ON THE DISTRIBUTION OF VALUES
OF CERTAIN WORD MAPS

MICHAEL LARSEN AND ANER SHALEV

Abstract. We prove that, for any positive integers \( m, n \), the word map \((x, y) \mapsto x^m y^n\) is almost measure preserving on finite simple groups. This extends the case \( m = n = 2 \) obtained in 2009. Along the way we obtain results of independent interest on fibers of word maps and on character values.

1. Introduction

Let \( F_d \) be the free group of rank \( d \), and let \( w \in F_d \) be a word. Let \( G \) be a finite group. Then \( w \) induces a word map \( w_G : G^d \to G \), induced by substitution, which we sometimes denote by \( w \). Word maps have been studied extensively in recent years. See for instance [LiS1], [Sh2], [LaS1], [LOST], [SS], [LaS2], [LaST], and the monograph [Se] by Segal.

The word map \( w_G \) induces a probability distribution \( P = P_{w,G} \) on \( G \), where for a subset \( X \subseteq G \) we have \( P(X) = |w_G^{-1}(X)|/|G|^d \). Let \( \mu = \mu_G \) be the uniform distribution on \( G \). We shall be interested in finding out how close \( P \) is to the uniform distribution, in other words, how large the \( L^1 \) distance \( \|P - \mu\|_1 \) can be.

If \( w \) is a primitive word, i.e., part of a free basis for \( F_d \), then \( P_{w,G} \) is clearly uniform for every finite group \( G \). Puder and Parzanchevski proved in [PP] that the converse holds too. In fact if \( P_{w,G} \) is uniform for infinitely many symmetric groups \( G = S_n \), then \( w \) is primitive.

In this paper we are interested in cases where \( P_{w,G} \) is almost uniform as \( G \) ranges over the family of finite (nonabelian) simple groups. This means that \( \|P_{w,G} - \mu_G\|_1 \to 0 \) as \( G \) ranges over finite simple groups and \( |G| \to \infty \).

The first result of this kind appears in [GS], where it is shown that the commutator map is almost uniform on finite simple groups. In the same paper, it is also shown that the word map \( x_1^2 x_2 x_1^2 \) is almost uniform on finite simple groups. Our main theorem generalizes this latter result as follows.

Theorem 1.1. Let \( m_1, m_2 \) be positive integers and let \( w = x_1^{m_1} x_2^{m_2} \). Then \( w \) is almost uniform on finite simple groups.

A particular case of this result, for \( G = \text{PSL}_2(q) \), was obtained by Bandman and Garion in [BG]. Theorem 1.18 in [LaS1] for the case of alternating groups \( G = A_n \) follows from Theorem 1.1 in [LaS1]. Hence it remains to deal with simple groups of Lie type.

Received by the editors August 6, 2013 and, in revised form, December 26, 2013.

2010 Mathematics Subject Classification. Primary 20P05, 20D06.

The first author was partially supported by NSF Grant DMS-1101424. The second author was partially supported by ERC Advanced Grant 247034 and the Vinik Chair in Mathematics. Both authors were partially supported by Binational Science Foundation United States-Israel Grant 2008194.

©2015 American Mathematical Society
Let us now outline the way Theorem 1.1 is proved.

In a large simple group $G$, there are many pairs of conjugacy classes $C_1, C_2$ such that choosing independent uniform random elements $y_1 \in C_1$ and $y_2 \in C_2$, the resulting probability distribution of $y_1y_2$ on $G$ is close to uniform. Indeed, this is shown in [Sh1]. The basic method to prove that a particular pair of conjugacy classes satisfies this property is to get good upper bounds on the size of irreducible character values at $C_1$ and $C_2$. One can prove that, for any given $\epsilon > 0$, most elements $g \in G$ satisfy the property that $|\chi(g)| \leq \chi(1)^\epsilon$ (see Proposition 4.2 below). Setting $y_1 = x_1^{m_1}, y_2 = x_2^{m_2}$, one then needs to prove that the inverse images by power maps of the set of “bad” elements of $G$ is also small. The difficulty is that the sizes of fibers of the $m$th power map vary enormously. The technical heart of this paper is devoted to the problem of controlling the size of “typical” fibers for groups of Lie type of high rank. Once this is achieved we prove Theorem 1.1 using character methods.

In the final section of the paper, we show that another family of words is almost uniform on finite simple groups. A word $w \in F_d$ is called admissible if every variable $x_i$ which occurs in $w$ occurs once with exponent 1 and once with exponent $-1$. For example, the commutator word is admissible, as well as many other words, such as $x_1 \cdots x_d x_1^{-1} \cdots x_d^{-1}$.

**Proposition 1.2.** Every admissible word $w \neq 1$ is almost uniform on finite simple groups.

This result was proved in 2010 and announced in the survey paper [Sh3] (see Theorem 4.6 there). It was also proved by Nath, subsequently and independently, in [N]. Our original proof of this result relied on [DN], but here we give a shorter proof based on the recent subsequent paper [PS] by Parzanchevski and Schul.

### 2. Random polynomials over finite fields

In this section, we show, roughly, that a random degree $n$ polynomial over $\mathbb{F}_q$ rarely has more than $O(\log n)$ factors over $\mathbb{F}_q[x]$. This is relevant because an element of $GL_n(\mathbb{F}_q)$ with many $m$th roots must have a highly factorable characteristic polynomial. Since we are not interested in $GL_n(\mathbb{F}_q)$ itself but in special linear, unitary, orthogonal, and symplectic groups, the precise statements must be modified accordingly.

We begin with a useful identity, which is essentially the Euler product formula for the zeta-function of $\mathbb{F}_q[x]$. Throughout the paper, we will denote by $P_n(x)$ the polynomial

$$\sum_{ij=n} \mu(i)x^j \mu(x),$$

where $\mu$ is the Möbius function.

