THE WARING PROBLEM FOR LIE GROUPS AND CHEVALLEY GROUPS

CHUN YIN HUI, MICHAEL LARSEN, ANER SHALEV

Abstract. The classical Waring problem deals with expressing every natural number as a sum of $g(k)$ k^{th} powers. Similar problems were recently studied in group theory, where we aim to present group elements as short products of values of a given word $w \neq 1$. In this paper we study this problem for Lie groups and Chevalley groups over infinite fields.

We show that for a fixed word $w \neq 1$ and for a classical connected real compact Lie group G of sufficiently large rank we have $w(G)^2 = G$, namely every element of G is a product of 2 values of w.

We prove a similar result for non-compact Lie groups of arbitrary rank, arising from Chevalley groups over $\mathbb{R}$ or over a p-adic field. We also study this problem for Chevalley groups over arbitrary infinite fields, and show in particular that every element in such a group is a product of two squares.

The first author was supported by ERC Advanced Grant no. 247034. The second author was partially supported by the Simons Foundation, the MSRI, NSF Grant DMS-1101424, and BSF Grant no. 2008194. The third author was partially supported by ERC Advanced Grant no. 247034, ISF grant no. 1117/13, BSF Grant no. 2008194 and the Vinik Chair of Mathematics which he holds.

1. Introduction

Let F_d be the free group on $x_1, \ldots, x_d$ and let $w = w(x_1, \ldots, x_d) \in F_d$ be a word. For every group G there is a word map $w = w_G : G^d \to G$ obtained by substitution. The image of this map is denoted by $w(G)$. The theory of word maps has developed significantly in the past decade; see [La, Sh1, S, LaSh1, LaSh2, LOST, LST, AGKSh, Sh2] and the references therein.

A major goal in these investigations is to prove theorems of "Waring type", i.e., to find small k such that, for every word $w \neq 1$ and for various groups G we have $w(G)^k = G$, namely every element of G is a product of k values of w.

A theorem of Borel [Bo1] states that if w is a non-trivial word then the word map it induces on simple algebraic groups G is dominant. Thus $w(G)$ contains a dense open subset, which easily implies $w(G(F))^2 = G(F)$ where F is an algebraically closed field (see Corollary 2.2 in [Sh2]). However, much more effort is required in order to prove similar results for fields F (finite or infinite) which are not algebraically closed.

In [Sh1] it is shown that, fixing $w \neq 1$, we have $w(G)^3 = G$ for all sufficiently large (nonabelian) finite simple groups G. This is improved in [LaSh1, LaSh2, LST] to $w(G)^2 = G$. Results of type $w(G)^3 = G$ were recently obtained in [AGKSh] for p-adic groups $G(\mathbb{Z}_p)$.

The purpose of this paper is to study similar problems for Lie groups and for infinite Chevalley groups. Our main results are as follows.

Theorem 1.1. *For every two non-trivial words w_1, w_2 there exists $N = N(w_1, w_2)$ such that if G is a classical connected real compact Lie group of rank at least N then*

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

In particular, for any $w \neq 1$ there is $N = N(w)$ such that $w(G)^2 = G$ for all classical connected real compact Lie groups of rank at least N.

We note that the assumption that the rank of G is large is necessary. By a theorem of E. Lindenstrauss (private communication) and A. Thom [T, Cor. 1.2], for any $n \geq 2$ and $\epsilon > 0$ there exists a word $1 \neq w \in F_2$ such that all elements of $w(\mathrm{U}(n))$ have distance $\leq \epsilon$ from the identity; here $\mathrm{U}(n)$ is the (anisotropic) unitary group of rank n over $\mathbb{R}$. Embedding a given G in $\mathrm{U}(n)$, we can arrange that $w(G)^2 \neq G$ or even $w(G)^k \neq G$ for any fixed k. We can also find a sequence $\{w_i\}$ of non-trivial words in two variables such that, for every compact group G, $w_i(G)$ converges to 1. On the other hand, we obtain a width two result for any connected real compact Lie group. Here S^1 denotes the unit circle of $\mathbb{C}^*$ as a maximal torus of SU(2), and $i = \sqrt{-1}$.

Theorem 1.2. *Let G be a connected compact semisimple real Lie group and w_1, w_2 non-trivial words.*

(i) *If $i \in S^1 \cap w_1(\mathrm{SU}(2)) \cap w_2(\mathrm{SU}(2))$, then $w_1(G)w_2(G) = G$.*
(ii) *If $w_1(\mathrm{SU}(2))^2 = \mathrm{SU}(2)$, then $w_1(G)^2 = G$.*

We also establish a width 2 result for non-compact Lie groups which arise from Chevalley groups over $\mathbb{R}$ or over a p-adic field. By a (simple) Chevalley group over a field F we mean a group generated by the root groups $X_\alpha(F)$ associated to a faithful representation of a complex (simple) semisimple Lie algebra (see [St, §3]), or equivalently, the commutator subgroup of $G_F(F)$, where G_F is a split (quasisimple) semisimple algebraic group over F. In this case there is no large rank assumption.

Theorem 1.3. *Let F be a field that contains either $\mathbb{R}$ or $\mathbb{Q}_p$ for some prime number p. Let w_1,w_2 be non-trivial words and G a simple Chevalley group over F. Then*

$$G \setminus Z(G) \subset w_1(G)w_2(G).$$

In particular, if $Z(G) = \{1\}$, then $w_1(G)w_2(G) = G$.

Without assumptions on the center of G this result easily implies $w_1(G)w_2(G)w_3(G) = G$ for any non-trivial words w_1, w_2, w_3.

Our last results deal with Chevalley groups over an arbitrary infinite field F. Here we have a general width 4 result, and width 3 and 2 in special cases.

Theorem 1.4. *Let w_1,w_2,w_3,w_4 be non-trivial words and let F be an infinite field.*

(i) *If G is a simple Chevalley group over F, then*
$$G \setminus Z(G) \subseteq w_1(G)w_2(G)w_3(G)w_4(G).$$
In particular, if $Z(G) = \{1\}$, then $w_1(G)w_2(G)w_3(G)w_4(G) = G$.
(ii) *If $G = \mathrm{SL}_n(F)$ and $n > 2$, then*
$$G \setminus Z(G) \subseteq w_1(G)w_2(G)w_3(G).$$
Hence, $w_1(\mathrm{PSL}(n,F))w_2(\mathrm{PSL}(n,F))w_3(\mathrm{PSL}(n,F)) = \mathrm{PSL}(n,F)$.

