ISRAEL JOURNAL OF MATHEMATICS 139 (2004), 149–156

WORD MAPS HAVE LARGE IMAGE

BY

MICHAEL LARSEN*

Department of Mathematics, Indiana University
Bloomington, IN 47405, USA
e-mail: larsen@math.indiana.edu

ABSTRACT

An element w in the free group on r letters defines a map $f_{w,G}\colon G^r \to G$ for each group G. In this note, we show that whenever $w \neq 1$ and G is a semisimple algebraic group, $f_{w,G}$ is dominant. As an application, we show that for fixed w and Γ_i a sequence of pairwise non-isomorphic finite simple groups,

$$\lim_{i\to\infty} \frac{\log|\Gamma_i|}{\log|f_{w,\Gamma_i}(\Gamma_i^r)|} = 1.$$

Let F_r be the free group on r generators $x_1, \ldots, x_r$. For any group G, each word

$$w = x_{a_1}^{b_1} x_{a_2}^{b_2} \cdots x_{a_m}^{b_m} \in F_r$$

defines a corresponding **word map** $f_{w,G}\colon G^r \to G$:

$$f_{w,G}(g_1, \ldots, g_r) = g_{a_1}^{b_1} g_{a_2}^{b_2} \cdots g_{a_m}^{b_m}.$$

The main result of this note is as follows:

THEOREM 1: *If G is a simple algebraic group over any field K and $w \neq 1$, then $f_{w,G}$ is a dominant morphism. In other words, $f_{w,G}(G)$ contains a non-trivial Zariski-open subset of G.*

As an application, we prove the following theorem, which answers a question of A. Shalev:

* Partially supported by NSFGrant DMS-0100537.
Received January 23, 2003

THEOREM 2: *If $w \neq 1$ and $\Gamma_1, \Gamma_2, \ldots$ is an infinite sequence of finite simple groups, no two isomorphic to one another, then*

$$\lim_{i\to\infty} \frac{\log|\Gamma_i|}{\log|f_{w,\Gamma_i}(\Gamma_i^r)|} = 1.$$

Without loss of generality, we may assume K is algebraically closed. If $\pi\colon G \to H$ is any morphism of algebraic groups, the diagram

$$(1) \qquad \begin{array}{ccc} G^r & \xrightarrow{f_{w,G}} & G \\ \downarrow{\scriptstyle \pi^r} & & \downarrow{\scriptstyle \pi} \\ H & \xrightarrow{f_{w,H}} & H \end{array}$$

commutes. Applying (1) when π is an isogeny, we see that it suffices to prove the theorem for G simply connected. Applying it to the factor inclusion maps when G is a product, we see that it suffices to consider the case of simply connected almost simple groups. Such groups are indexed by connected Dynkin diagrams, and we begin with type A.

LEMMA 1: *Theorem 1 holds for $G = \mathrm{SL}_n$.*

Proof: We use induction on n, the base case $n = 1$ being trivial. Define $\chi_n\colon \mathrm{SL}_n \to \mathbb{A}^{n-1}$ so that if $g \in \mathrm{SL}_n$ has characteristic polynomial

$$x^n - a_1x^{n-1} + a_2x^{n-2} - \cdots + (-1)^n,$$

then

$$\chi_n(g) = (a_1, a_2, \ldots, a_{n-1}).$$

Thus χ_n is constant on conjugacy classes of SL_n. Over the non-empty open subvariety of $\mathbb{A}^{n-1}$ corresponding to polynomials with non-zero discriminant, the fibers of χ_n are single conjugacy classes. Since $f_{w,\mathrm{SL}_n}(\mathrm{SL}_n^r)$ is a union of conjugacy classes of SL_n, it contains a dense open subset of SL_n if and only if its image under χ_n contains a dense open subset of $\mathbb{A}^{n-1}$.