**Lemma 2.1.** If $q$ is a prime power, then $P_n(q)$ is a positive integer for all $n \geq 1$, and we have a power series identity

$$\prod_{n=1}^\infty (1 - x^n)^{-P_n(q)} = \sum_{i=0}^\infty q^i x^i.$$

**Proof.** By a standard inclusion-exclusion argument, $P_n(q)$ is the number of irreducible monic polynomials of degree $n$ over $\mathbb{F}_q$ and is therefore a positive integer.
Moreover,
\[
\prod_{n=1}^{\infty} (1 - x^n)^{-\sum_{ij=n} \mu(i) q^j} = \exp \left( \sum_{n=1}^{\infty} \frac{\sum_{ij=n} \mu(i) q^j}{n} \sum_{k=1}^{\infty} x^{kn} \right)
\]
\[= \exp \left( \sum_{i,j,k} \frac{\mu(i) q^j x^{ijk}}{ijk} \right)
\]
\[= \exp \left( \sum_{j,m} \frac{q^j x^j}{jm} \sum_{ik=m} \mu(i) \right)
\]
\[= \exp \left( \sum_{j} \frac{q^j x^j}{j} \right)
\]
\[= (1 - qx)^{-1}.
\]

□

**Proposition 2.2.** Let \( a_1 \leq a_2 \) be positive and \( q \geq 2 \). Let \( e_1, e_2, \ldots \) denote an infinite sequence of integers such that

\[a_1 q^n / n \leq e_n \leq a_2 q^n / n\]

for all \( n \geq 1 \), and let \( d_0 = 1, d_1, \ldots \) be defined by

\[\sum_{n=0}^{\infty} d_n x^n := \prod_{n=1}^{\infty} (1 - x^n)^{-e_n}.
\]

Then there exist \( A_1 \) and \( A_2 \) depending only on \( a_1 \) and \( a_2 \), respectively, such that for all \( n \geq 0 \),

\[(n + 1)^{A_1} q^n \leq d_n \leq (n + 1)^{A_2} q^n.
\]

**Proof.** Lemma 2.1 gives the proposition immediately for one particular sequence, namely \( e_n := P_n(q) \). By the binomial theorem, it gives the theorem more generally for \( e_n := \lambda P_n(q) \) for any constant \( \lambda > 0 \). Regarding the \( d_i \) as functions in the \( e_j \), each \( d_i \) is nondecreasing in each \( e_j \) separately, so the proposition holds as long as \( a_1 P_n(q) \leq e_n \leq a_2 P_n(q) \) for all \( n \). As

\[\frac{\sum_{ij=n} \mu(i) q^j}{q^n}\]

is bounded away from 0 and \( \infty \) for all \( q \geq 2 \) and \( n \geq 1 \), the proposition holds. □

**Proposition 2.3.** Let \( e_n \) be a sequence satisfying \((\Pi)\) for some \( q, a_1 \), and \( a_2 \). Define \( c_{i,j} \) by

\[\sum_{i,j} c_{i,j} x^i y^j := \prod_{i=1}^{\infty} (1 - x^i y)^{-e_i}.
\]

There exist \( C \) and \( D > 1 \) depending only on \( a_1 \) and \( a_2 \) such that for all \( 0 \leq m \leq n \),

\[\frac{\sum_{j=m+1}^{n} c_{n,j}}{\sum_{j=0}^{n} c_{n,j}} \leq n^C D^{-m}.
\]
Proof. We have
\[(9/4)^n \sum_{j=m+1}^{n} c_{n,j} < \sum_{j=0}^{n} c_{n,j} (9/4)^j,\]
which is the \(x^n\) coefficient of
\[\prod_{i=1}^{\infty} (1 - (9/4)x^i)^{-e_i}.\]
This is less than or equal to the \(x^n\) coefficient of
\[(1 - (9/4)x)^{-e_1} \prod_{i=1}^{\infty} (1 - (3x/2)^i)^{-e_i} = (1 - (9/4)x)^{-e_1} \sum_{n=0}^{\infty} (3/2)^n d_n x^n.\]
By Proposition 2.2 there exists \(A_2 > 0\) such that
\[d_n \leq (n+1)^{A_2} q^n\]
so
\[\sum_{i=0}^{n} (9/4)^i \binom{i + e_1 - 1}{e_1 - 1} (3/2)^{n-i} d_{n-i} \leq (3/2)^n \binom{n + e_1 - 1}{e_1 - 1} (n+1)^{A_2} q^n \sum_{i=0}^{n} (3/2)^i = O(n^{A_2 + e_1 - 1} (3/2)^n q^n)\]
since \(q > 3/2\). Thus,
\[\sum_{j=m+1}^{n} c_{n,j} = O(n^{A_2} (2q/3)^n),\]
which, together with the lower bound \(n^{A_1} q^n\) for \(\sum_{j=0}^{n} c_{n,j}\) given by Proposition 2.2, implies the proposition. \(\Box\)

**Proposition 2.4.** Let \(\mathcal{L}_n(q)\) denote the set of monic polynomials \(P(x) \in \mathbb{F}_q[x]\) of degree \(n\) such that \(P(0) = (-1)^n\). For all \(k > 0\), there exists \(N\) such that if \(n \geq 2\) and \(q\) is a prime power, then the set of \(P(x) \in \mathcal{L}_n(q)\) such that \(P(x)\) splits into more than \(N\) irreducible factors has at most \(n^{k-1} |\mathcal{L}_n(q)|\) elements.

**Proof.** Let \(\mathcal{IL}_n(q)\) denote the set of reducible monic polynomials in \(\mathbb{F}_q[x]\), excluding \(x\). Thus \(\mathcal{IL}_n(q)\) can be identified with the set of \(n\)-element \(q\)-Frobenius orbits in \(\mathbb{F}_q^x\), which means
\[|\mathcal{IL}_n(q)| = \frac{\sum_{ij=n} \mu(i)(q^j - 1)}{n}.\]
Thus \(|\mathcal{IL}_n(q)| = P_n(q)\) except for \(n = 1\), and \(\mathcal{IL}_1(q) = q - 1\). The norm maps \(N_{\mathbb{F}_q^n/\mathbb{F}_q}: \mathbb{F}_q^x \to \mathbb{F}_q^x\) are surjective, so they combine to give morphisms \(N_n: \mathcal{IL}_n(q) \to \mathbb{F}_q^x = \text{GL}_1(\mathbb{F}_q)\) for which every fiber has the same cardinality, namely \(P_n(q)/(q-1)\), except when \(n = 1\), when the cardinality is 1.
If \( c_{n,m} \) denotes the number of elements in \( \mathcal{L}_n(q) \) with exactly \( m \) irreducible factors, then