For some specific words we obtain stronger results.

Theorem 1.5. *Let $w_1 = x^m$ and $w_2 = y^n$ where m,n are positive integers. Let G be a Chevalley group over an infinite field F.*

(i) *If G is a simple Chevalley group, then*

$$G \setminus Z(G) \subseteq w_1(G)w_2(G).$$

In particular, if $Z(G) = \{1\}$ then $w_1(G)w_2(G) = G$.

(ii) *If $m = n = 2$, then*

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

We also give an example showing that a non-trivial central element is not in the image of the word map x^4y^4 (Proposition 4.1). See also [LaSh3] for the probabilistic behavior of word maps induced by x^my^n on finite simple groups.

The fact that every element of G above is a product of two squares can be regarded as a non-commutative analogue of Lagrange's four squares theorem. A similar result for finite quasisimple groups can be found in [LST2].

This paper is organized as follows. In Section 2 we deal with compact Lie groups and prove Theorems 1.1 and 1.2. Section 3 is devoted to the proof of Theorem 1.3, and Theorems 1.4 and 1.5 are proved in Section 4.

2. Compact Lie groups

In this section we provide solutions for Waring type problems with width two for classical connected real compact Lie groups G with large rank, thus proving Theorem 1.1. It suffices to work with simply connected groups G, i.e. with $\mathrm{SU}(n)$, $\mathrm{Sp}(n)$, and $\mathrm{Spin}(n)$. Let us start with Gotô's theorem.

Theorem 2.1. [Go] *Let G be a connected compact semisimple Lie group and T a maximal torus of G. Then there exists $x \in N_G(T)$ such that $\mathrm{Ad}(x) - 1$ is non-singular on $\mathrm{Lie}(T)$. Hence, every element g of G is conjugate to $[x, t] := xtx^{-1}t^{-1}$ for some $t \in T$.*

Let w_1 and w_2 be non-trivial words. Every element of G can be conjugated into T so the width two result for G follows if we can prove $T \subset w_1(G)w_2(G)$. By Gotô's theorem, it suffices to show that $x \in w_1(G)$ and $x^{-1} \in w_2(G)$. This will be achieved by using the principal homomorphism [Se]. Identify S^1, the subgroup of the unit circle of $\mathbb{C}^*$, as a maximal torus of $\mathrm{SU}(2)$.

Lemma 2.2. *The primitive nth roots of unity $\zeta_n^{\pm 1} := e^{\pm\frac{2\pi i}{n}}$ both belong to $w_i(\mathrm{SU}(2)) \cap S^1$ for $i = 1, 2$ if n is sufficiently large.*

Proof. Since w_1 and w_2 are non-trivial, $w_i(\mathrm{SU}(2))$ contains a non-empty open subset of $\mathrm{SU}(2)$ for $i = 1, 2$ [La, Cor. 5]. As $\mathrm{SU}(2)$ is compact and connected and x and x^{-1} are conjugate for any $x \in \mathrm{SU}(2)$, it follows that $w_i(\mathrm{SU}(2)) \cap S^1$ is a closed arc and also a symmetric neighborhood of 1 in S^1 for $i = 1, 2$. Hence, the primitive n-th roots of unity $\zeta_n, \zeta_n^{-1} \in S^1$ belong to $w_i(\mathrm{SU}(2))$ for $i = 1, 2$ if n is sufficiently large. $\square$

Definition 1. We make the following definitions.

(1) Let I_n be the identity complex $n \times n$ matrix.
(2) Let 0_n be the zero complex $n \times n$ matrix.
(3) Let E_n^i be the diagonal complex $n \times n$ matrix whose (i, i)-entry is 1 and all other entries 0.
(4) Let L_n^i be the linear functional on diagonal complex $n \times n$ matrices such that $L_n^i(E_n^j) = \delta_{ij}$ (Kronecker delta) for all $1 \leq j \leq n$.
(5) Let $s_n \in \mathrm{U}(n)$ be the n-cycle

$$\begin{pmatrix} 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}.$$

Theorem 2.3. *For any non-trivial words w_1, w_2 and a sufficiently large n we have*

$$\mathrm{SU}(n) = w_1(\mathrm{SU}(n)) w_2(\mathrm{SU}(n)).$$

Proof. Consider the commutative diagram

$$\begin{array}{ccc} \mathrm{SL}(2,\mathbb{C}) & \xrightarrow{\widetilde{p}} & \mathrm{SL}(n,\mathbb{C}) \\ & \searrow^{p} & \downarrow{\scriptstyle \pi} \\ & & \mathrm{PSL}(n,\mathbb{C}) \end{array}$$

where p is the principal homomorphism associated to simple roots [FH]

$$\Delta := \{L_n^1 - L_n^2, L_n^2 - L_n^3, \dots, L_n^{n-1} - L_n^n\},$$

π the adjoint quotient, and $\widetilde{p}$ a lifting of p. Let

$$H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathfrak{sl}(2, \mathbb{C}).$$

The homomorphism $\widetilde{p}$ is isomorphic to Sym^{n-1} since $\alpha(d\widetilde{p}(H)) = 2$ for all $\alpha \in \Delta$ [Se, §2.3]. By restricting to suitable maximal compact subgroups, we obtain $\widetilde{p} : \mathrm{SU}(2) \to \mathrm{SU}(n)$. Identify S^1 as a maximal torus of $\mathrm{SU}(2)$. The set of eigenvalues of $\widetilde{p}(\zeta_m)$ is

$$\{\zeta_m^{n-1}, \zeta_m^{n-3}, \dots, \zeta_m^{3-n}, \zeta_m^{1-n}\}.$$

Then $\widetilde{p}(\zeta_{2n})$ is conjugate to $x_n := s_n$ if n is odd and $\widetilde{p}(\zeta_{2n})$ is conjugate to $x_n := s_n \cdot \zeta_{2n} I_n$ if n is even by comparing eigenvalues. Let T be the diagonal maximal torus of $\mathrm{SU}(n)$. Since $\mathrm{Ad}(x_n) - 1$ is non-singular on $\mathrm{Lie}(T)$ for all n, $x_n \in w_1(\widetilde{p}(\mathrm{SU}(2)))$ and $x_n^{-1} \in w_2(\widetilde{p}(\mathrm{SU}(2)))$ for $n \gg 0$ by Lemma 2.2, we are done by Gotô's theorem. □