The induction hypothesis and the inclusion $\mathrm{SL}_{n-1} \hookrightarrow \mathrm{SL}_n$ imply that the Zariski closure of the image of $\chi_n \circ f_{w,\mathrm{SL}_n}$ contains a dense open subset of the hyperplane

$$(2) \qquad \{(a_1, \ldots, a_{n-1}) \mid 1 - a_1 + a_2 - \cdots + (-1)^n = 0\}$$

corresponding to elements of SL_n with eigenvalue 1. On the other hand, SL_n is connected, so the Zariski closure of

$$\chi_n(f_{w,\mathrm{SL}_n}(\mathrm{SL}_n^r))$$

is connected. To prove that the closure is all of $\mathbb{A}^{n-1}$ (and therefore that f_{w,SL_n} is dominant), we need only show that some element of the image of $\chi_n \circ f_{w,\mathrm{SL}_n}$ is not contained in (2), i.e., that some element of SL_n in the image of the word map does not have 1 as an eigenvalue.

To do this, we begin with a global field F contained in K. Let D be a division algebra of degree n over F and $\mathrm{SL}_1(D)$ the multiplicative group of elements of $D^\times$ with reduced norm 1, which we regard as the group of F-points of an inner form S of SL_n over F. Let $x_1 \in \mathrm{SL}_1(D) = S(F)$ denote an element of infinite order and $x_1, x_2, x_3, \ldots$ a maximal sequence of elements in $S(F)$ such that x_{n+1} does not lie in the normalizer of the identity component of the Zariski closure X_n of the subgroup generated by $x_1, \ldots, x_n$. Such a sequence is finite since $\dim X_{n+1} > \dim X_n$. Let Γ be the subgroup of $\mathrm{SL}_1(D)$ generated by all the x_i. As Γ is finitely generated and Zariski-dense in the semisimple group S, the Tits alternative [3] implies it contains a subgroup isomorphic to F_r. The inclusions

$$F_r \subset \Gamma \subset \mathrm{SL}_1(D) \subset D$$

allow us to regard w as an element of $D \setminus \{1\}$. In particular, $w - 1 \in D$ is non-zero and so is invertible in D. As K is algebraically closed, $S(K) = \mathrm{SL}_n(K)$, so it follows that $f_{w,\mathrm{SL}_n}(\mathrm{SL}_n(K)^r)$ contains an element of the desired kind. ∎

At this point we know that $f_{w,G}$ is dominant for any semisimple group G whose Dynkin diagram components are all of type A. Suppose G is a group of this type and $G \hookrightarrow H$ is an injective homomorphism of semisimple groups of equal rank; that is, a maximal torus T of G is again a maximal torus of H. Then the image of $f_{w,G}$ contains a dense open subset of T. Let $\Psi\colon H \times H \to H$ be the conjugation morphism defined by

$$\Psi(h_1, h_2) = h_1 h_2 h_1^{-1}.$$

Then,

$$f_{w,H}(H^r) \supset \Psi(H \times f_{w,G}(G^r)) \supset \Psi(H \times (T \cap f_{w,G}(G^r))).$$

The restriction of Ψ to $H \times T$ is dominant since every semisimple element of H is conjugate to an element of T. Therefore, $f_{w,H}(H^r)$ is dense in H. Thus, we need only verify:

LEMMA 4: *Every simply connected almost simple Lie group H over K contains an equal rank semisimple subgroup whose Dynkin diagram components are all of type A.*

Proof: There are obvious inclusions

$$\mathrm{SL}_2^n \subset \mathrm{Sp}_{2n},$$

$$\mathrm{SL}_2^{2n} = \mathrm{Spin}_4^n \subset \mathrm{Spin}_{4n} \subset \mathrm{Spin}_{4n+1},$$
$$\mathrm{SL}_2^{2n-2} \times \mathrm{SL}_4 = \mathrm{Spin}_4^{n-1} \times \mathrm{Spin}_6 \subset \mathrm{Spin}_{4n+2} \subset \mathrm{Spin}_{4n+3}.$$

For the exceptional groups we use the fact that a closed root subsystem of an irreducible root system gives rise to a semisimple subgroup; if the subsystem has equal rank, the same will be true on the group level. We apply this to the (root system) inclusions

$$A_2^3 \subset E_6,\ A_1 \times A_3^2 \subset E_7,\ A_4^2 \subset E_8,\ A_2^2 \subset F_4,\ A_2 \subset G_2$$

to prove the lemma. ∎

This finishes the proof of Theorem 1. ∎

Corollary 5: *If G is a semisimple algebraic group and w is a non-trivial element of F_r, then $f_{w,G(\mathbb{R})}(G(\mathbb{R})^r)$ has non-empty interior.*