\[
\sum_{m,n} c_{n,m} x^n y^m = \frac{1}{q-1} \sum_{\chi} \prod_{n=1}^{\infty} \prod_{P \in \mathcal{I} \mathcal{L}_n(q)} (1 - \chi(N_n(P)) x^n y)^{-1}
\]

\[
= \frac{1}{q-1} \sum_{\chi} \prod_{n=1}^{\infty} (1 - x^{n \text{ord}(\chi)} y^{\text{ord}(\chi)})^{-|\mathcal{I} \mathcal{L}_n(q)|/\text{ord}(\chi)},
\]

where the sum ranges over all characters \( \chi \) of \( \text{GL}_1(\mathbb{F}_q) \). (The second equality holds because the composition of \( \chi \) and \( N_n \) gives a map from \( \mathcal{I} \mathcal{L}_n(q) \) to the cyclic group \( \langle e^{2\pi i/\text{ord}(\chi)} \rangle \) whose fibers all have the same cardinality.) Let \( c_{n,m}(\chi) \) denote the \( x^n y^m \) coefficient of

\[
\prod_{n=1}^{\infty} (1 - x^{n \text{ord}(\chi)} y^{\text{ord}(\chi)})^{-|\mathcal{I} \mathcal{L}_n(q)|/\text{ord}(\chi)}.
\]

Note that \( c_{n,m}(\chi) \) is real and nonnegative for all \( m, n, \) and \( \chi \). Proposition 2.2 implies that for all \( \chi \) of order \( \geq 2 \),

\[
\sum_{m=0}^{\infty} c_{m,n}(\chi) = O((n+1)^{A_2 q^{n/2}})
\]

for some absolute constant \( A_2 \). Therefore, the number of elements of \( \mathcal{L}_n(q) \) with more than \( m \) prime factors is

\[
\frac{\sum_{i=m+1}^{n} c_{n,i}(1)}{q-1} + O((n+1)^{A_2 q^{n/2-1}}),
\]

while

\[
\sum_{i=0}^{n} c_{n,i}(1) = q^{n-1} + O((n+1)^{A_2 q^{n/2}}).
\]

By Proposition 2.3,

\[
\frac{\sum_{i=m+1}^{n} c_{n,i}(1)}{\sum_{i=0}^{n} c_{n,i}(1)} = n^C D^{-m} = n^{C - \frac{m \log D}{\log n}},
\]

where \( C \) and \( D > 1 \) are absolute constants. It follows that if

\[
m > \frac{C + k}{\log D} \log n,
\]

then

\[
\frac{\sum_{i=m+1}^{n} c_{n,i}}{\sum_{i=0}^{n} c_{n,i}} < n^{-k}.
\]

\( \square \)

**Proposition 2.5.** Let \( \mathcal{U}_n(q) \) denote the set of monic polynomials \( P(x) \in \mathbb{F}_q[x] \) such that

\[
P(x) = (-x)^n P(1/x),
\]

where \( P \) denotes the polynomial obtained from \( P \) by applying the \( q \)-Frobenius to each coefficient. For all \( k > 0 \), there exists \( N \) such that if \( n \geq 2 \) and \( q \) is a prime power, then the set of \( P(x) \in \mathcal{U}_n(q) \) such that \( P(x) \) splits into more than \( N \log n \) irreducible factors over \( \mathbb{F}_q[x] \) has at most \( n^{-k} |\mathcal{U}_n(q)| \) elements.
Proof. The elements of \( \mathcal{U}_n(q) \) are in bijective correspondence with \( n \)-element multisets in \( \mathbb{F}_q \) with product 1 which are stable under the map \( T_q : x \mapsto x^{-q} \). Let \( \mathcal{I} \mathcal{U}_n(q) \) denote the set of minimal \( n \)-element \( T_q \)-stable subsets of \( \mathbb{F}_q^\times \). When \( n \) is even, we can identify \( \mathcal{I} \mathcal{U}_n(q) \) with \( (n \text{-element}) \) \( T_q \)-orbits of elements \( \alpha \in \mathbb{F}_q^\times \) such that \( \mathbb{F}_q(\alpha) = \mathbb{F}_{q^n} \). When \( n \) is odd, we can identify it with \( T_q \)-orbits of elements \( \alpha \in \ker \mathbb{F}_q^{2n} \to \mathbb{F}_q^\times \) such that \( \mathbb{F}_q(\alpha) = \mathbb{F}_{q^{2n}} \). Either way, the product of the elements in the orbit is \( 1 \). The product splits into more than \( 1 \) \( \times \) \( 1 \) and again \( 1 \). We choose \( \alpha \) such \( \mathbb{F}_q \) exists, then \( \mathcal{I} \mathcal{U}_n(q) \) to \( \ker \mathbb{F}_q \to \mathbb{F}_q^\times \) has the same cardinality. The argument now goes through exactly as for \( \mathcal{L}_n(q) \). □

Proposition 2.6. Let \( \mathcal{O}_{2n}(q) \) denote the set of monic polynomials \( P(x) \in \mathbb{F}_q[x] \) of degree \( 2n \) such that \( P(x) = x^{2n} P(1/x) \). For all \( k > 0 \), there exists \( N \) such that if \( n \geq 2 \) and \( q \) is a prime power, then the set of \( P(x) \in \mathcal{O}_{2n}(q) \) such that \( P(x) \) splits into more than \( N \log n \) irreducible factors in \( \mathbb{F}_q[x] \) has at most \( n^{-k} |\mathcal{O}_{2n}(q)| \) elements.

Proof. The elements of \( \mathcal{O}_{2n}(q) \) are in bijective correspondence with Frobenius-stable multisets in \( \mathbb{F}_q \) of cardinality \( 2n \) which are invariant under \( x \mapsto x^{-1} \) and have product 1.

