JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 22, Number 2, April 2009, Pages 437–466
S 0894-0347(08)00615-2
Article electronically published on September 12, 2008

WORD MAPS AND WARING TYPE PROBLEMS

MICHAEL LARSEN AND ANER SHALEV

Contents

1. Introduction

Waring's problem asks whether every natural number is a sum of $g(k)$ kth powers (where g is a suitable function). This was solved affirmatively by Hilbert in 1909. Optimizing $g(k)$ has been a central problem in additive number theory ever since (see [Na] for more detail and background).

Recently there has been considerable interest in group theoretic analogues of this phenomenon, where the aim is to present group elements as short products of certain "special" elements. These special elements can be powers or commutators or values of a general word w or elements of a special conjugacy class in the group.

The motivation for this is sometimes topological. Let G be a (topologically) finitely generated pro-p group. Using expressions of elements of the commutator subgroup G' as bounded products of commutators, Serre showed that G' is closed and deduced that every finite index subgroup of G is open. A recent deep result of Nikolov and Segal [NS1, NS2] shows that this holds for every finitely generated profinite group. Again the core of the proof is presenting group elements as short products of values of certain words.

Received by the editors February 1, 2007.

2000 *Mathematics Subject Classification.* Primary 20D06, 20G40; Secondary 14G15.

Key words and phrases. Word maps, finite simple groups, Waring's problem.

The first author was partially supported by NSF grant DMS-0354772.

The second author was partially supported by an Israel Science Foundation Grant.

Both authors were partially supported by a Bi-National Science Foundation United States-Israel Grant.

In the realm of finite simple groups such Waring type problems have been studied in even greater detail. We need some notation.

Let $w = w(x_1, \ldots, x_d)$ be a non-trivial group word, namely a non-identity element of the free group F_d on $x_1, \ldots, x_d$. Then we may write $w = x_{i_1}^{n_1} x_{i_2}^{n_2} \cdots x_{i_k}^{n_k}$ where $i_j \in \{1, \ldots, d\}$, n_j are integers, and we may assume further that w is reduced. Let G be a group. For $g_1, \ldots, g_d \in G$ we write

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

Let

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

be the set of values of w in G. For subsets $A, B \subseteq G$ let $AB = \{ab | a \in A, b \in B\}$ and $A^k = \{a_1 \cdots a_k | a_i \in G\}$.

Fix a non-trivial group word w and let G be a finite simple group. If G is large enough, then it follows from Jones [J] that $w(G) \neq \{1\}$ (namely w is not an identity in G). Can we then find a constant c (which may depend on w but not on G) such that $w(G)^c = G$?

Various instances of this problem have been solved affirmatively in the past decade or two. See Wilson [W] for the commutator word $w(x_1, x_2) = [x_1, x_2] = x_1^{-1} x_2^{-1} x_1 x_2$ and Martinez and Zelmanov [MZ] and Saxl and Wilson [SW] for power words $w = x_1^k$. It follows from their result that every element of a large enough finite simple group is a product of $f(k)$ kth powers.

In [LiSh] this is generalized to arbitrary words w. It is proved there that if $w(G) \neq \{1\}$, then $w(G)^c = G$, where the exponent $c = c(w)$ depends on w (but is not given explicitly). A somewhat surprising new result from [Sh] is that the exponent c can be chosen independent of the word w and may be, in fact, a very small number. More specifically *for every word $w \neq 1$ there is a positive integer $N = N(w)$ such that for every finite simple group G with $|G| \geq N(w)$ we have*

$$w(G)^3 = G.$$

The main purpose of this paper is to prove an even stronger result for certain families of finite simple groups, where the exponent 3 is replaced by 2 (see Theorems 1.6 and 1.7 below). Along the way we prove several results of independent interest, related to the size of $w(G)$ and to powers of certain conjugacy classes C in G.

Given a conjugacy class $C \neq 1$ in a finite simple group G, there exists a number k such that $C^k = G$. Substantial work has been devoted to the study of these numbers k and related so-called covering numbers (see, e.g., [AH, EGH, LL, LiSh]).

A particular challenge is to show that $C^2 = G$ in certain cases. Indeed a conjecture of Thompson states that every finite simple group G has a class C with this property. In spite of considerable progress this is still open in general.

Now let $C = \sigma^{S_n}$ be a conjugacy class in S_n. When can we say that $C^2 = A_n$? This problem has quite a long history. Gleason [Hs] seems to have been the first to observe that $C^2 = A_n$ if σ is an n-cycle. See also Bertram [Be]. Later this was generalized by Brenner [Br] to the case where σ consists of two cycles (or more generally two non-trivial cycles with some additional fixed points). The case of permutations with more general cycle structure remained wide open.

Our first result deals with permutations with any given number of cycles, provided n is sufficiently large. We denote the number of cycles (including 1-cycles) of a permutation σ by $\mathrm{cyc}(\sigma)$.

Theorem 1.1. *For every positive integer k there is a number $f(k)$ such that if $n \geq f(k)$ and σ is a permutation in S_n with $\operatorname{cyc}(\sigma) \leq k$, then $(\sigma^{S_n})^2 = A_n$.*

Moreover, there is an absolute constant c such that, if $n \geq c$ and σ is a permutation in S_n with $\operatorname{cyc}(\sigma) \leq n^{1/128}$, then $(\sigma^{S_n})^2 = A_n$.

By the Erdős-Turán theory (see [ET]), a randomly chosen permutation in S_n has $O(\log n)$ cycles. This gives rise to the following result.

Corollary 1.2. *(i) The probability that a randomly chosen permutation $\sigma \in S_n$ satisfies $(\sigma^{S_n})^2 = A_n$ tends to 1 as $n \to \infty$.*

(ii) The probability that a randomly chosen permutation $\sigma \in A_n$ satisfies $(\sigma^{A_n})^2 = A_n$ tends to 1 as $n \to \infty$.

Indeed, part (i) follows immediately, and part (ii) follows from (i) using the fact that for almost all $\sigma \in A_n$ we have $\sigma^{A_n} = \sigma^{S_n}$ (see [Sh], 3.3).

Corollary 1.2 sharpens a previous result showing that for almost all $\sigma \in A_n$ we have $(\sigma^{A_n})^3 = A_n$ (see Theorem 2.6 in [Sh]).

It is intriguing that the proof of Theorem 1.1 is non-elementary in the sense that it involves probabilistic arguments and new character-theoretic estimates. In particular we show that all character values $\chi(\sigma)$ of a permutation $\sigma \in S_n$ can be bounded in terms of $\operatorname{cyc}(\sigma)$ alone (see Theorem 7.2).

In order to apply Theorem 1.1 to Waring type problems, we need to show that the image $w(A_n)$ of a word map $w \neq 1$ contains conjugacy classes C with few cycles.

Theorem 1.3. *For every positive integer n there exists a permutation $\sigma_n \in A_n$ with the following properties:*

1. $\operatorname{cyc}(\sigma_n) \leq 17$*;*
2. *σ_n has at most 6 cycles of length > 1;*
3. *for each non-trivial word w there exists $N = N(w)$ such that if $n \geq N$, then $\sigma_n \in w(A_n)$.*

Our proof of Theorem 1.3 is highly non-elementary, involving algebraic geometry and results from analytic number theory, such as a version of Vinogradov's three primes theorem. The idea is to embed groups of the form $\mathrm{PSL}_2(\mathbb{F}_p)$ and their products in A_n and then focus on the properties of word maps on $\mathrm{SL}_2(\mathbb{F}_p)$.

It would be interesting to try to find an elementary proof of Theorem 1.3, as well as to improve it. In this context we pose the following:

Problem 1.4. What is the minimal number k such that (for $w \neq 1$ and $n \geq N(w)$) $w(A_n)$ always contains permutations with at most k cycles? Does $w(A_n)$ necessarily contain a cycle of length $n - k$ for some k which may depend on w but not on n?

We remark that for *some* n we can give an affirmative answer to this question. The following theorem answers a question which was suggested to us by Joseph Masters.

Theorem 1.5. *For every non-trivial word w, there exist infinitely many positive integers n such that $w(A_n)$ contains an n-cycle.*

In fact our proof shows that for any $\epsilon > 0$ and sufficiently large x there are at least $x^{1/2-\epsilon}$ positive integers $n \leq x$ such that $w(A_n)$ contains an n-cycle.

Equipped with the tools above, we can now improve earlier Waring type results for alternating groups, showing that $w(A_n)^2 = A_n$ if $n \gg 0$. In fact we prove a bit more.

Theorem 1.6. *For each pair of non-trivial words w_1, w_2 there exists $N = N(w_1, w_2)$ such that for all integers $n \geq N$ we have*

$$w_1(A_n)w_2(A_n) = A_n.$$

The idea of the proof is to combine Theorems 1.1 and 1.3, noting that $\sigma_n^{S_n} \subset w_i(A_n)$ for $i = 1, 2$ and $(\sigma_n^{S_n})^2 = A_n$.

We next establish a similar result for certain finite simple groups of Lie type. Indeed, if we limit our attention to groups of Lie type of bounded dimension, we can prove the following result:

Theorem 1.7. *Given an integer d and two non-trivial words w_1 and w_2, there exists an integer $N = N(d, w_1, w_2)$ such that if G is a simply connected almost simple algebraic group of dimension d over a finite field $\mathbb{F}$, $\Gamma = G(\mathbb{F})/Z(G(\mathbb{F}))$ is the finite simple group associated to G over $\mathbb{F}$, and $|\Gamma| \geq N$, then we have*

$$w_1(\Gamma)w_2(\Gamma) = \Gamma.$$

The method of the proof is to obtain a suitable surjectivity theorem at the level of algebraic groups and then to use the Riemann hypothesis for varieties over finite fields to show that the relevant fibers actually have points over $\mathbb{F}$.

As a consequence we obtain the following.

Corollary 1.8. *For each triple of non-trivial words w_1, w_2, w_3 there exists $N = N(w_1, w_2, w_3)$ such that if G is a finite simple group of order at least N, then*

$$w_1(G)w_2(G)w_3(G) = G.$$

Indeed, the case of groups of Lie type appears in [Sh], and Theorem 1.6 above completes the proof by dealing with alternating groups.

We conjecture this can be strengthened as follows.

Conjecture 1.9. *For each pair of non-trivial words w_1, w_2 there exists $N = N(w_1, w_2)$ such that if G is a finite simple group of order at least N, then*

$$w_1(G)w_2(G) = G.$$

Proving this for classical groups of unbounded rank seems quite challenging. However, combining this paper with [Sh], it follows that, if $w_1, w_2 \neq 1$ and G is a finite simple group, then

$$|w_1(G)w_2(G)|/|G| \to 1 \text{ as } |G| \to \infty.$$

Indeed by Theorem 1.6 above we may assume that G is of Lie type, and then the claim follows from Proposition 10.2 of [Sh] and its proof.

Let us now discuss the size of the subset $w(G)$. A related useful result of Borel [Bo] shows that the word map induced by w on simple algebraic groups is a dominant map. In [L] this is used to show that if G is a finite simple group and $\epsilon > 0$, then

$$|w(G)| \geq |G|^{1-\epsilon}$$

provided $|G| \geq f(w, \epsilon)$. In this paper we improve this bound for various families of finite simple groups.

We start with alternating groups. Often the key to estimating the size of $w(G)$ is finding special elements in it.

Indeed, using Theorem 1.3, one can easily deduce that, for $n \geq N(w)$,

$$|w(A_n)| \geq cn^{-6}|A_n|$$

for some absolute constant $c > 0$. In fact, we can improve on this estimate:

Theorem 1.10. *For each non-trivial word w and every $\epsilon > 0$, there exists $N = N(w, \epsilon)$ such that if $n \geq N$, then*

$$|w(A_n)| \geq n^{-\frac{29}{9}-\epsilon}|A_n|.$$

We can show that this bound is tight up to the value of the exponent. Indeed, consider a power word $w(x_1) = x_1^k$. Then by [L2] we have

$$|w(A_n)| \leq |w(S_n)| \leq an^{-b}n!,$$

where $b = 1 - \phi(k)/k$ and a is some constant (depending on k). Note that, choosing k suitably (e.g. as the product of the first m primes), we may arrange that $b \geq 1 - \epsilon$ for any fixed $\epsilon > 0$. This shows that the exponent in Theorem 1.10 must be at most -1.

It would be interesting to find out whether Theorem 1.10 can be improved as follows.

Problem 1.11. Is it true that $|w(A_n)| \geq n^{-1}|A_n|$ provided $w \neq 1$ and $n \geq N(w)$?

While we are unable to settle this for alternating groups, we obtain an analogous result for certain simple groups of Lie type.

Theorem 1.12. *Let G be a finite simple group of Lie type and of rank r. Let $w \neq 1$ be a word. Then if G is not of type A_r or ${}^2A_r$, we have*

$$|w(G)| \geq cr^{-1}|G|$$

for some absolute constant $c > 0$, provided $|G| \geq N(w)$.

It is interesting that our methods allow us to generalize various results on $w(G)$ to intersections of the form $\bigcap_{i=1}^{k} w_i(G)$, where $w_1, \ldots, w_k \neq 1$ are any given words. These generalizations are formulated in the last section of this paper.

Here we give some words on the structure of this paper. Sections 2–4 are geometric in nature. Section 2 is devoted to groups of Lie type and the proof of Theorem 1.12. In Section 3 we focus on Lie type groups of bounded dimension and prove Theorem 1.7. In Section 4 we make a closer analysis of word maps on groups of the type $\mathrm{SL}_2(\mathbb{F}_p)$ and $\mathrm{SL}_3(\mathbb{F}_p)$. Combined with estimates from analytic number theory, including a version of Vinogradov's three primes theorem, this leads to the proofs of Theorems 1.3, 1.5 and 1.10 in Section 5. Section 6, which is of a combinatorial nature, contains the elementary part of the proof of Theorem 1.1. In Section 7 we study character values of S_n on permutations with few cycles and squares of conjugacy classes of such permutations. In this way we obtain a probabilistic proof of Theorem 1.1. Section 7 then concludes with the deduction of Theorem 1.6. Finally, in Section 8 we formulate results on the intersection of the images of different word maps and show how to derive them using our methods.