Proof: By definition ([1] IV 17.3.7), smoothness of morphisms is an open property, so generic smoothness of a morphism of varieties can be checked at the generic point, where it is equivalent to separability of the extension of function fields ([1] 0_{IV} 19.6.1). As $f_{w,G}$ is a dominant morphism between varieties in characteristic 0, G^r contains a non-empty open subvariety of smooth points. As $G(\mathbb{R})$ is Zariski-dense in G, there exists a smooth point $x \in G^r(\mathbb{R})$. The image of x in $G(\mathbb{R})$ is an interior point by the implicit function theorem. ∎

Question 1: *Is $f_{w,G}$ always surjective at the algebraic variety level? How about at the level of $\mathbb{R}$-points?*

Finally, we prove Theorem 2. We use the classification of finite simple groups to divide the problem into three parts: groups of Lie type of bounded dimension, classical groups in the limit as rank tends to ∞, and alternating groups. We can disregard sporadic groups because we are interested only in behavior in the limit. We begin with the part of the problem directly related to the algebraic group case.

Proposition 7: *For any non-trivial word w and any root system Φ, there exists a constant $c > 0$ such that for all simple groups Γ of Lie type associated to the root system Φ,*

$$|f_{w,\Gamma}(\Gamma^r)| > c|\Gamma|.$$

Proof: The idea is to find an upper bound on the size of the fibers of $f_{w,\Gamma}$ by regarding them, more or less, as the $\mathbb{F}_q$-points of fibers of a morphism of varieties

$f_{w,G}\colon G^r \to G$, where G is a simple algebraic group with root system Φ and $\mathbb{F}_q$ is a finite field. The basic estimate is the naive one:

$$|X(\mathbb{F}_q)| < Cq^{\dim X},$$

but there are a number of technical difficulties in making this strategy work. To begin with, it is not quite accurate to identify Γ with a group of the form $G(\mathbb{F}_q)$. This is especially problematic when Γ is a Suzuki or Ree group. The constant C above has to be uniform across fibers of $f_{w,G}$ and independent of characteristic. Although by Theorem 1, generically the fibers of $f_{w,G}$ have dimension $(r-1)(\dim G)$, some fibers may have higher dimension, and we must account for these. Rather than developing from scratch a technology to deal with these problems, we appeal to [2], where such a technology already exists.

Let G be an adjoint simple group with root system Φ over an algebraically closed field K of characteristic p and $\Gamma \subset G(K)$. Without loss of generality, $|\Gamma| \gg 0$, so by [2] Prop. 3.5, Γ is sufficiently general. The dimension of fibers of $f_{w,G}$ is upper semicontinuous, so there exists a proper closed reduced subscheme $X_{w,G} \subset G^r$ such that $f_{w,G}$ restricted to $G^r \setminus X_{w,G}$ has constant fiber dimension.

The subscheme $X_{w,G}$ depends on the characteristic p, but the set of all such subschemes forms a constructible family in $\mathcal{G}^r$, where $\mathcal{G}/\operatorname{Spec}\mathbb{Z}$ is the adjoint Chevalley scheme with root system Φ. By [2] Th. 4.3,

$$|X_{w,G} \cap \Gamma^r| < c_1|\Gamma|^{\dim X_{w,G}/\dim G} \leq c_1|\Gamma|^{r-1/\dim G}.$$

The fibers Y_g of $f_{w,G}$ as g ranges over G and p ranges over all prime numbers again form a constructible family, so

$$|Y_g \cap \Gamma^r| < c_2|\Gamma|^{\dim Y_g/\dim G}.$$

Therefore,

$$|f_{w,\Gamma}(\Gamma^r)| \geq \frac{|\Gamma|^r - |X_{w,G} \cap \Gamma^r|}{c_2|\Gamma|^{r-1}} > \frac{1}{c_2}|\Gamma|\Big(1 - c_1|\Gamma|^{-1/\dim G}\Big) > \frac{|\Gamma|}{2c_2}$$

for $|\Gamma| \gg 0$. ∎

Proposition 8: *Let A_n denote the alternating group on n letters. Then for all $\epsilon > 0$ there exists N such that*

$$|f_{w,A_n}(A_n^r)| \geq |A_n|^{1-\epsilon}$$

for all $n \geq N$.