Let \( \mathcal{I} \mathcal{O}_m(q) \) denote the set of subsets of \( \mathbb{F}_q \) of cardinality \( m \) which are stable under Frobenius and the map \( x \mapsto x^{-1} \) and which are minimal among sets having this stability. The elements of \( \mathcal{I} \mathcal{O}_m(q) \) with one element are \( \{1\} \) and \( \{-1\} \), which are distinct if and only if \( q \) is odd. Suppose \( S \in \mathcal{I} \mathcal{O}_m(q) \) has at least two elements, and let \( \alpha \in S \). Now suppose \( \alpha^{-1} = \alpha^k \) for some \( k > 0 \). We choose \( k \) to be minimal, so

\[
S = \{\alpha, \alpha^q, \ldots, \alpha^q = \alpha^{-1}, \alpha^{-q}, \ldots, \alpha^{-q^{k-1}}\},
\]

and \( m = 2k \). If no such \( k \) exists, then

\[
S = \{\alpha, \alpha^q, \ldots, \alpha^{q^{k-1}}\} \amalg \{\alpha^{-1}, \alpha^{-q}, \ldots, \alpha^{-q^{k-1}}\},
\]

and again \( m = 2k \). We conclude that

\[
|\mathcal{I} \mathcal{O}_m(q)| = \begin{cases} 
2 & \text{if } m = 1 \text{ and } q \text{ is odd}, \\
1 & \text{if } m = 1 \text{ and } q \text{ is even}, \\
q - 2 & \text{if } m = 2 \text{ and } q \text{ is odd}, \\
q - 1 & \text{if } m = 2 \text{ and } q \text{ is even}, \\
0 & \text{if } m \geq 3 \text{ is odd}, \\
P_n(q) & \text{if } m = 2n \geq 4.
\end{cases}
\]

Let \( \mathcal{I} \mathcal{O}_{2n}^+(q) = \mathcal{I} \mathcal{O}_{2n}(q) \) if \( n \geq 2 \) and

\[
\mathcal{I} \mathcal{O}_{2}^+(q) = \mathcal{I} \mathcal{O}_{2}(q) \cup \{\{1, 1\}, \{-1, -1\}\}.
\]
where \( \{x, x\} \) denotes the multiset whose unique element \( x \) has multiplicity 2. In particular, \( |IO_{2n}(q)| = P_n(q) \) for all \( n \geq 1 \), and every element in \( O_{2n}(q) \) decomposes uniquely as a sum of elements in \( IO_{2n}^+(q) \) with \( \sum n_i = n \). If \( c_{n,m} \) denotes the number of elements in \( O_{2n}(q) \) whose root multiset decomposes into exactly \( m \) elements of \( IO_{2n}^+ \), then

\[
\sum_{m,n} c_{n,m} x^n y^m = \prod_{n=1}^{\infty} (1 - x^n y)^{-P_n(q)},
\]

so

\[
\sum_{i=m+1}^{n} c_{n,i} < n^C D^{-m},
\]

where \( C \) and \( D > 1 \) are absolute constants, and it follows that the proportion of such elements is \( < n^{-k} \) if \( N \) is sufficiently large. Finally, if \( P(x) \) has at least \( m \) irreducible factors, its root multiset must decompose into at least \( m/2 \) elements of \( IO_{2n}^+(q) \), and the proposition follows.

\[\square\]

3. Blocks of typical elements in classical groups

**Definition 3.1.** A classical group \( G \) over a finite field is a group of type \( SL_n, SU_n, SO_{2n}, Sp_{2n} \), or \( SO_{2n+1} \).

The classical groups admit natural injective representations of degree \( n, n, 2n, 2n, 2n, \) and \( 2n+1 \), respectively. We identify elements of classical groups with their images under these natural representations, so that, e.g., we can speak of the eigenvalues of an element \( g \in G(F_q) \). These eigenvalues form a multiset Spec \( g \) which is invariant under \( x \mapsto x^q \) in the first case, \( x \mapsto x^{-q} \) in the second case, and both in the remaining four cases. In the last case, \( 1 \) is an eigenvalue of odd multiplicity, and we define Spec \( 0 \) to be the spectrum less one copy of \( 1 \). For each \( g \), the characteristic polynomial of \( g \) (divided by \( x - 1 \) in the odd-orthogonal case) admits a unique decomposition into factors, i.e., elements of \( SL_n \) for \( G = SL_n, \) \( SU_n \) for \( G = SU_n, \) or \( IO_{2n}^+ \) for \( G \) self-dual which corresponds to the decomposition of Spec \( g \) (or Spec \( 0 \) in the odd-orthogonal case) into orbits. The total number of factors will be denoted Fact \( g \).

**Proposition 3.2.** There exist absolute constants \( A > 0 \) and \( B \) such that for every finite field \( \mathbb{F}_q \), every classical group \( G/F_q \), and semisimple element \( g \in G(F_q) \), we have

\[
|C_G(F_q)(g)| > A(\text{Fact } g)^B q^{\dim C_G(g)}.
\]

**Proof.** Consider first \( G = SL_n \). Let \( c_{i,j} \) denote the number of Galois orbits of eigenvalues of \( g \) of orbit size \( i \) and multiplicity \( j \). Setting \( C_i := \sum_j c_{i,j} \), we have

\[
|C_G(F_q)(g)| = \prod_{i,j} \frac{|GL_j(F_q)|^{c_{i,j}}}{q - 1} > q^{\dim C_G(g)} \prod_{i,j} \prod_{k=1}^{\infty} (1 - q^{-k})^{c_{i,j}} = q^{\dim C_G(g)} \prod_{i} \prod_{k=1}^{\infty} (1 - q^{-ki})^{C_i}.
\]
For $0 < x < 1/2$,
\[
\log(1 - x) = -\sum_{k=1}^{\infty} x^k/k > -\sum_{k=1}^{\infty} x^k > -2x,
\]
so
\[
\prod_{k=1}^{\infty} \left(1 - q^{-ki}\right) > e^{-2q^{-i}-2q^{-2i}-\ldots} > e^{-4q^{-i}}.
\]
Thus,
\[
|C_{G(\mathbb{F}_q)}(g)| > q^{\dim G} e^{-4\sum C_i q^{-i}}.
\]
As $C_i < q^i$ for each $i$ and $\sum_i C_i = \text{Fact } g$, we have
\[
\sum_{i=1}^{\infty} C_i q^{-i} < 1 + [\log_q \text{ Fact } g] < 1 + \frac{\log \text{ Fact } g}{\log 2}.
\]
Thus,
\[
e^{-4\sum C_i q^{-i}} > e^{-4(\text{Fact } g)^{4/\log 2}},
\]
which gives the proposition in this case. The other classical groups can be treated in the same way. \hfill \square

**Proposition 3.3.** There exist absolute constants $A$ and $B$ such that for every finite field $\mathbb{F}_q$, every classical group $G/\mathbb{F}_q$ of dimension $d$ and rank $r$, and every semisimple element $g \in G(\mathbb{F}_q)$, the set of elements in $G(\mathbb{F}_q)$ whose semisimple part is conjugate to $g$ has cardinality at most
\[
A(\text{Fact } g)^B q^{d-r}.
\]

