ISRAEL JOURNAL OF MATHEMATICS **219** (2017), 469–478 DOI: 10.1007/s11856-017-1487-x

ABOUT THE LENGTH OF LAWS FOR FINITE GROUPS

BY

Andreas Thom

TU Dresden, Institut für Geometrie, 01062 Dresden, Germany e-mail: andreas.thom@tu-dresden.de

ABSTRACT

We prove new upper bounds of the form $O(n/\log(n)^{2-\varepsilon})$ for the length of laws that hold for all groups of size at most n — improving on previous results of Bou-Rabee and Kassabov–Matucci. The methods make use of the classification of finite simple groups. Stronger bounds are proved in case the groups are assumed to be nilpotent or solvable.

1. Introduction

We denote the free group on two generators a, b by $\mathbf{F}_2 = \langle a, b \rangle$. For every group G, a word $w \in \mathbf{F}_2$ determines a word map $w \colon G \times G \to G$ by evaluation. We say that w is a law for G if the image of the corresponding word map on G consists only of the neutral element — that is, w(g,h)=1 for all $g,h \in G$. Every finite group admits laws, for example $a^n \in \mathbf{F}_2$ is a law for G for n := |G|. Recently, there has been some interest in finding short laws for specific groups or families of groups. This was first done systematically by Hadad for finite simple groups of Lie type in [9]. Bou-Rabee [1] started a program to determine the so-called residual finiteness growth of various infinite groups, which also involved the study of laws for symmetric groups $\operatorname{Sym}(n)$ (see [2] and independently [6]) and the family of all groups (resp. all nilpotent or all solvable groups) of size at most n. The best upper bounds for length of laws of $\operatorname{Sym}(n)$ are currently due to Kozma and the author [14], where the proof makes use of consequences of the Classification of Finite Simple Groups (CFSG).

Received October 19, 2015 and in revised form March 1, 2016

The aim of this note is to provide a construction of a non-trivial word $w_n \in \mathbf{F}_2$ of length $O(n/\log(n)^{2-\varepsilon})$ which is a law for every finite group of size at most n. We will first do this separately for solvable groups and semi-simple groups (in the sense of Fitting) and then combine the two results to obtain a result for general finite groups. This partially answers a question from Kassabov–Matucci [13, Question 18]. Our main result is stated as Theorem 5.1 at the end of the paper. Its proof is spread over the entire paper, combining results on nilpotent and solvable groups with the case of semi-simple groups and results of Fitting. In the course of the proof, we also provide new upper bounds for the length of laws that hold for all nilpotent resp. all solvable groups of size at most n.

Previously, upper bounds on the length of laws that hold for all groups of size at most n have been obtained by Bou-Rabee [1] who constructed such a law of length $O(n^3)$. Later, Kassabov and Matucci [13] improved the bound to $O(n^{3/2})$ using an elementary but technical result of Lucchini on permutation groups from [15]. Our methods rely on the CFSG and thus use a machinery which is considerably heavier than the methods used before.

The only known lower bound comes from the observation that $\operatorname{PSL}_2(p)$ does not satisfy any law shorter than p; see [5]. Since the size of $\operatorname{PSL}_2(p)$ is roughly p^3 , this implies that no law of length $o(n^{1/3})$ can hold for all groups of size at most n. We conjecture that the bound $n/\log(n)^2$ proved in this paper is sharp up to negligible factors — see also the discussion after Theorem 5.1.

2. Preliminaries

Let G be a group. For a word $w \in \mathbf{F}_2$ we set

$$Z(G,w):=\{(g,h)\in G\times G\mid w(g,h)=1\}$$

and call it the vanishing set of w. Clearly, w is a law for G if and only if $Z(G, w) = G \times G$. We denote the minimal word length of a word $w \in \mathbf{F}_2$ when written in terms of the generators $\{a, a^{-1}, b, b^{-1}\}$ by |w|.

The following lemma is the key in many steps of the argument. It allows to combine finite sets of words and increase the vanishing set. We called it the commutator lemma, and it has appeared in different forms in the work of Hadad [9, Lemma 3.3] and Kassabov–Matucci [13, Lemma 10]. In the following form, it was proved as [14, Lemma 2.2].

