Surjectivity and equidistribution of the word $x^a y^b$ on $PSL(2,q)$ and $SL(2,q)$

Tatiana BANDMAN and Shelly GARION

Institut des Hautes Études Scientifiques
35, route de Chartres
91440 – Bures-sur-Yvette (France)

Juin 2011

IHES/M/11/19

SURJECTIVITY AND EQUIDISTRIBUTION OF THE WORD $x^a y^b$ ON $\mathrm{PSL}(2,q)$ AND $\mathrm{SL}(2,q)$

TATIANA BANDMAN AND SHELLY GARION

Abstract. We determine the integers $a, b \geq 1$ and the prime powers q for which the word map $w(x,y) = x^a y^b$ is surjective on the group $\mathrm{PSL}(2,q)$ (and $\mathrm{SL}(2,q)$). We moreover show that this map is almost equidistributed for the family of groups $\mathrm{PSL}(2,q)$ (and $\mathrm{SL}(2,q)$). Our proof is based on the investigation of the trace map of positive words.

1. Introduction

1.1. **Word maps in finite simple groups.** During the last years there has been a great interest in *word maps* in groups, for an extensive survey see [Se]. These maps are defined as follows. Let $w = w(x_1, \dots, x_d)$ be a non-trivial *word*, namely a non-identity element of the free group F_d on the generators $x_1, \dots, x_d$. Then we may write $w = x_{i_1}^{n_1} x_{i_2}^{n_2} \dots x_{i_k}^{n_k}$ where $1 \leq i_j \leq d$, $n_j \in \mathbb{Z}$, and we may assume further that w is reduced. Let G be a group. For $g_1, \dots, g_d$ we write

$$w(g_1, \dots, g_d) = g_{i_1}^{n_1} g_{i_2}^{n_2} \dots g_{i_k}^{n_k} \in G,$$

and define

$$w(G) = \{w(g_1, \dots, g_d) : g_1, \dots, g_d \in G\},$$

as the set of values of w in G. The corresponding map $w : G^d \to G$ is called a *word map*.

Borel [Bo] showed that the word map induced by $w \neq 1$ on simple algebraic groups is a dominant map. Larsen [La] used this result to show that for every non-trivial word w and $\epsilon > 0$ there exists a number $C(w, \epsilon)$ such that if G is a finite simple group with $|G| > C(w, \epsilon)$ then $|w(G)| \geq |G|^{1-\epsilon}$. By recent work of Larsen, Shalev and Tiep [LS, LST], for every non-trivial word w there exists a constant $C(w)$ such that if G is a finite simple group satisfying $|G| > C(w)$ then $w(G)^2 = G$.

It is therefore interesting to find words w for which $w(G) = G$ for any finite simple non-abelian group G. Due to immense work spread over more than 50 years, it is now known that the commutator word $w = [x, y] \in F_2$ satisfies $w(G) = G$ for any finite simple group G (see [LOST10] and the references therein). On the other hand, it is easy to see that if G is a finite group and b is an integer which is not relatively prime to the order of G then $w(G) \neq G$ for the word $w = x^b$.

2000 *Mathematics Subject Classification.* 14G05, 14G15, 20D06, 20G40.

Key words and phrases. special linear group, word map, trace map, finite fields.

The words of the form $w = x^a y^b \in F_2$ have also attracted special interest. Due to recent work of Larsen, Shalev and Tiep [LST], it is known that any such word is surjective for sufficiently large finite simple groups (see [LST, Theorem 1.1.1 and Corollary 1.1.3]), more precisely,

Theorem 1.1. [LST]. *Let a, b be two non-zero integers. Then there exists a number $N = N(a, b)$ such that if G is a finite simple non-abelian group of order at least N, then any element in G can be written as $x^a y^b$ for some $x, y \in G$.*

By further recent results of Guralnick and Malle [GM] and of Liebeck, O'Brien, Shalev and Tiep [LOST11], some words of the form $x^b y^b$ are known to be surjective on *all* finite simple groups.

Theorem 1.2. [GM, Corollary 1.5]. *Let G be a finite simple non-abelian group and let b be either a prime power or a power of 6. Then any element in G can be written as $x^b y^b$ for some $x, y \in G$.*

Note that in general, the word $x^b y^b$ is not necessarily surjective on *all* finite simple groups. Indeed, if b is a multiple of the exponent of G then necessarily $x^b y^b = id$ for every $x, y \in G$. It is therefore interesting to find more examples for words of the form $x^b y^b$ which are *not* surjective on all finite simple groups.

More generally, one can ask whether it is possible to generalize Theorem 1.1 for other word maps. In particular, the following conjecture was raised:

Conjecture 1.3 (Shalev)**.** [Sh07, Conjectures 2.8 and 2.9]. *Let $w \neq 1$ be a word which is not a proper power of another word. Then there exists a number $C(w)$ such that, if G is either A_r or a finite simple group of Lie type of rank r, where $r > C(w)$, then $w(G) = G$.*

It is also interesting to investigate the *distribution* of the word map. Due to the work of Garion and Shalev [GS], it is known that the word $w = x^2 y^2$ is *almost equidistributed* for the family of finite simple groups, namely,

Theorem 1.4. [GS, Theorem 7.1]. *Let G be a finite simple group, and let $w : G \times G \to G$ be the map given by $w(x, y) = x^2 y^2$. Then there is a subset $S \subseteq G$ with $|S| = (1 - o(1))|G|$ such that $|w^{-1}(g)| = (1 + o(1))|G|$ for all $g \in S$. Where $o(1)$ denotes a function depending only on G which tends to zero as $|G| \to \infty$.*

Another question which was raised by Shalev [Sh07, Problem 2.10] is which words w induce an *almost equidistributed* map for the family of finite simple groups. In particular, does words of the form $w = x^a y^b$ induce *almost equidistributed* maps?

1.2. **The word $w(x, y) = x^a y^b$ on the groups $\mathrm{SL}(2, q)$ and $\mathrm{PSL}(2, q)$.** In this paper we analyze the word map $x^a y^b$ in the groups $\mathrm{SL}(2, q)$ and $\mathrm{PSL}(2, q)$. Analysis of Engel word maps in these groups was carried out in our previous work [BGG].

We start by determining precisely the positive integers a, b and prime powers q for which the word map $w = x^a y^b$ is surjective on $\mathrm{SL}(2, q) \setminus \{-id\}$ and on $\mathrm{PSL}(2, q)$.

Definition 1.5. Let $a, b \geq 1$ and let $q = p^e$ be a prime power. We say that the word $w = x^a y^b$ is *non-degenerate* with respect to q if and only if none of the following conditions holds:

- $p = 2$, a is a multiple of $2(q^2 - 1)$ and b is not relatively prime to $2(q^2 - 1)$;
- $p = 2$, b is a multiple of $2(q^2 - 1)$ and a is not relatively prime to $2(q^2 - 1)$;
- p is odd, a is a multiple of $\frac{p(q^2-1)}{4}$ and b is not relatively prime to $\frac{p(q^2-1)}{4}$;
- p is odd, b is a multiple of $\frac{p(q^2-1)}{4}$ and a is not relatively prime to $\frac{p(q^2-1)}{4}$.

Obviously, if the word map $w = x^a y^b$ is surjective on $\mathrm{PSL}(2, q)$ then it is necessarily non-degenerate with respect to q. On the other hand, we prove the following proposition.

Proposition 1.6. *If $w = x^a y^b$ is non-degenerate with respect to q, then all* semisimple *elements, namely matrices in* $\mathrm{SL}(2, q)$ *whose trace is not* ± 2*, are in the image of the word map w.*

Unfortunately, even if $w = x^a y^b$ is non-degenerate with respect to q, the image of $w = x^a y^b$ may not contain the *unipotent* elements, namely, matrices $\pm id \neq z \in \mathrm{SL}(2, q)$ satisfying $\mathrm{tr}(z) = \pm 2$. This phenomenon happens when one of the following obstructions occurs.

Definition 1.7. Let $a, b \geq 1$ and let q be a prime power. We define the following *obstructions*:

- *Obstruction (i):* $q = 2^e$, e is odd, and a, b are divisible by $\frac{2(q^2-1)}{3}$;
- *Obstruction (ii):* $q \equiv 3 \bmod 4$ and a, b are divisible by $\frac{p(q^2-1)}{8}$;
- *Obstruction (iii):* $q \equiv 11 \bmod 12$ and a, b are divisible by $\frac{p(q^2-1)}{6}$;
- *Obstruction (iv):* $q \equiv 5 \bmod 12$ and a, b are divisible by $\frac{p(q^2-1)}{12}$.

Theorem 1.8. *Let $e \geq 1$ and let $q = 2^e$. Let $a, b \geq 1$.*
Then the word map $w = x^a y^b$ is surjective on $\mathrm{SL}(2, q) = \mathrm{PSL}(2, q)$ *if and only if w is non-degenerate with respect to q and obstruction (i) does not occur.*

Theorem 1.9. *Let p be an odd prime number, $e \geq 1$ and $q = p^e$. Let $a, b \geq 1$.*
Then the word map $w = x^a y^b$ is surjective on $\mathrm{SL}(2, q) \setminus \{-id\}$ *if and only if w is non-degenerate with respect to q and none of the obstructions (ii),(iii),(iv) occurs.*

Theorem 1.10. *Let p be an odd prime number, $e \geq 1$ and $q = p^e$. Let $a, b \geq 1$.*
Then the word map $w = x^a y^b$ is surjective on $\mathrm{PSL}(2, q)$ *if and only if w is non-degenerate with respect to q and obstruction (ii) does not occur.*

For example, we deduce that the word $w = x^{42} y^{42}$ is *not* surjective on the groups $\mathrm{PSL}(2, 7)$ and $\mathrm{PSL}(2, 8)$.

The last theorem implies that for the family of groups $\mathrm{PSL}(2, q)$ one can give a precise estimation for the bound $N = N(a, b)$ appearing in Theorem 1.1.

Corollary 1.11. *For every $a, b \geq 1$, let*

$$Q = Q(a,b) = \max\{\sqrt{3a}, \sqrt{3b}\},$$

$$N = N(a,b) = \max\{\frac{3\sqrt{3}}{2}a^{3/2}, \frac{3\sqrt{3}}{2}b^{3/2}\}.$$

Then the word map $w = x^a y^b$ is surjective on the group $\mathrm{PSL}(2,q)$ for any $q > Q$, and hence whenever $|\mathrm{PSL}(2,q)| > N$.

However, the statement of Theorem 1.1 [LST] no longer holds for the quasi-simple group $\mathrm{SL}(2,q)$, as indicated by the following theorem and its corollary.

Theorem 1.12. *Let q be an odd prime power, and set $K = \max\left\{k : 2^k \text{ divides } \frac{q^2-1}{2}\right\}$. Let $a, b \geq 1$. Then $-id \neq x^a y^b$ for every $x, y \in \mathrm{SL}(2,q)$ if and only if 2^K divides both a and b.*

Corollary 1.13. *If $q \equiv \pm 3 \bmod 8$, then $x^4 y^4 \neq -id$ for every $x, y \in \mathrm{SL}(2,q)$.*

In addition, we show that for any $a, b \geq 1$, the word map $w = x^a y^b$ is *almost equiditributed* for the family of groups $\mathrm{PSL}(2,q)$ (and $\mathrm{SL}(2,q)$).

Theorem 1.14. *Let q be a prime power and let G be either the group $\mathrm{SL}(2,q)$ or the group $\mathrm{PSL}(2,q)$.*

Let $a, b \geq 1$ and let $w : G \times G \to G$ be the map given by $w(x,y) = x^a y^b$. Then there is a subset $S \subseteq G$ with $|S| = (1 - o(1))|G|$ such that $|w^{-1}(g)| = (1 + o(1))|G|$ for all $g \in S$. Where $o(1)$ denotes a function of q which tends to zero as $q \to \infty$.

1.3. **Organization and outline of the proof.** For the convenience of the reader, we describe the organization of the paper, as well as give a bird's eye view of the proofs.

In Section 2 we compute the *trace map* of the word $w(x,y) = x^a y^b$ (Lemma 2.3), and more generally, of any *positive* word in F_2 (Theorem 2.5). For any word $w = w(x,y) \in F_2$, the trace map $\mathrm{tr}(w)$ is a polynomial $P(s,u,t)$ in $s = \mathrm{tr}(x), t = \mathrm{tr}(y)$ and $u = \mathrm{tr}(xy)$.

In Section 3 we collect basic facts on the surjectivity of $w = x^a y^b$ on finite groups in general, and in Section 4 we describe some properties of the groups $\mathrm{SL}(2,q)$ and $\mathrm{PSL}(2,q)$ that are used later on.

By Lemma 2.3, $\mathrm{tr}(x^a y^b)$ is a *linear* polynomial in u. We deduce in Section 5 that if neither a nor b is divisible by the exponent of $\mathrm{PSL}(2,q)$, then any element in $\mathbb{F}_q$ can be written as $\mathrm{tr}(x^a y^b)$ for some $x, y \in \mathrm{SL}(2,q)$ (Corollary 5.3). This immediately implies Proposition 1.6, stating that if $w = x^a y^b$ is non-degenerate with respect to q, any *semisimple* element (namely, $z \in \mathrm{SL}(2,q)$ with $\mathrm{tr}(z) \neq \pm 2$) can be written as $z = x^a y^b$ for some $x, y \in \mathrm{SL}(2,q)$.

However, when z is *unipotent* (namely, $z \neq \pm id$ and $\mathrm{tr}(z) = \pm 2$) one has to be more careful, and a detailed analysis is done in Section 8. Indeed, it may happen that $w = x^a y^b$ is non-degenerate with respect to q, but nevertheless the image of the word map $w = x^a y^b$ does not contain any unipotent (see Propositions 6.4 and 6.5).

These are the ingredients needed for the proofs of Theorems 1.8, 1.9 and 1.10, on the surjectivity of the word $w = x^a y^b$ on $\mathrm{PSL}(2, q)$ and $\mathrm{SL}(2, q) \setminus \{-id\}$, which are presented in Section 6. In addition, we determine in Section 8.3 when $-id$ can be written as $x^a y^b$ for some $x, y \in \mathrm{SL}(2, q)$, thus proving Theorem 1.12.

