Max-Planck-Institut für Mathematik
Bonn

Criteria for equidistribution of solutions of matrix equations

by

Tatiana Bandman
Boris Kunyavskii

Max-Planck-Institut für Mathematik
Preprint Series 2011 (66)

Criteria for equidistribution of solutions of matrix equations

Tatiana Bandman
Boris Kunyavskii

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Department of Mathematics
Bar-Ilan University
52900 Ramat Gan
Israel

MPIM 11-66

CRITERIA FOR EQUIDISTRIBUTION OF SOLUTIONS OF MATRIX EQUATIONS

TATIANA BANDMAN, BORIS KUNYAVSKIĬ

Abstract. We study equidistribution of solutions of word equations of the form $w(x, y) = g$ in the family of finite groups $\mathrm{SL}(2, q)$. We provide criteria for equidistribution in terms of the trace polynomial of w. This allows us to get an explicit description of certain classes of words possessing the equidistribution property and show that this property is generic within these classes.

1. Introduction

Equidistribution of solutions of various (systems of) diophantine equations has been remaining one of central topics in number theory, arithmetic geometry, ergodic theory. It is not our goal to review vast literature in the area. The reader interested in evolution of ideas in this fascinating domain of mathematics may find instructive to overview materials of ICM's, starting from the foundational address by Linnik (Stockholm, 1962) until impressive contributions of the past two decades: Margulis, Sarnak (Kyoto, 1990); Dani, Ratner (Zürich, 1994); Eskin (Berlin, 1998); Ullmo (Beijing, 2002); Einsiedler–Lindenstrauss, Michel–Venkatesh, Tschinkel (Madrid, 2006); Oh, Shah (Hyderabad, 2010). Each of the approaches mentioned above assumes its own understanding of the notion of equidistribution. What most of them share in common is focusing on certain group actions arising in a natural way and allowing one to combine methods of number theory and dynamical systems with group-theoretic considerations.

Let us describe the circle of problems we are interested in. First, we want to study *polynomial matrix equations*. In the most general form, one can consider equations of the form $P(A_1, \dots, A_m, X_1, \dots, X_d) = 0$ where $n \times n$-matrices $A_1, \dots, A_m$ with entries from a ring R are *given* (both n and R are *fixed*, $X_1, \dots, X_d$ are *unknowns*, and P is an *associative noncommutative* polynomial). We, however, restrict our attention to a particular class of equations of the form $P(X_1, \dots, X_d) = A$ where A is a fixed matrix, $X_1, \dots, X_d$ are unknowns, and a solution must belong to a fixed subset $\mathcal{M} \subset \mathrm{M}(n, R)^d$. There are several cases

The authors were supported in part by the Minerva Foundation through the Emmy Noether Research Institute for Mathematics. The work was finished during the visit of the second author to the MPIM (Bonn). Support of these institutions is gratefully appreciated.

where such an equation has a solution for a "generic" A (here $R = K$ is an algebraically closed field):

- $\mathcal{M} = G(K)^d$ where $G(K)$ is the group of rational points of a connected semisimple algebraic group and $P = w \neq 1$ is a nontrivial word (=monomial in $X_1, X_1^{-1}, \dots, X_d, X_d^{-1}$ [Bo], [La]);
- $\mathcal{M} = \mathfrak{g}^d$ where the Lie algebra $\mathfrak{g}$ of a semisimple algebraic K-group and a Lie polynomial P satisfy some additional assumptions [BGKP];
- $\mathcal{M} = \mathrm{M}(n, K)^d$ and P satisfies some additional assumptions [KBMR].

If $R = \mathbb{Z}$, in all these cases we may interpret the situation as follows: the generic fibre of the morphism $\mathbb{P}\colon \mathbb{M}^d \to \mathbb{M}$ of $\mathbb{Z}$-schemes, induced by the polynomial P, is a *dominant* morphism of $\mathbb{Q}$-schemes.

One can ask whether the situation is similar in *special* fibres of the morphism P. As the notion of dominance does not make much sense for finite sets, we would like to formalize the following phenomena:

- all maps $P_q\colon (M_q)^d \to M_q$ have "large" images;
- the number $\#\{(A_1, \dots, A_d) \in (M_q)^d : P_q(A_1, \dots, A_d) = A\}$ (where $q = p^n$; $p = 2, 3, 5, \dots$; A runs over a "large" subset of M_q) is, in some reasonable sense, almost independent of A.

(Here M_q denotes the set of $\mathbb{F}_q$-points of the fibre of the scheme $\mathbb{M}$ at q, and P_q is the fibre of the morphism $\mathbb{P}$ at q.)

Roughly, the conditions formulated above mean that the equations $P(X_1, \dots, X_d) = A$, with the right-hand side running, for each q, over "almost whole" set M_q, have many and almost equally many solutions in $(M_q)^d$, respectively. We shall call such morphisms *p-almost equidistributed*, or *almost equidistributed* (depending on whether p in the second condition is or is not fixed); the word "almost" will often be dropped. See Section 2 for precise definitions.

According to [La], [LS], the word map is "fibrewise dominant" for any $w \neq 1$ and any Chevalley group G (i.e., the images of the maps P_q are "large"). Our main result (Theorem 2.14) provides a necessary and sufficient condition on the word w in two variables under which the corresponding morphism $w\colon \mathrm{SL}_2 \times \mathrm{SL}_2 \to \mathrm{SL}_2$ is almost equidistributed. This result can be viewed, on the one hand, as a refinement (in the SL_2-case) of equidistribution theorems of [LP], [LST] on general words w and general Chevalley groups G, and, on the other hand, as a generalization of equidistribution theorems for some particular words: [GS] (commutator words on any G), [BGG] (Engel words on SL_2), [BG] (positive words on SL_2).

Acting in the spirit of [GS], we deduce a criterion for $w\colon \mathrm{SL}_2 \times \mathrm{SL}_2 \to \mathrm{SL}_2$ to be *almost measure-preserving*.

Note that certain word maps are measure-preserving in a much stronger sense. Namely, if w is *primitive*, i.e., is a part of a basis of the free d-generated group F_d, then the corresponding word map $G^d \to G$ is measure-preserving for *every finite group* G, i.e., all fibres of this map have the same cardinality. Only primitive words possess this property, this was proven for $d = 2$ in [Pu] and recently extended to arbitrary d by Puder and Parzanchevski. It is well known (see, e.g., [MS]) that primitive words are asymptotically rare (negligible, in the terminology of [KS]). We are looking for criteria for equidistribution for more general words.

The criteria we are talking about are formulated in terms of the *trace polynomial* of the word w. It turns out (see our main results in Section 2; they are proved in Section 3) that "good" (equidistributed, measure-preserving) words are essentially those whose trace polynomial cannot be represented as a composition of two other polynomials. Since a "bad" trace polynomial turns out to be the trace polynomial of some power word (see Section 4), we conclude (see Section 5) that within certain natural classes of words a "random" word is "good" ("good" words, i.e., those whose trace map is p-equidistributed for all but finitely many primes p, form an exponentially generic set, in the sense of [KS]).

2. Main results

We start with precise definitions of notions described in the introduction. All schemes under consideration are assumed geometrically integral and of finite type.

We will follow the approach to equidistribution adopted in [GS]:

Definition 2.1. (cf. [GS, §3]) Let $f\colon X \to Y$ be a map between finite non-empty sets, and let $\varepsilon > 0$. We say that f is *ε-equidistributed* if there exists $Y' \subseteq Y$ such that

(i) $\#Y' > \#Y(1-\varepsilon)$;
(ii) $|f^{-1}(y) - \frac{\#X}{\#Y}| < \varepsilon\frac{\#X}{\#Y}$ for all $y \in Y'$.

Our setting is as follows. Let a family of maps of finite sets $P_q\colon X_q \to Y_q$ be given for every $q = p^n$. Assume that for all sufficiently large q the set Y_q is non-empty. For each such q take $y \in Y_q$ and denote

$$P_y = \{x \in X_q : P_q(x) = y\}$$

(P_y may be empty).

