * \\ 0 & \alpha^{-2} \end{pmatrix} x^{-1},$$

$$y_2 = x \begin{pmatrix} \alpha^{-2} & * \\ 0 & \alpha^2 \end{pmatrix} x^{-1},$$

where $\alpha + \alpha^{-1} = tr(g)$.

3. *There exists* $x \in SL_2(K)$ *such that*

$$y_1 = x \begin{pmatrix} \alpha^2 & 0 \\ 0 & \alpha^{-2} \end{pmatrix} x^{-1}$$

and we have several possibilities for y_2*:*

$$y_2 = x \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} x^{-1},$$

$$y_2 = x \begin{pmatrix} \alpha^2 & * \\ 0 & \alpha^{-2} \end{pmatrix} x^{-1},$$

$$y_2 = x \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} x^{-1},$$

$$y_2 = x \begin{pmatrix} \alpha^2 & 0 \\ * & \alpha^{-2} \end{pmatrix} x^{-1},$$

where $\alpha + \alpha^{-1} = tr(g)$.

For each pair (y_1, y_2) *described in cases 2 and 3 we have that* $X \subset C \cap \mathbf{B}$*, where* $\mathbf{B}$ *is a conjugate of* $\mathbf{B_0}$ *(the subgroup of upper triangular matrices) and* $\mathbf{B}$ *is uniquely determined by* (y_1, y_2).

Proof: It will be convenient to compute the intersection $C \cap y_1^{-1} C \cap y_2^{-1} C$ (just a change of notation). The results we will find will concern y_1 and y_2 (and now we need them for y_1^{-1} and y_2^{-1}), but it's not a problem: proving that $y_1 = 1$ or $y_2 = 1$ or $y_1 = y_2$ is equivalent to proving that $y_1^{-1} = 1$ or $y_2^{-1} = 1$ or $y_1^{-1} = y_2^{-1}$. If we come to the second or third case, again, it's not hard to see that it's equivalent for the pair (y_1^{-1}, y_2^{-1}) to be in the same case, and so we can prove the results for (y_1, y_2) instead of (y_1^{-1}, y_2^{-1}).

The conjugacy class of a regular semisimple element is completely determined by its trace (which is, the conjugacy class of this element is exactly the set of matrices with the same trace). If such an element has trace $t = \alpha + \alpha^{-1}$, then we have $\alpha^4 \neq 1$ (if $\alpha = \pm 1$, then the element is not regular semisimple, if $\alpha^2 = -1$, then the trace is 0 which contradicts our assumptions). So, from now on we work with C which is the set of matrices of trace $t = \alpha + \alpha^{-1}$ where α is as above.

Next observation is that for any $x, y_1 \in SL_2(K)$ we have

$$C \cap (x y_1 x^{-1})^{-1} C = x C x^{-1} \cap x y_1^{-1} x^{-1} C = x C x^{-1} \cap x y_1^{-1} C x^{-1} = x (C \cap y^{-1} C) x^{-1}.$$

This means that we can compute $C \cap y^{-1} C$ up to conjugation (taking a more convenient representative from our conjugacy class).

The conjugacy classes of $SL_2(K)$ are known. We will first run through representatives of these classes and determine the corresponding intersection $C \cap y_1^{-1} C$. We will not deal with the case $y_1 \pm 1$. Indeed, if $y_1 = 1$ we have the first case of our theorem and if $y_1 = -1$, we will get

$$y_1^{-1} C = -C$$

The matrices in C all have trace t while all the matrices in $-C$ have trace $-t$, which means there can't be any intersection (remember that $t \neq 0$), so the theorem obviously holds for $y_1 = -1$ and for any y_2. So, if $y_1 \neq \pm 1$, then it's conjugated to one of the following 4 (types of) elements:

$$y_0^{(1)} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \; y_0^{(2)} = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix},$$

$$y_0^{(3)} = \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix}, \beta \neq \pm 1, \beta \neq \alpha^{\pm 2}$$

$$y_0^{(4)} = \begin{pmatrix} \alpha^2 & 0 \\ 0 & \alpha^{-2} \end{pmatrix}$$

(here the superscript indicates the number of the case and the subscript 0 means that this is the "canonical" representative). Clearly, we could unite the last 2 cases into 1, but later it will become clear how calculations can be simplified if we distinguish them.

Now we want to find out something about $C \cap (y_0^{(i)})^{-1}C$. For each i we'll do the following: take a matrix $h \in C$; the condition that it also belongs to $(y_0^{(i)})^{-1}C$ is equivalent to imposing also the condition $y_0^{(i)}h \in C$. From this we can say something about h and therefore about the whole intersection. Let $h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a + d = t = \alpha + \alpha^{-1}$.

Case $i = 1$:

$$y_0^{(1)}h = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix},$$

$tr(y_0^{(1)}h) = a + c + d = t = a + c = tr(h)$, which implies $c = 0$. Then (since the determinant should be 1) we have $ad = 1$ and $a + d = \alpha + \alpha^{-1}$ which means $a = \alpha, d = \alpha^{-1}$ or $d = \alpha, a = \alpha^{-1}$. So $C \cap (y_0^{(1)})^{-1}C$ is given by the set containing all matrices of the following forms:

$$\begin{pmatrix} \alpha & k \\ 0 & \alpha^{-1} \end{pmatrix}, \begin{pmatrix} \alpha^{-1} & k \\ 0 & \alpha \end{pmatrix},$$

where $k \in K$ is parameter.

Case $i = 2$:

$$y_0^{(2)}h = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a+c & -b+d \\ -c & -d \end{pmatrix},$$

$tr(y_0^{(2)}h) = -a + c - d = t = a + d = tr(h)$, which implies $(-a + c - d) + (a + d) = t + t$, which implies $c = 2t$. Since also $a + d = t$, we parameterize them like this: $a = k, d = t - k$. For the moment h looks like $\begin{pmatrix} k & b \\ 2t & t-k \end{pmatrix}$. Also we impose the condition $det(h) = 1$:

$$ad - bc = 1 \Leftrightarrow k(t-k) - 2tb = 1 \Leftrightarrow -k^2 + kt - 1 = 2tb \Leftrightarrow b = (-k^2 + kt - 1)/2t$$

(recall that $t \neq 0$ and $char(K) \neq 2$). So $C \cap (y_0^{(2)})^{-1}C$ is given by the set containing all matrices of the following form:

$$\begin{pmatrix} k & (-k^2 + kt - 1)/2t \\ 2t & t - k \end{pmatrix},$$

where $k \in K$ is parameter.