In Section 7 we prove Theorem 1.14 and show that the word map $w = x^a y^b$ is almost equidistributed for the family of groups $\mathrm{PSL}(2, q)$ (and $\mathrm{SL}(2, q)$). The basic idea is to show that for a general $\alpha \in \mathbb{F}_q$, the surface

$$S_\alpha(\mathbb{F}_q) = \{P(s, u, t) = \mathrm{tr}(z) = \alpha\} \subset \mathbb{A}^3(\mathbb{F}_q)$$

is birational to a plane $\mathbb{A}^2_{s,t}$. As a result, we are able not only to find points on $S_\alpha(\mathbb{F}_q)$, but even to estimate their number.

Acknowledgement. Bandman is supported in part by Ministry of Absorption (Israel), Israeli Academy of Sciences and Minerva Foundation (through the Emmy Noether Research Institute of Mathematics).

Garion is supported by a European Post-doctoral Fellowship (EPDI), during her stay at the Institut des Hautes Études Scientifiques (Bures-sur-Yvette).

The authors are grateful to A. Shalev for discussing his questions and conjectures with them. They are also thankful for A. Mann and M. Larsen for useful discussions.

2. The trace map

2.1. **The trace map.** The *trace map* method is based on the following classical Theorem (see, for example, [Vo, Fr, FK] or [Mag, Go] for a more modern exposition).

Theorem 2.1 (Trace map). *Let $F = \langle x, y\rangle$ denote the free group on two generators. Let us embed F into $\mathrm{SL}(2, \mathbb{Z})$ and denote by tr the trace character. If w is an arbitrary element of F, then the character of w can be expressed as a polynomial*

$$\mathrm{tr}(w) = P(s, u, t)$$

with integer coefficients in the three characters $s = \mathrm{tr}(x), u = \mathrm{tr}(xy)$ and $t = \mathrm{tr}(y)$.

Note that the same remains true for the group $\mathrm{SL}(2, q)$. The general case, $\mathrm{SL}(2, R)$, where R is a commutative ring, can be found in [CMS].

The following theorem is originally due to Macbeath [Mac] and was used by Bandman, Grunewald, Kunyavskii and Jones to investigate verbal dynamical systems in the group $\mathrm{SL}(2, q)$ (see [BGKJ, Theorem 3.4]).

Theorem 2.2. [Mac, Theorem 1]. *For any $(s, u, t) \in \mathbb{F}_q^3$ there exist two matrices $x, y \in \mathrm{SL}(2, q)$ satisfying $\mathrm{tr}(x) = s, \mathrm{tr}(y) = t$ and $\mathrm{tr}(xy) = u$.*

2.2. **Trace map of the word $w(x,y)=x^ay^b$.** The following Lemma shows that the trace map of the word $w(x,y)=x^ay^b$ is a linear polynomial in $\operatorname{tr}(xy)$.

Lemma 2.3. *Let $w(x,y)=x^ay^b$ where $a,b\geq 1$ and $x,y\in \mathrm{SL}(2,q)$. Let $s=\operatorname{tr}(x), u=\operatorname{tr}(xy), t=\operatorname{tr}(y)$. Then*

$$\operatorname{tr} w(x,y)=u\cdot f_{a,b}(s,t)+h_{a,b}(s,t),$$

where

$$f_{a,b}(s,t),\ h_{a,b}(s,t)\in \mathbb{F}_q[s,t]$$

are polynomials satisfying:

- *the highest degree summand of $f_{a,b}(s,t)$ (of degree $a+b-2$) is:*
$$s^{a-1}t^{b-1};$$
- *the highest degree summand of $h_{a,b}(s,t)$ (of degree $a+b-2$) is:*
$$-(s^at^{b-2}+s^{a-2}t^b).$$

Proof. We need to prove that the polynomials $f(s,t)=f_{a,b}(s,t)$ and $h(s,t)=h_{a,b}(s,t)$ satisfy the following properties:

(i) the coefficient of u, $f(s,t)$, has precisely one monomial summand $s^{a-1}t^{b-1}$ with coefficient 1;
(ii) for all other monomial summands $c_{i,j}s^it^j,\ c_{i,j}\in\mathbb{F}_q$, of $f(s,t)$, the following inequalities hold: $i\leq a-1$, $j\leq b-1$, and $i+j<a+b-2$;
(iii) $h(s,t)$ contains the summand $(s^at^{b-2}+s^{a-2}t^b)$ with coefficient -1;
(iv) for all other monomial summands $c_{i,j}s^it^j,\ c_{i,j}\in\mathbb{F}_q$, of $h(s,t)$, the following inequalities hold: $i\leq a-2$, $j\leq b-2$, and so $i+j\leq a+b-4$.

We prove these properties by induction on $a+b$, using the well-known formula

$$\operatorname{tr}(AB)+\operatorname{tr}(AB^{-1})=\operatorname{tr}(A)\operatorname{tr}(B). \tag{1}$$

Induction base. $a\leq 3, b\leq 3$. In these cases,

$$\operatorname{tr}(xy)=u,\ \operatorname{tr}(x^2y)=us-t,\ \operatorname{tr}(xy^2)=ut-s,\ \operatorname{tr}(x^2y^2)=ust-s^2-t^2+2,$$

$$\operatorname{tr}(xy^3)=(t^2-1)u-st,\quad \operatorname{tr}(x^3y)=(s^2-1)u-st,$$

$$\operatorname{tr}(x^2y^3)=(st^2-s)u-s^2t-t^3+3t,\ \operatorname{tr}(x^3y^2)=(s^2t-t)u-s^3-st^2+3s,$$

$$\operatorname{tr}(x^3y^3)=(s^2t^2-s^2-t^2+1)u-s^3t-st^3+4st.$$

Induction hypothesis. Assume that the Lemma is valid for $a+b<n$ for some $n\geq 5$.

Induction Step. We prove the claim for $a+b=n$, by considering the following cases:

Case 1. $w(x,y)=x^ay^b,\ a\geq b$.

Using (1) we get:

$$\begin{aligned}
\operatorname{tr}(x^a y^b) &= \operatorname{tr}(x)\operatorname{tr}(x^{a-1}y^b) - \operatorname{tr}(xy^{-b}x^{-a+1}) \\
&= \operatorname{tr}(x)\operatorname{tr}(x^{a-1}y^b) - \operatorname{tr}(x^{a-2}y^b) \\
&= s(u\cdot f_{a-1,b}(s,t) + h_{a-1,b}(s,t)) - (u\cdot f_{a-2,b}(s,t) + h_{a-2,b}(s,t)) \\
&= u(s\cdot f_{a-1,b}(s,t) - f_{a-2,b}(s,t)) + (s\cdot h_{a-1,b}(s,t)) - h_{a-2,b}(s,t)) \\
&= u\cdot f_{a,b}(s,t) + h_{a,b}(s,t).
\end{aligned}$$

By the induction hypothesis, the resulting polynomial:

(i) is linear in u;

(ii) the highest degree summand of $f_{a,b}(s,t)$ is:

$$ss^{(a-1)-1}t^{b-1} = s^{a-1}t^{b-1};$$

(iii) for all other monomial summands $c_{i,j}s^i t^j$ of $f(s,t)$ the following inequalities hold: $i \le (a-1)-1+1 = a-1$, $j \le b-1$, and

$$i+j < (a-1)+1+b-2 = a+b-2;$$

(iv) the highest degree summand in $h(s,t)$ is:

$$-s(s^{a-1}t^{b-2} + s^{(a-1)-2}t^b) = -(s^a t^{b-2} + s^{a-2}t^b).$$

(v) for all other monomial summands $c_{i,j}s^i t^j$ of $h(s,t)$ the following inequalities hold: $i \le (a-1)-2+1 = a-2$, $j \le b-2$, and so

$$i+j \le (a-1)+1+b-4 = a+b-4;$$

Case 2. $w(x,y) = x^a y^b,\ a < b.$
Similarly we get:

$$\begin{aligned}
\operatorname{tr}(x^a y^b) &= \operatorname{tr}(x^a y^{b-1})\operatorname{tr}(y) - \operatorname{tr}(x^a y^{b-1}y^{-1}) \\
&= \operatorname{tr}(y)\operatorname{tr}(x^a y^{b-1}) - \operatorname{tr}(x^a y^{b-2}) \\
&= t(u\cdot f_{a,b-1}(s,t) + h_{a,b-1}(s,t)) - (u\cdot f_{a,b-2}(s,t) + h_{a,b-2}(s,t)) = \\
&= u(t\cdot f_{a,b-1}(s,t) + f_{a,b-2}(s,t)) + (t\cdot h_{a,b-1}(s,t) - h_{a,b-2}(s,t)) = \\
&= u\cdot f_{a,b}(s,t) + h_{a,b}(s,t).
\end{aligned}$$

Similarly to Case 1 we get a polynomial satisfying the desired properties. □

Remark 2.4. Assume that $a, b \neq 0$ but not necessarily positive. Since $\operatorname{tr}(xy^{-1}) = st-u$, we deduce from Lemma 2.3 that

$$\operatorname{tr}(x^a y^b) = u\cdot f_{a,b}(s,t) + h_{a,b}(s,t),$$

where the highest degree summand of $f_{a,b}(s,t)$ (of degree $a+b-2$) is $\pm s^{a-1}t^{b-1}$.

2.3. **Trace map of positive words.** We can moreover compute the trace map for any *positive* word in F_2, namely for any word of the form $w = x^{a_1}y^{b_1}\dots x^{a_k}y^{b_k}$ where

$$a_2,\dots,a_k,b_1,\dots,b_{k-1} \geq 1 \text{ and } a_1, b_k \geq 0.$$

We note that we can consider only words of the form $w = x^{a_1}y^{b_1}\dots x^{a_k}y^{b_k}$ where $a_1,b_1,\dots,a_k,b_k \geq 1$, and then we call k the *"length"* of this word.

Indeed, if $b_k = 0$ then $\mathrm{tr}(x^{a_1}y^{b_1}\dots x^{a_{k-1}}y^{b_{k-1}}x^{a_k}) = \mathrm{tr}(x^{a_1+a_k}y^{b_1}\dots x^{a_{k-1}}y^{b_{k-1}})$, is the trace map of a positive word of length $k-1$.

Theorem 2.5. *Let $G = \mathrm{SL}(2,q)$ and let*

$$w = x^{a_1}y^{b_1}\dots x^{a_k}y^{b_k}, \quad a_1,b_1,\dots,a_k,b_k \geq 1.$$

Denote $s = \mathrm{tr}(x), u = \mathrm{tr}(xy), t = \mathrm{tr}(y)$, and $A = \sum_{i=1}^k a_i$, $B = \sum_{i=1}^k b_i$.

Then $tr(w) = P(s,u,t) = \sum_{r=0}^k u^r p_r(s,t)$, where

- *$p_k(s,t) = s^{A-k}t^{B-k} + \Phi(s,t)$ is a polynomial in s,t and*
$$\deg_s \Phi(s,t) \leq A-k,\ \deg_t \Phi(s,t) \leq B-k,$$
$$\deg_s \Phi(s,t) + \deg_t \Phi(s,t) < A+B-2k;$$
- *for all $r < k$,*
$$\deg_s p_r(s,t) \leq A-k,\ \deg_t p_r(s,t) \leq B-k.$$

Proof. The proof is by induction on k. The case $k=1$ was treated in Lemma 2.3.

We may always assume that $a_1 \leq a_k$. Let

$$w_1(x,y) = x^{a_1}y^{b_1}\dots x^{a_{k-1}}y^{b_{k-1}},$$
$$w_2(x,y) = x^{a_k}y^{b_k},$$
$$w_3(x,y) = x^{a_1-a_k}y^{b_1}\dots x^{a_{k-1}}y^{b_{k-1}-b_k}.$$

Then, by (1),

$$\begin{aligned} \mathrm{tr}(w) &= \mathrm{tr}(x^{a_1}y^{b_1}\dots x^{a_k}y^{b_k}) \\ &= \mathrm{tr}(x^{a_1}y^{b_1}\dots x^{a_{k-1}}y^{b_{k-1}})\,\mathrm{tr}(x^{a_k}y^{b_k}) - \mathrm{tr}(x^{a_1-a_k}y^{b_1}\dots x^{a_{k-1}}y^{b_{k-1}-b_k}) \\ &= \mathrm{tr}(w_1(x,y))\,\mathrm{tr}(w_2(x,y)) - \mathrm{tr}(w_3(x,y)), \end{aligned} \tag{2}$$

By the induction assumption we have

$$\mathrm{tr}(w_1) = P_1(s,u,t) = \sum_{r=0}^{k-1} u^r \tilde{p}_r(s,t),$$
$$\mathrm{tr}(w_2) = uf + h,$$
$$\mathrm{tr}(w_3) = Q(s,u,t),$$

and

- $\tilde{p}_{k-1}(s,t) = s^{A-a_k-k+1}t^{B-b_k-k+1} + \Phi_1(s,t)$;
- $\deg_s \Phi_1(s,t) \leq A-a_k-k+1,\ \deg_t \Phi_1(s,t) \leq B-b_k-k+1$, and
$\deg_s \Phi_1(s,t) + \deg_t \Phi_1(s,t) < A+B-a_k-b_k-2k+2$;

- $\deg_s f = a_k - 1, \ \deg_t f = b_k - 1.$

We want to show that

$$\deg_u Q < k, \ \deg_s Q \le A - k, \ \deg_t Q \le B - k. \tag{3}$$

Since

$$\mathrm{tr}(w) = P(s,u,t) = P_1(s,u,t)(uf+h) - Q(s,u,t),$$

the theorem would follow from (3).

Consider the following cases.

Case 1. $w_3(x,y)$ is a positive word.

Then its length is either $k-1$, if both $a = a_1 - a_k > 0$ and $b = b_{k-1} - b_k > 0$, or $k-2$ if $a = 0$ or $b = 0$. Anyway, $\deg_u Q < k$, $\deg_s Q \le A - 2a_k - k + 2 \le A - k$, and $\deg_t Q \le B - 2b_k - k + 2 \le B - k$, as needed.