Definition 2.2. Fix a prime p. With the notation as above, we say that the family $P_q\colon X_q \to Y_q$, $q = p^n$, is *p-equidistributed* if there exist a positive integer n_0 and a function $\varepsilon_p\colon \mathbb{N} \to \mathbb{N}$ tending to 0 as $n \to \infty$ such that for all $q = p^n$ with $n > n_0$ the set Y_q contains a subset S_q with the following properties:

(i) $\#S_q < \varepsilon_p(q)\,(\#Y_q)$;
(ii) $|P_y - \frac{\#X_q}{\#Y_q}| < \varepsilon_p(q)\frac{\#X_q}{\#Y_q}$ for all $y \in Y_q \setminus S_q$.

Remark 2.3. Definition 2.2 means that for $q = p^n$ large enough, the map $X_q \to Y_q$ is $\varepsilon_p(q)$-equidistributed, in the sense of Definition 2.1.

Definition 2.4. We say that the family $P_q\colon X_q \to Y_q$ is *equidistributed* if it is p-equidistributed for all p and there exists a function $\varepsilon\colon \mathbb{N} \to \mathbb{N}$ tending to 0 as $n \to \infty$ such that for every p and every $q = p^n$ large enough, we have $\varepsilon_p(q) \le \varepsilon(q)$.

Remark 2.5. Typically, the situation of Definitions 2.2 and 2.4 arises for the family of special fibres of a morphism $\mathbb{P}\colon \mathbb{X} \to \mathbb{Y}$ of $\mathbb{Z}$-schemes (or, more generally, of O-schemes where O is the ring of integers of a global field) when $X_q = \mathbb{X}_q(\mathbb{F}_q)$, $Y_q = \mathbb{Y}_q(\mathbb{F}_q)$. In this situation we shorten our terminology and say that the morphism $\mathbb{P}$ is p-equidistributed (or equidistributed). Note that since $\mathbb{Y}$ is assumed geometrically integral, the condition $Y_q \neq \emptyset$ holds automatically if q is large enough.

We have adopted a slightly more flexible setting in Definitions 2.2 and 2.4 which allows broader applications, see Remark 2.16 below.

Let us now consider the case where $Y_q = G_q$ is a Chevalley group over $\mathbb{F}_q$, $X_q = (G_q)^d$ is a direct product of its d copies ($d \ge 2$ is fixed), and $P_q = P_{w,q}\colon (G_q)^d \to G_q$ is the morphism induced by some fixed word $w \in F_d$: to each d-tuple $(g_1, \dots, g_d)$ we associate the value $w(g_1, \dots, g_d)$.

In the present paper we focus our attention on a particular case $d = 2$, $G_q = \mathrm{SL}(2, q)$. Accordingly, we say that w is equidistributed (or p-equidistributed) if so is the family of maps $P_{w,q}\colon\ \mathrm{SL}(2,q)\times\mathrm{SL}(2,q) \to \mathrm{SL}(2,q)$ (or, in other words, if so is the morphism $\mathbb{P}_w\colon\ \mathrm{SL}_{2,\mathbb{Z}} \times \mathrm{SL}_{2,\mathbb{Z}} \to \mathrm{SL}_{2,\mathbb{Z}}$ of group schemes over $\mathbb{Z}$).

In such a situation, there is a natural way to associate to a word $w = w(x, y) \in F_2$ its *trace polynomial.* This construction goes back to the 19th century (Vogt, Fricke, Klein), see, e.g., [Ho] for a modern exposition: we embed F_2 into $\mathrm{SL}(2, \mathbb{Z})$ and denote by tr its trace character, then the trace of $w \in F_2$ can be expressed as $\mathrm{tr}(w) = f_w(s, u, t)$ where $f_w \in \mathbb{Z}[s, u, t]$ is an integer polynomial in three variables $s = \mathrm{tr}(x)$, $u = \mathrm{tr}(xy)$, $t = \mathrm{tr}(y)$. We denote by the same letters the induced morphisms of affine $\mathbb{Z}$-schemes

$$f_w\colon \mathbb{A}^3_{s,u,t} = \operatorname{Spec}\mathbb{Z}[s,u,t] \to \mathbb{A}^1_z = \operatorname{Spec}\mathbb{Z}[z],$$

of affine $\overline{\mathbb{F}}_p$-schemes:

$$f_{w,p}\colon\ \operatorname{Spec}\overline{\mathbb{F}}_p[s,u,t] \to \operatorname{Spec}\overline{\mathbb{F}}_p[z],$$

and also maps of sets of $\overline{\mathbb{F}}_p$-points:

$$f_{w,p}\colon \mathbb{A}^3_{s,u,t}(\overline{\mathbb{F}}_p) \to \mathbb{A}^1_z(\overline{\mathbb{F}}_p)$$

(here $\mathbb{A}^N_{x_1,\dots,x_N}$ stands for affine space with coordinates $x_1, \dots, x_N$).

Our criteria for equidistribution of w will be formulated in terms of the polynomial f_w. Some recollections and definitions on polynomials are on order.

Definition 2.6. Let $\mathbb{F}$ be a finite field. We say that $h \in \mathbb{F}[x]$ is a *permutation* polynomial if the set of its values $\{h(z)\}_{z\in\mathbb{F}}$ coincides with $\mathbb{F}$.

Theorem 2.7. [LN, Theorem 7.14] *Let $q = p^n$. A polynomial $h \in \mathbb{F}_q[x]$ is a permutation polynomial of all finite extensions of $\mathbb{F}_q$ if and only if $h = ax^{p^k} + b$, where $a \neq 0$ and k is a non-negative integer.*

The following notions are essential for our criteria.

Definition 2.8. Let F be a field. We say that a polynomial $P \in F[x_1, \dots, x_n]$ is *F-composite* if there exist $Q \in F[x_1, \dots, x_n], \deg Q \geq 1$, and $h \in F[z], \deg h \geq 2$, such that $P = h \circ Q$. Otherwise, we say that P is *F-noncomposite.*

Note that if E/F is a separable field extension, it is known [AP, Theorem 1 and Proposition 1] that P is F-composite if and only if P is E-composite. In particular, working over perfect ground fields, we may always assume, if needed, that F is algebraically closed.

Definition 2.9. Let $P \in \mathbb{Z}[x_1, \dots, x_n]$. Fix a prime p.

- We say that P is *p-composite* if the reduced polynomial $P_p \in \mathbb{F}_p[x_1, \dots, x_n]$ is $\mathbb{F}_p$-composite. Otherwise, we say that P is *p-noncomposite.*
- We say that a p-composite polynomial P is *p-special* if, in the notation of Definition 2.8, $P_p = h \circ Q$ where $h \in \mathbb{F}_p[x]$ is a permutation polynomial of all finite extensions of $\mathbb{F}_p$.

Definition 2.10. We say that a polynomial $P \in \mathbb{Z}[x_1, \dots, x_n]$ is *almost noncomposite* if for every prime p it is either p-noncomposite or p-special. Otherwise we say that P is *very composite.*

Remark 2.11. If a polynomial $P \in \mathbb{Z}[x_1, \dots, x_n]$ is $\mathbb{Q}$-noncomposite, it is p-noncomposite for all but finitely many primes p [BDN, 2.2.1]. If $P \in \mathbb{Z}[x_1, \dots, x_n]$ is $\mathbb{Q}$-composite, it is very composite.

Example 2.12. Consider the family of Dickson polynomials $\mathcal{D}_n(x, a)$. Denote $D_n(x) = \mathcal{D}_n(x, 1)$. We have $D_n(x) = 2T_n(x/2)$ where $T_n(x)$ is the n^{th} Chebyshev polynomial. If n is not prime then D_n is very composite (see, e.g., Section 4 below). If $n = p$ is prime, then D_n is almost noncomposite and p-special since $D_p(x) = x^p$ in $\mathbb{F}_p[x]$.