Case $i = 3$:

$$y_0^{(3)}h = \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \beta a & \beta b \\ \beta^{-1}c & \beta^{-1}d \end{pmatrix},$$

$tr(y_0^{(3)}h) = \beta a + \beta^{-1}d = t = a + d = tr(h)$, which implies that (a,d) is a solution of the linear system

$$\begin{cases} a + d = t, \\ \beta a + \beta^{-1}d = t. \end{cases}$$

with determinant $\beta^{-1} - \beta \neq 0$. Solving this system we have

$$a = \frac{t}{\beta + 1}, d = \frac{\beta t}{\beta + 1}.$$

Write $b = b'/(\beta+1), c = c'/(\beta+1)$. Now we impose the condition $det(h) = 1$:

$\beta t^2 - b'c' = (\beta+1)^2 \Leftrightarrow -b'c' = \beta^2+2\beta+1-\beta(\alpha+\alpha^{-1})^2 = \beta^2+2\beta+1-\beta\alpha^2-2\beta-\beta\alpha^{-2} = (\beta-\alpha^2)(\beta-\alpha^{-2})$.

In this case $\beta \neq \alpha^{\pm 2}$, so both b' and c' are nonzero and can be parameterized in this way:

$$b' = (\beta-\alpha^2)k,\ c' = -(\beta-\alpha^{-2})k^{-1}.$$

So $C \cap (y_0^{(3)})^{-1}C$ is given by the set containing all matrices of the following form:

$$\frac{1}{\beta+1}\begin{pmatrix} t & (\beta-\alpha^2)k \\ -(\beta-\alpha^{-2})k^{-1} & t\beta \end{pmatrix},$$

where $k \in K^\times$ is a parameter.

Case $i = 4$: in this case we do all the same computations as in the previous one, and we come to the same conditions

$$-c'b' = (\beta-\alpha^2)(\beta-\alpha^{-2}),$$
$$a = \frac{t}{\beta+1},\ d = \frac{\beta t}{\beta+1}.$$

But here $\beta = \alpha^2$ and this implies

$$a = \alpha^{-1},\ d = \alpha,\ b'c' = 0.$$

So, either $c' = 0$ (and hence $c = 0$ and we get upper triangular matrices) or $b' = 0$ (and hence $b = 0$ and we get lower triangular matrices). So $C \cap (y_0^{(4)})^{-1}C$ is given by the set containing all matrices of the following forms:

$$\begin{pmatrix} \alpha^{-1} & k \\ 0 & \alpha \end{pmatrix}, \begin{pmatrix} \alpha^{-1} & 0 \\ k & \alpha \end{pmatrix},$$

where $k \in K$ is parameter.

Now we know how $C \cap y_1^{-1}C$ might look like (up to conjugation). Now we need to find intersections with all possibilities of $y_2^{-1}C$. We proceed exactly as before. y_1 was the conjugate of $y_0^{(i)}$ (say, $y_1 = xy_0^{(i)}x^{-1}$) for some x, and so $C \cap y_1^{-1}C = x(C \cap (y_0^{(i)})^{-1}C)x^{-1}$. A matrix in this set has the form xhx^{-1} where h is as parameterized above (in each case). The condition that it belongs to $y_2^{-1}C =$(write $y_2 = xy'x^{-1}$ for the same x as before and for some y')$= (x(y')^{-1}x^{-1})C$ is equivalent to the condition $y_2xhx^{-1} \in C$ which is $xy'x^{-1}xhx^{-1} = xy'hx^{-1} \in C$ which is equivalent to the condition $y'h \in C$.

Let

$$y' = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$$

Case $i = 1$: For this case, $h = \begin{pmatrix} \alpha & k \\ 0 & \alpha^{-1} \end{pmatrix}$ or $\begin{pmatrix} \alpha^{-1} & k \\ 0 & \alpha \end{pmatrix}$,

$$y'h = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}\begin{pmatrix} \alpha & k \\ 0 & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} x_1\alpha & x_1k + x_2\alpha^{-1} \\ x_3\alpha & x_3k + x_4\alpha^{-1} \end{pmatrix},$$

or

$$y'h = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}\begin{pmatrix} \alpha^{-1} & k \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} x_1\alpha^{-1} & x_1k + x_2\alpha \\ x_3\alpha^{-1} & x_3k + x_4\alpha \end{pmatrix},$$

and so the trace of $y'h$ is $x_3k + x_1\alpha + x_4\alpha^{-1}$, or $x_3k + x_1\alpha^{-1} + x_4\alpha$. If $x_3 \neq 0$, in both cases there is at most 1 value for k for which the trace is equal to t, and so $C \cap y_1C \cap y_2C$ will contain at most 2 elements (1 for each form of the diagonal). If $x_3 = 0$ (and so, $x_4 = x_1^{-1}$), then x_1 is a solution of the following system:

$$\alpha x_1 + \alpha^{-1}x_1^{-1} = t,$$

or

$$\alpha x_1^{-1} + \alpha^{-1} x_1 = t.$$

The first equation gives $x_1 = 1$ and $x_1 = \alpha^{-2}$, so that y' is an upper triangular matrix with diagonal coefficients $(1,1)$ or (α^{-2}, α^2)

The second equation gives $x_1 = 1$ and $x_1 = \alpha^2$, so that y' is an upper triangular matrix with diagonal coefficients $(1,1)$ or (α^2, α^{-2}) (this type of matrices will also appear in case $i = 4$).

