Groups Geom. Dyn. 6 (2012), 409–439
DOI 10.4171/GGD/162

Groups, Geometry, and Dynamics

On the surjectivity of Engel words on PSL$(2, q)$

Tatiana Bandman, Shelly Garion and Fritz Grunewald

Abstract. We investigate the surjectivity of the word map defined by the n-th Engel word on the groups $\mathrm{PSL}(2,q)$ and $\mathrm{SL}(2,q)$. For $\mathrm{SL}(2,q)$ we show that this map is surjective onto the subset $\mathrm{SL}(2,q) \setminus \{-\mathrm{id}\} \subset \mathrm{SL}(2,q)$ provided that $q \geq q_0(n)$ is sufficiently large. Moreover, we give an estimate for $q_0(n)$. We also present examples demonstrating that this does not hold for all q. We conclude that the n-th Engel word map is surjective for the groups $\mathrm{PSL}(2,q)$ when $q \geq q_0(n)$. By using a computer, we sharpen this result and show that for any $n \leq 4$ the corresponding map is surjective for *all* the groups $\mathrm{PSL}(2,q)$. This provides evidence for a conjecture of Shalev regarding Engel words in finite simple groups. In addition, we show that the n-th Engel word map is almost measure-preserving for the family of groups $\mathrm{PSL}(2,q)$, with q odd, answering another question of Shalev.

Our techniques are based on the method developed by Bandman, Grunewald and Kunyavskii for verbal dynamical systems in the group $\mathrm{SL}(2,q)$.

Mathematics Subject Classification (2010). 14G05, 14G15, 20D06, 20G40, 37P25, 37P35, 37P55.

Keywords. Engel words, special linear group, arithmetic dynamics, periodic points, finite fields, trace map.

1. Introduction

1.1. Word maps in finite simple groups. During the last years there was 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 *group word*, that is, a non-identity element of the free group F_d on $x_1,\dots,x_d$. 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 may further assume 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

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

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

It is interesting to estimate the size of $w(G)$. 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 a celebrated result of Shalev [Sh09] one has that 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 $w(G)^3 = G$. These results were substantially improved by Larsen and Shalev [LS] for various families of finite simple groups and have recently been generalized by Larsen, Shalev and Tiep [LST].

One can therefore ask whether $w(G) = G$ for any non-trivial word w and all finite simple non-abelian groups G. The answer to this question is clearly negative. It is easy to see that if G is a finite group and m is an integer which is not relatively prime to the order of G then for the word $w = x_1^m$ one has that $w(G) \neq G$. Hence, if $v \in F_d$ is any word, then the word map corresponding to $w = v^m$ cannot be surjective. A natural question, suggested by Shalev, is whether these words are generally the only exceptions for non-surjective word maps in finite simple non-abelian groups. In particular, the following conjecture was raised:

Conjecture 1.1 (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 now known that for the commutator word $w = [x,y] \in F_2$, one has $w(G) = G$ for any finite simple non-abelian group G. This statement is the well-known *Ore Conjecture*, originally posed in 1951 and proved by Ore himself for the alternating groups [Or]. During the years, this conjecture was proved for various families of finite simple groups (see [LOST] and the references therein). Thompson [Th] established it for the groups $\mathrm{PSL}(n,q)$, later Ellers and Gordeev [EG] proved the conjecture for all finite simple groups of Lie type defined over a field with more than 8 elements, and recently the proof was completed for all finite simple groups in a celebrated work of Liebeck, O'Brien, Shalev and Tiep [LOST].

There was also an interest in quasisimple groups. By [Th] and [LOST], in every quasisimple classical group $\mathrm{SL}(n,q)$, $\mathrm{SU}(n,q)$, $\mathrm{Sp}(n,q)$, $\Omega^{\pm}(n,q)$, every element is a commutator (a *quasisimple* group G is a perfect group such that $G/Z(G)$ is simple). However it is not true that every element of every quasisimple group is a commutator, see the examples in [Bl].

1.2. Engel words. After considering the commutator word, it is natural to consider the Engel words. These words are defined recursively as follows.

Definition 1.2. The *n-th Engel word* $e_n(x,y) \in F_2$ is defined recursively by

$$e_1(x,y) = [x,y] = xyx^{-1}y^{-1},$$
$$e_n(x,y) = [e_{n-1},y] \quad \text{for } n > 1.$$

For a group G, the corresponding map $e_n\colon G \times G \to G$ is called the *n-th Engel word map*.

Now the following conjecture is naturally raised.

Conjecture 1.3 (Shalev). *Let $n \in \mathbb{N}$. Then the n-th Engel word map is surjective for any finite simple non-abelian group G.*

For some (small) finite simple non-abelian groups this conjecture was verified by O'Brien using the Magma computer program.

Note that in order to complete the proof of Ore's Conjecture, Liebeck, O'Brien, Shalev and Tiep used the classical criterion dating back to Frobenius, characterizing the possibility of writing an element g in a finite group G as a commutator by the non-vanishing of the character sum

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)},$$

(see [LOST] and the references therein). Unfortunately, it is unknown whether there is an analogous criterion for the possibility of writing an element as an Engel word e_n, $n > 1$. Hence, Shalev's Conjecture seems to be substantially more difficult than Ore's Conjecture, even for certain families of finite simple groups, such as $\mathrm{PSL}(2,q)$.

1.3. Engel words in $\mathrm{PSL}(2,q)$ and $\mathrm{SL}(2,q)$. We consider Engel words in the particular case of the groups $\mathrm{PSL}(2,q)$ and $\mathrm{SL}(2,q)$, in an attempt to prove Conjecture 1.3 for the group $\mathrm{PSL}(2,q)$.

By Thompson [Th], every element of $\mathrm{SL}(n,q)$, except when $(n,q) = (2,2), (2,3)$, is a commutator (including the central elements). Moreover, Blau [Bl] proved that with a few specified exceptions, every central element of a finite quasisimple group is a commutator. In particular, if G is a quasisimple group of simply connected Lie type, then every element of $Z(G)$ is a commutator. Interestingly, such a result fails to hold for Engel words.

Indeed, in the group $\mathrm{SL}(2,q)$, where q is odd, if $n \geq n_0(q)$ is large enough, then the central element $-\mathrm{id}$ cannot be written as an n-th Engel word, that is, $e_n(x,y) \neq -\mathrm{id}$ for any $x, y \in \mathrm{SL}(2,q)$ (see Proposition 4.8), implying that the n-th Engel word map is not surjective. This leads us to introduce the following notion of "almost surjectivity".

Definition 1.4. A word map $w\colon \mathrm{SL}(2,q)^d \to \mathrm{SL}(2,q)$ is *almost surjective* if $w(\mathrm{SL}(2,q)) = \mathrm{SL}(2,q) \setminus \{-\mathrm{id}\}$.

A method for investigating verbal dynamical systems in the group $\mathrm{SL}(2,q)$, using the so-called *trace map*, was introduced in [BGK]. We use this method to study the dynamics of the trace map instead of solving equations in groups. There is a special property of the Engel word $e_n(x,y)$ which makes the dynamics of the trace map particularly amenable to analysis: for a group G the morphism $G^2 \to G^2$ defined by $(x,y) \mapsto (e_n(x,y),y)$ is not dominant. Using this method we obtain the following result.

Theorem A. *Let $n \in \mathbb{N}$, then the n-th Engel word map is almost surjective for the group* $\mathrm{SL}(2,q)$ *provided that $q \geq q_0(n)$ is sufficiently large.*

We moreover give an estimate for $q_0(n)$, which, unfortunately, is exponential in n (see Corollary 5.8).

Theorem A certainly fails to hold for all groups $\mathrm{SL}(2,q)$. Indeed, we give examples for integers $n \geq 3$ and finite fields $\mathbb{F}_q$ for which the n-th Engel word map is *not* almost surjective for $\mathrm{SL}(2,q)$ (see Example 4.1). We moreover show that there is an infinite family of finite fields $\mathbb{F}_q$, such that if $n \geq n_0(q)$ is large enough, then the n-th Engel word map in not almost surjective on $\mathrm{SL}(2,q)$ (see Proposition 4.10).

Considering the group $\mathrm{PSL}(2,q)$, we see that Theorem A immediately implies that the n-th Engel word map is surjective for the group $\mathrm{PSL}(2,q)$ provided that $q \geq q_0(n)$. Thus, when n is small, one can verify by computer that the n-th Engel word map is surjective for the remaining groups $\mathrm{PSL}(2,q)$ with $q < q_0(n)$, hence for all the groups $\mathrm{PSL}(2,q)$.

Corollary B. *Let $n \leq 4$. Then the n-th Engel word map is surjective for all groups* $\mathrm{PSL}(2,q)$.

We have moreover shown that there are certain infinite families of finite fields $\mathbb{F}_q$ for which the n-th Engel word map in $\mathrm{PSL}(2,q)$ is always surjective for every $n \in \mathbb{N}$. The first family consists of all finite fields of characteristic 2 (see Proposition 4.11), and the second family contains infinitely many finite fields of odd characteristic (see Proposition 4.12). Following Conjecture 1.3 we believe that the surjectivity should in fact hold for all groups $\mathrm{PSL}(2,q)$.

1.4. Equidistribution and measure preservation. Another interesting question is the *distribution* of a word map. For a word $w = w(x_1,\dots,x_d) \in F_d$, a finite group G and some $g \in G$, we define

$$N_w(g) = \{(g_1,\dots,g_d) \in G^d \mid w(g_1,\dots,g_d) = g\}.$$

It is therefore interesting to estimate the size of $N_w(g)$, and especially to see whether w is *almost equidistributed*, that is, whether $|N_w(g)| \approx |G|^{d-1}$ for almost all $g \in G$. More precisely, we define:

Definition 1.5. A word map $w\colon G^d \to G$ is *almost equidistributed* for a family of finite groups $\mathcal{G}$ if any group $G \in \mathcal{G}$ contains a subset $S = S_G \subseteq G$ with the following properties:

(i) $|S| = |G|(1 - o(1))$,

(ii) $|N_w(g)| = |G|^{d-1}(1 + o(1))$ uniformly for all $g \in S$,

where $o(1)$ denotes a real number depending only on G which tends to zero as $|G| \to \infty$.

An important consequence (see §3 of [GS]) is that any "almost equidistributed" word map is also "almost measure-preserving", that is:

Definition 1.6. A word map $w\colon G^d \to G$ is *almost measure-preserving* for a family of finite groups $\mathcal{G}$ if every group $G \in \mathcal{G}$ satisfies the following:

(i) For every subset $Y \subseteq G$ we have

$$|w^{-1}(Y)|/|G|^d = |Y|/|G| + o(1).$$

(ii) For every subset $X \subseteq G^d$ we have

$$|w(X)|/|G| \geq |X|/|G|^d - o(1).$$

(iii) In particular, if $X \subseteq G^d$ and $|X|/|G|^d = 1 - o(1)$, then almost every element $g \in G$ can be written as $g = w(g_1, \ldots, g_d)$ where $g_1, \ldots, g_d \in X$.

Here $o(1)$ denotes a real number depending only on G which tends to zero as $|G| \to \infty$.

The following question was raised by Shalev.