Case 2. $a_1 - a_k > 0, \ b_{k-1} - b_k < 0.$

Then

$$\mathrm{tr}(w_3) = Q(s,u,t) = \mathrm{tr}(w_4(x,y))\,\mathrm{tr}(y^{b_k - b_{k-1}}) - \mathrm{tr}(w_5(x,y)),$$

where

$$w_4(x,y) = x^{a_1 - a_k + a_{k-1}} y^{b_1} \dots x^{a_{k-2}} y^{b_{k-2}},$$
$$w_5(x,y) = x^{a_1 - a_k} y^{b_1} \dots x^{a_{k-2}} y^{b_{k-2}} x^{a_{k-1}} y^{b_k - b_{k-1}}.$$

Thus, w_4 is a word of length $k-2$ and w_5 has length $k-1$, and both are positive words. Let $Q_1(s,u,t) = \mathrm{tr}(w_4(x,y))$, $Q_2(s,u,t) = \mathrm{tr}(w_5(x,y))$.

By the induction assumption,

$$\deg_u Q_1 = k-2, \ \deg_s Q_1 \le A - 2a_k - k + 2 \le A - k, \ \deg_t Q_1 \le B - b_k - b_{k-1} - k + 2;$$

$$\deg_u Q_2 = k-1, \ \deg_s Q_2 \le A - 2a_k - k + 1 \le A - k, \ \deg_t Q_2 \le B - 2b_{k-1} - k + 1 \le B - k.$$

Moreover, $T_1(t) = \mathrm{tr}(y^{b_k - b_{k-1}})$ is a polynomial in t of degree $b_k - b_{k-1}$, thus

$$\deg_t Q_1 T_1(t) \le B - b_k - b_{k-1} - k + 2 + b_k - b_{k-1} = B - 2b_{k-1} - k + 2 \le B - k.$$

Hence, for $Q = Q_1 T_1(t) - Q_2$ condition (3) is valid.

Case 3. $a_1 - a_k = 0, \ b_{k-1} - b_k < 0.$

In this case $w_3(x,y) = y^{b_1} \dots x^{a_{k-1}} y^{b_{k-1} - b_k}$ and

$$Q(s,u,t) = \mathrm{tr}(x^{a_2} \dots x^{a_{k-1}} y^{b_{k-1} - b_k + b_1}).$$

If $b_{k-1} - b_k + b_1 \ge 0$ then the word is positive of length $k-2$ and (3) is valid.

If $b_{k-1} - b_k + b_1 < 0$ then we perform the procedure described in **Case 2** for computing

$$Q(s,u,t) = \mathrm{tr}(x^{a_2} \dots x^{a_{k-1}} y^{b_{k-1} - b_k + b_1}) = \mathrm{tr}(w_4(x,y))\,\mathrm{tr}(y^{b_k - b_{k-1} - b_1}) - \mathrm{tr}(w_5(x,y)),$$

where

$$w_4(x,y) = x^{a_2 + a_{k-1}} y^{b_2} \dots x^{a_{k-2}} y^{b_{k-2}},$$
$$w_5(x,y) = x^{a_2} y^{b_2} \dots x^{a_{k-2}} y^{b_{k-2}} x^{a_{k-1}} y^{-b_{k-1} + b_k - b_1}.$$

The Length of w_4 is $k-3$, and the length of w_5 is $k-2$. Hence, $\deg_u Q = k-2$. Moreover, $\deg_s Q \le A - 2a_k - k + 2 \le A - k$ and

$$\deg_t Q \le B - b_1 - b_{k-1} - b_k - b_{k-1} + b_k - b_1 - k + 2 \le B - k.$$

Once more, we find out that conditions (3) are met by Q. □

Remark 2.6. Assume that $a_i, b_i \neq 0$ but not necessarily positive. In view of Remark 2.4, for the word $w = x^{a_1}y^{b_1}\dots x^{a_k}y^{b_k}$ equation (2) implies that

$$\mathrm{tr}(w) = \sum_0^k u^r G_r(s,t) \text{ and } G_k(s,t) = \prod_{i=1}^k f_{a_i,b_i}. \tag{4}$$

3. Basic facts on the word $w(x,y) = x^a y^b$ and finite groups

In this section we present some elementary facts regarding the surjectivity of the word map $w = x^a y^b$ on finite groups.

Proposition 3.1. *Let G be a finite group and let a be an integer. Then the word map corresponding to $w = x^a$ is surjective on G if and only if* $\gcd(|G|, a) = 1$.

Proof. Let $d = \gcd(|G|, a)$. If $d > 1$ then there exists some prime p which divides both a and $|G|$. Thus, G contains some element $g \neq id$ of order p, and moreover,

$$g^a = (g^p)^{a/p} = id.$$

Hence the word map $w = x^a$ is not 1 to 1, and cannot be surjective on G.

If $d = 1$ then there exists some integer l s.t. $l \cdot a \equiv 1 \pmod{|G|}$. Let $g \in G$ and take $x = g^l$, then

$$x^a = (g^l)^a = g^{l \cdot a} = g^1 = g,$$

as needed. □

Proposition 3.2. *Let G be a finite group and let a, b be two relatively prime integers. Then the word map corresponding to $w = x^a y^b$ is always surjective on G.*

Proof. Since a, b are relatively prime, there exist integers k, l s.t. $k \cdot a + l \cdot b = 1$. Let $g \in G$ and take $x = g^k$ and $y = g^l$, then $x^a y^b = g^{k \cdot a} g^{l \cdot b} = g^{k \cdot a + l \cdot b} = g^1 = g$. □

Proposition 3.3. *Let G be a finite group and let a, b be two integers. If either a or b is relatively prime to $|G|$ then the word map corresponding to $w = x^a y^b$ is surjective on G.*

Proof. Assume that a is relatively prime to $|G|$. Then there exists some integer l s.t. $l \cdot a \equiv 1 \pmod{|G|}$. Then for every $g \in G$, take $x = g^l$ and $y = id$. Thus,

$$x^a y^b = (g^l)^a \cdot id^b = g^{l \cdot a} \cdot id = g^1 = g.$$

□

Remark 3.4. Let G be a finite group and let $w = x^a y^b$. We can always assume that $0 \leq a, b < \exp(G)$. Moreover, if G is of even order, we can assume that $0 \leq a, b \leq \exp(G)/2$.

Indeed, let $a_1 = a \bmod \exp(G)$ and $b_1 = b \bmod \exp(G)$, then for every $x, y \in G$, $x^a y^b = x^{a_1} y^{b_1}$. Hence, $x^a y^b$ is surjective on G if and only if $x^{a_1} y^{b_1}$ is surjective on G.

If $\exp(G)$ is even, let

$$a_2 = \begin{cases} a_1 & \text{if } a_1 \leq \exp(G)/2 \\ \exp(G) - a_1 & \text{if } a_1 > \exp(G)/2 \end{cases} \text{ and } b_2 = \begin{cases} b_1 & \text{if } b_1 \leq \exp(G)/2 \\ \exp(G) - b_1 & \text{if } b_1 > \exp(G)/2 \end{cases}.$$

Then, for every $x, y \in G$, $x^{a_1} y^{b_1} = x^{\epsilon_1 a_2} y^{\epsilon_2 b_2}$, where $\epsilon_1, \epsilon_2 \in \{\pm 1\}$, and

$$\begin{aligned} &\{z = x^{a_2} y^{b_2} : \ x, y \in G\} = \{z = x^{-a_2} y^{b_2} : \ x, y \in G\} \\ =&\{z = x^{a_2} y^{-b_2} : \ x, y \in G\} = \{z = x^{-a_2} y^{-b_2} : \ x, y \in G\}. \end{aligned}$$

4. Properties of the groups SL(2, q) and PSL(2, q)

In this section we summarize some well-known properties of the groups SL(2, q) and PSL(2, q) (see for example [Do] and [Su]).

Let $q = p^e$, where p is a prime number and $e \geq 1$. Recall that GL(2, q) is the group of invertible 2×2 matrices over the finite field with q elements, which we denote by $\mathbb{F}_q$, and SL(2, q) is the subgroup of GL(2, q) comprising the matrices with determinant 1. Then PGL(2, q) and PSL(2, q) are the quotients of GL(2, q) and SL(2, q) by their respective centers. Also recall that PSL(2, q) is *simple* for $q \neq 2, 3$.

Denote $d = \gcd(2, q-1) = \begin{cases} 1 & \text{if } q \text{ is even} \\ 2 & \text{if } q \text{ is odd} \end{cases}.$

Then the orders of SL(2, q) and PSL(2, q) are $q(q-1)(q+1)$ and $\frac{1}{d}q(q-1)(q+1)$ respectively, and their respective exponents are $\frac{1}{d}p(q^2-1)$ and $\frac{1}{d^2}p(q^2-1)$.

One can classify the elements of SL(2, q) according to their possible Jordan forms. The following Table 1 lists the three types of (non-trivial) elements, according to whether the characteristic polynomial $P_t(\lambda) := \lambda^2 - t\lambda + 1$ of the matrix $A \in \mathrm{SL}(2, q)$ (where $t = \mathrm{tr}(A)$) has 0, 1 or 2 distinct roots in $\mathbb{F}_q$.

Table 1 shows that there is a deep connection between *traces* of elements in SL(2, q), their *orders* and their *conjugacy classes*, as is expressed in the following Lemmas.

Lemma 4.1.

- *If q is odd, then $x \in \mathrm{SL}(2, q)$ has order 4 if and only if $\mathrm{tr}(x) = 0$.*
- *$x \in \mathrm{SL}(2, q)$ has order 3 if and only if $\mathrm{tr}(x) = -1$.*
- *If $p \geq 5$, then $x \in \mathrm{SL}(2, q)$ has order 6 if and only if $\mathrm{tr}(x) = 1$.*

Moreover, for any $x \in \mathrm{SL}(2, q)$ satisfying $\mathrm{tr}(x) \neq 0, \pm 1, \pm 2$, there exists some $y \in \mathrm{SL}(2, q)$ such that $\mathrm{tr}(x) \neq \mathrm{tr}(y)$, but the orders of x and y are the same.

element type	roots of $P_t(\lambda)$	canonical form in $\mathrm{SL}(2,\overline{\mathbb{F}}_p)$	order in $\mathrm{SL}(2,q)$	order in $\mathrm{PSL}(2,q)$	conjugacy classes in $\mathrm{SL}(2,q)$
id	1 root	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	1	1	one element
$-id$	1 root	$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$	d	1	one element
unipotent	1 root	$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ $t=2$	p	p	d conjugacy classes each of size $\frac{q^2-1}{d}$
	1 root	$\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}$ $t=-2$	dp	p	d conjugacy classes each of size $\frac{q^2-1}{d}$
semisimple split	2 roots	$\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{-1}\end{pmatrix}$ where $\alpha \in \mathbb{F}_q^*$ and $\alpha+\alpha^{-1}=t$	divides $q-1$	divides $\frac{q-1}{d}$	for each t: one conjugacy class of size $q(q+1)$
semisimple non-split	no roots	$\begin{pmatrix}\alpha & 0\\ 0 & \alpha^{q}\end{pmatrix}$ where $\alpha \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ $\alpha^{q+1}=1$ and $\alpha+\alpha^q=t$	divides $q+1$	divides $\frac{q+1}{d}$	for each t: one conjugacy class of size $q(q-1)$

TABLE 1. Elements in the groups $\mathrm{SL}(2,q)$ and $\mathrm{PSL}(2,q)$.

Proof. If $m>2$ is an integer dividing $q-1$ then $\mathbb{F}_q\setminus\{0,1,-1\}$ contains $\phi(m)$ elements of order m, where ϕ denotes *Euler's phi function.* Similarly, if $m>2$ divides $q+1$ then $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ contains $\phi(m)$ elements α of order m satisfying $\alpha^{q+1}=1$.

Hence, if $m>2$ divides either $q-1$ or $q+1$, then

$$\#\{t\in\mathbb{F}_q:\ t=\mathrm{tr}(x),\ x\in\mathrm{SL}(2,q),\ |x|=m\}=\frac{\phi(m)}{2}.$$

The claim follows from the fact that $\phi(m)\geq 4$ if and only if $m\neq 1,2,3,4,6$. □

Lemma 4.2. *Assume that q is odd, take $\lambda\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ satisfying $\lambda^2\in\mathbb{F}_q$, and let $g=\begin{pmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{pmatrix}$. Then for any $x\in\mathrm{SL}(2,q)$, $gxg^{-1}\in\mathrm{SL}(2,q)$, and moreover,*

- *If $\mathrm{tr}(x)=2$ then exactly one of x, gxg^{-1} is conjugate in $\mathrm{SL}(2,q)$ to $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$;*
- *If $\mathrm{tr}(x)=-2$ then exactly one of x, gxg^{-1} is conjugate in $\mathrm{SL}(2,q)$ to $\begin{pmatrix}-1 & 1\\ 0 & -1\end{pmatrix}$.*

Proof. Let $x = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2,q)$, then $gxg^{-1} = \begin{pmatrix} \alpha & \beta\lambda^2 \\ \gamma\lambda^{-2} & \delta \end{pmatrix} \in \mathrm{SL}(2,q)$.

