Some word maps that are non-surjective on infinitely many finite simple groups

Sebastian Jambor Martin W. Liebeck E.A. O'Brien

Abstract

We provide the first examples of words in the free group of rank 2 which are not proper powers and for which the corresponding word maps are non-surjective on an infinite family of finite non-abelian simple groups.

1 Introduction

The theory of word maps on finite non-abelian simple groups – that is, maps of the form $(x_1, \ldots, x_k) \to w(x_1, \ldots, x_k)$ for some word w in the free group F_k of rank k – has attracted much recent attention. It was shown in [6, 1.6] that for a given nontrivial word w, every element of every sufficiently large finite simple group G can be expressed as a product of $C(w)$ values of w in G, where $C(w)$ depends only on w; and this has been dramatically improved to $C(w) = 2$ in [4, 5, 11]. Improving $C(w)$ to 1 is not possible in general, as is shown by power words x_1^n, which cannot be surjective on any finite group of order non-coprime to n.

Certain words are surjective on all groups – namely, those in cosets of the form $x_1^{e_1} \ldots . x_k^{e_k} F_k'$ where the e_i are integers with $\gcd(e_1, ..., e_k) = 1$ (see [10, 3.1.1]). The word maps for a small number of other words have been shown to be surjective on all finite simple groups. These include the commutator word $[x_1, x_2]$ (the Ore conjecture [7]), the words $x_1^p x_2^p$ (for a prime p) and variants [3, 8]. Other studies have restricted the simple groups under consideration to families such as $\mathrm{PSL}_2(q)$ (see, for example, [1]). Motivating some of this work is a conjecture of Shalev, stated in [1, Conjecture 8.3]: if $w(x_1, x_2)$ is not a proper power of a non-trivial word, then the corresponding word map is surjective on $\mathrm{PSL}_2(q)$ for all sufficiently large q.

2010 *Mathematics Subject Classification: 20D05, 20E10*

Theorem 1 gives a family of words which are counterexamples to Shalev's conjecture. We believe these are the first non-power words to be proved non-surjective on an infinite family of finite simple groups.

Theorem 1. *Let $k \geq 2$ be an integer such that $2k+1$ is prime, and let w be the word $x_1^2[x_1^{-2}, x_2^{-1}]^k$. Let $p \neq 2k+1$ be a prime of inertia degree $m > 1$ in $\mathbb{Q}(\zeta + \zeta^{-1})$, where ζ is a primitive $(2k+1)$-th root of unity, and $\left(\frac{2}{p}\right) = -1$. Then the word map $(x, y) \to w(x, y)$ is non-surjective on $\mathrm{PSL}_2(q)$ for all $q = p^n$ where n is a positive integer not divisible by 2 or by m.*

Corollary 2. *Let $k \geq 2$ be an integer such that $2k+1$ is prime, and let w be the word $x_1^2[x_1^{-2}, x_2^{-1}]^k$. Let $p \neq 2k+1$ be an odd prime such that $p^2 \not\equiv 1 \bmod 16$ and $p^2 \not\equiv 1 \bmod (2k+1)$, and let m be the smallest positive integer with $p^{2m} \equiv 1 \bmod (2k+1)$. Then the word map $(x, y) \to w(x, y)$ is non-surjective on $\mathrm{PSL}_2(q)$ for all $q = p^n$ where n is a positive integer not divisible by 2 or by m.*

The corollary will be deduced from Theorem 1 at the end of the paper. Taking $k = 2$ we obtain the following.

Corollary 3. *If $w = x_1^2[x_1^{-2}, x_2^{-1}]^2$, then the word map $(x, y) \to w(x, y)$ is non-surjective on $\mathrm{PSL}_2(p^{2r+1})$ for all non-negative integers r and all odd primes $p \neq 5$ such that $p^2 \not\equiv 1 \bmod 16$ and $p^2 \not\equiv 1 \bmod 5$.*

2 Proof of Theorem 1

Let K be a field and $G = \mathrm{SL}_2(K)$, and let $\chi : G \to K$ be the trace map. A classical result of Fricke and Klein implies for every word $w \in F_2$, the free group of rank 2, there is a unique polynomial $\tau(w) \in \mathbb{Z}[s, t, u]$ such that for all $x, y \in G$, $\chi(w(x, y))$ is equal to $\tau(w)$ evaluated at $s = \chi(x)$, $t = \chi(y)$, $u = \chi(xy)$. We call $\tau(w)$ the *trace* polynomial of w. A proof of this fact, providing a constructive method of computing $\tau(w)$ for a given word w, can be found in [9, 2.2]. The method is based on the following identities for traces of 2×2 matrices A, B of determinant 1:

$$\begin{aligned}
&\mathrm{Tr}(AB) = \mathrm{Tr}(BA) \\
&\mathrm{Tr}(A^{-1}) = \mathrm{Tr}(A) \\
&\mathrm{Tr}(A^2B) = \mathrm{Tr}(A)\mathrm{Tr}(AB) - \mathrm{Tr}(B).
\end{aligned}$$

Lemma 2.1. *For $k \in \mathbb{N}$ and $w \in F_2$,*

$$(-1)^k + \sum_{i=1}^{k} (-1)^{k-i} \tau(w^i) = \prod_{i=1}^{k} (\tau(w) + \zeta^i + \zeta^{-i}),$$

where ζ is a primitive $(2k+1)$-th root of unity.

