Abstract. Elements of the free group define interesting maps, known as word maps, on groups. It was previously observed by Lubotzky that every subset of a finite simple group that is closed under endomorphisms occurs as the image of some word map. We improve upon this result by showing that the word in question can be chosen to be in $v(F_n)$, the verbal subgroup of the free group generated by the word $v$, provided that $v$ is not a law on the finite simple group in question. In addition, we provide an example of a word $w$ that witnesses the chirality of the Mathieu group $M_{11}$. The paper concludes by demonstrating that not every subset of a group closed under endomorphisms occurs as the image of a word map.

Mathematics Subject Classification. 20D05, 20F10.

Keywords. Word maps, Finite simple groups, Chirality.

1. Introduction. The image of various word maps in finite simple groups has been a topic of considerable interest. Most famously the now-proven Ore conjecture [8] asked whether every element of a finite non-Abelian simple group $G$ is a commutator. Recently, for every finite non-Abelian simple group $G$, it was shown that if $N$ is the product of two prime powers, then every element of $G$ occurs as the product of two $N$-powers in $G$ [6].

A word $w$ is an element of the free group $F_n = F\langle x_1, \ldots, x_n \rangle$. For every group $G$, the word $w$ induces a map $w : G^n \to G$, where

$$(g_1, \ldots, g_n) \mapsto w(g_1, \ldots, g_n).$$

We write $w$ for both the word $w$ and the word map on $G$, and write $w(G)$ to mean the image $w(G^n)$ of the word map. In general, $w(G)$ is not a group, but merely a subset of $G$. We write $\langle w(G) \rangle$ for the group generated by $w(G)$. We will also write $\overline{g}$ to mean the tuple $(g_1, g_2, \ldots, g_n)$. In the notation now
established, the Ore conjecture asked whether for every finite simple group $G$, the word $w = [x, y] = x^{-1}y^{-1}xy$ satisfies $w(G) = G$.

Word maps represent an interesting class of functions on groups. In general, word maps are not homomorphisms, but they do respect automorphisms and endomorphisms of groups. Explicitly, we have the following lemma.

**Lemma 1.** Let $w \in F_n$ and $G$ be a group. Then for every $\bar{g} \in G$ and homomorphism $\varphi : G \to G$, the following holds.

$$\varphi (w(\bar{g})) = w(\varphi(g)).$$

Hence $w(G)$ is closed under all endomorphisms from $G$ to $G$. In examining word maps on finite simple groups, the question was asked at the conference ‘Words and Growth’ (Jerusalem, June 2012) if every subset of a finite simple group that is closed under endomorphisms of $G$ occurs as the image of some word map. Lubotzky responded in the affirmative with the following theorem.

**Theorem 2 ([9]).** Let $G$ be a finite simple group, $n > 1$, and let $A \subseteq G$ be such that $A$ is closed under all endomorphisms of $G$. Then there is a word $w \in F_n$ such that $A = w(G)$.

Here we do two things: We extend Lubotzky’s result by showing that the structure of $w$ realizing $A$ can be controlled in a very strong way; we also show that there are groups $G$ and $A \subseteq G$ with $A$ closed under endomorphisms such that $A$ is not $w(G)$ for any $w$. We also generalize Lubotzky’s result in another direction. Let $G = M_{11}$; we provide a word $w$ such that $w(G)$ contains exactly one of the conjugacy classes of order 11. The explicit realization of such a word provides a quick proof of observations by Gordeev et al. [5, 7.3–7.4].

**Theorem A.** Let $G$ be a finite simple group, $n > 1$, and $A \subseteq G$ such that $A$ is closed under automorphisms and $1 \in A$. Assume that $v \in F_n$ is not a law on $G$. Then there is a word $w \in \langle v(F_n) \rangle$ such that $A = w(G)$.

Theorem A shows that every subset of $G$ that is closed under endomorphisms of $G$ is the image of some word map $w$ in $v(F_n)$, but does identify the explicit $w$. However, it is possible in some cases to explicitly find $w$. We will show the following theorem which relates to the authors’ [2] earlier work on the chirality of groups.

