BOUNDING THE RESIDUAL FINITENESS OF FREE GROUPS

MARTIN KASSABOV AND FRANCESCO MATUCCI

Abstract. We find a lower bound to the size of finite groups detecting a given word in the free group, more precisely we construct a word w_n of length n in non-abelian free groups with the property that w_n is the identity on all finite quotients of size $\sim n^{2/3}$ or less. This improves on a previous result of Bou-Rabee and McReynolds quantifying the lower bound of the residual finiteness of free groups.

A group G is called *residually finite* if for any $w \in G$, $w \neq 1$ there exists a finite group H and a homomorphism $\varphi : G \to H$ such that $\varphi(w) \neq 1$. We will say that such group H *detects* the element w. One way to quantify this property is look at the minimal size of a finite group H which detects a given word, and study the behavior of this function. We define the following natural growth function to measure the residual finiteness of a group (introduced by Bou-Rabee in [2]):

$$k_G(w) := \min\{|H| \mid \text{there exists } \pi : G \to H, \pi(w) \neq 1\}$$

and

$$F_G^S(n) := \max\{k_G(w) \mid |w|_S \leq n\},$$

where S is a generating set of the group G and $|w|_S$ denotes the word length of w with respect to the generating set S.

We also write $f_1 \preceq f_2$ to mean that there exists a C such that $f_1(n) \leq C f_2(Cn)$ for all n, and we write $f_1 \simeq f_2$ to mean $f_1 \preceq f_2$ and $f_2 \preceq f_1$. It is easy to see that if G is finitely generated the growth type of the function F_G^S does not depend on the set S, assuming that it is finite.

In this short note, we will focus on the free group $\mathcal{F}_k$ on k generators. Bou-Rabee [2] and Rivin [9] have shown that $F_{\mathcal{F}_k}(n) \preceq n^3$. Both proofs are obtained by embedding the free group $\mathcal{F}_k$ into $\mathrm{SL}_2(\mathbb{Z})$ and then finding a suitable prime p such that a given word does not vanish in the quotient $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, for a slightly different proof see Remark 8.

Recently, Bou-Rabee and McReynolds [1] have shown (see Corollary 11) that $F_{\mathcal{F}_k}(n) \succeq n^{1/3}$. We improve this lower bound, establishing the following result:

Theorem 1. $F_{\mathcal{F}_k}(n) \succeq n^{2/3}$.

The main new ingredient in the proof of Theorem 1 is a result of Lucchini (Theorem 12) about finite permutation groups.

2000 *Mathematics Subject Classification.* Primary 20F69; Secondary 20E05, 20E07, 20E26.

Key words and phrases. Free group, residually finite group, identities in a group.

The first author was partially funded by grants from National Science Foundation DMS 0600244, 0635607 and 0900932.

Known results on the growth function F_G. The following lemma of Bou-Rabee [2] explains why the function F_G^S is independent on the generating set:

Lemma 2. *Let G be residually finite group generated by a finite set S. If H is a subgroup of G generated by a finite set T, then H is residually finite and $F_H^T(n) \preceq F_G^S(n)$.*

The proof of this lemma is based on the observation that any nontrivial element in H is also a nontrivial in G therefore it can be detected by some finite quotient.

Applying Lemma 2 twice with $G = H$, we see that we can drop the decoration S in $F_G^S(n)$. Moreover, this implies that the growth functions for all non-abelian finitely generated free groups are all equivalent. Hence, we will restrict to study the function $F_{\mathcal{F}_2}(n)$ for the free group on two generators.

Example 3. Most of the words in the free group $\mathcal{F}_k$ can be detected using relatively small quotients. For example, the word $w := z^2y^{23}x^{36}y^{33}z^{-26}$ in $\mathcal{F}_3$ has length 120, but can be detected through the homomorphism $\varphi : \mathcal{F}_3 \to \mathbb{Z}/3\mathbb{Z}$ which maps $\varphi(y) = 1 \pmod 3$ and $\varphi(x) = \varphi(z) = 0 \pmod 3$.