We can now formulate our main results.

Theorem 2.13. *Let $w \in F_2$. The morphism $\mathbb{P}_w\colon \mathrm{SL}_{2,\mathbb{Z}} \times \mathrm{SL}_{2,\mathbb{Z}} \to \mathrm{SL}_{2,\mathbb{Z}}$ is p-equidistributed if and only if the trace polynomial f_w is either p-noncomposite or p-special.*

Theorem 2.14. *Let $w \in F_2$. The morphism $\mathbb{P}_w\colon \mathrm{SL}_{2,\mathbb{Z}} \times \mathrm{SL}_{2,\mathbb{Z}} \to \mathrm{SL}_{2,\mathbb{Z}}$ is equidistributed if and only if the trace polynomial f_w is almost noncomposite.*

For a given word $w \in F_2$, let us now consider the family of groups $\hat{G}_q = \mathrm{PSL}(2, q)$ and the corresponding word maps $w_q\colon \hat{G}_q \times \hat{G}_q \to \hat{G}_q$.

Proposition 2.15. *If the morphism $\mathbb{P}_w\colon \mathrm{SL}_{2,\mathbb{Z}} \times \mathrm{SL}_{2,\mathbb{Z}} \to \mathrm{SL}_{2,\mathbb{Z}}$ is equidistributed (or p-equidistributed), then so is the family of maps $w_q\colon \hat{G}_q \times \hat{G}_q \to \hat{G}_q$.*

Remark 2.16. This proposition partially explains our flexibility in Definitions 2.2 and 2.4: since $\mathrm{PSL}(2, \mathbb{Z})$ does not exist as a group scheme, the family w_q cannot arise as the family of fibres of a word morphism of $\mathbb{Z}$-schemes.

3. Proofs

Fix a word w in F_2. We slightly change the general notation, and for a group Γ and $g \in \Gamma$ we denote

$$W_{g,\Gamma} = \{(x, y) \in \Gamma \times \Gamma : w(x, y) = g\}.$$

We will omit the subscript Γ when no confusion may arise. For $\Gamma = G_q = \mathrm{SL}(2, q)$ we denote this set by $W_{g,q}$ (or just W_g).

Since $\#G_q = q(q^2 - 1)$, we will replace, if needed, $\#G_q$ by q^3 in all asymptotic estimates.

Proof of Theorem 2.13. Slightly rephrasing Definition 2.2, we are going to prove that there exist positive numbers n_0, A, B, α, β, all independent of $g \in G_q$, such that for every $q > q_0 = p^{n_0}$ there exists $S_q \subset G_q$ with the following properties:

(i) $\#S_q/q^3 < Aq^{-\alpha}$;

(ii) for every $g \in T_q := G_q \setminus S_q$ we have $\left|\dfrac{\#W_{g,q}}{q^3} - 1\right| < Bq^{-\beta}$. (1)

Indeed, this is enough for proving that w is p-equidistributed: in Definition 2.2 one can then take $\varepsilon_p(q) := \max\{Aq^{-\alpha}, Bq^{-\beta}\}$.

Towards this end, we will use the following commutative diagram:

$$\begin{tikzcd} G_q \times G_q \arrow[r, "w"] \arrow[d, "\pi"'] & G_q \arrow[d, "\mathrm{tr}"] \\ \mathbb{A}^3_{s,u,t}(\mathbb{F}_q) \arrow[r, "f_w"] & \mathbb{A}^1_z(\mathbb{F}_q) \end{tikzcd} \qquad (2)$$

where

$$\pi(x, y) = (\mathrm{tr}(x), \mathrm{tr}(xy), \mathrm{tr}(y)). \qquad (3)$$

"Typical" fibres of the maps in this diagram should consist of $O(q^3)$ elements (for w and π), and of $O(q^2)$ elements (for tr and f_w). Below we will show how to attain this with an error term of order $O(q^{-\beta})$ by throwing away $O(q^{-\alpha})$ elements.

We will use an explicit Lang–Weil estimate of the following form: if $H \subset \mathbb{A}^3_{\mathbb{F}_q}$ is an *absolutely irreducible* hypersurface of degree d, then

$$|\#H(\mathbb{F}_q) - q^2| \le (d-1)(d-2)q^{3/2} + 12(d+3)^4 q$$

(see, e.g., [GL, Remark 11.3]), or, equivalently, $\#H(\mathbb{F}_q) = q^2(1 + r_1)$ with

$$|r_1| \le q^{-1/2}[(d-1)(d-2) + 12(d+3)^4 q^{-1/2}]. \tag{4}$$

(The remainder term $r_1 = r_1(H)$, as well as all remainder terms in the sequel, may depend on the hypersurface under consideration. To ease the notation, we do not include this dependence in formulas.)

For $d > 4$ and $q > 16$, equation (4) gives

$$|r_1| < q^{-1/2}(d^2 + 12 \cdot 2^4 d^4/4) < d^4 q^{-1/2}(1/d^2 + 48) < 50 d^4 q^{-1/2}. \tag{5}$$

Moreover, if $d > 4$ and $q > 4(50d^4)^2$, then $|r_1| < 1/2$. This remains true also for $d \le 3$. Without loss of generality, we may and will assume that the latter inequality is valid.

Step 1. Suppose that the polynomial f_w is p-noncomposite.

Denote the degree of f_w by d, the degree of the reduced polynomial $f_{w,p}$ is then at most d. Consider the corresponding reduced map $f_{w,p} \colon \mathbb{A}^3_{s,u,t}(\overline{\mathbb{F}}_p) \to \mathbb{A}^1_z(\overline{\mathbb{F}}_p)$.

Denote by $\sigma(f_{w,p})$ the spectrum of $f_{w,p}$, i.e., the set of all points $z \in \mathbb{A}^1_z(\overline{\mathbb{F}}_p)$ such that the hypersurface $H_z \subset \mathbb{A}^3_{s,u,t}(\overline{\mathbb{F}}_p)$, defined by the equation $f_w(s,u,t) = z$, is reducible. By a generalized Stein–Lorenzini inequality [Na], this set contains at most $d-1$ points. The same is true for each $\sigma_q(f_w) := \sigma(f_{w,p}) \cap \mathbb{F}_q$. Without loss of generality, we may and will assume that ± 2 are inside $\sigma_q(f_w)$ (by enlarging $\#\sigma_q(f_w)$ to $d+1$).

Let $z \in \mathbb{A}^1_z(\overline{\mathbb{F}}_p) \setminus \sigma(f_{w,p})$. Then H_z is an irreducible hypersurface and hence (4), (5) are valid for H_z.

Lemma 3.1. *Let $H \subset \mathbb{A}^3_{s,u,t}(\overline{\mathbb{F}}_p)$ be a hypersurface of degree d. Let $D(s,u,t) = (t^2-4)(s^2-4)(s^2+t^2+u^2-ust-4)$, and let $\Delta \subset \mathbb{A}^3_{s,u,t}$ be defined by the equation $D = 0$. Assume that $H \not\subset \Delta$. Then* (*see* (3)) *we have $\#\pi^{-1}(H)(\mathbb{F}_q) = \#H(\mathbb{F}_q)q^3(1 + r_2)$, where $|r_2| < 157d/q$.*

Proof. We use the following fact (see, [BG, Proposition 7.2]):

$$\#\pi^{-1}(s,u,t)(\mathbb{F}_q) = q^3(1 + \delta_1(s,u,t)),\ |\delta_1| \le 3/q,$$

if $(s,u,t) \notin \Delta(\mathbb{F}_q)$, and

$$\#\pi^{-1}(s,u,t)(\mathbb{F}_q) \le 2q^3(1 + 1/q)$$

if $(s,u,t) \in \Delta(\mathbb{F}_q)$.

Denote $H \cap \Delta$ by H_Δ. By Bezout's theorem, this is a curve of degree at most $7d$, hence $\#H_\Delta(\mathbb{F}_q) \le 7d(q+1)$.

