Glasgow Math. J. **56** (2014) 465–469. © Glasgow Mathematical Journal Trust 2013.
doi:10.1017/S0017089513000396.

IMAGES OF WORD MAPS IN FINITE SIMPLE GROUPS

ALEXANDER LUBOTZKY*
Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel
e-mail: alex.lubotzky@mail.huji.ac.il

(Received 28 November 2012; accepted 15 April 2013; first published online 30 August 2013)

Abstract. In response to questions by Kassabov, Nikolov and Shalev, we show that a given subset A of a finite simple group G is the image of some word map $w : G \times G \to G$ if and only if (i) A contains the identity and (ii) A is invariant under $\mathrm{Aut}(G)$.

2010 *Mathematics Subject Classification*. 20D05, 20F10.

1. Introduction. Let w be a word in the free group F_k of rank k. For every group G, w defines a 'word map' $w : G^k \to G$. Let $w(G)$ denote the image of this map. In recent years, there has been great interest in $w(G)$, especially when G is a finite simple group. For example, the Ore conjecture settled in [**9**] says that for $w = xyx^{-1}y^{-1}$, $w(G) = G$ for every non-abelian finite simple group. Similar results have been proved for a few other words. Another direction of research is: what is the width of G with respect to $w(G)$? In this respect, the most remarkable result [**6**] is that for every given w the width is two (i.e. every element of G is a product of two elements of $w(G)$) if G is large enough (depending on w). For more details, see the above mentioned papers, [**10**], [**12**] and the references therein.

In these results, the word is fixed and G is changed. Several recent papers have been devoted to the dual question: Given G, what kind of subsets can appear as $w(G)$ for some w. For example, Kassabov and Nikolov [**5**] showed that in A_n, $n \geq 7$, the set consisting of e and all the 3-cycles is $w(A_n)$ for some w (depending on n), which shows, in particular, that the width of G with respect to $w(G)$ can be arbitrarily large. They also showed, for $G = \mathrm{SL_n(q)}$, that there exists a word w with $w(G)$ equal to the identity and all transvections. (A similar result for some sequences of n and q has been proved earlier by Guralnick and Tiep.) Levy [**7**] showed that for $q = 2^{2^n}$, $n \geq 2$ and $G = \mathrm{SL_2(q)}$, there exists $w \in F_2$ for which $w(G)$ consists of the identity plus the union of four conjugacy classes of elements of order 17. See also [**3**] for related results. Some questions have been asked about the possible subsets of G, a finite simple group, to be equal to $w(G)$ for some w.

There are two clear necessary conditions for a subset $A \subseteq G$ to be equal to $w(G)$:

1. $e \in A$ (since $w(e, \ldots, e) = e$).
2. For every $\alpha \in \mathrm{Aut}(G)$, $\alpha(A) = A$ (since $\alpha(w(g_1, \ldots, g_k)) = w(\alpha(g_1), \ldots, \alpha(g_k))$.

During the conference 'Words and Growth' (Jerusalem, June 2012), Shalev asked whether this could also be sufficient. The goal of this note is to answer this question affirmatively.

*This work was supported by ERC, NSF and ISF

THEOREM 1. *Let G be a finite simple group and A be a subset of G such that $e \in A$ and for every $\alpha \in Aut(G)$, $\alpha(A) = A$. Then there exists a word $w \in F_2$, such that $w(G) = A$.*

The proof is fairly elementary but we make use, along the way, of a result of Guralnick and Kantor [**1**, Corollary, p. 745], asserting that for every finite simple group G and for every $e \neq a \in G$ there exists $b \in G$ such that $G = \langle a, b \rangle$, i.e. G is generated by a and b. The proof of this result requires the classification of the finite simple groups. Thus, our result also depends on the classification. (However, see Remark 3 in Section 2.) While it seems impossible at this stage to prove the Guralnick–Kantor result without the classification (in fact, without it, it is not even known that every finite simple group is generated by two elements) it might be that our result has a classification-free proof.

The method of proof has an interesting corollary.