We summarize the results of this case:

$$y_1 = x \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} x^{-1}$$

and we have several possibilities for y_2:

$$y_2 = x \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} x^{-1},$$

$$y_2 = x \begin{pmatrix} \alpha^2 & b \\ 0 & \alpha^{-2} \end{pmatrix} x^{-1},$$

$$y_2 = x \begin{pmatrix} \alpha^{-2} & b \\ 0 & \alpha^2 \end{pmatrix} x^{-1},$$

where b is arbitrary, $b \in K$.

Case $i = 2$: For this case, $h = \begin{pmatrix} k & (-k^2 + kt - 1)/2t \\ 2t & t - k \end{pmatrix}$,

$$y'h = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} k & (-k^2 + kt - 1)/2t \\ 2t & t - k \end{pmatrix} = \begin{pmatrix} x_1 k + 2x_2 t & x_1(-k^2 + kt - 1)/2t + x_2(t - k) \\ x_3 k + 2x_4 t & x_3(-k^2 + kt - 1)/2t + x_4(t - k), \end{pmatrix}$$

$$tr(y'h) - t = x_1 k + 2x_2 t + \frac{x_3(-k^2 + kt - 1)}{2t} + x_4(t - k) - t = -\frac{x_3}{2t}k^2 + (x_1 - x_4 + \frac{x_3}{2})k + (x_4 + 2x_2 - 1)t = 0.$$

This equation has at most 2 solutions unless both $x_3 = 0$ and $x_4 = x_1$, but then $x_1 = x_4 = \pm 1$. If $x_4 = 1$ the constant term is 0 if and only if $x_2 = 0$ (and so, $y' = 1$), if $x_4 = -1$, then $x_2 = 1$ and $y' = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = y_0^{(2)}$ and since $y_1 = x y_0^{(2)} x^{-1}$ and $y_2 = x y' x^{-1}$, we have $y_1 = y_2$.

Case $i = 3$: For this case,

$$h = \frac{1}{\beta + 1} \begin{pmatrix} t & (\beta - \alpha^2)k \\ -(\beta - \alpha^{-2})k^{-1} & t\beta \end{pmatrix},$$

$$y'h = \frac{1}{\beta + 1} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} t & (\beta - \alpha^2)k \\ -(\beta - \alpha^{-2})k^{-1} & t\beta \end{pmatrix} = \frac{1}{\beta + 1} \begin{pmatrix} x_1 t - x_2 k^{-1}(\beta - \alpha^{-2}) & x_1 k(\beta - \alpha^2) + x_2 t\beta \\ x_3 t - x_4 k^{-1}(\beta - \alpha^{-2}) & x_3 k(\beta - \alpha^2) + x_4 t\beta \end{pmatrix},$$

$$k(tr(y'h) - t) = \frac{1}{\beta + 1}\left(ktx_1 - x_2(\beta - \alpha^{-2}) + k^2 x_3(\beta - \alpha^2) + kx_4 t\beta\right) - kt =$$

$$= \frac{x_3(\beta - \alpha^2)}{\beta + 1}k^2 + \left(\frac{x_1}{\beta + 1} + \frac{x_4\beta}{\beta + 1} - 1\right)kt - \frac{x_2(\beta - \alpha^{-2})}{\beta + 1} = 0.$$

This equation has more than 2 solutions if and only if all 3 coefficients are 0, which implies $x_2 = x_3 = 0$ (and so $x_4 = x_1^{-1}$), and

$$x_1 + x_4\beta - (\beta + 1) = 0 \Leftrightarrow x_1 + x_1^{-1}\beta - (\beta + 1) = 0 \Leftrightarrow x_1^2 - (\beta + 1)x_1 + \beta = 0.$$

Then either $x_1 = 1$ (and so, $y' = 1$) or $x_1 = \beta, x_4 = \beta^{-1}$, $y' = \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} = y_0^{(3)}$ and since $y_1 = x y_0^{(3)} x^{-1}$ and $y_2 = x y' x^{-1}$, we have $y_1 = y_2$.

Case $i = 4$: For this case, $h = \begin{pmatrix} \alpha^{-1} & 0 \\ k & \alpha \end{pmatrix}$ or $\begin{pmatrix} \alpha^{-1} & k \\ 0 & \alpha \end{pmatrix}$. The second subtype has been seen in case 1. The first subtype leads us to

$$y'h = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & 0 \\ k & \alpha \end{pmatrix} = \begin{pmatrix} x_1\alpha^{-1} + x_2k & x_2\alpha \\ x_3\alpha^{-1} + x_4k & x_4\alpha \end{pmatrix},$$

$tr(y'h) = x_1\alpha^{-1} + x_2k + x_4\alpha$. There is at most 1 value for k when this trace is t, unless $x_2 = 0$. If $x_2 = 0$ (and so, $x_4 = x_1^{-1}$), we will have that x_1 is the solution of

$$\alpha^{-1}x_1 + \alpha x_1^{-1} = 0,$$

which gives $x_1 = 1$ and $x_1 = \alpha^2$, so that y' is a lower triangular matrix with diagonal coefficients $(1, 1)$ or (α^2, α^{-2}). Also y' can be an upper triangular matrix with diagonal coefficients $(1, 1)$ or (α^2, α^{-2}) (this type of matrices has already appeared in case $i = 1$). We summarize the results of this case:

$$y_1 = x \begin{pmatrix} \alpha^2 & 0 \\ 0 & \alpha^{-2} \end{pmatrix} x^{-1}$$

and we have several possibilities for y_2:

$$y_2 = x \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} x^{-1},$$

$$y_2 = x \begin{pmatrix} \alpha^2 & b \\ 0 & \alpha^{-2} \end{pmatrix} x^{-1},$$

$$y_2 = x \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} x^{-1},$$

$$y_2 = x \begin{pmatrix} \alpha^2 & 0 \\ b & \alpha^{-2} \end{pmatrix} x^{-1},$$

where b is arbitrary, $b \in K$.

□

For a prime p and $\gamma \in \bar{\mathbf{F}}_p^{\times}$, define

$$C_\gamma = \left\{ \begin{pmatrix} \gamma & t \\ 0 & \gamma^{-1} \end{pmatrix} \mid t \in \bar{\mathbf{F}}_p \right\}.$$

From the previous theorem we have seen that all y_2's for which case 2 or case 3 holds (but not case 1), are precisely sets which are conjugated to some C_γ. Therefore, we would like to estimate from above the cardinality of $H \cap xC_\gamma x^{-1}$. The next lemma gives us some information about it.