2. Word values in groups of Lie type

In this section, we use algebraic geometry and group-theoretic arguments to give lower bounds on $|w(\Gamma)|$ for certain groups Γ of Lie type, thus proving Theorem 1.12. Note that the bounds obtained are actually stronger than those we give for alternating groups. Although in the rest of the paper, G denotes a finite simple group, in this section and §3, G will always denote a simply connected, almost simple algebraic group defined over a finite field. To get a finite simple group Γ, we divide $G(\mathbb{F}_q)$ by its center. All simple groups of Lie type arise in this way, excepting the Suzuki and Ree groups. The Suzuki and Ree groups can also be treated by the methods of this section, but we exclude them to avoid unpleasant technicalities.

Proposition 2.1. *Let w be a non-trivial word and G a simply connected almost simple algebraic group over a finite field $\mathbb{F}_q$. Then there is a positive constant c depending only on w and $\dim G$ such that*

$$|w(G(\mathbb{F}_q))| > c|G(\mathbb{F}_q)|.$$

This proposition is proved as [L, Prop. 7] in a form that also includes the case of Ree and Suzuki groups. Here we give an alternative proof that uses standard techniques from algebraic geometry instead of results from [LP].

We use the following more or less standard result:

Lemma 2.2. *Let $\pi\colon \mathcal{X} \to \mathcal{Y}$ denote a dominant morphism between reduced schemes of finite type over $\mathbb{Z}$. Then there exist constants c_1 and c_2 such that for every prime p and every point $y \in \mathcal{Y}(\mathbb{F}_p)$, we have*

$$|\{x \in \mathcal{X}(\mathbb{F}_p)\colon \pi(x) = y\}| \leq c_1 p^{\dim \pi^{-1} x}$$

and if $\pi^{-1}y$ is non-empty and geometrically irreducible, then

$$|\{x \in \mathcal{X}(\mathbb{F}_p)\colon \pi(x) = y\}| \geq p^{\dim \pi^{-1} y}(1 - c_2 p^{-1/2}).$$

Proof. By the Lefschetz trace formula, these results are immediate consequences of standard facts about étale cohomology groups: the boundedness of the compactly supported cohomology groups of the fibers of π, the trace map on the top-dimensional cohomology of (geometrically irreducible) varieties, and the weight estimates for the eigenvalues of the Frobenius map on these cohomology groups (see [AGV, XVIII 2.9] and [De, 3.3.1].) □

We now prove the proposition.

Proof. An algebraic group G of this kind is specified by a connected Dynkin diagram Δ, an automorphism of this diagram (which is determined up to inner automorphism by its order $g \leq 3$), and a finite field $\mathbb{F}_q$. It suffices to prove this proposition for each fixed choice of Δ and g.

First we treat the split case, $g = 1$. In this case, Δ determines a simply connected Chevalley scheme $\mathcal{G}$ over Spec $\mathbb{Z}$ of which G is the $\mathbb{F}_q$-fiber, and w determines a morphism of schemes $\mathcal{G}^d \to \mathcal{G}$ which we denote π_w. If π_w has all fibers of dimension $\leq (d-1)\dim G$, then we are done by Lemma 2.2, since $|G(\mathbb{F}_q)| \geq c_1 q^{\dim G}$ and each fiber has at most $c_2 q^{(d-1)\dim G}$ points of $G(\mathbb{F}_q)^d$ for some positive constants c_1 and c_2 independent of q. The difficulty is that it might happen, a priori, that most points in $G(\mathbb{F}_q)^d$ lie in fibers of π_w of dimension greater than $(d-1)\dim G$.

To show that this does not in fact happen for large q, we note first that π_w is dominant; moreover, it is dominant for every fiber of $\mathcal{G}^d$ over Spec $\mathbb{Z}$ [Bo]. Fiber dimension is a constructible function [G3, 9.5.5], so the Zariski closure of the set of geometric points $\overline{s}$ for which

$$\dim \pi_w^{-1}(\overline{s}) > (d-1)\dim G$$

is a proper closed subset of $\mathcal{G}$. Let $\mathcal{X}$ denote its inverse image in $\mathcal{G}^d$. By [Bo], $\mathcal{X}$ is a proper closed subvariety of $\mathcal{G}^d$ for all p which does not contain the generic point of any fiber of $\mathcal{G}^d$ over Spec $\mathbb{Z}$. By Lemma 2.2, for all $q \gg 0$, at least half of the points of $G(\mathbb{F}_q)^d$ do not lie in $\mathcal{X}(\mathbb{F}_q)$, and the proposition follows.

Finally, we treat the case $g \geq 2$. Instead of defining a split group scheme $\mathcal{G}$ over Spec $\mathbb{Z}$, we define a non-split group scheme $\pi\colon \mathcal{G} \to \mathcal{S}$ for some higher-dimensional base $\mathcal{S}$ such that $\mathcal{G}$ splits over a finite étale Galois cover $\mathcal{S}'$ over $\mathcal{S}$ of degree g. For example, we may take

$$\mathcal{S} = \operatorname{Spec} \mathbb{Z}[1/g][x^g, x^{-g}] \amalg \operatorname{Spec} \mathbb{F}_g[x^g - x]$$

and

$$\mathcal{S}' = \operatorname{Spec} \mathbb{Z}[1/g][x, x^{-1}] \amalg \operatorname{Spec} \mathbb{F}_g[x].$$

The crucial point is that the base is large enough that for every $\mathbb{F}_q$ there exists an $\mathbb{F}_q$-valued point s of $\mathcal{S}$ whose preimage in $\mathcal{S}'$ is $\mathbb{F}_{q^g}$, since this guarantees that every $G/\mathbb{F}_q$ with the given Dynkin diagram and diagram automorphism can be obtained as the fiber of $\mathcal{G}$ for some $\mathbb{F}_q$ point of $\mathcal{S}$. □

We can now prove Theorem 1.12.

Proof. The case of groups of type E, F, and G and of classical groups of any fixed dimension follows from Proposition 2.1. We need therefore consider only orthogonal groups and symplectic groups. We begin with the symplectic case.

Let V be a 2-dimensional vector space over the field $\mathbb{F}_{q^r}$. We endow V with an area form A. We define a bilinear form on V, regarded as a vector space over $\mathbb{F}_q$, as follows:

$$\langle v_1, v_2 \rangle = \operatorname{tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q} A(v_1 \wedge v_2).$$

This form is obviously antisymmetric and non-degenerate. It therefore determines an inclusion

$$i\colon \mathrm{SL}_2(\mathbb{F}_{q^r}) \to \mathrm{Sp}_{2r}(\mathbb{F}_q).$$

If $x \in \mathrm{SL}_2(\mathbb{F}_{q^r})$ has eigenvalues $\lambda^{\pm 1}$, then $i(x)$ has eigenvalues $\lambda^{\pm q^k}$, $k = 0, 1, 2, \ldots, r-1$. As long as these eigenvalues are pairwise distinct, $i(x)$ is a regular semisimple symplectic matrix. This can be achieved by insisting for every proper subfield $\mathbb{F}_{q^d}$, λ belongs neither to $\mathbb{F}_{q^d}^\times$ nor to the norm-1 subgroup of $\mathbb{F}_{q^{2d}}$ over $\mathbb{F}_{q^d}$. The subset of $\mathrm{SL}_2(\mathbb{F}_{q^r})$ consisting of elements which violate either condition has cardinality $O(q^{3r/2})$, so by Proposition 2.1, we can find at least $c_1 q^{3r}$ elements of $w(\mathrm{SL}_2(\mathbb{F}_{q^r}))$ which are regular semisimple in $\mathrm{Sp}_{2r}(\mathbb{F}_q)$. If semisimple elements $a, b \in \mathrm{SL}_2(\mathbb{F}_{q^r})$ have eigenvalues $\alpha^{\pm 1}$, $\beta^{\pm 1}$ respectively, then $i(a)$ and $i(b)$ have the same eigenvalues if and only if $\alpha = \beta^{q^i}$ or $\alpha^{-1} = \beta^{q^i}$ for some $i \in \{0, 1, \ldots, r-1\}$. Thus there are at least $c_2 r^{-1} q^r$ distinct conjugacy classes of regular semisimple elements in $i(w(\mathrm{SL}_2(\mathbb{F}_{q^r}))) \subset w(\mathrm{Sp}_{2r}(\mathbb{F}_q))$. The centralizer of any regular semisimple element $i(a)$ in $\mathrm{Sp}_{2r}(\mathbb{F}_q)$ coincides with the image of the centralizer of a in $\mathrm{SL}_2(\mathbb{F}_{q^r})$; it is therefore of order $q^r \pm 1$. Thus,

$$|i(w(\mathrm{SL}_2(\mathbb{F}_{q^r})))| \geq c_2 r^{-1} \frac{q^r}{q^r + 1} |\mathrm{Sp}_{2r}(\mathbb{F}_q)|.$$

This proves the theorem for groups of type C.

For the cases B and D, we begin by observing that given a vector space V over $\mathbb{F}_{q^k}$ and a non-degenerate quadratic form $Q_0\colon V \to \mathbb{F}_{q^k}$ defined over $\mathbb{F}_{q^k}$, we can define a non-degenerate quadratic form on V regarded as an $\mathbb{F}_q$-vector space as follows:

$$Q(v) = \operatorname{tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q} Q_0(v).$$

This gives an inclusion $\mathrm{Spin}(V, Q_0) < \mathrm{Spin}(V, Q)$. Composing this map with an isomorphism $\mathrm{SL}_2(\mathbb{F}_{q^{2k}}) \cong \mathrm{Spin}_4^-(\mathbb{F}_{q^k})$, we obtain an inclusion

$$\mathrm{SL}_2(\mathbb{F}_{q^{2k}}) \to \mathrm{Spin}_{4k}^{\pm}(\mathbb{F}_q) \tag{2.1}$$

for some choice of signs. By the classification of quadratic forms over finite fields, every space W of dimension ≥ 4 with a non-degenerate quadratic form over $\mathbb{F}_q$ can be decomposed as $W_1 \perp W_2$, where W_1 is isomorphic to a space V obtained as above and $\dim W_2 \leq 6$. We choose such a decomposition and let i denote the map

$$\mathrm{SL}_2(\mathbb{F}_{q^{2k}}) \times \mathrm{Spin}(W_2) \to \mathrm{Spin}(W)$$

obtained by combining (2.1) with the natural map

$$\mathrm{Spin}(W_1) \times \mathrm{Spin}(W_2) \to \mathrm{Spin}(W).$$

Note that i is at most two-to-one since $\mathrm{SO}(W_1) \times \mathrm{SO}(W_2) \to \mathrm{SO}(W)$ is injective. If $k \geq 4$, $b \in \mathrm{Spin}(W_2)$ is regular semisimple, and the eigenvalues of a semisimple element $a \in \mathrm{SL}_2(\mathbb{F}_{q^{2k}})$ are not contained in a proper subfield of $\mathbb{F}_{q^{2k}}$, then the image of $i(a, b)$ in $\mathrm{SO}(W)$ has all eigenvalues distinct and is therefore regular semisimple. By Proposition 2.1, the number of such pairs (a, b) with $a \in w(\mathrm{SL}_2(\mathbb{F}_{q^{2k}}))$ is at least

$$c_3 q^{2k} q^{\frac{\dim W_2}{2}} = c_3 q^{\frac{\dim W}{2}},$$

and the number of semisimple conjugacy classes in $w(\mathrm{Spin}(W))$ determined by such pairs is at least $c_4 r^{-1} q^{\frac{\dim W}{2}}$. For q greater than some constant c_5 (independent of k), we can further specify that $b \in w(\mathrm{Spin}(W_2))$ at the cost of replacing c_4 by c_6. The centralizer of $i(a, b)$ in $\mathrm{Spin}(W)$ is a maximal torus of $\mathrm{Spin}(W)$ containing a maximal torus of $\mathrm{Spin}(W_1)$; it therefore has at most

$$(q^{2k} + 1)(q + 1)^{\frac{\dim W_2}{2}} \leq c_7 q^{\frac{\dim W}{2}}$$

elements. We conclude that the total number of elements of $\mathrm{Spin}(W)$ conjugate to elements of $i(\mathrm{SL}_2(\mathbb{F}_{q^{2k}}) \times \mathrm{Spin}(W_2))$ is at least $\frac{c_6}{c_7} r^{-1} |\mathrm{Spin}(W)|$.

Finally, we consider the case that $q \leq c_5$. In this case, we take $b = 1$, so $i(a, b)$ is not regular; its centralizer is $\mathrm{Spin}(W_2)$ times a maximal torus of $\mathrm{Spin}(W_1)$. The order of the centralizer is therefore less than $c_5^{(\dim W_2)^2} q^{\frac{\dim W}{2}}$, and the argument goes through as before. □

3. Waring's problem in bounded dimension

In this section we focus on simple groups of Lie type G in bounded dimension. Using geometric methods and establishing the irreducibility of certain fibers (see Theorem 3.3 below), we obtain a best possible solution of Waring's problem for such groups, namely $w(G)^2 = G$ provided $|G|$ is large enough. Moreover, we prove a somewhat stronger result, namely Theorem 1.7 dealing with two different words.

We begin with a basic geometric lemma:

Proposition 3.1. *Consider the diagram*

$$\begin{tikzcd} & X \arrow[dl, "f"'] \arrow[dr, "g"] & \\ Y \arrow[rr, dashed] & & Z \end{tikzcd}$$

of affine varieties over an algebraically closed field k. If Y is normal, f is generically smooth and surjective, and g factors through f at the level of closed points, then g factors through f as a morphism of algebraic varieties.