LEMMA 2.1: Let w_1, \ldots, w_m be non-trivial words in \mathbf{F}_2 . Then there exists a non-trivial word $w \in \mathbf{F}_k$ such that for all groups G we have:

$$Z(G, w) \supset Z(G, w_1) \cup \cdots \cup Z(G, w_m).$$

Moreover, the length of w is bounded by $16 \cdot m^2 \max |w_i|$.

Lemma 2.1 can be used to construct laws for a single group but also laws for families of groups. Indeed, applying it to laws for G and H yields a law that holds for both G and H. We will apply the lemma in both ways.

The preceding lemma is enough to prove the upper bound of Bou-Rabee on laws that hold for all finite groups of size at most n. Indeed, every element of a group of order at most n has order at most n. Hence, $G \times G = \bigcup_{k=1}^{n} Z(G, a^k)$. The lemma provides a law of length $16n^3$. The result of Kassabov-Matucci starts with this observation and treats groups with an element of order exceeding $n^{1/2}$ separately in order to obtain the improved bound $O(n^{3/2})$; see [13].

The following lemma allows us to deal with extensions of groups.

LEMMA 2.2: Let $1 \to H \to G \to G/H \to 1$ be an extension of groups. Let $w' \in \mathbf{F}_2$ be a non-trivial law for H and $w'' \in \mathbf{F}_2$ be a non-trivial law for G/H. There exists a non-trivial law $w \in \mathbf{F}_2$ for G of length bounded by |w'|(|w''|+2).

Proof. We set $w(a,b) := w'(w''(a,b),xw''(a,b)x^{-1})$, where we choose $x \in \{a,a^{-1},b,b^{-1}\}$ so that w''(a,b) and $xw''(a,b)x^{-1}$ are free in \mathbf{F}_2 . This proves the claim.

The preceding lemma will allow us to decompose a group into its solvable radical and the corresponding semi-simple quotient. But we will also apply it to study automorphism groups of finite simple groups and reduce the case of semi-simple groups to that of simple groups.

3. Nilpotent and solvable groups

Let G be a group. We define the lower central series of G by setting $\gamma_1(G) = G$ and defining $\gamma_{k+1}(G) = [G, \gamma_k(G)]$ for all $k \geq 1$. Similarly, the derived series is defined by $G^{(0)} := G$ and $G^{(k+1)} := [G^{(k)}, G^{(k)}]$ for all $k \geq 0$. A group is called *nilpotent* if $\gamma_{k+1}(G) = 1$ for some $k \in \mathbb{N}$ and the smallest such k is called the nilpotency class of G. A group is called *solvable* if $G^{(k)} = 1$ for some $k \in \mathbb{N}$ and

the smallest such k is called the solvability class of G. It is a classical result of Hall that $G^{(k)} \subset \gamma_{2^k}(G)$ for all $k \geq 0$.

It is well-known that the nilpotency class of a nilpotent group can be estimated by the size. More precisely, we have that $\gamma_k(G) = 1$ whenever $k > \log_2(n)$, for a finite group G of order n. Indeed, this is obvious since $|\gamma_m(G)/\gamma_{m+1}(G)| \geq 2$, whenever $\gamma_m(G) \neq 1$. By a result of Elkasapy and the author [3, Theorem 2.2], there exists a non-trivial word $v_k \in \mathbf{F}_2$ of length at most $O(k^{3/2})$ which lies in $\gamma_k(\mathbf{F}_2)$. This implies the following proposition (compare [3, Theorem 5.1] for a slightly sharper bound):

PROPOSITION 3.1: Let $n \in \mathbb{N}$. There exists a word $v_n \in \mathbf{F}_2$ of length bounded by $O(\log(n)^{3/2})$ which is a law for all nilpotent groups of size at most n.

In order to treat solvable groups, we need to recall a few more notions. Let G be a solvable group of size at most n. By a result of Fitting, there exists a unique maximal, normal, and nilpotent subgroup of G. This group is called the Fitting subgroup and we denote it by $N \triangleleft G$. See [10] for general background on this and related concepts that will come up. It is a classical fact that the canonical map $G \to \operatorname{Aut}(N)$, given by the conjugation action, has kernel equal to the center of N.