Moreover, if $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ then $gxg^{-1} = \begin{pmatrix} 1 & \lambda^2 \\ 0 & 1 \end{pmatrix}$ is not conjugate to x in $\mathrm{SL}(2,q)$, since λ^2 is not a square of some element in $\mathbb{F}_q$. □

Corollary 4.3. *Let $w \in F_2$ be some non-trivial word, let $z \neq \pm id$ be some matrix in $\mathrm{SL}(2,q)$, and assume that z can be written as $z = w(x,y)$ for some $x, y \in \mathrm{SL}(2,q)$. Then for any matrix $\pm id \neq z' \in \mathrm{SL}(2,q)$ with $\mathrm{tr}(z') = \mathrm{tr}(z)$ there exist $x', y' \in \mathrm{SL}(2,q)$ such that $z' = w(x', y')$.*

Proof. If q is even, or if q is odd and $\mathrm{tr}(z) \neq \pm 2$, then necessarily $z' = hzh^{-1}$ for some $h \in \mathrm{SL}(2,q)$, so one can take $x' = hxh^{-1}$ and $y' = hyh^{-1}$, and then

$$w(x', y') = w(hxh^{-1}, hyh^{-1}) = hw(x,y)h^{-1} = hzh^{-1} = z'.$$

Assume that q is odd, and let $z' \in \mathrm{SL}(2,q)$ be some element with $\mathrm{tr}(z') = 2 = \mathrm{tr}(z)$, then by Lemma 4.2, z' is either conjugate in $\mathrm{SL}(2,q)$ to z or to gzg^{-1} (where $g \in \mathrm{SL}(2,q^2)$).

If $z' = hzh^{-1}$ for some $h \in \mathrm{SL}(2,q)$, take $x' = hxh^{-1}$ and $y' = hyh^{-1}$, and then

$$w(x', y') = w(hxh^{-1}, hyh^{-1}) = hw(x,y)h^{-1} = hzh^{-1} = z'.$$

If $z' = hgzg^{-1}h^{-1}$ for some $h \in \mathrm{SL}(2,q)$, take $x' = hgxg^{-1}h^{-1}$ and $y' = hgyg^{-1}h^{-1}$, and then $x', y' \in \mathrm{SL}(2,q)$ and moreover,

$$w(x', y') = w(hgxg^{-1}h^{-1}, hgyg^{-1}h^{-1}) = hgw(x,y)g^{-1}h^{-1} = hgzg^{-1}h^{-1} = z'.$$

Similarly, if $\mathrm{tr}(z') = -2 = \mathrm{tr}(z)$, then $z' = w(x', y')$ for some $x', y' \in \mathrm{SL}(2,q)$. □

5. Surjectivity of the trace map of $w(x,y) = x^a y^b$ on $\mathbb{F}_q$

Recall that by Lemma 2.3, the trace map of $w(x,y) = x^a y^b$ can be written as

$$\mathrm{tr}\, w(x,y) = u \cdot f_{a,b}(s,t) + h_{a,b}(s,t).$$

The following proposition shows that if neither a nor b is divisible by the exponent of $\mathrm{PSL}(2,q)$, then the polynomial $f_{a,b}(s,t)$ does not vanish identically on $\mathbb{A}^2_{s,t}(\mathbb{F}_q)$.

Proposition 5.1. *Let $a, b \geq 1$ and assume that neither a nor b is divisible by $\frac{p(q^2-1)}{d^2}$. Then $f_{a,b}(s,t)$ does not vanish identically on $\mathbb{A}^2_{s,t}(\mathbb{F}_q)$.*

In particular, the following table summarizes the possible nine cases.

	$p \nmid a$	$\frac{q-1}{d} \nmid a$	$\frac{q+1}{d} \nmid a$
$p \nmid b$	$f_{a,b}(2,2) \neq 0$	$f_{a,b}(s_1,2) \neq 0$	$f_{a,b}(s_2,2) \neq 0$
$\frac{q-1}{d} \nmid b$	$f_{a,b}(2,t_1) \neq 0$	$f_{a,b}(s_1,t_1) \neq 0$	$f_{a,b}(s_2,t_1) \neq 0$
$\frac{q+1}{d} \nmid b$	$f_{a,b}(2,t_2) \neq 0$	$f_{a,b}(s_1,t_2) \neq 0$	$f_{a,b}(s_2,t_2) \neq 0$

where:
$s_1 = \operatorname{tr}(x_1)$, x_1 *is any element of order* $q-1$*;*
$s_2 = \operatorname{tr}(x_2)$, x_2 *is any element of order* $q+1$*;*
$t_1 = \operatorname{tr}(y_1)$, y_1 *is any element of order* $q-1$*;*
$t_2 = \operatorname{tr}(y_2)$, y_2 *is any element of order* $q+1$*.*

Proof. If $f_{a,b}(s,t)$ vanishes identically on $\mathbb{A}^2_{s,t}(\mathbb{F}_q)$, then $\operatorname{tr} w(x,y) = h_{a,b}(s,t)$ does not depend on u. We have to show that it is not the case for every $\mathbb{F}_q$. Take

$$x(\lambda, c) = \begin{pmatrix} \lambda & c \\ 0 & \frac{1}{\lambda} \end{pmatrix}, \quad y(\mu, d) = \begin{pmatrix} \mu & 0 \\ d & \frac{1}{\mu} \end{pmatrix}.$$

Then for any m, n,

$$x(\lambda, u)^n = \begin{pmatrix} \lambda^n & ch_n(\lambda) \\ 0 & \frac{1}{\lambda^n} \end{pmatrix}, \quad y(\mu, v)^m = \begin{pmatrix} \mu^m & 0 \\ dh_n(\mu) & \frac{1}{\mu^m} \end{pmatrix}.$$

Lemma 5.2.

$$h_n(\zeta) = \frac{\zeta^{2n} - 1}{\zeta^{n-1}(\zeta^2 - 1)}.$$

Proof. We use induction on n. For $n = 1$ we have $h_n(\zeta) = 1$.

Assume that for $n > 1$ it is proved. Then, by computing $x(\zeta, c)^{n+1} = x^n x$ and $y(\zeta, d)^{n+1} = y^n y$ from the induction assumption we obtain, respectively,

$$h_{n+1}(\zeta) = \zeta^n + \frac{h_n(\zeta)}{\zeta}; \quad h_{n+1}(\zeta) = \zeta h_n(\zeta) + \frac{1}{\zeta^n}. \tag{5}$$

Both relation lead to the same result:

$$h_{n+1}(\zeta) = \zeta^n + \frac{\zeta^{2n} - 1}{\zeta^n(\zeta^2 - 1)} = \frac{\zeta^{2n}(\zeta^2 - 1) + \zeta^{2n} - 1}{\zeta^n(\zeta^2 - 1)} = \frac{\zeta^{2n+2} - 1}{\zeta^n(\zeta^2 - 1)};$$

$$h_{n+1}(\zeta) = \zeta \frac{\zeta^{2n} - 1}{\zeta^{n-1}(\zeta^2 - 1)} + \frac{1}{\zeta^n} = \frac{\zeta^2(\zeta^{2n} - 1) + (\zeta^2 - 1)}{\zeta^n(\zeta^2 - 1)} = \frac{\zeta^{2n+2} - 1}{\zeta^n(\zeta^2 - 1)}.$$

□

Now, a direct computation shows that

$$\operatorname{tr}(x(\lambda, c)^a y(\mu, d)^b) = \lambda^a \mu^b + cdh_a(\lambda)h_b(\mu) + \frac{1}{\lambda^a \mu^b}.$$

We have to show that for every field $\mathbb{F}_q$ there are $x(\lambda, c)$ and $y(\mu, d)$ such that

$$h_a(\lambda)h_b(\mu) = \frac{(\lambda^{2a} - 1)(\mu^{2b} - 1)}{(\lambda^2 - 1)(\mu^2 - 1)\lambda^{a-1}\mu^{b-1}} \neq 0.$$

Note that $h_n(1) = n$.

Let $\alpha \in \mathbb{F}_q$ be an element such that $\alpha^{q-1} = 1, \alpha^m \neq 1$ for any $m < q-1$, and let $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ be an element satisfying that $\beta^{q+1} = 1, \beta^m \neq 1$ for any $m < q+1$.

Since $\frac{p(q^2-1)}{d^2} \nmid a$ it follows that either p or $\frac{q-1}{d}$ or $\frac{q+1}{d}$ does not divide a. Similarly, either p or $\frac{q-1}{d}$ or $\frac{q+1}{d}$ does not divide b.

Thus, we need to consider nine cases, and in each case we have to find $x(\lambda, c)$ and $y(\mu, d)$ such that $h_a(\lambda)h_b(\mu) \neq 0$. The following table shows that this is possible.

	$p \nmid a$	$\frac{q-1}{d} \nmid a$	$\frac{q+1}{d} \nmid a$
$p \nmid b$	$\lambda = \mu = 1$	$\lambda = \alpha, \mu = 1$	$\lambda = \beta, \mu = 1$
$\frac{q-1}{d} \nmid b$	$\lambda = 1, \mu = \alpha$	$\lambda = \alpha, \mu = \alpha$	$\lambda = \beta, \mu = \alpha$
$\frac{q+1}{d} \nmid b$	$\lambda = 1, \mu = \beta$	$\lambda = \alpha, \mu = \beta$	$\lambda = \beta, \mu = \beta$

□

We can now deduce that if neither a nor b is divisible by the exponent of PSL$(2,q)$, then the trace map of the word $w(x,y) = x^a y^b$ is surjective onto $\mathbb{F}_q$.

Corollary 5.3. *Let $a, b \geq 1$ and assume that neither a nor b is divisible by $\frac{p(q^2-1)}{d^2}$. Then every $\alpha \in \mathbb{F}_q$ can be written as $\alpha = \mathrm{tr}(x^a y^b)$ for some $x, y \in \mathrm{SL}(2,q)$.*

Proof. According to Lemma 2.3 the trace of $w = x^a y^b$ can be written as

$$\mathrm{tr}(w) = u \cdot f(s,t) + h(s,t),$$

where $s = \mathrm{tr}(x), u = \mathrm{tr}(xy), t = \mathrm{tr}(y)$. Namely, it is linear in u and the coefficient of u is a non-trivial polynomial $f(s,t)$ in s and t.

By Proposition 5.1, $f(s,t)$ does not vanish identically on $\mathbb{A}^2_{s,t}(\mathbb{F}_q)$, and hence for every $\alpha \in \mathbb{F}_q$ there is a solution $(s,u,t) \in \mathbb{F}_q^3$ to the equation

$$u \cdot f(s,t) + h(s,t) = \alpha.$$

□

6. Surjectivity of $w(x,y) = x^a y^b$ on SL$(2,q) \setminus \{-id\}$ and PSL$(2,q)$

In this Section we prove Theorems 1.8, 1.9 and 1.10 on the surjectivity of the word map $w(x,y) = x^a y^b$ on SL$(2,q) \setminus \{-id\}$ and PSL$(2,q)$.

By Remark 3.4, throughout this section we can assume that $1 \leq a, b \leq \frac{p(q^2-1)}{d^2}$.

The following two Corollaries follow from the general arguments presented in Section 3.

Corollary 6.1. *If either a is relatively prime to $\frac{p(q^2-1)}{d^2}$ or b is relatively prime to $\frac{p(q^2-1)}{d^2}$, then the word $w(x,y) = x^a y^b$ is surjective on* SL$(2,q)$, *and hence on* PSL$(2,q)$.

Proof. The claim follows immediately from Proposition 3.3. □

Corollary 6.2. *If either $a = \frac{p(q^2-1)}{d^2}$ and b is not relatively prime to $\frac{p(q^2-1)}{d^2}$; or $b = \frac{p(q^2-1)}{d^2}$ and a is not relatively prime to $\frac{p(q^2-1)}{d^2}$; then the word map $w(x,y) = x^a y^b$ is* not *surjective on* PSL$(2,q)$, *and hence not on* SL$(2,q) \setminus \{-id\}$.

Proof. The claim follows immediately from Proposition 3.1. □

Remark 6.3. It follows that the only interesting cases to consider are when $a, b < \frac{p(q^2-1)}{d^2}$, and both a and b are *not* relatively prime to $\frac{p(q^2-1)}{d^2}$.

We can now deduce Proposition 1.6, stating that if $w = x^a y^b$ is non-degenerate with respect to q, then any *semisimple* element z (namely, when $\mathrm{tr}(z) \neq \pm 2$) can be written as $z = x^a y^b$ for some $x, y \in \mathrm{SL}(2, q)$.

Proof of Proposition 1.6. Assume that $w = x^a y^b$ is non-degenerate with respect to q. Without loss of generality, we may assume that $1 \leq a, b \leq \frac{p(q^2-1)}{d^2}$. If $a, b < \frac{p(q^2-1)}{d^2}$ then the result immediately follows from Corollary 5.3 and Section 4. Otherwise, either a or b is relatively prime to $\frac{p(q^2-1)}{d^2}$, and the result follows from Corollary 6.1. □

Unfortunately, a similar result fails to hold when z is *unipotent*, namely when $z \neq \pm id$ and $\mathrm{tr}(z) = \pm 2$. This case will be discussed in detail in Section 8, where we shall prove the following two propositions.

Proposition 6.4. *Let* $1 \leq a, b < \frac{p(q^2-1)}{d^2}$. *Then the image of the word map* $w = x^a y^b$ *contains any non-trivial element* $z \in \mathrm{SL}(2, q)$ *with* $\mathrm{tr}(z) = 2$, *if and only if none of the following obstructions occurs:*

(i) $q = 2^e$, *e is odd and* $a, b \in \{\frac{2(q^2-1)}{3}, \frac{4(q^2-1)}{3}\}$;
(ii) $q \equiv 3 \bmod 4$ *and* $a = b = \frac{p(q^2-1)}{8}$;
(iii) $q \equiv 11 \bmod 12$ *and* $a = b = \frac{p(q^2-1)}{6}$;
(iv) $q \equiv 5 \bmod 12$ *and* $a, b \in \{\frac{p(q^2-1)}{6}, \frac{p(q^2-1)}{12}\}$.

Proposition 6.5. *Assume that q is odd and let* $1 \leq a, b < \frac{p(q^2-1)}{4}$. *Then the image of the word map* $w = x^a y^b$ *contains any element* $z \neq -id$ *with* $\mathrm{tr}(z) = -2$, *unless* $q \equiv 3 \bmod 4$ *and* $a = b = \frac{p(q^2-1)}{8}$.

We can now prove the main theorems.

Proof of Theorem 1.8. Let $q = 2^e$. If $w = x^a y^b$ degenerates with respect to q, then by Corollary 6.2 the word map w is not surjective on $\mathrm{SL}(2, q)$. If obstruction *(i)* occurs then by Proposition 6.4*(i)*, the image of $w = x^a y^b$ does not contain any non-trivial element $z \in \mathrm{SL}(2, q)$ with $\mathrm{tr}(z) = 0$, and hence it cannot be surjective on $\mathrm{SL}(2, q)$.