Proof. Let A, B, and C denote the coordinate rings of X, Y, and Z, respectively. They are Jacobson rings [G3, 10.4.6], so that every non-empty locally closed subset of X, Y, or Z contains at least one closed point [G3, 10.1.2]. Let K and L denote the function fields of X and Y, respectively. We have the diagram

$$\begin{tikzcd}
 & L & A \arrow[l, hook'] & \\
K \arrow[ur, hook] & B \arrow[l, hook'] \arrow[ur, "\phi_f"] & & C. \arrow[ul, "\phi_g"'] \arrow[ll, dashed]
\end{tikzcd}$$

Surjectivity of f implies that every prime ideal of B contains $\ker \phi_f$, and as B is an integral domain, this means that ϕ_f is injective. We regard B as a subring of A via ϕ_f. Our goal is to prove that $\phi_g(C) \subset B$. Suppose not. Let $h \in A$ denote an element of $\phi_g(C) \setminus B$. Thus f factors through

$$f_h \colon \operatorname{Spec} B[h] \to \operatorname{Spec} B.$$

We consider four cases:

(1) $L(h) = L$.
(2) $L(h)$ is an inseparable extension of L.
(3) $L(h)$ is a non-trivial separable extension of L.
(4) $L(h)$ is a transcendental extension of L.

In case (1), as B is normal and $h \in L \setminus B$, there exists a prime ideal $\mathfrak{p}$ of B of height 1 such that $h \notin B_{\mathfrak{p}}$ [Ma, Th. 38]. In other words, $\mathfrak{p}$ does not lie in the image of f_h, contrary to the surjectivity hypothesis on f.

In case (2), the extension $L \to K$ is inseparable, contrary to the hypothesis that f is generically smooth.

In case (3), the morphism $X \to \operatorname{Spec} B[h]$ is dominant (since $B[h] \subset A$). By [G4, 17.6.1], there exists a dense open set $U_1 \subset \operatorname{Spec} B[h]$ for which the morphism f_h is étale and by [G1, 1.8.4], a dense open set $U_2 \subset \operatorname{Spec} B[h]$ contained in the image of X in $\operatorname{Spec} B[h]$. Thus $\overline{f_h(U_1^c \cup U_2^c)}^c$ is a non-empty open set in $\operatorname{Spec} B$ over which f_h is étale and every point in $\operatorname{Spec} B[h]$ lies in the image of X. By [G3, 15.5.9], by passing to a smaller open set if necessary, the cardinality of every fiber of f_h equals $[L(h) : L]$. It follows that there exist closed points $x_1, x_2 \in X$ with the same image in $\operatorname{Spec} B$ but distinct images in $\operatorname{Spec} B[h]$. If $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are the corresponding maximal ideals of A, then h maps to different elements in $A/\mathfrak{m}_1 = k$ and $A/\mathfrak{m}_2 = k$. Adding a suitable element of k to h, we may assume that h maps to 0 in $A/\mathfrak{m}_1$ but not in $A/\mathfrak{m}_2$ and therefore some element of C maps to $\mathfrak{m}_1$ but not to $\mathfrak{m}_2$. It follows that x_1 and x_2 have distinct images in $\operatorname{Spec} C$, contrary to hypothesis.

The argument is the same in case (4), except that $\operatorname{Spec} B[h] \to \operatorname{Spec} B$ has the property that the inverse image of every point in $\operatorname{Spec} B$ is infinite. □

Proposition 3.2. *Let G be a simply connected, almost simple algebraic group over an algebraically closed field k. If $X \subset G$ is a conjugacy class of positive dimension, then for all sufficiently large integers n, the morphism $\pi_n \colon X^n \to G$ obtained by multiplying coordinates in G is generically smooth and surjective.*

Proof. Let X_i denote the Zariski closure of $\pi_i(X^i)$. As X^i is irreducible, X_i is the closure of a single point and therefore irreducible. The sequence $\dim X_1, \dim X_2, \ldots$ is non-decreasing and must therefore stabilize, so we may assume $\dim X_n = \dim X_{n+1} = \cdots$. If $x_1, x_2 \in X(k)$, then

$$x_1 X_n \cup x_2 X_n \subset X_{n+1},$$

so $x_1 X_n = x_2 X_n$, and

$$x_1^{-1} x_2 X_n = X_n. \tag{3.1}$$

Let Y_i denote the Zariski-closure of $\phi_i(X^{2i})$ (or, equivalently, the closure of $\phi_i(X(k)^{2i})$), where

$$\phi_i(x_1, \ldots, x_{2i}) = x_1^{-1} x_2 x_3^{-1} x_4 \cdots x_{2i-1}^{-1} x_{2i}.$$

If n is sufficiently large, $\dim Y_m = \dim Y_{m+1}$, so

$$x_1^{-1} x_2 Y_m = x_1^{-1} x_2' Y_m,$$

or

$$x_2^{-1} x_2' Y_m = Y_m$$

for all $x_2, x_2' \in X(k)$. This implies that $Y_m Y_m = Y_m$ and therefore Y_m is a connected algebraic subgroup of G. As X is conjugation-invariant, Y_m is a normal subgroup, and it follows that $Y_m = G$. By (3.1),

$$X_n = Y_m X_n = G X_n = G.$$

Let Z_i denote the Zariski closure of the complement of $\pi_i(X^i)$. For $i \geq n$, Z_i is a proper closed subvariety of G. If $x_1, x_2 \in X(k)$, then

$$Z_{n+1} \subset x_1 Z_n \cap x_2 Z_n.$$

If $x_1 Z_n = x_2 Z_n$ for all $x_1, x_2 \in X(k)$, then Z_n is invariant under translation by $Y_m = G$, which is impossible. Thus $x_1 Z_n \neq x_2 Z_n$ for some $x_1, x_2 \in X(k)$. If we form a vector out of the number of irreducible components of Z_n of each dimension, arranged from $\dim Z_n$ to 0 in decreasing order, then the vector of Z_n exceeds that of Z_{n+1} in the lexicographic order. We conclude that $Z_n = \emptyset$ for $n \gg 0$, and this gives surjectivity.

For generic smoothness, it suffices to find points $x_1, \ldots, x_n \in X(k)$ such that the map $G^n \to G$ given by

$$(g_1, \ldots, g_n) \mapsto g_1 x_1 g_1^{-1} g_2 x_2 g_2^{-1} \cdots g_n x_n g_n^{-1}$$

is smooth at the identity in G^n. Equivalently, we must prove that the space

$$\begin{aligned} L(x_1, \ldots, x_n) := (1 - \mathrm{ad}(x_1))(\mathfrak{g}) + \mathrm{ad}(x_1)(1 - \mathrm{ad}(x_2))(\mathfrak{g}) \\ + \cdots + \mathrm{ad}(x_1 \cdots x_{n-1})(1 - \mathrm{ad}(x_n))(\mathfrak{g}) \end{aligned}$$

equals $\mathfrak{g}$ for suitable $x_1, \ldots, x_n$. As

$$L(x_1, \ldots, x_n) = (1 - \mathrm{ad}(x_1))(\mathfrak{g}) + \mathrm{ad}(x_1)(L(x_2, \ldots, x_n)),$$

we have

$$\dim L(x_1, \ldots, x_n) \geq \dim L(x_2, \ldots, x_n)$$

with equality if and only if

$$(\mathrm{ad}(x_1^{-1}) - 1)(\mathfrak{g}) \subset L(x_2, \ldots, x_n).$$

Now,

$$S_X := \mathrm{Span}_{x\in X}(\mathrm{ad}(x^{-1})-1)(\mathfrak{g})$$

is invariant under the adjoint action of G. As x is not in the center of G, $S_X \neq 0$. If the adjoint representation of $\mathfrak{g}$ is irreducible, which is usually the case since G is almost simple, it follows that $S_X = \mathfrak{g}$. To see that this is true in general, we observe that since every element of G is a product of elements of X,

$$S_X = \mathrm{Span}_{g\in G}(\mathrm{ad}(g)-1)(\mathfrak{g}),$$

and G acts trivially on $\mathfrak{g}/S_X$. As G is simply connected, there is no non-trivial quotient of $\mathfrak{g}$ on which G acts trivially (see, e.g., [Pi, 1.11]), so $S_X = \mathfrak{g}$, as claimed.

Therefore, the dimension determined by a sequence in X can always be increased by prepending a suitable element of X unless it already equals $\dim\mathfrak{g}$. The proposition follows. □

We can now prove our basic irreducibility theorem:

Theorem 3.3. *Let w_1 and w_2 denote non-trivial words in n_1 and n_2 letters, respectively, and let $w \in F_{n_1+n_2}$ denote their juxtaposition. Let G be a simply connected almost simple algebraic group over an algebraically closed field k. Then for all non-central elements $g \in G(k)$, the fiber $\pi_w^{-1}(g)$ is irreducible.*

We remark that the hypothesis that G is simply connected is really needed. Otherwise, we can take $w_1 = x_1x_2x_1^{-1}x_2^{-1}$ and $w_2 = x_3x_4x_3^{-1}x_4^{-1}$ and the resulting morphism π_w factors through the universal cover of G.

Proof. We can express the fiber $\pi_w^{-1}(g)$ as the fiber product over G of π_{w_1} and a second morphism, namely the composition of π_{w_2} with the "reflection" map $x \mapsto gx^{-1}$. We will prove that this fiber product is geometrically irreducible.

Let A denote the coordinate ring of G and K the field of fractions of A. Let K_i denote the separable closure of K in the fraction field of $A^{\bigotimes n_i}$, where the morphism $A \to A^{\bigotimes n_i}$ is that associated to π_{w_i}. Let L_i be the splitting field of K_i over K and $\lambda_i\colon K \to L_i$ the natural inclusion map.

For any $g \in G(k)$, we define reflection, conjugation, and translation maps $G \to G$ as follows:

$$\rho_g(x) = gx^{-1},\ \chi_g(x) = gxg^{-1},\ \tau_g(x) = gx.$$

The induced automorphisms of A and K are also denoted ρ_g, χ_g, and τ_g, respectively. Let

$$\chi_{g,i}(x_1,\dots,x_{n_i}) = (gx_1g^{-1},\dots,gx_{n_i}g^{-1}).$$

We claim that if g does not lie in the center of $G(k)$, then λ_1 and $\lambda_2\circ\rho_g$ give linearly disjoint finite extensions of K. As $A^{\bigotimes n_i}$ is geometrically irreducible over K_i [G2, 4.5.10] and fiber products of geometrically irreducible schemes over a field are again geometrically irreducible [G2, 4.5.8], this claim implies the theorem. As L_1 and L_2 are Galois over K, it is equivalent to prove that there do not exist subfields $\tilde K_1$ and $\tilde K_2$ of L_1 and L_2, properly containing K, such that $\tilde K_1$ and $\tilde K_2$ are isomorphic as K-extensions.

Suppose, on the contrary, that such an isomorphism $\iota\colon \tilde K_1 \to \tilde K_2$ exists. The injective homomorphisms λ_i factor through $\tilde K_i$, and we write κ_i for the corresponding homomorphisms $K \hookrightarrow \tilde K_i$. Then we have the following diagram, in which the horizontal maps are isomorphisms and the vertical maps are finite field extensions:

$$\begin{tikzcd}
\tilde{K}_1 \arrow[r, "\chi_{h,1}"] & \tilde{K}_1 \arrow[r, "\iota"] & \tilde{K}_2 \arrow[r, "\chi_{h,2}^{-1}"] & \tilde{K}_2 \arrow[r, "\iota^{-1}"] & \tilde{K}_1 \\
K \arrow[r, "\chi_h"] \arrow[u, "\kappa_1"'] & K \arrow[r, "\rho_g"] \arrow[u, "\kappa_1"'] & K \arrow[r, "\chi_h^{-1}"] \arrow[u, "\kappa_2"'] & K \arrow[r, "\rho_g^{-1}"] \arrow[u, "\kappa_2"'] & K. \arrow[u, "\kappa_1"']
\end{tikzcd}$$

The composition of horizontal arrows gives a diagram

$$\begin{tikzcd}
\tilde{K}_1 \arrow[r, "\sigma_{g,h}"] & \tilde{K}_1 \\
K \arrow[r, "\tau_{hgh^{-1}g^{-1}}"] \arrow[u, "\kappa_1"] & K, \arrow[u, "\kappa_1"']
\end{tikzcd}$$

where $\sigma_{g,h}$ is an isomorphism depending on g and h.

Let $\tilde{A}$ denote the integral closure of A in $\tilde{K}_1$. As A is finitely generated over the field K, it is a Japanese ring [G2, 7.7.4], so $\tilde{A}$ is a finitely generated A-module. The map κ_1 restricts to an injective ring homomorphism $A \to \tilde{A}$; by a slight abuse of notation, we denote by κ_1 also the corresponding homomorphism of affine varieties $\tilde{G} \to G$, where $\tilde{G} = \operatorname{Spec} \tilde{A}$. We fix $e \in \tilde{G}(k)$ lying over the identity in G. For every $h_1, h_2 \in G$, σ_{g,h_1} and $\chi_{h_2,1}$ induce automorphisms of $\tilde{G}$. Fix h_1 which does not commute with g and let h_2 vary over G. By taking the commutator of σ_{g,h_1} and $\chi_{h_2,1}$, we obtain a morphism $\Sigma\colon X \times \tilde{G} \to \tilde{G}$, where X is the conjugacy class of $h_1 g h_1^{-1} g^{-1}$, and each point of X gives an automorphism of $\tilde{G}$ which covers the corresponding translation of G. We write Σ_n for the morphism $X^n \times \tilde{G} \to \tilde{G}$ defined recursively by

$$\Sigma_n(x_1, \ldots, x_n, y) = \Sigma(x_1, \Sigma_{n-1}(x_2, \ldots, x_n, y)),$$

for $n \geq 2$ and $\Sigma_1 = \Sigma$. Let $\Sigma_{n,e}\colon X^n \to \tilde{G}$ be defined by

$$\Sigma_{n,e}(x_1, \ldots, x_n) = \Sigma_n(x_1, \ldots, x_n, e).$$

The composition $\Sigma_{n,e} \circ \kappa_1$ gives the restriction to X^n of the usual n-fold multiplication morphism $G^n \to G$.

