Fibers of word maps and composition factors

Contributed talk at the Groups St Andrews Conference 2017

Alexander Bors

Dept. of Mathematics, University of Salzburg

August 10, 2017

Word maps: Definition and examples

Definition 1

Let $d \in \mathbb{N}$, $w \in \mathrm{F}(X_1, \ldots, X_d)$ a (reduced) word, G a group. The *word map over G with respect to w* is the function $w_G : G^d \to G$ mapping $(g_1, \ldots, g_d) \mapsto w(g_1, \ldots, g_d)$.

Examples

1. $d = 1$, $w = X_1^e$, $e \in \mathbb{Z}$. Then $w_G : G \to G$ is the e-th power function on G.
2. $d = 2$, $w = X_1 X_2$. Then $w_G : G^2 \to G$ is the group multiplication of G.
3. $d = 2$, $w = [X_1, X_2] = X_1 X_2 X_1^{-1} X_2^{-1}$. Then $w_G : G^2 \to G$ is the commutator map of G.

Word maps: Some notable results

In recent years: Intense interest in word maps, particularly on **nonabelian finite simple groups** and particularly in their **images** and **fibers** (preimages of one-element sets). Examples:

1. For every nonabelian finite simple group S, the commutator map $S^2 \to S$ is surjective (the celebrated *Ore Conjecture*, posed in 1951); Liebeck, O'Brien, Shalev, Tiep (2010), see [8, Theorem 1].
2. For each $w \in \mathrm{F}(X_1, \ldots, X_d) \setminus \{1\}$, there is a constant $N(w) > 0$ such that for all nonabelian finite simple groups S with $|S| \geq N$, every element of S can be written as a product of two values of the word map w_S (a result similar to Waring's theorem from number theory); Larsen, Shalev, Tiep (2011), see [7, Corollary 1.1.2].

Word maps: Some notable results cont.

3. For each $w \in \mathrm{F}(X_1, \ldots, X_d) \setminus \{1\}$, there are constants $N(w), \eta(w) > 0$ such that for all nonabelian finite simple groups S with $|S| \geq N$, the largest fiber size of w_S is at most $|S|^{d-\eta}$. In particular, for fixed w, the largest fiber of size of w_S is $o(|S|^d)$ for $|S| \to \infty$; Larsen, Shalev (2012), see [5, Theorem 1.2]. For a recent, much stronger result, see [6, Theorem 1.1].

Equivalent reformulation of the above "In particular": For all $w \in \mathrm{F}(X_1, \ldots, X_d) \setminus \{1\}$ and all $\rho \in (0, 1]$, the order of a nonabelian finite simple group S such that w_S has a fiber of size at least $\rho|S|^d$ (i.e., of **proportion** at least ρ) is bounded in terms of ρ.

Question

What can one say in general about a finite group G under the assumption that w_G has a fiber of proportion at least ρ?

Large nonabelian composition factors

Theorem 1 (B., 2016+), [1, Theorem 1.1.2]

Let $w \in \mathrm{F}(X_1, \ldots, X_d) \setminus \{1\}$, $\rho \in (0,1]$. There are constants $C_1(w,\rho), C_2(w,\rho) > 0$ such that the following hold for any finite group G where w_G has a fiber of proportion at least ρ:

1. No finite alternating group of degree greater than $C_1(w,\rho)$ is a composition factor of G.
2. No finite simple group of Lie type of untwisted Lie rank greater than $C_2(w,\rho)$ is a composition factor of G.

What about simple Lie type groups of bounded rank?

Large nonabelian composition factors cont.

Theorem 2 (Larsen and Shalev, 2017+), cf. [6, Theorem 1.7]

Let $w \in \mathrm{F}(X_1, \ldots, X_d) \setminus \{1\}$, $r \in \mathbb{N}$, $\rho \in (0, 1]$. There are constants $N(w, \rho), \epsilon(w, \rho) > 0$ such that for any finite group G where w_G has a fiber of proportion at least ρ, no finite simple group of Lie type of rank at most r and order greater than N is a composition factor of G.

By combining Theorems 1 and 2 (or referring to [6, Theorem 1.1]), we get:

Corollary

Let $w \in \mathrm{F}(X_1, \ldots, X_d) \setminus \{1\}$, $\rho \in (0, 1]$. There is a constant $C(w, \rho) > 0$ such that a finite group G where w_G has a fiber of proportion at least ρ has no nonabelian composition factors of order greater than $C(w, \rho)$.

Small nonabelian composition factors

What about nonabelian composition factors of small order?

Definition 2

Let $w \in \mathrm{F}(X_1, \ldots, X_d)$.

1. We call w *multiplicity-bounding* if and only if for each nonabelian finite simple group S and each $\rho \in (0,1]$, there is a constant $m(w, S, \rho) > 0$ such that for every finite group G where w_G has a fiber of proportion at least ρ, the multiplicity of S as a composition factor of G is at most $m(w, S, \rho)$.
2. We call w *index-bounding* if and only if for each $\rho \in (0,1]$, there is a constant $I(w, \rho) \in (0,1]$ such that for every finite group G where w_G has a fiber of proportion at least ρ, we have $[G : \mathrm{Rad}(G)] \leq I(w, \rho)$, where $\mathrm{Rad}(G)$ denotes the *solvable radical of* G.

Small nonabelian composition factors cont.

Remarks

1. As Larsen and Shalev observe in [6, proof of Theorem 1.10], the above Corollary implies (via a short argument) that the word properties of being multiplicity-bounding resp. index-bounding are equivalent.
2. Not every nonempty reduced word is multiplicity-bounding. For example, for $w = X_1^{30}$, w_G is constant for $G = \mathcal{A}_5^n$ for all $n \in \mathbb{N}$.