COROLLARY 2. *For every finite simple group G, there is $w(x, y) \in F(x, y)$, the free group on two generators with the following property:*

$$\text{For every } (a, b) \in G \times G, \quad w(a, b) \neq e \text{ if and only if } \langle a, b \rangle = G.$$

So w can 'test' whether two elements generate G. Unfortunately, our method of proof while formally 'effective' (in the sense that we can bound the length of w, see Remark 4 at the end of Section 2) does not really give a useful description of the word w of Theorem 1 or Corollary 2. So, after all, the methods of [**5**] and [**7**] have some advantage in spite of proving only very special cases of the theorem.

2. Proof of the theorem. Let G be a finite simple group and $A \subset G$ with $e \in A$ and $\alpha(A) = A$ for every $\alpha \in \mathrm{Aut}(G)$. If G is abelian then clearly either $A = \{e\}$ or $A = G$ and in both cases the result is trivial, so from now on we assume G is non-abelian.

Let $\{(a_i, b_i) | i = 1, \ldots, |G|^2\}$ be the set of all ordered pairs of elements of G such that for $i = 1, \ldots, \ell$, the pair $\{a_i, b_i\}$ generates G i.e., $G = \langle a_i, b_i \rangle$, while for $i = \ell + 1, \ldots, |G|^2$, it does not. Every i gives rise to a unique homomorphism $\varphi_i : F = F_2 \to G$ defined by $\varphi_i(x) = a_i$, $\varphi_i(y) = b_i$ when $F = F_2$ is the free group on x and y. Denote $N_i = \mathrm{Ker}\varphi_i$ and let $M = \bigcap_{i=1}^{|G|^2} N_i$ and $N = \bigcap_{i=1}^{\ell} N_i$. So for $i = 1, \ldots, \ell$, φ_i is an epimorphism and $F/N_i \simeq G$, while for $i > \ell$, F/N_i is isomorphic to a proper subgroup of G.

Let $\varphi_M = (\varphi_1, \ldots, \varphi_{|G|^2})$ be the diagonal map from F to $G^{|G|^2}$ and $H = \varphi_M(F)$. We want to describe the structure of H as a subgroup of $G^{|G|^2}$.

Write $G^{|G|^2}$ as $E \times D$, where E is the product of the first ℓ copies of G (the ones corresponding to epimorphisms to G) and D is the product of all the others. Let K be the kernel of the projection from H to E and E' its image there, and let L be the kernel of the projection from H to D and D' will denote the image. The group K is a subgroup of D, whose projection to every single copy of G in D is a proper subgroup of G. So K has no Jordan–Hölder factor isomorphic to G. On the other hand, $E' \cong H/K$ which is the projection of H to E is a subdirect product of G^{ℓ} such that its projection to every single copy of G is onto. Hence E' is isomorphic (since G is finite and simple) to $G^{r'}$ for some $r' \leq \ell$.

We can determine precisely what is r'. Let us postpone this computation for a moment, but observe first that L, the kernel of the projection from H to D, must be equal to the projection E' of H to E since it is a subgroup of this projection and both

https://doi.org/10.1017/S0017089513000396 Published online by Cambridge University Press

are isomorphic to $G^{r'}$, since all the r' Jordan–Hölder factors of H should appear in L, as H/L has no Jordan–Hölder factor isomorphic to G. Thus, $H = E' \times D'$.

Note also that an element $\overline{u} = (u_1, \ldots, u_\ell)$ is in E' if and only if whenever $\alpha \circ \varphi_i = \varphi_j$ for some $1 \leq i, j \leq \ell$ and $\alpha \in \mathrm{Aut}(G)$, $\alpha(u_i) = u_j$.

Let us now calculate r':

The group $\mathrm{Aut}(G)$ acts on the pairs $\{(a_i, b_i)\}$ and similarly on the homomorphisms $\{\varphi_i\}$, preserving the first ℓ of them (the epimorphisms). The action on these epimorphisms is free: indeed, if $\alpha \in \mathrm{Aut}(G)$ and $\alpha \circ \varphi_i = \varphi_i$ (or equivalently $(\alpha(a_i), \alpha(b_i)) = (a_i, b_i)$) then α is the identity automorphism of G. Thus, the first ℓ homomorphisms, i.e. the ℓ epimorphisms, form $r = \frac{\ell}{|\mathrm{Aut}(G)|}$ orbits. Now $F_2/N \simeq H/K$ is the maximal quotient of F_2 which is isomorphic to a direct power $G^{r'}$ of G. By a result of Hall [**4**, Corollary 7], $r' = r = \frac{\ell}{|\mathrm{Aut}(G)|}$.