By Proposition 3.2, the composition of $\Sigma_{n,e}\colon X^n \to \tilde{G}$ and $\tilde{G} \to G$ is surjective and generically smooth for all sufficiently large integers n. It follows that $\Sigma_{n,e}$ itself is generically smooth and dominant. If the Zariski-closure $\tilde{Z}_n$ of the complement of the image of $\Sigma_{n,e}$ is non-empty, then there exist $x_1, x_2 \in X(k)$ such that $\Sigma(x_1, \tilde{Z}_n) \neq \Sigma(x_2, \tilde{Z}_n)$ (because the images of these two subvarieties of $\tilde{G}$ in G are distinct). As

$$\tilde{Z}_{n+1} \subset \Sigma(x_1, \tilde{Z}_n) \cap \Sigma(x_2, \tilde{Z}_n),$$

we see the vector of component dimensions of $\tilde{Z}_n$ is greater than that of $\tilde{Z}_{n-1}$. For n sufficiently large, therefore, $\tilde{Z}_n$ is empty, i.e., $\Sigma_{n,e}$ is surjective.

We would like to apply Proposition 3.1 to the upper triangle of the diagram

(3.2)
$$\begin{tikzcd}
& X^n \times \tilde{G} \arrow[dl, "\Sigma_{n,e}\times \mathrm{id}"'] \arrow[dr, "\Sigma_n"] & \\
\tilde{G} \times \tilde{G} \arrow[rr, dashed, "\tilde{\mu}"] \arrow[d, "\kappa_1\times\kappa_1"'] & & \tilde{G} \arrow[d, "\kappa_1"] \\
G \times G \arrow[rr] & & G.
\end{tikzcd}$$

We observe first that the pentagon of solid arrows in (3.2) commutes because the diagram

$$\begin{tikzcd}
X \times \tilde{G} \arrow[r, "\Sigma"] \arrow[d, "\mathrm{id}\times\kappa_1"'] & \tilde{G} \arrow[d, "\kappa_1"] \\
X \times G \arrow[r] & G
\end{tikzcd}$$

commutes. The variety $\tilde{G}\times\tilde{G}$ is normal since $\tilde{G}$ is so by construction. To check that there exists a morphism $\tilde{\mu}$ at the level of closed points, we note that if $x_1, \ldots, x_n$ belong to $X(k)$, the resulting map $\Sigma_n(x_1, \ldots, x_n, \cdot)$ is an automorphism of $\tilde{G}$ which covers translation by $x_1 \cdots x_n$. Our claim asserts that, at least at the level of closed points, this automorphism depends only on $\Sigma_{n,e}(x_1, \ldots, x_n)$ and not on the actual n-tuple $(x_1, \ldots, x_n)$. Indeed, if we fix $\tilde{g} \in \tilde{G}$ and let $g = \kappa_1(\tilde{g})$, there is a unique automorphism of $\tilde{G}$ covering τ_g and sending e to $\tilde{g}$. Thus, we may apply Proposition 3.1 to define $\tilde{\mu}$. The resulting diagram commutes (i.e., the lower rectangle does so) because it commutes at the level of closed points.

We claim that the arrow $\tilde{\mu}$ in (3.2) is a multiplication morphism making $(\tilde{G}, e)$ into an algebraic group and $\tilde{G} \to G$ into a central isogeny. As G is simply connected, this implies that κ_1 is an isomorphism [Ti, 1.5.4] and therefore that $K = \tilde{K}_1$, which proves the theorem.

To prove that $\tilde{\mu}$ satisfies the associativity axiom, we compare the two maps $\tilde{G}^3 \to \tilde{G}$ given by $\tilde{\mu}(\tilde{\mu}(x, y), z)$ and $\tilde{\mu}(x, \tilde{\mu}(y, z))$. We have a diagram

$$\begin{tikzcd}
\tilde{G}^3 \arrow[r, shift left] \arrow[r, shift right] \arrow[d, "\kappa_1^3"'] & \tilde{G} \arrow[d, "\kappa_1"] \\
G^3 \arrow[r] & G.
\end{tikzcd}$$

The closed subvariety of $\tilde{G}^3$ on which the two arrows agree is also open since the fibers of $\tilde{G} \to G$ are finite. It is non-empty since it contains (e, e, e). As $\tilde{G}^3$ is connected, $\tilde{\mu}$ is associative.

Next we construct the inverse on $\tilde{G}$. We choose an automorphism of $\tilde{G}$ which covers the composition $\tau_{h^{-1}} \circ \rho_h$ (which maps $x \mapsto x^{-1}$). This automorphism sends e to some element of $\tilde{G}$ lying over the identity of G. By composing with a deck transformation, we can find a new automorphism of $\tilde{G}$ which sends e to itself and covers the inverse map on G. Again we use connectedness to show that this morphism satisfies the diagram for inverse maps with respect to $\tilde{\mu}$. Thus $(\tilde{G}, \tilde{\mu}, e)$ is an algebraic group and the covering map $\tilde{G} \to G$ is a surjective homomorphism, i.e., an isogeny. As it is separable, it is central. The theorem follows. □

We can now deduce Theorem 1.7

Proof. As in the proof of Proposition 2.1, it suffices to consider a fixed Dynkin diagram Δ and a group scheme $\pi\colon \mathcal{G} \to \mathcal{S}$ such that every simply connected, almost simple algebraic group $G/\mathbb{F}_q$ with Dynkin diagram Δ is isomorphic to $\mathcal{G}_s$ for some $s \in \mathcal{S}(\mathbb{F}_q)$. Next we consider the morphism

$$\pi_w\colon \mathcal{G}^{n_1+n_2} \to \mathcal{G}$$

(where the fiber power is taken relative to $\mathcal{S}$) given by a word w which is a juxtaposition of the words w_1 and w_2 taken in disjoint variables. If $s \in \mathcal{S}(\mathbb{F}_q)$ and $x \in \mathcal{G}_s(\mathbb{F}_q)$ is a non-central element, then by Theorem 3.3, the fiber of π_w over s is geometrically irreducible, so by Lemma 2.2, if $q \gg 0$, $x \in w(\mathcal{G}_s(\mathbb{F}_q))$. If Γ denotes the quotient of $\mathcal{G}_s(\mathbb{F}_q)$ by its center, it follows that the image of x in Γ lies in $w(\Gamma)$. This accounts for all elements of Γ except the identity, which trivially lies in $w(\Gamma)$. □

4. Special word values in $\mathrm{SL}_2(\mathbb{F}_p)$ and $\mathrm{SL}_3(\mathbb{F}_p)$

In this section we take a closer look at 2 and 3-dimensional special linear groups, which play a key role in our results for alternating groups. Our main results below prove that $w(\mathrm{SL}_3(\mathbb{F}_p))$ contains elements of maximal order in $\mathrm{SL}_3(\mathbb{F}_p)$ and $w(\mathrm{SL}_2(\mathbb{F}_p))$ contains elements of nearly maximal order in $\mathrm{SL}_2(\mathbb{F}_p)$ under certain conditions on p.

Theorem 4.1. *For every non-trivial word w there exists a constant $\epsilon > 0$ such that for every prime p such that*

$$\frac{\phi(p^2+p+1)}{p^2+p+1} > 1-\epsilon, \tag{4.1}$$

there exists an element of order p^2+p+1 in $w(\mathrm{SL}_3(\mathbb{F}_p))$.

Proof. Let

$$A_3 := \mathrm{Spec}\ \mathbb{Z}[a_{11}, a_{12}, \ldots, a_{33}]/(\det(a_{ij})-1),$$

$\mathrm{SL}_3 := \mathrm{Spec}\ A_3$, and $\mathbb{A}^1 = \mathrm{Spec}\ \mathbb{Z}[x]$. Let $\pi_w\colon \mathrm{SL}_3^d \to \mathrm{SL}_3$ denote the word map. Let $\tau_1, \tau_2\colon \mathrm{SL}_3 \to \mathbb{A}^1$ denote the characters of the tautological representation and its dual, respectively, and let $\tau = (\tau_1, \tau_2)\colon \mathrm{SL}_3 \to \mathbb{A}^2$. Thus, the characteristic polynomial of $w(x_1, \ldots, x_d)$ is

$$\chi(z) = \chi_{(x_1,\ldots,x_d)}(z) := z^3 - \tau_1(w(x_1,\ldots,x_d))z^2 + \tau_2(w(x_1,\ldots,x_d))z - 1.$$

Let $K_{3,d}$ denote the fraction field of $A_3^{\bigotimes d}$. We have the following basic lemma.

Lemma 4.2. *The splitting field of the polynomial $\chi(z) \in K_{3,d}[z]$ over $\overline{\mathbb{Q}}K_{3,d}$ has Galois group S_3.*

Proof. Suppose $\chi(z)$ has a root $\alpha \in \overline{\mathbb{Q}}K_{3,d}$. Then there exists a number field E such that $\alpha \in EK_{3,d}$, and choosing a rational prime p split in E, we may regard α as an element of $\mathbb{Q}_pK_{3,d}$ and therefore as a regular function on some non-trivial open subset $U \subset \mathrm{SL}^d_{3,\mathbb{Q}_p}$. Now $\chi(z)$, regarded as a polynomial-valued function on $\mathrm{SL}^d_{3,\mathbb{Q}_p}$, is invariant under conjugation by $\mathrm{SL}_{3,\mathbb{Q}_p}$, diagonally embedded. As $\chi(z)$ has at most three roots and SL_3 is connected, it follows that α is also $\mathrm{SL}_{3,\mathbb{Q}_p}$-invariant.

Let $\mathbb{Q}_{p^3}$ denote the unramified cubic extension of $\mathbb{Q}_p$ and let $D \subset M_3(\mathbb{Q}_{p^3})$ denote a $\mathbb{Q}_p$-central division algebra of degree 3. Let $\mathrm{SL}_1(D) \subset D^\times$ denote the kernel of the reduced norm, so $\mathrm{SL}_1(D) \subset \mathrm{SL}_3(\mathbb{Q}_{p^3})$. As $\mathrm{SL}_1(D)$ is Zariski-dense in SL_3 and w is dominant, there exists $(g_1, \ldots, g_d) \in \mathrm{SL}_1(D)^d \cap U(\mathbb{Q}_{p^3})$ such that the specialization $\chi_{(g_1,\ldots,g_d)}(z) \in \mathbb{Q}_{p^3}[z]$ is square-free. As α is SL_3-invariant and $(g_1^\sigma, \ldots, g_d^\sigma)$ is SL_3-conjugate to $(g_1, \ldots, g_d)$ for each $\sigma \in \mathrm{Gal}(\mathbb{Q}_{p^3}/\mathbb{Q}_p)$, it follows that the specialization $\alpha_{(g_1,\ldots,g_d)}$ actually belongs to $\mathbb{Q}_p$. By definition, $\alpha_{(g_1,\ldots,g_d)}$ is an eigenvalue of $w(g_1, \ldots, g_d) \in \mathrm{SL}_1(D)$, and as D is a division algebra, this means that $w(g_1, \ldots, g_d) = \alpha_{(g_1,\ldots,g_d)}$, which is impossible since $\chi_{(g_1,\ldots,g_d)}(z)$ is square-free. The contradiction proves that $\chi(z)$ is irreducible in $\overline{\mathbb{Q}}K_{3,d}[z]$.

It remains to show that the Galois group of the splitting field is S_3 rather than $\mathbb{Z}/3\mathbb{Z}$, in other words, that the discriminant $\delta \in K_{3,d}$ of $\chi(z)$ is not a perfect square. If this is not true, there exists a number field E such that $\sqrt{\delta} \in EK_{3,d}$, and choosing p split in E, we may write $\delta = \gamma^2$, with $\gamma \in \mathbb{Q}_pK_{3,d}$. Reasoning as before, γ is invariant by the conjugation action of SL_3. Now let D denote the *quaternion* algebra over $\mathbb{Q}_p$. The embedding $D \subset M_2(\mathbb{Q}_{p^2})$ gives an embedding $\mathrm{SL}_1(D) \to \mathrm{SL}_2(\mathbb{Q}_{p^2})$; composing with the embedding of SL_2 in SL_3 (given by the direct sum of the trivial representation and the tautological representation), we have an embedding $\mathrm{SL}_1(D) \to \mathrm{SL}_3(\mathbb{Q}_{p^2})$. The image is generically regular semisimple, and w is dominant on SL_2, so there exists $(g_1, \ldots, g_d) \in \mathrm{SL}_1(D)^d \subset \mathrm{SL}_3(\mathbb{Q}_{p^2})$ such that the specialization of γ to $(g_1, \ldots, g_d)$ is non-zero. As $(g_1^\sigma, \ldots, g_d^\sigma)$ is SL_3-conjugate to $(g_1, \ldots, g_d)$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}_{p^2}/\mathbb{Q}_p)$, this specialization lies in $\mathbb{Q}_p$, and therefore the specialization of δ to $(g_1, \ldots, g_d)$ is a non-zero perfect square in $\mathbb{Q}_p$. However, $w(g_1, \ldots, g_d)$ has eigenvalues 1, λ, and λ^{-1} where $\lambda \notin \mathbb{Q}_p$, so the discriminant of

$$\chi_{(g_1,\ldots,g_d)}(z) = (z-1)(z-\lambda)(z-\lambda^{-1})$$

is *not* a perfect square in $\mathbb{Q}_p$. The contradiction proves the lemma. □

Let $\mathcal{T} \subset \mathrm{SL}_3$ denote the $\mathbb{Z}$-subscheme of diagonal matrices. Thus S_3 acts on $\mathcal{T}$, and $\mathcal{T}/S_3 \cong \mathbb{A}^2$. Let $\mathcal{X}$ denote the fiber product of SL_3^d and $\mathcal{T}$ over the base $\mathcal{T}/S_3$:

$$\begin{tikzcd}
 & \mathcal{X} \arrow[dl] \arrow[dr] & \\
\mathrm{SL}_3^d \arrow[r, "\pi_w"] \arrow[dr] & \mathrm{SL}_3 \arrow[d, "\tau"] & \mathcal{T} \arrow[l, hook'] \arrow[dl] \\
 & \mathcal{T}/S_3 \cong \mathbb{A}^2_{\mathbb{Z}}. &
\end{tikzcd}$$