Question 1.7 (Shalev, [Sh07], Problem 2.10). Which words w induce almost measure-preserving word maps $w\colon G^d \to G$ on finite simple groups G?

It was proved in [GS] that the commutator word $w = [x, y] \in F_2$ as well as the words $w = [x_1, \ldots, x_d] \in F_d$, d-fold commutators in any arrangement of brackets, are almost equidistributed, and hence also almost measure-preserving, for the family of finite simple non-abelian groups.

A natural question, suggested by Shalev, is whether this remains true also for the Engel words. We prove that this is indeed true for the family of groups PSL$(2,q)$, where q is odd.

Theorem C. *Let $n \in \mathbb{N}$. Then the n-th Engel word map is almost equidistributed, and hence also almost measure-preserving, for the family of groups* $\{\mathrm{PSL}(2,q) \mid$ *q is odd*$\}$.

Since it is well known that almost all pairs of elements in $\mathrm{PSL}(2,q)$ are generating pairs (see [KL]), we deduce that, for any $n \in \mathbb{N}$, the probability that a randomly chosen element $g \in \mathrm{PSL}(2,q)$, where q is odd, can be written as an Engel word $e_n(x,y)$ where x, y generate $\mathrm{PSL}(2,q)$, tends to 1 as $q \to \infty$.

It was proved in [MW] that when $q \geq 13$ is odd, every nontrivial element of $\mathrm{PSL}(2,q)$ is a commutator of a generating pair. One can therefore ask if a similar result also holds for the Engel words.

1.5. Notation and layout. Throughout the paper we use the following notation:

$G = \mathrm{PSL}(2,q)$;

$\widetilde{G} = \mathrm{SL}(2,q)$;

$\overline{\mathbb{F}}_q$ is the algebraic closure of the finite field $\mathbb{F}_q$;

$|M|$ is the number of points in a set M;

$\mathbb{A}^k_{x_1,\dots,x_k}$ is the k-dimensional affine space with coordinates $x_1,\dots,x_k$;

$p(s,u,t) = s^2 + t^2 + u^2 - sut - 2$;

$d(X)$ is the degree of a projective set X;

$g(X)$ is the geometric genus of a projective curve X;

$f^{(n)}$ stands for n-th iteration of a morphism f.

Some words on the layout of this paper. In Section 2 we recall the general method developed in [BGK] for investigating verbal systems in the group $\mathrm{SL}(2,q)$. We apply this method to Engel words in Section 3. In Section 4 we discuss the surjectivity (and non-surjectivity) of Engel words in the groups $\mathrm{SL}(2,q)$ and $\mathrm{PSL}(2,q)$ for certain families of finite fields. The proof of our main theorem, Theorem A, appears in Section 5. In Section 6 we check the surjectivity of short Engel words for all groups $\mathrm{PSL}(2,q)$ and prove Corollary B. The proof of the equidistribution theorem, Theorem C, appears in Section 7. In Section 8 we discuss further questions and conjectures.

2. The trace map

The main idea is to use the method that was introduced in [BGK] to investigate verbal dynamical systems. This method is based on the following classical Theorem (see, for example, [Vo], [Fr], [FK] or [Ma], [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 $\widetilde{G} = \mathrm{SL}(2, q)$. The general case, $\mathrm{SL}(2, R)$, where R is a commutative ring, can be found in [CMS].

The construction used below is described in detail in [BGK]. In this construction, $\mathrm{SL}(2, \overline{\mathbb{F}}_q)$ is considered as an affine variety, which we shall denote by $\widetilde{G}$ as well, since no confusion may arise. We will also consider $\mathrm{SL}(2, \mathbb{F}_q)$ as a special fiber at q of a $\mathbb{Z}$-scheme $\mathrm{SL}(2, \mathbb{Z})$.

For any $x, y \in \widetilde{G}$ denote $s = \mathrm{tr}(x)$, $t = \mathrm{tr}(y)$ and $u = \mathrm{tr}(xy)$, and define a morphism $\pi\colon \widetilde{G} \times \widetilde{G} \to \mathbb{A}^3_{s,u,t}$ by

$$\pi(x, y) := (s, u, t).$$

Theorem 2.2 ([BGK], Theorem 3.4). *For every $\mathbb{F}_q$-rational point $Q = (s_0, u_0, t_0) \in \mathbb{A}^3_{s,u,t}$, the fiber $H = \pi^{-1}(Q)$ has an $\mathbb{F}_q$-rational point.*

Let $\omega(x, y)$ be a word in two variables and let $\tilde{\varphi}\colon \widetilde{G} \times \widetilde{G} \to \widetilde{G}$ be a morphism defined by $\tilde{\varphi}(x, y) = \omega(x, y)$.

The *Trace Map Theorem* implies that there exists a morphism $\psi\colon \mathbb{A}^3_{s,u,t} \to \mathbb{A}^3_{s,u,t}$ such that

$$\psi(\pi(x, y)) = \pi(\tilde{\varphi}(x, y), y). \tag{2.1}$$

This map is called the “trace map”, and it satisfies

$$\psi(s, u, t) := \big(f_1(s, u, t), f_2(s, u, t), t\big), \tag{2.2}$$

where $f_1(s, u, t) = \mathrm{tr}(\tilde{\varphi}(x, y))$ and $f_2(s, u, t) = \mathrm{tr}(\tilde{\varphi}(x, y)y)$.

Define $\varphi = (\tilde{\varphi}, \mathrm{id})\colon \widetilde{G}\times\widetilde{G} \to \widetilde{G}\times\widetilde{G}$ by $\varphi(x, y) = (\tilde{\varphi}(x, y), y)$. Then, according to (2.1) and (2.2), the following diagram commutes:

$$\begin{array}{ccc} \widetilde{G} \times \widetilde{G} & \xrightarrow{\varphi} & \widetilde{G} \times \widetilde{G} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \mathbb{A}^3_{s,u,t} & \xrightarrow{\psi} & \mathbb{A}^3_{s,u,t}. \end{array} \tag{2.3}$$

Therefore, the main idea is to study the properties of the morphism ψ instead of the corresponding word map ω.

As will be shown later, the morphism ψ corresponding to Engel words is much simpler. Moreover, it follows from Theorem 2.2 that the surjectivity of ψ implies the surjectivity of φ (see Proposition 3.6).

3. Trace maps of Engel words

Let $e_n = e_n(x, y)\colon \widetilde{G} \times \widetilde{G} \to \widetilde{G}$ be the n-th Engel word map, and let $s_n = \mathrm{tr}(e_n(x, y))$. Then

$$s_1 = \mathrm{tr}(e_1(x, y)) = \mathrm{tr}([x, y]) = s^2 + t^2 + u^2 - ust - 2 = p(s, u, t).$$

Moreover, for $n \geq 1$,

$$\operatorname{tr}(e_n(x,y)y) = \operatorname{tr}(e_{n-1}ye_{n-1}^{-1}y^{-1}y) = \operatorname{tr}(e_{n-1}ye_{n-1}^{-1}) = \operatorname{tr}(y) = t. \tag{3.1}$$

Therefore, for $n \geq 1$,

$$s_{n+1} = \operatorname{tr}(e_{n+1}) = p(s_n, t, t) = s_n^2 - s_n t^2 + 2t^2 - 2. \tag{3.2}$$

In the notation of diagram (2.3) we have

$$\psi(s,u,t) = (p(s,u,t), t, t). \tag{3.3}$$

This yields a corresponding map $\psi_{n+1}\colon \mathbb{A}^3_{s,u,t} \to \mathbb{A}^3_{s,u,t}$, which satisfies

$$\psi_{n+1}(s,u,t) = \psi^{(n+1)}(s,u,t) = \psi(s_n,u,t) = (p(s_n,t,t),t,t) = (s_{n+1},t,t). \tag{3.4}$$

Remark 3.1. If $n \geq 1$ and $\operatorname{tr}(y) \neq 0$ then $e_n(x,y) \neq -\mathrm{id}$, since $\operatorname{tr}((-\mathrm{id})y) = -\operatorname{tr}(y) \neq \operatorname{tr}(y)$ in contradiction to (3.1).

Define $H = \{(x,y) \in \tilde{G} \times \tilde{G} \mid \operatorname{tr}(xy) = \operatorname{tr}(y)\}$ and $A = \{(s,u,t) \in \mathbb{A}^3_{s,u,t} \mid u = t\} \cong \mathbb{A}^2_{s,t}$. Then $\pi(H) \subseteq A$. Eq. (3.4) now shows that in order to find the image of $\psi_n\colon \mathbb{A}^3_{s,u,t} \to \mathbb{A}^3_{s,u,t}$, one may consider its restriction $\mu^{(n)}\colon \mathbb{A}^2_{s,t} \to \mathbb{A}^2_{s,t}$, where $\mu(s,t) = (s^2 - st^2 + 2t^2 - 2, t)$.

Definition 3.2. Let us introduce the following morphisms:

- $\varphi_n\colon \tilde{G} \times \tilde{G} \to \tilde{G} \times \tilde{G}$, $\varphi_n(x,y) = (e_{n+1}(x,y), y)$, $\varphi_n(x,y) = \varphi_0^{(n+1)}(x,y)$;
- $\theta\colon \tilde{G} \times \tilde{G} \to \tilde{G}$, $\theta(x,y) = x$;
- $\tau\colon \tilde{G} \to \mathbb{A}^1_s$, $\tau(x) = \operatorname{tr}(x)$;
- $\lambda_1\colon \mathbb{A}^2_{s,t} \to \mathbb{A}^1_s$, $\lambda_1(s,t) = s$;
- $\lambda_2\colon \mathbb{A}^3_{s,u,t} \to \mathbb{A}^2_{s,t}$, $\lambda_2(s,u,t) = (s,t)$;
- $\mu\colon \mathbb{A}^2_{s,t} \to \mathbb{A}^2_{s,t}$, $\mu(s,t) = (s^2 - st^2 + 2t^2 - 2, t)$;
- $\mu_n = \mu^{(n)}$;
- $\rho_n\colon \mathbb{A}^2_{s,t} \to \mathbb{A}^1_s$, $\rho_n = \lambda_1 \circ \mu_n$.

These morphisms determine the following commutative diagram:

$$\begin{array}{ccccccc}
\tilde{G} \times \tilde{G} & \xrightarrow{\varphi_0} & H & \xrightarrow{\varphi_0^{(n)}} & H & \xrightarrow{\theta} & \tilde{G} \\
\downarrow \pi & & \downarrow \pi & & \downarrow \pi & & \\
\mathbb{A}^3_{s,u,t} & \xrightarrow{\psi} & A & \xrightarrow{\psi^{(n)}} & A & & \downarrow \tau \\
& & \downarrow \lambda_2 & & \downarrow \lambda_2 & & \\
& & \mathbb{A}^2_{s,t} & \xrightarrow{\mu_n} & \mathbb{A}^2_{s,t} & \xrightarrow{\lambda_1} & \mathbb{A}^1_s.
\end{array} \tag{3.5}$$

Remark 3.3. $\theta \circ \varphi_n(x, y) = e_{n+1}(x, y)$ and $\psi_{n+1}(s, u, t) = (\rho_n \circ \lambda_2(\psi(s, u, t), t, t))$.

