Groups Geom. Dyn. 5 (2011), 501–507
DOI 10.4171/GGD/136

Groups, Geometry, and Dynamics

Powers in finite groups

Nikolay Nikolov and Dan Segal

For Fritz Grunewald on his 60th birthday

Abstract. If G is a finitely generated profinite group then the verbal subgroup G^q is open. In a d-generator finite group every product of qth powers is a product of $f(d,q)$ qth powers.

Mathematics Subject Classification (2010). 20E20, 20F20.

Keywords. Power subgroups, verbal width, profinite groups.

1. Introduction

1.1. The main result. For a group H and positive integer q the qth power subgroup is

$$H^q = \langle h^q \mid h \in H \rangle .$$

Every element of H^q is a product of qth powers; let us say that H^q has *width* n if each such element is equal to a product of n qth powers (we don't assume that n is minimal).

Theorem 1. *Let $q, d \in \mathbb{N}$. Then there exists $f = f(d,q)$ such that H^q has width f whenever H is a d-generator finite group.*

Straightforward arguments show that this is equivalent to

Corollary 1. *If G is a finitely generated profinite group and $q \in \mathbb{N}$ then the (algebraically defined) subgroup G^q has finite width, and is closed in G.*

Together with the positive solution of the Restricted Burnside Problem ([Z1], [Z2]) this in turn implies

Corollary 2. *If G is a finitely generated profinite group then G^q is open in G for every $q \in \mathbb{N}$.*

The deduction of the corollaries from Theorem 1 is explained in [NS], §1, and in Chapter 4 of [W]. Theorem 1 strengthens [NS], Theorem 1.8 and Corollary 2 generalizes [NS], Theorem 1.5.

For $q, d \in \mathbb{N}$ let

$$\beta(d,q)$$

denote the order of the d-generator restricted Burnside group of exponent q; this is the maximal order of any finite d-generator of exponent dividing q. The minimal size of a generating set for a group H is denoted $\mathrm{d}(H)$. If H is finite and $\mathrm{d}(H) \le d$ then $|H : H^q| \le \beta(d,q)$, so by Schreier's formula we have $\mathrm{d}(H^q) \le d\beta(d,q)$. Taking

$$\delta(d,q) = d\beta(d,q) \cdot f(d,q)$$

we see that Theorem 1 implies

Theorem 2. *Let $q, d \in \mathbb{N}$. Then there exists $\delta = \delta(d,q)$ such that H^q can be generated by δ qth powers in H whenever H is a d-generator finite group.*

1.2. Wider implications. The main results of [NS] show that certain verbal subgroups are necessarily closed in a finitely generated profinite group, namely those associated to a locally finite word or to a simple commutator. This list can now be extended:

Theorem 3. *If G is a finitely generated profinite group and w is a non-commutator word then the verbal subgroup $w(G)$ is open in G.*

This greatly generalizes [NS], Theorem 1.3. It follows immediately from Corollary 2 since $w(G)$ contains G^q where $q = |\mathbb{Z}/w(\mathbb{Z})|$. Taking G to be the free profinite group on d generators and w any non-commutator word, we may infer the existence of $f(d,w)$ and $\delta(d,w)$ such that if H is any d-generator finite group, then

- every product of w-values or their inverses in H is equal to such a product of length $f(d,w)$,
- the verbal subgroup $w(H)$ is generated by $\delta(d,w)$ w-values

(cf. [NS], §1, or [W], §4.1).

Let us say that a group word w is *good* if $w(G)$ is closed in G whenever G is a finitely generated profinite group. The word $w = w(x_1, \ldots, x_k)$ may be considered as an element of the free group F on $\{x_1, \ldots, x_k\}$. Recall that w is a *commutator word* if $w \in F'$, the derived group of F. It is shown in [JZ] that if $1 \ne w \in F''(F')^p$ then $w(G)$ is *not* closed in the free pro-p group G on two generators (p being any prime). Thus for a non-trivial word w,

$$w \notin F' \implies w \text{ good} \implies w \notin F''(F')^p \quad \text{for all } p.$$

The first implication is certainly strict, since simple commutators are good; whether the second implication is reversible is an intriguing open question, discussed at length in [W], Chapter 4.

This paper should be seen as a sequel to [NS], which contains all the difficult arguments needed for Theorem 1. In particular, that paper establishes (1) a weaker version of this theorem, restated below as Proposition 1, and (2) an implicit proof that Theorem 1 would follow from Theorem 2; this is sketched in §4 below. As we shall see, Theorem 2 can in turn be deduced quite easily from (1) and another result in [NS].

The original motivation for [NS] was to establish that every subgroup of finite index in a finitely generated profinite group is open ('Serre's problem'). This of course follows at once from Corollary 2, and our initial strategy was indeed an attempt to prove the latter. Our failure to do so forced us to develop machinery for dealing with other verbal subgroups; this did the job just as well, and in fact better, in the sense that the resulting proof was independent of the solution of the Restricted Burnside Problem. Moreover, as far as we know, all the machinery of [NS] is needed to complete the proof of Theorem 1.