This argument works, because the word w has nontrivial image in the abelianization $\mathbb{Z}^3$ of $\mathcal{F}_3$. In general, if a word $w \in \mathcal{F}_k$ is detected by the abelianization $\mathbb{Z}^k$, it is also detected in a suitable (relatively small) finite quotient of $\mathbb{Z}^k$. Bou-Rabee [2] used the prime number theorem to show:

Theorem 4. *$F_{\mathbb{Z}^k}(n) \simeq \log(n)$.*

Therefore, for any $w \in \mathcal{F}_k \setminus [\mathcal{F}_k, \mathcal{F}_k]$ one has $k_{\mathcal{F}_k}(w) \le C \log |w|$. This is sufficient to show that the value of the function $k_{\mathcal{F}_k}$ on a random word of length n is bounded above by a constant [9].

Theorem 4 can be generalized to nilpotent and soluble groups, but one needs to replace the logarithmic bound of Theorem 4 with a polylogarithmic one. This suggests that the words w in $\mathcal{F}_k$, where $k_{\mathcal{F}_k}(w)$ is large, are the ones which lie deep in the lower central/derived series.

Rephrasing in terms of laws. One possible way to study the function F_G is to notice that an element w can be detected by a finite quotient of size at most n if and only if $w \notin G_n$, where G_n is the intersection of all normal subgroups of G of index at most n. Thus, one can derive properties of the function F_G by estimating the word length of shortest element in the group G_n.

For example, let G be the free group $\mathcal{F}_k$. It is well known [6] that $\mathcal{F}_k$ has $a_n^{\triangleleft}(\mathcal{F}_k) < n^{4k \log n}$ normal subgroups of index at most n (for all large enough n), therefore the intersection

$$\mathcal{F}_{k,n} = \bigcap_{H \trianglelefteq \mathcal{F}_k, [\mathcal{F}_k : H] \le n} H$$

has index at most

$$[\mathcal{F}_k : \mathcal{F}_{k,n}] \le n^{a_n^{\triangleleft}} < n^{n^{4k \log n}},$$

for every n large enough. This shows that $\mathcal{F}_{k,n}$ has an element w_n of length at most $\log[\mathcal{F}_k : \mathcal{F}_{k,n}] \le e^{4k \log^2 n} \log n$. By construction w_n can not be detected by any finite group of size at most n, therefore $k_{\mathcal{F}_k}(w_n) > n$. This shows that

Lemma 5. *$F_{\mathcal{F}_k}(n) \succeq e^{\sqrt{\log n}}$.*

Of course this lower bound is not optimal, there are two reasons for that – first the bound $[\mathcal{F}_k : \mathcal{F}_{k,n}]$ is very far from the correct one; and second the shortest element in $\mathcal{F}_{k,n}$ is very likely to have length significantly smaller than $\log[\mathcal{F}_k : \mathcal{F}_{k,n}]$.

An equivalent, but slightly more convenient way to study the group $\mathcal{F}_{k,n}$ is to consider laws in finite groups.

Definition 6. Given a group Γ an *identity* or *law* in Γ on k letters is a word $w(x_1,\dots,x_k)$ in the free group $\mathcal{F}_k$ such that $w(g_1,\dots,g_k) = 1$, for all elements $g_1,\dots,g_k \in \Gamma$. We denote by $L_{\Gamma,k} \lhd \mathcal{F}_k$ the subgroup of all identities in Γ and by $\alpha_k(\Gamma)$ the length of the shortest identity in a group Γ.

It is easy to see that

$$\mathcal{F}_{k,n} = \bigcap L_{\Gamma,k}$$

where the intersection is taken over all isomorphic classes of finite groups Γ of size at most n. In particular one has

- if $\alpha_k(\Gamma) > l$ for some finite group Γ of order n, then $\mathcal{F}_{k,n}$ does not contain any words of length l, which implies that $F_{\mathcal{F}_k}(l) \le n$;
- if a word $w \in \mathcal{F}_k$ is an identity in any finite group of order at most n then $k_{\mathcal{F}_k}(w) \ge n$, i.e., $F_{\mathcal{F}_k}(|w|) \ge n$.

These two observations allow us to obtain upper and lower bounds for $F_{\mathcal{F}_k}$ by using results about identities in finite groups. The following result of Hadad [4] can be used to obtain an upper bound for $F_{\mathcal{F}_k}(n)$.