Eq. (3.3) shows that the morphism $\widetilde{G}^2 \to \widetilde{G}^2$ defined as $(x, y) \mapsto (e_n(x, y), y)$ is not dominant, since the trace map ψ of the first Engel word $e_1(x, y) = [x, y]$ maps the three-dimensional affine space $\mathbb{A}^3$ into a plane $A = \{u = t\}$. One can consider the trace maps of the following Engel words e_{n+1} as the compositions of this map ψ with the endomorphism μ_n of A.

First, in Proposition 3.4, we find the image $\psi(\mathbb{A}^3) \subset A$ and then in Proposition 3.6 we establish the connection between the image of μ_n and the range of the corresponding Engel word e_{n+1}. In the next section we shall study the properties of μ_n.

Proposition 3.4. *The image* $\Psi_q = \psi(\mathbb{A}^3_{s,u,t}(\mathbb{F}_q))$ *is equal to:*

(1) $A(\mathbb{F}_q)$ *if q is even;*
(2) $A(\mathbb{F}_q) \setminus Z_q \subset A(\mathbb{F}_q)$ *if q is odd, where*

$$Z_q = \{(s, t, t) \in A \mid t^2 = 4 \text{ and } s - 2 \text{ is not a square in } \mathbb{F}_q\}.$$

Proof. We have $(s, t, t) \in \Psi_q$ if $C_{s,t}(\mathbb{F}_q) \neq \emptyset$, where

$$C_{s,t} = \{(s', u, t) \mid p(s', u, t) = s\}.$$

Now

$$p(s', u, t) - s = s'^2 + u^2 + t^2 - us't - 2 - s.$$

Case 1. *q is even*. Then the equation

$$p(s', u, t) - s = s'^2 + u^2 + t^2 - us't - 2 - s = 0$$

has an obvious solution $s' = 0, u^2 = t^2 + s$, since every number in $\mathbb{F}_q$ is a square.

Case 2. *$q \geq 3$ is odd*. Then

$$p(s', u, t) - s = s'^2 + u^2 + t^2 - us't - 2 - s = (s' - \tfrac{ut}{2})^2 - u^2(\tfrac{t^2-4}{4}) + t^2 - 2 - s.$$

Thus, $C_{s,t}$ for a fixed t, is a smooth conic if $t^2 - 2 - s \neq 0$ and $t^2 \neq 4$, with at most two points at infinity. If $t^2 - 2 - s = 0$ then $C_{s,t}$ is a union of two lines

$$\left\{(s' - \tfrac{ut}{2}) - \tfrac{u}{2}\sqrt{t^2 - 4} = 0\right\} \cup \left\{(s' - \tfrac{ut}{2}) + \tfrac{u}{2}\sqrt{t^2 - 4} = 0\right\}$$

which have a point $(s' = 0, u = 0)$ defined over any field provided $t^2 - 4 \neq 0$.

If $t^2 - 4 = 0$, then the equation

$$p(s', u, t) - s = (s' - \tfrac{ut}{2})^2 + 2 - s = 0$$

has a solution if and only if $s - 2$ is a perfect square. □

Definition 3.5. Let us define the following sets:

$$\begin{aligned} E_{n+1} &= \theta \circ \varphi_n(\widetilde{G} \times \widetilde{G}) \\ &= \{z \in \widetilde{G} \mid \text{ there exists } (x,y) \in \widetilde{G} \times \widetilde{G} \text{ such that } e_{n+1}(x,y) = z\}; \\ Y_q &= \lambda_2(\Psi_q); \\ Y'_q &= \lambda_2(\Psi_q) \setminus \{(s,t) \mid t = 0\}; \\ T_n(\mathbb{F}_q) &= \rho_n(Y_q); \\ T'_n(\mathbb{F}_q) &= \rho_n(Y'_q). \end{aligned}$$

Proposition 3.6. (A) *If $q > 2$ is even and $a \in \mathbb{F}_q$, then the following two statements are equivalent:*

(i) $a \in T_n(\mathbb{F}_q) = \rho_n(\lambda_2(A(\mathbb{F}_q)))$;

(ii) *any element $z \in \widetilde{G}$ with* $\mathrm{tr}(z) = a$ *belongs to E_{n+1}.*

(B) *If $q > 3$ is odd and $a \in \mathbb{F}_q$, $a \neq -2$, then the following two statements are equivalent:*

(i) $a \in T_n(\mathbb{F}_q) = \rho_n(\lambda_2(\Psi_q))$;

(ii) *any element $z \in \widetilde{G}$ with* $\mathrm{tr}(z) = a$ *belongs to E_{n+1}.*

(C) *If $q > 3$ is odd and $-2 \in T'_n(\mathbb{F}_q)$ then every element $z \in \widetilde{G}$, $z \neq -\mathrm{id}$, with* $\mathrm{tr}(z) = -2$ *belongs to E_{n+1}.*

Proof. If $z = e_{n+1}(x,y)$, then $a = \mathrm{tr}(z) = \rho_n \circ \lambda_2(\psi(\mathrm{tr}(x), \mathrm{tr}(xy), \mathrm{tr}(y)))$. Thus we need to prove the implications (i) $\Longrightarrow$ (ii).

Assume that $a = \rho_n(s,t)$ for some $(s,t) \in Y_q = \lambda_2(\Psi_q)$. Since ψ is surjective onto Ψ_q, there exists a point $(s',u,t) \in \mathbb{A}^3(\mathbb{F}_q)$ such that $(s,t,t) = \psi(s',u,t)$. Since the morphism π is surjective for any field, one can find $(x',y') \in \widetilde{G} \times \widetilde{G}$ such that $\pi(x',y') = (s',u,t)$. Let $v = e_{n+1}(x',y')$, then $\mathrm{tr}(v) = a$ (see diagram (3.5)).

Case 1. *Either q is even and $a \neq 0$, or q is odd and $a \neq \pm 2$.*

In this case, $a = \mathrm{tr}(z) = \mathrm{tr}(v)$ implies that v is conjugate to z, i.e. $z = gvg^{-1}$ for some $g \in \widetilde{G}$. Therefore $e_{n+1}(gx'g^{-1}, gy'g^{-1}) = gvg^{-1} = z$, and so one can take $x = gx'g^{-1}, y = gy'g^{-1}$.

Case 2. *Either q is even and $a = 0$, or q is odd and $a = 2$.*

Observe that 2 always belongs to $T_n(\mathbb{F}_q)$ since $2 - 2 = 0$ is a perfect square and $(2,t)$ is a fixed point of μ_n.

It suffices to prove that all matrices $w = \left(\begin{smallmatrix} 1 & c \\ 0 & 1 \end{smallmatrix}\right)$, $c \in \mathbb{F}_q$, are in the image E_n. Since

$$e_n\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} d & 0 \\ 0 & \frac{1}{d} \end{pmatrix}\right) = \begin{pmatrix} 1 & b(1-d^2)^n \\ 0 & 1 \end{pmatrix},$$

one can take some $0 \neq d \in \mathbb{F}_q$ with $d^2 \neq 1$ and $b = \frac{c}{(1-d^2)^n}$.

Case 3. *q is odd and $a = -2$.*

If $-2 \in T_n'(\mathbb{F}_q)$ then $v \neq -\mathrm{id}$ by Remark 3.1. Choose $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $\alpha^2 \in \mathbb{F}_q$. Let

$$m = \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix}.$$

Then $mvm^{-1} \in \widetilde{G}$ and, moreover, either v or mvm^{-1} is conjugate to z in $\widetilde{G}$.

If v is conjugate to z, then we proceed as in case 1.

If mvm^{-1} is conjugate to z, then we consider the pair $(x'' = mx'm^{-1}, y'' = my'm^{-1}) \in \widetilde{G} \times \widetilde{G}$. We have $mvm^{-1} = e_{n+1}(x'', y'')$, and we may continue as in case 1. □

Corollary 3.7. *If $a \in \mathbb{F}_q$, $a \neq -2$, belongs to the image $\rho_n(\mathbb{A}^2_{s,t})(\mathbb{F}_q)$, then any element $z \in \widetilde{G}$ with $\mathrm{tr}(z) = a$ belongs to E_n.*

Proof. Indeed, $\rho_n(\mathbb{A}^2_{s,t}) \subseteq \rho_{n-1}(\lambda_2(\Psi_q))$ because $\psi(s,t,t) = (\rho(s,t), t, t)$. □

Definition 3.8. When q is odd, the point $(s,t) \in \mathbb{A}^2_{s,t}$ is called an *exceptional* point if either $t = 0$ or $t^2 = 4$. The set of all exceptional points is denoted by Υ.

Corollary 3.9. *If either q is even and $a \in \rho_n(\mathbb{A}^2_{s,t})$, or q is odd and $a \in \rho_n(\mathbb{A}^2_{s,t} \setminus \Upsilon)$, then any element $z \in \widetilde{G} = \widetilde{G}(\mathbb{F}_q)$ with $\mathrm{tr}(z) = a$ belongs to E_{n+1}, i.e., there exists $(x, y) \in \widetilde{G} \times \widetilde{G}$ such that $z = e_{n+1}(x, y)$.*

Corollary 3.10. *If q is odd and $T_n(\mathbb{F}_q)$ contains either a or $-a$ for every $a \in \mathbb{F}_q$, then the Engel word map e_{n+1} is surjective on* PSL$(2, q)$.

Proof. This follows from Proposition 3.6 (B) and the fact that both elements $z \in$ SL$(2, q)$ and $-z \in$ SL$(2, q)$ represent the same element of PSL$(2, q)$. □

4. Surjectivity and non-surjectivity of Engel words over special fields

The following examples show that the n-th Engel word map (for $n \geq 3$) is not always almost surjective on SL$(2, q)$ (in the light of Proposition 3.6). However, it is still conjectured that it is surjective on PSL$(2, q)$ (see Conjecture 1.3).

Example 4.1. In the following cases, computer experiments using Magma show that there is no solution to $\rho_n = a$ in $\mathbb{F}_q$.

- There is no solution in $\mathbb{F}_{11}$ to $\rho_n = 9$ for every $n \geq 2$.
- There is no solution in $\mathbb{F}_{13}$ to $\rho_n = 4$ for every $n \geq 5$.
- There is no solution in $\mathbb{F}_{17}$ to $\rho_n = 10$ for every $n \geq 2$, to $\rho_n = 4$ for every $n \geq 4$, and to $\rho_n = 5$ for every $n \geq 5$.

- There is no solution in $\mathbb{F}_{23}$ to $\rho_n = 16$ for every $n \geq 2$.
- There is no solution in $\mathbb{F}_{53}$ to $\rho_n = 31$ for every $n \geq 8$.
- There is no solution in $\mathbb{F}_{67}$ to $\rho_n = 4$ for every $n \geq 10$.

Remark 4.2. In fact, it is sufficient to check any of the above examples for all integers $n \leq q$, since for every $(s,t) \in \mathbb{F}_q^2$ there exists some $N \leq q$ such that $\mu_N(s,t)$ is a periodic point of μ.

Following some further extensive computer experiments using MAGMA, in which we checked all $q < 600$ and $n < 50$, we moreover suggest these conjectures (see also Proposition 4.10 below).