Lemma 4.3 *For any $p \geq 5$, any $\gamma \in \bar{\mathbf{F}}_p^{\times}$, any $x \in SL_2(\bar{\mathbf{F}}_p)$ and any symmetric generating set H of $SL_2(\mathbf{F}_p)$ containing 1, we have:*

$$|H \cap xC_\gamma x^{-1}| = \left| H \cap x \left\{ \begin{pmatrix} \gamma & t \\ 0 & \gamma^{-1} \end{pmatrix} \mid t \in \bar{\mathbf{F}}_p \right\} x^{-1} \right| \leq 2\alpha^2 |H|^{1/3}$$

where $\alpha = trp(H)$.

Proof: We first deal with the fact that x and γ are not necessarily in $SL_2(\mathbf{F}_p)$. We have $xC_\gamma x^{-1} \cap SL_2(\mathbf{F}_p) \subset x\mathbf{B}_0x^{-1} \cap SL_2(\mathbf{F}_p)$, and there are 3 possibilities for the latter: either $x\mathbf{B}_0x^{-1} \cap SL_2(\mathbf{F}_p) = 1$, or $x\mathbf{B}_0x^{-1} \cap SL_2(\mathbf{F}_p) = T$ is a non-split maximal torus of $SL_2(\mathbf{F}_p)$, or $x\mathbf{B}_0x^{-1} \cap SL_2(\mathbf{F}_p) = B$ is an $SL_2(\mathbf{F}_p)$-conjugate of the group $B_0 = \mathbf{B}_0 \cap SL_2(\mathbf{F}_p)$ of upper-triangular matrices (this is a standard property of linear algebraic groups over finite fields).

In the first case there is nothing to do.

In the second case we note that γ and γ^{-1} are the eigenvalues of any element in $SL_2(\mathbf{F}_p) \cap xC_\gamma x^{-1}$ and there are at most 2 elements in a maximal torus with given eigenvalues. Then obviously we have $|H \cap xC_\gamma x^{-1}| \leq 2 \leq 2\alpha^2|H|^{1/3}$.

In the last case we can assume that $x \in SL_2(\mathbf{F}_p)$ and $\gamma \in \mathbf{F}_p$. Using $SL_2(\mathbf{F}_p)$-conjugation, we can assume that $x = 1$. Then either the intersection is empty (and the result is true) or we can fix

$$g_0 = \begin{pmatrix} \gamma & t_0 \\ 0 & \gamma^{-1} \end{pmatrix} \in H \cap C_\gamma$$

and observe that for any $g \in H \cap C_\gamma$ we have

$$g_0^{-1}g \in H^{(2)} \cap C_1,$$

hence

$$|H \cap C_\gamma| \leq |H^{(2)} \cap C_1| = |H^{(2)} \cap \mathbf{U}_0|,$$

which reduces further to the case $\gamma = 1$. We fix an element $h \in H - \mathbf{B}_0$, i.e.,

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $c \neq 0$. It exists, because otherwise $H \subset \mathbf{B} \cap SL_2(\mathbf{F}_p)$ would not be a generating set of $SL_2(\mathbf{F}_p)$. Now we consider the following map:

$$\psi : \begin{cases} \mathbf{U}^* \times \mathbf{U}^* \times \mathbf{U}^* \to \mathbf{G} \\ (u_1, u_2, u_3) \mapsto u_1hu_2h^{-1}u_3 \end{cases}$$

where $\mathbf{U}^* = \mathbf{U}_0 - 1$ (later it will become clear why we can't take $\mathbf{U}_0^3$ as a domain). Note that since $h \in H$, we have $\psi((\mathbf{U}^* \cap H^{(2)})^3) \subset H^{(8)}$. Crucially, we claim that for any $x \in \mathbf{G}$, the fiber $\psi^{-1}(x)$ contains at most 1 element. If this is true, we get

$$|\mathbf{U}^* \cap H^{(2)}|^3 \leq |H^{(8)}| \leq \alpha^6|H|,$$

and therefore

$$|\mathbf{U}_0 \cap H^{(2)}| = |\mathbf{U}^* \cap H^{(2)}| + 1 = 2\alpha^2|H|^{1/3},$$

which is the result we need. Now we prove the claim via direct computation. Precisely, if

$$u_i = \begin{pmatrix} 1 & t_i \\ 0 & 1 \end{pmatrix} \in \mathbf{U}^*,$$

then matrix multiplication leads to

$$\psi(u_1, u_2, u_3) = \begin{pmatrix} 1 - t_1t_2c^2 - t_2ac & * \\ -t_2c^2 & * \end{pmatrix},$$

and since $c \neq 0$, t_2 is uniquely determined (and thus also u_2). Now, t_1 (and so, u_1) is also uniquely determined ($c \neq 0, t_2 \neq 0$ and this is the reason why the domain of our map is not $\mathbf{U}_0^3$). Finally, $u_3 = (u_1hu_2h^{-1})^{-1}x$ is also uniquely determined. $\square$

4.2 Non-concentration inequality

Now we have proved all the preparation lemmas and we can prove the desired non-concentration inequality:

Theorem 4.4 (Non-concentration inequality) *Let $p \geq 3$ be a prime number and let $g \in SL_2(\mathbf{F}_p) = G$ be a regular semisimple element with non-zero trace. Let $\mathbf{CL}(g) \subset SL_2(\bar{\mathbf{F}}_p) = \mathbf{G}$ be the conjugacy class of g. If $H \subset G$ is a symmetric generating set containing 1, we have:*

$$|\mathbf{CL}(g) \cap H| \leq 7\alpha^{2/3}|H|^{2/3},$$

where $\alpha = trp(H)$, unless $\alpha > |H|^{1/28}$.