Let $\mathcal{Y}$ denote the integral closure of $\mathbb{A}^2$ in SL_3^d, and write $\psi\colon \mathrm{SL}_3^d \to \mathcal{Y}$ and $\phi\colon \mathcal{Y} \to \mathbb{A}^2$ for the maps factoring $\mathrm{SL}_3^d \to \mathbb{A}^2$. Thus ψ has a geometrically irreducible generic fiber and ϕ is finite. By the openness of geometric connectivity [G3, 9.7.7], there exists a non-empty subscheme $\mathcal{U} \subset \mathbb{A}^2$ such that over $\mathcal{U}$, ψ has geometrically irreducible fibers. Shrinking $\mathcal{U}$, we may assume that $\mathcal{T}_{\mathcal{U}} \to \mathcal{U}$ is étale and (by [G3, 9.5.5]), all fibers of ψ have the generic fiber dimension (which, since π_w and τ are dominant, is $8d-2$). Let S_p denote the set of $s \in \mathrm{SL}_3(\mathbb{F}_p)^d$ such that s lies over $(u_1, u_2) \in \mathcal{U}(\mathbb{F}_p)$ and the polynomial $z^3 - u_1z^2 + u_2z - 1$ is irreducible in $\mathbb{F}_p[z]$. By Lemma 4.2, $\mathcal{X} \to \operatorname{Spec} \mathbb{Z}$ has a geometrically irreducible generic fiber and therefore geometrically irreducible fibers over $\mathbb{F}_p$ for all $p \gg 0$. We may therefore apply the Chebotarev density theorem in the function field case (see, e.g., [Ln]) to obtain

$$|S_p| = \frac{1}{3}p^{8d} + O(p^{8d-1/2}),$$

where the implied constant does not depend on p. By Lemma 2.2,

$$|\psi(S_p)| = \frac{1}{3}p^2 + O(p^{3/2}),$$

so

$$|\phi(\psi(S_p))| \geq \frac{1}{3\deg\phi}p^2 + O(p^{3/2}).$$

On the other hand, the set of pairs $(u_1, u_2) \in \mathbb{F}_p^2$ such that $z^3 - u_1z^2 + u_2z - 1$ is irreducible over $\mathbb{F}_p$ with roots which fail to generate the norm-1 subgroup of $\mathbb{F}_{p^3}^\times$ has cardinality at most

$$p^2 + p + 1 - \phi(p^2 + p + 1) < \epsilon(p^2 + p + 1) < 2\epsilon p^2.$$

If $\epsilon < \frac{1}{6\deg\phi}$, the theorem follows for all p greater than some constant N_w depending only on w. By choosing ϵ even smaller, we can guarantee that (4.1) is never satisfied for $p \leq N_w$. □

Next we prove a variant of this result for SL_2. The condition on the prime p is weaker, but the conclusion about $w(\mathrm{SL}_2(\mathbb{F}_p))$ is also weaker.

Theorem 4.3. *For every non-trivial word w there exists an odd integer N_w such that if $p \equiv 1 \pmod 4$ is prime, $p+1$ is relatively prime to N_w, and $p > N_w$, then $w(\mathrm{SL}_2(\mathbb{F}_p))$ contains an element of order $\frac{p+1}{2}$ or order $p+1$.*

Proof. Let

$$\mathrm{SL}_2 = \mathrm{Spec}\,\mathbb{Z}[a_{11},\ldots,a_{22}]/(\det(a_{ij})-1),\ \mathcal{T} = \mathrm{Spec}\,\mathbb{Z}[a_{11},a_{22}]/(a_{11}a_{22}-1).$$

Thus, $\mathcal{T}/S_2 = \mathbb{A}^1$. Let $\tau\colon \mathrm{SL}_2 \to \mathbb{A}^1$ denote the trace map. We define $\mathcal{Y}$ as the integral closure of $\mathbb{A}^1$ in SL_2^d, so we have a diagram

$$\begin{tikzcd}
 & \mathrm{SL}_2^d \arrow[dl, "\psi"'] \arrow[dr, "\pi_w"] \arrow[dd] & \\
\mathcal{Y} \arrow[dr, "\phi"'] & & \mathrm{SL}_2 \arrow[dl, "\tau"] \\
 & \mathbb{A}^1. &
\end{tikzcd}$$

We choose N_w to be divisible by $\deg\phi$ and sufficiently large. Let $k > 1$ be an odd positive integer prime to N_w. Let $\mathcal{T}^{(k)} = \mathcal{T}$ and $\mathcal{A}^{(k)} = \mathbb{A}^1$, and let $p_k\colon \mathcal{T}^{(k)} \to \mathcal{T}$ denote the kth power map, while $q_k\colon \mathcal{A}^{(k)} \to \mathbb{A}^1$ is the "Chebyshev map" defined to make the diagram

$$\begin{tikzcd}
\mathcal{T}^{(k)} \arrow[r] \arrow[d, "p_k"'] & \mathcal{T}^{(k)}/S_2 = \mathcal{A}^{(k)} \arrow[d, "q_k"] \\
\mathcal{T} \arrow[r] & \mathcal{T}/S_2 = \mathbb{A}^1
\end{tikzcd}$$

commute. Note that p_k and $\mathcal{T}^{(k)} \to \mathbb{A}^1$ are not Galois over $\mathbb{Z}$ but become so after base change to $\mathbb{Z}[\zeta_k]$, whereas q_k is not Galois even over $\overline{\mathbb{Q}}$.

We define $\mathcal{X}$, $\mathcal{X}^{(k)}$, and $\mathcal{Y}^{(k)}$ as fiber products:

$$\begin{tikzcd}
 & \mathcal{X}^{(k)} \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathcal{T}^{(k)} \arrow[d] \arrow[dr] & \mathcal{Y}^{(k)} \arrow[dl, crossing over] \arrow[dr, crossing over] & \mathcal{X} \arrow[dl] \arrow[d] \\
\mathcal{A}^{(k)} \arrow[dr, "q_k"'] & \mathcal{T} \arrow[d, "\tau"] & \mathcal{Y} \arrow[dl, "\phi"] \\
 & \mathbb{A}^1. &
\end{tikzcd}$$

By the argument of Lemma 4.2, the map $\mathcal{X} \to \operatorname{Spec} \mathbb{Z}$ has a geometrically irreducible generic fiber. As k is prime to the degree of $\mathcal{X} \to \mathcal{T}$, $\mathcal{X}^{(k)} \to \operatorname{Spec} \mathbb{Z}$ has a geometrically irreducible generic fiber as well. It follows that $\mathcal{X}^{(k)}_{\mathbb{F}_p}$ is a geometrically connected curve for all $p \gg 0$. Let $\mathcal{U} \subset \mathbb{A}^1$ denote a non-empty open subscheme over which τ and ϕ are étale. In particular, $\pm 2 \notin \mathcal{U}$. Let A_p, $A_p^{(k)}$, T_p, $T_p^{(k)}$, Y_p, $Y_p^{(k)}$, X_p, and $X_p^{(k)}$ denote the $\mathbb{F}_p$-fiber of the inverse image of $\mathcal{U}$ in $\mathbb{A}^1$, $\mathcal{A}^{(k)}$, $\mathcal{T}$, $\mathcal{T}^{(k)}$, $\mathcal{Y}$, $\mathcal{Y}^{(k)}$, $\mathcal{X}$, and $\mathcal{X}^{(k)}$, respectively. Thus, $X_p^{(k)} \to X_p$ and $Y_p^{(k)} \to Y_p$ are degree-k finite étale maps of open, non-singular, geometrically irreducible curves over $\mathbb{F}_p$. If $k < p$, then these étale maps extend to tamely ramified maps of the associated non-singular projective curves, so the Riemann-Hurwitz formula says that the genera of $X_p^{(k)}$ and $Y_p^{(k)}$ are $O(k)$. By the Weil bound,

$$|X_p(\mathbb{F}_p)| = p + O(\sqrt{p}),\ |X_p^{(k)}(\mathbb{F}_p)| = p + O(k\sqrt{p}),$$

and

$$|Y_p(\mathbb{F}_p)| = p + O(\sqrt{p}),\ |Y_p^{(k)}(\mathbb{F}_p)| = p + O(k\sqrt{p}).$$

If p is sufficiently large, every point $y \in Y(\mathbb{F}_p)$ lies in $\psi(\mathrm{SL}_2(\mathbb{F}_p)^d)$ by Lemma 2.2. It lies in the image of $X(\mathbb{F}_p) \to Y(\mathbb{F}_p)$ if and only if $\phi(y)$ is the trace of an element of $s \in w(\mathrm{SL}_2(\mathbb{F}_p))$ lying in an $\mathbb{F}_p$-split torus. If not, it is the trace of an element s lying in a non-split torus. In this case, if k divides $p+1$, then the preimage of y in $Y_p^{(k)}(\mathbb{F}_p)$ consists of k-points or none, depending on whether s is or is not divisible by k in $\mathrm{SL}_2(\mathbb{F}_p)$.

Let

$$Z_p = Y(\mathbb{F}_p) \setminus \operatorname{im}(X(\mathbb{F}_p) \to Y(\mathbb{F}_p)),\ Z_p^{(k)} = Y(\mathbb{F}_p)^{(k)} \setminus \operatorname{im}(X(\mathbb{F}_p)^{(k)} \to Y(\mathbb{F}_p)^{(k)}).$$

If $y \in Z_p$, then $\phi(y)$ is the trace of $s \in w(\mathrm{SL}_2(\mathbb{F}_p))$ such that the centralizer of s is a non-split maximal torus of SL_2. If k divides $\frac{p+1}{2}$, then the map $Z_p^{(k)} \to Z_p$ is k to 1, since every non-split semisimple element of $\mathrm{SL}_2(\mathbb{F}_p)$ which is divisible by k has k kth roots. Our goal is to show that

$$Z_p^\circ := Z_p \setminus \bigcup_{\substack{k|(p+1)/2 \\ k>1}} \operatorname{im}(Z_p^{(k)} \to Z_p)$$

is not empty. By Möbius inversion,

$$\begin{aligned}|Z_p^\circ| &= \sum_{k|(p+1)/2} \mu(k)|\mathrm{im}(Z_p^{(k)} \to Z_p)| = \sum_{k|(p+1)/2} \mu(k)\frac{|Z_p^{(k)}|}{k} \\ &= \sum_{k|(p+1)/2} (\mu(k)\frac{p}{2k} + O(\sqrt{p})) \\ &= \frac{\phi((p+1)/2)}{(p+1)/2} + O(\sqrt{p}d((p+1)/2)),\end{aligned}$$

where $\phi(m)$ and $d(m)$ denote the Euler ϕ-function and the number of divisors. As $d(m) = o(m^\epsilon)$ and $\frac{m}{\phi(m)} = o(m^\epsilon)$, for p sufficiently large we have Z_p° non-empty. It follows that there exists $s \in w(\mathrm{SL}_2(\mathbb{F}_p))$ non-split semisimple and not divisible by any odd integer. As p is 1 (mod 4), the order of s must be $p+1$ or $\frac{p+1}{2}$. □

5. Alternating groups, I: Analytic number theory

In this section we deduce Theorems 1.3, 1.5, and 1.10 from the theorems of §4 and some deep results from analytic number theory.

We begin with the proof of Theorem 1.3.

Proof. We are given a non-identity word w. By Theorem 4.3, for every prime $p > N_w$ such that $p \equiv 1 \pmod 4$ and $p+1$ is not divisible by any odd prime $\leq N_w$, there exist $z_{p,1}, \ldots, z_{p,d} \in \mathrm{SL}_2(\mathbb{F}_p)$ such that $w(z_{p,1}, \ldots, z_{p,d})$ is of order $\frac{p+1}{2}$ or $p+1$. The action of $\mathrm{SL}_2(\mathbb{F}_p)$ on $\mathbb{P}^1(\mathbb{F}_p)$ determines an injective homomorphism $\mathrm{PSL}_2(\mathbb{F}_p) \to A_{p+1}$. Let $\zeta_{p,i}$ denote the image of $z_{p,i}$. As $p+1$-cycles are odd, $w(\zeta_{p,1}, \ldots, \zeta_{p,d})$ consists of two $\frac{p+1}{2}$-cycles.

Next we claim that for every integer M sufficiently large in terms of N_w, there exists an integer r in the interval $[M-11, M]$ such that $r-3$ is the sum of three primes p_i such that $p_i > N_w$, $p_i \equiv 1 \pmod 4$, and $p_i + 1$ is not divisible by any odd prime $\leq N_w$. We do this by applying Ayoub's version of Vinogradov's three primes theorem [Ay], asserting that every sufficiently large integer r can be written in at least $cr^2 \log^{-3} r$ ways as a sum of three primes lying in any specified residue classes a_1, a_2, $a_3 \pmod m$ as long as r is congruent to $a_1 + a_2 + a_3 \pmod m$. For r sufficiently large, this is enough to ensure that p_1, p_2, p_3 can be chosen to be larger than N_w.