Conjecture 4.3. *For every finite field $\mathbb{F}_q$, $a \in \mathbb{F}_q$ and $n \in \mathbb{N}$, unless either $a = 1$ and $\sqrt{2} \notin \mathbb{F}_q$, or the triple (q,a,n) appears in one of the cases in Example 4.1, one has that ρ_n attains the value a.*

Conjecture 4.4. *For every finite field $\mathbb{F}_q$, $a \in \mathbb{F}_q$ and $n \in \mathbb{N}$, either a or $-a$ is in the image of ρ_n.*

Observe that if the first conjecture is true then so is the second.

We continue by considering some special infinite families of finite fields. We will mainly use the following properties of the maps μ_n and ρ_n.

Properties 4.5. (1) $\mu(1,t) = (t^2-1,t)$;
(2) $\mu(t^2-1,t) = (t^2-1,t)$;
(3) $\mu(2,t) = (2,t)$;
(4) $\mu(t^2-2,t) = (2,t)$;
(5) $\rho_n(s,0) = x^{2^n} + \frac{1}{x^{2^n}}$ if $s = x + \frac{1}{x}$;
(6) $\rho_n(s,t) = (s-1)^{2^n} + 1$ if $t^2 = 2$;
(7) $\rho_n(s,t) = (s-2)^{2^n} + 2$ if $t^2 = 4$.

Corollary 4.6. *Let $t \in \mathbb{F}_q$. Then $t^2 - 1$ is in $T_n(\mathbb{F}_q)$ for every n.*

Proof. Item (2) implies that the point (t^2-1,t) is a fixed point of μ. Moreover, if $t^2 = 4$, then $(t^2-1)-2 = 1$ is always a square, and hence $t^2 - 1 \in \Psi_q$ for every q. □

We shall now explain why $-\mathrm{id}$ cannot appear in the image of long enough Engel words, motivating Definition 1.4 of "almost surjectivity".

Proposition 4.7. *If $n \geq 1$ and $q \geq 7$ is an odd prime power, then there is a solution $(x,y) \in \widetilde{G}^2$ to the equation $e_{n+1}(x,y) = -\mathrm{id}$ if and only if there exists some $c \in \mathbb{F}_{q^2}$ satisfying $c^{2^n} = -1$.*

Proof. Assume that $e_{n+1}(x, y) = -\mathrm{id}$. Then, by Remark 3.1, there exists some $b \in \mathbb{F}_q$ such that $\rho_n(b, 0) = -2$. According to Properties 4.5 (5),

$$\rho_n(b, 0) = c^{2^n} + \frac{1}{c^{2^n}},$$

where $c \in \mathbb{F}_{q^2}$ is defined by the equation $b = c + \frac{1}{c}$. Thus,

$$c^{2^n} + \frac{1}{c^{2^n}} = -2,$$

implying that

$$\left(c^{2^{n-1}} + \frac{1}{c^{2^{n-1}}}\right)^2 = 0,$$

and so

$$c^{2^n} = -1.$$

On the other direction, assume that there exists some $c \in \mathbb{F}_{q^2}$ satisfying $c^{2^n} = -1$, let $b = c + \frac{1}{c}$, and denote

$$A = \begin{pmatrix} c & 0 \\ 0 & \frac{1}{c} \end{pmatrix}.$$

Consider the rational curve C defined by $s^2 + u^2 = b + 2$. Note that $b + 2 \neq 0$ since $c \neq -1$. Thus, being a smooth rational curve, $C(\mathbb{F}_q)$ has at least $q - 1$ points. If $q \geq 7$, there are points (s, u) in $C(\mathbb{F}_q)$ such that $s \neq \pm 2$. Let (s, u) be such a point, and let $x_0, y_0 \in \mathrm{SL}(2, q)$ be any pair of matrices such that $\mathrm{tr}(x_0) = s$, $\mathrm{tr}(x_0 y_0) = u$, $\mathrm{tr}(y_0) = 0$.

We shall show that $e_{n+1}(x_0, y_0) = -\mathrm{id}$. Consider x_0 and y_0 as elements of $\widetilde{G}_1 = \mathrm{SL}(2, F_1)$, where F_1 is a quadratic extension of $\mathbb{F}_q$ such that $c \in F_1$. Let $\pi_1 \colon \widetilde{G}_1^2 \to \mathbb{A}^3(F_1)$ be the trace projection:

$$\pi_1(x, y) = (\mathrm{tr}(x), \mathrm{tr}(xy), \mathrm{tr}(y)).$$

Then any pair (x_1, y_1) satisfying $\pi_1(x_1, y_1) = (s, u, 0)$ is conjugate to the pair (x_0, y_0) in $\widetilde{G}_1$, that is, there exists $g \in \widetilde{G}_1$ such that $x_1 = g x_0 g^{-1}$, $y_1 = g y_0 g^{-1}$.

Hence, $e_{n+1}(x_0, y_0)$ is conjugate in $\widetilde{G}_1$ to $e_{n+1}(x_1, y_1)$.

Take

$$x_1 = \begin{pmatrix} \frac{sc}{c+1} & \frac{uc}{c+1} \\ \frac{-u}{c+1} & \frac{s}{c+1} \end{pmatrix}, \quad y_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

A direct computation shows that

$$[x_1, y_1] = \begin{pmatrix} \frac{(u^2+s^2)c^2}{(c+1)^2} & 0 \\ 0 & \frac{(u^2+s^2)}{(c+1)^2} \end{pmatrix} = A.$$

Let us now compute $e_n(A, y_1)$. Let

$$X(a) = \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix}.$$

Then

$$[X(a), y_1] = \begin{pmatrix} a^2 & 0 \\ 0 & \frac{1}{a^2} \end{pmatrix},$$

and so

$$e_n(X(a), y_1) = \begin{pmatrix} a^{2^n} & 0 \\ 0 & \frac{1}{a^{2^n}} \end{pmatrix}.$$

Since $A = X(c)$, then $e_n(A, y_1) = -\mathrm{id}$. In addition, $A = e_1(x_1, y_1)$, and hence $e_{n+1}(x_1, y_1) = -\mathrm{id}$. But then $e_{n+1}(x_0, y_0)$ is conjugate to $-\mathrm{id}$, and therefore $e_{n+1}(x_0, y_0) = -\mathrm{id}$ as well. □

Proposition 4.8. *For every odd prime power q there is a number $n_0 = n_0(q)$ such that $e_n(x, y) \neq -\mathrm{id}$ for every $n > n_0$ and every $x, y \in \widetilde{G} = \mathrm{SL}(2, q)$.*

Remark 4.9. If $n > q$ then the equation $c^{2^n} = -1$ has no solution in $\mathbb{F}_{q^2}$, and hence $e_n(x, y) \neq -\mathrm{id}$ for every $x, y \in \mathrm{SL}(2, q)$.

However, $-\mathrm{id}$ can be written as a commutator of two matrices in $\mathrm{SL}(2, q)$, where q is odd. Indeed, take $a, b \in \mathbb{F}_q$ satisfying $a^2 + b^2 = -1$. Then

$$\left[\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} a & b \\ b & -a \end{pmatrix}\right] = -\mathrm{id}.$$

(See [Th] and [Bl] for a general result regarding central elements in $\mathrm{SL}(n, q)$ and other quasisimple groups.)

We moreover show that there exists an infinite family of finite fields $\mathbb{F}_q$, for which the n-th Engel word map in $\mathrm{SL}(2, q)$ is not even almost surjective for sufficiently large $n \geq n_0(q)$.

Proposition 4.10. *Let $\mathbb{F}_q$ be a finite field which does not contain $\sqrt{2}$. Then there exists some integer $n_0 = n_0(q)$ such that $\rho_n \neq 1$ for every $n > n_0$.*

Proof. Since the set of points $(s, t) \in \mathbb{A}^2(\mathbb{F}_q)$ is finite, every point is either periodic or preperiodic for μ_n. This means that for every $(s, t) \in \mathbb{A}^3(\mathbb{F}_q)$ there are numbers $\tilde{n}(s, t)$ and $m(s, t) < \tilde{n}(s, t)$ such that

$$\mu_{\tilde{n}(s,t)}(s, t) = \mu_{m(s,t)}(s, t).$$

For a point (s, t) we define $n(s, t)$ as the minimum of all possible $\tilde{n}(s, t)$.

Let

$$n_0 = \max\{n(s,t) \mid (s,t) \in \mathbb{A}^2(\mathbb{F}_q)\}.$$

Then every $(s,t) \in R_{n_0} = \mu_{n_0}(\mathbb{A}^2(\mathbb{F}_q))$ is periodic and $R_n = R_{n_0}$ for any $n \geq n_0$. In order to show that $\rho_n \neq 1$ it is sufficient to show that $(1,t) \notin R_{n_0}$ for any t, i.e., to show that $(1,t)$ is not periodic. Indeed, $\mu(1,t) = (t^2-1,t)$, which is a fixed point for any t. Thus, for every $k > 0$ we have $\mu_k(1,t) = (t^2-1,t) \neq (1,t)$ if $t^2 \neq 2$. □

On the other hand, we show that there are certain infinite families of finite fields $\mathbb{F}_q$ for which the n-th Engel word map in $\mathrm{PSL}(2,q)$ is always surjective for every $n \in \mathbb{N}$. The first family consists of all finite fields of characteristic 2, and the second family contains infinitely many finite fields of odd characteristic.

Proposition 4.11. *For every $n \geq 1$, the Engel word map e_n is surjective on the group* $\mathrm{PSL}(2,q)$ *for $q = 2^e$, $e > 1$.*

Proof. In this case

$$\mu(s,t) = (s^2 - st^2, t), \quad \rho(s,0) = s^2.$$

Thus $\rho(s,0)$ is an isomorphism of $\mathbb{A}^1_s(\mathbb{F}_q)$, as well as any of its iterations $\rho_n(s,0)$. According to Proposition 3.6, this implies the surjectivity of the n-th Engel word map on $\mathrm{PSL}(2,q) = \mathrm{SL}(2,q)$. □

Proposition 4.12. *For every $n \geq 1$, the Engel word map e_{n+1} is surjective on the group* $\mathrm{PSL}(2,q)$ *if $\sqrt{2} \in \mathbb{F}_q$ and $\sqrt{-1} \notin \mathbb{F}_q$.*

Proof. By Corollary 3.10, we need to show that either $a \in T_n(\mathbb{F}_q)$ or $-a \in T_n(\mathbb{F}_q)$ for every $a \in \mathbb{F}_q$.

In this case, the map $x \to x^2$ is a bijection on the subset of perfect squares of $\mathbb{F}_q$. It follows that if $a = b^2$ for some $b \in \mathbb{F}_q$, then for every n, there is some $b_n \in \mathbb{F}_q$ such that $a = b_n^{2^n}$. Moreover, for every $a \in \mathbb{F}_q$ either $a = b^2$ for some $b \in \mathbb{F}_q$ or $a = -b^2$ for some $b \in \mathbb{F}_q$.