Proof: g is a regular semisimple element with $tr(g) \neq 0$. We define the map ϕ that we have already seen before:

$$\phi : \begin{cases} \mathbf{Cl}(g) \times \mathbf{Cl}(g) \times \mathbf{Cl}(g) \to \mathbf{G} \times \mathbf{G} \\ (x_1, x_2, x_3) \mapsto (x_1x_2, x_1x_3) \end{cases}$$

and denote

$$Z = (\mathbf{Cl}(g) \cap H)^3,\ W = \phi(Z),$$

so that

$$|\mathbf{Cl}(g) \cap H|^3 = \sum_{(y_1,y_2)\in W} |\phi^{-1}(y_1, y_2) \cap Z| = S_0 + S_1 + S_2,$$

where S_i denotes the sum restricted to $W_i \subset W$, where W_0 is the subset where the fiber has order at most 2, while W_1 corresponds to those (y_1, y_2) where case (1) of Pink's theorem holds and W_2 corresponds to those (y_1, y_2), where *only* cases (2) or (3) of Pink's Theorem hold (which means, we don't put into W_2 pairs (y_1, y_2) with $y_1 = 1$ or $y_2 = 1$ or $y_1 = y_2$). We will prove the following estimates:

$$S_0 \leq 2|H^{(2)}|^2 \leq 2\alpha^2|H|^2,$$

$$S_1 \leq 3|H^{(2)}|^2 \leq 4|H^{(2)}|^2 \leq 4\alpha^2|H|^2,$$

$$S_2 \leq 32\alpha^{34/3}|H|^{5/3}.$$

Assuming this, we will get immediately

$$|\mathbf{Cl}(g) \cap H| \leq 6^{2/3}\alpha^{2/3}|H|^{2/3} + 2^{5/3}\alpha^{34/9}|H|^{5/9}.$$

Now either the second term is smaller or equal than the first and we get

$$|\mathbf{Cl}(g) \cap H| \leq 6^{2/3}\alpha^{2/3}|H|^{2/3} + 2^{5/3}\alpha^{34/9}|H|^{5/9} \leq 2 \cdot 6^{2/3}\alpha^{2/3}|H|^{2/3} \leq 7\alpha^{2/3}|H|^{2/3}$$

and this is the result we need, or the second term is bigger, which means

$$2^{5/3}\alpha^{34/9}|H|^{5/9} > 6^{2/3}\alpha^{2/3}|H|^{2/3} > 2^{5/3}\alpha^{2/3}|H|^{2/3},$$

which implies

$$\alpha > |H|^{1/28},$$

which is the alternative. Now it remains to check the bounds on S_i

1. S_0 : fibers over W_0 have at most 2 elements, hence also their intersection with Z, so $S_0 \leq 2|W_0| \leq 2|W| \leq 2|H^{(2)}|^2$

2. S_1 : this case splits into 3 almost identical subcases, corresponding to $y_1 = 1$, $y_2 = 1$, $y_1 = y_2$. We only check the bound for one of them, say, for $S_{1.1}$. We have:

$$S_{1.1} \leq \sum_{y_2 \in H^{(2)}} |\phi^{-1}(1, y_2) \cap Z|.$$

By Lemma 4.1, we have:

$$|\phi^{-1}(1, y_2) \cap Z| = |(x_1, x_1^{-1}, x_1^{-1} y_2) \in (\mathbf{CL}(g) \cap H)^3| \leq |H|$$

for any given $y_2 \in H^{(2)}$, since $x_1 \in H$ determines the triple $(x_1, x_1^{-1}, x_1^{-1} y_2)$. So we get

$$S_{1.1} \leq |H^{(2)}||H| \leq |H^{(2)}|^2,$$

and similarly for the other 2 cases.

3. S_2 : Here we also sum over y_1 first, which is $\neq \pm 1$ ($y_1 = 1$ has been already considered in W_1 and $y = -1$, as it's easy to see and has been mentioned in the proof of Pink's theorem, will never appear in any specific case of Pink's theorem and therefore pairs of type $(-1, y_2)$ can only belong to W_0). The number of y_1's can be bounded with $|H^{(2)}|$. Now we have fixed y_1 and we want to count the number of possible y_2's for this fixed y_1. As before, we define

$$C_\gamma = \left\{ \begin{pmatrix} \gamma & t \\ 0 & \gamma^{-1} \end{pmatrix} \mid t \in \bar{\mathbf{F}}_p \right\}.$$

As we have seen in the proof of Pink's theorem, for each y_1 there are at most 4 classes of matrices y_2 for which the second or the third case of this theorem holds and each class is a conjugate of some C_γ (remember that we are not considering $y_1 = 1$, $y_2 = 1$, $y_1 = y_2$). So, we need to estimate the size of an intersection of the type $H^{(2)} \cap x C_\gamma x^{-1}$, but this is what we already can do thanks to lemma 4.3. So, for a fixed y_1 the number of possible y_2's is

$$|\{y_2 \mid (y_1, y_2) \in W_2\}| \leq 8 trp(H^{(2)})^2 |H^{(2)}|^{1/3} \leq 8\alpha^{25/3} |H|^{1/3}$$

(the factor 8 accounts for 4, which is the number of classes of y_2, and the factor 2 in the lemma).

Now y_1 and y_2 are fixed. Then the size of the fiber $\phi^{-1}(y_1, y_2) \cap Z$ is determined by the number of possibilities for x_1. As the latter satisfies

$$x_1 \in \mathbf{Cl}(g) \cap \mathbf{B} \cap H,$$

and $\mathbf{Cl}(g) \cap \mathbf{B}$ is a conjugate of a union of the type $C_\gamma \cup C_{\gamma^{-1}}$ we see that we must estimate the size of an intersection of the type

$$H \cap C_\gamma$$

for some fixed $\gamma \in \mathbf{F}_p^\times$, since this will lead us to the estimate for the number of possibilities for x_1. Using lemma 4.3 again, we get

$$|\phi^{-1}(y_1, y_2) \cap Z| \leq 4\alpha^2 |H|^{1/3}.$$

This gives

$$S_2 \leq 32\alpha^{31/3} |H|^{2/3} |H^{(2)}| \leq 32\alpha^{34/3} |H|^{5/3},$$

as desired.