Next, we work with the real compact symplectic group

$$\mathrm{Sp}(n) := \mathrm{U}(2n) \cap \mathrm{Sp}(2n, \mathbb{C}),$$

where $\mathrm{Sp}(2n, \mathbb{C})$ is the subgroup of $\mathrm{GL}(2n, \mathbb{C})$ that preserves the form

$$\begin{pmatrix} 0_n & I_n \\ -I_n & 0_n \end{pmatrix}.$$

Theorem 2.4. *For any non-trivial words w_1, w_2 and a sufficiently large n we have*

$$\mathrm{Sp}(n) = w_1(\mathrm{Sp}(n)) w_2(\mathrm{Sp}(n)).$$

Proof. Let T be the maximal torus of $\mathrm{Sp}(n)$ consisting of diagonal matrices with complex entries. Let $x_n \in N_{\mathrm{Sp}(n)}(T)$ be the element

$$\begin{pmatrix} s_n & 0_n \\ 0_n & s_n \end{pmatrix} \cdot \begin{pmatrix} I_n - E_n^1 & E_n^1 \\ -E_n^1 & I_n - E_n^1 \end{pmatrix}.$$

Then it is easy to see that $\mathrm{Ad}(x_n) - 1$ is non-singular on $\mathrm{Lie}(T)$. By Gotô's theorem, it suffices to show that $x_n \in w_1(\mathrm{Sp}(n))$ and $x_n^{-1} \in w_2(\mathrm{Sp}(n))$ for all sufficiently large n.

Consider the commutative diagram

$$\begin{array}{ccc} \mathrm{SL}(2,\mathbb{C}) & \xrightarrow{\widetilde{p}} & \mathrm{Sp}(2n,\mathbb{C}) \\ & \searrow^{p} & \downarrow \pi \\ & & \mathrm{PSp}(2n,\mathbb{C}) \end{array}$$

where p is the principal homomorphism associated to simple roots [FH]

$$\Delta := \{L_{2n}^1 - L_{2n}^2, L_{2n}^2 - L_{2n}^3, ..., L_{2n}^{n-1} - L_{2n}^n, 2L_{2n}^n\},$$

π the adjoint quotient, and $\widetilde{p}$ a lifting of p. Let $H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathfrak{sl}(2, \mathbb{C})$. Since $\alpha(d\widetilde{p}(H)) = 2$ for all $\alpha \in \Delta$ [Se, §2.3], the set of weights of $\widetilde{p}$, viewed as a $2n$-dimensional representation, is

$$\{2n-1, 2n-3, ..., 1, -1, ..., 3-2n, 1-2n\}.$$

By restricting to suitable maximal compact subgroups, we obtain $\widetilde{p} : \mathrm{SU}(2) \to \mathrm{Sp}(n)$.

Identify S^1 as a maximal torus of SU(2). The set of eigenvalues of $\widetilde{p}(\zeta_m)$ is

$$\{\zeta_m^{2n-1}, \zeta_m^{2n-3}, ..., \zeta_m^{3-2n}, \zeta_m^{1-2n}\}.$$

Define $e_1 := (1, 0, ..., 0) \in \mathbb{C}^{2n}$. Since x_n satisfies $x_n^{2n} + 1 = 0$ and the set of vectors

$$\{x_n e_1, x_n^2 e_1, ..., x_n^{2n} e_1\}$$

is linearly independent, the characteristic polynomial of x_n is $t^{2n} + 1$. In $\mathrm{Sp}(n)$, the characteristic polynomial determines the conjugacy class. (Indeed, the diagonal matrices with entries $\lambda_1, \ldots, \lambda_n, \lambda_1^{-1}, \ldots, \lambda_n^{-1}$ form a single orbit under the action of the Weyl group.) Since $\widetilde{p}(\zeta_{4n})$ and x_n have the same characteristic polynomial, it follows that they are conjugate in $\mathrm{Sp}(n)$. Hence, x_n and x_n^{-1} respectively belong to $w_1(\widetilde{p}(\mathrm{SU}(2)))$ and $w_2(\widetilde{p}(\mathrm{SU}(2)))$ when n is sufficiently large by Lemma 2.2. We are done. □

We then consider the compact special orthogonal group $\mathrm{SO}(n)$ and its simply connected cover $\mathrm{Spin}(n)$ for $n \geq 3$.

Theorem 2.5. *For any non-trivial words w_1, w_2 and a sufficiently large n we have*

$$\mathrm{SO}(n) = w_1(\mathrm{SO}(n))w_2(\mathrm{SO}(n)).$$

Proof. Since we have a morphism $\mathrm{SO}(2n) \to \mathrm{SO}(2n+1)$ such that the image of a maximal torus of $\mathrm{SO}(2n)$ is a maximal torus of $\mathrm{SO}(2n+1)$, it suffices to deal with $\mathrm{SO}(2n)$. This is a maximal compact subgroup of $\mathrm{SO}(2n, \mathbb{C})$. Let $K(2n, \mathbb{C})$ be the subgroup of $\mathrm{SL}(2n, \mathbb{C})$ preserving the form

$$\begin{pmatrix} 0_n & I_n \\ I_n & 0_n \end{pmatrix}.$$

Since $K(2n, \mathbb{C})$ is isomorphic to $\mathrm{SO}(2n, \mathbb{C})$ [FH] and has a diagonal maximal torus, we use $K(2n, \mathbb{C})$ and $K(2n) := \mathrm{U}(2n) \cap K(2n, \mathbb{C})$ (a maximal compact of $K(2n, \mathbb{C})$) instead of $\mathrm{SO}(2n, \mathbb{C})$ and $\mathrm{SO}(2n)$. One checks that the diagonal maximal torus T of $K(2n)$ is equal to the diagonal maximal torus of $\mathrm{Sp}(n)$. Let s'_{n-1} be the $n \times n$ matrix

$$\begin{pmatrix} 1 & 0 & ... & 0 & 0 \\ 0 & 0 & ... & 0 & 1 \\ 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & 1 & 0 \end{pmatrix}$$

which fixes $e_1 := (1, 0, ..., 0) \in \mathbb{C}^n$ and is an $(n-1)$-cycle on the natural complement of e_1 in $\mathbb{C}^n$. Let $x_n \in N_{K(2n)}(T)$ be the element

$$\begin{pmatrix} s'_{n-1} & 0_n \\ 0_n & s'_{n-1} \end{pmatrix} \cdot \begin{pmatrix} I_n - E_n^1 - E_n^2 & E_n^1 + E_n^2 \\ E_n^1 + E_n^2 & I_n - E_n^1 - E_n^2 \end{pmatrix}.$$