Proof: Let $\phi(n)$ and $\tau(n)$ denote the Euler ϕ-function and the number of divisors function, respectively. For any $\epsilon > 0$ and any sufficiently large prime power q, $\tau(q) < q^\epsilon$; as $\tau(n)$ is multiplicative, $\tau(n) = o(n^\epsilon)$. Therefore, the number of elements of order $< n^{1-\epsilon}$ in $\mathbb{Z}/n\mathbb{Z}$ is

$$\sum_{\substack{d|n \\ d<n^{1-\epsilon}}} \phi(d) \leq \tau(n)n^{1-\epsilon} < n^{\epsilon/2}(n^{1-\epsilon}) < n^{1-\epsilon/2}$$

for $n \gg 0$.

Now, let p be an odd prime, $\Gamma = \mathrm{PSL}_2(\mathbb{F}_p)$, $I_p = f_{w,\Gamma}(\Gamma^r)$. We claim that for $p \gg 0$, I_p contains an element of order $> p^{1-\epsilon}$. Let $\Delta_1 \cong \mathbb{Z}/\frac{p-1}{2}\mathbb{Z}$ (resp. $\Delta_2 \cong \mathbb{Z}/\frac{p+1}{2}\mathbb{Z}$) denote subgroups of Γ associated to a split (resp. non-split) torus in PGL_2. Two elements $x, y \in \Delta_i$ are conjugate in Γ if and only if $x = y^{\pm 1}$. The centralizer of any non-identity element of Δ_i is Δ_i itself, so the conjugacy class of such an element has order $|\Gamma|/|\Delta_i|$, and no such conjugacy class meets both Δ_1 and Δ_2. We conclude that if $p \gg 0$, the set of elements in Γ conjugate to some element of order $< p^{1-\epsilon}$ is at most $|\Gamma|p^{-\epsilon/2}$. By Proposition 7, I_p contains an element of order $\geq p^{1-\epsilon}$ if $p \gg 0$.

Next we consider the action of Γ on the finite projective line $\mathbb{P}^1(\mathbb{F}_p)$ (by fractional linear transformations). This gives an embedding

$$\mathrm{PSL}_2(\mathbb{F}_p) \hookrightarrow A_{p+1}.$$

A non-identity element of Δ_1 (resp. Δ_2) fixes 2 (resp. 0)points of $\mathbb{P}^1(\mathbb{F}_p)$; if its order is d, its image in A_{p+1} consists of $\frac{p-1}{d}$ (resp. $\frac{p+1}{d}$) d-cycles and 2 (resp. 0) 1-cycles. Let

$$S = \{p + 1 \mid p \text{ prime}\}.$$

By the prime number theorem, the greedy algorithm guarantees that there exists an integer B such that every interval of length B in the set of positive integers contains the sum of a sequence of elements of S, each larger than the sum of all that come after. In other words, for every positive integer n,

$$A_n \supset A_{p_1+1} \times \cdots \times A_{p_k+1} \supset \mathrm{PSL}_2(\mathbb{F}_{p_1}) \times \cdots \times \mathrm{PSL}_2(\mathbb{F}_{p_k}),$$

where

$$n - B \leq p_1 + 1 + \cdots + p_k + 1 \leq n, \quad p_i + 1 \in S, \quad k \leq \log_2 n.$$

It follows that $f_{w,A_n}(A_n^r)$ has an element which decomposes in $c = O(n^\epsilon \log n)$ cycles (including cycles of length 1). The centralizer of a product of c cycles in S_n has order $\leq n^c c! = o(|A_n|^\epsilon)$ for $n \gg 0$. Therefore, $f_{w,A_n}(A_n^r)$ contains a conjugacy class with more than $|A_n|^{1-\epsilon}$ elements. ∎

PROPOSITION 9: *For all $w \neq 1$ and $\epsilon > 0$ there exists N such that if Γ is a finite simple group of Lie type of rank $> N$ then*

$$|f_{w,\Gamma}(\Gamma^r)| > |\Gamma|^{1-\epsilon}.$$

Proof: Suppose Γ has a central extension $\tilde{\Gamma}$ in the set of groups

(3)
$$\{\mathrm{SL}_n(\mathbb{F}_q), \mathrm{SO}_{n,n}(\mathbb{F}_q), \mathrm{SO}_{2n+1}(\mathbb{F}_q), \mathrm{SO}_{n+2,n}(\mathbb{F}_q), \mathrm{Sp}_{2n}(\mathbb{F}_q), \mathrm{SU}_{2n}(\mathbb{F}_q), \mathrm{SU}_{2n+1}(\mathbb{F}_q)\}.$$