Our next result lists some interesting examples of index-bounding words. We give it in its original form (asserting that those words are multiplicity-bounding, not index-bounding).

Small nonabelian composition factors cont.

Theorem 3 (B., 2017+), [2, Theorem 1.1.2]

The following reduced words are multiplicity-bounding:

1. X_1^e for $e \in (2\mathbb{Z}+1) \cup \{\pm 2, \pm 4, \pm 6, \pm 10, \pm 14, \pm 20, \pm 22\}$. Moreover, X_1^e with $e \in \{\pm 8, \pm 12, \pm 16, \pm 18, \pm 24, \pm 30\}$ is *not* multiplicity-bounding.
2. The words $\gamma_d(X_1, \ldots, X_d)$, defined recursively via $\gamma_1 := X_1$ and $\gamma_{d+1} := [X_{d+1}, \gamma_d]$.
3. All nonempty reduced words of length at most 8 except for $X_i^{\pm 8}$.

Moreover, there is an algorithm, implemented by the author in GAP [4], which on input $e \in \mathbb{Z}$ decides whether X_1^e is multiplicity-bounding [2, Theorem 5.1]. Whether there is such a decision algorithm for reduced words in general is open.

Application: Approximability of word maps by homomorphisms

- Various authors have studied finite groups G having an automorphism α mapping certain minimum proportions of elements of G to their e-th power, for a fixed $e \in \{-1, 2, 3\}$.
- For example: A finite group G with an automorphism inverting more than $\frac{3}{4}|G|$ (resp. $\frac{4}{15}|G|$) elements of G is abelian (resp. solvable), folklore due to Miller (1929) [10, first paragraph] (resp. Potter (1988) [11, Corollary 3.2]).
- Recently, Mann proposed a general approach for tackling such problems, working for all $e \in \mathbb{Z}$ and even when replacing the word "automorphism" by the weaker "endomorphism". It consists in rewriting the assumption on G into a lower bound on the proportion of solutions of a certain word equation over G.

Application: Approximability of word maps by homomorphisms cont.

Theorem 4 (Mann, 2017+), [9, Theorem 9]

Let $\rho \in (0,1]$. There is a constant $\eta(\rho) \in (0,1]$ such that for all $e \in \mathbb{Z}$ and all finite groups G having an endomorphism φ with $\varphi(x) = x^e$ for at least $\rho|G|$ many $x \in G$, the following word equation over G in three variables x, y, z has at least $\eta|G|^3$ many solutions: $(xyz)^e = x^e y^e z^e$.

One can generalize this further. Fix $w \in \mathrm{F}(X_1, \ldots, X_d)$ and a number $\rho \in (0,1]$, and consider the condition on a finite group G that there is a homomorphism $\varphi : G^d \to G$ such that

$$|\{\vec{g} \in G^d \mid w_G(\vec{g}) = \varphi(\vec{g})\}| \geq \rho|G|^d.$$

Application: Approximability of word maps by homomorphisms cont.

Theorem 5 (B., 2017+), [3, Theorem 1.2]

There is an explicit function $f:(0,1]\to(0,1]$ such that the following holds for all $w\in\mathrm{F}(X_1,\ldots,X_d)$, all $\rho\in(0,1]$ and all finite groups G: If there is a homomorphism $\varphi: G^d\to G$ agreeing with w_G on at least $\rho|G|^d$ many arguments, then the following word equation in $3d$ pairwise distinct variables s_i,t_i,u_i, $i=1,\ldots,d$, has at least $f(\rho)|G|^{3d}$ many solutions in G^{3d}:

$$w(s_1^{-1}t_1u_1,\ldots,s_d^{-1}t_du_d)=$$
$$w(s_1,\ldots,s_d)^{-1}w(t_1,\ldots,t_d)w(u_1,\ldots,u_d).$$

Application: Approximability of word maps by homomorphisms cont.

Corollary (B., 2017+), [3, Corollary 3.1]

A finite group G for which the group multiplication $G^2 \to G$ agrees with some homomorphism $G^2 \to G$ on at least $\rho|G|^2$ many pairs has its commuting probability explicitly bounded away from 0 in terms of ρ.

References

1. A. Bors, Fibers of automorphic word maps and an application to composition factors, to appear in *J. Group Theory*, `https://doi.org/10.1515/jgth-2017-0024`.
2. A. Bors, Fibers of word maps and the multiplicities of nonabelian composition factors, submitted (2017), preprint available on arXiv, `https://arxiv.org/abs/1703.00408`.
3. A. Bors, Approximability of word maps by homomorphisms, preprint (2017), `https://arxiv.org/abs/1708.00477`.
4. The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.6* (2016), `http://www.gap-system.org`.
5. M. Larsen and A. Shalev, Fibers of word maps and some applications, *J. Algebra* **354** (2012), 36–48.

References cont.

6 M. Larsen and A. Shalev, Words, Hausdorff dimension and randomly free groups, preprint (2017), https://arxiv.org/abs/1706.08226.

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

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

9 A. Mann, Groups satisfying identities with high probability, *Int. J. Alg. Comp.* (B.I. Plotkin issue), to appear.

10 G.A. Miller, Groups which admit automorphisms in which exactly three-fourths of the operators correspond to their inverses, *Proc. Nat. Acad. Sci. USA* **15**(2) (1929), 89–91.

11 W.M. Potter, Nonsolvable groups with an automorphism inverting many elements, *Arch. Math. (Basel)* **50**(4) (1988), 292–299.