The main results all depend on the classification of finite simple groups, which underpins much of [NS]. The proof of Theorem 1 also relies on the solution of the Restricted Burnside Problem. This is inevitable: indeed, Jaikin shows in §5.1 of [JZ] how a positive solution to the Restricted Burnside Problem for a prime power exponent p^n can be deduced directly from Corollary 1 with $q = p^{n+1}$.

Earlier special cases of Theorem 1 were established in [MZ], [SW] (for simple groups) and [S] (for soluble groups).

2. Preliminary results

Henceforth all groups are assumed to be finite. We fix a positive integer q. For a group G and $m \in \mathbb{N}$ we write

$$\begin{aligned} G_q &= \{g^q \mid g \in G\}, \\ G_q^{*m} &= \{h_1 h_2 \dots h_m \mid h_1, \dots, h_m \in G_q\}. \end{aligned}$$

Thus G^q has width m precisely when $G^q = G_q^{*m}$.

The largest integer k such that G involves the alternating group $\mathrm{Alt}(k)$ as a section is denoted $\alpha(G)$.

Proposition 1 ([NS], Theorem 1.8). *Let $d, k \in \mathbb{N}$. Then there exists $h = h(k, d, q)$ such that G^q has width h whenever G is a d-generator finite group with $\alpha(G) \leq k$.*

The next result is a slight weakening of [NS], Proposition 10.1:

Proposition 2. *There exist $m = m(q)$ and $C(q)$ with the following property: if N is a perfect normal subgroup of G and $N/\mathrm{Z}(N) \cong S_1 \times \cdots \times S_n$ where each S_i is a non-abelian simple group with $|S_i| > C(q)$ then*

$$N \cdot G_q^{*m} = G_q^{*m}.$$

We also need two simple lemmas. The first is a mild extension of a well-known result due to Gaschütz [G]; the proof given (for example) in [FJ], Lemma 15.30, adapts easily to yield this version:

Lemma 1. *Let $X \subseteq G$ and $N \lhd G$. Suppose that*

$$G = N \langle X, y_1, \ldots, y_n \rangle$$

with $n \geq \mathrm{d}(G)$. Then there exist $a_1, \ldots, a_n \in N$ such that $G = \langle X, a_1 y_1, \ldots, a_n y_n \rangle$.

Lemma 2. *Let $N \lhd G$. Then G has a subgroup L with $NL = G$ and $\alpha(L) \leq \max\{\alpha(G/N), 4\}$.*

Proof. Let S be a Sylow 2-subgroup of N and put $L = \mathrm{N}_G(S)$. Then $NL = G$ by the Frattini argument. If $\alpha(L) \geq 5$ then $\alpha(L) = \max\{\alpha(G/N), \alpha(L \cap N)\}$. The result follows since $L \cap N$ is an extension of a 2-group by a group of odd order. □

3. Generators

Fix $k \geq 5$ such that $k! > 2C(q)$, and let $\mathcal{C}$ denote the class of all groups G with $\alpha(G) \leq k$. Put $m = m(q)$.

Proposition 3. *Let G be a d-generator group. Then $G = \langle X \cup Y \rangle$ where $|X| \leq d$, $|Y| \leq d$, $X \subseteq G_q^{*m}$ and $\langle Y \rangle \in \mathcal{C}$.*

Proof. Let N be a minimal normal subgroup of G. Arguing by induction on the order of G, we may suppose that $G = N \langle X' \cup Y' \rangle$ where $|X'| \leq d$, $|Y'| \leq d$, $X' \subseteq G_q^{*m}$ and $N \langle Y' \rangle / N \in \mathcal{C}$. Applying Lemma 2 to the group $N \langle Y' \rangle$, we obtain a set Y^* with $|Y^*| = |Y'|$ such that $N \langle Y^* \rangle = N \langle Y' \rangle$ and $\langle Y^* \rangle \in \mathcal{C}$. Then $G = N \langle X' \cup Y^* \rangle$. Say $X' = \{x_1, \ldots, x_d\}$ and $Y^* = \{y_1, \ldots, y_d\}$ (allowing repeats if necessary).

Case 1. Suppose that $N \notin \mathcal{C}$. By Lemma 1, there exist $a_1, \ldots, a_d \in N$ such that $G = \langle Y^*, a_1 x_1, \ldots, a_d x_d \rangle$. As $N \notin \mathcal{C}$, N must be a direct product of non-abelian simple groups of order exceeding $C(q)$. It follows by Proposition 2 that $a_i x_i \in G_q^{*m}$ for each i. The result follows with $X = \{a_1 x_1, \ldots, a_d x_d\}$, $Y = Y^*$.