By choosing the basis

$$\{E_{2n}^1 - E_{2n}^{n+1}, E_{2n}^2 - E_{2n}^{n+2}, ..., E_{2n}^n - E_{2n}^{2n}\}$$

for $\mathrm{Lie}(T)$, the $\mathrm{Ad}(x_n)$-action on $\mathrm{Lie}(T)$ is given by the $n \times n$ matrix

$$\begin{pmatrix} -1 & 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & ... & 0 & 1 \\ 0 & -1 & 0 & ... & 0 & 0 \\ 0 & 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & ... & 1 & 0 \end{pmatrix}.$$

One sees that $\mathrm{Ad}(x_n) - 1$ is non-singular on $\mathrm{Lie}(T)$. By Gotô's theorem, it suffices to show that $x_n \in w_1(K(2n))$ and $x_n^{-1} \in w_2(K(2n))$ for all sufficiently large n. Since x_n is conjugate in $\mathrm{GL}(2n, \mathbb{C})$ to the permutation matrix

$$\begin{pmatrix} 0 & 1 & 0 & ... & 0 & 0 \\ 1 & 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & ... & 0 & 1 \\ 0 & 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & ... & 1 & 0 \end{pmatrix},$$

the characteristic polynomial of x_n is $(t^2 - 1)(t^{2n-2} - 1)$.

Consider the commutative diagram

$$\begin{array}{ccc} \mathrm{SL}(2, \mathbb{C}) & \xrightarrow{\widetilde{p}} & K(2n, \mathbb{C}) \\ & \searrow^{p} & \downarrow \pi \\ & & K(2n, \mathbb{C})/\{\pm I_{2n}\} \end{array}$$

where p is the principal homomorphism associated to simple roots [FH]

$$\Delta := \{L_{2n}^1 - L_{2n}^2, L_{2n}^2 - L_{2n}^3, ..., L_{2n}^{n-1} - L_{2n}^n, L_{2n}^{n-1} + L_{2n}^n\},$$

π the adjoint quotient, and $\widetilde{p}$ a lifting of p. Let $H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathfrak{sl}(2, \mathbb{C})$. Since $\alpha(d\widetilde{p}(H)) = 2$ for all $\alpha \in \Delta$ [Se, §2.3], the multiset of weights of the $2n$-dimensional representation $\widetilde{p}$ is

$$\{2n-2, 2n-4, ..., 2, 0, 0, -2, ..., 4-2n, 2-2n\}.$$

By restricting to suitable maximal compact subgroups, we obtain $\widetilde{p} : \mathrm{SU}(2) \to K(2n)$. Identify S^1 as a maximal torus of $\mathrm{SU}(2)$. The multiset of eigenvalues of $\widetilde{p}(\zeta_m)$ is

$$\{\zeta_m^{2n-2}, \zeta_m^{2n-4}, ..., \zeta_m^{2}, 1, 1, \zeta_m^{-2}, ..., \zeta_m^{4-2n}, \zeta_m^{2-2n}\}.$$

It is not in general true that two diagonal orthogonal matrices are conjugate in $\mathrm{SO}(2n)$ if and only if they have the same characteristic polynomial, because the Weyl group of $\mathrm{SO}(2n)$ is only an index 2 subgroup of $S_n \ltimes (\mathbb{Z}/2\mathbb{Z})^n$. However, it is true in the case of matrices for which 1 is an eigenvalue. Since $\widetilde{p}(\zeta_{4n-4})$ and x_n both have characteristic polynomial

$$(t^2-1)(t^{2n-2}-1)$$

and have eigenvalue 1, it follows that they are conjugate in $K(2n)$. Hence, x_n and x_n^{-1} respectively belong to $w_1(\widetilde{p}(\mathrm{SU}(2)))$ and $w_2(\widetilde{p}(\mathrm{SU}(2)))$ when n is sufficiently large by Lemma 2.2. We are done. $\square$

Theorem 2.6. *For any non-trivial words w_1, w_2 and a sufficiently large n we have*

$$\mathrm{Spin}(n) = w_1(\mathrm{Spin}(n))w_2(\mathrm{Spin}(n)).$$

Proof. Since we have a morphism $\mathrm{Spin}(2n) \to \mathrm{Spin}(2n+1)$ such that the image of a maximal torus of $\mathrm{Spin}(2n)$ is a maximal torus of $\mathrm{Spin}(2n+1)$, it suffices to deal with $\mathrm{Spin}(2n)$. Consider the commutative diagram

$$\begin{array}{ccc} \mathrm{SU}(2) & \xrightarrow{\hat{p}} & \mathrm{Spin}(2n) \\ & \searrow^{\widetilde{p}} & \downarrow{\scriptstyle \widetilde{\pi}} \\ & & K(2n) \end{array}$$

where $\widetilde{\pi}$ is the natural projection and $\hat{p}$ is a lift of $\widetilde{p}$. Recall that the maximal torus T and the element $x_n \in N_{K(2n)}(T)$ are constructed in the proof of Theorem 2.5. Since x_n and x_n^{-1} respectively belong to $w_1(\widetilde{p}(\mathrm{SU}(2)))$ and $w_2(\widetilde{p}(\mathrm{SU}(2)))$ when n is sufficiently large, $w_1(\mathrm{Spin}(2n))$ and $w_2(\mathrm{Spin}(2n))$ respectively contain $\hat{x}_n$ and $\hat{x}_n^{-1}$ such that $\widetilde{\pi}(\hat{x}_n) = x_n$ by the diagram. Let $\hat{T}$ be the maximal torus of $\mathrm{Spin}(2n)$ such that $\widetilde{\pi}(\hat{T}) = T$. We also have $\hat{x}_n \in N_{\mathrm{Spin}(2n)}(\hat{T})$. Consider commutative diagram

$$\begin{array}{ccc} \mathrm{Lie}(\hat{T}) & \xrightarrow{\mathrm{Ad}(\hat{x}_n)-1} & \mathrm{Lie}(\hat{T}) \\ \downarrow{\scriptstyle d\widetilde{\pi}} & & \downarrow{\scriptstyle d\widetilde{\pi}} \\ \mathrm{Lie}(T) & \xrightarrow{\mathrm{Ad}(x_n)-1} & \mathrm{Lie}(T) \end{array}$$

Since $d\widetilde{\pi}$ and $\mathrm{Ad}(x_n) - 1$ are non-singular, $\mathrm{Ad}(\hat{x}_n) - 1$ is also non-singular. We are done by Gotô's theorem. □

We end this section with a proof of Theorem 1.2.