On the other hand, if $w = x^a y^b$ is non-degenerate with respect to q and obstruction *(i)* does not hold, then by Proposition 1.6 and Proposition 6.4*(i)*, any element $z \in \mathrm{SL}(2, q)$ is in the image of the word map $w = x^a y^b$. □

Proof of Theorem 1.9. Let q be an odd prime power. If $w = x^a y^b$ degenerates with respect to q, then by Corollary 6.2 the word map w is not surjective on $\mathrm{SL}(2, q) \setminus \{-id\}$. If one of obstructions *(ii), (iii), (iv)* occurs then by Proposition 6.4, the image of $w = x^a y^b$ does not contain any non-trivial element $z \in \mathrm{SL}(2, q)$ with $\mathrm{tr}(z) = 2$, and hence it cannot be surjective on $\mathrm{SL}(2, q) \setminus \{-id\}$.

On the other hand, if $w = x^a y^b$ is non-degenerate with respect to q and none of the obstructions *(ii), (iii), (iv)* holds, then by Proposition 1.6, Proposition 6.4 and Proposition 6.5, any element $z \in \mathrm{SL}(2,q) \setminus \{-id\}$ is in the image of the word map $w = x^a y^b$. □

Proof of Theorem 1.10. Let q be an odd prime power. Observe that the word map $w = x^a y^b$ is surjective on PSL$(2,q)$ if and only if for every $z \in \mathrm{SL}(2,q)$ either z or $-z$ can be written as $x^a y^b$ for some $x, y \in \mathrm{SL}(2,q)$.

If $w = x^a y^b$ degenerates with respect to q, then by Corollary 6.2 the word map w is not surjective on PSL$(2,q)$. If obstruction *(ii)* occurs then by Proposition 6.4 and Proposition 6.5 the image of $w = x^a y^b$ does not contain any element $\pm id \neq z \in \mathrm{SL}(2,q)$ with $\mathrm{tr}(z) = 2$ or $\mathrm{tr}(z) = -2$, and hence it cannot be surjective on PSL$(2,q)$.

On the other hand, if $w = x^a y^b$ is non-degenerate with respect to q and obstruction *(ii)* does not hold, then by Proposition 1.6, Proposition 6.4 and Proposition 6.5, for any element $z \in \mathrm{SL}(2,q)$, either z or $-z$ can be written as $x^a y^b$ for some $x, y \in \mathrm{SL}(2,q)$, as needed. □

Proof of Corollary 1.11. If q is odd, then by Theorem 1.10, the word map $w = x^a y^b$ is surjective on PSL$(2,q)$ whenever

$$\frac{p(q^2-1)}{8} > \max\{a, b\}.$$

Thus, one has to prove that

$$q > \sqrt{3a} \implies \frac{p(q^2-1)}{8} > a \tag{6}$$

and

$$|\,\mathrm{PSL}(2,q)| = \frac{q(q^2-1)}{2} > \frac{3\sqrt{3}}{2} a^{3/2} \implies \frac{p(q^2-1)}{8} > a. \tag{7}$$

Assume that $q > \sqrt{3a}$. Since $q \geq 3$ then $q^2 - 1 \geq \frac{8}{9} q^2$. Therefore,

$$\frac{p(q^2-1)}{8} \geq \frac{3(q^2-1)}{8} \geq \frac{3 \cdot 8 \cdot q^2}{9 \cdot 8} = \frac{q^2}{3} > a.$$

Moreover, the inequality

$$\frac{3\sqrt{3}}{2} a^{3/2} < |\,\mathrm{PSL}(2,q)| = \frac{q(q^2-1)}{2} < \frac{q^3}{2},$$

implies that $q > \sqrt{3a}$.

This estimate is sharp. Indeed, if $a = p = q = 3$, we have

$$q = 3 = \sqrt{3a}, \quad \frac{p(q^2-1)}{8} = 3 = a.$$

If q is even, then by Theorem 1.8, the word map $w = x^a y^b$ is surjective on $\mathrm{PSL}(2, q)$ whenever

$$\frac{2(q^2-1)}{3} > \max\{a, b\}.$$

Thus, in this case one has to prove that

$$q > \sqrt{3a} \implies \frac{2(q^2-1)}{3} > a \tag{8}$$

and

$$|\mathrm{PSL}(2,q)| = q(q^2-1) > \frac{3\sqrt{3}}{2} a^{3/2} \implies \frac{2(q^2-1)}{3} > a. \tag{9}$$

If $q > \sqrt{3a}$ then

$$\frac{2(q^2-1)}{3} \geq \frac{2(3a-1)}{3} = 2a - \frac{2}{3} > a.$$

Let us prove (9). If $q = 2$, then $q(q^2-1) = 6 \leq \frac{3\sqrt{3}}{2} a^{3/2}$ for any $a \geq 2$. Hence, we may assume that $q \geq 4$, and then $\frac{2(q^2-1)}{3} \geq 10 > 3$. It follows that (9) is valid for $a = 2, 3$. On the other hand,

$$q(q^2-1) > \frac{3\sqrt{3}}{2} a^{3/2} \implies q^3 > \frac{3\sqrt{3}}{2} a^{3/2}$$

$$\implies q^2 > \frac{3a}{2^{\frac{2}{3}}} \implies \frac{2(q^2-1)}{3} > 2^{\frac{1}{3}} a - \frac{2}{3} \geq a$$

if $a \geq 3$. □

7. Equidistribution of the word map $w(x, y) = x^a y^b$ on $\mathrm{PSL}(2, q)$

The goal of this section is to prove Theorem 1.14. We first consider the case $\tilde{G} = \mathrm{SL}(2, q)$. In this case, the Theorem follows from the following Proposition.

Proposition 7.1. *Denote $\tilde{G} = \mathrm{SL}(2, q)$, let $a, b \geq 1$ and let $w : \tilde{G} \times \tilde{G} \to \tilde{G}$ be the map given by $w(x, y) = x^a y^b$. Then there are a subset $\tilde{S} \subseteq \tilde{G}$, and numbers $A_1(a, b), A_2(a, b)$ such that:*

- *(i)* $|\tilde{S}| = \big(1 - \epsilon(q)\big)|\tilde{G}|$, *where* $0 \leq \epsilon(q) \leq \frac{A_1(a,b)}{q}$;
- *(ii)* $|M_g| = q^3(1 + \delta(q))$ *for any* $g \in \tilde{S}$, *where* $M_g = \{(x, y) \in \tilde{G}^2 \mid w(x, y) = g\}$ *and* $|\delta(q)| \leq \frac{A_2(a,b)}{q}$.

Proof. We fix a, b and maintain the notation of Section 2 omitting only the indices a, b. Let $D = a + b - 1$.

Consider the following commutative diagram of morphisms:

$$\begin{array}{ccc} \tilde{G} \times \tilde{G}(\mathbb{F}_q) & \xrightarrow{\pi} & \mathbb{A}^3_{s,u,t}(\mathbb{F}_q) \\ \downarrow w & \searrow \varphi & \downarrow \psi \\ \tilde{G}(\mathbb{F}_q) & \xrightarrow{\tau} & \mathbb{A}^1_s(\mathbb{F}_q) \end{array} \tag{10}$$

In this diagram:

- $\mathbb{A}^n_{x_1,x_2,\dots}$ denotes an $n-$dimensional affine space with coordinates $x_1, x_2, \dots$;
- $\pi(x,y) = (\mathrm{tr}(x), \mathrm{tr}(xy), \mathrm{tr}(y)) \in \mathbb{A}^3_{s,u,t}$;
- $w(x,y) = x^a y^b \in \tilde{G}$;
- $\psi(s,u,t) = uf(s,t) + h(s,t)$;
- $\tau(x) = \mathrm{tr}(x) \in \mathbb{A}^1_s$;
- $\varphi(x,y) = \mathrm{tr}(w(x,y))$.

By definition, $M_g = w^{-1}(g)$. Let $t \in \mathbb{F}_q$. Denote:

- $N_t = \varphi^{-1}(t) \subseteq \tilde{G}^2$,
- $L_t = \psi^{-1}(t) \subseteq \mathbb{A}^3_{s,u,t}$,
- $T_t = \tau^{-1}(t) \subseteq \tilde{G}$,
- $p(s,u,t) = s^2 + u^2 + t^2 - ust - 4$,
- $\nu_i(t)$, $i = 1, 2$, are solutions of the quadratic equation $x^2 - tx + 1 = 0$,
- $\omega_t^2 = t^2 - 4$.

Note that $\nu_1(t) \neq \nu_2(t)$ if and only if $t \neq 2$. For odd q the condition $\omega_t \in \mathbb{F}_q$ is equivalent to the condition $\nu_{1,2} \in \mathbb{F}_q$.

Recall that if $\pm 2 \neq t \in \mathbb{F}_q$, then all the elements in T_t are conjugate (see Section 4). Thus, if $\mathrm{tr}(g) = t$, then $|M_g| = \frac{|N_t|}{|T_t|}$. From Table 1 in Section 4 we deduce that

$$|T_t| = q^2(1 + \delta_1(t)), \tag{11}$$

where

$$\delta_1(t) = \begin{cases} 0 & \text{if } \omega_t = 0 \\ \frac{1}{q} & \text{if } \omega_t \neq 0 \textit{ and } \nu_{1,2}(t) \in \mathbb{F}_q \\ \frac{-1}{q} & \text{if } \omega_t \neq 0 \textit{ and } \nu_{1,2}(t) \notin \mathbb{F}_q \end{cases}.$$

Hence, in all the cases above, $|\delta_1| \leq \frac{1}{q}$.

We divide the proof into three steps.

Step 1. *Fibers of* π.

Proposition 7.2. (a) *If* $t^2 \neq 4$, *then*

$$|\pi^{-1}(s,u,t)(\mathbb{F}_q)| \begin{cases} = q^3(1 + \delta_2(t)) & \textit{if } p(s,u,t) \neq 0 \\ \leq 2q^3(1 + \frac{1}{q}) & \textit{if } p(s,u,t) = 0 \end{cases},$$

where $|\delta_2| \leq \frac{3}{q}$ *for every* (s,u,t).

(b) $|\pi^{-1}(s,u,\pm 2)(\mathbb{F}_q)| \begin{cases} = q^3 - q & \textit{if } p(s,u,2) \neq 0 \\ \leq 2q^3(1+\delta_1(s)) & \textit{if } p(s,u,2) = 0 \end{cases}.$

The proof of this Proposition follows from the next two Lemmas.

For a fixed $y \in \tilde{G}$ with $\mathrm{tr}(y) = t$, let

$$K_{s,u}(y) = \{x \in \tilde{G} \mid \pi(x,y) = (s,u,t)\}.$$

Lemma 7.3. *Let $t^2 \neq 4$ and $y_t = \begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix}$. Then*

$$|K_{s,u}(y_t)(\mathbb{F}_q)| = \begin{cases} q \pm 1 & \textit{if } p(s,u,t) \neq 0 \\ 1 & \textit{if } p(s,u,t) = 0,\ \nu_{1,2}(t) \notin \mathbb{F}_q \\ 2q-1 & \textit{if } p(s,u,t) = 0,\ \nu_{1,2}(t) \in \mathbb{F}_q \end{cases}. \tag{12}$$

Proof. If $\omega_t \neq 0$ then $K_{s,u}(y_t)$ consists of the matrices

$$x = \begin{pmatrix} \alpha & \beta \\ u + \beta - \alpha t & s - \alpha \end{pmatrix},$$

such that

$$\alpha(s-\alpha) - (u + \beta - \alpha t)\beta = 1. \tag{13}$$

Assume that q is odd. Then (13) is equivalent to

$$\left(\frac{st-2u}{2} + \frac{\omega_t^2 \beta}{2}\right)^2 - \omega_t^2\left(\alpha - \frac{\beta t}{2} - \frac{s}{2}\right)^2 - p(s,u,t) = 0.$$

Thus, if $p(s,u,t) \neq 0$ then $K_{s,u}(y_t)$ is a non-degenerate conic; whereas if $p(s,u,t) = 0$ then $K_{s,u}(y_t)$ is a pair of intersecting straight lines, which are not defined over $\mathbb{F}_q$ if $\omega_t \notin \mathbb{F}_q$, or defined over $\mathbb{F}_q$ if $\omega_t \in \mathbb{F}_q$.

Assume that $q = 2^e$. Substituting $\tilde{\alpha} = \alpha + \frac{u}{t}$, $\tilde{\beta} = \beta + \frac{s}{t}$, we reduce (13) to

$$\tilde{\alpha}^2 + \tilde{\beta}^2 + t\tilde{\alpha}\tilde{\beta} = \frac{p(s,u,t)}{t^2}. \tag{14}$$

Thus, since $t \neq 0$, we have a conic for $p(s,u,t) \neq 0$. Hence, $|K_{s,u}(y_t)(\mathbb{F}_q)| = q \pm 1$ if $p(s,u,t) \neq 0$.