Since N is nilpotent, N is a product of p-groups $N = \prod_p N(p)$, and we obtain also $\operatorname{Aut}(N) = \prod_p \operatorname{Aut}(N(p))$. For the p-group N(p), the Frattini subgroup $\Phi(N(p))$ is equal to $N(p)^p[N(p),N(p)]$ and we denote the Frattini quotient by $V(p) = N(p)/\Phi(N(p))$. The quotient group V(p) is a vector space over the finite field $\mathbb{Z}/p\mathbb{Z}$. Since $|V(p)| \leq |N(p)| \leq n$, the dimension $m(p) := \dim_{\mathbb{Z}/p\mathbb{Z}} V(p)$ of V(p) over $\mathbb{Z}/p\mathbb{Z}$ is bounded by $\log_2(n)$.

We consider the natural homomorphism α_p : $\operatorname{Aut}(N(p)) \to \operatorname{Aut}(V(p)) = \operatorname{GL}_{m(p)}(p)$ with $m(p) \leq \log_2(n)$. Clearly, the image of G in $\operatorname{GL}_{m(p)}(p)$ is solvable since G is assumed to be solvable. By a result of Zassenhaus [18, Satz 7], the solvability class of a linear group is logarithmic in the dimension of the vector space on which it acts. Later, Huppert [11] proved that the solvability class of a solvable subgroup of $\operatorname{GL}_{m(p)}(p)$ cannot exceed $1+7\log_2(m(p))$. Newman [16, Theorem A_S] determined the optimal bound to be $5\log_9(m(p)) + O(1)$. Thus, we obtain that the solvability class of the image of G in $\prod_p \operatorname{GL}_{m(p)}(p)$ cannot exceed $5\log_9(2) \cdot \log_2(\log_2(n)) + O(1)$.

Using the results from [3, Theorem 2.2] again, we know that there exists a non-trivial word $v_k \in \mathbf{F}^{(k)}$ of length bounded from above by roughly $2^{11k/6}$.

Applying this with $k = \lfloor 5 \log_9(2) \cdot \log_2(\log_2(n)) + C \rfloor$ for some suitable constant C, we obtain a word of length bounded by $2^C \cdot \log_2(n)^{5 \log_9(2) \cdot 11/6}$ that is a law for the image $\alpha(G)$ of the homomorphism $\alpha \colon G \to \prod_p \mathrm{GL}_{m(p)}(p)$. Note that $5 \log_9(2) \cdot 11/6 \leq 3$.

Burnside showed (see for example [8, Chapter 5, Theorem 1.4]) that the kernel of the map from $\operatorname{Aut}(N(p))$ to $\operatorname{GL}_{m(p)}(p)$ is a p-group and thus the group $\operatorname{ker}\left(\alpha\colon G\to \prod_p\operatorname{GL}_{m(p)}(p)\right)$ is nilpotent, being an extension of (a subgroup of) a product of p-groups by the center of N. Clearly, the size of the kernel is also bounded by n. Thus, we apply Proposition 3.1 to obtain a law of length bounded by $O(\log(n)^{3/2})$ for the kernel. Altogether, we can now use Lemma 2.2 to obtain a word of length bounded by $O(\log(n)^{9/2})$ that works for all solvable groups of size at most n.

In other words, we have proved the following proposition:

PROPOSITION 3.2: For every $n \in \mathbb{N}$ there exists a word $v_n \in \mathbf{F}_2$ of length bounded by $O(\log(n)^{9/2})$ which is a law for all solvable groups of size at most n.

We note that the analysis from above showed that any solvable group of size n has solvability class bounded by $O(\log \log(n))$. This was known from work of Glasby [7]. However, Glasby's estimates are not sufficient to establish Proposition 3.2 in this form. It is easy to see that this double-logarithmic bound is actually sharp. Indeed, the 2-Sylow subgroup of $\operatorname{Sym}(2^n)$ is the n-fold iterated wreath product of $\mathbb{Z}/2\mathbb{Z}$. Its cardinality is 2^{2^n-1} and its solvability class is equal to n.

4. Semi-simple groups

Let us first discuss finite non-abelian simple groups before we get to semi-simple groups.