Assume that $z \in \mathrm{PSL}(2,q)$ and $z \neq e_{n+1}(x,y)$. Let $\mathrm{tr}(z) = a$. Then, by Corollary 4.6, neither $a+1$ nor $-a+1$ is a square in $\mathbb{F}_q$. It follows that $a+1 = -c^2$ and $-a+1 = -b^2$ for some $b,c \in \mathbb{F}_q$. Hence, $a = b^2+1 = b_n^{2^n}+1 = \rho_n(b_n+1,\sqrt{2})$ according to Properties 4.5 (6), yielding $a \in T_n(\mathbb{F}_q)$. □

5. Engel words in $\mathrm{SL}(2,q)$ for sufficiently large q

In this section we prove Theorem A and show that the n-th Engel word map e_n is almost surjective on $\mathrm{SL}(2,q)$ if $q \geq q_0(n)$ is sufficiently large. We moreover give an explicit estimate for $q_0(n)$, which, unfortunately, is exponential in n.

Our proof has a geometrical flavor. Let us briefly describe it and explain the geometric idea behind our calculations. Consider the diagram (3.5). Instead of solving the equation $\operatorname{tr}(e_{n+1}(x,y)) = a$, we look for points defined over a ground field $\mathbb{F}_q$ in the curve $\{\mu_n(s,t) = a\}$. This is an affine curve. In order to use the Weil inequality, we have to know that it has an absolutely irreducible component defined over the ground field $\mathbb{F}_q$, and we need to estimate its genus and the number of punctures.

To this end we represent the curve as a tower of double covers of a rational curve (see eq. (5.2)). The geometrical interpretation of this procedure is an embedding of the curve into an affine space of a higher dimension $\mathbb{A}^{n+2}_{z_1,\dots,z_n,\varkappa,t}$. Then we consider the closure X of this curve in the corresponding projective space $\mathbb{P}^{n+2}_{x_1:\dots:x_n:y:d:w}$.

It appears (see Lemma 5.2) that the intersection of X with the hyperplane at infinity consists of smooth points defined over $\mathbb{F}_q$ for any q. Thus every irreducible component of X is defined over $\mathbb{F}_q$ as well. Indeed, assume that an irreducible component (say, X_i) is defined over an extension of $\mathbb{F}_q$ and is not invariant under the action of the corresponding Galois group Γ, then the Γ-invariant points would belong to the intersection $X_i \cap \gamma(X_i)$, $\gamma \in \Gamma$, and therefore, the points defined over $\mathbb{F}_q$ would not be smooth.

The rest of the proof deals with the estimation of the genus and the number of punctures.

By Proposition 4.11 we may assume that q is odd. We continue to use the notation introduced in Definition 3.2.

Theorem 5.1. *For every $n \in \mathbb{N}$ there exists $q_0 = q_0(n)$ such that $\rho_n\colon \mathbb{A}^2_{s,t} \setminus \Upsilon \to \mathbb{A}^1_s$ is surjective for every field $\mathbb{F}_q$ with $q \geq q_0$. Moreover, if n is a prime, then there is an orbit of μ of length precisely n.*

Proof. Together with the endomorphism $\mu\colon \mathbb{A}^2_{s,t} \to \mathbb{A}^2_{s,t}$ we may define the following endomorphism $m\colon \mathbb{A}^2_{z,\varkappa} \to \mathbb{A}^2_{z,\varkappa}$ by

$$m(z,\varkappa) = (z(z-\varkappa), \varkappa). \tag{5.1}$$

A direct computation shows that μ may be reduced to (5.1) by the substitution $z = s-2$, $\varkappa = t^2 - 4$.

Similarly to the morphisms $\lambda_1(s,t) = s$ and $\rho_n = \lambda_1 \circ \mu^{(n)}$, we may define the morphisms $l\colon \mathbb{A}^2_{z,\varkappa} \to \mathbb{A}^1_z$, $l(z,\varkappa) = z$, and $r_n = l \circ m^{(n)}$.

First, we note that $s = 2$ is always in the image of ρ_n (see Proposition 3.6). Note also that $(s,t) = (-2,0)$ cannot be a periodic point since $\mu(-2,0) = (2,0)$, which is a fixed point.

Now assume that some $a+2 \in \mathbb{F}_q, a \neq 0$ is in the image of ρ_n. This is equivalent to $a = r_n(z,\varkappa)$ for some $z \in \mathbb{F}_q$ and $\varkappa = t^2-4$, $t \in \mathbb{F}_q$. The last statement implies that the following system of equations has a solution in $\mathbb{F}_q$:

$$\begin{cases} z_2 = z_1(z_1 - \varkappa), \\ \quad \vdots \\ z_n = z_{n-1}(z_{n-1} - \varkappa), \\ a = z_n(z_n - \varkappa), \\ \varkappa = t^2 - 4. \end{cases} \tag{5.2}$$

Similarly, the orbit of length n is defined by the following system:

$$\begin{cases} z_2 = z_1(z_1 - \varkappa), \\ \quad \vdots \\ z_n = z_{n-1}(z_{n-1} - \varkappa), \\ z_1 = z_n(z_n - \varkappa), \\ \varkappa = t^2 - 4. \end{cases} \tag{5.3}$$

If n is a prime, then system (5.3) describes all the points in an orbit either of exact length n or of exact length 1. In the latter case, these points are $z_i = \varkappa + 1$, $i = 1, \dots, n$, and $z_i = 0$, $i = 1, \dots, n$.

Consider the projective space $\mathbb{P}^{n+2}(\overline{\mathbb{F}}_q)$ with homogeneous coordinates $\{x_1 : \dots : x_n : y : d : w\}$. Assume that $z_i = \frac{x_i}{w}$, $i = 1 \dots, n$, $\varkappa = \frac{y}{w}$, $t = \frac{d}{w}$. Then system (5.2) defines in $\mathbb{P}^{n+2}$ a projective set

$$X = \begin{cases} x_2 w = x_1(x_1 - y), \\ \quad \vdots \\ x_n w = x_{n-1}(x_{n-1} - y), \\ a w^2 = x_n(x_n - y), \\ y w = d^2 - 4w^2. \end{cases} \tag{5.4}$$

Similarly, system (5.3) defines a projective set

$$X_1 = \begin{cases} x_2 w = x_1(x_1 - y), \\ \quad \vdots \\ x_n w = x_{n-1}(x_{n-1} - y), \\ x_1 w = x_n(x_n - y), \\ y w = d^2 - 4w^2. \end{cases} \tag{5.5}$$

Lemma 5.2. *The intersections $S = X \cap \{w = 0\}$ and $S_1 = X_1 \cap \{w = 0\}$ consist of 2^n smooth points with $w = 0, d = 0, y = 1$ and $x_i = 0$ or 1 (for $i = 1, \dots, n$).*

Proof. If there was a point in X with $w = 0$, $y = 0$, then, according to (5.4) (respectively (5.5)), d and all x_i would vanish as well, which is impossible. Thus, $y \neq 0$ at the points of S and S_1. But then (5.4) (respectively (5.5)) implies that every x_i is either 0 or y at the points of S (respectively S_1).

It follows, in particular, that the sets X and X_1 have no components of dimension greater than 1 since the intersection of each such component with $\{w = 0\}$ would be positive dimensional.

Let us compute the Jacobian matrices of these systems. We have for (5.4)

$$\begin{bmatrix} \partial_d & \partial_w & \partial_y & \partial_{x_1} & \partial_{x_2} & \dots & \partial_{x_{n-1}} & \partial_{x_n} \\ \\ 0 & -x_2 & -x_1 & 2x_1 - y & -w & \dots & 0 & 0 \\ 0 & -x_3 & -x_2 & 0 & 2x_2 - y & -w & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & -x_n & -x_{n-1} & 0 & 0 & \dots & 2x_n - y & -w \\ 0 & -2aw & -x_n & 0 & 0 & \dots & 0 & 2x_n - y \\ 2d & -8w - y & -w & 0 & 0 & \dots & 0 & 0 \end{bmatrix}$$

and similarly for (5.5)

$$\begin{bmatrix} \partial_d & \partial_w & \partial_y & \partial_{x_1} & \partial_{x_2} & \dots & \partial_{x_{n-1}} & \partial_{x_n} \\ \\ 0 & -x_2 & -x_1 & 2x_1 - y & -w & \dots & 0 & 0 \\ 0 & -x_3 & -x_2 & 0 & 2x_2 - y & -w & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & -x_n & -x_{n-1} & 0 & 0 & \dots & 2x_n - y & -w \\ 0 & -x_1 & -x_n & -w & 0 & \dots & 0 & 2x_n - y \\ 2d & -8w - y & -w & 0 & 0 & \dots & 0 & 0 \end{bmatrix}.$$

Since at the points of S and S_1 the ranks of these matrices are $n + 1$, every point is smooth. □

Remark 5.3. In particular, we have proved that the map ρ_n is surjective over every algebraically closed field. Indeed, every component of X has dimension at least one, thus no fiber is contained in the set $\{w = 0\}$.

Consider an irreducible component A_i (over $\overline{\mathbb{F}}_q$) of X of degree d_i. If it was not defined over $\mathbb{F}_q$, then every point in A_i, which is rational over $\mathbb{F}_q$, would be singular. But, according to Lemma 5.2, A_i has smooth points defined over $\mathbb{F}_q$ (namely, $A_i \cap S$). Thus, A_i is defined over $\mathbb{F}_q$. Similarly, every irreducible component B_i of X_1 is defined over $\mathbb{F}_q$.

Let $\omega\colon \mathbb{P}^{n+2} \to \mathbb{P}^2_{x_1,d,w}$ be defined as $\omega(x_1 : \dots : x_n : y : d : w) = (x_1 : d : w)$. Then ω induces a birational map of every A_i (respectively B_i) on its image

$R_i = \omega(A_i)$ (respectively $U_i = \omega(B_i)$) because of (5.4) (respectively (5.5)). Thus, A_i is birational to the closure R_i in $\mathbb{P}^2$ of an irreducible component of the set

$$\tilde{Y}^{(n)} = \{r_n(z_1, t^2 - 4) = a\} \subset \mathbb{A}^2_{z_1,t},$$

which becomes

$$Y^{(n)} = \{\rho_n(s,t) = a + 2\} \subset \mathbb{A}^2_{s,t}$$

after the following change of coordinates $(z_1, t) \to (s = 2 + z_1, t)$ (respectively, $(x_1, d, w) \to (x_1 + 2w, d, w)$). Similarly, B_i is birational to the closure U_i in $\mathbb{P}^2$ of an irreducible component of the set

$$Z^{(n)} = \{\rho_n(s,t) = s\} \subset \mathbb{A}^2_{s,t}.$$

The plane curves R_i and U_i are defined over the ground field as the projections of A_i and B_i respectively. Let $d_n \le 3^{2^n}$ and $j_n \le 3^{2^n}$ be the degrees of R_i and U_i respectively.

For the number $N(q)$ of points over the field $\mathbb{F}_q$ in an irreducible curve C of degree d in $\mathbb{P}^2$ we use the following analogue of the Weil inequality (see [AP], [GL], Corollary 7.4, and [LY], Corollary 2):

$$|C(\mathbb{F}_q) - (q+1)| \le (d-1)(d-2)\sqrt{q}.$$

Hence, we obtain

$$|R_i(\mathbb{F}_q)| \ge q + 1 - d_n^2\sqrt{q},$$

and

$$|U_i(\mathbb{F}_q)| \ge q + 1 - j_n^2\sqrt{q}.$$

Now we need to check how many of these points can be exceptional or at infinity. All these points are the intersection points with 4 lines: $d = 0$, $d = \pm 2w$, $w = 0$. By the Bézout's Theorem there are at most $4d_n$ (respectively, $4j_n$) such points.