Theorem 7. *The length of the shortest identities in* $\mathrm{SL}_2(\mathbb{F}_q)$ *and* $\mathrm{PSL}_2(\mathbb{F}_q)$ *satisfies*

$$\frac{q-1}{3} \le \alpha_k(\mathrm{PSL}_2(\mathbb{F}_q)) \le \alpha_k(\mathrm{SL}_2(\mathbb{F}_q)) < 10(q+2).$$

Remark 8. Let w be a word in the free group of length n. By the above result w is not an identity in the group $\mathrm{PSL}_2(\mathbb{F}_p)$ for any prime $p > 3n+1$, therefore w is not in the kernel of some map $\mathcal{F}_k \to \mathrm{PSL}_2(\mathbb{F}_p)$, i.e., $k_{\mathcal{F}_2}(w) \le |\mathrm{PSL}_2(\mathbb{F}_p)| = (p^3-p)/2$. Thus, we have $F_{\mathcal{F}_k}\left(\frac{p-1}{3}\right) \le (p^3-p)/2$, i.e., $F_{\mathcal{F}_k}(n) \preceq n^3$.

Remark 9. It seems the methods [4] can be used to show that the shortest identity satisfied in all groups of the form $\mathrm{SL}_2(R)$, where R is a finite commutative ring of size at most N, has length CN^2. If this is indeed the case then one can improve the upper bound $F_{\mathcal{F}_k}(n) \preceq n^3$ to $F_{\mathcal{F}_k}(n) \preceq n^{3/2}$.

On the other side, it is easy see that $w = x^{n!}$ is an identity in any group of order at most n. This can be used to obtain a lower bound for $F_{\mathcal{F}_k}(n)$, which is weaker then Lemma 5. However, there is an easy way to improve this bound by constructing a shorter identity by using the following lemma [4], which plays a central role in the proof of the upper bound in Theorem 7.

Lemma 10. *Let* $r_1 > \dots > r_m$ *be a finite sequence of integers. There exist a nontrivial word* $w = w_{r_1,\dots,r_m} \in \mathcal{F}_2$ *of length at most* $4m^2 \cdot (r_1+1)$ *with the following property:* w *is a law in any finite group* Γ *such that every* $\gamma \in \Gamma$ *is a solution to at least one of these equations*

$$X^{r_1} = 1, \dots, X^{r_m} = 1.$$

Sketch of the proof: The nontrivial word $w = w_{r_1,\dots,r_m}$ is built by taking a suitable iterated commutator of (conjugates of) the powers $x^{r_1},\dots,x^{r_m}$ of the first letter x. For example, if $m = 4$ we build

$$[x^{r_1},(x^{r_2})^y], \qquad [x^{r_3},(x^{r_4})^y],$$

and then take their commutator

$$w := [[x^{r_1},(x^{r_2})^y],[x^{r_3},(x^{r_4})^y]].$$

For general m one needs to be careful to create a commutator word w that has no internal cancellation. □

This lemma gives the following lower bound for the function $F_{\mathcal{F}_k}(n)$.[1]

Corollary 11. $F_{\mathcal{F}_k}(n) \succeq n^{1/3}$.

Proof. The order of any element in a finite group is at most the size of the group. By Lemma 10, we can build a word $v_n := w_{n,n-1,\dots,1}$ which is an identity in any finite group of size $\le n$. Moreover the length of v_n is $|v_n| \le 4n^2(n+1)$, thus $F_{\mathcal{F}_k}(4n^3+4n^2) > n$. □

Improvement of Corollary 11. This construction can be significantly improved if one combines it with a result of Lucchini about permutation groups [7].

Theorem 12. *Let Γ be a transitive permutation group of degree $n > 1$ whose point-stabilizer subgroup is cyclic. Then $|\Gamma| \le n^2 - n$.*

Remark 13. Unlike many similar results about permutation groups, the proof of Lucchini's result is elementary and does not rely on the Classification of Finite Simple Groups.

In the proof of Theorem 1 we will use the following corollary to Lucchini's result[2], which will give us information in case a group has an element of "large order".