We have

$$\begin{aligned}\#\pi^{-1}(H)(\mathbb{F}_q) &= \#\pi^{-1}(H \setminus H_\Delta)(\mathbb{F}_q) + \#\pi^{-1}(H_\Delta)(\mathbb{F}_q)\\ &\leq \#(H \setminus H_\Delta)(\mathbb{F}_q)q^3(1+\alpha_1) + \#H_\Delta(\mathbb{F}_q)q^3\alpha_2,\end{aligned}$$

where $|\alpha_1| \leq 3/q$ and $|\alpha_2| \leq 2(1+1/q) \leq 3$. Thus

$$\begin{aligned}\#\pi^{-1}(H)(\mathbb{F}_q) &= \#H(\mathbb{F}_q)q^3\left[\left(1 - \frac{\#H_\Delta(\mathbb{F}_q)}{\#H(\mathbb{F}_q)}\right)(1+\alpha_1) + \frac{\#H_\Delta(\mathbb{F}_q)}{\#H(\mathbb{F}_q)}\alpha_2\right]\\ &= \#H(\mathbb{F}_q)q^3(1+r_2)\end{aligned}$$

with

$$\begin{aligned}|r_2| &\leq \frac{\#H_\Delta(\mathbb{F}_q)}{\#H(\mathbb{F}_q)}(1+|\alpha_1|+|\alpha_2|)+|\alpha_1|\\ &\leq \frac{7d(q+1)}{q^2(1+r_1)}(1+|\alpha_1|+|\alpha_2|)+|\alpha_1|\\ &\leq \frac{7d \cdot 2q \cdot (11/2)}{q^2/2} + \frac{3}{q} \leq \frac{157d}{q}.\end{aligned}$$

□

Let S'_q be the set of all $z \in \mathbb{F}_q$ such that $H_z \subset \Delta$ (see Lemma 3.1). This set is finite, and $\#S'_q \leq 7$ since Δ is of degree 7 and thus cannot contain more than 7 irreducible components.

Let $\tau\colon G_q \to \mathbb{A}^1$ be the trace map, $\tau(g) = \mathrm{tr}(g)$. We have $\#\tau^{-1}(z) \leq q(q+1)$.

We define $\tilde{S}_q := \sigma_q(f_w) \cup S'_q$ and $S_q := \tau^{-1}(\tilde{S}_q)$. By construction,

$$\#S_q \leq (d+8)q(q+1) \leq q^3\frac{2(d+8)}{q}.$$

According to Lemma 3.1, for any $z \in T_q$ we have

$$\#\pi^{-1}(H_z)(\mathbb{F}_q) = \#H_z(\mathbb{F}_q)q^3(1+r_2) = q^5(1+r_1)(1+r_2).$$

On the other hand, all $g \in G_q$ with $\mathrm{tr}(g) = z \in T_q$ are conjugate, and there are $\#\tau^{-1}(z) = q(q \pm 1)$ such elements. Hence for every such g we have (see diagram(2))

$$\#W_g = \frac{\#\pi^{-1}(H_z)(\mathbb{F}_q)}{q(q\pm 1)} = \frac{q^5(1+r_1)(1+r_2)}{q(q\pm 1)} = q^3(1+r_3)$$

with

$$|r_3| \leq 2(|r_1|+|r_2|+|r_1r_2|) \leq 2|r_1|+3|r_2|.$$

Recall that $q \geq 4(50d^4)^2$, hence

$$|r_3| \leq 2 \cdot 50d^4q^{-1/2} + 3 \cdot 157d/q \leq q^{-1/2}(100d^4+1).$$

So for $q > q_0 = 4(50d^4)^2$, in equation (1) we can take

$$A = 2(d+8), \alpha = 1, B = 100d^4+1, \beta = 1/2. \tag{6}$$

Thus f_w is p-equidistributed.

Remark 3.2. Note that q_0 and all numbers in (6) depend only on w (through d, the degree of the trace polynomial f_w) and not on p.

Step 2. Suppose that the polynomial f_w is p-composite.

This means that $f_w(s,u,t) = R(Q(s,u,t))$ where $R \in \mathbb{F}_p[x]$ is a polynomial in one variable of degree $d_1 \geq 2$ and $Q \in \mathbb{F}_p[s,u,t]$ is a noncomposite polynomial in three variables.

Consider three separate cases.

Case 1. f_w is p-special, i.e., R is a permutation polynomial of all fields $\mathbb{F}_q$, $q = p^n$. For any $z \in \mathbb{F}_q$ there is a unique $x \in \mathbb{F}_q$ such that the hypersurface $H_z \subset \mathbb{A}^3$, defined by the equation $f_w(s,u,t) = z$, coincides with the hypersurface $\tilde{H}_x$, defined by the equation $Q(s,u,t) = x$. Since Q is noncomposite, **Step 1** implies that w is p-equidistributed in this case.

Remark 3.3. In this case, the parameters q_0, A, B, α, β also do not depend on p. They depend on the word w, this time through the degree of Q which is less than the degree of the trace polynomial of w.

Case 2. R is not a permutation polynomial for $\mathbb{F}_q$, $q = p^n$. Then it is not a permutation polynomial for any extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$.

According to [Wa], [WSC], there exists a subset $U_m \subset \mathbb{A}^1_z(\mathbb{F}_{q^m})$ such that

- $\#U_m \geq (q^m - 1)/d_1$;
- $R^{-1}(s)(\mathbb{F}_{q^m}) = \emptyset$ for every $s \in U_m$.

It follows that $f_w^{-1}(s)(\mathbb{F}_{q^m}) = \emptyset$ for every m and every $s \in U_m$. So the polynomial $\pi \circ f_w$ also omits at least $(q^m - 1)/d_1$ values, and hence so does $w \circ \mathrm{tr}$ (see diagram (2)), i.e., $w(G_{q^m} \times G_{q^m})$ contains no elements $g \in G_{q^m}$ with $\mathrm{tr}(g) \in U_m$. For every $s \in \mathbb{F}_{q^m}$, $s \neq \pm 2$, the group G_{q^m} contains at least $(q^m)^2 - q^m$ elements with trace s. Thus w omits at least

$$q^m(q^m - 1)[(q^m - 1)/d_1 - 2] \approx (q^m)^3/d_1$$

values. Hence w is not p-equidistributed.

Case 3. R is a permutation polynomial for $\mathbb{F}_q$ but not for an extension $\mathbb{F}_{q^m}$. Then we can start with $\mathbb{F}_{q^m}$ and proceed as in **Case 2.**

Theorem 2.13 is proved. □

Proof of Theorem 2.14. If f_w is almost noncomposite, then, according to Remarks 3.2 and 3.3, the word is equidustributed.

If f_w is very composite, then for some p it is p-composite but not p-special and, by Theorem 2.13, it is not p-equidistributed. Hence it is not equidistributed. □

Proof of Proposition 2.15. We can assume that q is odd. Consider the commutative diagram

$$\begin{tikzcd} G_q \times G_q \arrow[r, "w_1"] \arrow[d, "\rho'"] \arrow[dr, "\varkappa"] & G_q \arrow[d, "\rho"] \\ \hat{G}_q \times \hat{G}_q \arrow[r, "w_2"] & \hat{G}_q \end{tikzcd}$$

where ρ and ρ' are natural projections, and w_1 and w_2 correspond to the map $(x, y) \to w(x, y)$ on $G_q \times G_q$ and on $\hat{G}_q \times \hat{G}_q$, respectively.

Suppose w is p-equidistributed with respect to $\{G_q\}$ so that for $q > q_0$ we have inequalities (1) with parameters A, B, α, β. Define $\hat{S}_q := \rho(S_q)$, $\hat{T}_q := \hat{G}_q \setminus \hat{S}_q$.