Proof. We adapt the proof of [9, Proposition 2.6]. Assume first that $w = x_1$. Let $A := \begin{pmatrix} 0 & 1 \\ -1 & s \end{pmatrix}$. By the uniqueness of the trace polynomial,

$\tau(w^i) = \mathrm{Tr}(A^i) = \mathrm{Tr}\begin{pmatrix} y^i & 0 \\ 0 & y^{-i} \end{pmatrix} = y^i + y^{-i}$, where $y + y^{-1} = s$. Hence

$$\begin{aligned} \textstyle\sum_{i=1}^{k}(-1)^{k-i}\tau(w^i) + (-1)^k &= \textstyle\sum_{i=1}^{k}(-1)^{k-i}y^i + \sum_{i=1}^{k}(-1)^{k-i}y^{-i} + (-1)^k \\ &= y^{-k}\textstyle\sum_{i=0}^{2k}(-1)^i y^i \\ &= y^{-k}\textstyle\prod_{i=1}^{2k}(y+\zeta^i) \\ &= \textstyle\prod_{i=1}^{k}(y+\zeta^i)(1+\zeta^{-i}y^{-1}) \\ &= \textstyle\prod_{i=1}^{k}(s+\zeta^i+\zeta^{-i}). \end{aligned}$$

Note that for $v, v_1, v_2 \in F_2$,

$$\tau(v(v_1, v_2)) = \tau(v)(\tau(v_1), \tau(v_2), \tau(v_1 v_2)),$$

so the general case is derived from the special case $w = x_1$ by polynomial evaluation at $s = \tau(w)$, i.e., setting $v = x_1^i$, $v_1 = w$, $v_2 = 1$. ■

Lemma 2.2. *Let $k \in \mathbb{N}$. The trace polynomial of $w = x_1^2[x_1^{-2}, x_2^{-1}]^k$ factors over $\mathbb{Z}[\zeta + \zeta^{-1}]$ as*

$$(s^2 - 2)\prod_{i=1}^{k}(s^4 - s^3tu + s^2t^2 + s^2u^2 - 4s^2 + 2 + \zeta^i + \zeta^{-i}),$$

where ζ is a primitive $(2k+1)$-th root of unity.

Proof. Let $c = [x_1^{-2}, x_2^{-1}]$. We claim that

$$\tau(x_1^2 c^k) = (\tau(x_1)^2 - 2)(\sum_{i=1}^{k}(-1)^{k-i}\tau(c^i) + (-1)^k).$$

The result then follows by Lemma 2.1, since $\tau(x_1) = s$ and $\tau(c) = s^4 - s^3tu + s^2t^2 + s^2u^2 - 4s^2 + 2$.

The proof is by induction on k. The claim is easily verified for $k = 1, 2$. For $k > 1$ it is equivalent to $\tau(x_1^2 c^k) = (\tau(x_1)^2 - 2)\tau(c^k) - \tau(x_1^2 c^{k-1})$. Using the rule $\tau(x^2 y) = \tau(x)\tau(xy) - \tau(y)$ for all $x, y \in F_2$ and the fact that $x_1^{-2}x_2^{-1} = x_2^{-1}x_1^{-2}c$, we deduce that

$$\begin{aligned} \tau(x_1^2 c^k) &= (\tau(x_1)^2 - 1)\tau(c^k) - \tau(x_1)\tau(x_1 x_2 x_1^{-2} x_2^{-1} c^{k-1}) \\ &= (\tau(x_1)^2 - 1)\tau(c^k) - \tau(x_1)\tau(x_1^{-1} c^k) \\ &= (\tau(x_1)^2 - 1)\tau(c^k) - \tau(x_1^{-2} c^k) - \tau(c^k). \end{aligned}$$

Thus it suffices to prove that $\tau(x_1^{-2}c^k) = \tau(x_1^2 c^{k-1})$. Now $\tau(x_1^{-2}c^k) = \tau(c)\tau(c^{k-1}x_1^{-2}) - \tau(c^{k-2}x_1^{-2})$. By induction, for $k \geq 3$ this is equal to $\tau(c)\tau(x_1^2 c^{k-2}) - \tau(x_1^2 c^{k-3})$, which is equal to $\tau(x_1^2 c^{k-1})$. ■