□

Corollary 4.5 (Involving dichotomy) *1. For all prime numbers p, all subsets $H \subset SL_2(\mathbf{F}_p)$ and all maximal tori $\mathbf{T} \subset SL_2(\bar{\mathbf{F}}_p)$, if $\mathbf{T}$ and H are not involved, we have:*

$$|H \cap \mathbf{T}| \leq 4.$$

2. *If $p \geq 5$ and $H \subset SL_2(\mathbf{F}_p) = G$ is a symmetric generating set containing 1 with $H^{(3)} \neq SL_2(\mathbf{F}_p)$, we have:*

$$|\mathbf{T}_{reg} \cap H^{(2)}| \geq 14^{-1}\alpha^{-14/3}|H|^{1/3}$$

for any maximal torus $\mathbf{T} \subset SL_2(\bar{\mathbf{F}}_p)$ which is not involved with H, where $\alpha = trp(H)$, unless

$$\alpha > |H|^{1/168}.$$

Proof:

1. Since H and $\mathbf{T}$ are not involved, $H \cap \mathbf{T}$ doesn't contain regular semisimple elements with nonzero trace. So $H \cap \mathbf{T}$ can contain either regular semisimple elements with trace 0, and in $\mathbf{T}$ there are at most 2 of them, or $H \cap \mathbf{T}$ can contain elements which are not regular semisimple, and in $\mathbf{T}$ there are 2 of them: ± 1. Therefore, this intersection contains at most 4 elements.

2. We apply the orbit-stabilizer theorem 2.3. Let $T = \mathbf{T} \cap G$ be a maximal torus in G. Fixing any $g \in T_{reg}$, we have $T = C_G(g)$, the stabilizer of g in G for its conjugacy action on itself. We find that

$$|\mathbf{T} \cap H^{(2)}| = |T \cap H^{(2)}| \geq \frac{|H|}{|\{hgh^{-1} \mid h \in H\}|}$$

for any symmetric subset H. Since H is involved with $\mathbf{T}$, we can select $g \in \mathbf{T}_{sreg} \cap H = T_{sreg} \cap H$ and the denominator on the right becomes

$$|\{hgh^{-1} \mid h \in H\}| \leq |H^{(3)} \cap Cl(g)| \leq |H^{(3)} \cap \mathbf{Cl}(g)|,$$

where $Cl(g)$ (resp., $\mathbf{Cl}(g)$) is the conjugacy class of g in G (resp., in $\mathbf{G}$). Applying the non-concentration inequality to $H^{(3)}$, we will further have

$$|H^{(3)} \cap \mathbf{Cl}(g)| \leq 7trp(H^{(3)})^{2/3}|H^{(3)}|^{2/3}.$$

From Ruzsa's theorem we have $trp(H^{(3)}) \leq \alpha^6$, so we will have

$$|H^{(3)} \cap \mathbf{Cl}(g)| \leq 7(\alpha^6)^{2/3}(|H|\alpha)^{2/3} = 7|H|^{2/3}\alpha^{14/3},$$

unless $trp(H^{(3)}) > |H^{(3)}|^{1/28}$, which implies

$$\alpha^6 \geq trp(H^{(3)}) > |H^{(3)}|^{1/28} = (|H|\alpha)^{1/28},$$

$$\alpha^{168} > |H|\alpha \Rightarrow \alpha > |H|^{1/167},$$

which is even better than we need.

Therefore,

$$|\mathbf{T} \cap H^{(2)}| \geq \frac{|H|}{|\{hgh^{-1} \mid h \in H\}|} \geq \frac{|H|}{|H^{(3)} \cap \mathbf{Cl}(g)|} \geq \frac{|H|}{7|H|^{2/3}\alpha^{14/3}} = 7^{-1}\alpha^{-14/3}|H|^{1/3}.$$

Now we note that there are exactly 2 elements in $\mathbf{T} \cap H^{(2)}$ that are not regular semisimple (they are ± 1), therefore

$$|\mathbf{T}_{reg} \cap H^{(2)}| = |\mathbf{T} \cap H^{(2)}| - 2 \geq 7^{-1}\alpha^{-14/3}|H|^{1/3} - 2.$$

If the first term is ≥ 4 (denote it by A for the moment), then

$$\frac{A}{2} \geq 2 \Leftrightarrow A - \frac{A}{2} \geq 2 \Leftrightarrow A - 2 \geq \frac{A}{2}.$$

In this case the previous sum can be estimated as follows:

$$|\mathbf{T}_{reg} \cap H^{(2)}| \geq 14^{-1}\alpha^{-14/3}|H|^{1/3}$$

and this is the result we need. If $A < 4$ we will get

$$7^{-1}\alpha^{-14/3}|H^{1/3}| < 4 \Leftrightarrow \alpha^{14/3} > \frac{|H|^{1/3}}{28} \Leftrightarrow \alpha > \frac{|H|^{1/14}}{28^{3/14}}.$$

To get the desired alternative we need to have

$$\frac{|H|^{1/14}}{28^{3/14}} \geq |H|^{1/168} \Leftrightarrow |H|^{11/168} \geq 28^{3/14} \Leftrightarrow |H| \geq 28^{36/11}.$$

But what do we do if $|H| < 28^{36/11}$? We use proposition 2.2. It says that if $H^{(3)} \neq G$, then $\alpha \geq 2^{1/2}$. To get the desired alternative, we need to have

$$\alpha \geq 2^{1/2} \geq |H|^{1/168} \Leftrightarrow |H| \leq 2^{84}.$$

But in our case $|H| < 28^{36/11} < 2^{84}$ and so the desired alternative is achieved.

□

5 Proof of the main theorem and bounding the diameter

Here we state theorem 1.2 in a slightly modified, but equivalent way:

Theorem 5.1 (Helfgott) *Let p be a prime number, $H \subset SL_2(\mathbf{F}_p)$ is a symmetric generating subset of $SL_2(\mathbf{F}_p)$ containing 1. Then if $H^{(3)} \neq SL_2(\mathbf{F}_p)$, we have*

$$trp(H) \geq |H|^{\delta},$$

where $\delta = 1/3024$.