We note the inclusions

$$A_n \subset \mathrm{SL}_n(\mathbb{F}_q) \subset \mathrm{SO}_{n,n}(\mathbb{F}_q) \subset \mathrm{SO}_{2n+1}(\mathbb{F}_q) \subset \mathrm{SO}_{n+2,n}(\mathbb{F}_q) \subset \mathrm{SL}_{2n+2}(\mathbb{F}_q), \tag{4}$$

$$A_n \subset \mathrm{SL}_n(\mathbb{F}_q) \subset \mathrm{Sp}_{2n}(\mathbb{F}_q) \subset \mathrm{SL}_{2n}(\mathbb{F}_q), \tag{5}$$

and

$$A_n \subset \mathrm{SL}_n(\mathbb{F}_q) \subset \mathrm{SU}_{2n}(\mathbb{F}_q) \subset \mathrm{SU}_{2n+1}(\mathbb{F}_q) \subset \mathrm{SL}_{4n+2}(\mathbb{F}_q). \tag{6}$$

Suppose there exists a constant $\delta < 1$ (depending on w) such that for all $n \gg 0$ there exists $x \in f_{w,A_n}(A_n^r) \subset A_n$ whose images in $\mathrm{SL}_m(\mathbb{F}_q)$ for

$$m \in \{2n+2, 2n, 4n+2\}$$

all have centralizer orders $O(q^{n^{1+\delta}})$. This implies the same upper bound for the centralizer of the image y of x in $\tilde{\Gamma}$. The order of $\tilde{\Gamma}$ is at least

$$|\mathrm{SL}_n(\mathbb{F}_q)| = \frac{1}{q-1}\prod_{i=0}^{n-1}(q^n - q^i) > q^{n^2-1}\prod_{j=2}^{\infty}(1-q^{-j}) > \frac{q^{n^2-1}}{2},$$

so the conjugacy class of y in $\tilde{\Gamma}$ has order at least $|\tilde{\Gamma}|^{1-\epsilon}$ if $n \gg 0$. In mapping from $\tilde{\Gamma}$ to Γ the size of a conjugacy class goes down by at most a factor of $2n+1$. The estimate $O(q^{n^{1+\delta}})$ is therefore enough to prove the proposition.

The composed maps $A_n \subset \mathrm{SL}_m(\mathbb{F}_q)$ in (4), (5), and (6) factor through A_{2n+2}, A_{2n}, and A_{4n+2} respectively, and an element in A_n consisting of c cycles maps to an element with $2c+2$, $2c$, and $4c+2$ cycles respectively. As in Proposition 8, we can find $z \in A_m$, the image of $x \in A_n$, such that z consists of $O(m^\epsilon \log m)$ cycles.

Regarding z as a permutation matrix in $\mathrm{SL}_m(\mathbb{F}_q)$, we consider its centralizer in the matrix algebra $M_m(\mathbb{F}_q)$. If $(a_{i,j})$ is a matrix commuting with the permutation matrix associated with a permutation σ, then

$$a_{i,j} = a_{\sigma(i),\sigma(j)}$$

for all i, j. Therefore, the whole matrix is determined by any set of rows representing all σ-orbits. If σ has $\leq 4c+2$ orbits, the centralizer has order $\leq q^{(4c+2)m}$. Therefore the centralizer of the image of z in $\mathrm{SL}_m(\mathbb{F}_q)$ (or in any subgroup thereof) has order $O(q^{m^{1+2c}})$. The proposition, and therefore Theorem 2, follows. ∎

ACKNOWLEDGEMENT: I would like to thank A. Shalev for some interesting discussions regarding this paper and acknowledge the hospitality of The Hebrew University, where most of the work was carried out.

References

[1] J. Dieudonné and A. Grothendieck, *Éléments de Géométrie Algébrique IV*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **20** (1964), **24** (1965), **28** (1966), **32** (1967).

[2] M. Larsen and R. Pink, *Finite subgroups of algebraic groups*, preprint.

[3] J. Tits, *Free subgroups in linear groups*, Journal of Algebra **20** (1972), 250–270.