**Proof.** To count elements with Jordan decomposition $su$ such that $s$ is conjugate to $g$, we first count conjugates $s$ of $g$, and then count the number of unipotent elements in $C_{G}(s)$ (which does not depend on the choice of conjugate $s$). By a standard estimate,
\[
c_1 q^{\dim G} < |G(\mathbb{F}_q)| < c_2 q^{\dim G}
\]
for some nonzero constants $c_1$ and $c_2$ which do not depend on $G$. By Proposition 3.2,
\[
|g^{G(\mathbb{F}_q)}| = \frac{|G(\mathbb{F}_q)|}{|C_{G(\mathbb{F}_q)}(g)|} < c_3 (\text{Fact } g)^{-Bq^{d-\dim G_{G(\mathbb{F}_q)}}}.
\]
Every unipotent element of $C_{G(\mathbb{F}_q)}(g)$ lies in the identity component of the reductive algebraic group $C_{G}(g)$, so by a theorem of Steinberg [St, Corollary 15.3], the number of unipotent elements in $C_{G(\mathbb{F}_q)}(g)$ is exactly $q^{\dim G_{G(\mathbb{F}_q)}}$. The proposition follows. \hfill \square

**Proposition 3.4.** For all $\epsilon > 0$, there exists $k$ such that for every finite field $\mathbb{F}_q$ and classical group $G/\mathbb{F}_q$, there exists a subset $S \subset G(\mathbb{F}_q)$ with $|S| \leq \epsilon |G(\mathbb{F}_q)|$, such that for all $g \notin S$, $\text{Fact } g < k \log n$.

**Proof.** This follows immediately from Proposition 3.3, the trivial bound $\text{Fact } g \leq n$, and the bounds given by Propositions 2.4, 2.5 and 2.6 in the cases $G = \text{SL}_n$, $G = \text{SU}_n$, and $G$ is self-dual, respectively. \hfill \square
Theorem 3.5. For all positive integers \( m \) and every \( \epsilon > 0 \), there exists \( l \) such that for every classical group \( G/\mathbb{F}_q \) there exists \( S \subset G(\mathbb{F}_q) \) with \( |S| \leq \epsilon |G(\mathbb{F}_q)| \), such that for all \( g \notin S \),

\[
|\{ h \in G(\mathbb{F}_q) \mid h^m = g^m \}| < q^{\log^4 n}.
\]

Proof. Whether we are in the \( IL \), the \( IU \), or the \( IO \) setting, if \( X \subset \mathbb{F}_q^X \) is an orbit such that \( \alpha^m = \beta^m \) implies \( \alpha = \beta \) for all \( \alpha, \beta \in X \), then

\[
X_m := X \amalg \zeta_m X \amalg \cdots \amalg \zeta_m^{m-1} X
\]

decomposes into a disjoint union of at most \( m \) orbits, and each orbit has cardinality \( \geq |X| \). Indeed, each such orbit \( Y \) is contained in \( X_m \) and maps onto \( X \) by the map sending \( \alpha \in Y \) to the unique \( \beta \in X \) such that \( \alpha^m = \beta^m \). It follows that the number of elements \( IL_n(q), IU_n(q), \text{ or } IO_n(q) \), respectively, with a root in the set \( X_m \) is at most \( O(mq^{n-1}|X|) \).

Moreover, whether we are in the \( IL \), the \( IU \), or the \( IO \) setting, if \( \alpha \) and \( \zeta_m^i \alpha \) are distinct elements of the same orbit \( X \) of size \( k \), then without loss of generality we may assume that

\[
\zeta_m^i \alpha = \alpha^{\pm q^j}
\]

for some \( j \leq k/2 \). The number of such elements for a given \( i \) is \( \leq q^{k/2} + 1 \), so the number of elements in \( IL_n(q), IU_n(q), \text{ or } IO_n(q) \) which have two distinct roots whose ratio is an \( m \)th root of unity is \( O(mq^{n/2}) \).

By removing \( \epsilon |G(\mathbb{F}_q)| \) elements from \( G(\mathbb{F}_q) \) we can assume by Proposition 3.4 that for all remaining elements \( g \), we have \( \text{Fact } g = O(\log n) \). By omitting all elements whose characteristic polynomial has a factor of degree \( \gg \log n \) with two distinct roots whose ratio is an \( m \)th root of unity or two factors of degree \( \gg \log n \) with roots whose ratio is an \( m \)th root of unity, we may further assume that there are at most \( O(\log n) \) eigenvalues of \( g^m \) with multiplicity \( \geq 1 \) and each such eigenvalue has multiplicity \( O(\log n) \).

To bound the order of the set of \( m \)th roots of \( g^m \) in \( G(\mathbb{F}_q) \) we embed this group in a larger group \( G \), which is defined to be \( \text{GL}_n(\mathbb{F}_q), \text{GL}_n(\mathbb{F}_{q^2}), \text{GL}_{2n}(\mathbb{F}_q), \text{GL}_{2n}(\mathbb{F}_{q^2}), \text{ or } \text{GL}_{2n+1}(\mathbb{F}_q), \) depending on whether \( G \) is linear, unitary, even-orthogonal, symplectic, or odd-orthogonal, and bound the number of \( m \)th roots of \( g^m \) in \( G \). Since \( h \) commutes with \( g^m = h^m \), all of the \( m \)th roots \( h \) lie in \( C_G(g^m) \). We can decompose the natural module on which \( G \) acts (\( \mathbb{F}_q^n, \mathbb{F}_{q^2}^n, \mathbb{F}_{q^2}^{2n}, \) or \( \mathbb{F}_{q^2}^{2n+1} \)) as a direct sum of two subspaces, \( V_1 \) and \( V_2 \), such that the action of \( g^m \) respects this decomposition, \( \dim V_2 = O(2^n) \), no eigenvalue of \( g^m \) acting on \( V_1 \) coincides with any eigenvalue of \( g^m \) acting on \( V_2 \), \( g^m \) has regular semisimple action on \( V_1 \), and the number of irreducible factors (over \( F := \mathbb{F}_q \) or \( F := \mathbb{F}_{q^2} \), as the case may be) of \( g^m \) acting on \( V_1 \) is \( O(\log n) \). Thus, every \( m \)th root \( h \) of \( g^m \) respects the decomposition \( V_1 \oplus V_2 \), and we can identify any such \( h \) with a pair \( (h_1, h_2) \in \text{Aut}_\mathbb{F}(V_1) \times \text{Aut}_\mathbb{F}(V_2) \). The centralizer of \( h_1^m \) in \( \text{Aut}_\mathbb{F}(V_1) \) is a product of \( O(\log n) \) cyclic groups, so there are at most \( m^{O(\log n)} \) possibilities for \( h_1 \). There are at most \( |\text{Aut}_\mathbb{F}(V_2)| = q^{O(\log^4 n)} \) possibilities for \( h_2 \). The theorem follows. \( \square \)
4. The main theorem