PROPOSITION 4.1: Let $n \in \mathbb{N}$. There exists a non-trivial word $w_n \in \mathbf{F}_2$ of length bounded by $O(n/\log(n)^2)$ that is a law for all finite non-abelian simple groups of size at most n.

Proof. This uses the CFSG. The worst case in terms of length of laws is the family $PSL_2(q)$ with $q = p^k$ some prime power. It is well-known that the group $PSL_2(p^k)$ admits a law of length $O(p^k)$; see [9]. Indeed, it is easy to see

that every element of $\operatorname{PSL}_2(p^k)$ has order dividing either p^k-1, p or p^k+1 , corresponding to the diagonalizable, the unipotent, and the irreducible case. Thus, combining a^{p^k-1} , a^p and a^{p^k+1} using Lemma 2.1 yields a law for $\operatorname{PSL}_2(p^k)$ of length $O(p^k)$, where the implied constant depends on neither p nor k. At the same time the group $\operatorname{PSL}_2(p^k)$ has size roughly p^{3k} . Combining all such laws for pairs (p,k) with $p^{3k} \leq n$ using Lemma 2.1, we obtain a law with the desired bound on the length. Indeed, it is an easy consequence of the prime number theorem that there are at most $O(n^{1/3}/\log(n))$ prime powers less than $n^{1/3}$. Thus, we obtain a law of length $O((n^{1/3}/\log(n))^2 n^{1/3})$. This proves the claim for finite simple groups of the form $\operatorname{PSL}_2(q)$.

For all other families the maximal element order (m.e.o.) of the group is bounded by $O(n^{1/4})$ by results summarized in work of Kantor–Seress [12]. Indeed, this is well-known for Alt(n) — by a classical result of Landau, the maximal order of an element in Alt(n) is bounded by $\exp(c(n\log(n))^{1/2})$, for some small and explicit constant. The following table summarizes the situation for families of classical Chevalley groups of unbounded rank (twisted or untwisted). The first row contains a lower bound for the size of the group, up to a universal multiplicative factor. The second row contains an upper bound for the maximal element order, again up to some universal multiplicative factor. All information about the maximal element order is taken from the exposition in [12].

We now come to the families of bounded rank. These contain twisted forms of classical Chevalley groups that only exist in small rank, exceptional Chevalley groups (twisted and untwisted) and Suzuki–Ree groups. Our material stems again from [12].

We easily see that the only case for which the maximal element order cannot be bounded by $O(n^{1/4})$ is $A_1(q) = PSL_2(q)$. Since we are only interested in asymptotic bounds, we can ignore sporadic groups and Tits' group.

Thus, we can apply Lemma 2.1 to the list $a, a^2, \ldots, a^{Cn^{1/4}}$ for some suitable constant C in order to obtain a law of length $O(n^{3/4})$ that applies to all simple groups of size at most n and different from $\mathrm{PSL}_2(q)$. Combining now the law for the $\mathrm{PSL}_2(q)$'s and the law for the remaining families using Lemma 2.1 again, we can finish the proof.

The study of semi-simple groups goes back to the work of Fitting; see [4] for the original reference. Recall that an isotypical semi-simple group (in the sense of Fitting) is a group G which fits into a chain of inclusions

$$H^k \subset G \subset \operatorname{Aut}(H) \wr \operatorname{Sym}(k),$$

where k is a positive integer, the group $\operatorname{Sym}(k)$ acts on k points, and H is some finite non-abelian simple group. Let G be an isotypical semi-simple group of size at most n. Denote by m the size of H. It is clear that $m^k \leq n$ and hence $k \leq \log(n)$. Note that the group $\operatorname{Aut}(H) \wr \operatorname{Sym}(k)$ fits into an extension

$$1 \to \operatorname{Aut}(H)^k \to \operatorname{Aut}(H) \wr \operatorname{Sym}(k) \to \operatorname{Sym}(k) \to 1.$$