The Mathieu group $M_{11}$ has two conjugacy classes of order 11 that are the inverse of each other. We construct a word whose image contains exactly one of these conjugacy classes. Furthermore, although the word is long in length, it is short as a straight-line program.

**Theorem B.** Let $G$ be the Mathieu group $M_{11}$ and let $w$ be the word

$$[x^{-440}(x^{-440})^{-1}y^{-440}x^{-440}, (y^{-440})(x^{-440}y^{-440})y^{-440}].$$

Then $w(G)$ contains an element $g$ such that $o(g) = 11$ and $g^{-1} \notin w(G)$, i.e. the word $w$ witnesses the chirality of $G$.

If $G$ is an arbitrary group $G$, then one might ask if being closed under endomorphisms of $G$ is a sufficient condition for a subset $A$ to be $w(G)$ for some $G$. We will show in Section 3 that this is false, even for Abelian groups.
Theorem C. Let $G$ be the cyclic group of order 12. Then
\[ A = \{ x^2 : x \in G \} \cup \{ x^3 : x \in G \}, \]
is closed under endomorphisms of $G$, but is not the image of any word map over $G$.

2. Proof of Theorems A and B. Our proof of Theorem A will rely on work done on the varieties of groups. Recall that a variety $B$ is the class of all groups satisfying some set of laws $X$, i.e. a group $G$ is in $B$ if and only if for every word $w \in X$ and every $n$-tuple $\overline{g} \in G$, we have that $w(\overline{g}) = 1$. For example, the variety of Abelian groups is defined by the law $w = x^{-1}y^{-1}xy$.

Similarly, solvable groups with derived length $n$ or nilpotent groups of class $m$ are varieties.

For a finite group $G$, there are only finitely many word maps on $n$ variables over $G$. Moreover, if $w$, and $v$ are two word maps from $G^n \to G$, then $w \cdot v$ is a word map from $G^n \to G$ given by $(w \cdot v)(\overline{g}) = w(\overline{g})v(\overline{g})$. Hence the set of word maps on $n$ variables over $G$ forms a group $F_n(G)$. We can equivalently define $F_n(G)$ as follows.

Let $K_n(G)$ be the set of all $n$-variable laws on $G$. Then $K_n(G)$ is a characteristic subgroup of $F_n(G)$ and $F_n(G) = F_n/G_n(G)$.

The group $F_n(G)$ is the free group of rank $n$ in the variety generated by $G$. In particular, every $n$-generated group in the variety generated by $G$ occurs as a quotient of $F_n(G)$. H. Neumann [10, p. 141] states without proof that $F_n(G) = G^{d(n)} \times H$ for a finite group $G$, where $H$ is the direct product of all proper subgroups of $G$ and $d(n)$ is the number of orbits of Aut($G$) acting on the generating $n$-tuples of $G$. We will prove a weaker statement. It is also the case that $G^{d(n)}$ is $n$-generated, but $G^{d(n)+1}$ is not [7].

Lemma 3. Let $G$ be a finite simple group. Then
\[ F_n(G) = G^{d(n)} \times H \]
for some group $H$.

Proof. Since a word map $w$ respects endomorphisms of $G$, the map $w$ is defined by its value on a set of representatives of the diagonal action of the automorphism groups of $G$ on $G^n$. Moreover, the number of possible values of $w$ on an orbit representative $(\overline{g})$ is at most $|\langle \overline{g} \rangle|$, the size of the subgroup generated by the orbit. There are exactly $d(g)$ orbits of $n$-tuples corresponding to $n$-tuples that generate $G$, and some number of other orbits.

Therefore $F_n(G)$ is a subgroup of the direct product $G^{d(n)} \times H$, where $H$ is some direct product of proper subgroups of $G$. Every group of rank $n$ that satisfies the same laws as $G$ occurs as a quotient of $F_n(G)$. Hence $G^{d(n)}$ must occur as a quotient of $F_n(G)$. \qed

Before proving Theorem A, we need the following lemma which follows from the work of Kantor and Guralnick [4, Corollary p. 745], which depends heavily on the classification of finite simple groups.