In this section we prove Theorem 1.1. More precisely, we prove the following:

**Theorem 4.1.** Let $m_1$ and $m_2$ be fixed positive integers. For a given group $G$, let $f: G^2 \to G$ denote the map

$$f(x_1, x_2) = x_1^{m_1} x_2^{m_2}.$$ 

Let $\mu_G$ denote the uniform distribution on $G$ and $\mu_{G \times G}$ the uniform distribution on $G^2$. Then,

$$\lim_{G} \|\mu_G - f_* \mu_{G \times G}\|_1 = 0$$

if the limit is taken over any sequence of pairwise distinct finite simple groups.

Here $f_* \mu_{G \times G}(X) := \mu_{G \times G}(f^{-1}(X))$, where $X \subseteq G$.

The proof uses, among other tools, the representation zeta function $\zeta^G$ of $G$, which we now define.

For a real number $s > 0$ set

$$\zeta^G(s) = \sum_{\chi \in \text{Irr } G} \chi(1)^{-s}.$$ 

We need the following result, which may be of independent interest.

**Proposition 4.2.** Fix $\epsilon > 0$, and let $G$ be a finite simple group. Then the probability that, for $g \in G$, $|\chi(g)| \leq \chi(1)^\epsilon$ for all irreducible characters $\chi$ of $G$ tends to 1 as $|G| \to \infty$.

**Proof.** By [LiS3] we have, for a fixed $s > 0$, $\zeta^G(s) = 1 + o(1)$ unless $G$ is a finite simple group of Lie type of bounded rank.

By Lemma 2.2 of [Sh1], the probability that $|\chi(g)| \leq \chi(1)^\epsilon$ for all irreducible characters $\chi$ of $G$ is at least $2 - \zeta^G(2\epsilon)$. If $G$ is not of Lie type of bounded rank, then the latter expression is $1 - o(1)$ as required. If $G$ is of Lie type of bounded rank, then the probability that $g \in G$ is regular semisimple is $1 - o(1)$, and for regular semisimple elements $g$ there exists $N$ depending on the rank of $G$ such that $|\chi(g)| \leq N$ for all $\chi \in \text{Irr } G$ [GLL Theorem 3]. If $G$ is large enough, we have $N \leq \chi(1)^\epsilon$ for all $1 \neq \chi \in \text{Irr } G$, and the result follows. \hfill \Box

A subset $S$ of a group $G$ is said to be normal if it is closed under conjugation by elements of $G$ (namely, $S$ is a union of conjugacy classes of $G$).

**Proposition 4.3.** For all positive integers $r, m$ and every $\epsilon > 0$, there exists $N$ such that for every group $G$ of Lie type of rank $r$ there exists a normal subset $S \subseteq G$ with $|S| \leq \epsilon |G|$ such that $|\chi(g^m)| \leq N$ for every $g \in G \setminus S$ and every irreducible character $\chi$ of $G$.

**Proof.** Note that this case includes the Suzuki and Ree groups, so we express $G$ as a quotient $\hat{G}/Z(\hat{G})$, where $\hat{G} := G(\mathbb{F}_q)^F$, $\hat{G}$ is a simply connected simple algebraic group, $F$ is a Frobenius map, and $Z$ denotes center. Fixing the rank of $\hat{G}$ gives an upper bound for the order of the Weyl group of $G$ and the number of simple roots of $G$. For every regular semisimple element $a \in \hat{G}$, we choose a regular semisimple element $\tilde{a}$ of $\hat{G}$ which lies over $a$. To bound $|\chi(a)|$ for every irreducible character of $G$, it suffices to bound $|\chi(\tilde{a})|$ for every irreducible character of $\hat{G}$. Letting $\tilde{A}$ denote the centralizer of $\tilde{a}$ in $\hat{G}$, we can deduce this by applying [GLL Theorem 3] to the pair $(\hat{G}, \tilde{A})$. 

If \( \tilde{G}_m \) denotes the set of \( x \in \tilde{G} \) such that \( x^m \) fails to be regular semisimple, then \( \tilde{G}_m \) consists of the \( F \)-fixed points of a proper Zariski-closed subset of \( G(\mathbb{F}_q) \) since the \( m \)th power map is dominant and the regular semisimple locus is open and dense in \( G \). By the argument of [LaS2, Proposition 3.4],

\[
|\tilde{G}_m| = O(|G|^{1-1/\dim \mathbb{G}}).
\]

By choosing \( N \) sufficiently large, we may take \( |G| \) as large as we wish and thereby obtain the proposition. \( \square \)

We can now prove Theorem 4.1.

**Proof.** As this is an asymptotic statement, it suffices to consider only alternating groups and groups of Lie type. For alternating groups, Theorem 4.1 is a special case of [LaS1, Theorem 1.18].