For any $q \ge 2d_n^4$ we have

$$q + 1 - d_n^2\sqrt{q} \ge 2d_n^4 + 1 - d_n^4\sqrt{2} = d_n^4(2 - \sqrt{2}) + 1 > 4d_n.$$

Similarly, for $q \ge 2j_n^4$,

$$q + 1 - j_n^2\sqrt{q} \ge 2j_n^4 + 1 - j_n^4\sqrt{2} = j_n^4(2 - \sqrt{2}) + 1 > 4j_n.$$

Thus, if $q \ge \max\{2d_n^4, 2j_n^4\}$, then $(R_i \setminus \Upsilon)(\mathbb{F}_q) \ne \emptyset$ and $(U_i \setminus \Upsilon)(\mathbb{F}_q) \ne \emptyset$, which completes the proof of Theorem 5.1. □

Corollary 5.4. *The map* $e_n \colon \tilde{G} \times \tilde{G} \to \tilde{G}$ *is almost surjective if* $\tilde{G} = \mathrm{SL}(2, q)$ *and* $q \ge q_0(n)$ *is big enough.*

Proof. According to Corollary 3.9, the almost surjectivity of e_{n+1} on $\mathrm{SL}(2,q)$ follows from the surjectivity of ρ_n onto $\mathbb{A}^2_{s,t} \setminus \Upsilon$, which was proven in Theorem 5.1 for any $q \geq q_0(n)$. □

In order to make the estimation for $q_0(n)$ more precise a detailed study of system (5.4) is needed.

Proposition 5.5. *The curve X defined in (5.4) is irreducible provided $a \neq 0$. Let $\tilde{\nu}\colon \widetilde{X} \to X$ be the normalization of X. Then the genus $g(\widetilde{X}) \leq 2^n(n-1)+1$ and $\tilde{\nu}^{-1}(S)$ contains at most 2^n points.*

Proof. We will work over an algebraic closure of a ground field. For $k = 1,\dots,n$, we denote by C_k a curve defined in $\mathbb{P}^{n-k+2}$ by

$$C_k = \begin{cases} x_{k+1}w = x_k(x_k - y), \\ \quad\vdots \\ x_n w = x_{n-1}(x_{n-1} - y), \\ aw^2 = x_n(x_n - y). \end{cases} \tag{5.6}$$

Lemma 5.6. *If $a \neq 0$ and q is odd, then the system (5.6) for $k = 1$ defines in $\mathbb{P}^{n+1}$ a smooth irreducible projective curve C_1 of genus $g(C_1) \leq 2^{n-1}(n-2)+1$.*

Proof. Let g_k denote the genus $g(C_k)$ (if C_k is irreducible).

We shall prove by induction on $r = n-k$ that all curves C_k are irreducible and moreover

$$g_k \leq 2^{n-k}(n-k-1)+1.$$

Step 1. It is obvious that C_n $(r = 0)$ is an irreducible conic in $\mathbb{P}^2$ and that $g_n = 0$. At a point $(\alpha : \beta : 1) \in C_n$ we may use the affine coordinates $z_i = \frac{x_i}{w}, \varkappa = \frac{y}{w}$. A local parameter on C_n at this point may be taken as $z_n - \alpha$ since

$$\varkappa - \beta = (z_n - \alpha)\left(1 + \frac{\alpha - \beta}{z_n}\right)$$

(see, for example, [DS], I, Chapter 2, §1.6, for a definition of a local parameter).

The induction step. Assume that for $r = n-k$ the assertion is valid, namely:

- the curve C_k is smooth and irreducible;
- $z_k - \alpha_k$ is a local parameter at every point $(\alpha_k : \dots : \alpha_n : \beta : 1) \in C_k$ $(w \neq 0)$;
- $g_k \leq 2^{n-k}(n-k-1)+1$.

The curve C_{k-1} is a double cover of C_k since to the equations defining C_k one equation for the new variable x_{k-1} is added:

$$x_k w = x_{k-1}(x_{k-1} - y).$$

Thus,

$$x_{k-1} = \frac{y}{2} \pm \sqrt{\frac{y^2}{4} + wx_k}.$$

It follows that the double points are

$$x_{k-1} = \frac{y}{2}, \quad x_k = -\frac{y^2}{4w}.$$

Note that $w \neq 0$ at a ramification point. Indeed, if $w = 0$ and $\sqrt{\frac{y^2}{4} + wx_k} = 0$ then $y = 0$, which is impossible in the light of Lemma 5.2. Thus we may take $w = 1$.

Hence in affine coordinates, at the double point $(\frac{\beta}{2} : -\frac{\beta^2}{4} : \cdots : \alpha_n : \beta : 1) \in C_{k-1}$, we have

- $\frac{\beta^2}{4} + z_k$ is a local parameter on C_k by the induction hypothesis;
- $(z_{k-1} - \frac{\beta}{2})^2 = \frac{\beta^2}{4} + z_k$.

It follows that

- this point is a ramification point indeed;
- $z_{k-1} - \frac{\beta}{2}$ is a local parameter on C_{k-1} at this point;
- C_{k-1} is smooth at this point.

Outside the ramification points, the projection $C_{k-1} \to C_k$ is *étale*. At infinity all the points are smooth, see Lemma 5.2. Therefore, since C_k is smooth and irreducible by the induction assumption, then C_{k-1} is smooth and irreducible as well.

Let us compute the number of ramification points. We have

$$\begin{gathered} x_{k-1} = \frac{y}{2}, \quad x_k = -\frac{y^2}{4}, \quad x_{k+1} = -\frac{y^2}{4}\Big(-\frac{y^2}{4} - y\Big), \ \ldots, \\ x_{k+s} = p_s(y), \ \ldots, x_n = p_{n-k}(y), \quad a = p_{n-k+1}(y), \end{gathered} \tag{5.7}$$

where $p_s(y)$ is a polynomial in y and $\deg p_s(y) = 2^{s+1}$. Hence the last equation has $l \leq 2^{n-k+2}$ distinct roots.

By the Hurwitz formula (see e.g. [DS], I, Chapter 2, §2.9) and the induction estimate for g_k we obtain

$$\begin{aligned} g_{k-1} &= 2g_k - 1 + \tfrac{l}{2} \\ &\leq 2(2^{n-k}(n-k-1) + 1) - 1 + 2^{n-k+1} \\ &= 2^{n-(k-1)}(n-k) - 2 \cdot 2^{n-k} + 2^{n-k+1} + 2 - 1 \\ &= 2^{n-(k-1)}(n-k) + 1. \end{aligned}$$

This completes the induction. Thus, $g_1 \leq 2^{n-1}(n-2) + 1$. □

Now the curve X is obtained from C_1 by adding one more equation

$$wy = d^2 - 4w^2$$

(this is the last equation of system (5.4)). It follows that X is a double cover of C_1 with double points at $w = 0$ or $y = -4w$. At every such point $y \neq 0$. Moreover, X is smooth at every point of S (see Lemma 5.2), hence every point of S is a ramification point. Thus, X is irreducible. Moreover, $\tilde{\nu}$ is one-to-one at these points.

Any other double point is either a ramification point or a double self-intersection. Since $d^2 = wy + 4w^2$, these are points with $y = -4w$. Similarly to (5.7), there can be at most 2^n such points at X.

From the Hurwitz formula we obtain

$$g(\widetilde{X}) \leq 2g(C_1) - 1 + 2^n = 2(1 + 2^{n-1}(n-2)) - 1 + 2^n = 2^n(n-1) + 1.$$

This completes the proof of Proposition 5.5. □

Remark 5.7. The more detailed analysis of the curve X shows that it is not smooth only if $a = -4$. If $a \neq -4$ the normalization is not needed.

Corollary 5.8. *For any $n > 2$, the map $e_{n+1}\colon \widetilde{G} \times \widetilde{G} \to \widetilde{G}$ is almost surjective if $\widetilde{G} = \mathrm{SL}(2, q)$ and $q > 2^{2n+3}(n-1)^2$.*

Proof. We want to prove that any number $a \in \mathbb{F}_q$ is attained by r_n. Since the normalization $\widetilde{X}$ of X is defined over the ground field (see [Sa], Chapter 1, §6.4 and §7), every point $\tilde{x} \in \widetilde{X}(\mathbb{F}_q)$ provides a point $\tilde{\nu}(\tilde{x}) \in X(\mathbb{F}_q)$. In order to exclude the exceptional points, we should take away from X the following points:

- 2^n points of S;
- 2^{n+1} points with $y = 0$, $d = \pm 2w$;
- 2^n points with $y = -4w$, $d = 0$.

Since (for $a = -2$) the points with $y = -4w, d = 0$ may be self-intersections, we should count them twice. Thus we need that $|\widetilde{X}(\mathbb{F}_q)| > 5 \cdot 2^n$.

We shall use the Weil inequality (see [AP]) once more. For a field $\mathbb{F}_q$ we need that

$$q + 1 - 2g\sqrt{q} - \delta > 0,$$

where, by Proposition 5.5, $g \leq 2^n(n-1)+1$, and $\delta = 5 \cdot 2^n$. Take $q \geq 2^{2n+3}(n-1)^2$.

Then

$$\begin{aligned} &q + 1 - 2g\sqrt{q} - \delta \\ &\quad \geq 2^{2n+3}(n-1)^2 + 1 - 2(2^n(n-1) + 1)2^{n+1}(n-1)\sqrt{2} - 5 \cdot 2^n \\ &\quad \geq 2^n(2^{n+3}(n-1)^2 - 2^{n+2}(n-1)^2\sqrt{2} - 4\sqrt{2}(n-1) - 5) > 0 \end{aligned}$$

for any $n > 2$. □

6. Short Engel words in PSL$(2, q)$

In this section we prove Corollary B and show that for any $n \leq 4$ the n-th Engel word map is surjective for all groups PSL$(2, q)$. From Corollary 3.10 it follows that in order to prove that the map $e_{n+1} \colon G \times G \to G$ is surjective, one should check that for every $a \in \mathbb{F}_q$ either a or $-a$ belongs to the image T_n of ρ_n. For a fixed n and q big enough it follows from Theorem 5.1, and so for small values of q it may be verified by computer. Indeed, we have done the following calculations for small values of n using the Magma computer program.

Case $e_1 = [x, y]$. In this case, the surjectivity follows from Proposition 3.4, Proposition 3.6 and Remark 4.9. This provides an alternative proof to the well-known fact that any element in the group SL$(2, q)$ (and in the group PSL$(2, q)$), when $q > 3$, is a commutator (see [Th]).