Corollary 14. *Let Γ be a finite group and let $x \in \Gamma$ such that $|x| \ge \sqrt{|\Gamma|}$. Then there is an integer $\ell < \sqrt{|\Gamma|}$ such that $\langle x^\ell \rangle \trianglelefteq \Gamma$.*

Proof. The action of Γ on the cosets $\Gamma/\langle x \rangle$ is transitive. If N is the kernel of the action, then $N \le \langle x \rangle$ is cyclic and, by Lucchini's Theorem $[\Gamma : N] < |\Gamma : \langle x \rangle|^2$. Since

$$[\Gamma : \langle x \rangle][\langle x \rangle : N] = [\Gamma : N] < [\Gamma : \langle x \rangle]^2,$$

then

$$\ell := [\langle x \rangle : N] < [\Gamma : \langle x \rangle] \le \sqrt{|\Gamma|}.$$

Thus, $\langle x^\ell \rangle \le N \trianglelefteq \Gamma$, since N is cyclic, we have $\langle x^\ell \rangle \trianglelefteq \Gamma$. □

Remark 15. The previous result shows that if a group Γ has elements of order larger than $\sqrt{\Gamma}$, there are restrictions on the structure of Γ. The next natural step would be to study a group Γ with elements of order larger than $\sqrt[3]{\Gamma}$. We observe that the Classification of Finite Simple Groups implies that any non-abelian finite simple group S does not have elements of order more than $|S|^{1/3}$, thus it seems likely that

[1] This was obtained independently by Bou-Rabee and McReynolds in [1].

[2] This was obtained independently by Herzog and Kaplan in [5] in 2001 and became known to the authors only after the completion of this work.

existence an element in a finite group Γ of order more $|\Gamma|^{1/3}$ implies restrictions on the structure of Γ.

Lemma 16. *Let n be a positive integer, then the word $v_n \in \mathcal{F}_2$ constructed in Corollary 11 is a law in every group of order $|\Gamma| \leq \frac{1}{9}n^2$.*

Proof. We want to show that the commutator word $v_n \in \mathcal{F}_2$ is a law on any group Γ of order $|\Gamma| \leq \frac{1}{9}n^2$, so we evaluate $v_n(\gamma_1, \gamma_2)$ on any two elements $\gamma_1, \gamma_2 \in \Gamma$. There are two cases:

(1) If $|\gamma_1| \leq n$, then $\gamma_1^k = 1$ for some $k < n$, thus $v_n(\gamma_1, \gamma_2) = 1$.
(2) If $|\gamma_1| > n$ then, by Corollary 14, there is a power $\ell < n/3$ such that the cyclic group $N := \langle \gamma_1^\ell \rangle$ is normal in Γ. There exist at least two powers γ_1^s, γ_1^t, for suitable $s < n/2 < t < n$ such that $\gamma_1^s, \gamma_1^t \in N$. However, by construction v_n is a commutator of two words w' and w'' which are built as commutators conjugates of powers of x^i. Since N is normal and the powers x^s and x^t are involved in w' and w'' respectively and we have that $w'(\gamma_1, \gamma_2), w''(\gamma_1, \gamma_2) \in N$. The group N is abelian which implies that
$$v_n(\gamma_1, \gamma_2) = [w'(\gamma_1, \gamma_2), w'(\gamma_1, \gamma_2)] \in [N, N] = 1.$$

In both cases we have seen that $v_n(\gamma_1, \gamma_2) = 1$, hence v_n is an identity in Γ. □

The previous Lemma immediately implies that there exists a word of length n in $\mathcal{F}_2$ which cannot be detected by any group of size $n^{2/3}$ or less.

Proof of Theorem 1. By Lemma 16 we have a word v_n which is the identity in any finite group of size $\leq \frac{1}{9}n^2$ and, by Lemma 10, the length of v_n is $|v_n| \leq 4n^2(n+1)$. Therefore $F_{\mathcal{F}_k}(4n^3 + 4n^2) > \frac{1}{9}n^2$. □

Remark 17. Theorem 1 and Remark 8 are also valid if the free group is replaced by a surface group. The lower bound follows from Lemma 2, Theorem 1 and the observation that any surface group contains a free subgroup. Rivin has showed in [9] that the upper bound of Remark 8 can be extended to surface groups.