Proof of Theorem 1

Let $q = p^n$ be as in the hypothesis of the theorem, let $K = \mathbb{F}_q$, and let w be the word $x_1^2[x_1^{-2}, x_2^{-1}]^k$. The ring of integers of $\mathbb{Q}(\zeta + \zeta^{-1})$ is $\mathbb{Z}[\zeta + \zeta^{-1}]$ (see [12, Proposition 2.16]). Since $2k+1$ is prime, $\mathbb{Z}[\zeta + \zeta^{-1}] = \mathbb{Z}[\zeta^i + \zeta^{-i}]$ for every $1 \leq i \leq k$. Let $P \trianglelefteq \mathbb{Z}[\zeta^i + \zeta^{-i}]$ be a prime above p. Then $\mathbb{Z}[\zeta^i + \zeta^{-i}]/P = \mathbb{F}_{p^m}$, in particular $\zeta^i + \zeta^{-i}$ is a primitive element of $\mathbb{F}_{p^m}$ for every $1 \leq i \leq k$.

Suppose that some triple $(s,t,u) \in \mathbb{F}_q^3$ is a zero of the trace polynomial $\tau(w)$. By Lemma 2.2, $\tau(w)$ factors as

$$(s^2-2)\prod_{i=1}^{k}(s^4 - s^3tu + s^2t^2 + s^2u^2 - 4s^2 + 2 + \zeta^i + \zeta^{-i}),$$

over $\mathbb{F}_{p^m}$, so $(s,t,u) \in \mathbb{F}_q^3 \subseteq \mathbb{F}_{q^m}^3$ must be a zero of one of the factors. Since s^2-2 is irreducible over $\mathbb{F}_q$, (s,t,u) must be a zero of $s^4 - s^3tu + s^2t^2 + s^2u^2 - 4s^2 + 2 + \zeta^i + \zeta^{-i}$ for some i. This implies that $\zeta^i + \zeta^{-i} \in \mathbb{F}_q$, which is a contradiction. Hence no element of $\mathrm{SL}_2(q)$ of the form $w(x,y)$ can have trace zero. ■

Proof of Corollary 2
Let $q = p^n$ be as in the hypothesis of the corollary. The hypothesis $p^2 \not\equiv 1 \bmod 16$ is equivalent to $\left(\frac{2}{p}\right) = -1$. By the cyclotomic reciprocity law (see for example [12, Theorem 2.13]), the inertia degree of p in $\mathbb{Q}(\zeta)$ is m or $2m$. In the former case, m must be odd. Thus in both cases the inertia degree of p in $\mathbb{Q}(\zeta+\zeta^{-1})$ is m, since $\mathbb{Q}(\zeta+\zeta^{-1})$ is a subfield of index 2 in $\mathbb{Q}(\zeta)$. Now $p^2 \not\equiv 1 \bmod (2k+1)$ implies $m > 1$, and the conclusion follows from Theorem 1. ■

Remark. Our search for non-surjective words was assisted by [2], which lists representatives of minimal length for certain automorphism classes of words in F_2.

Acknowledgements. The first author was supported by the DFG priority program SPP 1388. The second author is grateful to the Royal Society for an International Exchange grant, and to Nikolay Nikolov for very helpful discussions. All authors were supported by the Marsden Fund of New Zealand via grant UOA 1015.

References

[1] T. Bandman, S. Garion and F. Grunewald, On the surjectivity of Engel words on PSL(2,q), to appear in *Groups, Geometry and Dynamics.*

[2] B. Cooper and E. Rowland, Growing words in the free group on two generators, to appear in *Illinois J. Math.*

[3] R.M. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces, *J. Amer. Math. Soc.* **25** (2012), 77–121.

[4] M. Larsen and A. Shalev, Word maps and Waring type problems. *J. Amer. Math. Soc.* **22** (2009), 437–466.

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

[6] M.W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications, *Annals of Math.* **154** (2001), 383–406.

[7] M.W. Liebeck, E.A. O'Brien, A. Shalev, and P.H. Tiep, The Ore conjecture, *J. Eur. Math. Soc.* **12** (2010), 939–1008.

[8] M.W. Liebeck, E.A. O'Brien, A. Shalev, and P.H. Tiep, Products of squares in finite simple groups, *Proc. Amer. Math. Soc.* **140** (2012), 21–33.

[9] W. Plesken and A. Fabiańska, An L_2-quotient algorithm for finitely presented groups, *J. Algebra* **322** (2009), 914–935.

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

[11] A. Shalev, Word maps, conjugacy classes, and a noncommutative Waring-type theorem, *Annals of Math.* **170** (2009), 1383–1416.

[12] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, Vol. 83, Springer-Verlag, New York, 1982.

Sebastian Jambor, Lehrstuhl B für Mathematik, RWTH Aachen, D-52056 Aachen, Germany. Email: sebastian.jambor@rwth-aachen.de

Martin W. Liebeck, Department of Mathematics, Imperial College, London SW7 2AZ, UK. Email: m.liebeck@imperial.ac.uk

E.A. O'Brien, Department of Mathematics, University of Auckland, New Zealand. Email: e.obrien@auckland.ac.nz