For any element $\hat{g} \in \hat{G}_q$ the set $\rho^{-1}(\hat{g})$ contains precisely two elements g_1, g_2 of G_q. Therefore,

- $\#\hat{S}_q = \#S_q/2 = \#G_q\varepsilon_p(q)/2 = \#\hat{G}_q\varepsilon_p(q)$;
- $W_{\hat{g},\hat{G}_q} = \rho'(W_{g_1,G_q} \cup W_{g_2,G_q})$;
- $\#W_{\hat{g},\hat{G}_q} = (\#W_{g_1,G_q} + \#W_{g_2,G_q})/4$;
- for every $\hat{g} \in \hat{T}_q$ we have

$$\#W_{\hat{g},\hat{G}_q} = (\#W_{g_1,G_q} + \#W_{g_2,G_q})/4 = \#G_q(1+\varepsilon_p(q))/2 = \#\hat{G}_q(1+\varepsilon_p(q)).$$

Hence, w is p-equidistributed on $\{\hat{G}\}_q$ with the same parameters as on $\{G_q\}$. □

Remark 3.4. In [GS] there is a discussion on relationship between two close properties of word maps on finite groups: be equidistributed and preserve the uniform measure. In our context, the proof of Theorem 2.14 allows us to formulate this relationship explicitly.

Corollary 3.5. *Assume that a word w has an almost noncomposite trace polynomial f_w of degree d. Let $q > 4(50d^4)^2$, and let $\varepsilon(d, q) = 3(100d^4 + 1)q^{-1/2}$. Let $G = \mathrm{SL}(2, q)$ or $G = \mathrm{PSL}(2, q)$. Then the word map $w\colon G \times G \to G$ is $\varepsilon(d, q)$-measure-preserving in the sense of* [GS].

Proof. According to (6), the word map w is $\varepsilon(d, q)/3$-equidistributed, in the sense of Definition 2.1, and hence $\varepsilon(d, q)$-measure-preserving, by [GS, Proposition 3.2]. □

4. Composite trace polynomials

Our goal in this section is to describe words in two variables whose trace polynomial is composite.

Throughout this section $T_n(x)$ stands for the n^{th} Chebyshev polynomial, and $D_n(x) = 2T_n(x/2)$ for the n^{th} Dickson polynomial. It is well known (see, e.g., [LMT, (2.2)]) that this polynomial satisfies $D_n(x + 1/x) = x^n + 1/x^n$ and is completely determined by this functional equation.

We always assume that $w(x,y)$ is written in the form

$$w = x^{a_1}y^{b_1}\dots x^{a_r}y^{b_r} \tag{7}$$

and is reduced (all integers a_i, b_j are nonzero). We call the number r *complexity* of w.

Definition 4.1. We say that two reduced words $w = x^{a_1}y^{b_1}\dots x^{a_r}y^{b_r}$ and $v = x^{c_1}y^{d_1}\dots x^{c_{r'}}y^{d_{r'}}$, written in form (7), are *trace-similar* if $r = r'$, the array $\{|a_i|\}$ is a rearrangement of $\{|c_i|\}$, and the array $\{|b_i|\}$ is a rearrangement of $\{|d_i|\}$.

We start with a list of facts we are going to use:

(i) Any two decompositions of a polynomial $f(x)$ in one variable into noncomposite polynomials

$$f = \varphi_1 \circ \varphi_2 \circ \dots \circ \varphi_r = \psi_1 \circ \psi_2 \circ \dots \circ \psi_{r'}$$

contain the same number of polynomials: $r = r'$; the degrees of polynomials in one decomposition are the same as those in the other, except, perhaps, for the order in which they occur [Ri].

(ii) Let $n = p_1p_2\dots p_k$ be a prime decomposition of n. Then we have $T_n = T_{p_1} \circ \dots \circ T_{p_k}$ with any order of $p_1, p_2, \dots, p_k$, and this is the only decomposition of T_n up to composition with linear polynomials [Ri].

(iii) Assume that two reduced words $w = x^{a_1}y^{b_1}\dots x^{a_r}y^{b_r}$ and $v = x^{c_1}y^{d_1}\dots x^{c_{r'}}y^{d_{r'}}$, written in form (7), have the same trace polynomial $f_w(s,u,t) = f_v(s,u,t)$. Then w and v are trace-similar [Ho].

Example 4.2. The words $w = xy$ and $v = xy^{-1}$ are trace-similar but have different trace polynomials: $\operatorname{tr}(w) = u$, $\operatorname{tr}(v) = st - u$.

The words $x^2y^{-1}xy$ and x^2yxy^{-1} are trace-similar, have the same trace polynomial but are not conjugate in F_2 [Ho].

Further on we will work over the field $\mathbb{C}$.

Proposition 4.3. *Let $w(x,y) = x^{a_1}y^{b_1}\dots x^{a_r}y^{b_r}$, $A = \sum a_i$, $B = \sum b_i$. Assume that either $A \neq 0$ or $B \neq 0$. Assume that the trace polynomial $f_w(s,u,t)$ is $\mathbb{C}$-composite, $f_w(s,u,t) = h(q(s,u,t))$, where $q \in \mathbb{C}[s,u,t]$ and $h \in \mathbb{C}[z]$, $\deg h \leq 2$. Then $h = D_d(z)$ for some $d \geq 2$.*

Proof. Taking $y = \mathrm{id}$, $x = \mathrm{id}$, $x = y^{-1}$, and $x = y$, we get, respectively (taking into account that $\operatorname{tr}(g^{-1}) = \operatorname{tr}(g)$):

$$\begin{aligned} f_w(s,s,2) &= h(q(s,s,2)) = D_{|A|}(s), \\ f_w(2,t,t) &= h(q(2,t,t)) = D_{|B|}(t), \\ f_w(s,2,s) &= h(q(s,2,s)) = D_{|A-B|}(s), \\ f_w(s,s^2-2,s) &= h(q(s,s^2-2,s)) = D_{|A+B|}(s). \end{aligned}$$

These decompositions, together with property (ii) and the condition $\deg h \geq 2$, imply that there is a common divisor $d \geq 2$ of all the nonzero numbers from the list A, B, $A-B$, $A+B$ such that $h(z) = D_d(z)$. □

Proposition 4.4. *Let w be a reduced word of complexity r written in form (7). If its trace polynomial f_w is $\mathbb{C}$-composite, $f_w(s,u,t) = h(q(s,u,t))$ where $q \in \mathbb{C}[s,u,t]$ and $h(x) = \mu x^n + \dots$ is a polynomial in one variable of degree n, then $r = nm$ and w is trace-similar to $v(x,y)^n$ where v is a word of complexity m.*

Proof. First note that the trace polynomial of $w_i(x,y) = x^{a_i}y^{b_i}$ is linear in u: $f_{w_i}(s,u,t) = ug_{a_i,b_i}(s,t) + h_{a_i,b_i}(s,t)$, see [BG]. Moreover,

$$P_w(s,u,t) = \sum_{k=0}^{r} u^k G_k(s,t) \text{ and } G_r(s,t) = \prod_{k=1}^{r} g_{a_i,b_i}(s,t). \tag{8}$$

All polynomials belong to $\mathbb{Z}[s,u,t]$.

We need the following lemma.

Lemma 4.5. *Let $w'(x,y) = x^a y^b$ so that $f_{w'}(x,y) = ug_{a,b}(s,t) + h_{a,b}(s,t)$. Then*

$$g_{a,b}(s,s) = \frac{D_{|a+b|}(s) - D_{|a-b|}(s)}{s^2-4}, \tag{9}$$

$$h_{a,b}(s,s) = \frac{(s^2-2)D_{|a-b|}(s) - 2D_{|a+b|}(s)}{s^2-4}. \tag{10}$$

Proof of Lemma 4.5. We have

$$\operatorname{tr} x^a x^{-b} = 2g_{a,b}(s,s) + h_{a,b}(s,s) = D_{|a-b|}(s), \tag{11}$$

$$\operatorname{tr} x^a x^b = (s^2-2)g_{a,b}(s,s) + h_{a,b}(s,s) = D_{|a+b|}(s) \tag{12}$$

Computing $g_{a,b}(s,s)$, $h_{a,b}(s,s)$ from (11) and (12), we obtain (9) and (10). □

We now continue the proof of the proposition.