For any two conjugacy classes \( C_1 \) and \( C_2 \) of \( G \) (possibly equal), we denote by \( \mu_{C_1 \times C_2} \) the uniform distribution on the set \( C_1 \times C_2 \subset G^2 \). We can write

\[
\mu_{G \times G} = \sum_{C_1 \subset G} \sum_{C_2 \subset G} \frac{|C_1||C_2|}{|G|^2} \mu_{C_1 \times C_2},
\]

where the sums are taken over conjugacy classes. Thus,

\[
\|\mu_G - f_*\mu_{G \times G}\|_1 \leq \sum_{C_1 \subset G} \sum_{C_2 \subset G} \frac{|C_1||C_2|}{|G|^2} \|\mu_G - f_*\mu_{C_1 \times C_2}\|_1.
\]

If \( S \) is a normal subset of \( G \) such that \( \frac{|S|}{|G|} \leq \frac{\epsilon}{5} \) and

\[
\|\mu_G - f_*\mu_{C_1 \times C_2}\|_1 \leq \frac{\epsilon}{5}
\]

for all conjugacy classes \( C_1, C_2 \subset G \setminus S \), then

\[
\|\mu_G - f_*\mu_{C_1 \times C_2}\|_1 \leq \sum_{C_1 \subset G \setminus S} \sum_{C_2 \subset G \setminus S} \frac{|C_1||C_2|}{|G|^2} \|\mu_G - f_*\mu_{C_1 \times C_2}\|_1
\]

\[
+ \sum_{C_1 \subset S} \sum_{C_2 \subset G} \frac{|C_1||C_2|}{|G|^2} \|\mu_G - f_*\mu_{C_1 \times C_2}\|_1
\]

\[
+ \sum_{C_1 \subset G} \sum_{C_2 \subset S} \frac{|C_1||C_2|}{|G|^2} \|\mu_G - f_*\mu_{C_1 \times C_2}\|_1
\]

\[
\leq \frac{\epsilon}{5} + 2\frac{\epsilon}{5} + 2\frac{\epsilon}{5} = \epsilon.
\]

It therefore suffices to prove that as \( |G| \to \infty \), we can choose a normal subset \( S \) such that \( \frac{|S|}{|G|} \) and

\[
(3) \quad \max_{C_1, C_2 \subset G \setminus S} \|\mu_G - f_*\mu_{C_1 \times C_2}\|_1
\]

both tend to zero.

If \( c_1 \in C_1, c_2 \in C_2 \), and \( g \in G \), the probability that uniformly chosen conjugates \( x_1 \) and \( x_2 \) of \( c_1 \) and \( c_2 \), respectively, satisfy \( x_1^m x_2^{m_2} = g \) is

\[
\frac{1}{|G|} \sum_{x} \frac{\chi(c_1^m)\chi(c_2^{m_2})\chi(g)}{\chi(1)},
\]
where $\chi$ ranges over all irreducible characters of $G$. We claim that for the desired $L^1$ estimate, it suffices to prove that there exists a normal set $S'$ of $G$ of cardinality $o(|G|)$, such that for all $g \in G \setminus S'$ and all $c_1, c_2 \in G \setminus S$,

$$\sum_{\chi \neq 1} \frac{\chi(c_1^{m_1})\chi(c_2^{m_2})\chi(g)}{\chi(1)} = o(1).$$

Indeed, if $\mu_1$ denotes the measure obtained on $G$ by restricting $f_*\mu_{C_1 \times C_2}$ to $G \setminus S'$ and extending by zero, and

$$\mu_2 = f_*\mu_{C_1 \times C_2} - \mu_1,$$

then the $\mu_i$ are nonnegative measures, so

$$\|\mu_1\|_1 + \|\mu_2\|_1 = \|f_*\mu_{C_1 \times C_2}\|_1 = 1.$$

Moreover,

$$\|\mu_G - \mu_1\|_1 \leq \frac{|S'|}{|G|} + \max_{g \in G \setminus S'} \frac{1}{|G|} \sum_{\chi} \frac{\chi(c_1^{m_1})\chi(c_2^{m_2})\chi(g)}{\chi(1)}.$$

As

$$\|\mu_G - f_*\mu_{C_1 \times C_2}\|_1 \leq \|\mu_G - \mu_1\|_1 + \|\mu_2\|_1 = \|\mu_G - \mu_1\|_1 + 1 - \|\mu_1\|_1$$

$$\leq \|\mu_G - \mu_1\|_1 + 1 - (\|\mu_G\|_1 - \|\mu_G - \mu_1\|_1)$$

$$= 2\|\mu_G - \mu_1\|_1,$$

the claim follows.

We consider first the case that the rank $r$ of $G$ is sufficiently large. In particular, this means that $G$ is of linear, unitary, orthogonal, or symplectic type, which means that there exists a classical group $\tilde{G}$ over a finite field $\mathbb{F}_q$ and a subgroup $\tilde{G} \subset G(\mathbb{F}_q)$ of index $\leq 2$ such that $\tilde{G}$ is a central extension of $G$ of degree $\leq r$. By Theorem 3.5 there exists a normal subset $\tilde{S}$ of $\tilde{G}$ of cardinality $o(|\tilde{G}|)$ such that for every $g \in G \setminus \tilde{S}$ the fibers of the $m_1$th power and $m_2$th power maps containing $g$ have cardinality $q^{O(\log^* r)}$. If $G^{sc}$ is the simply connected covering group of $G$, then $G^{sc}(\mathbb{F}_q) \to G$ is a universal central extension and therefore factors through $\tilde{G}$. In particular, every irreducible representation of $\tilde{G}$ can be regarded as an irreducible representation of $G^{sc}(\mathbb{F}_q)$. Applying Proposition 1.2 we conclude that the (normal) set of all elements $g \in G \setminus \tilde{S}$ such that

$$\max(|\chi(g)|, |\chi(g^{m_1})|, |\chi(g^{m_2})|) > \chi(1)^{1/4}$$

for some irreducible character $\chi$ of $\tilde{G}$ has cardinality $o(|\tilde{G}|)$. By [LiS3, Theorem 1.2], if $r$ is sufficiently large,

$$\sum_{\chi \neq 1} \chi(1)^{-1/4} = o(1).$$

Defining $\tilde{f}$ to be the map $(x_1, x_2) \mapsto x_1^{m_1}x_2^{m_2}$ on $\tilde{G}$,

$$\|\mu_{\tilde{G}} - \tilde{f}_*\mu_{\tilde{G} \times \tilde{G}}\|_1 = o(1).$$

As the diagram

$$\begin{array}{ccc}
\tilde{G} \times \tilde{G} & \xrightarrow{\tilde{f}} & \tilde{G} \\
\downarrow & & \downarrow \\
G \times G & \xrightarrow{f} & \tilde{G}
\end{array}$$