Proof: If $p \leq 5$ we can check the theorem numerically. So we assume $p \geq 7$ to be able to apply theorem 3.1. We will show that

$$\alpha = trp(H) \geq 2^{-1/2}|H|^{1/1512}$$

for $p \geq 7$. Then using theorem 2.2, we derive

$$\alpha = trp(H) \geq max(2^{1/2}, 2^{-1/2}|H|^{1/1512}) \geq |H|^{1/3024}.$$

By theorem 3.1, there exists at least 1 maximal torus $\mathbf{T}$ involved with $H^{(3)}$ (hence also with $L = H^{(4)}$). If, among all tori involved with L, there is 1 for which the main bound in the corollary 4.5 (applied to L) fails, we obtain the alternative from this theorem:

$$trp(L) \geq |L|^{1/168} \geq |H|^{1/168},$$

and since $trp(L) \leq \alpha^9$ by Ruzsa's theorem, we have

$$\alpha \geq |H|^{1/1512} \geq 2^{-1/2}|H|^{1/1512},$$

which is the result we need. Otherwise, we distinguish 2 cases.

Case 1: There exists a maximal torus $\mathbf{T}$ involved with L such that for any $g \in G$ the torus $g\mathbf{T}g^{-1}$ is also involved with L. Writing $T = \mathbf{T} \cap G$, we note that the maximal tori

$$gTg^{-1} = (g\mathbf{T}g^{-1}) \cap G$$

are distinct for g taken among representatives of $G/N_G(T)$. Indeed,

$$gTg^{-1} = hTh^{-1} \Leftrightarrow h^{-1}gTg^{-1}h = T \Leftrightarrow h^{-1}g \in N_G(T) \Leftrightarrow g \in hN_G(T).$$

Then we have

$$|L^{(2)}| \geq \sum_{g \in G/N_G(T)} |L^{(2)} \cap g\mathbf{T}_{reg}g^{-1}| \geq 14^{-1}\beta^{-14/3}|L|^{1/3}\frac{|G|}{|N_G(T)|},$$

where $\beta = trp(L)$, since each $g\mathbf{T}g^{-1}$ is involved with L and there can't be any "overlaps" since a regular semisimple element can't lie in more than 1 maximal torus and we are in the case where the upper bound holds for all tori involved with L. Now from Ruzsa's theorem we have

$$\frac{|L^{(2)}|}{|H|} = \frac{|H^{(8)}|}{|H|} \leq \alpha^6,$$

$$|H| \geq \alpha^{-6}|L^{(2)}| \geq 14^{-1}\alpha^{-6}\beta^{-14/3}|L|^{1/3}\frac{p^3-p}{2(p+1)} = 28^{-1}\alpha^{-6}\beta^{-14/3}|L|^{1/3}p(p-1) \geq 28^{-1}\alpha^{-6}\beta^{-14/3}|L|^{1/3}(p-1)^2.$$

Also as before we have

$$\beta = tpr(L) = trp(H^{(4)}) \leq \alpha^9,$$

hence the previous inequality becomes

$$|H| \geq 28^{-1}\alpha^{-6}\alpha^{-42}|L|^{1/3}(p-1)^2 = 28^{-1}\alpha^{-48}|L|^{1/3}(p-1)^2 \geq 28^{-1}\alpha^{-48}|H|^{1/3}(p-1)^2,$$

$$|H|^{2/3} \geq 28^{-1}\alpha^{-48}(p-1)^2 \Leftrightarrow |H| \geq 28^{-3/2}\alpha^{-72}(p-1)^3,$$

which for $p \geq 7$ implies $|H| \geq 250^{-1}\alpha^{-72}|G|$. Indeed, we need to check that

$$28^{-3/2}\alpha^{-72}(p-1)^3 \geq 250^{-1}\alpha^{-72}|G| \Leftrightarrow \frac{250}{28^{3/2}} \geq \frac{p^3-p}{(p-1)^3} = \frac{p(p+1)}{(p-1)^2} = f(p).$$

$(1,\infty)$ is the interval where the function on the right decreases. Since we are interested in $p \geq 7$, we compute $f(7)$ (the value of this function in other primes will be smaller), multiply it by $28^{3/2}$ and see that the result is around $230 < 250$ (that's how the number 250 was chosen). So, we return back to what we got:

$$|H| \geq 250^{-1}\alpha^{-72}|G|.$$

Then we have 2 possibilities:

1) $\alpha \leq 500^{-1/72}|G|^{1/648}$

Then from the previous inequality we get

$$|H| \geq 250^{-1}\alpha^{-72}|G| \geq 250^{-1}(500^{-1/72}|G|^{1/648})^{-72}|G| = 2|G|^{-1/9}|G| = 2|G|^{8/9},$$

and using theorem 2.5, we get $H^{(3)} = G$ which contradicts our assumptions.

2)$\alpha > 500^{-1/72}|G|^{1/648}$, then since $500^{-1/72} > 2^{-1/2}$, we have

$$\alpha > 2^{-1/2}|G|^{1/648} > 2^{-1/2}|G|^{1/1512} \geq 2^{-1/2}|H|^{1/1512}$$

and this is the result we need.

Case 2: Since we know that some torus is involved with L, the complementary situation to case 1 is that there is a maximal torus $\mathbf{T}$ involved with $L = H^{(4)}$ and an element $g \in G$ such that $g\mathbf{T}g^{-1} = \mathbf{T}_1$ is not involved with L. The first remark is that we can assume, possibly after changing g and $\mathbf{T}$, that $g \in H$.