According to (9), we have

$$g_{a,b}(s,s) = \frac{(\cos((a+b)\varphi) - (\cos((a-b)\varphi)}{2(\cos^2(\varphi)-1)} = -\frac{\sin(a\varphi)\sin(b\varphi)}{\sin^2(\varphi)}$$

where $2\cos(\varphi) = s$.

Let $q(s,u,t) = \sum\limits_{k=0}^{m} u^k H_k(s,t)$. Then

$$f_w(s,u,t) = h(q(s,u,t)) = \mu u^{mn} H_m^n(s,t) + \Phi(u,s,t)$$

where $\deg_u \Phi(u,s,t) < mn$. Hence $r = nm$ and $\mu H_m^n(s,t) = G_r(s,t) = \prod\limits_{i=1}^{r} g_{a_i,b_i}(s,t)$ (cf.(8)).

Therefore,

$$\mu H_m^n(s,s) = (-1)^r \frac{\prod_{i=1}^{r} \sin(a_i\varphi)\sin(b_i\varphi)}{(\sin^2(\varphi))^r}.$$

We may assume that $|a_1| = \max\{|a_i|\}$. Choose $N > \max\{|b_i|\}$ and consider the word $w_N(x,y) = w(x^N, y)$. Then

$$f_{w_N}(s,t) = f_w(D_N(s), \alpha(s,u,t), t) = h(q(D_N(s), \alpha(s,u,t), t))$$

where $\alpha(s,u,t) = \operatorname{tr}(x^N y) = ug_{N,1}(s,t) + h_{N,1}(s,t)$. Thus

$$q(D_N(s), \alpha(s,u,t), t) =: q_1(s,u,t) = \sum_{k=0}^{m} u^k F_k(s,t)$$

and

$$f_{w_N}(s,u,t) = h(q_1(s,u,t)) = \mu u^{mn} F_m^n(s,t) + \Phi_1(u,s,t),$$

where $\deg_u \Phi_1(u,s,t) < mn$. Hence, since the words w and w_N have the same complexity r, we have

$$F_m^n(s,s) = (-1)^r \frac{\prod_{i=1}^{r} \sin(Na_i\varphi)\sin(b_i\varphi)}{(\sin^2(\varphi))^r}. \tag{13}$$

At the point $\varphi = \frac{\pi}{Na_1}$, the order of zero of the product is equal to the number $\lambda(a_1)$ of appearances of $|a_1|$ in the list $|a_1|, \dots, |a_r|$. Thus $\lambda(a_1) = nm_1$ where m_1 is the order of the zero of $F_m(s,s)$ at the point $s = 2\cos(\pi/(Na_1))$.

We may now divide (13) by $(\sin(Na_1\varphi))^{nm_1}$ and repeat the same argument for $|a_i| = \max\{|a_j| : |a_j| \neq |a_1|\}$.

Repeating this procedure, we conclude that there are $a_1, \dots, a_\nu$ such that the list $|a_1|, \dots, |a_r|$ contains nm_1 times $|a_1|, \dots,$ nm_ν times $|a_\nu|$, and nothing else. Note that $\sum_{k=1}^{\nu} nm_k = r = nm$, since altogether we have r elements in the list.

In a similar way, looking at the word $w(x, y^M)$ for M big enough, we conclude that there are $b_1, \dots, b_\mu$ such that the list $|b_1|, \dots, |b_r|$ contains np_1 times $|b_1|, \dots,$ np_μ times $|b_\mu|$, and nothing else. Note that $\sum_{k=1}^{\mu} np_k = r = nm$.

Since $\sum_{k=1}^{\nu} m_k = \sum_{k=1}^{\mu} p_k = m$, we may define a word

$$v(x,y) = x^{\tau_1} y^{\varkappa_1} \dots x^{\tau_m} y^{\varkappa_m}$$

of complexity m in such a way that among $|\tau_i|$ there will be m_i of $|a_i|$, $1 \leq i \leq \nu$, and among $|\varkappa_i|$ there will be p_i of $|b_i|$, $1 \leq i \leq \mu$.

By construction, $v^n(x,y)$ is trace-similar to $w(x,y)$ which completes the proof of the proposition. □

Proposition 4.6. *Let $w(x,y) = x^a y^b \dots$ be a reduced word of complexity n such that $f_w(s,u,t) = D_n(q(s,u,t))$ for some q. Then $w(x,y) = (x^a y^b)^n$.*

Proof. According to Proposition 4.4, every such w is the product of syllables $x^{\pm a} y^{\pm b}$.

Assume that by cyclic permutation and exchanging roles of x and y one can modify w to a word $v = v_1 \dots v_n$, $v_k = x^{\pm a} y^{\pm b}$, $k = 1, \dots, n$, containing repeated syllables, i.e., such that for some $i < j$ we have $v_i = v_j$. Then we consider the word

$$\tilde{v} = v_i \dots v_j \dots v_n v_1 \dots v_{i-1}.$$

The word $\tilde{v}$ will be called a *convenient* form of w. Note that either $f_w(s,u,t) = f_{\tilde{v}}(s,u,t)$ or $f_w(s,u,t) = f_{\tilde{v}}(t,u,s)$. If this procedure is impossible, we say that w is already in a convenient form. First consider the case where $a = b = 1$.

Lemma 4.7. *Let $w(x,y) = xy \dots x^{\pm 1} y^{\pm 1} = w_1 \dots w_n$ be a word in a convenient form, where w_i are syllables of the form $x^{\pm 1} y^{\pm 1}$.*

Let $u = \operatorname{tr}(xy), s = \operatorname{tr}(x), t = \operatorname{tr}(y)$. Then

$$f_w(s,u,t) = \epsilon u^n - \epsilon mstu^{n-1} + \dots + g(s,t)$$

is a polynomial of degree n in u such that

- *the coefficient at u^n is $\epsilon = \pm 1$;*
- *m is a non-negative integer, and $m = 0$ if and only if $w = (xy)^n$;*
- *the coefficient at u^{n-1} is ϵmst;*
- *the coefficient $f_w(s,0,t)$ at u^0 is a polynomial g in s,t of degree strictly less than $2n$.*

It is important here that we defined u as the trace of the first syllable.

Proof of Lemma 4.7. First consider the case when there are no repeated syllables.

n=1: $\operatorname{tr}(xy) = u$.

n=2: • $\operatorname{tr}(xyxy^{-1}) = -u^2 + ust - t^2 + 2$,

- $\operatorname{tr}(xyx^{-1}y^{-1}) = u^2 - ust + t^2 + s^2 - 2$,
- $\operatorname{tr}(xyx^{-1}y) = \operatorname{tr}(yxyx^{-1}) = -u^2 + ust - s^2 + 2$.

n=3: • the words $a_1 = x\mathbf{y}\mathbf{x}^{\mathbf{-1}}\mathbf{y}\mathbf{x}^{\mathbf{-1}}y^{-1}$, $a_2 = \mathbf{xyx}y^{-1}x^{-1}\mathbf{y}$ and $a_3 = \mathbf{x}yx^{-1}\mathbf{y}^{\mathbf{-1}}\mathbf{x}\mathbf{y}^{\mathbf{-1}}$ are not in a convenient form;

- for $a_4 = xyxy^{-1}x^{-1}y^{-1}$, we have

$$\begin{aligned}\operatorname{tr}(a_4) = f_{a_4}(s,u,t) &= (ust - u^2 - t^2 + 2)u - \operatorname{tr}(x^3 y) \\ &= (ust - u^2 - t^2 + 2)u - u(s^2 - 2) + (st - u) \\ &= -u^3 + stu^2 + u(3 - t^2 - s^2) + st;\end{aligned}$$

