Short Laws for Finite Groups

Henry Bradford (joint work with Andreas Thom)
henry.bradford@mathematik.uni-goettingen.de

GEORG-AUGUST-UNIVERSITÄT GÖTTINGEN

What Are Laws?

Fix x, y an ordered basis for the rank-2 free group F_2 and let G be any group.

Recall that for any $(g,h) \in G \times G$, there exists a unique homomorphism $F_2 \to G$ extending $x \mapsto g$, $y \mapsto h$.

Let $w \in F_2$ be non-trivial. There is an induced *word map* $w_G : G \times G \to G$ given by:

$$w_G(g,h) = \pi_{(g,h)}(w).$$

Definition 1. *We call w a* law *for G if:*

$$w_G(G \times G) = \{1_G\}.$$

Example 2. *G is abelian if and only if $[x,y]$ is a law for G.*

Example 3. *Suppose w is a law for G. Then w is a law for every subgroup and every quotient of G.*

Example 4. *Suppose G is finite. Then $x^{|G|}$ is a law for G.*

Henceforth G is a finite group. **We are interested in the length of the *shortest* law for G.** We exhibit bounds for the asymptotic behaviour of this quantity for sequences of finite groups.

Previous Work

Particular recent interest has focused on finite simple groups and their relatives.

Theorem 5 (Hadad, 2011 [4]; Kozma-Thom, 2014 [5])**.** *Let G be a finite group of Lie type of rank r over a field of order q. Then there is a word $w \in F_2$ of length:*

$$O(q^{O(r)})$$

which is a law for G.

Theorem 6 (Kozma-Thom, 2014 [5])**.** *There exists a law for $\mathrm{Sym}(n)$ of length at most:*

$$\exp(O(\log(n)^4 \log\log(n))).$$

In another direction, Thom constructs **laws which are simultaneously valid in all finite groups up to a given order.**

Theorem 7 (Thom 2015 [7])**.** *For all $n \in \mathbb{N}$, there exists a word $w_n \in F_2$ of length*

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

such that for every finite group G satisfying $|G| \leq n$, w_n is a law for G.

Results for Arbitrary Groups

Theorem 8 (B-Thom, 2016)**.** *For all $n \in \mathbb{N}$ there exists a word $w_n \in F_2$ of length*

$$O(n^{2/3} \log(n)^{O(1)})$$

such that for every finite group G satisfying $|G| \leq n$, w_n is a law for G.

The main term $n^{2/3}$ improves upon the n from Theorem 7 and is believed to be best possible.

Results for Simple Groups

Theorem 9 (B-Thom, 2016)**.** *Let G be a finite group of Lie type over a field of order q, such that the natural module for G has dimension d. Then G has a law of length:*

$$O_d(q^{\lfloor d/2 \rfloor} \log(q)^{O_d(1)}).$$

The exponent $\lfloor d/2 \rfloor$ in Theorem 9 is sharp, as the following example shows.

Example 10 (Hadad, 2011 [4])**.** *Let $G = \mathrm{SL}_2(q)$, let $t \in \mathbb{F}_q$ and let:*

$$g(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \ h(t) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.$$

Suppose $w \in F_2$ is a law for G. Then $w_G(g(t), h(t)) = I_2$ for all $t \in \mathbb{F}_q$. Viewing the entries of $w_G(g(t), h(t)) - I_2$ as polynomials in t (of degree $\leq |w|$) which vanish identically on $\mathbb{F}_q$, it follows that $|w| \geq q$. $\mathrm{SL}_2(q^{\lfloor d/2 \rfloor}) \hookrightarrow \mathrm{SL}_d(q)$ (by restriction of scalars) so $\mathrm{SL}_d(q)$ has no law of length less than $q^{\lfloor d/2 \rfloor}$.