Proof. Let G be any connected compact semisimple real Lie group.

(i) Since $S^1 \cap w_i(\mathrm{SU}(2))$ $(i = 1, 2)$ is a connected closed arc, symmetric about the x-axis of the complex plane (Lemma 2.2), we obtain

$$\zeta_{2n}^{\pm} \in S^1 \cap w_1(\mathrm{SU}(2)) \cap w_2(\mathrm{SU}(2))$$

for all $n \geq 2$ by the assumption. Hence, $w_1(\mathrm{SU}(n))w_2(\mathrm{SU}(n)) = \mathrm{SU}(n)$ for all $n \geq 2$ by the proof of Theorem 2.3. Since every element of G is conjugate to some element in a maximal torus and G contains an equal rank semisimple subgroup H with type A simple factors, we are done.

(ii) There exists $x_1, x_2 \in w_1(\mathrm{SU}(2))$ such that $x_1x_2 = -1$. We may assume $x_1, x_2 \in S^1$. Then one sees easily that $\zeta_4 \in S^1 \cap w_1(\mathrm{SU}(2))$ by Lemma 2.2. We obtain $w_1(G)^2 = G$ by (i) □

3. Non-compact groups

In this section we study Waring type problems for split semisimple Lie groups G over a local field of characteristic 0 ($\mathbb{R}$, $\mathbb{C}$, or finite extension of $\mathbb{Q}_p$) and prove Theorem 1.3. A key result we need (related to the Thompson conjecture) was proved by Ellers and Gordeev [EG1, EG2, EG3]:

Theorem 3.1. *Let G be a simple Chevalley group over a field F. Let g_1 and g_2 be two regular semisimple elements in G from a maximal split torus and let C_1 and C_2 be the conjugacy classes of g_1 and g_2, respectively. Then*

$$G \setminus Z(G) \subseteq C_1C_2.$$

In order to prove Theorem 1.3 we also need the following.

Lemma 3.2. *Let F be an infinite field and w a non-trivial word of d letters. Then the following hold:*

(i) *$w(\mathrm{SL}_2(F))$ contains infinitely many semisimple elements of different traces.*
(ii) *If F contains either $\mathbb{R}$ or $\mathbb{Q}_p$ for some p, then $w(\mathrm{SL}_2(F))$ contains infinitely many split semisimple elements of different traces.*

Proof. Let F be an infinite field and F^* the non-zero elements of F. Let $\mathrm{SL}_2(F^*)$ be the subset of $\mathrm{SL}_2(F)$ such that all the four entries are non-zero. Then $\mathrm{SL}_2(F^*)$ is Zariski dense in SL_2. For any element

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathrm{SL}_2(F^*),$$

we can find three non-trivial F-morphisms from $\mathbb{A}^1$ to SL_2 with variable x that map 0 to A:

$$u_1(x) := \begin{pmatrix} a_1 & a_2 + x \\ a_3 & a_4 + b_1(x) \end{pmatrix},$$
$$u_2(x) := \begin{pmatrix} a_1 & a_2 \\ a_3 + x & a_4 + b_2(x) \end{pmatrix},$$
$$u_3(x) := \begin{pmatrix} a_1 + x & a_2 \\ a_3 + b_3(x) & a_4 \end{pmatrix},$$

where $b_1(x), b_2(x), b_3(x) \in F[x]$. The tangent vectors of the curves at A are:

$$\begin{pmatrix} 0 & 1 \\ 0 & b_1'(0) \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & b_2'(0) \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ b_3'(0) & 0 \end{pmatrix}$$

respectively, which are linearly independent and span the tangent space of SL_2 at A. Hence, we obtain a dominant F-morphism from $\mathbb{A}^3$ to SL_2 given by $(x, y, z) \mapsto u_1(x)u_2(y)u_3(z)$. Similarly, there exists a dominant F-morphism $U : \mathbb{A}^{3d} \to \mathrm{SL}_2^d$. For any non-constant F-morphism $\pi : \mathrm{SL}_2^d \to \mathbb{A}^1$, the composition $\pi \circ U : \mathbb{A}^{3d} \to \mathbb{A}^1$ is still non-constant. Therefore, one can find $f : \mathbb{A}^1 \to \mathrm{SL}_2^d$ (defined over F) such that $\pi \circ f : \mathbb{A}^1 \to \mathbb{A}^1$ is non-constant.

Put $\pi := \mathrm{Tr} \circ w$, the trace of word w. Since w is non-trivial, π is a non-constant morphism. Hence, we can find f as above such that $\pi \circ f \in F[x]$ is a non-constant polynomial. This proves (i).

Now suppose F contains either $\mathbb{R}$ or $\mathbb{Q}_p$ for some p. Put $\pi := (\mathrm{Tr} \circ w)^2 - 4$, the discriminant of word w. As $\mathbb{Q} \subset F$ is infinite, we find a $\mathbb{Q}$-morphism f to obtain a non-constant polynomial $\pi(f(x)) \in \mathbb{Q}[x]$. Then $P(x) := \mathrm{Tr}(w(f(x)) \in \mathbb{Q}[x]$ is also non-constant. To prove (ii), it suffices to show that $y^2 = P(x)^2 - 4$ has infinitely many solutions in the field F. We write $P(x) = c_0 + \cdots + c_k x^k$, where $c_k \neq 0$ and $k \geq 1$.

Consider the curve X over $\mathbb{Q}$ given in projective coordinates by

$$c_k^2 u^{2k} - \Big(\sum_{i=0}^{k} c_i v^i w^{k-i}\Big)^2 + 4w^{2k}.$$

As $P := (1 : 1 : 0)$ is a non-singular point, by the (real or p-adic) implicit function theorem, there is an infinite (real or p-adic) neighborhood of P in $X(F)$. Letting $y := c_k u^k / w^k$ and $x := v/w$, this implies that $y^2 = P(x)^2 - 4$ has infinitely many solutions in F. □

***Proof of Theorem 1.3*:**

Proof. In light of Theorem 3.1, it suffices to prove the theorem for $F = \mathbb{R}$ and $\mathbb{Q}_p$. Suppose w is a non-trivial word of d letters. Let D be the group of diagonal matrices in $\mathrm{SL}_2(F)$. Any Chevalley group G over F is the commutator subgroup of the group of F-rational points of a corresponding quasisimple algebraic group G_F, and we have the following commutative diagram of algebraic groups over F:

(1)
$$\begin{array}{ccc} \mathrm{SL}_{2,F} & \xrightarrow{\tilde{p}} & G_F \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} \\ \mathrm{PGL}_{2,F} & \xrightarrow{p} & G_F^{\mathrm{ad}} \end{array}$$

where π_1 and π_2 are adjoint quotient maps, G_F^{ad} is the adjoint group of G_F, p is the principal homomorphism associated to a system of simple roots [Se, §2], and $\tilde{p}$ is a lifting of p. Since $w(\mathrm{SL}_2(F))$ contains infinitely many elements in D by Lemma 3.2(ii) and the image of a generic element of $\pi_1(D) \subset \mathrm{PGL}_2(F)$ under p is regular [Se, §2.3], $w(\tilde{p}(\mathrm{SL}_2(F)))$ contains a regular split semisimple element. This semisimple element belongs to $w(G)$ since $\mathrm{SL}_2(F)$ is equal to its commutator subgroup [Th]. Therefore, we obtain

$$G \setminus Z(G) \subseteq w_1(G)w_2(G)$$

for non-trivial words w_1 and w_2 by Theorem 3.1. □

We now state some easy consequences of Theorem 1.3. Let F be as above.

Corollary 3.3. *Let w_1,w_2,w_3 be non-trivial words and G a Chevalley group over F. Then*

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

Proof. Suppose the Chevalley group G is associated to the complex semisimple Lie algebra $\mathfrak{g}$. Let $\widetilde{G}$ be the universal group [St, p.45] of G. We have a central extension $\pi : \widetilde{G} \to G$ [St, §7] and $\widetilde{G}$ is the direct product of universal groups $\widetilde{G_1}, ..., \widetilde{G_k}$ associated to simple factors of $\mathfrak{g}$. It suffices to prove the corollary for $\widetilde{G_i}$. By Theorem 1.3,

$$\widetilde{G_i} \backslash Z(\widetilde{G_i}) \subset w_1(\widetilde{G_i}) w_2(\widetilde{G_i}).$$

Since the center $Z(\widetilde{G_i})$ is finite, $w_3(\widetilde{G_i})$ contains some non-central element g. Then $g^{-1} \cdot Z(\widetilde{G_i}) \subset w_1(\widetilde{G_i}) w_2(\widetilde{G_i})$ and we are done. □

Corollary 3.4. *Let w_1,w_2 be non-trivial words and $G^{\mathrm{ad}} := G/Z(G)$ where G is a Chevalley group over F. Then*

$$G^{\mathrm{ad}} = w_1(G^{\mathrm{ad}}) w_2(G^{\mathrm{ad}}).$$

Proof. Suppose the Chevalley group G is associated to the complex semisimple Lie algebra $\mathfrak{g}$. Let $\widetilde{G}$ be the universal group of G. We have a central extension $\pi : \widetilde{G} \to G$ and $\widetilde{G}$ is the direct product of universal groups $\widetilde{G_i}$ associated to simple factors of $\mathfrak{g}$. Since the identity element of G always belongs to any word image and $\widetilde{G}/Z(\widetilde{G}) = G/Z(G)$, it suffices to prove the corollary for $\widetilde{G_i}$ which is done by Theorem 1.3. □

4. Chevalley groups

The method we used in §3 leads to the proof of Theorem 1.4, given below.

Proof. (i) Applying Theorem 3.1 it suffices to show that $w_1(G)w_2(G)$ and $w_3(G)w_4(G)$ contain split regular semisimple elements. By the principal homomorphism and diagram (1), it suffices to show that

$$w_1(\mathrm{SL}_2(F)) w_2(\mathrm{SL}_2(F))$$

contains an infinite set of split semisimple elements of $\mathrm{SL}_2(F)$ of different traces. Since F is infinite and the words are non-trivial, $w_1(\mathrm{SL}_2(F))$ and $w_2(\mathrm{SL}_2(F))$ both contain regular semisimple elements by Lemma 3.2(i). If either $w_1(\mathrm{SL}_2(F))$ or $w_2(\mathrm{SL}_2(F))$ contains split regular semisimple elements, then we are done. Otherwise, let C_1 and C_2 be conjugacy classes respectively of non-split regular semisimple elements of $w_1(\mathrm{SL}_2(F))$ and $w_2(\mathrm{SL}_2(F))$. Then the diagonal matrix $\mathrm{diag}(\lambda, \lambda^{-1}) \in C_1C_2$ if and only if $-\lambda \in \chi(C_1)\chi(C_2)$ [VW, Lemma 6.2], where $\chi(C_i)$ is the set of $(2,1)$ entries of C_i (*corner invariant*) for $i = 1, 2$ [VW, §3]. Since F is infinite, the corner invariants $\chi(C_1), \chi(C_2)$ are infinite and we are done.

(ii) An n by n matrix M is said to be *cyclic* if every Jordan block of M is of multiplicity one. Let G be $\mathrm{SL}_n(F)$ with $n > 2$. A conjugacy class C of G is cyclic if every element of C is cyclic. If C_1, C_2, C_3 are cyclic conjugacy classes of G, then any non-scalar element of G belongs to the product $C_1C_2C_3$ [Lev, Theorem 3]. Therefore, it suffices to show that $w_1(G)$ contains a cyclic element. Since F is infinite, $w_1(\mathrm{SL}_2(F))$ contains a regular semisimple element by Lemma 3.2(i). By the principal homomorphism and diagram (1), $w_1(G)$ contains a regular semisimple (and therefore cyclic) element g_1. □

Let us now prove Theorem 1.5.

Proof. (i) Since G is a simple Chevalley group over an infinite field, for every integer $k > 0$ it has a maximal split torus T containing a kth power which is split regular. Recall that $w_1 = x^m$ and $w_2 = y^n$. Therefore $w_1(T)$ and $w_2(T)$ both contain split regular semisimple elements. Thus, for $i = 1, 2$, $w_i(G)$ contains a conjugacy class of C_i of a split regular semisimple element. By Theorem 3.1, we obtain $G \setminus Z(G) \subseteq w_1(G)w_2(G)$, proving the result.