- the word $a_5 = xyx^{-1}y^{-1}x^{-1}y$ may be modified to a_4 by cyclic permutation and exchanging roles of x and y, thus $\operatorname{tr}(a_5) = \operatorname{tr}(a_4)$;

- $a_6 = xyx^{-1}yxy^{-1}$ may be modified to a_4 by cyclic permutation and changing roles of y and y^{-1}, thus

$$\operatorname{tr}(a_6) = P_{a_4}(s, st-u, t) = u^3 - u^2st + u(s^2t^2 + t^2 + s^2 - 3) + st(4 - t^2 - s^2).$$

n=4:
- $b_1 = \mathbf{xyx}y^{-1}x^{-1}y^{-1}x^{-1}\mathbf{y}$ and $b_2 = x\mathbf{yx^{-1}yx^{-1}}y^{-1}xy^{-1}$ are not in a convenient form;
- for $b_3 = xyxy^{-1}x^{-1}yx^{-1}y^{-1}$ we have

$$\begin{aligned}\operatorname{tr}(b_3) = f_{b_3}(s,u,t) &= (ust - u^2 - t^2 + 2)^2 - \operatorname{tr}(x^2yx^2y^{-1})\\ &= (ust - u^2 - t^2 + 2)^2 - [(us - t)(s^2 - 2)t - (us - t)^2 - t^2 + 2]\\ &= u^4 - 2u^3st + u^2h_1 + uh_2 + (t^2 - 2)^2 + t^2(s^2 - 2) + 2t^2 - 2,\end{aligned}$$

where h_1, h_2 are polynomials in s, t;
- $b_4 = xyx^{-1}yxy^{-1}x^{-1}y^{-1}$ may be modified to b_3 by cyclic permutation, and substituting x by y^{-1} and y by x^{-1};
- $b_5 = xyx^{-1}y^{-1}xy^{-1}x^{-1}y$ may be modified to b_3 by cyclic permutation, and substituting x by y and y by x;
- $b_6 = xyx^{-1}y^{-1}x^{-1}yxy^{-1}$ may be modified to b_3 by cyclic permutation, and substituting x by x^{-1} and y by y^{-1}.

Note that these substitutions do not change u, and the coefficient m is not zero in convenient words.

Any word of complexity ≥ 5 must have repeated syllables. The case with repeated syllables will be proved by induction on the complexity n. Assume that for all words in a convenient form of complexity $k \leq n$ the statement of the lemma is valid.

Consider $w(x,y) = w_1 \dots w_n$ where $w_1 = xy$, $w_i = x^{\pm 1}y^{\pm 1}, i = 2, \dots, n$, $w_{j+1} = w_1$, $0 < j \leq n-1$. Thus $w = v_1v_2$ where $v_1 = w_1 \dots w_j$, $v_2 = w_{j+1} \dots w_n$. Denote $v_3 = v_1v_2^{-1}$, it is of complexity $n-2$ since its first syllable is xy and the last is $(xy)^{-1}$. By induction hypothesis,

$$\begin{aligned}&\operatorname{tr}(v_1) = \epsilon_1 u^j - \epsilon_1 m_1 stu^{j-1} + \cdots + g_1, \deg g_1 < 2j;\\ &\operatorname{tr}(v_2) = \epsilon_2 u^{n-j} - \epsilon_2 m_2 stu^{n-j-1} + \cdots + g_2, \deg g_2 < 2(n-j).\end{aligned}$$

The word v_3 may not be in a convenient form. This means that $u = \operatorname{tr}(xy)$ may not be the trace of the first syllable of v_3. Anyway,

$$\operatorname{tr}(v_3) = \epsilon_3 \hat{u}^{n-2} - \epsilon_3 m_3 st\hat{u}^{n-3} + \cdots + g_3, \deg g_3 < 2(n-2),$$

where $\hat{u}$ is either u or $st - u$. In both cases its degree in u is at most $n-2$ and the coefficient at u^0 is of degree at most $2(n-2)$. Therefore

$$\begin{aligned}\operatorname{tr}(w) &= \operatorname{tr}(v_1)\operatorname{tr}(v_2) - \operatorname{tr}(v_3)\\ &= \epsilon_1\epsilon_2 u^n - \epsilon_1\epsilon_2 st(m_1 + m_2)u^{n-1} + \cdots + g_1g_2 - g_3.\end{aligned}$$

Here the degree of the polynomial $g_1g_2 - g_3$, which is the coefficient at u^0, is less than $2j + 2(n-j) = 2n$. Moreover, $m_1 + m_2$ may be zero only if $m_1 = m_2 = 0$, which means, by induction hypotheses, that $v_1 = w_1^j$, $v_2 = w_1^{n-j}$, so $w = w_1^n$. □

We continue the proof of Proposition 4.6: assume that $w(x,y) = w_1 \dots w_n$, where $w_1 = x^a y^b$, $w_i = x^{\pm a} y^{\pm b}$, is written in a convenient form, and $f_w(s,u,t) = D_n(q(s,u,t))$. We denote $z = x^a, v = y^b$, i.e., $w(x,y) = \tilde{w}(z,v)$, and $\tilde{w}$ is a word of the type considered in Lemma 4.7. Let $\tilde{s} = D_{|a|}(s)$, $\tilde{t} = D_{|b|}(t)$, and $\tilde{u} = \operatorname{tr}(x^a y^b) = u g_{a,b}(s,t) + h_{a,b}(s,t)$, where $g_{a,b}, h_{a,b}$ are polynomials in s,t and $g_{a,b} \not\equiv 0$ (see [BG]). Since q is of degree 1 in u, we have $q = \alpha(s,t)\tilde{u} + \beta(s,t)$, with rational coefficients α and β. According to Lemma 4.7, we have

$$\begin{aligned} f_w(s,u,t) &= \epsilon \tilde{u}^n - \epsilon m \tilde{s}\tilde{t}\tilde{u}^{n-1} + \dots + g(\tilde{s},\tilde{t}) = q^n - nq^{n-2} + \dots \\ &= (\alpha(s,t)\tilde{u} + \beta(s,t))^n - n(\alpha(s,t)\tilde{u} + \beta(s,t))^{n-2} + \dots \end{aligned} \tag{14}$$

It follows that

$$\alpha(s,t) = \alpha = \text{const}, \;\; \alpha^n = \epsilon, \;\text{ and } \beta(s,t) = -\frac{\epsilon m \tilde{s}\tilde{t}}{n\alpha^{n-1}} = -\frac{m\alpha\tilde{s}\tilde{t}}{n}.$$

Substituting $q = \alpha\tilde{u} - m\alpha\tilde{s}\tilde{t}/n$ into (14), we get:

$$\begin{aligned} f_w(s,u,t) &= \epsilon \tilde{u}^n - \epsilon m \tilde{s}\tilde{t}\tilde{u}^{n-1} + \dots + g(\tilde{s},\tilde{t}) \\ &= \left(\alpha\tilde{u} - m\alpha\tilde{s}\tilde{t}/n\right)^n - n\left(\alpha\tilde{u} - m\alpha\tilde{s}\tilde{t}/n\right)^{n-2} + \dots \end{aligned}$$

Thus, the coefficient at $(\tilde{u})^0$ is a polynomial in $\tilde{s}\tilde{t}$ of degree n, hence it is a polynomial in $\tilde{s},\tilde{t}$ of degree $2n$, which implies, by Lemma 4.7, that $\beta \equiv 0$ and $\tilde{w} = (zv)^n$. □

Remark 4.8. The statements of Propositions 4.3, 4.4 and 4.6 remain valid if we replace $\mathbb{C}$ by (the algebraic closure of) a sufficiently big prime field $\mathbb{F}_p$, and "composite" by "p-composite" ($p > p_0$ depending on w).