We choose $r = 12\lfloor \frac{M-6}{12} \rfloor + 3$ so that r is the sum of three primes each congruent to 1 (mod 12). If p_i is such a prime, $p_i + 1$ is not divisible by 3. For every prime ℓ greater than 3, every residue class (mod ℓ) can be written as the sum of three residue classes from 1 to $\ell - 2$, so we can impose (mod ℓ) conditions on p_1, p_2, p_3 consistent with $\ell \nmid p_i + 1$ and $p_1 + p_2 + p_3 + 3 \equiv r \pmod \ell$. By the Chinese remainder theorem and Ayoub's result, the element

$$w((\zeta_{p_1,1}, \zeta_{p_2,1}, \zeta_{p_3,1}), \ldots (\zeta_{p_1,d}, \zeta_{p_2,d}, \zeta_{p_3,d})) \in A_{p_1+1} \times A_{p_2+1} \times A_{p_3+1} \subset A_{r+3}$$

consists of 6 cycles, so by the inclusion $A_{r+3} \subset A_M$, there is an element in $w(A_M)$ with at most 17 cycles, of which at most 6 are non-trivial. We can construct a sequence of elements $\sigma_M \in A_M$ in this way for which the bound N_w tends to ∞ as M goes to ∞. □

Theorem 5.1. *For every $\epsilon > 0$ and $\frac{11}{20} < \alpha < 1$ there exists a constant $\delta > 0$ such that for all positive integers m, the number of primes p between $m - m^\alpha$ and m which satisfy* (4.1) *is at least $\frac{\delta m^\alpha}{\log m} - 1$.*

Proof. First, it suffices to prove the theorem for m sufficiently large, since δ can always be reduced to make $\frac{\delta m^\alpha}{\log m} - 1$ negative for any particular m. Second, we may replace (4.1) with the condition

$$\sum_{\substack{q \mid p^2+p+1 \\ q \text{ prime}}} \frac{1}{q} < \epsilon_2.$$

Indeed,

$$\log \frac{\phi(p^2+p+1)}{p^2+p+1} = \sum_{\substack{q \mid p^2+p+1 \\ q \text{ prime}}} \log(1 - \frac{1}{q}) > -2 \sum_{\substack{q \mid p^2+p+1 \\ q \text{ prime}}} \frac{1}{q},$$

so it suffices to choose $\epsilon_2 < \frac{-\log(1-\epsilon)}{2}$.

We fix a large positive integer k. Let $P_{k,m}$ denote the set of primes in $[m - m^\alpha, m]$ which are 2 (mod 3) and 1 modulo every other prime $q \le k$. Thus,

$$\sum_{p \in P_{k,m}} \sum_{\substack{q \mid p^2+p+1 \\ q \text{ prime}}} \frac{1}{q} = \sum_{q > k} \sum_{\substack{p \in P_{k,m} \\ p^2+p+1 \in q\mathbb{Z}}} \frac{1}{q}. \tag{5.1}$$

We now use an estimate for the number of primes in short intervals. We need to further restrict the primes to lie in an arithmetic progression. We therefore use the result of [BHP]. This asserts, in particular, that if a and b are relatively prime integers, $a \le \log^2 m$, and m is sufficiently large in absolute terms, then the number of primes $p \equiv b \pmod a$ such that $p \in [m - m^\alpha, m]$ differs by at most 1% from $\frac{m^\alpha}{\phi(a)\log m}$. Let a_k denote the product of all primes $\le k$. There are at most two residue classes (mod qa_k) which are congruent to 2 (mod 3), congruent to 1 modulo every other prime $\le k$ and congruent to a root of $x^2 + x + 1 \pmod q$. Therefore, the contribution of a particular value q to the right-hand side of (5.1) is at most

$$\frac{2.02 m^\alpha}{\phi(a_k)(q-1)q\log m}$$

assuming that k is sufficiently large and $a_k q \le \log^2 m$, while

$$|P_{k,m}| \ge \frac{.99 m^\alpha}{\phi(a_k)\log m}.$$

Summing over q,

$$\sum_{k < q \le \frac{\log^2 m}{a_k}} \sum_{\substack{p \in P_{k,m} \\ p^2+p+1 \in q\mathbb{Z}}} \frac{1}{q} = O\left(\frac{m^\alpha}{\phi(a_k)k\log m}\right).$$

For $q > \frac{\log^2 m}{a_k}$ we use the naive estimate that there are at most $\frac{m^\alpha}{a_k q} + 1$ primes in $[m - m^\alpha, m]$ in a given residue class (mod $a_k q$) and therefore,

$$\sum_{\substack{p \in P_{k,m} \\ p^2+p+1 \in q\mathbb{Z}}} \frac{1}{q} \le \frac{2m^\alpha}{a_k q^2} + \frac{2}{q}.$$

We need only consider primes $q \leq m^2 + m + 1$, so

$$\sum_{\frac{\log^2 m}{a_k} < q \leq m^2+m+1} \sum_{\substack{p \in P_{k,m} \\ p^2+p+1 \in q\mathbb{Z}}} \frac{1}{q} = O(m^\alpha / \log^2 m).$$

Fixing k and sending m to infinity, it follows that the sum (5.1) is $O(\frac{m^\alpha}{\phi(a_k)k \log m})$ and therefore that the mean value of the (positive) summand on the left-hand side is $O(1/k)$. If k is sufficiently large, the fraction of primes in $P_{k,m}$ for which $\sum_{\substack{q | p^2+p+1 \\ q \text{ prime}}} \frac{1}{q} < \epsilon_2$ is at least $1/2$, and therefore, the fraction of all primes in $[m - m^\alpha, m]$ for which this is true can be bounded away from zero. □

We now easily deduce Theorem 1.5.

Proof. Fix ϵ between 0 and $1/3$ and let p be a prime satisfying condition (4.1). In particular, this implies that $n := p^2 + p + 1$ is not divisible by 3, so the center of $\mathrm{SL}_3(\mathbb{F}_p)$ is trivial. Then $\mathrm{SL}_3(\mathbb{F}_p)$ maps injectively to A_n (via its action on a parabolic subgroup). By Theorem 4.1 there exists an element $g \in w(\mathrm{SL}_3(\mathbb{F}_p))$ of order n. We easily see that the image of g in A_n is an n-cycle lying in $w(A_n)$.

Finally, by Theorem 5.1 there are infinitely many such primes p, proving the result. □

By choosing α in Theorem 5.1 sufficiently close to 1, we also prove the remark following the statement of Theorem 1.5.

We can now prove Theorem 1.10

Proof. Fix a word w. Fix α between $\frac{11}{20}$ and 1 and choose $\beta \in (11/20, \alpha)$. By Theorem 5.1 and Theorem 4.1, there exists n such that for all $m = m_1 > n$, there are at least $m^{\beta/2}$ primes p in $[m^{1/2} - m^{\alpha/2}/2, m - m^{\alpha/2}/4]$ for which $w(A_{p^2+p+1})$ contains a $p^2 + p + 1$-cycle. We choose p_1 to be among these primes and define $m_2 = m_1 - (p_1^2 + p_1 + 1)$. If n is originally chosen large enough and $m > n$, then

$$m^{\frac{1+\beta}{2}} < m_2 < m^{\frac{1+\alpha}{2}}.$$

We now iterate this process, choosing $p_2 \in [m_2^{1/2} - m_2^{\alpha/2}/2, m_2^{1/2} - m_2^{\alpha/2}/4]$ and so on, until $m_r < n$. In particular,

$$m^{(\frac{1+\beta}{2})^i} < m_{i+1} < m^{(\frac{1+\alpha}{2})^i}$$

for $0 \leq i < r$. Therefore,

$$m = m_r + \sum_{i=1}^{r-1} p_i^2 + p_i + 1,$$

and $w(A_m)$ contains a cycle which is a product of $p_i^2 + p_i + 1$-cycles and m_r 1-cycles. The order of the conjugacy class of such a cycle is

$$\frac{m!}{m_r! \prod_{i=1}^{r-1}(p_i^2 + p_i + 1)} > \frac{Cm!}{\prod_{i=1}^{r-1} m_i} > \frac{Cm!}{\prod_{i=0}^{r-2} m^{(\frac{1+\alpha}{2})^i}} > \frac{Cm!}{m^{\frac{2}{1-\alpha}}},$$

where C does not depend on m. The number of choices for $p_1, p_2, \ldots, p_{r-1}$ is at least

$$\prod_{i=1}^{r-1} m_i^{\frac{\beta}{2}} > \prod_{i=0}^{r-2} m^{\frac{\beta}{2}(\frac{1+\beta}{2})^i} = m^{\frac{\beta}{1-\beta}\left(1-\left(\frac{1+\beta}{2}\right)^{r-1}\right)}.$$

Thus, the union of all conjugacy classes of this kind in $w(A_m)$ has cardinality at least

$$\frac{Cm!m^{\frac{\beta}{1-\beta}\left(1-\left(\frac{1+\beta}{2}\right)^{r-1}\right)}}{m^{\frac{2}{1-\alpha}}}.$$

By taking m sufficiently large, we can make r as large as we please. We can also make α and β as close to $\frac{11}{20}$ as we wish. Therefore, we may make

$$\frac{2}{1-\alpha} - \frac{\beta}{1-\beta}\left(1-\left(\frac{1+\beta}{2}\right)^{r-1}\right)$$

as close to

$$\frac{2-\frac{11}{20}}{1-\frac{11}{20}} = \frac{29}{9}$$

as we wish. □

6. Alternating groups, II: A combinatorial construction

In general it is difficult to say when a given conjugacy class in a symmetric group appears in the product of two other conjugacy classes. In this section we present an explicit construction that can be used to show that certain conjugacy classes are contained in the squares of other classes. This constitutes the elementary part of the proof of Theorem 1.1.

We denote the number of fixed points of a permutation $\sigma \in S_n$ by $\mathrm{fix}(\sigma)$.

Proposition 6.1. *Let n be a positive integer and $\alpha, \beta \in S_n$ permutations belonging to conjugacy classes A and B, respectively. If*

$$\mathrm{fix}(\beta) \geq 7\mathrm{cyc}(\alpha)$$

and β is even, then $B \subset A^2$.

Proof. Let $[a, b]$ denote the sequence of consecutive integers $a \leq x \leq b$; such a sequence will be called an *interval of length* $1 + b - a$. Given sequences $S_1, \ldots, S_r$, let $j(S_1, \ldots, S_r)$ denote their concatenation. If S is a sequence and k is an integer, $T_k(S)$ is the sequence obtained by adding k to each element of S. If S is a k-term sequence of distinct integers in $[1, n]$, let (S) denote the corresponding k-cycle in S_n. Let $0 = a_0 < a_1 < \ldots < a_m = n$ be defined so that

$$\gamma = ([a_0 + 1, a_1])([a_1 + 1, a_2]) \cdots ([a_{m-1} + 1, a_m]) \in A.$$

We want to find $\delta \in A$ such that $\gamma\delta \in B$.

Let b_k denote the number of k-cycles in β. Let

$$\begin{aligned}
c_1 &= b_1 = \mathrm{fix}(\beta) \geq 7\mathrm{cyc}(\alpha) = 7m,\\
c_2 &= b_2,\\
c_3 &= b_3 + b_5 + b_7 + \cdots,\\
c_4 &= b_4 + b_6 + b_8 + \cdots,\\
d_3 &= c_3,\\
d_4 &= \lfloor c_2/2 \rfloor,\\
d_6 &= c_2 - 2d_4,\\
d_8 &= \lfloor c_4/2 \rfloor.
\end{aligned}$$

As $b_2+b_4+b_6+\cdots$ is even, so is c_2+c_4, so c_2 and c_4 are both even or both odd and $c_4=2d_8+d_6$.

Our first task is a packing problem: to find a set Σ consisting of d_i intervals of length i for $i=3,4,6,8$, each contained in some $[a_k+1,a_{k+1}]$, such that the resulting intervals are mutually disjoint. To show that such a packing is possible, we iterate, starting from $k=0$ and packing as many intervals of length $i\in\{3,4,6,8\}$ as possible (up to a limit of d_i intervals of length i) into each interval $[a_k+1,a_{k+1}]$ in turn, starting from the right endpoint and working toward the left, so the union of intervals at any point in the construction is "right-justified." For each k, we denote by $I_{k,1},I_{k,2},\ldots,I_{k,p_k}$ the successive elements of Σ in $[a_k+1,a_{k+1}]$.

If the packing process terminates before all the upper limits d_i have been achieved, then the number of free spaces in all the $[a_k+1,a_{k+1}]$ combined is $\leq 7m$. Since $b_1=\mathrm{fix}(\beta)\geq 7m$, we have

$$3d_3+4d_4+6d_6+8d_8=2c_2+3c_3+4c_4\leq b_2+b_3+b_4+\cdots\leq n-7m,$$

which is a contradiction. It follows that the packing is indeed possible, so

$$|\{(k,l)\colon |I_{k,l}|=i\}|=d_i$$

for $i=3,4,6,8$.

We define l_k so that for each k from 0 to $m-1$, the union of the intervals $I_{k,1},I_{k,2},\ldots,I_{k,p_k}$ is $[l_k+1,a_{k+1}]$. We write $e_{k,i}$ for the left endpoint of $I_{k,i}$ and define

$$S_{k,i}=\begin{cases}T_{e_{k,i}}(2,0,1) & \text{if } |I_{k,i}|=3,\\ T_{e_{k,i}}(3,0,1,2) & \text{if } |I_{k,i}|=4,\\ T_{e_{k,i}}(5,2,0,3,4,1) & \text{if } |I_{k,i}|=6,\\ T_{e_{k,i}}(7,5,2,0,3,6,4,1) & \text{if } |I_{k,i}|=8.\end{cases} \tag{6.1}$$

Note in particular that the first term of $S_{k,i}$ is the last term of $I_{k,i}$. If $|I_{k,i}|=3$ (resp. $|I_{k,i}|=6$), we say that $e_{k,i}+1$ is a *special point of odd type* (resp. *even type*). Intervals of length 4 in Σ have no special points. If $|I_{k,i}|=8$, there are two special points of even type in the interval: $e_{k,i}+1$ and $e_{k,i}+6$. We assign each special point a label, i.e., a positive integer λ, in such a way that there are $b_{2\lambda+1}$ special points of odd type with label λ and $b_{2\lambda+2}$ special points of even type with label λ.

Let X_k denote the interval $[a_k+1,l_k]$ and Y_k the subset of X_k consisting of a_k+x such that x is odd and $a_k+x+1\leq l_k$. Thus $|X_k|\leq 2|Y_k|+1$. Setting

$$X=X_0\cup X_1\cup\cdots\cup X_{m-1},\ Y=Y_0\cup Y_1\cup\cdots\cup Y_{m-1},$$

we have $|X|\leq 2|Y|+m$. Thus,

$$\begin{aligned}|Y|&\geq\frac{n-3d_3-4d_4-6d_6-8d_8-m}{2}=\frac{n-2c_2-3c_3-4c_4-m}{2}\\ &=\frac{-m+b_1}{2}+\sum_{i=5}^{\infty}\lfloor\frac{i-3}{2}\rfloor b_i\geq 3m+\sum_{i=5}^{\infty}\lfloor\frac{i-3}{2}\rfloor b_i.\end{aligned} \tag{6.2}$$

There exists a permutation $\epsilon\in S_n$ with the following properties:

- Every cycle of length ≥ 2 contains exactly one element of $[1,n]\setminus Y$, and this element is special.
- The length of a cycle containing a special point of label λ is λ.

The existence of ϵ follows from (6.2).

For $0 \leq k < m$, we define a cycle

$$\delta_k = (j(S_{k,1}, \ldots, S_{k,p_k}, R_k)),$$

where R_k is the reverse of the sequence $[a_k + 1, l_k]$. Thus, $\delta_0 \delta_1 \cdots \delta_{m-1}$ belongs to A. We define

$$\delta = \epsilon \delta_0 \cdots \delta_{m-1} \epsilon^{-1} \in A.$$

We claim $\gamma\delta$ belongs to B, i.e., that it has exactly b_j j-cycles for each j. As $\sum_j j b_j = n$, it suffices to prove that there are at least b_j j-cycles for each j. There are four cases to check: $j = 1$, $j = 2$, $j \geq 3$ odd, and $j \geq 4$ even.

For $j = 1$, we note that every element of $x \in R_k$ such that x and $x - 1$ are fixed by ϵ satisfies $\gamma\delta(x) = \gamma(x - 1) = x$. Thus,

$$\begin{aligned}
\mathrm{fix}(\gamma\delta) &\geq n - \sum_{k,i} |I_{k,i}| - 2|Y \setminus \mathrm{fix}(\epsilon)| \\
&= n - 3d_3 - 4d_4 - 6d_6 - 8d_8 - 2|Y \setminus \mathrm{fix}(\epsilon)| \\
&= n - 2c_2 - 3c_3 - 4c_4 - 2|Y \setminus \mathrm{fix}(\epsilon)| \\
&= n - 2b_2 - 3b_3 - 4b_4 - 3b_5 - 4b_6 - \cdots - 2|Y \setminus \mathrm{fix}(\epsilon)| \\
&= n - 2b_2 - 3b_3 - 4b_4 - 5b_5 - 6b_6 - \cdots \\
&= b_1.
\end{aligned}$$

For $j = 2$ we consider all $I_{k,i} \in \Sigma$ which are of length 4. For each such interval, $\gamma\delta$ maps

$$\begin{aligned}
e_{k,i} &\mapsto \gamma\delta_k(e_{k,i}) = \gamma(e_{k,i} + 1) = e_{k,i} + 2, \\
e_{k,i} + 1 &\mapsto \gamma\delta_k(e_{k,i} + 1) = \gamma(e_{k,i} + 2) = e_{k,i} + 3, \\
e_{k,i} + 2 &\mapsto \gamma\delta_k(e_{k,i} + 2) = \gamma(e_{k,i} - 1) = e_{k,i}, \\
e_{k,i} + 3 &\mapsto \gamma\delta_k(e_{k,i} + 3) = \gamma(e_{k,i}) = e_{k,i} + 1.
\end{aligned}$$

This produces a total of $2d_4$ 2-cycles. If there is an interval $I_{k,i}$ of length 6, then $\gamma\delta$ maps

$$\begin{aligned}
e_{k,i} + 5 &\mapsto \gamma\delta_k(e_{k,i} + 5) = \gamma(e_{k,i} + 2) = e_{k,i} + 3, \\
e_{k,i} + 3 &\mapsto \gamma\delta_k(e_{k,i} + 3) = \gamma(e_{k,i} + 4) = e_{k,i} + 5.
\end{aligned}$$

Thus, $\gamma\delta$ has at least $2d_4 + d_6 = c_2 = b_2$ cycles of length 2.

If $j \geq 3$ is odd, let $\lambda = (j - 1)/2$. There are b_j special points of odd type with label λ. Each belongs to an interval $I_{k,i}$ of length 3. The special point in such an interval is $e_{k,i} + 1$. Thus $\gamma\delta$ maps

$$\begin{aligned}
e_{k,i} &\mapsto \epsilon(e_{k,i} + 1) + 1, \\
\epsilon^r(e_{k,i} + 1) + 1 &\mapsto \epsilon^{r+1}(e_{k,i} + 1) + 1,\ 1 \leq r < \lambda, \\
e_{k,i} + 2 &\mapsto e_{k,i} + 1, \\
\epsilon^{r+1}(e_{k,i} + 1) &\mapsto \epsilon^r(e_{k,i} + 1),\ 1 \leq r < \lambda, \\
\epsilon(e_{k,i} + 1) &\mapsto e_{k,i},
\end{aligned}$$

producing a j-cycle. It follows that $\gamma\delta$ has at least b_j j-cycles.

If $j \geq 4$ is even, let $\lambda = j/2 - 1$. There are b_j special points of even type with label λ. Each special point with label λ in an interval $I_{k,i}$ of length 8 contributes a j-cycle because $\gamma\delta$ maps

$$\begin{aligned}
e_{k,i} &\mapsto e_{k,i} + 4,\\
e_{k,i} + 4 &\mapsto \epsilon(e_{k,i} + 1) + 1,\\
\epsilon^r(e_{k,i} + 1) + 1 &\mapsto \epsilon^{r+1}(e_{k,i} + 1) + 1,\ 1 \leq r < \lambda,\\
e_{k,i} + 2 &\mapsto e_{k,i} + 1,\\
\epsilon^{r+1}(e_{k,i} + 1) &\mapsto \epsilon^r(e_{k,i} + 1),\ 1 \leq r < \lambda,\\
\epsilon(e_{k,i} + 1) &\mapsto e_{k,i},
\end{aligned}$$

and

$$\begin{aligned}
e_{k,i} + 3 &\mapsto \epsilon(e_{k,i} + 6) + 1,\\
\epsilon^r(e_{k,i} + 6) + 1 &\mapsto \epsilon^{r+1}(e_{k,i} + 6) + 1,\ 1 \leq r < \lambda,\\
e_{k,i} + 7 &\mapsto e_{k,i} + 6,\\
\epsilon^{r+1}(e_{k,i} + 6) &\mapsto \epsilon^r(e_{k,i} + 6),\ 1 \leq r < \lambda,\\
\epsilon(e_{k,i} + 6) &\mapsto e_{k,i} + 5,\\
e_{k,i} + 5 &\mapsto e_{k,i} + 3.
\end{aligned}$$

Likewise, if $I_{k,i}$, of length 6, has a special point with label λ, then $\gamma\delta$ maps

$$\begin{aligned}
e_{k,i} &\mapsto e_{k,i} + 4,\\
e_{k,i} + 4 &\mapsto \epsilon(e_{k,i} + 1) + 1,\\
\epsilon^r(e_{k,i} + 1) + 1 &\mapsto \epsilon^{r+1}(e_{k,i} + 1) + 1,\ 1 \leq r < \lambda,\\
e_{k,i} + 2 &\mapsto e_{k,i} + 1,\\
\epsilon^{r+1}(e_{k,i} + 1) &\mapsto \epsilon^r(e_{k,i} + 1),\ 1 \leq r < \lambda,\\
\epsilon(e_{k,i} + 1) &\mapsto e_{k,i}.
\end{aligned}$$

Thus, again we have at least b_j j-cycles, and this finishes the proof. □

7. Alternating groups, III: Characters and probability

Here we prove a character bound for symmetric groups which may have some independent interest and combine it with Proposition 6.1 and a probabilistic argument to prove that conjugacy classes of permutations which contain a small number of cycles have the property that their squares cover all of A_n.

This proves Theorem 1.1 and answers an old question of J. L. Brenner (but falls short of his strong conjecture [Br]). For our purposes, however, it is more than enough; combining it with Theorem 1.3, we deduce Theorem 1.6, giving a best possible solution for Waring's problem for A_n. This will complete the proof of all results stated in the Introduction.

Recall that the irreducible characters $\chi \in Irr(S_n)$ are parameterized by partitions λ of n, which correspond to the Young diagram. Let χ_λ be the character corresponding to a diagram λ.

We define *layers* of a diagram λ as follows. The first layer consists of the first row and column of λ. Once we remove the first layer, we obtain a smaller diagram λ'. The layers of λ are defined recursively as the layers of λ' together with the first layer of λ.

We shall use the Murnaghan-Nakayama Rule [Ja, 21.1]. By a *rim r-hook* ν in a λ-diagram, we mean a connected part of the rim containing r nodes, which can be removed to leave a proper diagram, denoted by $\lambda\backslash\nu$. If, moving from right to left, the rim hook ν starts in row i and finishes in column j, then the *leg-length* $l(\nu)$ is defined to be the number of nodes below the ij-node in the λ-diagram.

Proposition 7.1 (Murnaghan-Nakayama Rule)**.** *Let $\rho\pi \in S_n$, where ρ is an r-cycle and π is a permutation of the remaining $n-r$ points. Then*

$$\chi_\lambda(\rho\pi) = \sum_\nu (-1)^{l(\nu)} \chi_{\lambda\backslash\nu}(\pi),$$

where the sum is over all rim r-hooks ν in a λ-diagram.

We shall now bound the character values of a permutation as a function of its number of cycles alone.

Theorem 7.2. *Let $\sigma \in S_n$ be a permutation with k cycles (including 1-cycles). Then*

$$|\chi(\sigma)| \leq 2^{k-1}k!$$

for all irreducible characters χ of S_n.

Proof. We argue by induction on k. For $k=1$ our permutation σ is an n-cycle, and it is a well-known consequence of Proposition 7.1 that $|\chi(\sigma)| \leq 1$, and moreover, if $\chi(\sigma) \neq 0$, then the Young diagram of χ consists of a single layer.

Suppose now that $k \geq 2$ and let $\chi = \chi_\lambda$. Write $\sigma = \rho\pi$ where ρ is an r-cycle and π is a permutation on the remaining $n-r$ points. We now apply the Murnaghan-Nakayama Rule above. Since π decomposes into $k-1$ cycles, induction yields

$$|\chi_{\lambda\backslash\nu}(\pi)| \leq 2^{k-2}(k-1)!$$

for all rim r-hooks ν in the diagram λ.

To complete the proof, we may assume $\chi_\lambda(\sigma) \neq 0$.

Claim. The number of rim r-hooks in λ is at most $2k$.

To show this, first note that, by repeatedly applying the Murnaghan-Nakayama Rule, we see that λ has at most k layers (otherwise $\chi_\lambda(\sigma) = 0$).

Now, each rim r-hook ν of λ has a starting point, its rightmost upmost point, and an endpoint, its leftmost downmost point. Each of these points determines the rim r-hook uniquely (by going r steps on the boundary in the suitable direction). We define the starting point and the endpoint of each layer of the diagram λ in a similar manner.

Since the remaining part $\lambda\backslash\nu$ of the diagram should be connected, either the starting point of ν is the starting point of some layer of λ or the endpoint of ν is the endpoint of some layer of λ. Since there are at most k layers, it now follows that the number of rim r-hooks in λ is at most $2k$, proving the claim.

The Murnaghan-Nakayama Rule now expresses $\chi_\lambda(\sigma)$ as a sum of at most $2k$ terms, each of absolute value at most $2^{k-2}(k-1)!$. This yields

$$|\chi_\lambda(\sigma)| \leq 2k \cdot 2^{k-2}(k-1)! = 2^{k-1}k!,$$

completing the proof of the theorem. □

Note that $|\chi(\sigma)|$ may be close to $(k!)^{1/2}$, for instance take $\sigma = 1$ (so $k = n$) and χ a character of highest degree. This shows that the upper bound in Theorem 7.2 cannot be significantly improved, at least for large k.

Given conjugacy classes $C_i = x_i^G$ $(i = 1, 2)$ in a finite group G, let P_{C_1,C_2} denote the distribution of the random variable $y = y_1y_2$, where $y_i \in C_i$ is randomly chosen with uniform distribution on C_i. The following is standard.

Lemma 7.3. *With the above notation we have, for $g \in G$,*

$$P_{C_1,C_2}(g) = |G|^{-1} \sum_{\chi \in Irr(G)} \frac{\chi(x_1)\chi(x_2)\chi(g^{-1})}{\chi(1)}.$$

For a finite group G define

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

where s is a real number.

We need the following two results from [LiSh2], related to character degrees.

Lemma 7.4. *For $s > 0$ we have $\zeta_{S_n}(s) = 2 + O(n^{-s})$.*

Lemma 7.5. *Let $\lambda = \lambda_1, \ldots, \lambda_m$ be a partition of n such that $\lambda_1 \geq m$. Let $t = n - \lambda_1$. Then*

(i) $\chi_\lambda(1) \geq \binom{n-t}{t}$.

(ii) If $t \geq \epsilon n$ for some $\epsilon > 0$, then $\chi_\lambda(1) \geq c^n$ where $c > 1$ depends on ϵ.

We can now prove Theorem 1.1.

Proof. Throughout this proof, we assume without further comment that n is sufficiently large. Let σ be a permutation in S_n with

$$\mathrm{cyc}(\sigma) \leq n^{1/128}.$$

We have to show that $(\sigma^{S_n})^2 = A_n$.

We first claim that

$$|\chi(\sigma)| \leq \chi(1)^{1/63}, \tag{7.1}$$

for all irreducible characters χ of S_n.

This is clear if $\chi(1) = 1$ so suppose $\chi = \chi_\lambda$ is a non-linear character, where $\lambda = \lambda_1, \ldots, \lambda_m$ is a partition. Since we are only interested in absolute values, we may replace a partition by its transpose and assume that $\lambda_1 \geq m$ (so Lemma 7.5 is applicable).

Write $\lambda_1 = n - t$ and $k = cyc(\sigma)$. Then Theorem 7.2 and our assumption on k yield

$$|\chi_\lambda(\sigma)| \leq 2^{k-1}k! \leq (n^{1/128})^{n^{1/128}}. \tag{7.2}$$

If $t \geq n/3$, Lemma 7.5(ii) gives an exponential lower bound on $\chi_\lambda(1)$, so (7.1) follows.