By a result of Kozma and the author [14] there exists a group law for $\operatorname{Sym}(k)$ of length bounded by $\exp(C \log(k)^4 \log \log(k))$. This result also relies on the CFSG. For the purpose of this proof, we can work with an explicit law of length bounded by $\exp(C(k \log(k))^{1/2})$; see [2] or [14] for a discussion. Moreover, the automorphism group $\operatorname{Aut}(H)$ of a non-abelian finite simple group H fits into an exact sequence

$$1 \to H \to \operatorname{Aut}(H) \to \operatorname{Out}(H) \to 1,$$

where the group $\operatorname{Out}(H)$ is solvable of class 3. This assertion is usually called Schreier's Conjecture and was only proved as a consequence of the CFSG. Thus, if H admits a law of length bounded by $O(m/\log(m)^2)$ by Proposition 4.1, then Lemma 2.2 allows to construct a law of length bounded by $O(m/\log(m)^2)$ also for $\operatorname{Aut}(H)$. Note that this will also be a law for $\operatorname{Aut}(H)^k$. Using Lemma 2.2 again, we can combine this with the law for $\operatorname{Sym}(k)$ and obtain a law for G. The length will be bounded by

$$O(m \log(m)^{-2} \exp(C(k \log(k))^{1/2}),$$

where the construction only depended on m and k. We treat the case k = 1, m = n and $k = \log(n), m = n^{1/2}$ separately and combine the results using Lemma 2.1. Note that each isotypical semi-simple group of cardinality less than or equal to n will be covered by one of the two cases, since $k \geq 2$ implies $m \leq n^{1/2}$. Thus, the resulting word will be a law for all isotypical semi-simple groups of size at most n. It is easy to see that the dominating contribution comes from k = 1, m = n. This proves Proposition 4.1 for isotypical semi-simple groups.

A group is called semi-simple (in the sense of Fitting) if it does not contain any non-trivial abelian normal subgroups; see for example [17, p. 89] for a modern reference. (Note that the term semi-simple is ambiguously used in group theory.) By a result of Fitting, a general semi-simple group G is contained in a product of isotypical semi-simple groups $G_{(H,k)}$, where $H^k \subset G_{(H,k)} \subset \operatorname{Aut}(H) \wr \operatorname{Sym}(k)$ and also $H^k \subset G$. Since all bounds depended only on the fact that $|H^k| \leq |G|$, the proof of Proposition 4.1 for isotypical semi-simple groups extends verbatim to the case of general semi-simple groups.

Thus, we can summarize our analysis as follows.

PROPOSITION 4.2: Let $n \in \mathbb{N}$. There exists a non-trivial word $w_n \in \mathbf{F}_2$ of length bounded by $O(n/\log(n)^2)$ that is a law for all finite semi-simple groups of size at most n.

This finishes the discussion of the case of semi-simple groups.

5. General case

We are now ready to prove our main result. The general case is done by combining our results for solvable and for semi-simple groups. By a result of Fitting [4], every finite group has a solvable normal subgroup such that the quotient is semi-simple.

Let G be a finite group of size at most n with solvable normal subgroup S and semi-simple quotient L := G/S. Clearly, either $|S| \leq \log(n)^{9/2}$ or $|L| \leq n/\log(n)^{9/2}$. We apply Lemma 2.2 in both situations and combine the laws that we obtain from Proposition 3.2 and Proposition 4.2. In the first case, a word of length bounded by $O(\log(\log(n)^{9/2})^{9/2} \cdot n \log(n)^{-2})$ exists that serves as a law. In the second case, we obtain a word of length bounded by

$$O(\log(n)^{9/2} \cdot n/\log(n)^{9/2} \log(n/\log(n)^{9/2})^{-2}) = O(n\log(n/\log(n)^{9/2})^{-2}).$$

Combining the two cases using Lemma 2.1, we obtain a word of length $O(n \log \log(n)^{9/2}/\log(n)^2)$ and claim that it is a law for all groups of size at most n. Indeed, any finite group of size at most n will satisfy one of the two conditions — finally, this proves our main theorem.

THEOREM 5.1: For every $n \in \mathbb{N}$ there exists a non-trivial word $w_n \in \mathbf{F}_2$ of length

$$O\left(\frac{n\log\log(n)^{9/2}}{\log(n)^2}\right)$$

that is a law for all finite groups of size at most n. In particular, the length of w_n is sublinear in n.