Case 2. Suppose that $N \in \mathcal{C}$. Applying Lemma 1 again we find $a_1, \ldots, a_d \in N$ such that $G = \langle X', a_1 y_1, \ldots, a_d y_d \rangle$. Put $Y = \{a_1 y_1, \ldots, a_d y_d\}$. Then $\langle Y \rangle \leq N \langle Y^* \rangle \in \mathcal{C}$ and the result follows with $X = X'$. □

We can now prove Theorem 2. Let H be a d-generator group. According to Proposition 3,

$$H = \langle X \cup Y \rangle$$

where $|X| \leq d$, $|Y| \leq d$, $X \subseteq H_q^{*m}$ and $\langle Y \rangle \in \mathcal{C}$. We apply Proposition 1 to the group $T = \langle Y \rangle$: this shows that

$$T^q = T_q^{*h}$$

where $h = h(k, d, q)$. Put $\beta = |T : T^q|$; then $\beta \leq \beta(d, q)$, and we have $T^q = \langle Z \rangle$ where $|Z| \leq d\beta$.

Let $\{s_1, s_2, \ldots, s_\beta\}$ be a transversal to the cosets of T^q in T, put

$$P = \langle X \cup Z \rangle ,$$
$$K = \langle P^{s_1}, \ldots, P^{s_\beta} \rangle .$$

Then $K \lhd H = KT$ and $|H : K| \leq |T : T^q| = \beta$. Since $H^q = \langle H_q \rangle \geq K$, it follows that $H^q = K \langle W \rangle$ for some subset W of H_q of size at most $\log_2 \beta$.

Now each element of Z is a product of h qth powers in T and each element of X is a product of m qth powers in H; as H^q is generated by W together with β conjugates of $X \cup Z$, it follows that H^q can be generated by

$$\log_2 \beta + \beta(dm + d\beta h)$$

qth powers in H.

4. Products of powers

In the terminology of [W], Theorem 2 says that the word x^q is *d-restricted* for every d. Given this, Theorem 1 becomes a special case of [W], Theorem 4.7.9. However it seems worthwhile to make this note self-contained modulo the paper [NS], so in this section we sketch the deduction of Theorem 1.

This is an application of the main technical result of [NS]; to state it we need

Definition. Let G be a finite group and K a normal subgroup. Then K is *a ceptable* if

(i) $K = [K, G]$ and

(ii) whenever $Z < N \leq K$ are normal subgroups of G, the factor N/Z is not of the form S or $S \times S$ for a non-abelian simple group S.

The 'Key Theorem' stated in [NS], §2, is

Proposition 4. *Let K be an acceptable normal subgroup of $G = \langle g_1, \ldots, g_\delta \rangle$. Then*

$$K = \Big(\prod_{i=1}^{\delta} [K, g_i] \Big)^{*f_1} \cdot K_q^{*f_2}$$

where f_1 and f_2 depend only on q and δ.

(For a subset X of K we write X^{*f} for the set $\{x_1 x_2 \ldots x_f \mid x_1, \ldots, x_f \in X\}$.)

Let H be a d-generator group and set $G = H^q$. As before, we have $\mathrm{d}(G) \leq d' = d\beta(d,q)$. Now G has a series of characteristic subgroups

$$K_1 \geq K_3 \geq K_4 \geq K_5$$

such that

- K_5 is acceptable in G,
- K_3 is perfect and $K_4/K_5 = \mathrm{Z}(K_3/K_5)$,
- K_3/K_4 is a direct product of non-abelian simple groups of order exceeding $C(q)$,
- K_1/K_3 is soluble,
- $|G : K_1| \leq \gamma = \gamma(d', q)$,

where $\gamma(d', q)$ depends only on d' and q. The proof, which is quite straightforward (given the classification of finite simple groups), appears in [NS], §2 (see Proof of Theorem 1.6).

According to Theorem 2 there exist $g_1, \ldots, g_\delta \in H_q$ such that $G = \langle g_1, \ldots, g_\delta \rangle$ where $\delta = \delta(d,q)$. Then $[h, g_i] \in H_q^{*2}$ for any $h \in H$ and each i, so applying Proposition 4 we deduce that

$$K_5 \subseteq H_q^{*(2\delta f_1 + f_2)}.$$

Proposition 2 shows that $K_3 \subseteq H_q^{*m} \cdot K_5$. Now let $k' \geq \max\{5, q+2\}$ be such that $k'! > 2\gamma(d', q)$. Then $\alpha(H/K_3) \leq k'$; thus Proposition 1 gives

$$H^q \subseteq H_q^{*h} \cdot K_3$$

where $h = h(k', d, q)$. Putting everything together we get $H^q \subseteq H_q^{*f}$ where

$$f = h + m + 2\delta f_1 + f_2,$$

a number that depends only on d and q. This completes the proof of Theorem 1.

Added in proof. The authors have recently improved the main results of [NS], yielding an alternative approach to Theorems 1, 2 and 3. See 'Generators and commutators in finite groups; abstract quotients of compact groups', arXiv:1102.3037v1 [math.GR].

References

[FJ] M. D. Fried and M. Jarden, *Field arithmetic*. Ergeb. Math. Grenzgeb. (3) 11, Springer-Verlag, Berlin 1986. