A REFINED WARING PROBLEM FOR FINITE SIMPLE GROUPS

MICHAEL LARSEN\textsuperscript{1} and PHAM HUU TIEP\textsuperscript{2}

\textsuperscript{1} Department of Mathematics, Indiana University, Bloomington, IN 47405, USA; email: mjlarsen@indiana.edu
\textsuperscript{2} Department of Mathematics, University of Arizona, Tucson, AZ 85721, USA; email: tiep@math.arizona.edu

Received 28 July 2014; accepted 23 February 2015

Abstract

Let $w_1$ and $w_2$ be nontrivial words in free groups $F_{n_1}$ and $F_{n_2}$, respectively. We prove that, for all sufficiently large finite nonabelian simple groups $G$, there exist subsets $C_1 \subseteq w_1(G)$ and $C_2 \subseteq w_2(G)$ such that $|C_i| = O(|G|^{1/2} \log^{1/2} |G|)$ and $C_1 \cdot C_2 = G$. In particular, if $w$ is any nontrivial word and $G$ is a sufficiently large finite nonabelian simple group, then $w(G)$ contains a thin base of order $2$. This is a nonabelian analog of a result of Van Vu [‘On a refinement of Waring’s problem’, Duke Math. J. 105(1) (2000), 107–134.] for the classical Waring problem. Further results concerning thin bases of $G$ of order $2$ are established for any finite group and for any compact Lie group $G$.

2010 Mathematics Subject Classification: 20C33 (primary); 20D06 (secondary)

1. Introduction

Let $F_n$ denote the free group in $n$ generators and $w \in F_n$ a nontrivial element. For every group $G$, the word $w$ induces a function $G^n \to G$, which we also denote $w$. In joint work with Aner Shalev [LS2, LST], the authors proved that, if $G$ is a finite simple group whose order is sufficiently large in terms of $w$, then $w(G^n)$ is a basis of order $2$; that is, every element of $G$ can be written as the product of two elements of $w(G^n)$. In particular, for any positive integer $m$, the $m$th powers in $G$ form a basis of order $2$ for all sufficiently large finite simple groups; this example explains the use of the term ‘Waring problem’ in the title of this paper.
The refinement we have in mind is indicated by a result of Van Vu [Vu] on the classical Waring problem. Vu observed that the $m$th powers in the set $\mathbb{N}$ of natural numbers form a thick basis of sufficiently large order $s$, in the sense that the number of representations of $n \in \mathbb{N}$ as a sum of $s$ $m$th powers grows polynomially with $n$. He proved that the $m$th powers contain thin subbases of order $s$, that is, subsets $X$ for which every element of $\mathbb{N}$ can be written as a sum of $s$ elements of $X$, but the growth of the number of representations is logarithmic. He asked one of us if there is an analogous result in the group-theoretic setting, that is, if $w(G^n)$ contains a thin subbase of order 2. The main result of this paper gives an affirmative answer to this question; in fact, the growth of the average number of representations of $g \in G$ is $O(\log |G|)$.

More precisely, our result is as follows. We state it asymmetrically, that is, in the more general case that we have two possibly different words $w_1$ and $w_2$ instead of a single word $w$.

**Theorem 1.1.** Let $w_1$ and $w_2$ be nontrivial words in free groups $F_{n_1}$ and $F_{n_2}$, respectively. For all sufficiently large finite nonabelian simple groups $G$, there exist subsets $C_1 \subseteq w_1(G)$ and $C_2 \subseteq w_2(G)$ such that $|C_i| = O(|G|^{1/2} \log^{1/2} |G|)$ and $C_1 C_2 = G$.

It is known that, for many words $w$, we have $w(G^n) = G$ for all $G$ sufficiently large. For instance, the commutator word in $F_2$ satisfies this equality for all finite simple $G$; see [EG], [LBST]. In this case, we are looking for a thin subbase of $G$ itself, and we prove that such order-2 subbases $X_G$ exist, not merely for finite simple groups but for all finite groups, where the average number of representations of $G$ as a product of two elements in $X_G$ is $O(1)$ as $|G| \to \infty$; see Corollary 5.4. We conclude with an analogous result for compact Lie groups; see Proposition 6.4 and Theorem 6.5.

### 2. The probabilistic method

Given subsets $X$ and $Y$ of a finite group $G$ with $XY = G$, we would like to find subsets $X_0 \subseteq X$ and $Y_0 \subseteq Y$ such that $X_0 Y_0$ is still all of $G$, while $|X_0||Y_0|$ is only slightly larger than $|G|$. In this section, we show that appropriately large random subsets $X_0 \subseteq X$ and $Y_0 \subseteq Y$ usually have the property that $X_0 Y_0$ includes every element of $G$ that has many representations of the form $xy$, $x \in X$, $y \in Y$.

**Lemma 2.1.** Let $a$, $b$, $n$ be positive integers, $N$ a set of cardinality $n$, $A \subseteq N$ a fixed subset of cardinality $a$, and $B \subseteq N$ a random subset chosen uniformly from
all \( b \)-element subsets of \( N \). Then

\[
\Pr[A \cap B = \emptyset] \leq e^{-ab/n}.
\]

**Proof.** The statement is trivial if \( a + b > n \), so we assume that \( a + b \leq n \). The probability that \( A \cap B = \emptyset \) is

\[
\frac{(n-a)\binom{n-a}{b}}{\binom{n}{b}} = \frac{(n-a)! (n-b)!}{n! (n-a-b)!} = \frac{(n-a)(n-a-1) \cdots (n-a-b+1)}{n(n-1) \cdots (n-b+1)} 
\leq (1 - a/n)^b \leq e^{-ab/n}.
\]

The following lemma gives a somewhat cruder but more general estimate than Lemma 2.1.

**Lemma 2.2.** Let \( a, b, n \) be positive integers, \( N \) a set of cardinality \( n \), \( A \subseteq N \) a fixed subset of cardinality \( a \), and \( B \subseteq N \) a random subset chosen uniformly from all \( b \)-element subsets of \( N \). Then

\[
\Pr\left( |A \cap B| \leq \frac{ab}{e^2 n} \right) \leq (2.2)e^{-5ab/2e^2n}.
\]

**Proof.** Assume that \( \max(a + b - n, 0) \leq k \leq \min(a, b) \) so that \( k \) is a possible size for \( A \cap B \). For \( k > 0 \) we have \( k! > (k/e)^k \), and so the probability that \( |A \cap B| = k \) is

\[
\frac{\binom{a}{k} \binom{n-a}{b-k}}{\binom{n}{b}} = \frac{a! b! (n-a)! (n-b)!}{k! (a-k)! (b-k)! n! (n-a-b+k)!} 
\leq \frac{b^k a^k (n-a)^{b-k}}{(k/e)^k n^k (n-k)^{b-k}} \leq \frac{(ab/n)^k}{(k/e)^k} \exp\left(-\frac{(b-k)(a-k)}{n-k}\right) 
\leq \exp(f(k)),
\]

where

\[
f(x) := x + x \log ab/n - x \log x - g(x), \quad g(x) := (a - x)(b - x)/(n - x).
\]

Let \( r := ab/e^2 n \leq \min(a/e^2, b/e^2) \). Then, when \( 0 < x \leq r \), we have \( f'(x) > 2 \), and so \( f(x) \) is increasing on \((0, r]\), and \( f(x) - f(x - 1) > 2 \) when \( 1 < x \leq r \). Also,

\[
g(r) \geq \frac{ab(1 - e^{-2})^2}{n} > 5.5r, \quad f(r) = 3r - g(r) < -2.5r.
\]
It follows that
\[
\Pr(0 < |A \cap B| \leq r) \leq \sum_{i=1}^{[r]} \exp(f(i)) < \frac{1}{1 - e^{-2}} \exp(f(r)) < \frac{e^{-2.5r}}{1 - e^{-2}} < (1.2)e^{-2.5r}.
\]
Together with Lemma 2.1, this implies the claim. \qed

**Proposition 2.3.** Let \( c > 0 \) be a constant, and let \( X, Y, \) and \( Z \) be subsets of a finite group \( G \) such that, for all \( z \in Z \),
\[
|\{(x, y) \in X \times Y \mid xy = z\}| \geq \frac{c|X||Y|}{|G|}.
\]
Let \( x_0 \leq |X| \) and \( y_0 \leq |Y| \) be positive integers such that \( x_0y_0 \geq (2e^2/c)|G| \log |G| \).

Then there exist subsets \( X_0 \subseteq X \) and \( Y_0 \subseteq Y \), with \( x_0 \) and \( y_0 \) elements, respectively, such that \( X_0Y_0 \supseteq Z \).

**Proof.** Let \( n \) denote the order of \( G \), which we may assume is at least 2. We choose \( X_0 \) and \( Y_0 \) at random independently and uniformly from the subsets of \( X \) of cardinality \( x_0 \) and the subsets of \( Y \) of cardinality \( y_0 \), respectively. It suffices to prove that, for each \( z \in Z \), the probability that \( z \in X_0Y_0 \) is more than \( 1 - 1/n \).

(Indeed, in this case the probability that \( X_0Y_0 = G \) is larger than \( 1 - n/n = 0 \); that is, \( X_0Y_0 = G \).) Let \( S_z \) denote the set of pairs \( (x, y) \in X \times Y \) such that \( xy = z \), and let \( \pi_X \) and \( \pi_Y \) denote the projection maps from \( X \times Y \) to \( X \) and \( Y \), respectively.

We want to prove that the probability that \( \pi_Y^{-1}(Y_0) \cap \pi_X^{-1}(X_0) \cap S_z \) is nonempty is more than \( 1 - 1/n \).

As \( G \) is a group, the restrictions of \( \pi_X \) and \( \pi_Y \) to \( S_z \) are injective, so
\[
|\pi_X^{-1}(X_0) \cap S_z| = |\pi_X(S_z) \cap X_0|,
\]
\[
|\pi_Y^{-1}(Y_0) \cap \pi_X^{-1}(X_0) \cap S_z| = |\pi_Y(\pi_X^{-1}(X_0) \cap S_z) \cap Y_0|.
\]

It suffices to prove that the probability that \( \pi_X(S_z) \cap X_0 \) has at least \( (x_0|S_z|)/(e^2|X|) \) elements is at least \( 1 - 1/2n \), and that the conditional probability that \( \pi_Y(\pi_X^{-1}(X_0) \cap S_z) \cap Y_0 \) is nonempty given that
\[
|\pi_X(S_z) \cap X_0| \geq \frac{x_0|S_z|}{e^2|X|}
\]
is at least \( 1 - 1/2n \).
By hypothesis,
\[
\frac{|X_0| \pi_X(S_z)}{|X|} = \frac{x_0 |S_z|}{|X|} \geq \frac{cx_0 |Y|}{n} \geq \frac{cx_0 y_0}{n} \geq 2e^2 \log n.
\]

By Lemma 2.2, the probability that
\[
|X_0 \cap \pi_X(S_z)| = |\pi_X^{-1}(X_0) \cap S_z| \leq \frac{x_0 |S_z|}{e^2 |X|}
\]
is at most \(2.2/n^5 < 1/2n\). If (2.1) holds, then
\[
\frac{|Y_0| \pi_X^{-1}(X_0) \cap S_z}{|Y|} \geq \frac{x_0 y_0 |S_z|}{e^2 |X||Y|} \geq \frac{2n \log n |S_z|}{c |X||Y|} \geq 2 \log n.
\]
By Lemma 2.1, the probability of \(Y_0\) being disjoint from a subset of \(Y\) of cardinality at least \((x_0 |S_z|)/(e^2 |X|)\) is at most \(1/n^2 \leq 1/2n\).

**Corollary 2.4.** Let \(w_1\) and \(w_2\) be two nontrivial words, and let \(S\) be a finite simple group. To prove Theorem 1.1 for \((w_1, w_2, S)\), it suffices to show that there exist subsets \(X \subseteq w_1(S), Y \subseteq w_2(S)\), and a subset \(S_1 \subseteq S\) of cardinality at most \(|S|^{1/2}\), such that the following hold.

(i) \(w_1(S)w_2(S) = S\).

(ii) \(|\{(x, y) \in X \times Y \mid xy = g\}| \geq \frac{|X| \cdot |Y|}{2|S|}\) for all \(g \in S \setminus S_1\).

(iii) \(|X|, |Y| \geq 2e|S|^{1/2} \log^{1/2} |S|\).

**Proof.** Choose \(x_0 = y_0 := [2e|S|^{1/2} \log^{1/2} |S|]\) (note that we still have \(x_0 \leq |X|\) and \(y_0 \leq |Y|\)). By Proposition 2.3 with \(c = 1/2\), there exist subsets \(X_0 \subseteq X\) and \(Y_0 \subseteq Y\) with \(X_0Y_0 \supseteq S \setminus S_1\), \(|X_0| = x_0\), and \(|Y_0| = y_0\). For each \(z \in S_1\), by (i) there exists \((x_z, y_z) \in w_1(S) \times w_2(S)\) such that \(z = x_zy_z\). Now set
\[
C_1 := X_0 \cup \{x_z \mid z \in S_1\}, \quad C_2 := Y_0 \cup \{y_z \mid z \in S_1\}.
\]

**Corollary 2.5.** If \(x_0\) and \(y_0\) are integers in \([1, |G|]\) such that \(x_0y_0 > 2e^2|G| \log |G|\), then there exist subsets \(X_0\) and \(Y_0\) of \(G\) of cardinality \(x_0\) and \(y_0\), respectively, such that \(X_0Y_0 = G\).

**Proof.** Set \(X = Y = Z := G\) and \(c = 1\) in Proposition 2.3.
Corollary 2.6. There exists a square root $R$ of $G$, that is, a subset such that $R^2 = G$, with $|R| \leq 2^{1/2}e|G|^{1/2} \log^{1/2} |G|$.

In fact, we will show that $G$ has a square root of size $O(|G|^{1/2})$; see Corollary 5.4. Analogs of this result for compact Lie groups will be proved in Section 6; cf. Proposition 6.4 and Theorem 6.5.

3. Simple groups of Lie type

In what follows, we say that $S$ is a finite simple group of Lie type of rank $r$ defined over $\mathbb{F}_q$ if $S = G^F/\mathbf{Z}(G^F)$ for a simple simply connected algebraic group $G$ over $\mathbb{F}_q$, of rank $r$, and a Steinberg endomorphism $F : G \to G$, with $q$ the common absolute value of the eigenvalues of $F$ on the character group of an $F$-stable maximal torus $T$ of $G$. In particular, this includes the Suzuki–Ree groups, for which $q$ is a half-integer power of 2 or 3. By slight abuse of terminology, we will say that an element $s \in S$ is regular semisimple if some inverse image of $s$ is so in $G^F$.

The aim of this section is to prove the following theorem.

Theorem 3.1. Let $w_1$ and $w_2$ be two nontrivial words. Then there is $N = N(w_1, w_2)$ with the following property. For any finite nonabelian simple group $S$ of Lie type of order at least $N$, there exist conjugacy classes $s_1^S \subseteq w_1(S)$, $s_2^S \subseteq w_2(S)$, and a subset $S_1 \subset S$ of cardinality at most $|S|^{1/2}$, such that the following hold.

(i) $w_1(S)w_2(S) = S$.

(ii) $|(x, y) \in s_1^S \times s_2^S \mid xy = g| \geq \frac{|s_1^S| \cdot |s_2^S|}{2|S|}$ for all $g \in S \setminus S_1$.

(iii) $|s_i^S| \geq 4e|S|^{1/2} \log^{1/2} |S|$.

Note that condition (i) follows from the main result of [LST], and (ii) is equivalent to

$$\left| \sum_{1s \neq \chi \in \text{Irr}(S)} \frac{\chi(s_1)\chi(s_2)\bar{\chi}(g)}{\chi(1)} \right| \geq \frac{1}{2}, \quad \forall g \in S \setminus S_1. \quad (3.1)$$

Also, Theorem 3.1 and Corollary 2.4 immediately imply Theorem 1.1 for sufficiently large nonabelian simple groups of Lie type.

First we recall the following consequence of [La, Proposition 7].
**Lemma 3.2.** For any $r_0$ and any nontrivial word $w \neq 1$, there exists a constant $c = c(w, r_0)$ such that

$$|w(S)| \geq c|S|$$

for all finite simple group $S$ of Lie type of rank $\leq r_0$.

**Corollary 3.3.** For any $r_0$ and any nontrivial word $w \neq 1$, there exists a constant $Q = Q(w, r_0)$ such that

(i) $w(S)$ contains a regular semisimple element $s$ and

(ii) $|x^S| \geq 4e|S|^{1/2} \log^{1/2}|S|$ for any regular semisimple element $x \in S$

for all finite simple groups $S$ of Lie type of rank $\leq r_0$ defined over $\mathbb{F}_q$ with $q \geq Q$.

**Proof.** According to [GL, Theorem 1.1], the proportion of regular semisimple elements in $S$ defined over $\mathbb{F}_q$ is more than $1 - f(q)$, with

$$f(q) := \frac{3}{q - 1} + \frac{2}{(q - 1)^2}.$$  

Applying Lemma 3.2 and choosing $Q$ so that $f(Q) < c(w, r_0)$, we see that $w(S)$ contains a regular semisimple element $s$ whenever the rank of $S$ is at most $r_0$ and $q \geq Q$.

Next, view $S$ as $G/Z(G)$ for $G := G^F$, and consider an inverse image $g \in G$ of $x$ in $G$ that is regular semisimple. Note that $|C_G(g)| \leq (q + 1)^r$, and so $|C_G(xZ(G))| \leq (q + 1)^r|Z(G)|$. Also, $|G| > (q - 1)^{3r}$ and $|Z(G)| \leq r_0 + 1$. Therefore,

$$|s^S| = \frac{|S|}{|C_S(x)|} = \frac{|G|}{|C_G(xZ(G))|} \geq \frac{|G|}{(q + 1)^r(r_0 + 1)} > |S|^{3/5} > 4e|S|^{1/2} \log^{1/2}|S|$$

when $q \geq Q$ and we choose $Q$ large enough. 

Next we recall the following fact.

**Lemma 3.4.** For any $r_0$, there is a constant $C = C(r_0)$ such that

$$|\chi(s)| \leq C$$

for all finite simple group $S$ of Lie type of rank $\leq r_0$, for all regular semisimple elements $s \in S$, and for all $\chi \in \text{Irr}(S)$.
Proof. Note that, if $S$ is not a Suzuki–Ree group, then the statement is a direct consequence of [GLL, Proposition 5]. But in fact the same proof goes through in the case that $S$ is a Suzuki–Ree group. \hfill \square

**Proposition 3.5.** Theorem 3.1 holds for Suzuki and Ree groups, with $S_1 = \{1\}$.

**Proof.** Let $S = 2B_2(q^2), 2G_2(q^2)$, or $2F_4(q^2)$. By [LST, Proposition 6.4.1] and Corollary 3.3, there exists $Q_1 = Q(w_1, w_2)$ such that $w_1(S)w_2(S) = S$, and $w_i(S)$ contains a regular semisimple element $s_i$ satisfying the condition 3.3(ii) for $i = 1, 2$, whenever $q \geq Q_1$. By Lemma 3.4, there is some $C > 0$, independent of $q$, such that $|\chi(s_i)| \leq C$ for all $\chi \in \text{Irr}(S)$ and $i = 1, 2$. We will now prove that there is some $B > 0$, independent of $q$, such that

$$\sum_{1 \neq \chi \in \text{Irr}(S)} \frac{|\chi(g)|}{\chi(1)} \leq \frac{B}{q} \tag{3.2}$$

for all $1 \neq g \in S$. Taking $q \geq \max(Q_1, 2BC^2)$, we will achieve (3.1).

First let $S = 2B_2(q^2)$ with $q \geq \sqrt{8}$. The character table of $S$ is known; see, for example, [Bu]. In particular, $\text{Irr}(S)$ consists of $q^2 + 3$ characters: $1_S$, two characters of degree $q(q^2 - 1)/\sqrt{2}$, and the remaining characters of degree $\geq (q^2 - 1)(q^2 - q\sqrt{2} + 1)$. Furthermore,

$$|\chi(g)| \leq q\sqrt{2} + 1$$

for all $1 \neq \chi \in \text{Irr}(S)$ and $1 \neq g \in S$. It follows that

$$\sum_{1 \neq \chi \in \text{Irr}(S)} \frac{|\chi(g)|}{\chi(1)} \leq (q\sqrt{2} + 1) \left( \frac{2\sqrt{2}}{q(q^2 - 1)} + \frac{q^2}{(q^2 - 1)(q^2 - q\sqrt{2} + 1)} \right) < \frac{5}{q},$$

as stated.

Next suppose that $S = 2G_2(q^2)$ with $q \geq \sqrt{27}$. The character table of $S$ is known; see, for example, [Wa]. In particular, $\text{Irr}(S)$ consists of $q^2 + 8$ characters: $1_S$, one character of degree $q^4 - q^2 + 1$, six characters of degree $\geq q(q^2 - 1)/(q^2 - q\sqrt{3} + 1)/\sqrt{12}$, and the remaining characters of degree $\geq q^6/2$. Furthermore, $|\chi(g)| \leq \sqrt{|C_S(g)|} \leq q^3$ for all $1 \neq g \in S$. It follows that

$$\sum_{1 \neq \chi \in \text{Irr}(S)} \frac{|\chi(g)|}{\chi(1)} \leq q^3 \left( \frac{1}{q^4 - q^2 + 1} + \frac{6\sqrt{12}}{q(q^2 - 1)(q^2 - q\sqrt{3} + 1)} + \frac{q^2}{q^6/2} \right) < \frac{5}{q},$$

as stated.
Suppose now that $S = 2 F_4(q^2)$ with $q \geq \sqrt{8}$. The (generic) character table of $S$ is known in principle, but not all character values are given explicitly in [Chevie] (in particular, ten families of characters are not listed therein). On the other hand, according to [FG, Lu2], Irr($S$) consists of $q^4 + 4q^2 + 17$ characters: $\chi_0 := 1_S$, four characters $\chi_{1,2,3,4}$ of degree

$$\chi_{1,2}(1) = q(q^4 - 1)(q^6 + 1)/\sqrt{2},$$
$$\chi_{3}(1) = q^2(q^4 - q^2 + 1)(q^8 - q^4 + 1),$$
$$\chi_{4}(1) = (q^2 - 1)(q^4 + 1)(q^{12} + 1),$$

and the remaining characters of degree $> q^{20}/48$ (when $q \geq \sqrt{8}$). The orders $|C_S(g)|$ are listed in [Chevie]; in particular, $|C_S(g)| < 2q^{30}$ when $1 \neq g \in S$. It follows that $|\chi(g)| < \sqrt{|C_S(g)|} < \sqrt{2}q^{15}$, and so

$$\sum_{\chi \in \text{Irr}(S)} \frac{|\chi(g)|}{\chi(1)} < \frac{\sqrt{2}q^{15}(q^4 + 4q^2 + 12)}{q^{20}/48} + \frac{\sqrt{2}q^{15}}{(q^2 - 1)(q^4 + 1)(q^{12} + 1)} < \frac{144}{q}.$$  

(3.3)

Among all nontrivial conjugacy classes of $S$, there are two classes $g_1^S$ with

$$|C_S(g_1)| = q^{24}(q^2 - 1)(q^4 + 1),$$
$$|C_S(g_2)| = q^{20}(q^4 - 1),$$

and all the other ones have centralizers of order $< 4q^{20}$; cf. [Chevie]. Hence if $g \notin \{1\} \cup g_1^S \cup g_2^S$ then $|\chi_i(g)| < 2q^{10}$, and so

$$\sum_{\chi = \chi_{1,2,3}} \frac{|\chi(g)|}{\chi(1)} \leq \frac{3 \cdot 2q^{10}}{q(q^4 - 1)(q^6 + 1)/\sqrt{2}} < \frac{10}{q}.$$  

(3.4)

Finally, for $g = g_{1,2}$, using [Chevie] one can check that

$$|\chi_{1,2}(g)| \leq q(q^6 - q^4 + 1)/\sqrt{2},$$
$$|\chi_3(g)| \leq q^8 - q^4 + q^2,$$

whence

$$\sum_{\chi = \chi_{1,2,3}} \frac{|\chi(g)|}{\chi(1)} \leq \frac{\sqrt{2}q(q^6 - q^4 + 1)}{q(q^4 - 1)(q^6 + 1)/\sqrt{2}} + \frac{q^8 - q^4 + q^2}{(q^2 - 1)(q^4 + 1)(q^{12} + 1)} < \frac{1}{q}.$$  

(3.5)

Taken together, (3.3)–(3.5) imply (3.2) for $S = 2 F_4(q^2)$.\[\square\]

**Proposition 3.6.** Theorem 3.1 holds for all (sufficiently large) finite nonabelian simple groups $S$ of Lie type of bounded rank, with $S_1 = \{1\}$.

**Proof.** By Proposition 3.5, we may assume that $S$ is not a Suzuki or Ree group. Assume that $S$ is defined over $\mathbb{F}_q$ and of rank $\leq r_0$. Then we view $S$ as $G^F/Z(G^F)$
for some simple simply connected algebraic group \( G \), of rank \( r \leq r_0 \), and some Steinberg endomorphism \( F : G \to G \). According to [LS2, Theorem 1.7], \( w_1(S)w_2(S) = S \) when \( q \) is large enough. By [LST, Corollary 5.3.3], there exists a positive constant \( \delta = \delta(w_1, w_2, r_0) \) such that, for any \( F \)-stable maximal torus \( T \) of \( G \), and for \( i = 1, 2 \),

\[
|T^F \cap w_i(G^F)| \geq \delta |T^F| \geq \delta(q - 1)^r.
\]

On the other hand, part (3) of the proof of [Lu1, Theorem 2.1] shows that \( T^F \) contains at most \( 2^r r^2 (q + 1)^{r-1} \) nonregular elements. Hence, if we choose

\[
q > \max(5, 1 + 3^{10} r_0^2 / \delta),
\]

then \( T^F \cap w_i(G^F) \) contains a regular semisimple element. Now we apply this observation to a pair of \( F \)-stable maximal tori \( T_1, T_2 \) of \( G \) that is weakly orthogonal in the sense of [LST, Definition 2.2.1], and get regular semisimple elements \( s_i \in T^F \cap w_i(G^F) \) for \( i = 1, 2 \). By [LST, Proposition 2.2.2], if \( \chi \in \text{Irr}(G^F) \) is nonzero at both \( s_1 \) and \( s_2 \), then \( \chi \) is unipotent (and so trivial at \( Z(G^F) \)). In this case, the results of [DL] imply that \( \chi(s_1) \) does not depend on the particular choice of the element \( s_1 \) of given type, and similarly for \( \chi(s_2) \). Also, \( |s_i^S| \geq 4e|S|^{1/2} \log^{1/2} |S| \) if \( q > \max(Q(w_1, r_0), Q(w_2, r_0)) \); cf. Corollary 3.3.

We claim that we can find such a pair \( T_1, T_2 \) so that there are \( \kappa \leq 4 \) characters \( \chi \in \text{Irr}(G^F) \) with \( \chi(s_1) \chi(s_2) \neq 0 \), and moreover \( |\chi(s_1) \chi(s_2)| = 1 \) for all such \( \chi \). Indeed, this can be done with \( \kappa = 2 \) for \( G^F \) of type \( A_r \) by [MSW, Theorem 2.1], of type \( 2A_r \) by [MSW, Theorem 2.2], of type \( C_r \) by [MSW, Theorem 2.3], of type \( B_r \) by [MSW, Theorem 2.4], of type \( 2D_r \) by [MSW, Theorem 2.5], and of type \( D_{2r+1} \) by [MSW, Theorem 2.6]. For type \( D_{2r} \), we can get \( \kappa = 4 \) by using [GT, Proposition 2.3]. For the exceptional groups of Lie type, we can get \( \kappa = 2 \) by using [LM, Theorem 10.1]. Certainly, if \( \kappa = 2 \), then these characters are the trivial character and the Steinberg character \( St \) of \( G^F \).

Now consider any nontrivial element \( g \in S \). Since \( S \) is simple, \( St \) is faithful, and so \( |St(g)| < St(1) \). But \( St(g) \in \mathbb{Z} \) divides \( St(1) \), so we get \( |St(g)/St(1)| \leq 1/2 \) and

\[
\sum_{1 \neq \chi \in \text{Irr}(S)} \left| \frac{\chi(s_1) \chi(s_2) \bar{\chi}(g)}{\chi(1)} \right| \cdot \frac{|St(g)|}{St(1)} \leq 1/2,
\]

as desired. Finally, assume that \( \kappa = 4 \) (so \( G^F \) is of type \( D_{2r} \)). By [LST, Theorem 1.2.1], we have

\[
\sum_{1 \neq \chi \in \text{Irr}(S)} \left| \frac{\chi(s_1) \chi(s_2) \bar{\chi}(g)}{\chi(1)} \right| \leq 3q^{-1/481} < 1/2
\]

if \( q > 6^{481} \).
To deal with (classical) groups of unbounded rank, we recall the notion of the support of an element of a classical group [LST, Definition 4.1.1]. For \( g \in GL_n(F) \subset GL_n(\bar{F}) \), the support is the codimension of the largest eigenspace of \( g \) acting on \( F^n \). The support of any element in a classical group \( G(\bar{F}) \) is the support of its image under the natural representation \( \rho : G(\bar{F}) \to GL_n(\bar{F}) \). Most elements have large support; we have the following quantitative estimate.

**Lemma 3.7.** Let \( S \) be a finite simple classical group of rank \( r \geq 8 \), and \( B \geq 1 \) any constant. If \( r \geq 8B + 3 \), then the set \( S_1 \) of elements of support \( < B \) can contain at most \( |S|^{1/2} \) elements of \( S \).

**Proof.** We will bound the total number \( N \) of elements \( g \) of support \( \leq B \) in \( L = SL_n(q), SU_n(q), Sp_n(q), \) or \( SO_n^\pm(q) \) (note that \( S \hookrightarrow L/Z(L) \)). Let \( V = \bar{F}^n \), respectively \( \bar{F}_2, \bar{F}_2^\pm, \bar{F}_2^\pm, \bar{F}_2^\pm, \) denote the natural \( L \)-module. By the results in [FG, Section 3], the number of conjugacy classes in \( L \) is less than \( 16q^r \leq q^{r+4} \). Since \( B < n/2 \), \( g \) has a primary eigenvalue \( \lambda \in \bar{F}_2^\times \), respectively \( \lambda^{q+1} = 1, \lambda = \pm 1 \), or \( \lambda = \pm 1 \); cf. [LST, Proposition 4.1.2]. Moreover, one can show that \( V \) admits a \( g \)-invariant decomposition \( V = U \oplus W \) into a direct (orthogonal if \( L \neq SL_n(q) \)) sum of (nondegenerate if \( L \neq SL_n(q) \)) subspaces, with \( U \leq \text{Ker}(g - \lambda \cdot 1_V) \) and \( m := \dim(U) \geq n - 2B \) (see [LST, Lemma 6.3.4] for the orthogonal case).

Consider the case \( L = SL_n^\epsilon(q) \), with \( \epsilon = + \) for \( SL \) and \( \epsilon = - \) for \( SU_n(q) \). Then \( C_L(g) \) contains \( SL_m^\epsilon(q) \). It follows that

\[
|g^L| \leq \frac{|SL_n^\epsilon(q)|}{|SL_m^\epsilon(q)|} < \frac{2q^{n^2-1}}{q^{m^2-1/2}} < 4q^{n^2-m^2} < q^{4nB+2},
\]
as \( n \geq m \geq n - 2B \). Hence,

\[
N \leq q^{n(4B+1)+3} \leq q^{(n^2-3)/2} \leq |S|^{1/2}.
\]

Suppose now that \( L = SO_n^\pm(q) \). Then \( C_L(g) \) contains \( SO_m^\pm(q) \). It follows that

\[
|g^L| \leq \frac{|SO_n^\pm(q)|}{|SO_m^\pm(q)|} < \frac{q^{n(n-1)/2}}{q^{m(m-1)/2/2}} = 2q^{(n-m)(n+m-1)/2+1} \leq q^{(2n-1)B+2},
\]

and so

\[
N \leq q^{B(2n-1)+r+6} \leq q^{(n(n-1)/2-1)/2} \leq |S|^{1/2}.
\]

Consider the case \( L = Sp_n(q) \), so \( n = 2r \) and \( m \) are even. Then \( C_L(g) \) contains \( Sp_m(q) \). It follows that

\[
|g^L| \leq \frac{|Sp_n(q)|}{|Sp_m(q)|} < \frac{q^{n(n+1)/2}}{q^{m(m+1)/2}} = 2q^{(n-m)(m+n+1)/2+1} \leq q^{(2n+1)B+2},
\]
and so
\[ N \leq q^{B(2n+1)+r+6} \leq q^{(n(n+1)/2-1)/2} \leq |S|^{1/2}. \]

\begin{theorem}
Theorem 3.1 holds for all simple classical groups of sufficiently large rank.
\end{theorem}

\begin{proof}
(a) View \( S = G/\mathbb{Z}(G) \) with \( G = G^F \) as above, and let \( r := \text{rank}(G) \). We will show that there are some \( r_0 = r_0(w_1, w_2) > 8 \) and \( B = B(w_1, w_2) \) such that Theorem 3.1 holds when \( r \geq r_0 \), for suitable regular semisimple elements \( s_1, s_2 \in S \) and with \( S_1 \) being the set of elements in \( S \) of support \( < B \). By Lemma 3.7, \( |S_1| \leq |S|^{1/2} \) if \( r_0 \geq 8B + 3 \).

Again, note that, for any regular semisimple element \( h \in G \), \( C_G(h) \) is a maximal torus (as \( G \) is simply connected), and so \( |C_G(h)| \leq (q+1)^r \). It follows that \( |C_G(h\mathbb{Z}(G))| \leq (q+1)^r|\mathbb{Z}(G)| \), and so \( |C_S(h\mathbb{Z}(G))| \leq (q+1)^r \). Also, \( |G| > q^{r(r+1)} \) and \( |\mathbb{Z}(G)| \leq r + 1 \). So when \( r \geq r_0 > 8 \) we have
\[ |C_S(h\mathbb{Z}(G))| \leq (q+1)^r < \left( \frac{q^{r(r+1)}}{r+1} \right)^{1/3} < |S|^{1/3}. \]

In particular, \( s_1 \) and \( s_2 \) satisfy condition (iii) of Theorem 3.1 when \( r_0 \geq 9 \).

As mentioned above, condition (i) of Theorem 3.1 follows from [LST, Theorem 1.1.1]. So it suffices to establish (3.1) for all \( g \in S \setminus S_1 \).

(b) Suppose first that \( G^F \) is a special linear, special unitary, or symplectic group. By Propositions 6.2.4 and 6.1.1 of [LST], there is some \( r_1 = r_1(w_1, w_2) \) with the following property. When \( r \geq r_1 \), there are regular semisimple elements \( s_i \in w_i(S) \) for \( i = 1, 2 \) such that there are at most \( \kappa \leq 4 \) irreducible characters \( \chi_i \in \text{Irr}(S) \) with \( \chi_i(s_1) \chi_i(s_2) \neq 0, 1 \leq i \leq \kappa \), and \( \chi_1 = 1_S \). Moreover, \( |\chi_i(s_1) \chi_i(s_2)| = 1 \) for \( 1 \leq i \leq \kappa \). Now we choose \( B \geq 1443^2 \) and consider any \( g \in S \setminus S_1 \). By [LST, Theorem 1.2.1],
\[ \frac{|\chi(g)|}{\chi(1)} < q^{-\sqrt{B}/481} \leq 1/8, \]
whence
\[ \left| \sum_{1 \neq \chi \in \text{Irr}(S)} \frac{\chi(s_1) \chi(s_2) \bar{\chi}(g)}{\chi(1)} \right| \leq \sum_{i=2}^\kappa \frac{|\chi_i(g)|}{\chi_i(1)} < 3/8, \]
as required. In fact, if \( G^F \) is a symplectic group, then \( \kappa = 2 \), \( \chi_2 = \text{St} \), \( |\chi_2(g)/\chi(1)| \leq 1/q \leq 1/2 \) for all \( 1 \neq g \in S \), and so we can take \( S_1 = \{1\} \).

(c) Suppose now that \( G^F \) is a simple orthogonal group. By Propositions 6.3.5 and 6.3.7 of [LST], there exist some \( r_2 = r_2(w_1, w_2) \), \( \kappa = \kappa(w_1, w_2) \), and \( C = C(w_1, w_2) \) with the following property. When \( r \geq r_2 \), there are regular
semisimple elements $s_i \in w_i(S)$ for $i = 1, 2$ such that there are at most $\kappa$ irreducible characters $\chi_i \in \text{Irr}(S)$ with $\chi_i(s_1)\chi_i(s_2) \neq 0$, $1 \leq i \leq \kappa$, and $\chi_1 = 1_S$. Moreover, $|\chi_i(s_1)\chi_i(s_2)| \leq C$ for $1 \leq i \leq \kappa$. Now we choose $B \geq 1443^2$ such that
\[(\kappa - 1)C^22^{-\sqrt{B}/481} < 1/2.
\]
Then, for any $g \in S \setminus S_1$, by [LST, Theorem 1.2.1], we have
\[
\left| \sum_{1 \neq \chi \in \text{Irr}(S)} \frac{\chi(s_1)\chi(s_2)\bar{\chi}(g)}{\chi(1)} \right| \leq \sum_{i=2}^{\kappa} \frac{C^2|\chi_i(g)|}{\chi_i(1)} < (\kappa - 1)C^22^{-\sqrt{B}/481} < 1/2.
\]
Hence we are done by choosing $r_0 := \max(r_1, r_2, 9, 8B + 3)$.

\[
\square
\]

4. Alternating groups

Suppose that $G$ is a group and that $X$ and $Y$ are subsets. If we have subsets $X_1, \ldots, X_k \subseteq X$, $Y_1, \ldots, Y_k \subseteq Y$, and $Z_1, \ldots, Z_k \subseteq Z$ such that $Z_i \subseteq X_iY_i$ and $\bigcup Z_i = G$, then, setting $X_0 = X_1 \cup \cdots \cup X_k$ and $Y_0 = Y_1 \cup \cdots \cup Y_k$, we have $X_0Y_0 = G$. We use this construction to find $X_0 \subseteq w_1(A_n)$ and $Y_0 \subseteq w_2(A_n)$ such that $X_0Y_0 = A_n$ and $|X_0|, |Y_0|$ are of order $n!^{1/2}\sqrt{\log n!}$.

We begin by noting that, for any word $w$ and any group $G$, $w(G)$ is a characteristic set, that is, invariant under every automorphism of $G$. In particular, $w(A_n)$ is a union of $S_n$-conjugacy classes. If $g_1, g_2 \in A_n$ and $C_1$ and $C_2$ denote their $S_n$-conjugacy classes, then
\[
|\{(c_1, c_2) \in C_1 \times C_2 \mid c_1c_2 = g\}| = \frac{|C_1||C_2|}{n!} \sum_{\chi} \frac{\chi(g_1)\chi(g_2)\bar{\chi}(g)}{\chi(1)}.
\]

We recall a basic upper bound estimate [LS1, Theorem 1.1] for $|\chi(g)|$. For $g \in S_n$ and $i \in \mathbb{N}$, let $\Sigma_i(g)$ denote the union of all $g$-cycles of length $\leq i$ in $\{1, \ldots, n\}$. Define $e_1(g), e_2(g), \ldots$ so that
\[
n^{e_1(g)+\cdots+e_i(g)} = \max(1, |\Sigma_i(g)|)
\]
for all $i \in \mathbb{N}$. Define
\[
E(g) = \sum_{i=1}^{\infty} \frac{e_i(g)}{i}.
\]
Then for all $\epsilon > 0$ there exists $N$ such that, for all $n > N$, all $g \in S_n$, and all irreducible characters $\chi$ of $S_n$,
\[
|\chi(g)| \leq |\chi(1)|^{E(g)+\epsilon}.
\]
For example, if \( g \) has a bounded number of cycles, and \( n \) is sufficiently large in terms of \( \epsilon \),
\[
|\chi(g)| \leq |\chi(1)|^\epsilon.
\]
If \( g \) has no more than \( n^{2/3} \) fixed points and \( n \) is sufficiently large in terms of \( \epsilon \), then
\[
|\chi(g)| \leq |\chi(1)|^{5/6+\epsilon}.
\]

By a result of Liebeck and Shalev [LiS, Theorem 1.1], for all \( s > 0 \),
\[
\lim_{n \to \infty} \sum_{\chi \in \text{Irr}(S_n)} \chi(1)^{-s} = 2.
\]
Note that the trivial character and the sign character each contribute 1 to the above sum; excluding them from the sum, the limit would be zero. Of course, thus if \( g_1, g_2, \) and \( g \) are all even permutations, then the trivial character and the sign character each contribute \((|C_1||C_2|)/n!\) to expression (4.1). From this, we conclude the following.

**Proposition 4.1.** For all \( \epsilon > 0 \) and integers \( k_1 \) and \( k_2 \), there exists an integer \( N = N(\epsilon, k_1, k_2) \) such that, if \( n > N \) and \( C_1 \) and \( C_2 \) are even conjugacy classes in \( S_n \) consisting of \( k_1 \) and \( k_2 \) cycles, respectively, then every \( g \in A_n \) with no more than \( n^{2/3} \) fixed points is represented in at least
\[
(1 - \epsilon)\frac{|C_1||C_2|}{|A_n|}
\]
different ways as \( x_1x_2, x_1 \in C_1, x_2 \in C_2 \).

Now, by [LS2, Theorem 1.3], if \( n \) is sufficiently large, \( w_1(A_n) \) and \( w_2(A_n) \) each contain elements \( g_1 \) and \( g_2 \), respectively, with at most 6 cycles of length \( > 1 \) and \( \leq 17 \) cycles in total. So there is some constant \( A \) such that \( |C_{S_n}(g_i)| < An^6 \) for \( i = 1, 2 \), whence
\[
|w_i(A_n)| \geq |(g_i)^{S_n}| > 2e(n!)^{1/2} \log^{1/2} n!.
\]
Defining \( Z_1 \) as the set of elements of \( A_n \) with no more than \( n^{2/3} \) fixed points, it follows from Proposition 2.3 that there exist \( X_1 \) and \( Y_1 \) contained in \( w_1(A_n) \) and \( w_2(A_n) \), respectively, such that \( Z_1 \subseteq X_1Y_1 \).

What remains is to define \( X_i, Y_i, Z_i \) for \( i \geq 2 \) to cover the elements of \( A_n \) with more than \( n^{2/3} \) fixed points.

The number of elements of \( A_n \) with at least \( m := \lceil 2n/3 \rceil \) fixed points is less than
\[
\sum_{i=m}^{n} \binom{n}{i}(n-i)! < \sum_{i=m}^{n} \frac{n!}{i!} \leq \frac{2n!}{m!} \leq n^{1/3+o(1)}.
\]
Therefore, we can represent each element $g$ with at least $m$ fixed points as $x_g y_g$, $x_g \in w_1(A_n)$, $y_g \in w_2(A_n)$, and we can define $X_2$ to be the union of all such $x_g$ and $Y_2$ the union of all such $y_g$. Note that

$$|X_2|, |Y_2| < (n!)^{1/3+o(1)}.$$ 

This reduces the problem to elements $g$ with

$$n^{2/3} \leq |\text{Fix}(g)| \leq 2n/3.$$ 

For each $T \subseteq \{1, 2, \ldots, n\}$ with $m := |T| \in [n^{2/3}, 2n/3]$, we define $S_T \subseteq S_n$ to be the pointwise stabilizer of $T$ in $S_n$ and $A_T$ to be the pointwise stabilizer of $T$ in $A_n$. Thus $S_T$ is isomorphic to $S_{n-m}$ and $A_T$ is isomorphic to $A_{n-m}$, where $n - m \in [n/3, n - n^{2/3}]$. For each $T$, we choose an $S_T$-conjugacy class $C_{1,T}$ in $w_1(A_T)$ and an $S_T$-conjugacy class $C_{2,T}$ in $w_2(A_T)$, each consisting of at most 17 cycles when regarded as elements of $S_{n-m}$ (Of course there are $|T|$ additional 1-cycles when we regard them as elements of $S_n$.) If $n$ is sufficiently large, $n - m$ is larger than the constant $N$ of Proposition 4.1, and we conclude that every fixed point free element of $A_{n-m}$ can be written in at least

$$(1 - \epsilon) \frac{|C_{1,T}| |C_{2,T}|}{|A_{n-m}|}$$

ways. Applying Proposition 2.3 and arguing as above, we conclude that there exist subsets $X_T$ and $Y_T$ of $C_{1,T}$ and $C_{2,T}$, respectively, such that $X_T Y_T$ contains all elements of $S_n$ with fixed point set exactly $T$, and $|X_T|$ and $|Y_T|$ are bounded above by

$$c(n - m)!^{1/2} \log^{1/2}(n - m)!,$$

where $c$ is independent of $n$ or $m$. An upper bound for the cardinality of $\bigcup_T X_T$ is

$$cn \log n \sum_{n^{2/3} \leq m \leq 2n/3} \binom{n}{m} (n - m)!^{1/2}$$

$$\leq cn^3 \max \left\{ \binom{n}{m} (n - m)!^{1/2} \bigg| n^{2/3} \leq m \leq 2n/3 \right\} ,$$

and likewise for $\bigcup_T Y_T$.

For $m \geq n^{2/3}$, we have by Stirling’s approximation

$$m! > (m/e)^m .$$

So, when $n > (2e^2)^3$ is large enough, we have that

$$\frac{\binom{n}{m} (n - m)!^{1/2}}{(n!)^{1/2}} = \frac{\prod_{j=n-m+1}^{n} j^{1/2}}{m!} < \frac{n^{m/2}}{e^{-m} m^m}$$

$$= \left( \frac{e^2 n}{m^2} \right)^{m/2} < \left( \frac{e^2}{n^{1/3}} \right)^{(n^{2/3})/2} < \left( \frac{1}{2} \right)^{(n^{2/3})/2} < \frac{1}{cn^3} .$$
In this case, the cardinalities of $\bigcup_T X_T$ and $\bigcup_T Y_T$ are less than $n^{1/2}$. It follows that $X_1$, $X_2$, and all the $X_T$ together have cardinality $O((n!)^{1/2} \log^{1/2} n)$, and likewise for $Y$. That concludes the proof of Theorem 1.1 in the alternating case.

5. Groups as products of two subsets

**Lemma 5.1.** Let $G$ be a cyclic group of prime order $p$, and $x$ any real number with $2 \leq x \leq p$. Then there exist subsets $X$ and $Y$ of $G$ with $|X| \leq x$ and $|Y| \leq 2p/x$ such that $XY = G$.

**Proof.** Identify $G$ with the additive group $\mathbb{Z}/p\mathbb{Z}$ and its elements with 0, 1, \ldots, $p - 1$. The cases $2 \leq p \leq 7$ are obvious, so we will assume that $p \geq 11$. Since the roles of $x$ and $2p/x$ are symmetric, we may assume that $x \geq \sqrt{2p} > 4$. Now if $x \geq p - 2$ then $G = X + Y$ with $X := \{2j \mid 0 \leq j \leq (p - 1)/2\}$ and $Y = \{0, 1\}$. Suppose that $p - 2 > x \geq \sqrt{2p}$. Setting $a := \lfloor x \rfloor \leq x$ and $b := \lceil p/a \rceil \geq p/a$, we see that $b < \max(p/a + 1, 2p/x)$ and $G = X + Y$ for

$$X := \{0, 1, \ldots, a - 1\}, \quad Y = \{ja \mid 0 \leq j \leq b - 1\}.$$ 

**Lemma 5.2.** Let $G$ be a finite nonabelian simple group of order $n$. Then $G$ possesses a maximal subgroup $M$, with $|M| \geq \sqrt{n}$ if $G = J_3$ and $|M| \geq \sqrt{2n}$ otherwise.

**Proof.** The case of 26 sporadic simple groups can be checked using [Atlas]. If $G = A_n$ with $n \geq 5$, take $M := A_{n-1}$. So we may assume that $G$ is a finite simple group of Lie type. If $G$ is a classical group, then the smallest index of proper subgroups of $G$ is listed in [KL, Table 5.2.A], whence the statement follows. If $G$ is an exceptional group, then [MMT, Table 3.5] lists a subgroup $N$ of $G$, and one can check that $|N| \geq \sqrt{2n}$.

**Theorem 5.3.** Let $G$ be any finite group of order $n$, and $x$ any real number with $2 \leq x \leq n$. Then there exist subsets $X$ and $Y$ of $G$ with $|X| \leq x$ and $|Y| \leq 2n/x$ such that $XY = G$.

**Proof.** We proceed by induction on $|G|$. Note that the roles of $x$ and $y := 2n/x$ in the statement are symmetric, and so without loss of generality we may assume that $x \leq y$, that is $x \leq \sqrt{n}/2$.

(a) Suppose that there is a subgroup $H < G$ with $|H| > x$. By the induction hypothesis, there exist subsets $X'$, $Y' \subseteq H$ with $X'Y' = H$, $|X'| \leq x$, and $|Y'| \leq 2|H|/x$. Decompose $G = \bigcup_{i=1}^m H y_i$ with $m = [G : H]$, and let $X := X'$ and $Y := \bigcup_{i=1}^m Y' y_i$. Then $XY = G$, $|X| \leq x$, and $|Y| \leq m|Y'| \leq 2|G|/x$. 

Learn more about academic publishing with Cambridge Core.
Next, let us consider the possibility that $H < G$ is a subgroup with $x/2 < |H| < x$. Then setting $X := H$ and $Y$ a set of coset representatives of $H$ in $G$, we get $G = XY$, $|X| \leq x$, and $|Y| = [G : H] \leq 2n/x$.

Thus we are done if $G$ possesses a proper subgroup of order $\geq x/2$.

(b) Suppose now that $G$ admits a nontrivial normal subgroup $H$ with $|H| < x/2$. By the induction hypothesis applied to $G/H$ and $x' := x/|H|$, there exist subsets $X', Y' \subseteq G/H$ with $|X'| \leq x'$, $|Y'| \leq 2|G/H|/x' = 2n/x$, and $X'Y' = G/H$. Now let $X$ denote the full inverse image of $X'$ in $G$, and let $Y$ denote a set of coset representatives in $G$ for $Y'$. Then $G = XY$, $|X| = |X'| \cdot |H| \leq x$, and $|Y| = |Y'| \leq 2n/x$.

(c) Assume that $G$ is not simple: $1 \neq N < G$ for some $N < G$. If $|N| \geq x/2$, then we are done by (a). Otherwise, we are done by (b).

It remains to consider the case when $G$ is simple. If $G$ is abelian, then we can apply Lemma 5.1. Otherwise, by Lemma 5.2 there is a maximal subgroup $M < G$ of order $\geq \sqrt{n} > x/2$, and so we are again done by (a).

\[ \text{COROLLARY 5.4. Any finite group } G \text{ admits a square root } R, \text{ that is, a subset } R \subseteq G \text{ such that } R^2 = G, \text{ with } |R| \leq \sqrt{8|G|}. \]

\textit{Proof.} Taking $x = \sqrt{2|G|}$ in Theorem 5.3, we see that $G = XY$ with $|X|, |Y| \leq x$. Now set $R := X \cup Y$. \qed

6. Square roots of a Lie group

In this section we show that the results of Section 5 extend in a suitable sense to compact Lie groups. We would like to say that the minimum dimension of a square root of $G$ is half the dimension of $G$, but we need a suitable definition of dimension. Hausdorff dimension does not do the job; indeed, it is not difficult to see that $S^1$ can be written as $XY$, where $X$ and $Y$ are both of Hausdorff dimension 0. It turns out that upper Minkowski dimension is the better notion for our purposes.

We begin by recalling some basic definitions. A good reference is [Ta]. For $\delta > 0$, we define the $\delta$-packing number of a bounded metric space $X$, $N_\delta(X)$, to be the maximum number of disjoint open balls of radius $\delta$ in $X$. We recall that the upper Minkowski dimension, $\overline{\dim} X$, of a bounded metric space $X$ is given by the formula

$$\overline{\dim} X = \limsup_{\delta > 0} -\frac{\log N_\delta(X)}{\log \delta}.$$ 

If $\phi : X \to Y$ is a surjective Lipschitz map with constant $L$, then $N_{L\delta}(Y) \leq N_\delta(X)$, so $\overline{\dim} \phi(X) \leq \overline{\dim} X$. 

Downloaded from https://www.cambridge.org/core. IP address: 52.11.211.149, on 17 Oct 2019 at 11:13:54, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/fms.2015.4
If $[-1, 1]$ is endowed with the usual metric $d(x, y) = |x - y|$, then

$$N_\delta([-1, 1]) = \lfloor 1/\delta \rfloor,$$

and it follows that $\overline{\dim} [-1, 1] = 1$. If the ring $\mathbb{Z}_p$ of $p$-adic integers is endowed with the usual metric $d(x, y) = |x - y|_p$, it follows that

$$N_\delta(\mathbb{Z}_p) = p^{\max(0, 1 + \lfloor -\log_p \delta \rfloor)},$$

so $\overline{\dim} \mathbb{Z}_p = 1$.

Upper Minkowski dimension is well suited to our purposes because of the following elementary proposition, which is well known for subsets of Euclidean spaces [Ma, 8.10–8.11].

**Proposition 6.1.** Let $(X, d_X)$ and $(Y, d_Y)$ be bounded metric spaces, and let $d$ be a metric on $X \times Y$ such that

$$\max(d_X(x_1, x_2), d_Y(y_1, y_2)) \leq d((x_1, y_1), (x_2, y_2)) \leq d_X(x_1, x_2) + d_Y(y_1, y_2).$$

Then

$$\overline{\dim} X \times Y \leq \overline{\dim} X + \overline{\dim} Y,$$

with equality if $\log N_\delta(X)/ \log \delta$ and $\log N_\delta(Y)/ \log \delta$ both converge as $\delta \to 0$.

**Proof.** If $x_1, \ldots, x_m$ are the centers of a maximal collection of disjoint open balls of radius $\delta$ in $X$, then balls of radius $2\delta$ centered at $x_1, \ldots, x_m$ cover $X$, and likewise for $Y$. The product of any ball of radius $2\delta$ in $X$ and any ball of radius $2\delta$ in $Y$ is contained in some ball of radius $4\delta$ in $X \times Y$, so $X \times Y$ can be covered by $N_\delta(X)N_\delta(Y)$ balls of radius $4\delta$. Given any disjoint collection of balls of radius $4\delta$ in $X \times Y$, no two centers can lie in the same ball of radius $4\delta$. Thus,

$$N_{4\delta}(X \times Y) \leq N_\delta(X)N_\delta(Y),$$

which proves (6.1). On the other hand, if $x_1, \ldots, x_m$ are centers of disjoint balls of radius $\delta$ in $X$ and $y_1, \ldots, y_n$ are centers of disjoint balls of radius $\delta$ in $Y$, then $(x_i, y_j)$ are the centers of disjoint balls of radius $\delta$ in $X \times Y$, so

$$N_\delta(X \times Y) \geq N_\delta(X)N_\delta(Y).$$

It follows that

$$\lim_{\delta \to 0} \frac{-\log N_\delta(X \times Y)}{\log \delta} = \lim_{\delta \to 0} \frac{-\log N_\delta(X)}{\log \delta} + \lim_{\delta \to 0} \frac{-\log N_\delta(Y)}{\log \delta}$$

if both limits on the right-hand side exist. \qed
Now let $G$ be a compact Lie group. We say that a metric $d$ on $G$ is compatible if it is left invariant and right invariant by $G$ and there exists a coordinate map from some open neighborhood of the identity $e$ of $G$ to some open set in $\mathbb{R}^n$ which is Lipschitz in some neighborhood of $e$. If this is true for some coordinate map, it is true for all coordinate maps at $e$, since smooth maps between open sets in $\mathbb{R}^n$ are locally Lipschitz. Likewise, a compatible metric on a compact $p$-adic Lie group is a translation-invariant metric for which there exists a coordinate map from some open neighborhood of $e$ to some open set in $\mathbb{Q}_p^n$, and the choice of coordinate map does not matter. We recall [Bo, III, Section 4, no. 3] that every real (respectively, $p$-adic) Lie group admits an exponential map from a neighborhood of 0 in $\mathbb{R}^n$ (respectively, $\mathbb{Q}_p^n$) which is bijective and whose inverse is a coordinate map.

**Proposition 6.2.** Let $G$ be a compact Lie group endowed with a compatible metric. Then $\dim G$ coincides with the usual topological dimension of $G$.

**Proof.** By Proposition 6.1, $\dim I^n = n$, where $I$ is any open interval in $\mathbb{R}$, and it follows that $\dim U = n$ for any bounded open set in $\mathbb{R}^n$. If $\phi : U \to G$ is a bi-Lipschitz coordinate map, then $U' := \phi(U)$ is an open subset of $G$ of dimension $n$. Therefore, any translate of $U'$ in $G$ has dimension $n$, and likewise for any finite union of such translates. By compactness, $G$ itself is such a union, so $\dim G = \dim G$. □

There is also a $p$-adic version of the same proposition, whose proof is the same.

**Proposition 6.3.** Let $G$ be a compact $p$-adic Lie group endowed with a compatible metric. Then $\dim G$ coincides with the usual topological dimension of $G$.

We can now prove our lower bound for square roots of a real or $p$-adic Lie group.

**Proposition 6.4.** If $X$ and $Y$ are subsets of a compact real or $p$-adic Lie group $G$ endowed with a compatible metric $d$ and $XY = G$, then $\dim X + \dim Y \geq \dim G$. In particular, if $X$ is a square root of $G$, $\dim X \geq (\dim G)/2$.

**Proof.** Defining the metric $e$ on $G \times G$ by
\[
e((g_1, h_1), (g_2, h_2)) := d(g_1, g_2) + d(h_1, h_2),
\]
we have
\[
d(g_1h_1, g_2h_2) \leq d(g_1h_1, g_1h_2) + d(g_1h_2, g_2h_2) = e((g_1, h_1), (g_2, h_2)).
\]
Thus, the multiplication map $m : G \times G \to G$ is Lipschitz. It follows that

$$\dim \overline{XY} = \overline{\dim m(X \times Y)} \leq \dim X \times Y \leq \dim X + \dim Y.$$ 

If $XY = G$, then

$$\dim X + \dim Y \geq \dim G = \dim G.$$ 

The more interesting direction is the converse.

**Theorem 6.5.** Let $G$ be a compact real or $p$-adic Lie group, endowed with a compatible metric. Then $G$ has a square root of dimension $(\dim G)/2$.

**Proof.** Let $G$ be a real (respectively, $p$-adic) Lie group, $L$ the Lie algebra, and $\exp$ the exponential map from a neighborhood $U$ of $0$ in $L$ to a neighborhood $N$ of $e \in G$. Let $v \in L$ be a sufficiently small nonzero element, specifically, an element satisfying $[-1, 1]v \subset U$ (respectively, $\mathbb{Z}_p v \subset U$). Then the function $e_v : [-1, 1] \to G$ (respectively, $e_v : \mathbb{Z}_p \to G$) defined by $e_v(t) = \exp(tv)$ is Lipschitz. Let $C_v$ denote the image of $e_v$.

Choose a basis $v_1, \ldots, v_n$ of sufficiently small vectors in $L$. If $n = 2k$, let $X_0 = C_{v_1} \cdots C_{v_k}$ and $Y = C_{v_{k+1}} \cdots C_{v_{2k}}$. As $X_0$ and $Y$ are each images of sets of dimension $k$ under Lipschitz maps, $\dim X_0, \dim Y \leq k = (\dim G)/2$. On the other hand, $X_0Y$ contains a neighborhood of $e$ in $G$, so, letting $X$ denote a suitable finite union of left translates of $X$, we have $XY = G$ and $\dim X \leq k$. Thus $X \cup Y$ is a square root of $G$ of dimension $(\dim G)/2$.

If $n = 2k + 1$, we observe that there exist subsets $A$ and $B$ of $[-1, 1]$ such that $\overline{\dim A} = \overline{\dim B} = 1/2$ and $A + B = [-1, 1]$. We can take, for instance, the Cantor sets

$$A = -a_0 + \sum_{i=1}^{\infty} a_i 4^{-i}, \quad a_i \in \{0, 1\}; \quad B = \sum_{i=1}^{\infty} b_i 4^{-i}, \quad b_i \in \{0, 2\}.$$ 

Likewise, there exist $A, B \subset \mathbb{Z}_p$ of dimension $1/2$ such that $A + B = \mathbb{Z}_p$, for instance,

$$A = \sum_{i=1}^{\infty} a_i p^{2i}, \quad a_i \in \{0, 1, \ldots, p - 1\};$$

$$B = \sum_{i=1}^{\infty} b_i p^{2i}, \quad b_i \in \{0, p, 2p, \ldots, (p - 1)p\}.$$ 

Now, setting

$$X_0 = C_{v_1} \cdots C_{v_k} \exp(Av_{k+1}), \quad Y = \exp(Bv_{k+1})C_{v_{k+2}} \cdots C_{v_{2k+1}},$$
we see that
\[ X_0 Y = C_{v_1} \cdots C_{v_{2k+1}} \]
contains a neighborhood of \( e \), while \( \dim X_0, \dim Y \leq k + 1/2 \). The rest of the argument goes as before.

**Acknowledgements**

Michael Larsen was partially supported by NSF grant DMS-1101424 and a Simons Fellowship. Pham Huu Tiep was partially supported by NSF grant DMS-1201374 and the Simons Foundation Fellowship 305247.

**References**