In summary, the group $H = \varphi_M(F_2)$ is a direct product $H = E' \times D'$, where E' is a subgroup of $E = G^\ell$ isomorphic to G^r, embedded 'diagonally' in G^ℓ twisted by $\mathrm{Aut}(G)$. The other part D' is a subgroup of $D = G^{|G|^2 - \ell}$ whose structure is less clear, but D' has no Jordan–Hölder factor isomorphic to G.

Let us now look at the set $A' = A \setminus \{e\}$. This set is a union of orbits of $\mathrm{Aut}(G)$ acting on G. We first observe that the number of orbits is less or equal r. Indeed, by the Guralnick–Kantor result mentioned in the introduction [**1**, Corollary, p. 745], every $a \in A'$ is part of a two-element set of generators, so there exists at least one $b \in G$ such that $\langle a, b\rangle = G$ and so there exists $1 \leq i \leq \ell$ such that $(a_i, b_i) = (a, b)$. The orbit of a in G, i.e. $\{\alpha(a) | \alpha \in \mathrm{Aut}(G)\}$, gives an orbit of pairs (equivalently, of epimorphisms) $\{(\alpha(a_i), \alpha(b_i)) | \alpha \in \mathrm{Aut}(G)\}$. In general, there may be more than one orbit of epimorphisms corresponding to a as there may be b and b' such that $\langle a, b\rangle = \langle a, b'\rangle = G$ while (a, b) and (a, b') are not on the same $\mathrm{Aut}(G)$ orbit.

Let us now define the following element $\overline{z} = (z_i)_{i=1}^{|G|^2}$ of $G^{|G|^2} = E \times D$:

$$z_i = \begin{cases} a_i & \text{if } i \leq \ell \text{ and } a_i \in A', \\ e & \text{otherwise.} \end{cases}$$

We first claim that $\overline{z}$ is in $H = E' \times D'$. Clearly, its projection to D is the identity, so we just need to check that its projection to E is in E'. However, this is clear as by its definition, $\overline{z}$ is on the 'twisted diagonal' group defining E' as a subgroup of E, and A' is $\mathrm{Aut}(G)$-invariant. We also observe that all the elements of A' show up as some coordinates of $\overline{z}$. This follows from the Guralnick–Kantor result, which ensures that every $a \in A'$ has a mate b, with $(a, b) = (a_i, b_i)$ for some $1 \leq i \leq \ell$.

The description of H above shows that $\overline{z}$ is an element of $H = \varphi_M(F_2) \in G^{|G|^2}$. Spelling out the meaning of this, we see that there exists $w \in F_2$ such that for every $i = 1, \ldots, |G|^2$, $\varphi_i(w) = z_i$. However, $\varphi_i(w) = w(a_i, b_i)$. This means that w is a word in F_2, with $w(G) = \{z_i\}_{i=1}^{|G|^2} = \{e\} \cup A' = A$ and the theorem is proved.

The proof shows that

$$w(a, b) = \begin{cases} a \in A' & \text{and } \langle a, b\rangle = G, \\ e & \text{otherwise.} \end{cases}$$

Applying this for the set $A = G$, we deduce Corollary 2.

https://doi.org/10.1017/S0017089513000396 Published online by Cambridge University Press

REMARKS. **1.** The proof actually shows that if $f : G \times G \to G$ is any function which is $\mathrm{Aut}(G)$-invariant (i.e. for every $\alpha \in \mathrm{Aut}\, G$ and every $a, b \in G$, $f(\alpha(a), \alpha(b)) = \alpha(f(a, b))$) and $f(a, b) = e$ if $\langle a, b\rangle \neq G$, then there exists $w \in F_2$ such that $f(a, b) = w(a, b)$ for all $a, b \in G$. One can take for example

$$f(a,b) = \begin{cases} aba^{-1}b^{-1} & \text{if } \langle a, b\rangle = G, \\ e & \text{otherwise.} \end{cases}$$