Lemma 4 ([4]). For every non-trivial element $g$ of a finite simple group $G$, there is an $h \in G$ such that $G = \langle g, h \rangle$. 
In particular, it is the case that for every finite simple group $G$, the number $d(n)$ is greater than the number of conjugacy classes of $G$.

**Proof of Theorem A.** Since $v$ is not a law on $G$, we know that $\langle v(G) \rangle = G$. By Lemma 3, we see that

$$\langle v(F_n(G)) \rangle = \langle v(G^{d(n)}) \rangle \times \langle v(H) \rangle = G^{d(n)} \times \langle v(H) \rangle$$

for the appropriate group $H$.

Hence there is a word map $w \in v(F_n(G))$ that is defined by its value on the generating tuples with a value from the group $G^{d(n)} \times v(H)$. Given $A$, we can write $A$ as a union of $m \leq d(n)$ automorphism classes. There is a $w$ so that on $m$ different orbits of generating tuples of $G$, the value of $w$ is one of the distinct automorphism classes in $A$ and $w$ vanishes elsewhere.

Now we need to find a word in $\langle v(F_n(G)) \rangle$ such that it induces the word map $w$ on $G$. Consider the word maps $x_1, \ldots, x_n$, i.e. the maps induced by the words $x_1, \ldots, x_n$. These word maps generate $F_n(G)$. Since $w \in \langle v(F_n(G)) \rangle$, we can write

$$w = \prod_i v(u_{i,1}, \ldots, u_{i,n}),$$

where each $u_{i,j}$ is a product of $x_1, \ldots, x_n$. We will abuse notation and write $u_{i,j}(x_1, \ldots, x_n)$ for a word in $F_n$ such that $u_{i,j}(x_1, \ldots, x_n) = u_{i,j} \in v(F_n(G))$. Then the word

$$w = \prod_i v(u_{i,1}(x_1, \ldots, x_n), \ldots, u_{i,n}(x_1, \ldots, x_n)) \in v(F_n)$$

induces the word map $w$ on $G$ which has image $A$. □

We will find a commutator word below that realizes an interesting property of the Mathieu group of order 7920.

In [3], the authors were interested in finding chiral word maps $w$, i.e. for some group $G$, we have that $g \in w(G)$, but $g^{-1} \notin w(G)$. Gordeev et al. [5] call the pair $(G, w)$ a chiral pair. They note that for groups known to be chiral, it is not always easy to produce a chiral pair, or witness of the chirality. For example, the Mathieu group $G = M_{11}$ of order 7920 is chiral as a result of Lubotzky’s theorem or Theorem A. However, prior to this work, there were no known examples of words $w$ such that $(G, w)$ is a chiral pair.

We will now show that the word

$$w = [x^{-440}(x^{-440})(y^{-440})x^{-440}, (y^{-440})(x^{-440}y^{-440})y^{-440}]$$

of length 9680 witnesses the chirality of the Mathieu Group $M_{11}$.

**Proof of Theorem B.** We will use Magma [1] to calculate $w(G)$. We note that this could be done directly in a few minutes. However, as the reader might be interested in finding other word maps over other groups, we will demonstrate the techniques we used that allow for a significantly faster computation of $w(G)$. 
All elements of $M_{11}$ have order either 1, 2, 3, 4, 5, 6, 8, or 11. For an element $g$ of $M_{11}$, we have

$$g^{-440} = \begin{cases} 
1 & \text{if } o(g) \notin \{3, 6\}, \\
g & \text{if } o(g) = 3, \\
g^4 & \text{if } o(g) = 6.
\end{cases}$$

If $a \in G$ does not have order 3 or 6, then $w(a, b) = w(1, b) = 1$ for all $a \in G$ since $w$ is a commutator. Similarly, if $b \in G$ does not have order 3 or 6, then $w(a, b) = w(a, 1) = 1$ for all $a \in G$. Moreover, $w(a, b) = w(a^4, b^4)$ for all $a, b \in G$. Hence to determine $w(G)$, we need to determine $w(a, b)$, where both $a$ and $b$ have order 3. There are 93600 such tuples from $G$. Let $X = \{a \in G : o(a) = 3\}$. Let $v = [x(x^y)x, y(x^y)y]$. We note that $w(a, b) = v(a, b)$ for all $a, b \in X$. Hence $w(G)$ is equal to the image of the map

$$v : X \times X \to G,$$

where $v(a, b)$ is the evaluation of the word $v$ on $a$ and $b$. By restricting our domain to $X$, the computation is very fast. We see that $w(G)$ has elements of order 1,2,4,5,6, and 11. However, all of the elements of order 11 that occur in the image of $w$ are conjugate. For $g \in M_{11}$ with $o(g) = 11$, we have that $g^{-1} \notin g^G$. We conclude that $w$ witnesses the chirality of $M_{11}$.