Indeed, to check this claim, we start with g and $\mathbf{T}$ as above. Since H is a generating set, we can write

$$g = h_1 \cdots h_m$$

for some $m \geq 1$ and some $h_i \in H$. Then

$$\mathbf{T}_1 = h_1 \cdots h_m \mathbf{T} h_m^{-1} \cdots h_1^{-1}.$$

We know that $\mathbf{T}_1$ is not involved with L while $\mathbf{T}$ is. We do the following: erase the first and the last term in this product; we will get the torus

$$\mathbf{T}_2 = h_2 \cdots h_m \mathbf{T} h_m^{-1} \cdots h_2^{-1}.$$

If this new torus is already involved with L, we take $\mathbf{T}_2$ and h_1 instead of $\mathbf{T}$ and g. Otherwise, if $\mathbf{T_2}$ is not yet involved with L, continue erasing. At a certain point we will get that the torus

$$\mathbf{T}_i = h_i \cdots h_m \mathbf{T} h_m^{-1} \cdots h_i^{-1}$$

is not yet involved with L, while the next one,

$$\mathbf{T}_{i+1} = h_{i+1} \cdots h_m \mathbf{T} h_m^{-1} \cdots h_{i+1}^{-1}$$

is involved with L. Then we take $\mathbf{T}_{i+1}$ and h_i instead of $\mathbf{T}$ and g.

We remark that this will surely happen. In the worst case, we will have to erase all h_i's and get that the torus $\mathbf{T}_m = h_m \mathbf{T} h_m^{-1}$ is not involved with L, while the torus $\mathbf{T}$ is. But then we can take $\mathbf{T}$ and h_m. From

now on we will write h instead of g, keep the notation $\mathbf{T}$ for the torus which is involved with L and we put $\mathbf{S} = h\mathbf{T}h^{-1}$. We apply theorem 2.4 with $(H, K) = (H^{(2)}, \mathbf{S} \cap G = S)$ and $n = 5$. This gives

$$\frac{|(H^{(2)})^{(6)}|}{|H^{(2)}|} \geq \frac{|(H^{(2)})^{(5)} \cap S|}{|(H^{(2)})^{(2)} \cap S|},$$

i.e.,

$$\frac{|H^{(12)}|}{|H^{(2)}|} \geq \frac{|H^{(10)} \cap S|}{|H^{(4)} \cap S|}.$$

But since $L = H^{(4)}$ and $\mathbf{S}$ are not involved, their intersection can contain at most 4 elements (by the easy part of corollary 4.5), and therefore we get

$$\frac{|H^{(12)}|}{|H^{(2)}|} \geq \frac{1}{4}|H^{(10)} \cap S|.$$

Also we have

$$h(H^8 \cap \mathbf{T})h^{-1} \subset H^{(10)} \cap \mathbf{S},$$

so that

$$|H^{(10)} \cap \mathbf{S}| \geq |H^8 \cap \mathbf{T}| = |L^{(2)} \cap \mathbf{T}| \geq 28^{-1}\beta^{-14/3}|L|^{1/3},$$

where $\beta = trp(L)$ (since L and $\mathbf{T}$ are involved and we are in the case where the bound from corollary 3.6 holds for all tori involved with L).

$$\frac{|H^{(12)}|}{|H^{(2)}|} \geq \frac{1}{4}28^{-1}\beta^{-14/3}|L|^{1/3} = 112^{-1}\beta^{-14/3}|L|^{1/3}.$$

From Ruzsa's theorem we have

$$\beta = trp(H^{(4)}) \leq \alpha^9$$

and

$$\frac{|H^{(12)}|}{|H^{(2)}|} \leq \frac{|H^{(12)}|}{|H|} \leq \alpha^{10},$$

and so finally we get

$$\alpha^{10} \geq 112^{-1}\beta^{-14/3}|L|^{1/3} \geq 112^{-1}\alpha^{-42}|H|^{1/3},$$

which implies

$$\alpha \geq 112^{-1/52}|H|^{1/156}.$$

Since $112^{-1/52} > 2^{-1/2}$, we finally get

$$\alpha \geq 2^{-1/2}|H|^{1/156} \geq 2^{-1/2}|H|^{1/1512}.$$

□

Proof of Babai's conjecture for $SL_2(\mathbf{F}_p)$: given a generating set H, we apply Helfgott's theorem l times (l will be chosen later):

$$|H^{(3^l)}| \geq |H|^{(1+\delta)^l}.$$

Now we will choose l such that

$$|H|^{(1+\delta)^l} > |G|$$

and therefore we will get

$$|H^{3^l}| > |G|.$$

Since this is absurd, we will get that $H^{(3^l)} = G$ and the diameter of the Cayley graph is not bigger than 3^l. Now we choose l:

$$|H|^{(1+\delta)^l} > |G| \Leftrightarrow (1+\delta)^l \log|H| > \log|G| \Leftrightarrow (1+\delta)^l > \frac{\log|G|}{\log|H|},$$

which gives

$$l\log(1+\delta) > \log\frac{\log|G|}{\log|H|} \Leftrightarrow l > \frac{1}{\log(1+\delta)}\log\frac{\log|G|}{\log|H|}.$$

Take

$$l = \left\lceil \frac{\log\log|G|}{\log(1+\delta)} \right\rceil,$$

this will give us

$$\log diam(\Gamma(G,H)) \leq \log 3^l = l\log 3 \leq \log 3\left(\frac{\log\log|G|}{\log(1+\delta)} + 1\right) \leq 3323\log\log|G| + \log 3 = \log(3(\log|G|)^{3323})$$

(here we computed $\log 3/\log(1+1/3024)$ explicitly), which gives us

$$diam(\Gamma(G,H)) \leq 3(\log|G|)^{3323}.$$

□

References

[1] E. Kowalski: Explicit growth and expansion for SL_2. Int. Math. Res. Not. IMRN, (24):5645–5708, 2013.

[2] E. Kowalski: Expander graphs, lecture notes for ETH Zurich Fall Semester course.

[3] H. Helfgott: Growth and generation in $SL_2(Z/pZ)$, Ann. of Math. 167 (2008), 601-623.

[4] F. Digne and J. Michel: Representations of finite groups of Lie type, L.M.S Student Texts 21, Cambridge University Press 1991.

[5] W. Fulton and J. Harris: Representation theory, GTM 129, Springer 1991.

[6] R.W. Carter: Finite groups of Lie type, Wiley Interscience 1985.

[7] L. Babai and A. Seress: On the diameter of permutation groups, European J. Combin. 13 (1992), 231–243.