2. Recall the well-known result that almost every pair $(a, b) \in G \times G$ generates G. From this and Remark 1, one can deduce that for every $\varepsilon > 0$, if G is large enough and p a probability function on G which is $\mathrm{Aut}(G)$-invariant (i.e. $p : G \to \mathbb{R} \geq 0$, for every $\alpha \in \mathrm{Aut}(G)$ and $a \in G$, $p(\alpha(a)) = a$ and $\sum_{a \in G} p(a) = 1$) there exists a word $w \in F_2$ such that for every $c \in G$, $|\frac{|\{(a,b) \in G \times G | w(a,b) = c\}|}{|G|^2} - p(c)| < \varepsilon$.

3. The proof of the theorem needs the classification only to ensure that every $a \in A' = A \backslash \{e\}$ is part of a generating 2-set. Without the classification, the proof shows that if A' is a set of elements such that every $a \in A'$ is part of a generating 2-set then $A = A' \cup \{e\}$ is the image of some word map. It follows that Corollary 2 does not rely on the classification. We thank M. Kassabov for this last observation. Furthermore, as observed by the referee, if the finite simple group G is generated by k element, then the proof of Theorem 1 shows that Theorem 1 holds for G and A with some $w \in F_{k+1}$, without using at all the classification of finite simple groups.

4. It is not so easy to find a word w as in Corollary 2 explicitly. Our proof is effective in the sense that we can bound the length of w in the proof. For example, $|G|^{|G|^2}$ is a bound (maybe by using some ideas and results on the uniformity of expanders one can do better); but these bounds are too large to be useful. Our work suggests to study quantitative versions of Theorem 1 and Corollary 2. The work of Hadad [**2**] can be thought of as a step in this direction for $A = \{e\}$.

5. Theorem 1 has been extended by Levy [**8**] to some almost simple and quasisimple finite groups.

6. The analogous result of Theorem 1 in the context of rings (where word maps are replaced by noncommutative polynomials) is going back to Kaplansky. See [**11**] and references therein for the history and some results.

ACKNOWLEDGEMENT. The author is grateful to R. Guralnick, M. Kassabov, N. Nikolov and A. Shalev for some interesting discussions during and after the above noted conference.

REFERENCES

1. R. M. Guralnick and W. M. Kantor, Probabilistic generation of finite simple groups. Special issue in honor of Helmut Wielandt, *J. Algebra* **234** (2000), 743–792.

2. U. Hadad, On the shortest identity in finite simple groups of Lie type, *J. Group Theory* **14** (2011), 37–47.

3. S. Jambor, M. W. Liebeck and E. A. O'Brien, Some word maps that are non-surjective on infinitely many finite simple groups, *Bull. LMS* (2013), doi: 101112/blms/bdt10. (arXiv:1205.1952).

4. W. M. Kantor and A. Lubotzky, The probability of generating a finite classical group, *Geom. Dedicata* **36** (1990), 67–87.

5. M. Kassabov and N. Nikolov, Words with few values in finite simple groups, preprint (arXiv:1112.5484). *Q. J. Math*. (2012), doi: 10.1093/qmath/has018.

6. M. Larsen, A. Shalev and P. H. Tiep, The Waring problem for finite simple groups, *Ann. Math.* **174** (2011), 1885–1950.

7. M. Levy, Word maps with small image in simple groups, preprint (arXiv:1206.1206).

8. M. Levy, Images of word maps in almost simple groups and quasisimple groups, preprint (arXiv:1301.7188).

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

10. D. Segal, *Words: Notes on verbal width in groups*, London Mathematical Society Lecture Note Series, 361 (Cambridge University Press, Cambridge, UK, 2009), xii+121 pp.

11. S. Spenko, On the image of a noncommutative polynomial, *J. Algebra* **377** (2013), 298–311.

12. J. S. Wilson, *Finite index subgroups and verbal subgroups in profinite groups*, Séminaire Bourbaki, vol. 2009/2010. Exposés 1012–1026. Astérisque No. 339 (2011), Exp. No. 1026, x, 387–408.