we have

$$\|f_*\mu_{G \times G} - \tilde{f}_*\mu_{\tilde{G} \times \tilde{G}}\|_1 = o(1).$$
commutes, we deduce
\[ \| \mu_G - f_* \mu_{G \times G} \|_1 = o(1). \]
Next we consider the case that the rank \( r \) is bounded but greater than 1. This includes the cases of Suzuki and Ree groups. Let \( \tilde{G} = G^{sc}(\mathbb{F}_q)_F \), where \( F \) is a Frobenius map. By Proposition 4.3, there exists a normal subset \( \tilde{S} \subset \tilde{G} \) such that for all \( g \in \tilde{G} \) and every irreducible character \( \chi \) of \( g \),
\[ \max(\| \chi(g) \|, |\chi(g^{m_1})|, |\chi(g^{m_2})|) = O(1). \]
If \( S \) denotes the image of \( \tilde{S} \) in \( G \), it follows that \( |S| = o(|G|) \) (since the degree of the morphism \( G^{ac} \rightarrow G \) is bounded by rank), and that (4) holds for \( g \in G \setminus S \) and \( \chi \) any character of \( G \). By Theorem 1.1 and Corollary 1.3 of [LS3],
\[ \sum_{\chi \neq 1} \frac{1}{|\chi(1)|} = \zeta^G(1) - 1 = o(1) \]
for all finite \( G \) not of rank 1. This implies the theorem.

Finally, we consider the case of groups of the form \( G = \text{PSL}_2(q) \). It suffices to prove the theorem for \( \text{SL}_2(\mathbb{F}_q) \). As there are \( O(m) \) regular semisimple classes in \( \text{SL}_2(\mathbb{F}_q) \) whose \( m \)th power fails to be regular semisimple, it suffices to prove that (3) tends to zero if \( G \setminus S \) contains only regular semisimple elements.

By elementary algebra one checks that \( x \in \text{SL}_2(\mathbb{F}_q) \) is regular semisimple if and only if \( \text{tr}(x) \notin \{-2, 2\} \) and that if \( a_1, a_2, a_3 \in \mathbb{F}_q \setminus \{-2, 2\} \) such that
\[ a_1^2 + a_2^2 + a_3^2 \neq a_1a_2a_3 + 4, \]
the diagonal conjugation action of \( \text{SL}_2(\mathbb{F}_q) \) on
\[ \{(x_1, x_2, x_3) \in \text{SL}_2(\mathbb{F}_q)^3 : x_1x_2x_3 = e, \text{tr}(x_i) = a_i \forall i \in \{1, 2, 3\}\} \]
is simply transitive (see also [Ma], where such triples are studied). In particular, the number of ways to write \( x^{-1}_3 \) as a product of a conjugate of \( x_1 \) and a conjugate of \( x_2 \) equals the order of the centralizer of \( x_3 \) in \( \text{SL}_2(\mathbb{F}_q) \), which is either \( q-1 \) or \( q+1 \) depending on whether \( x_3 \) belongs to a split or a nonsplit torus of \( \text{SL}_2(\mathbb{F}_q) \).
From this, we deduce that (3) tends to zero as long as \( G \setminus S \) contains only regular semisimple elements. \( \square \)

5. Admissible words

We conclude this paper by proving Proposition 1.2. Let \( w \in F_d \) \((d \geq 1)\) be a word. For a finite group \( G \), let \( N_w(g) \) be the number of solutions of the equation \( w(g_1, \ldots, g_d) = g \), where \( g_i \in G \). Then \( N_w \) is a class function on \( G \), hence it can be expressed as \( N_w = \sum_{\chi \in \text{Irr} G} N_w^\chi \cdot \chi \), where \( N_w^\chi \in \mathbb{C} \) are the so-called Fourier coefficients, which have been studied by many authors.

Now let \( w \) be as in Proposition 1.2, namely \( 1 \neq w \in F_d \) is admissible in the variables \( x_1, \ldots, x_d \). Without loss of generality we may assume that \( x_1, \ldots, x_d \) all occur in \( w \).

By formula (1.5) of [PS] we have
\[ N_w^\chi = |G|^{d-1}/\chi(1)^{d-r}, \]
where \( r \) is a certain integer depending on \( w \) and satisfying \( 1 \leq r \leq d+1 \). If \( r = d+1 \), then \( N_w^\chi = |G|^{d-1}\chi(1) \) for all \( \chi \in \text{Irr} G \), so \( N_w = |G|^{d-1} \sum_\chi \chi(1) \chi \). This implies that the word map \( w : G^d \rightarrow G \) is identically 1 so \( w = 1 \) in \( F_d \), a contradiction. It follows that \( r \leq d \).
Next, by Theorem 4.2 in [PS], \( r \) is not congruent to \( d \) modulo 2. Setting \( k = d - r \) we obtain \( k \geq 1 \).

Clearly \( P_{w,G} = N_w/|G|^d \), and this yields

\[
P_{w,G} = \frac{1}{|G|} \sum_{\chi \in \text{Irr } G} \chi(1)^{-k} \cdot \chi.
\]

By Lemma 2.3 of [GS], if \( P = |G|^{-1} \sum_{\chi \in \text{Irr } G} a_{\chi} \chi \) and \( a_1 = 1 \), then \( \|P - \mu_G\|_1 \leq (\sum_{1 \neq \chi \in \text{Irr } G} |a_{\chi}|^2)^{1/2} \). Applying this we obtain

\[
\|P_{w,G} - \mu_G\|_1 \leq \left( \sum_{1 \neq \chi \in \text{Irr } G} \chi(1)^{-2k} \right)^{1/2} = (\zeta^G(2k) - 1)^{1/2}.
\]

By [LiS2] we have \( \zeta^G(2k) \to 1 \) as \( |G| \to \infty \). Therefore \( \|P_{w,G} - \mu_G\|_1 \to 0 \), and this completes the proof of Proposition 1.2.

REFERENCES

[BG] T. Bandman and S. Garion, Surjectivity and equidistribution of the word \( x^a y^b \) on \( \text{PSL}(2,q) \) and \( \text{SL}(2,q) \), Internat. J. Algebra Comput. 22 (2012), no. 2, 1250017, 33, DOI 10.1142/S0218196712500178. MR2903751


ON THE DISTRIBUTION OF VALUES OF CERTAIN WORD MAPS


DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, INDIANA 47405

E-mail address: mjlarson@indiana.edu

EINSTEIN INSTITUTE OF MATHEMATICS, HEBREW UNIVERSITY, GIVAT RAM, JERUSALEM 91904, ISRAEL

E-mail address: shalev@math.huji.ac.il