Case $e_2 = [x, y, y]$. We need to prove that the map ρ_1 is surjective. Indeed, the equation

$$\rho_1(s, t) - a = s^2 - st^2 + 2t^2 - 2 - a = 0$$

defines a smooth curve of genus 1 with two punctures if $a^2 \neq 4$. Thus if $q > 7$ it has a point over $\mathbb{F}_q$. The case $a = 2$ was dealt with in Proposition 3.6. The cases $q = 5, 7$ can easily be checked by a computer. Therefore, e_2 is surjective on SL$(2, q) \setminus \{-\mathrm{id}\}$, and hence on PSL$(2, q)$ for any $q > 3$.

Case $e_3 = [x, y, y, y]$. Recall that by Example 4.1, e_3 is no longer surjective on SL$(2, q)$. In this case, the curve $\rho_2(s, t) - a$ has genus $2^2 + 1 = 5$ and it has at most 20 punctures at ∞, $t^2 = 4$ and $t = 0$. Thus the techniques of Section 5 may be applied for any q which satisfies

$$q + 1 - 10\sqrt{q} - 20 > 0,$$

that is, for any $q \geq 137$. For $q < 137$ the surjectivity on PSL$(2, q)$ was checked by a computer.

Case $e_4 = [x, y, y, y, y]$. In this case $g = 17$, and the computations were done for all $q \leq 1240$.

7. Equidistribution of the Engel words in PSL$(2, q)$

In this section we prove Theorem C by showing first that the n-th Engel word map is almost equidistributed for the family of groups SL$(2, q)$, where q is odd, and then explaining how this implies that the n-th Engel word map is almost equidistributed (and hence also almost measure-preserving) for the family of groups $\mathrm{PSL}(2, q)$, where q is odd.

More precisely, for $g \in \widetilde{G} = \mathrm{SL}(2, q)$, let

$$E_n(g) = \{(x, y) \in \widetilde{G} \times \widetilde{G} \mid e_n(x, y) = g\}.$$

By Definition 1.5 we then need to prove the following:

Proposition 7.1. *If q is an odd prime power, then the group $\widetilde{G} = \mathrm{SL}(2, q)$ contains a subset $S = S_{\widetilde{G}} \subseteq \widetilde{G}$ with the following properties:*

(i) $|S| = |\widetilde{G}|(1 - \epsilon)$,

(ii) $|\widetilde{G}|(1 - \epsilon) \leq |E_n(g)| \leq |\widetilde{G}|(1 + \epsilon)$ *uniformly for all* $g \in S$,

where $\epsilon \to 0$ *as* $q \to \infty$.

For the commutator word $e_1 = [x, y]$, Theorem C has already been proved in [GS], Proposition 5.1. Hence we may assume that $n > 1$. Following Section 5 we continue to assume that q is odd. We maintain the notation of Definition 3.2.

Proof of Proposition 7.1. Consider the commutative diagram of morphisms

$$\begin{array}{ccccc}
\widetilde{G} \times \widetilde{G} & \xrightarrow{\ \pi\ } & \mathbb{A}^3_{s,u,t} & \xrightarrow{\ p'\ } & \mathbb{A}^2_{s,t} \\
\downarrow{\scriptstyle \gamma} & \searrow^{\alpha} & & \swarrow^{\rho_n} & \downarrow{\scriptstyle \mu_n} \\
\widetilde{G} & \xrightarrow{\ \tau\ } & \mathbb{A}^1_s & \xleftarrow{\ \lambda_1\ } & \mathbb{A}^2_{s,t}.
\end{array}$$

Here $\gamma = \theta \circ \varphi_n = e_{n+1}$, $p'(s, u, t) = (s^2 + t^2 + u^2 - ust - 2, t)$, and α is a composition of the corresponding morphisms in the diagram.

We denote $f^{-1}(a) = f^{-1}(a)(\mathbb{F}_q)$. Let $a \in \mathbb{F}_q$, $a \neq \pm 2$. Then $\alpha^{-1}(a)$ is a union of the fibers $\Gamma_z = \gamma^{-1}(z)$, where $z \in \widetilde{G}$ is an element with $\mathrm{tr}(z) = a$. Since $a \neq \pm 2$, any Γ_z may be obtained from any other $\Gamma_{z'}$ (with $\mathrm{tr}(z') = a$) by conjugation, and so $|E_n(z)| = |E_n(z')|$. Hence,

$$|\gamma^{-1}(z)| = \frac{|\alpha^{-1}(a)|}{|\tau^{-1}(a)|}. \tag{7.1}$$

Recall that $|\mathrm{SL}(2, q)| = q^3 - q$. Take the set $S = S_{\widetilde{G}} = \{z \in \widetilde{G} \mid \mathrm{tr}(z) \neq \pm 2\}$. Then

$$|S| = q^3 - 2q^2 - q = q^3(1 - O(1/q)),$$

satisfying condition (i).

In order to prove condition (ii) it is enough to show that for any $z \in \widetilde{G}$ with $\mathrm{tr}(z) = a \neq \pm 2$,

$$|\gamma^{-1}(z)| = q^3(1 + \tilde{\epsilon}),$$

where $\tilde{\epsilon} \to 0$ as $q \to \infty$.

It is well known that

$$|\tau^{-1}(a)| = q^2(1 + \epsilon_1(q)), \tag{7.2}$$

where $|\epsilon_1(q)| \le \frac{1}{q}$ (see, for example [Do]).

On the other hand, $\alpha = \rho_n \circ p' \circ \pi$. Let us estimate $|\alpha^{-1}(a)|$.

Lemma 7.2. *Let $\tilde{p} = p' \circ \pi$. Then there are constants M_1 and M_2 such that for every $(s,t) \in \mathbb{A}^2_{s,t}$, $s \neq 2$, the following holds:*

(1) *If $t^2 \neq 4$ and $s \neq t^2 - 2$, then $|\tilde{p}^{-1}(s,t)| = q^4(1 + \epsilon_2)$, where $|\epsilon_2| \le \frac{M_1}{q}$.*

(2) *If $t^2 = 4$, then $|\tilde{p}^{-1}(s,t)| \le M_2 q^4$.*

Proof. We use the notation of Proposition 3.4.

(1) Assume that $t^2 \neq 4$ and $s \neq t^2 - 2$. According to case 2 of Proposition 3.4,

$$|p'^{-1}(s,t)| = |C_{s,t}(\mathbb{F}_q)| = q \pm 1. \tag{7.3}$$

For a point $(s', u, t) \in C_{s,t}(\mathbb{F}_q)$ we shall now compute $|\pi^{-1}(s', u, t)|$. We fix a matrix

$$y_t = \begin{pmatrix} t & 1 \\ -1 & 0 \end{pmatrix}$$

with $t^2 \neq 4$. Direct computation shows that $(x, y_t) \in \pi^{-1}(s', u, t)$ if

$$x = \begin{pmatrix} a & b \\ u + b - at & s' - a \end{pmatrix}$$

satisfies

$$\delta^2 - \omega^2\sigma^2 = p(s', u, t) - 2,$$

where

$$\omega^2 = t^2 - 4, \quad \sigma = a - \frac{bt}{2} - \frac{s'}{2}, \quad \delta = -u + \frac{s't}{2} + \frac{\omega^2 b}{2}.$$

Thus, we have a conic once more, and the number of such x is therefore $q \pm 1$. Together with (7.2) and (7.3) one has

$$|\tilde{p}^{-1}(s,t)| = (q \pm 1)(q \pm 1)q^2(1 + \epsilon_1(q)) = q^4(1 + \epsilon_2(q)),$$

where

$$|\epsilon_2| \le \frac{2}{q} + |\epsilon_1(q)| + O\left(\frac{1}{q^2}\right) \le \frac{4}{q}.$$

(2.1) Assume that $t = 2$. Then (see case 2 of Proposition 3.4)

$$|C_{s,t}(\mathbb{F}_q)| \le 2q, \tag{7.4}$$

where $s-2=v^2$, and $s'-u=\pm v$ for some $v\in\mathbb{F}_q$ and any $(s',u,t)\in C_{s,t}(\mathbb{F}_q)$.

We now consider matrices of the form

$$y_r=\begin{pmatrix}1 & r\\ 0 & 1\end{pmatrix}.$$

A pair $(x,y_r)\in\pi^{-1}(s',u,2)$ if

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

and

$$a(s'-a)-bc=1,\quad rc+s'=u.$$

This implies that

$$c=\frac{u-s'}{r}=\frac{\pm\omega}{r},\quad b=\frac{a(s'-a)-1}{c},\quad \omega^2=t^2-4.$$

Hence for a fixed y_r there are at most $2q$ possible matrices x defined by the value of a and by the sign of c. Together with (7.2) we get

$$|\pi^{-1}(s',u,2)|\le 2q(q^2+q).$$

It follows from (7.4) that

$$|\tilde{p}^{-1}(s,2)|\le 2q(q^2+q)2q\le 5q^4.$$

(2.2) Assume that $t=-2$. Similarly to (2.1) we get

$$|\tilde{p}^{-1}(s,2)|\le 2q(q^2+q)2q\le 5q^4.$$

To complete the proof we may take $M_1=4$ and $M_2=10$. □

We proceed with the proof of Proposition 7.1. By Theorem 5.1 and Proposition 5.5, the fiber $R_a=\rho_n^{-1}(a)$ of ρ_n is isomorphic to a general fiber of $X_{a-2}=r_n^{-1}(a-2)$ and is a curve of genus $g_n<G_n$, where the bound G_n depends only on n. Moreover, it has at most 2^n points at infinity and $2\cdot 2^n$ points with $t^2=4$. It does not have points of the form (t^2-2,t) since $\mu(t^2-2,t)=(2,t)$, which is a fixed point.

Let $A=R_a\cap\{t^2\neq 4\}$ and $B=R_a\cap\{t^2=4\}$. According to the Weil estimate,

$$|A(\mathbb{F}_q)|=q(1+\epsilon_3(n,q)),$$

where

$$|\epsilon_3(n,q)|\le\frac{1+2\sqrt{q}\cdot G_n+3\cdot 2^n}{q}.$$

Hence, according to Lemma 7.2 (1),

$$|\tilde{p}^{-1}(A)(\mathbb{F}_q)|=q(1+\epsilon_3(n,q))q^4(1+\epsilon_2):=q^5(1+\epsilon_4(n,q)),$$

where

$$|\epsilon_4(n,q)| \le |\epsilon_3(n,q)| + |\epsilon_2| + |\epsilon_3(n,q)| \cdot |\epsilon_2| = O(\tfrac{1}{\sqrt{q}}).$$

There are at most 2^{n+1} points in B. Thus by Lemma 7.2 (2),

$$|\tilde{p}^{-1}(B)(\mathbb{F}_q)| \le 2^{n+1} q^4 M_2.$$

Therefore,

$$|\alpha^{-1}(a)| = q^5(1 + \epsilon_5(n,q)), \tag{7.5}$$

where

$$|\epsilon_5(n,q)| \le |\epsilon_4(n,q)| + \frac{2^{n+1} M_2}{q} = O\Big(\frac{1}{\sqrt{q}}\Big).$$

Finally, from (7.1) and (7.5) we obtain

$$|\gamma^{-1}(z)| = \frac{|\alpha^{-1}(a)|}{|\tau^{-1}(a)|} = \frac{q^5(1+\epsilon_5(n,q))}{q^2(1+\epsilon_1(q))} = q^3\Big(1 + O\Big(\frac{1}{\sqrt{q}}\Big)\Big),$$

as needed. □

We shall now show that Proposition 7.1 implies that the n-th Engel word map is also almost equidistributed for the family of groups PSL$(2,q)$, where q is odd.