If $p(s,u,t) = 0$ then (14) provides

$$(\nu_1(t)\tilde{\alpha} + \tilde{\beta})(\nu_2(t)\tilde{\alpha} + \tilde{\beta}) = 0 \tag{15}$$

Thus, if $\nu_{1,2}(t) \in \mathbb{F}_q$ we have two intersecting lines, whereas if $\nu_{1,2}(t) \notin \mathbb{F}_q$ we have precisely one point $(0,0)$. ∎

Lemma 7.4. *Let $t = 2$, $\lambda \neq 0$, and $v_\lambda = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$. Then*

$$|K_{s,u}(v_\lambda)(\mathbb{F}_q)| = \begin{cases} q & \text{if } p(s,u,2) \neq 0 \\ 0 & \text{if } p(s,u,2) = 0,\ \nu_{1,2}(s) \notin \mathbb{F}_q \\ 2q \text{ or } q & \text{if } p(s,u,2) = 0,\ \nu_{1,2}(s) \in \mathbb{F}_q \end{cases}. \tag{16}$$

Proof. If $\lambda \neq 0$ then $K_{s,u}(v_\lambda)$ consists of the matrices

$$x = \begin{pmatrix} \alpha & \beta \\ \frac{u-s}{\lambda} & s - \alpha \end{pmatrix},$$

such that

$$\alpha(s-\alpha) - \beta\frac{u-s}{\lambda} = 1.$$

Thus if $p(s,u,2) = (s-u)^2 \neq 0$ then we have q points; whereas if $p(s,u,2) = (s-u)^2 = 0$, then we have

- either two disjoint lines, if $\nu_{1,2}(s) \in \mathbb{F}_q$, $\nu_1 \neq \nu_2$ (for odd q it means that $w_s \neq 0, w_s \in \mathbb{F}_q$);
- or one line, if $\nu_{1,2}(s) \in \mathbb{F}_q, \nu_1 = \nu_2$ (for odd q it means that $w_s = 0$);
- no points, if $\nu_{1,2}(s) \notin \mathbb{F}_q$, (for odd q it means that $w_s \notin \mathbb{F}_q$).

□

Proof of Proposition 7.2.

(a) Indeed, $|\pi^{-1}(s,u,t)(\mathbb{F}_q)| = |K_{s,u}(y_t)(\mathbb{F}_q)| \cdot |T_t|$, thus the claim follows from Lemma 7.3 and Equation (11). Moreover,

$$|\delta_2(t)| \leq |\delta_1(t)| + \frac{1}{q} + |\delta_1(t)|\frac{1}{q} \leq \frac{3}{q}.$$

(b) There are two or three conjugacy classes of matrices y with $\mathrm{tr}(y) = 2$. If $u \neq s$, then $y \neq id$, thus there are $q^2 - 1$ different matrices y to consider, and according to Equation (16),

$$|\pi^{-1}(s,u,\pm 2)(\mathbb{F}_q)| = (q^2-1)q.$$

If $p(s,u,2) = 0$, i.e. $s = u$, then summation over the classes yields

$$|\pi^{-1}(s,u,\pm 2)(\mathbb{F}_q)| \leq 2q(q^2-1) + q^2(1+\delta_1(s)) \leq 2q^3\big(1 + \frac{1}{q}\big).$$

For $t = -2$ the proof is similar.

□

Step 2. *Definition of the set $\tilde{S}$.*

Let

$$A = \{(s,t) \in \mathbb{A}^2_{s,t} \mid f(s,t) = 0\},$$
$$B_\zeta = \{(s,t) \in \mathbb{A}^2_{s,t} \mid h(s,t) = \zeta\},$$
$$C = \{(s,u,t) \in \mathbb{A}^3_{s,u,t} \mid p(s,u,t) = 0\}.$$

Note that C is absolutely irreducible for every field $\mathbb{F}_q$. We first define the set $\Sigma \subset \mathbb{F}_q$ by the following rules.

- *Rule 1.* Assume that there exists $\zeta \in \mathbb{F}_q$ satisfying $p\big(s, \frac{\zeta - h(s,t)}{f(s,t)}, t\big) \equiv 0$ on C. Then $\zeta \in \Sigma$.
- *Rule 2.* Assume that there is an irreducible (over $\overline{\mathbb{F}}_q$) component $A' \subseteq A$ and $\zeta \in \mathbb{F}_q$ such that $h(s,t) \equiv \zeta$ on A'. Then $\zeta \in \Sigma$. Note that since $\deg A = D$ (by Lemma 2.3) there are at most D such numbers.
- *Rule 3.* $2 \in \Sigma$ and $-2 \in \Sigma$.

Remark 7.5. By the above construction, Σ contains all the values ζ such that $A \cap B_\zeta$ contains a curve or $L_\zeta \cap C$ is not a curve.

Now, we can define the sets $\tilde{T} = \tau^{-1}(\Sigma)$ and $\tilde{S} = \tilde{G} \setminus \tilde{T}$.

Lemma 7.6. $|\tilde{S}| = |\tilde{G}|(1 - \varepsilon(q))$, *where* $|\varepsilon(q)| \leq \frac{3+D}{q-1}$.

Proof. Indeed, by construction, $|\Sigma| \leq (3 + D)$. Thus by (11), $|\tilde{T}| \leq (3 + D)q^2\big(1 + \frac{1}{q}\big)$. Hence,

$$|\tilde{S}| = |\tilde{G}| - |\tilde{T}| = |\tilde{G}|(1 - \varepsilon(q)),$$

where

$$|\varepsilon(q)| \leq \frac{(3 + D)q^2(1 + \frac{1}{q})}{q^3 - q} = \frac{3 + D}{q - 1}.$$

□

Step 3. *Estimation of $|M_g|$.*

Let $\zeta \in \mathbb{F}_q \setminus \Sigma$. Then $L_\zeta = \psi^{-1}(\zeta) = Y_\zeta \cup R_\zeta \cup Q_\zeta$, where

$$Y_\zeta = \{(s,u,t) \in L_\zeta \mid p(s,u,t) \neq 0, f(s,t) \neq 0\},$$
$$R_\zeta = \{(s,u,t) \in L_\zeta \mid p(s,u,t) = 0, f(s,t) \neq 0\},$$
$$Q_\zeta = \{(s,u,t) \in L_\zeta \mid f(s,t) = 0\}.$$

In the estimation of the sizes of the above sets, we will use the following fact, which is the case $n = 1$ of [GL, Proposition 12.1].

Claim 7.7. *Let $X \subseteq \mathbb{P}^N$ be a projective curve in the projective space $\mathbb{P}^N$ of degree D defined over $\mathbb{F}_q$. Then*

$$|X(\mathbb{F}_q)| \leq D(q + 1). \qquad (17)$$

Lemma 7.8. $|Q_\zeta(\mathbb{F}_q)| \leq D^2 q$.

Proof. If $f(s,t) = 0$ and $(s,u,t) \in L_\zeta$, then $h(s,t) = \zeta$, i.e.$(s,t) \in A \cap B_\zeta$. Since $\zeta \notin \Sigma$, the set $A \cap B_\zeta$ is finite. Both curves have degree at most D (by Lemma 2.3), hence, by Bézout's Theorem, $|A \cap B_\zeta| \leq D^2$. On the other hand there is no restriction on the value of u. Hence, $|Q_\zeta(\mathbb{F}_q)| \leq D^2 q$. □

Lemma 7.9. $|R_\zeta(\mathbb{F}_q)| \leq 3D(q+1)$.

Proof. Indeed, $R_\zeta(\mathbb{F}_q) = \{p(s,u,t) = 0, uf(s,t) + h(s,t) = \zeta\}$ is a curve, since $\zeta \notin \Sigma$. By Bézout's Theorem, $\deg(R_\zeta) \leq 3D$. Hence, according to Equation (17), $|R_\zeta(\mathbb{F}_q)| \leq 3D(q+1)$. □

Lemma 7.10. $|Y_\zeta(\mathbb{F}_q)| = q^2(1 + \delta_3(q))$ *where* $|\delta_3(\zeta)| \leq \frac{2D}{q}$.

Proof. Since $\deg A = D$, by Equation (17), $|A(\mathbb{F}_q)| \leq D(q+1)$. Hence

$$q^2 - |(\mathbb{A}^2_{s,t} \setminus A)(\mathbb{F}_q)| \leq D(q+1).$$

For every point $(s,t) \in (\mathbb{A}^2_{s,t} \setminus A)(\mathbb{F}_q)$ there is precisely one point $(s, \frac{\zeta - h(s,t)}{f(s,t)}, t) \in Y_\zeta$. Thus,

$$|Y_\zeta(\mathbb{F}_q)| = |(\mathbb{A}^2_{s,t} \setminus A)(\mathbb{F}_q)| = q^2(1 + \delta_3(q)),$$

and

$$|\delta_3(\zeta)| \leq \frac{D(q+1)}{q^2} \leq \frac{2D}{q}.$$

□

We can now estimate $|M_g| = \frac{|N_\zeta|}{|T_\zeta|}$. By Proposition 7.2, we have

$$|\pi^{-1}(Y_\zeta)(\mathbb{F}_q)| = q^5(1 + \delta_4),$$

where

$$|\delta_4| \leq \frac{2D}{q} + \frac{3}{q} + \frac{2D}{q}\frac{3}{q} \leq \frac{8D+3}{q},$$

and

$$|\pi^{-1}(R_\zeta \cup Q_\zeta)(\mathbb{F}_q)| \leq \big(D^2 q + 3D(q+1)\big) 2q^3\big(1 + \frac{1}{q}\big) \leq 2(D^2 + 6D)q^4\big(1 + \frac{1}{q}\big).$$

Therefore

$$\begin{aligned} ||N_\zeta(\mathbb{F}_q)| - q^5(1 + \delta_4)| &= |\pi^{-1}(L_\zeta)(\mathbb{F}_q)| - |\pi^{-1}(Y_\zeta)(\mathbb{F}_q)| \\ &\leq 2(D^2 + 6D)q^4\big(1 + \frac{1}{q}\big), \end{aligned}$$

implying that

$$|N_\zeta(\mathbb{F}_q)| = q^5(1 + \delta_5),$$

where

$$\delta_5 \leq \frac{8D+3}{q} + \frac{2(D^2+6D)(1+\frac{1}{q})}{q} \leq \frac{4D^2 + 32D + 3}{q}.$$

We conclude that

$$|M_g| = \frac{|N_\zeta|}{|T_\zeta|} = \frac{q^5(1+\delta_5)}{q^2(1+\delta_1)} = q^3(1+\delta_6(\zeta)),$$

where

$$|\delta_6(\zeta)| \leq \frac{4D^2+32D+3}{q} + \frac{2}{q} = \frac{4D^2+32D+5}{q}.$$

For completing the proof of Proposition 7.1 it is sufficient to take

$$A_1(a,b) = 2(3+D) \geq \frac{(3+D)q}{q-1},$$

and

$$A_2(a,b) = 4D^2+32D+5.$$

□

We can now prove Theorem 1.14 for the group $G = \mathrm{PSL}(2,q)$.

Proof of Theorem 1.14 for $G = \mathrm{PSL}(2,q)$. Assume that q is odd, denote $G = \mathrm{PSL}(2,q)$ and consider the commutative diagram

$$\begin{array}{ccc} \tilde{G}\times\tilde{G}(\mathbb{F}_q) & \xrightarrow{w_1} & \tilde{G}(\mathbb{F}_q) \\ \downarrow \rho' & \searrow \varkappa & \downarrow \rho \\ G\times G(\mathbb{F}_q) & \xrightarrow{w_2} & G(\mathbb{F}_q) \end{array} \tag{18}$$

where

- $\rho : \tilde{G} \to G$ is the natural projection $\tilde{G} \to \tilde{G}/Z(\tilde{G})$;
- $\rho' : \tilde{G}\times\tilde{G} \to G\times G$ is the projection induced by ρ;
- w_1, w_2 correspond to the map $(x,y) \to x^a y^b$ on $\tilde{G}\times\tilde{G}$ and on $G\times G$ respectively.

Define $S = \rho(\tilde{S})$. Since for any $z \in G$, $\rho^{-1}(z)$ contains precisely two elements of $\tilde{G}$, then Proposition 7.1 implies that

$$|S| = \frac{|\tilde{G}|(1-\varepsilon(q))}{2} = |G|(1-\varepsilon(q)).$$

Take $z \in S$, then $\rho^{-1}(z) = \{z_1, z_2\}$, and denote $H_z = w_2^{-1}(z)$. Let $y \in \tilde{G}$ and denote $M_y = w_1^{-1}(y)$. Then $M_{z_1} \cup M_{z_2} = \rho^{-1}(w_2^{-1}(z)) = \rho^{-1}(H_z)$.

Thus,

$$|H_z| = \frac{|M_{z_1}| + |M_{z_2}|}{4} = \frac{2q^3(1+\delta(q))}{4} = |G|(1+\delta'(q)),$$

where $|\delta'(q)| \to 0$ when $q \to \infty$. □

8. Non-surjectivity of some words $w(x,y) = x^ay^b$

In this section we prove Propositions 6.4 and 6.5, and in particular, we show that there are certain fields q and positive integers a,b such that the trace map corresponding to the word $w = x^ay^b$ is surjective on $\mathbb{F}_q$, by Corollary 5.3, however, the word $w = x^ay^b$ itself is not surjective on $\mathrm{SL}(2,q)$ (or $\mathrm{PSL}(2,q)$), since the image of w does not contain $-id$ or unipotent elements, yielding the obstructions described in Definition 1.7.

8.1. **Proof of Propositions 6.4 and 6.5.**

Proof of Proposition 6.4. Since $\frac{p(q^2-1)}{d^2} \nmid a$ it follows that either p or $\frac{q-1}{d}$ or $\frac{q+1}{d}$ does not divide a. Similarly, either p or $\frac{q-1}{d}$ or $\frac{q+1}{d}$ does not divide b.

We may consider the following four cases:

Case 1: $p \nmid a$.

Take $x = \begin{pmatrix} 1 & \frac{1}{a} \\ 0 & 1 \end{pmatrix}$ and $y = id$. Then $x^ay^b = x^a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and the claim follows from Corollary 4.3.

For the other cases, it is sufficient to find some $x, y \in \mathrm{SL}(2,q)$ with $s = \mathrm{tr}(x), t = \mathrm{tr}(y)$ satisfying:

$$f_{a,b}(s,t) \neq 0 \text{ and } \mathrm{tr}(x^a) \neq \mathrm{tr}(y^b). \tag{19}$$

Indeed, if $f_{a,b}(s,t) \neq 0$ then one can find some $u \in \mathbb{F}_q$ such that

$$\mathrm{tr}(w) = u \cdot f(s,t) + h(s,t) = 2.$$

Hence, there exist some matrices $x_1, y_1 \in \mathrm{SL}(2,q)$ satisfying $\mathrm{tr}(x_1) = s, \mathrm{tr}(y_1) = t$ and $\mathrm{tr}(x_1y_1) = u$ and so $\mathrm{tr}(x_1^ay_1^b) = 2$. Moreover, $x_1^ay_1^b \neq id$ since

$$\mathrm{tr}(x_1^a) = \mathrm{tr}(x^a) \neq \mathrm{tr}(y^b) = \mathrm{tr}(y_1^b).$$

Therefore, by Corollary 4.3, there exist $x_2, y_2 \in \mathrm{SL}(2,q)$ such that $z = x_2^ay_2^b$ as needed.