(ii) Suppose the Chevalley group G is associated to complex semisimple Lie algebra $\mathfrak{g}$. Let $\widetilde{G}$ be the universal group of G. We have the central extension $\pi : \widetilde{G} \to G$ and $\widetilde{G}$ is the direct product of universal groups $\widetilde{G_i}$ associated to simple factors of $\mathfrak{g}$. We just need to deal with the case that G is universal and $\mathfrak{g}$ is simple. Since $G \backslash Z(G) \subset w_1(G)w_2(G)$ by (i), it suffices to show $Z(G) \subset w_1(G)w_2(G)$. Let Λ and R be respectively the weight lattice and root lattice of $\mathfrak{g}$. We have [St, p.45]

$$Z(G) = \mathrm{Hom}(\Lambda/R, F^*)$$

and

Type of $\mathfrak{g}$	Λ/R
$A_n = \mathfrak{sl}(n+1)$ $(n \geq 1)$	$\mathbb{Z}/(n+1)\mathbb{Z}$
$B_n = \mathfrak{so}(2n+1)$ $(n \geq 2)$	$\mathbb{Z}/2\mathbb{Z}$
$C_n = \mathfrak{sp}(2n)$ $(n \geq 3)$	$\mathbb{Z}/2\mathbb{Z}$
$D_n = \mathfrak{so}(2n)$ $(n \geq 5$, odd$)$	$\mathbb{Z}/4\mathbb{Z}$
$D_n = \mathfrak{so}(2n)$ $(n \geq 4$, even$)$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
E_6	$\mathbb{Z}/3\mathbb{Z}$
E_7	$\mathbb{Z}/2\mathbb{Z}$
E_8	$\{1\}$
F_4	$\{1\}$
G_2	$\{1\}$

Since $|\Lambda/R|$ is odd if $\mathfrak{g} = \mathfrak{sl}(2n+1), E_6, E_8, F_4, G_2$ $(n \geq 1)$, every element of $Z(G)$ is a square in these cases. If $\mathrm{char}(F) = 2$, then $Z(G)$ is trivial for the remaining $\mathfrak{g}$ and (ii) is true. Assume $\mathrm{char}(F) \neq 2$.

Case $\mathfrak{g} = \mathfrak{sl}(2n)$ $(n \geq 1)$:
We have $G = \mathrm{SL}_{2n}(F)$ and $Z(G) = \{rI_{2n} : \ r \in F, \ r^{2n} = 1\}$. Define $J_r := \begin{pmatrix} 0 & 1 \\ r & 0 \end{pmatrix}$ whenever $r \in F$ is a (not necessarily primitive) $2n$-th root of unity. When $n = 1$, the non-trivial center of G is a square since

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = J_{-1}^2.$$

When $n > 1$, every center element of $\mathrm{SL}_{2n}(F)$ is a product of 2 squares since

$$rI_{2n} = \begin{pmatrix} J_r & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & J_r & 0 \\ 0 & \dots & 0 & J_r \end{pmatrix}^2$$

if $(-r)^n = 1$ and

$$rI_{2n} = \begin{pmatrix} I_2 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & I_2 & 0 \\ 0 & \dots & 0 & J_{-1} \end{pmatrix}^2 \begin{pmatrix} J_r & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & J_r & 0 \\ 0 & \dots & 0 & J_{-r} \end{pmatrix}^2$$

if $(-r)^n = -1$.

Case $\mathfrak{g} = \mathfrak{so}(2n+1)$ $(n \geq 2), \mathfrak{sp}(2n)$ $(n \geq 3), \mathfrak{so}(4n)$ $(n \geq 2), E_7$:
By using the facts that

- $\mathfrak{sp}(2) = \mathfrak{sl}(2) = \mathfrak{so}(3)$,
- $\mathfrak{sl}(2) \times \mathfrak{sl}(2) = \mathfrak{so}(4) \subset \mathfrak{so}(5) = \mathfrak{sp}(4)$,
- $\prod_1^7 \mathfrak{sl}(2) \subset E_7$,

there exists a semisimple subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ such that $\mathfrak{h}$ and $\mathfrak{g}$ have the same rank and every simple factor of $\mathfrak{h}$ is $\mathfrak{sl}(2)$. Since G is the commutator subgroup of $G_F(F)$, where G_F is a split, quasisimple algebraic group of type $\mathfrak{g}$, there exists a split, semisimple, algebraic subgroup $H_F \subset G_F$ of type $\mathfrak{h}$ (the Zariski closure in G_F of the group generated by $X_\alpha(F)$ for all α belonging to the root subsystem of $\mathfrak{h}$ in the root system of $\mathfrak{g}$) such that $Z(G) \subset Z(H_F)$. Let m be the rank of G_F and $\pi : \widetilde{H}_F \cong \prod_1^m \mathrm{SL}_2 \to H_F$ the universal cover. Since $Z(\widetilde{H}_F)$ surjects on

$Z(H_F)$,

$$Z(\widetilde{H}_F) = \prod_1^m Z(\mathrm{SL}_2) = \prod_1^m Z(\mathrm{SL}_2(F)),$$

and $-I_2$ is a square, every element of $Z(G)$ is a square in

$$\pi(\textstyle\prod_1^m \mathrm{SL}_2(F)) = \pi(\prod_1^m [\mathrm{SL}_2(F), \mathrm{SL}_2(F)])$$

$$\subset [H_F(F), H_F(F)] \subset [G_F(F), G_F(F)] = G.$$

We are done.