Denote by $\bar{g}$ the image of $g \in \widetilde{G} = \mathrm{SL}(2,q)$ in $G = \mathrm{PSL}(2,q)$. Since q is odd, one may identify $\bar{g}$ with the pair $\{\pm g\}$.

Let $S' = \{g \in \widetilde{G} \mid g \in S \text{ and } -g \in S\} \subseteq S$. Then, by Proposition 7.1 (i), $|S'| \le |\widetilde{G}|(1-2\epsilon)$. Hence, if $\bar{S}'$ is the image of the set S' in $G = \mathrm{PSL}(2,q)$, then

$$|\bar{S}'| \le |G|(1-2\epsilon).$$

For $\bar{g} \in G = \mathrm{PSL}(2,q)$, denote

$$\bar{E}_n(\bar{g}) = \{(\bar{x},\bar{y}) \in G \times G \mid e_n(\bar{x},\bar{y}) = \bar{g}\}.$$

Observe that

$$e_n(x,y) = e_n(-x,y) = e_n(x,-y) = e_n(-x,-y)$$

for any $x, y \in \widetilde{G}$. Thus

$$4 \cdot \bar{E}_n(\bar{g}) = E_n(g) \cup E_n(-g)$$

(this is a disjoint union) and so

$$\frac{|\bar{E}_n(\bar{g})|}{|G|} = \frac{|E_n(g)| + |E_n(-g)|}{2 \cdot |\widetilde{G}|}.$$

Therefore, by Proposition 7.1 (ii), for any $\bar{g} \in \bar{S}'$ one has

$$(1-\epsilon)|G| \le \bar{E}_n(\bar{g}) \le (1+\epsilon)|G|,$$

completing the proof of Theorem C.

8. Concluding remarks

The *trace map* is an efficient way to translate an Algebraic word problem on $\mathrm{PSL}(2,q)$ to the language of Geometry and Dynamics, which has already been used fruitfully in [BGK]. We use it in this paper for studying the Engel words, but actually the same could be done for any other word with the same dynamical properties. Thus, one may ask the following questions:

Question 8.1. What are the words for which the corresponding trace map $\psi(s,u,t) = (f_1(s,u,t), f_2(s,u,t), t)$ has the following property $(*)$ for almost all q:

$(*)$ For every $a \in \mathbb{F}_q$ the set $\{f_1(s,u,t) = a\}$ is an absolutely irreducible affine set.

Question 8.2. What are the words for which the trace map

$$\psi(s,u,t) = (f_1(s,u,t), f_2(s,u,t), t)$$

has an invariant plane A and the curves $\{\psi|_A = a\}$ are absolutely irreducible for a general $a \in \mathbb{F}_q$ and for almost all q?

We believe that these two questions are closely related to the following variant of Shalev's Conjecture 1.1:

Conjecture 8.3 (Shalev). *Assume that $w = w(x,y)$ is not a power word, that is, it is not of the form $v(x,y)^m$ for some $v \in F_2$ and $m \in \mathbb{N}$. Then $w(G) = G$ for $G = \mathrm{PSL}(2,q)$.*

One can moreover ask these questions for finite simple non-abelian groups in general.

Question 8.4. What is an analogue of the trace map for other finite simple non-abelian groups – in particular, for the Suzuki groups $\mathrm{Sz}(q)$? (See [BGK], §4.)

Another interesting question is related to the explicit estimates for q in Proposition 5.5. The genus of the curve X given there is very large, and this leads to an exponential bound for q, as a function of n, for which $X(\mathbb{F}_q) \neq \emptyset$. On the other hand, computer experiments using Magma demonstrate that this estimate should be at most polynomial. It would be very interesting to investigate X and to understand this phenomenon.

Acknowledgments. 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 Max-Planck-Institute for Mathematics (Bonn) and the Institut des Hautes Études Scientifiques (Bures-sur-Yvette).

This project started during the visit of Bandman and Garion to the Max-Planck-Institute for Mathematics (Bonn) in 2009 and continued during the visit of Grunewald to the Hebrew University of Jerusalem and Bar-Ilan University (2010).

Bandman and Garion are most grateful to B. Kunyavskii for his constant and very valuable help, to S. Vishkautsan and Eu. Plotkin for numerous and useful comments. The authors thank A. Shalev for discussing his questions and conjectures with them. They are also grateful to M. Larsen, A. Reznikov and V. Berkovich.

Finally the authors would like to thank the referee for valuable comments.

Fritz Grunewald has unexpectedly passed away in March 2010. This project started as a joint project with him, and unfortunately it is published only after his death. Fritz Grunewald has greatly inspired us and substantially influenced our work. He is deeply missed.

References

[AP] Y. Aubry and M. Perret, A Weil theorem for singular curves. In *Arithmetic, geometry and coding theory* (Luminy, 1993), Walter de Gruyter, Berlin 1996, 1–7. Zbl 0873.11037 MR 1394921

[BGK] T. Bandman, F. Grunewald, and B. Kunyavskiĭ, Geometry and arithmetic of verbal dynamical systems on simple groups. *Groups Geom. Dyn.* **4** (2010), 607–655. Zbl 05880956 MR 2727656

[Bl] H. I. Blau, A fixed-point theorem for central elements in quasisimple groups. *Proc. Amer. Math. Soc.* **122** (1994), 79–84. Zbl 0816.20017 MR 1254833

[Bo] A. Borel, On free subgroups of semi-simple groups. *Enseign. Math.* (2) **29** (1983), 151–164. Zbl 0533.22009 MR 702738

[Mag] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: The user language. *J. Symbolic Comput.* **24** (1997), 235–265. Zbl 0898.68039 MR 1484478

[CMS] J. Cossey, S. O. Macdonald, and A. P. Street, On the laws of certain finite groups. *J. Austral. Math. Soc.* **11** (1970), 441–489. Zbl 0232.20044 MR 0283058

[DS] V. I. Danilov and V. V. Shokurov, *Algebraic curves, algebraic manifolds and schemes*. Encyclopaedia Math. Sci. 23, Springer, Springer-Verlag, Berlin 1998. Zbl 0901.14013 MR 1658464

[Do] L. Dornhoff, *Group representation theory. Part A: Ordinary representation theory*. Marcel Dekker Inc., New York 1971. Zbl 0227.20002 MR 0347959

[EG] E. W. Ellers and N. Gordeev, On the conjectures of J. Thompson and O. Ore. *Trans. Amer. Math. Soc.* **350** (1998), 3657–3671. Zbl 0910.20007 MR 1422600

[Fr] R. Fricke, Über die Theorie der automorphen Modulgruppen. *Nachr. Akad. Wiss. Göttingen Math.-Phsy. Kl.* **1896** (1896), 91–101. JFM 27.0326.02

[FK] R. Fricke and F. Klein, *Vorlesungen über die Theorie der automorphen Funktionen*. Vol. 1, 2, B. G. Teubner, Leipzig 1897, 1912. JFM 28.0334.01 JFM 32.0430.01

[GS] S. Garion and A. Shalev, Commutator maps, measure preservation, and T-systems. *Trans. Amer. Math. Soc.* **361** (2009), 4631–4651. Zbl 1182.20015 MR 2506422

[GL] S. R. Ghorpade and G. Lachaud, Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. *Moscow Math. J.* **2** (2002), 589–631; Corrigenda and addenda: Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields, *ibid.* **9** (2009), 431–438. Zbl 1101.14017 MR 1988974

[Go] W. Goldman, An exposition of results of Fricke and Vogt. Preprint 2004. arXiv:math/0402103

[Ha] R. Hartshorne, *Algebraic geometry*. Graduate Texts in Math. 52, Springer-Verlag, New York 1977. Zbl 0367.14001 MR 0463157

[KL] W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group. *Geom. Dedicata* **36** (1990), 67–87. Zbl 0718.20011 MR 1065213

[La] M. Larsen, Word maps have large image. *Israel J. Math.* **139** (2004), 149–156. Zbl 1130.20310 MR 2041227

[LS] M. Larsen and A. Shalev, Word maps and Waring type problems. *J. Amer. Math. Soc.* **22** (2009), 437–466. Zbl 1206.20014 MR 2476780

[LST] M. Larsen, A. Shalev, and P. H. Tiep, The Waring problem for finite simple groups. *Ann. of Math.* (2) **174** (2011), 1885–1950. Zbl 06005486 MR 2846493

[LY] D. B. Leep and C. C. Yeomans, The number of points on a singular curve over a finite field. *Arch. Math.* (*Basel*) **63** (1994), 420–426. Zbl 0819.11023 MR 1300736

[LOST] M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep, The Ore conjecture. *J. Eur. Math. Soc.* (*JEMS*) **12** (2010), 939–1008. Zbl 1205.20011 MR 2654085

[Ma] W. Magnus, Rings of Fricke characters and automorphism groups of free groups. *Math. Z.* **170** (1980), 91–103. Zbl 0433.20033 MR 558891

[MW] D. McCullough and M. Wanderley, Writing elements of $\mathrm{PSL}(2,q)$ as commutators. *Comm. Algebra* **39** (2011), 1234–1241. Zbl 1214.20046 MR 2782601

[Or] O. Ore, Some remarks on commutators. *Proc. Amer. Math. Soc.* **2** (1951), 307–314. Zbl 0043.02402 MR 0040298

[Sa] P. Samuel, *Méthodes d'algèbre abstraite en géométrie algébrique*. Seconde edition, corrigee, Ergeb. Math. Grenzgeb. 4, Springer-Verlag, Berlin 1967. Zbl 0146.16901 MR 0213347

[Se] D. Segal, *Words: notes on verbal width in groups*. London Math. Soc. Lecture Note Ser. 361, Cambridge University Press, Cambridge 2009. Zbl 1198.20001 MR 2547644

[Sh07] A. Shalev, Commutators, words, conjugacy classes and character methods. *Turkish J. Math.* **31** (2007), Suppl., 131–148. Zbl 1162.20014 MR 2369828

[Sh09] A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem. *Ann. of Math.* (2) **170** (2009), 1383–1416. Zbl 1203.20013 MR 2600876

[Th] R. C. Thompson, Commutators in the special and general linear groups. *Trans. Amer. Math. Soc.* **101** (1961), 16–33. Zbl 0109.26002 MR 0130917

[Vo] H. Vogt, Sur les invariants fundamentaux des equations différentielles linéaires du second ordre. Ann. Sci. École Norm. Sup. (3) **6** (1889), Suppl., 3–71. JFM 21.0314.01 http://www.numdam.org/item?id=ASENS_1889_3_6__S3_0

Received September 23, 2010; revised March 30, 2011

T. Bandman, Department of Mathematics, Bar-Ilan University, 52900 Ramat Gan, Israel
E-mail: bandman@macs.biu.ac.il

S. Garion, Mathematisches Institut, Universität Münster, Einsteinstr. 62, 48149 Münster, Germany
E-mail: shellyg@ihes.fr

F. Grunewald, Mathematisches Institut, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, 40225 Düsseldorf, Germany