3. **Proof of Theorem C.** Recall that every word $w(x_1, \ldots, x_n)$ can be written in the form

$$w = x_1^{k_1} \ldots x_n^{k_n}v(x_1, \ldots, x_n),$$

where $v \in F'_n$.

By applying Nielsen transformations to $w$, we see that there is an automorphism $\sigma \in \text{Aut}(G)$ such that $\sigma(w) = w' = x_1^k c$, where $k$ is $\text{gcd}(k_1, \ldots, k_n)$ and $c \in F'_n$. Moreover, $w$ is a law on a group $G$ if and only if $w'$ is a law on $G$. Since automorphisms preserve the image of a word map, we see that $w(G) = w'(G)$. Hence for a finite Abelian group, the only images of word maps are exactly the images of the power maps, e.g., $\{x^k : x \in G\}$ for some $k$. We now prove Theorem C by showing that not every subset of a group $G$ that is closed under endomorphisms occurs as word map.

**Proof of Theorem C.** Let $G = \langle a | a^{12} \rangle$ be the cyclic group of order 12. Then the images of the power maps in $G$ are exactly

1. $\{x^{12}\}, \ G = \{x^1\}, \ \{1, a^2, a^4, a^6, a^8, a^{10}\} = \{x^2\}, \ \{1, a^3, a^6, a^9\} = \{x^3\}$
2. $\{1, a^4, a^8\} = \{x^4\}, \ \{1, a^6\} = \{x^6\}.$

Every union of subsets closed under endomorphisms is closed under endomorphisms. However, there is no power map, equivalently no word map, that has the set $\{1, a^2, a^3, a^4, a^6, a^8, a^9, a^{10}\}$ as its image.

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
References

[1] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symb. Comput. 24(3–4), 235–265 (1997)

[2] Cocke, W., Ho, M.-C.: On the symmetry of images of word maps in groups. Comm. Algebra 46(2), 756–763 (2018)

[3] Cocke, W., Ho, M.-C.: The probability distribution of word maps on finite groups. J. Algebra 518, 440–452 (2019)

[4] Guralnick, R.M., Kantor, W.M.: Probabilistic generation of finite simple groups. J. Algebra 234(2), 743–792 (2000). Special issue in honor of Helmut Wielandt

[5] Gordeev, N.L., Kunyavskiı, B.É., Plotkin, E.B.: Geometry of word equations in simple algebraic groups over special fields. Uspekhi Mat. Nauk. 73(5(443)), 3–52 (2018)

[6] Guralnick, R.M., Liebeck, M.W., O’Brien, E.A., Shalev, A., Tiep, P.H.: Surjective word maps and Burnside’s $p^a q^b$ theorem. Invent. Math. 213(2), 589–695 (2018)

[7] Hall, P.: The Eulerian functions of a group. Q. J. Math. os-7(1), 134–151 (1936)

[8] Liebeck, M.W., O’Brien, E.A., Shalev, A., Tiep, P.H.: The Ore conjecture. J. Eur. Math. Soc. (JEMS) 12(4), 939–1008 (2010)

[9] Lubotzky, A.: Images of word maps in finite simple groups. Glasg. Math. J. 56(2), 465–469 (2014)

[10] Neumann, H.: Varieties of Groups. Springer, New York (1967)

William Cocke
Department of Mathematics
University of Wisconsin–Madison
Madison
USA
e-mail: cocke@math.wisc.edu

Meng-Che Ho
Department of Mathematics
Purdue University
Lafayette
USA
e-mail: ho140@purdue.edu

Received: 21 February 2019