Note that the law that is constructed in the proof of the previous theorem is a completely explicit combination of powers and commutators — the construction itself does not depend on the CFSG. Note also that the proof depends on the CFSG only in using the following two facts:

- (i) The order of elements in a non-abelian simple group G different from $\operatorname{PSL}_2(p^k)$ is bounded from above by $O(|G|^{1/4})$.
- (ii) The outer automorphism group of a non-abelian finite simple group is solvable of class at most 3.

In Theorem 5.1, there is room for improvement in the factor $\log \log(n)^{9/2}$ (even though we were not able to remove it completely, an additional argument shows that one can replace it with $\log^*(n)^2$, where \log^* denotes the iterated logarithm, i.e., $\log^*(n)$ is the smallest number k such that the k-fold iteration of the logarithm yields a number less than or equal to 1) and we believe that $n/\log(n)^2$ is close to the truth, i.e., that the result in Theorem 5.1 is almost sharp. However, it seems notoriously difficult to prove non-trivial lower bounds for the length of laws. This problem also arises in the study of the symmetric group (see [14]), where the best known lower bounds for the length of a law for $\operatorname{Sym}(n)$ are still linear in n. In that direction it would also be very interesting to determine if the bounds in the proof of Proposition 4.1 are sharp. This is of interest since $\operatorname{Sym}(n)$ contains $\operatorname{PSL}_2(p^k)$ for all $p^k < n$ and hence a result in this direction would provide a non-trivial lower bound for the length of laws of $\operatorname{Sym}(n)$. However, any of this seems currently out of reach.

ACKNOWLEDGMENTS. This research was supported by ERC Starting Grant No. 277728. I thank Martin Kassabov for interesting discussions on this topic and

helpful comments on this paper. I thank Laci Pyber for pointing out the work of Glasby [7] and the unknown referee for useful comments.

References

- [1] K. Bou-Rabee, Quantifying residual finiteness, J. Algebra 323 (2010), 729-737.
- [2] K. Bou-Rabee and B. McReynolds, Asymptotic growth and least common multiples in groups, Bull. Lond. Math. Soc. 43 (2011), 1059–1068.
- [3] A. Elkasapy and A. Thom, On the length of the shortest non-trivial element in the derived and the lower central series, J. Group Theory 18 (2015), 793–804.
- [4] H. Fitting, Beiträge zur theorie der Gruppen von endlicher ordnung, Jahresbericht DMV.
- [5] A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev and B. Virág, On the girth of random Cayley graphs, Random Structures Algorithms 35 (2009), 100–117.
- [6] R. A. Gimadeev and M. N. Vyalyi, Identical relations in symmetric groups and separating words with reversible automata, in Computer science—theory and applications, Lecture Notes in Comput. Sci., Vol. 6072, Springer, Berlin, 2010, pp. 144–155.
- [7] S. Glasby, The composition and derived lengths of a soluble group, J. Algebra 120 (1989), 406–413.
- [8] D. Gorenstein, Finite groups, Harper & Row, New York-London, 1968.
- [9] U. Hadad, On the shortest identity in finite simple groups of Lie type, J. Group Theory 14 (2011), 37–47.
- [10] J. Hall, Marshall, The theory of groups, (1959), xiii+434.
- [11] B. Huppert, Lineare auflösbare Gruppen, Math. Z. 67 (1957), 479–518 (German).
- [12] W. M. Kantor and A. Seress, Large element orders and the characteristic of Lie-type simple groups, J. Algebra 322 (2009), 802–832.
- [13] M. Kassabov and F. Matucci, Bounding the residual finiteness of free groups, Proc. Amer. Math. Soc. 139 (2011), 2281–2286.
- [14] G. Kozma and A. Thom, Divisibility and groups laws, Math. Ann. 364 (2016), 79–95.
- [15] A. Lucchini, On the order of transitive permutation groups with cyclic point-stabilizer, Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. 9 (1998), 241–243 (1999) (English, with English and Italian summaries).
- [16] M. F. Newman, The soluble length of soluble linear groups, Math. Z. 126 (1972), 59–70.
- [17] D. J. S. Robinson, A course in the theory of groups, 2 ed., Graduate Texts in Mathematics, Vol. 80, Springer-Verlag, New York, 1996.
- [18] H. Zassenhaus, Beweis eines Satzes über diskrete Gruppen, Abh. Math. Sem. Univ. Hamburg 12 (1937), 289–312 (German).