If $n^{1/127} \leq t < n/3$, then Lemma 7.5(i) yields

$$\chi(1) \geq \binom{n-t}{t} \geq 2^t \geq 2^{n^{1/127}}.$$

Combining this with (7.2), we obtain (7.1).

Finally, suppose $1 \leq t < n^{1/127}$. Let f denote the number of fixed points of σ. We use [MS, (14)] to show that

$$|\chi(\sigma)| \leq t! \sum_{a,b\geq 0, a+2b\leq t} \binom{f}{a}\binom{k-f}{b} \leq t! \sum_{0\leq i\leq t} \binom{k}{i} \leq t! \cdot (t+1) \cdot k^t.$$

Using the bounds $k \leq k_0 := n^{1/128}$ and $t \leq t_0 := n^{1/127}$, this gives

$$|\chi(\sigma)| \leq (t_0 k_0)^t = n^{(1/128+1/127)t}.$$

It is easy to see that for $t \leq n^{1/127}$ and fixed $\delta > 0$ we have

$$n^{(1-1/127-\delta)t} \leq \binom{n-t}{t}.$$

Choosing δ such that $1/128 + 1/127 = (1 - 1/127 - \delta) \cdot 1/63$ and noting that $\delta > 0$, it follows that

$$|\chi(\sigma)| \leq \binom{n-t}{t}^{1/63} \leq \chi(1)^{1/63}.$$

This completes the proof of (7.1).

Now, let $C = \sigma^{S_n}$ and let π denote an even permutation.

If π has more than $7n^{1/128}$ fixed points, then we have $\pi \in C^2$ by Proposition 6.1. We therefore assume from now on that $\text{fix}(\pi) < 7n^{1/128}$. By [MS, Theorem B], this implies

$$|\chi(\pi^{-1})| \leq |\chi(1)|^{30/31}.$$

By Lemma 7.3 we have

$$P_{C,C}(\pi) = \frac{1}{n!} \sum_{\chi\in Irr(S_n)} \frac{\chi(\sigma)^2\chi(\pi^{-1})}{\chi(1)}.$$

The condition on the sign of π shows that the contribution of the linear characters of S_n to $P_{C,C}(\pi)$ is $2/n!$. On the other hand,

$$\Big| \sum_{\{\chi:\ \chi(1)>1\}} \frac{\chi(\sigma)^2\chi(\pi^{-1})}{\chi(1)} \Big| \leq \sum_{\{\chi:\ \chi(1)>1\}} \frac{(\chi(1)^{1/63})^2\chi(1)^{30/31}}{\chi(1)} = \sum_{\{\chi:\ \chi(1)>1\}} \chi(1)^{-s},$$

where $s = 1/31 - 2/63 > 0$. Combining this with Lemma 7.4, we conclude that

$$|P_{C,C}(\pi) - 2/n!| \leq \frac{1}{n!}(\zeta_{S_n}(s) - 2) = O(n^{-s}/n!).$$

This implies $P_{C,C}(\pi) > 0$, so $\pi \in C^2$.

The theorem is proved. □

Combining various tools above, we can finally prove Theorem 1.6.

Proof. We have to show, given words $w_1, w_2 \neq 1$, that $w_1(A_n)w_2(A_n) = A_n$ for all $n \geq N(w_1, w_2)$.

We use Theorem 1.3 and its notation. Let $N = N(w_1, w_2) := \max_{i=1,2} N(w_i)$, and let $n \geq N$. Then Theorem 1.3 shows that there exists a permutation $\sigma_n \in w_1(A_n) \cap w_2(A_n)$ consisting of at most 17 cycles (of which some pairs have the same length, so $\sigma_n^{A_n} = \sigma_n^{S_n}$). Clearly $\sigma_n^{S_n} \subseteq w_1(A_n) \cap w_2(A_n)$ and by Theorem 1.1 we have

$$w_1(A_n)w_2(A_n) \supseteq (w_1(A_n) \cap w_2(A_n))^2 \supseteq (\sigma_n^{S_n})^2 = A_n.$$

The theorem is proved. □

8. Intersection theorems

Our methods enable us to deduce somewhat surprising results concerning intersections of the form $\bigcap_{i=1}^k w_i(G)$, where $w_1, \ldots, w_k$ are given words. Note that in free groups such intersections may well be trivial. However, we can prove that in the groups considered in this paper such intersections are very large. More precisely, we have

Theorem 8.1. *Let $k \geq 1$ and let $w_1, \ldots, w_k$ be non-trivial words.*

(i) There exists $N = N(w_1, \ldots, w_k)$ such that for all $n \geq N$ we have

$$(w_1(A_n) \cap \ldots \cap w_k(A_n))^2 = A_n.$$

(ii) For every $\epsilon > 0$ there exists $N = N(w_1, \ldots, w_k, \epsilon)$ such that

$$|w_1(A_n) \cap \ldots \cap w_k(A_n)| \geq n^{-\frac{29}{9}-\epsilon}|A_n|.$$

Indeed, part (i) follows from Theorems 1.1 and 1.3, using the fact that, for $n \gg 0$, $\sigma_n^{S_n} \subseteq \bigcap_{i=1}^k w_i(A_n)$.

The proof of part (ii) is essentially that of Theorem 1.10.

Our next result is an intersection theorem for groups of Lie type.

Theorem 8.2. *Let $k \geq 1$ and let $w_1, \ldots, w_k$ be non-trivial words. Let G be a simply connected almost simple algebraic group over a finite field $\mathbb{F}_q$.*

(i) There is a positive constant c depending only on $w_1, \ldots, w_k$ and $\dim G$ such that

$$|w_1(G(\mathbb{F}_q)) \cap \ldots \cap w_k(G(\mathbb{F}_q))| \geq c|G(\mathbb{F}_q)|.$$

(ii) There is a number N depending only on $w_1, \ldots, w_k$ such that, if G has rank r and is not of type A_r or ${}^2A_r$ and if $|G(\mathbb{F}_q)| \geq N$, then

$$|w_1(G(\mathbb{F}_q)) \cap \ldots \cap w_k(G(\mathbb{F}_q))| \geq cr^{-1}|G(\mathbb{F}_q)|,$$

where $c > 0$ is an absolute constant.

(iii) There is a number N depending only on $w_1, \ldots, w_k$ and $\dim G$ such that, if $\Gamma = G(\mathbb{F}_q)/Z(G(\mathbb{F}_q))$ is a finite simple group associated with G and if $|\Gamma| \geq N$, then

$$(w_1(\Gamma) \cap \ldots \cap w_k(\Gamma))^2 = \Gamma.$$

The proofs of all three statements are modelled on the $k = 1$ case, replacing the morphism $w\colon G^n \to G$ (or in the case of (ii), $w\colon \mathrm{SL}_2^n \to \mathrm{SL}_2$) with the fiber product, relative to G, of the morphisms $w_i\colon G^{n_i} \to G$ (respectively $w_i\colon \mathrm{SL}_2^{n_i} \to \mathrm{SL}_2$).

Acknowledgments

The first author would like to thank Nicholas Katz for some useful correspondence.

References

[AGV] M. Artin, A. Grothendieck, and J.L. Verdier, Avec la collaboration de P. Deligne et B. Saint-Donat, *Théorie des topos et cohomologie étale des schémas. Tome 3. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964*, Lecture Notes in Mathematics, Vol. 305. Springer-Verlag, Berlin-New York, 1973. MR0354654 (50:7132)

[AH] Z. Arad and M. Herzog (Eds.), *Products of Conjugacy Classes in Groups*, Springer Lecture Notes **1112**, Springer-Verlag, Berlin, 1985. MR0783067 (87h:20001)

[Ay] R. Ayoub, On Rademacher's extension of the Goldbach-Vinogradoff theorem, *Trans. Amer. Math. Soc.* **74** (1953), 482–491. MR0053960 (14:847a)

[BHP] R. C. Baker, G. Harman, and J. Pintz, The exceptional set for Goldbach's problem in short intervals. *Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995)*, 1–54, London Math. Soc. Lecture Note Ser., 237, Cambridge Univ. Press, Cambridge, 1997. MR1635718 (99g:11121)

[Be] E. Bertram, Even permutations as a product of two conjugate cycles, *J. Comb. Th. Ser. A* **12** (1972), 368–380. MR0297853 (45:6905)

[Bo] A. Borel, On free subgroups of semisimple groups, *Enseign. Math.* **29** (1983), 151–164. MR0702738 (85c:22009)

[Br] J.L. Brenner, Covering theorems for finite nonabelian simple groups. IX. How the square of a class with two nontrivial orbits in S_n covers A_n, *Ars Combinatoria* **4** (1977), 151–176. MR0576549 (58:28162a)

[De] P. Deligne, La conjecture de Weil. II. *Inst. Hautes Études Sci. Publ. Math.* **52** (1980), 137–252. MR0601520 (83c:14017)

[EGH] E.W. Ellers, N. Gordeev, and M. Herzog, Covering numbers for Chevalley groups, *Israel J. Math.* **111** (1999), 339-372. MR1710745 (2001i:20103)

[ET] P. Erdős and P. Turán, On some problems of a statistical group theory. I, *Z. Wahrscheinlichkeitstheorie Verw. Gabiete* **4** (1965), 175-186. MR0184994 (32:2465)

[G1] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas I, *Inst. Hautes Études Sci. Publ. Math.* **20** (1964), 259 pp. MR0173675 (30:3885)

[G2] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas II, *Inst. Hautes Études Sci. Publ. Math.* **24** (1965), 231 pp. MR0199181 (33:7330)

[G3] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas III, *Inst. Hautes Études Sci. Publ. Math.* **28** (1966), 255 pp. MR0217086 (36:178)

[G4] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV, *Inst. Hautes Études Sci. Publ. Math.* **32** (1967), 361 pp. MR0238860 (39:220)

[Hs] D. Husemoller, Ramified coverings of Riemann surfaces. *Duke Math. J.* **29** (1962), 167–174. MR0136726 (25:188)

[Ja] G.D. James, *The representation theory of the symmetric groups*, Lecture Notes in Math. **682**, Springer-Verlag, Berlin, 1978. MR0513828 (80g:20019)

[J] G.A. Jones, Varieties and simple groups, *J. Austr. Math. Soc.* **17** (1974), 163-173. MR0344342 (49:9081)

[Ln] S. Lang, Sur les séries L d'une variété algébrique. *Bull. Soc. Math. France* **84** (1956), 385–407. MR0088777 (19:578c)

[L] M. Larsen, Word maps have large image, *Israel J. Math.* **139** (2004), 149–156. MR2041227 (2004k:20094)

[L2] M. Larsen, How often is a partition an n'th power?, arXiv: math.CO/9712223.

[LP] M. Larsen and R. Pink, Finite subgroups of algebraic groups. Preprint, 1999.

[LL] R. Lawther and M.W. Liebeck, On the diameter of a Cayley graph of a simple group of Lie type based on a conjugacy class, *J. Comb. Theory, Ser. A* **83** (1998), 118-137. MR1629452 (99k:20036)

[LiSh] M.W. Liebeck and A. Shalev, Diameter of simple groups: sharp bounds and applications, *Annals of Math.* **154** (2001), 383–406. MR1865975 (2002m:20029)

[LiSh2] M.W. Liebeck and A. Shalev, Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks, *J. Algebra* **276** (2004), 552–601. MR2058457 (2005e:20076)

[Lish3] M.W. Liebeck and A. Shalev, Fuchsian groups, finite simple groups, and representation varieties, *Invent. Math.* **159** (2005), 317–367. MR2116277 (2005j:20065)

[MZ] C. Martinez and E.I. Zelmanov, Products of powers in finite simple groups, *Israel J. Math.* **96** (1996), 469–479. MR1433702 (97k:20050)

[Ma] H. Matsumura, *Commutative Algebra*, W. A. Benjamin Co., New York, 1970. MR0266911 (42:1813)

[MS] T.W. Müller and J-C. Schlage-Puchta, Character Theory of Symmetric Groups, Subgroup Growth of Fuchsian Groups, and Random Walks, *Adv. Math.* **213** (2007), no. 2, 919–982. MR2332616

[Na] M.B. Nathanson, *Additive number theory: The classical bases*, Graduate Texts in Mathematics **164**, Springer, 1996. MR1395371 (97e:11004)

[NS1] N. Nikolov and D. Segal, On finitely generated profinite groups, I: Strong completeness and uniform bounds, *Annals of Math.* **165** (2007), 171–238. MR2276769 (2008f:20052)

[NS2] N. Nikolov and D. Segal, On finitely generated profinite groups, II: Product decompositions of quasisimple groups, *Annals of Math.* **165** (2007), 239–273. MR2276770 (2008f:20053)

[Pi] R. Pink, Compact subgroups of linear algebraic groups, *J. Algebra* **206** (1998), no. 2, 438–504. MR1637068 (99g:20087)

[SW] J. Saxl and J.S. Wilson, A note on powers in simple groups, *Math. Proc. Camb. Phil. Soc.* **122** (1997), 91–94. MR1443588 (98e:20022)

[Sh] A. Shalev, Word maps, conjugacy classes, and a non-commutative Waring-type theorem, to appear in *Annals of Math.*

[Ti] J. Tits, Classification of algebraic semisimple groups, in *Algebaic Groups and Discontinuous Subgroups* (Proc. Sympos. Pure Math., Boulder, Colo., 1965), Amer. Math. Soc., Providence, R.I., 1966, pp. 33–62. MR0224710 (37:309)

[W] J.S. Wilson, First-order group theory, in *Infinite Groups 1994*, de Gruyter, Berlin, 1996, pp. 301–314. MR1477188 (99f:03045)

Department of Mathematics, Indiana University, Bloomington, Indiana 47405
E-mail address: larsen@math.indiana.edu

Einstein Institute of Mathematics, Hebrew University, Givat Ram, Jerusalem 91904, Israel
E-mail address: shalev@math.huji.ac.il