5. Generic words

In this section, we address the following question: picking up a "generic" word w, should we expect that it is equidistributed? There is a large body of literature dedicated to the notion of genericity, and there are several different approaches to this notion. We mostly follow the setting adopted in [KS].

Definition 5.1 (cf. [KS])**.** Denote by $\mathcal{R}$ some set of reduced words $w \in F_2$ written in form (7). For a word of complexity r, let $\ell(w) = \sum_{i=1}^r (|a_i| + |b_i|)$ denote the length of w. Let $S \subseteq \mathcal{R}$. Set

$$\rho(n,S) = \#\{w \in S : \ell(w) \le n\},$$

$$\mu(n,S) = \frac{\rho(n,S)}{\rho(n,\mathcal{R})}.$$

We say that S is

- *generic* if

$$\lim_{n\to\infty} \mu(n,S) = 1,$$

- *exponentially generic* if it is generic and the convergence is exponentially fast,
- *negligible* if this limit equals 0,
- *exponentially negligible* if it is negligible and the convergence is exponentially fast.

Evidently, S is (exponentially) generic if and only if the complement $\mathcal{R} \setminus S$ is (exponentially) negligible.

Recall that the abelianization homomorphism $F_d \to \mathbb{Z}^d$ is defined by taking a fixed basis of F_d to a fixed basis of $\mathbb{Z}^d$. Denote by C_d the kernel of this homomorphism. Define $\mathcal{R} := \{w : w \notin C_2\}$. The class $\mathcal{R}$ includes many natural classes of words (say, positive words, words of odd length, etc.). Further, define $\mathcal{R}'$ as the set of words in $\mathcal{R}$ of *prime* complexity.

Proposition 5.2. *The set of words $w \in \mathcal{R}'$, such that the corresponding word morphism $w\colon \mathrm{SL}_{2,\mathbb{Z}} \times \mathrm{SL}_{2,\mathbb{Z}} \to \mathrm{SL}_{2,\mathbb{Z}}$ is p-equidistributed for all but finitely many primes p, is exponentially generic in $\mathcal{R}$.*

Proof. Let $w \in \mathcal{R}'$. As $w \in \mathcal{R}$, it satisfies the hypotheses of Proposition 4.3. Suppose that w does *not* satisfy the assumption of our proposition, i.e., there exist infinitely many primes p such that the trace morphism $f_{w,p}$ is *not* p-equidistributed. Then by Propositions 4.3 and 4.6, taking into account Remark 4.8, we conclude that $w = (x^a y^b)^r$. It remains to refer to [AO] where it is proven that the property of a word to be a proper power of another word is exponentially negligible. Hence the set of words satisfying the hypotheses of the proposition is exponentially generic in $\mathcal{R}'$. □

Remark 5.3. We believe that with some more effort, one can significantly strengthen Proposition 5.2 by dropping the primality restriction on r, and maybe even by extending $\mathcal{R}$ to the class of all reduced words. We leave this to experts in word combinatorics.

6. Concluding remarks

It is tempting to generalize our results in the following directions:

(i) extend them from words in two letters to words in d letters, $d > 2$;
(ii) keep $d = 2$ but consider arbitrary finite Chevalley groups;
(iii) combine (i) and (ii).

Whereas in case (i) one can still hope to use trace polynomials, which exist for any d, to produce criteria for equidistribution, cases (ii) and (iii) require some new terms for formulating such criteria and new tools for proving them.

One can try yet another direction: consider equidistribution problems for matrix *algebras* and for polynomials more general than word polynomials (see Introduction). Even the case of 2×2-matrices is completely open.

Acknowledgements. We thank S. Garion, I. Kapovich, M. Larsen, and A. Shalev for useful discussions.

References

[AP] I. V. Arzhantsev, A. P. Petravchuk, *Closed polynomials and saturated subalgebras of polynomial algebras*, Ukrain. Mat. Zh. **59** (2007) 1587–1593 = Ukrainian Math. J. **59** (2007) 1783–1790.

[AO] G. N. Arzhantseva, A. Yu. Ol'shanskii, *The class of groups all of whose subgroups with lesser number of generators are free is generic*, Mat. Zametki **59** (1996) 489–496; English transl.: Math. Notes **59** (1996) 350–355.

[BG] T. Bandman, S. Garion, *Surjectivity and equidistribution of the word $x^a y^b$ on $PSL(2,q)$ and $SL(2,q)$*, `arXiv:1106.1619`, to appear in Intern. J. Algebra Computation.

[BGG] T. Bandman, S. Garion, F. Grunewald, *On the surjectivity of Engel words on $PSL(2,q)$*, `arXiv:1008.1397`, to appear in Groups, Geometry, and Dynamics.

[BGKP] T. Bandman, N. Gordeev, B. Kunyavskiĭ, E. Plotkin, *Equations in simple Lie algebras*, `arXiv:1012.4106`, submitted.

[BGK] T. Bandman, F. Grunewald, B. Kunyavskiĭ (with an appendix by N. Jones), *Geometry and arithmetic of verbal dynamical systems on simple groups*, Groups, Geometry, and Dynamics **4** (2010) 607–655.

[BDN] A. Bodin, P. Dèbes, S. Najib, *Indecomposable polynomials and their spectrum*, Acta Arith. **139** (2009) 79–100.

[Bo] A. Borel, *On free subgroups of semisimple groups*, Enseign. Math. **29** (1983) 151–164; reproduced in Œuvres - Collected Papers, vol. IV, Springer-Verlag, Berlin–Heidelberg, 2001, pp. 41–54.

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

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

[Ho] R. D. Horowitz, *Characters of free groups represented in the two-dimensional special linear group*, Comm. Pure Appl. Math. **25** (1972) 635–649.

[KBMR] A. Kanel-Belov, S. Malev, L. Rowen, *The images of non-commutative polynomials evaluated on 2×2 matrices*, `arXiv:1005.0191`, to appear in Proc. Amer. Math. Soc.

[KS] I. Kapovich, P. Schupp, *Random quotients of the modular group are rigid and essentially incompressible*, J. reine angew. Math. **628** (2009) 91–119.

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

[LP] M. Larsen, R. Pink, *Finite subgroups of algebraic groups*, J. Amer. Math. Soc. **24** (2011) 1105–1158.

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

[LST] M. Larsen, A. Shalev, P. H. Tiep, *Waring problem for finite simple groups*, Ann. Math. **174** (2011) 1885–1950.

[LMT] R. Lidl, G. L. Mullen, G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure Appl. Math., vol. 65, Longman Scientific &

Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993.

[LN] R. Lidl, H. Niederreiter, *Finite Fields*, Encycl. Math. Appl., vol. 20, Addison-Wesley Publ. Company, Ma., 1983.

[MS] A. G. Myasnikov, V. Shpilrain, *Automorphic orbits in free groups*, J. Algebra **269** (2003) 18–27.

[Na] S. Najib, *Une généralisation de l'inégalité de Stein–Lorenzini*, J. Algebra **292** (2005) 566–573.

[Pu] D. Puder, *Primitive words, free factors and measure preservation*, `arXiv:1104.3991`.

[Ri] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922) 51–66.

[Sh1] A. Shalev, *Commutators, words, conjugacy classes and character methods*, Turkish J. Math. **31** (2007) 131–148.

[Sh2] A. Shalev, *Word maps, conjugacy classes, and a non-commutative Waring-type theorem*, Ann. Math. **170** (2009) 1383–1416.

[Wa] D. Wan, *A p-adic lifting and its application to permutation polynomials*, in: "Finite Fields, Coding Theory and Advances in Communications and Computing" (G. L. Mullen, P. J.–S. Shiue, eds.), Lecture Notes Pure Appl. Math., vol. 141, Marcel Dekker, New York, 1993, pp. 209–216.

[WSC] D. Wan, P. J.-S. Shiue, C. Chen, *Value sets of polynomials over finite fields*, Proc. Amer. Math. Soc. **119** (1993) 711–717.

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

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

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

E-mail address: `kunyav@macs.biu.ac.il`