Case 2: $\frac{q-1}{d} \nmid a$ and $\frac{q+1}{d} \nmid b$.

Let x and y be two matrices of orders $q-1$ and $q+1$ respectively, and let $s = \mathrm{tr}(x)$ and $t = \mathrm{tr}(y)$. According to the table in Proposition 5.1, $f_{a,b}(s,t) \neq 0$. Moreover, since x is a split element while y is a non-split element, and since $x^a \neq \pm id$, $y^b \neq \pm id$, then $\mathrm{tr}(x^a) \neq \mathrm{tr}(x^b)$, implying (19).

Case 3: $\frac{q-1}{d} \nmid a$ and $\frac{q-1}{d} \nmid b$.

Let x, y be some matrices of order $q-1$ and note that $x^a \neq \pm id$ and $y^b \neq \pm id$. Observe that unless either $|x^a| = |y^b| = 3$ or $|x^a| = |y^b| = 4$, for all elements x, y of order $q-1$, one can find two matrices x, y of order $q-1$ satisfying $\mathrm{tr}(x^a) \neq \mathrm{tr}(y^b)$ (see Lemma 4.1). Let $s = \mathrm{tr}(x)$ and $t = \mathrm{tr}(y)$. According to the table in Proposition 5.1, $f_{a,b}(s,t) \neq 0$, and so (19) holds.

Since $a,b \leq \frac{p(q^2-1)}{2}$ the only cases left to consider are cases $(i),(iii),(v)$ of Remark 8.1. In Proposition 8.4 we will show that in all these cases the image of $w=x^a y^b$ contains every non-trivial element $z \in \mathrm{SL}(2,q)$ with $\mathrm{tr}(z)=2$.

Case 4: $\frac{q+1}{d} \nmid a$ and $\frac{q+1}{d} \nmid b$.

Let x,y be some matrices of order $q+1$ and note that $x^a \neq \pm id$ and $y^b \neq \pm id$. Similarly to Case 3, observe that unless either $|x^a|=|y^b|=3$ or $|x^a|=|y^b|=4$, for all elements x,y of order $q+1$, one can find two matrices x,y of order $q+1$ satisfying $\mathrm{tr}(x^a) \neq \mathrm{tr}(y^b)$ (see Lemma 4.1). Let $s=\mathrm{tr}(x)$ and $t=\mathrm{tr}(y)$. According to the table in Proposition 5.1, $f_{a,b}(s,t) \neq 0$, and so (19) holds.

Since $a,b \leq \frac{p(q^2-1)}{2}$ the only cases left to consider are cases $(ii),(iv),(vi)$ of Remark 8.1. In Proposition 8.3 we will show that in all these cases the image of $w=x^a y^b$ contains no non-trivial element $z \in \mathrm{SL}(2,q)$ with $\mathrm{tr}(z)=2$, yielding the obstructions given in the proposition. □

Proof of Proposition 6.5. Since $\frac{p(q^2-1)}{4} \nmid a$ it follows that either p or $\frac{q-1}{2}$ or $\frac{q+1}{2}$ does not divide a. Similarly, either p or $\frac{q-1}{2}$ or $\frac{q+1}{2}$ does not divide b.

We may consider the following six cases:

Case 1: $p \nmid a$ and $p \nmid b$.

Take: $x = \begin{pmatrix} 1 & -2/a \\ 0 & 1 \end{pmatrix}, \quad y = \begin{pmatrix} 1 & 0 \\ 2/b & 1 \end{pmatrix}$.

Then $x^a = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \quad y^b = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, and so $z = x^a y^b = \begin{pmatrix} -3 & -2 \\ 2 & 1 \end{pmatrix} \neq -id$, satisfies that $\mathrm{tr}(z)=-2$, and the result follows from Corollary 4.3.

For the other cases, it is sufficient to find some $x,y \in \mathrm{SL}(2,q)$ with $s=\mathrm{tr}(x), t=\mathrm{tr}(y)$ satisfying:

$$f_{a,b}(s,t) \neq 0 \text{ and } \mathrm{tr}(x^a) \neq -\mathrm{tr}(y^b). \tag{20}$$

Indeed, if $f_{a,b}(s,t) \neq 0$ then one can find some $u \in \mathbb{F}_q$ such that

$$\mathrm{tr}(w) = u \cdot f(s,t) + h(s,t) = -2.$$

Hence, there exist some matrices $x_1,y_1 \in \mathrm{SL}(2,q)$ satisfying $\mathrm{tr}(x_1)=s, \mathrm{tr}(y_1)=t$ and $\mathrm{tr}(x_1y_1)=u$ and so $\mathrm{tr}(x_1^a y_1^b)=-2$. Moreover, $x_1^a y_1^b \neq -id$ since

$$\mathrm{tr}(x_1^a) = \mathrm{tr}(x^a) \neq -\mathrm{tr}(y^b) = -\mathrm{tr}(y_1^b).$$

Therefore, by Corollary 4.3, there exist $x_2,y_2 \in \mathrm{SL}(2,q)$ such that $z=x_2^a y_2^b$ as needed.

Case 2: $p \nmid a$ and $\frac{q-1}{2} \nmid b$.

Let y be some matrix of order $q-1$ and let $t=\mathrm{tr}(y)$. According to the table in Proposition 5.1, $f_{a,b}(2,t) \neq 0$. Moreover, since y is a non-split element and $y^b \neq \pm id$ then $\mathrm{tr}(y^b) \neq \pm 2$, implying (20).

Case 3: $p \nmid a$ and $\frac{q+1}{2} \nmid b$.

The proof is the same as in Case 2.

Case 4: $\frac{q-1}{2} \nmid a$ and $\frac{q+1}{2} \nmid b$.
Let x and y be two matrices of orders $q-1$ and $q+1$ respectively, and let $s = \mathrm{tr}(x)$ and $t = \mathrm{tr}(y)$. According to the table in Proposition 5.1, $f_{a,b}(s,t) \neq 0$. Moreover, since x is a split element while y is a non-split element, and since $x^a \neq \pm id$, $y^b \neq \pm id$, then $\mathrm{tr}(x^a) \neq \pm \mathrm{tr}(y^b)$, implying (20).

Case 5: $\frac{q-1}{2} \nmid a$ and $\frac{q-1}{2} \nmid b$.
Let x, y be some elements of order $q-1$ and note that $x^a \neq \pm id$ and $y^b \neq \pm id$. Observe that unless $\mathrm{tr}(x^a) = \mathrm{tr}(y^b) = 0$ for all elements x, y of order $q-1$, one can find two matrices x, y of order $q-1$ satisfying $\mathrm{tr}(x^a) \neq -\mathrm{tr}(y^b)$ (see Lemma 4.1). Let $s = \mathrm{tr}(x)$ and $t = \mathrm{tr}(y)$. According to the table in Proposition 5.1, $f_{a,b}(s,t) \neq 0$, and so (20) holds.

Now, the only case left is $q \equiv 1 \bmod 4$ and $a = b = \frac{p(q^2-1)}{8}$ (see Remark 8.1(*iii*)). In Proposition 8.4 we will show that in this case the image of $w = x^a y^b$ contains every element $z \neq -id$ with $\mathrm{tr}(z) = -2$.

Case 6: $\frac{q+1}{2} \nmid a$ and $\frac{q+1}{2} \nmid b$.
Let x, y be some elements of order $q+1$ and note that $x^a \neq \pm id$ and $y^b \neq \pm id$. Similarly to Case 5, observe that unless $\mathrm{tr}(x^a) = \mathrm{tr}(y^b) = 0$ for all elements x, y of order $q+1$, one can find two matrices x, y of order $q+1$ satisfying $\mathrm{tr}(x^a) \neq -\mathrm{tr}(y^b)$ (see Lemma 4.1). Let $s = \mathrm{tr}(x)$ and $t = \mathrm{tr}(y)$. According to the table in Proposition 5.1, $f_{a,b}(s,t) \neq 0$, and so (20) holds.

Now, the only case left is $q \equiv 3 \bmod 4$ and $a = b = \frac{p(q^2-1)}{8}$ (see Remark 8.1(*iv*)). In Proposition 8.3 we will show that in this case the image of $w = x^a y^b$ contains no element $z \neq -id$ with $\mathrm{tr}(z) = -2$, yielding the obstruction given in the proposition. □

8.2. **Obstructions for surjectivity of the word $w(x, y) = x^a y^b$.**

Remark 8.1. In the course of the proof of Propositions 6.4 and 6.5, we need to consider the following special cases:

(*i*) q is even, $|x^a|, |y^b| \in \{1, 2, 3\}$ for all $x, y \in \mathrm{SL}(2, q)$, and $|x^a| = |y^b| = 3$ if $|x| = |y| = q-1$:
Namely, $q = 2^e$, e is even, $\frac{q-1}{3}|a$, $q+1|a$, $2|a$ (and similarly for b). Hence, a and b are multiples of
$$\mathrm{lcm}\left(\frac{q-1}{3}, q+1, 2\right) = \frac{2(q^2-1)}{3},$$
namely, $a, b \in \{\frac{2(q^2-1)}{3}, \frac{4(q^2-1)}{3}\}$. By Remark 3.4, it is enough to consider the case $a = b = \frac{2(q^2-1)}{3}$.

(*ii*) q is even, $|x^a|, |y^b| \in \{1, 2, 3\}$ for all $x, y \in \mathrm{SL}(2, q)$, and $|x^a| = |y^b| = 3$ if $|x| = |y| = q+1$:

Namely, $q = 2^e$, e is odd, $\frac{q+1}{3}|a$, $q-1|a$, $2|a$ (and similarly for b). Hence, a and b are multiples of

$$\mathrm{lcm}\left(\frac{q+1}{3}, q-1, 2\right) = \frac{2(q^2-1)}{3},$$

namely, $a, b \in \{\frac{2(q^2-1)}{3}, \frac{4(q^2-1)}{3}\}$. By Remark 3.4, it is enough to consider the case $a = b = \frac{2(q^2-1)}{3}$.

(iii) q ia odd, $|x^a|, |y^b| \in \{1, 2, 4\}$ for all $x, y \in \mathrm{SL}(2,q)$, and $|x^a| = |y^b| = 4$ if $|x| = |y| = q-1$:

Namely, $q \equiv 1 \bmod 4$, $\frac{q-1}{4}|a$, $\frac{q+1}{2}|a$, $p|a$ (and similarly for b). Hence,

$$a = b = \mathrm{lcm}\left(\frac{q-1}{4}, \frac{q+1}{2}, p\right) = \frac{p(q^2-1)}{8}.$$

(iv) q is odd, $|x^a|, |y^b| \in \{1, 2, 4\}$ for all $x, y \in \mathrm{SL}(2,q)$, and $|x^a| = |y^b| = 4$ if $|x| = |y| = q+1$:

Namely, $q \equiv 3 \bmod 4$, $\frac{q+1}{4}|a$, $\frac{q-1}{2}|a$, $p|a$ (and similarly for b). Hence,

$$a = b = \mathrm{lcm}\left(\frac{q+1}{4}, \frac{q-1}{2}, p\right) = \frac{p(q^2-1)}{8}.$$

(v) q is odd, $|x^a|, |y^b| \in \{1, 2, 3\}$ for all $x, y \in \mathrm{SL}(2,q)$, and $|x^a| = |y^b| = 3$ if $|x| = |y| = q-1$:

Namely, $q \equiv 1 \bmod 6$, $\frac{q-1}{3}|a$, $\frac{q+1}{2}|a$, $p|a$ (and similarly for b). Hence a and b are multiples of

$$\mathrm{lcm}\left(\frac{q-1}{3}, \frac{q+1}{2}, p\right) = \begin{cases} \frac{p(q^2-1)}{6} & \text{if } q \equiv 1 \bmod 12 \\ \frac{p(q^2-1)}{12} & \text{if } q \equiv 7 \bmod 12 \end{cases}.$$

(vi) q is odd, $|x^a|, |y^b| \in \{1, 2, 3\}$ for all $x, y \in \mathrm{SL}(2,q)$, and $|x^a| = |y^b| = 3$ if $|x| = |y| = q+1$:

Namely, $q \equiv 5 \bmod 6$, $\frac{q+1}{3}|a$, $\frac{q-1}{2}|a$, $p|a$ (and similarly for b). Hence a and b are multiples of

$$\mathrm{lcm}\left(\frac{q+1}{3}, \frac{q-1}{2}, p\right) = \begin{cases} \frac{p(q^2-1)}{6} & \text{if } q \equiv 11 \bmod 12 \\ \frac{p(q^2-1)}{12} & \text{if } q \equiv 5 \bmod 12 \end{cases}.$$

In order to investigate these obstructions in detail, we need the following technical result on unipotent elements.

It follows from Theorem 2.2 and Section 4 that for any matrix $z \in \mathrm{SL}(2,q)$ with $\mathrm{tr}(z) \neq \pm 2$ and any two integers $m, n > 2$ dividing $p(q^2-1)$, one can find two matrices x and y, such that $x^m = id = y^n$ and $z = xy$. However, a similar result fails to hold if z is *unipotent.*

Proposition 8.2. *Let $z \in \mathrm{SL}(2,q)$ be a unipotent element (i.e. $z \neq \pm id$ and $\mathrm{tr}(z) = \pm 2$), and let $m, n > 2$ be two integers dividing $p(q^2-1)$. Then there exist $x, y \in \mathrm{SL}(2,q)$, such that $x^m = id = y^n$ and $z = xy$, if and only if none of the following conditions hold:*

(i) $q = 2^e$, e *is odd,* $\mathrm{tr}(z) = 0$ *and* $m = n = 3$;
(ii) $q \equiv 3 \bmod 4$, $\mathrm{tr}(z) = \pm 2$ *and* $m = n = 4$;
(iii) $q \equiv 5 \bmod 6$, $\mathrm{tr}(z) = 2$ *and* $m = n = 3$.