Open questions. From Theorem 1 and Bou-Rabee's result on the upper bound, one can ask the following natural question:

Question 18. Is it true that $F_{\mathcal{F}_k}(n) \simeq n$?

Question 19. What is the asymptotic behavior of the index of $[\mathcal{F}_2 : \mathcal{F}_{2,n}]$ as a function of n?

Let $\mathcal{F}_{2,n}^{\max}$ denote the intersection of all maximal normal subgroup in $\mathcal{F}_2$ of index at most n. It can be shown that $[\mathcal{F}_2 : \mathcal{F}_{2,n}^{\max}] \preceq e^{n^{4/3}}$, therefore $[\mathcal{F}_2 : \mathcal{F}_{2,n}] \succeq e^{n^{4/3}}$. This suggest that $[\mathcal{F}_2 : \mathcal{F}_{2,n}] \simeq e^{n^\alpha}$ for some α.

We define the *divisibility function* of the free group $D_{\mathcal{F}_k} : \mathcal{F}_k \setminus \{1\} \to \mathbb{N}$. The function is defined by
$$D_{\mathcal{F}_k}(w) = \min_{H \leq \mathcal{F}_k} \{[\mathcal{F}_k : H] \mid w \notin H\}.$$

Bogopolski asked the following question in the Kourovka notebook [8].

Question 20. Does there exist a $C = C(k) > 0$ such that $D_{\mathcal{F}_k}(w) \leq C \log(|w|)$?

Bou-Rabee and McReynolds [1] showed that this question has a negative answer establishing the following result on the lower bound.

Theorem 21. $\max_{|w|\leq n} D_{\mathcal{F}_k}(w) \not\preceq \log(n)$.

On the other hand, Buskin [3] has an upper estimate using Stallings automata:

Theorem 22. $D_{\mathcal{F}_k}(w) \leq \frac{|w|}{2} + 2$.

Acknowledgments. The authors thank Nikolai Nikolov, Khalid Bou-Rabee, Ben McReynolds and Enric Ventura for helpful discussions. The authors would also like to thank Oleg Bogopolski and Mikhail Ershov for providing the reference [3] and Avinoam Mann for providing the reference [5]. Finally the authors would like to thank the referees for a careful reading which improved the form of this paper.

The authors gratefully acknowledge the support from the Centre de Recerca Matemàtica, Barcelona and the Universitat Politécnica de Catalunya where most of work has been done in June 2009.

References

1. K. Bou-Rabee and D. B. McReynolds. Asymptotic growth and least common multiples in groups. *preprint*. `arXiv:math.GR/0907.3681v1`.
2. Khalid Bou-Rabee. Quantifying residual finiteness. *Journal of Algebra*. to appear, `arXiv:math.GR/0807.0862v4`.
3. N. V. Buskin. Economical separability in free groups. *Siberian Mathematical Journal*, 50(4):603–608, 2009.
4. Uzy Hadad. On the shortest identity in finite simple groups of lie type. *Journal of Group Theory*. to appear, `arXiv:math.GR/0808.0622v1`.
5. M. Herzog and G. Kaplan, Large cyclic subgroups contain non-trivial normal subgroups. *Journal of Group Theory*, 4(3), 247-253, 2001.
6. Alexander Lubotzky and Dan Segal. *Subgroup growth*, volume 212 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 2003.
7. Andrea 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(4):241–243 (1999), 1998.
8. V. D. Mazurov and E. I. Khukhro, editors. *The Kourovka notebook*. Russian Academy of Sciences Siberian Division Institute of Mathematics, Novosibirsk, sixteenth edition, 2006. Unsolved problems in group theory, Including archive of solved problems.
9. Igor Rivin. Geodesics with one self-intersection, and other stories. *preprint*. `arXiv:math.GT/0901.2543v3`.

Cornell University, Department of Mathematics, 590 Malott Hall, Ithaca, NY 14853, USA

Current address: School of Mathematics, University of Southampton, University Road, Southampton, SO17 1BJ, UK

E-mail address: `kassabov@math.cornell.edu`

University of Virginia, Department of Mathematics, Charlottesville, VA 22904, USA

E-mail address: `fm6w@virginia.edu`