Case $\mathfrak{g} = \mathfrak{so}(4n+2)$ $(n \geq 2)$:
Since $\mathfrak{h} = \mathfrak{so}(6) \times \prod_1^{n-1} \mathfrak{so}(4)$ is a maximal rank semisimple subalgebra of $\mathfrak{g} = \mathfrak{so}(4n+2)$, we find a split, semisimple algebraic subgroup $H_F \subset G_F$ of type $\mathfrak{h}$ such that $Z(G) \subset Z(H_F)$. Let $\pi : \widetilde{H}_F \cong \mathrm{SL}_4 \times \prod_1^{n-1} \mathrm{SL}_3 \to H_F$ be the universal cover. Since $Z(G_F(\bar{F})) = \mathbb{Z}/4\mathbb{Z} \subset Z(H_F(\bar{F}))$ and $|Z(\mathrm{SL}_3(\bar{F}))|$ is odd, π is injective on SL_4. Since $Z(G)$ is a subgroup of $H_F(F)$ of order a power of 2,

$$Z(G) \subset \pi(\mathrm{SL}_4) \cap H_F(F) \cong \mathrm{SL}_4(F)$$

by injectivity. Since every element of $\mathrm{SL}_4(F)$ is a product of two squares from above and

$$\mathrm{SL}_4(F) = [\mathrm{SL}_4(F), \mathrm{SL}_4(F)] \subset [H_F(F), H_F(F)] \subset [G_F(F), G_F(F)] = G,$$

we are done. □

Let G be a Chevalley group of the form $\mathrm{SL}_2(F)$ for F an infinite field. If either m or n is congruent to 1, 2, or 3 (mod 4), then every element of G is of the form $x^m y^n$ since

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^k = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

if $k \equiv 2 \pmod 4$ (and of course odd powers preserve elements of $Z(G)$). However, this is not true in general.

Proposition 4.1. *If $G = \mathrm{SL}_2(F)$ where F is of characteristic zero and $[F(\zeta_8) : F] = 4$ (e.g., $F = \mathbb{Q}$), then x^4y^4 does* not *represent $-I_2$.*

Proof. If $A^4 = -B^4$ for elements $A, B \in \mathrm{SL}_2(F)$ and $\lambda^{\pm 1}$ and $\mu^{\pm 1}$ are respectively the eigenvalues of A and B, then without loss of generality we may assume $\lambda/\mu = \zeta_8$, and $\mathrm{Gal}(F(\zeta_8)/F) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ acts on $\{\lambda^{\pm 1}\}$ and $\{\mu^{\pm 1}\}$. One of the automorphisms $\zeta_8 \mapsto \zeta_8^3$ or $\zeta_8 \mapsto \zeta_8^7$ fixes exactly one of λ and μ, so either λ^2 or μ^2 lies in $\{\pm i\}$. However, λ and μ lie in quadratic extensions of F and by hypothesis, every primitive 8-th root of unity generates a degree 4 extension of F. □

References

[AGKSh] N. Avni, T. Gelander, M. Kassabov and A. Shalev, Word values in p-adic and adelic groups, *Bull. London Math. Soc.* **45** (2013), no. 6, 1323-1330.

[Bo1] A. Borel, On free subgroups of semisimple groups, *L'Enseignement Mathématique* (2) **29** (1983), no. 1-2, 151?64.

[EG1] E. W. Ellers and N. L. Gordeev, Gauss decomposition with prescribed semisimple part in classical Chevalley groups, *Communications in Algebra* **22** (1994, no.14), 5935-5950.

[EG2] E. W. Ellers and N. L. Gordeev, Gauss decomposition with prescribed semisimple part in classical Chevalley groups II: Exceptional cases, *Communications in Algebra* **23** (1995, no.8), 3085-3098.

[EG3] E. W. Ellers and N. L. Gordeev, Gauss decomposition with prescribed semisimple part in classical Chevalley groups III: Finite twisted groups, *Communications in Algebra* **24** (1996, no.14), 4447-4475.

[ET] A. Elkasapy and A. Thom, About Gotô's method showing surjectivity of word maps, *Indiana University Math. J.* **63** (2014), no. 5, 1553-1565.

[FH] W. Fulton and J. Harris, Representation Theory, Graduate Texts in Mathematics 129 (1st ed.), Springer-Verlag, Berlin, 1991.

[Go] M. Gotô, A theorem on compact semi-simple groups. *Journal of the Mathematical Society of Japan* **1**, (1949), 270–272.

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

[LaSh1] M. Larsen and A. Shalev, Word maps and Waring type problems, *Journal of the American Mathematical Society* **22** (2009), 437–466.

[LaSh2] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications, *Inventiones mathematicae* **174** (2008), no. 3, 645–687.

[LaSh3] M. Larsen and A. Shalev, On the distribution of values of certain word maps, *Transactions of the American Mathematical Society*, to appear, arXiv:1308.1286.

[Lev] A. Lev, Products of cyclic conjugacy classes in the groups $\mathrm{PSL}(n, F)$, *Linear Algebra and its Applications* **179** (1993), 59–83.

[LST] M. Larsen, A. Shalev and P. H. Tiep, The Waring problem for finite simple groups, *Annals of Mathematics* **174** (2011), 1885–1950.

[LST2] M. Larsen, A. Shalev and P. H. Tiep, Waring problem for finite quasisimple groups, *International Mathematics Research Notices* rns109 (2012), 26 pages.

[LOST] M. W. Liebeck, E. A. O'Brien, A. Shalev and P. H. Tiep, The Ore Conjecture, *Journal of the European Mathematical Society* **12** (2010), 939–1008.

[S] D. Segal, *Words: notes on verbal width in groups*, London Math. Soc. Lecture Note Series **361**, Cambridge University Press, Cambridge, 2009.

[Se] J.-P. Serre, Exemples de plongements des groupes $\mathrm{PSL}_2(\mathbb{F}_p)$ dans des groupes de Lie simples, *Inventiones mathematicae* **124**, (1996), 525–562.

[Sh1] A. Shalev, Word maps, conjugacy classes, and a non-commutative Waring-type theorem, *Annals of Mathematics* **170** (2009), 1383–1416.

[Sh2] A. Shalev, Some problems and results in the theory of word maps, *Erdős Centennial*, Lovász et al., eds Bolyai Soc. Math. Studies **25** (2013), 611–649.

[St] R. Steinberg, Lectures on Chevalley Groups, Yale University, 1967.

[T] A. Thom, Convergent sequences in discrete groups, *The Canadian Mathematical Bulletin* **56** (2013), no. 2, 424–433.

[Th] R. C. Thompson, Commutators in the special and general linear groups, *Transactions of the American Mathematical Society* **101** (1961), 16–33.

[VW] L. N. Vaserstein and E. Wheland, Products of conjugacy classes of two by two matrices, *Linear Algebra and its Applications* **230** (1995), 165–188.

Chun Yin Hui, Mathematics Research Unit, University of Luxembourg, 6 rue Richard Coudenhove-Kalergi, L-1359 Luxembourg
E-mail address: pslnfq@gmail.com

Michael Larsen, Department of Mathematics, Indiana University, Bloomington, IN 47405, U.S.A.
E-mail address: mjlarsen@indiana.edu

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