Proof. If $m, n > 2$ are two integers dividing $p(q^2-1)$, then one can find $m', n' > 2$ satisfying $m'|m$, $n'|n$ and moreover, either $m' = p$ or $m'|q-1$ or $m'|q+1$, and either $n' = p$ or $n'|q-1$ or $n'|q+1$. Thus, there exist some matrices x, y in $\mathrm{SL}(2,q)$ such that x has order m' and y has order n', namely $x^{m'} = id = x^{n'}$, and so $x^m = id = x^n$.

Assume that $\mathrm{tr}(z) = 2$. If $m' = p$ then we can take $x = z$ and $y = id$. Thus we may assume that both m' and n' are relatively prime to p. Hence, unless $m' = n' = 3$ or $m' = n' = 4$, one can find two matrices $x_1, y_1 \in \mathrm{SL}(2,q)$ such that $x_1^{m'} = id = y_1^{n'}$ and $\mathrm{tr}(x_1) \neq \mathrm{tr}(y_1)$ (see Lemma 4.1). Let $s = \mathrm{tr}(x_1)$ and $t = \mathrm{tr}(y_1)$.

By Theorem 2.2, there exist two matrices $x_2, y_2 \in \mathrm{SL}(2,q)$ with $s = \mathrm{tr}(x_2)$, $t = \mathrm{tr}(y_2)$ and $\mathrm{tr}(x_2y_2) = 2$. Since $s \neq t$ then $x_2y_2 \neq id$, and hence, by Corollary 4.3, there exist some $x, y \in \mathrm{SL}(2,q)$ with $\mathrm{tr}(x) = s$ and $\mathrm{tr}(y) = t$ satisfying $z = xy$.

Now, assume that $\mathrm{tr}(z) = -2$. Unless $m' = n' = 4$, one can find two matrices $x_1, y_1 \in \mathrm{SL}(2,q)$ such that $x_1^{m'} = id = y_1^{n'}$ and $\mathrm{tr}(x_1) \neq -\mathrm{tr}(y_1)$ (see Lemma 4.1). Let $s = \mathrm{tr}(x_1)$ and $t = \mathrm{tr}(y_1)$. By Theorem 2.2, there exist two matrices $x_2, y_2 \in \mathrm{SL}(2,q)$ with $s = \mathrm{tr}(x_2)$, $t = \mathrm{tr}(y_2)$ and $\mathrm{tr}(x_2y_2) = -2$. Since $s \neq -t$ then $x_2y_2 \neq -id$, and hence, by Corollary 4.3, there exist some $x, y \in \mathrm{SL}(2,q)$ with $\mathrm{tr}(x) = s$ and $\mathrm{tr}(y) = t$ satisfying $z = xy$.

It is left to consider the cases $m' = n' = 4$ and $m' = n' = 3$.

For an odd q, in case $m' = n' = 4$ we have $s = \mathrm{tr}(x) = \mathrm{tr}(y) = t = 0$, and $\omega_t^2 = -4$. In Lemma 7.3 it is shown that such pair with $x \neq y^{-1}$ exists if and only if $\omega_t \in \mathbb{F}_q$, therefore if and only if $q \equiv 1 \bmod 4$.

In case $m' = n' = 3$ we have $s = \mathrm{tr}(x) = \mathrm{tr}(y) = t = -1$ and $\omega_t^2 = -3$. Hence, $\omega_t \in \mathbb{F}_{p^e}$ if and only if either e is even or e is odd and $p \equiv 1 \bmod 6$, namely if and only if $q = p^e \equiv 1 \bmod 6$.

In case $q = 2^e$ and $m' = n' = 3$ we have $s = \mathrm{tr}(x) = \mathrm{tr}(y) = t = 1$, and $\nu_{1,2}$ are the roots of the polynomial $\alpha^2 + \alpha + 1$. These roots belong to the field $\mathbb{F}_{2^e}$ if and only if e is even. □

The following proposition shows that the condition that neither a nor b is divisible by the exponent of $\mathrm{PSL}(2,q)$ is not sufficient for the surjectivity of the word $x^a y^b$ on $\mathrm{PSL}(2,q)$ (and on $\mathrm{SL}(2,q) \setminus \{-id\}$), yielding the obstructions given in Propositions 6.4 and 6.5.

Proposition 8.3. *Let q be a prime power, $a, b \geq 1$, and $z \in \mathrm{SL}(2,q)$ a unipotent element, satisfying the conditions given in the following table.*

	$q=p^e$	a,b	*conditions for* z	m
(i)	$q=2^e$, *e is odd*	$a=b=\frac{2(q^2-1)}{3}$	$z\neq id$ *with* $\mathrm{tr}(z)=0$	3
(ii)	$q\equiv 3 \bmod 4$	$a=b=\frac{p(q^2-1)}{8}$	$z\neq \pm id$ *with* $\mathrm{tr}(z)=\pm 2$	4
(iii)	$q\equiv 5 \bmod 12$	$a,b\in\{\frac{p(q^2-1)}{6},\frac{p(q^2-1)}{12}\}$	$z\neq id$ *with* $\mathrm{tr}(z)=2$	3
(iv)	$q\equiv 11 \bmod 12$	$a=b=\frac{p(q^2-1)}{6}$	$z\neq id$ *with* $\mathrm{tr}(z)=2$	3

Then, in all these cases, z does not belong to the image of $w=x^ay^b$.

Proof. By Remark 8.1, for every $x,y\in \mathrm{SL}(2,q)$ either $x^a=\pm id$ or x^a is of order m, and similarly for y^b. If $z=x^ay^b$ is unipotent then necessarily $x^a\neq \pm id$ and $y^b\neq \pm id$, hence both x^a and y^b are of order m. Assume that z is given as above. According to Proposition 8.2, in all these cases z cannot be written as a product of two matrices of order m, hence, z is not in the image of the word map $w=x^ay^b$. □

Proposition 8.4. *Let q be a prime power, $a,b\geq 1$, and $z\in \mathrm{SL}(2,q)$ a unipotent element, satisfying the conditions given in the following table.*

	$q=p^e$	a,b	*conditions for* z	m
(i)	$q=2^e$, *e is even*	$a=b=\frac{2(q^2-1)}{3}$	$z\neq id$ *with* $\mathrm{tr}(z)=0$	3
(ii)	$q\equiv 1 \bmod 4$	$a=b=\frac{p(q^2-1)}{8}$	$z\neq \pm id$ *with* $\mathrm{tr}(z)=\pm 2$	4
(iii)	$q\equiv 1 \bmod 12$	$a=b=\frac{p(q^2-1)}{6}$	$z\neq id$ *with* $\mathrm{tr}(z)=2$	3
(iv)	$q\equiv 7 \bmod 12$	$a,b\in\{\frac{p(q^2-1)}{6},\frac{p(q^2-1)}{12}\}$	$z\neq id$ *with* $\mathrm{tr}(z)=2$	3

Then, in all these cases, z is in the image of $w=x^ay^b$.

Proof. According to Proposition 8.2 in all these cases there exist two matrices of order m, x_1 and y_1, such that $z=x_1y_1$. Moreover, by Remark 8.1, any element x order $q-1$ satisfies that x^a has order m. Hence, there exist some $x\in \mathrm{SL}(2,q)$ of order $q-1$ such that $x^a=x_1$ (see Section 4). Similarly, one can find some $y\in \mathrm{SL}(2,q)$ of order $q-1$ such that $y^b=y_1$, and then $x^ay^b=z$ as needed. □

8.3. **Missing $-id$ in the word map.**

Proof of Theorem 1.12. Assume that q is odd and let $K=\max\left\{k: 2^k \textit{ divides } \frac{q^2-1}{2}\right\}$.

Observe that since $2^K \mid \frac{q^2-1}{2}$ and $\gcd(q-1,q+1)=2$, then exactly one of the following holds:

- either $q-1=2^K\cdot m$ and $q+1=2\cdot l$ for some odd integers l,m;
- or $q+1=2^K\cdot m$ and $q-1=2\cdot l$ for some odd integers l,m.

If $2^K\nmid a$ then one can write $a=2^ka'$ for some $k<K$ and some odd integer a'. Without loss of generality we may assume that $q-1=2^K\cdot m$ for some odd integer m.

Let $x_1\in \mathrm{SL}(2,q)$ be some element of order $q-1$ and let $x=x_1^{2^{K-k-1}}$, then

$$x^a=(x^{2^k})^{a'}=(x_1^{2^{K-1}})^{a'}=(x_1^{\frac{q-1}{2}})^{ma'}=(-id)^{ma'}=-id,$$

and hence $-id = x^a id^b$ as needed.

On the other direction, if $2^K \mid a$ then since any element x in $\mathrm{SL}(2,q)$ is either of order p or of order dividing $q-1$ or of order dividing $q+1$, we deduce that x^a is either trivial or of odd order. Similarly, if $2^K \mid b$ then for any element $y \in \mathrm{SL}(2,q)$, y^b is either trivial or of odd order.

If $-id = x^a y^b$ then neither x^a nor y^b is trivial. Let l and m be the orders of x^a and y^b respectively, then both l, m are odd and divide either $q-1$ or $q+1$. Without loss of generality we may assume that both orders of x and y divide $q-1$, and that x^a, and so also y^b, are in diagonal form, namely:

$$x^a = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \quad y^b = \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix},$$

for some $\lambda, \mu \in \mathbb{F}_q$ satisfying $\lambda^l = 1$ and $\mu^m = 1$.

Hence,

$$-id = x^a y^b = \begin{pmatrix} \lambda\mu & 0 \\ 0 & \lambda^{-1}\mu{-1} \end{pmatrix},$$

implying that $\lambda\mu = -1$, but then, since lm is odd,

$$-1 = (-1)^{lm} = (\lambda\mu)^{lm} = (\lambda^l)^m (\mu^m)^l = 1 \cdot 1 = 1,$$

yielding a contradiction. $\square$

References

[BGG] T. Bandman, S. Garion, F. Grunewald, *On the Surjectivity of Engel Words on* PSL$(2,q)$, to appear in Groups Geom. Dyn.

[BGKJ] T. Bandman, F. Grunewald, B. Kunyavskii, N. Jones, *Geometry and arithmetic of verbal dynamical systems on simple groups*, Groups Geom. Dyn. **4**, no. 4, (2010), 607–655.

[Bo] A. Borel, *On free subgroups of semisimple groups*, Enseign. Math. (2) **29** (1983), no. 1-2, 151–164.

[CMS] J. Cossey, Sh. O. Macdonald, A. P. Street, *On the laws of certain finite groups*, J. Australian Math. Soc. **11** (1970), 441–489.

[Do] L. Dornhoff, *Group Representation Theory*, Part A, Marcel Dekker, 1971.

[Fr] R. Fricke, *Über die Theorie der automorphen Modulgruppen*, Nachr. Akad. Wiss. Göttingen (1896), 91–101.

[FK] R. Fricke, F. Klein, *Vorlesungen der automorphen Funktionen*, vol. 1–2, Teubner, Leipzig, 1897, 1912.

[GS] S. Garion, A. Shalev, *Commutator maps, measure preservation, and T-systems*, Trans. Amer. Math. Soc. **361** (2009), no. 9, 4631–4651.

[GL] Ghorpade, Sudhir R., Lachaud, Gilles, *Etale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. Dedicated to Yuri I. Manin on the occasion of his 65th birthday,* Mosc. Math. J. **2** (2002), no. 3, 589–631.

[Go] W. Goldman, *An exposition of results of Fricke and Vogt*, preprint available at http://www.math.umd.edu/˜wmg/publications.html .

[GM] R. Guralnick, G. Malle, *Products of conjugacy classes and fixed point spaces*, preprint availiable at arXiv:1005.3756.

[La] M. Larsen, *Word maps have large image*, Israel J. Math. **139** (2004), 149–156.

[LS] M. Larsen, A. Shalev, *Word maps and Waring type problems*, J. Amer. Math. Soc. **22** (2009), no. 2, 437–466.

[LST] M. Larsen, A. Shalev, P.H. Tiep, *Waring problem for finite simple groups*, to appear in Annals of Math.

[LOST10] M.W. Liebeck, E.A. O'Brien, A. Shalev, P.H. Tiep, *The Ore conjecture*, J. European Math. Soc. **12** (2010), 939–1008.

[LOST11] M.W. Liebeck, E.A. O'Brien, A. Shalev, P.H. Tiep, *Products of squares in finite simple groups*, to appear in Proc. Amer. Math. Soc.

[Mac] A. M. Macbeath, *Generators of the linear fractional groups*, Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967). Amer. Math. Soc., Providence, R.I. (1969) 14–32.

[Mag] W. Magnus, *Rings of Fricke characters and automorphisms groups of free groups*, Math. Z. **170** (1960), 91–102.

[Se] D. Segal, *Words: notes on verbal width in groups*, London Mathematical Society Lecture Note Series **361**, Cambridge University Press, Cambridge, 2009.

[Sh07] A. Shalev, *Commutators, words, conjugacy classes and character methods*, Turkish J. Math. **31** (2007), suppl., 131–148.

[Sh09] A. Shalev, *Word maps, conjugacy classes, and a non-commutative Waring-type theorem*, Annals of Math. **170** (2009), 1383–1416.

[Su] M. Suzuki. *Group theory*, vol. 1, Springer-Verlag, 1982.

[Vo] H. Vogt, *Sur les invariants fundamentaux des equations différentielles linéaires du second ordre*, Ann. Sci. E.N.S, 3-ième Sér. **4** (1889), Suppl. S.3–S.70.

Bandman: Department of Mathematics, Bar-Ilan University, 52900 Ramat Gan, ISRAEL

E-mail address: bandman@macs.biu.ac.il

Garion: Institut des Hautes Études Scientifiques, 91440 Bures-sur-Yvette, FRANCE

E-mail address: shellyg@ihes.fr