Residual Finiteness Growth

Recall that a finitely generated group Γ is *residually finite* if every non-trivial $g \in \Gamma$ has non-trivial image in some finite quotient of Γ. Define:

$$k_\Gamma(g) = \min\{|Q| : \exists \pi : \Gamma \to Q, \pi(g) \neq 1_Q\}.$$

Fix a finite generating set S for Γ and let:

$$\mathcal{F}_\Gamma^S(n) = \max\{k_\Gamma(g) : 1_\Gamma \neq g \in \Gamma, |g|_S \leq n\}.$$

$\mathcal{F}_\Gamma^S$ was introduced by Bou-Rabee [2], who started the process of establishing asymptotic bounds for various groups Γ. **Intuitively, if $\mathcal{F}_\Gamma^S$ grows slowly then elements of Γ are easy to detect in finite quotients.** For this reason, particular attention has been paid to free groups, which have very rich families of finite quotients. Here we can apply Theorem 8:

Theorem 11 (B-Thom, 2016)**.** *Let Γ be a non-abelian finite rank free group. Then:*

$$\mathcal{F}_\Gamma^S(n) \gg_S n^{3/2} / \log(n)^{O(1)}.$$

Basic Tools

We have two simple ways of constructing new laws from old.

Lemma 12. *Let $1 \to N \to G \to Q \to 1$ be an extension of groups. Suppose N, Q satisfy laws of length n_N, n_Q, respectively. Then G satisfies a law of length at most $n_N(n_Q + 2)$.*

For the second Lemma, we introduce the following notation:

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

So w is a law for G iff $Z(G,w) = G \times G$.

Lemma 13. *Let $w_1, \ldots, w_m \in F_2$ be non-trivial words. Then there exists a non-trivial word $w \in F_2$ of length at most $16m^2 \max_i |w_i|$ such that for all groups G,*

$$Z(G,w) \supseteq Z(G,w_1) \cup \ldots \cup Z(G,w_m).$$

Diameters

Using Lemma 13 we divide the proof of Theorem 9 into two cases: generating and non-generating pairs. For generating pairs we apply bounds on the diameter of G.

Recall that the *diameter* of a finite group G with respect to a generating set S is:

$$\mathrm{diam}(G,S) = \min\{l \in \mathbb{N} : B_S(l) = G\}$$

where:

$$B_S(l) = \{g \in G : |g|_S \leq l\}$$

and the diameter of G itself is:

$$\mathrm{diam}(G) = \max\{\mathrm{diam}(G,S) : S \subseteq G, \langle S \rangle = G\}.$$

Theorem 14 (Breuillard-Green-Tao, Pyber-Szabo, 2010 [3],[6])**.** *Let G be a finite simple group of Lie type of rank r. Then:*

$$\mathrm{diam}(G) \leq (\log|G|)^{O_r(1)}.$$

Theorem 14 is useful because it allows us to quickly reach a large subset of G on which the word map of a short word vanishes. In groups of Lie type, this subset will usually be a split maximal torus.

Maximal Subgroups

For non-generating pairs we use known descriptions of maximal subgroups in groups of Lie type and an induction argument.

Example 15. *Suppose $H \leq \mathrm{SL}_d(q)$ preserves a non-trivial proper subspace of $\mathbb{F}_q^d$ of dimension a. Then there is an extension:*

$$1 \to N \to H \to Q \to 1$$

with $Q \leq \mathrm{GL}_a(q) \times \mathrm{GL}_{d-a}(q)$ and $N \leq SL_d(q)$ nilpotent (hence of class at most $d-1$). Assuming Theorem 9 for smaller d and repeatedly applying Lemma 12, H satisfies a law of the required length.

By Aschbacher's Theorem [1], maximal subgroups of classical groups **either satisfy "geometric" restrictions** (such as those in Example 15) **or are almost simple**, and can be dealt with on a case-by-case basis (thanks to CFSG).

Similar taxonomies of maximal subgroups are known for exceptional groups.

References

[1] M. Aschbacher. On the maximal subgroups of the finite classical groups. Invent. Math. 76 (1984), 469-514

[2] K. Bou-Rabee. Quantifying residual finiteness. J. Algebra 323 (2010), 729-737

[3] E. Breuillard, B. Green, T. Tao. Approximate subgroups of linear groups. Geom. Funct. Anal. 21 (2011), 774-819

[4] U. Hadad. On the shortest identity in finite simple groups of Lie type. J. Group Theory 14 (2011) no. 1, 37-47

[5] G. Kozma, A. Thom. Divisibility and laws in finite simple groups. Mathematische Annalen 361, Issue 1 (2016), 79-95

[6] L. Pyber, E. Szabo. Growth in finite simple groups of Lie type. J. Amer. Math. Soc. 29, Issue 1 (2016) 95-146.

[7] A. Thom. About the length of laws for finite groups. arXiv:1508.07730 [math.GR]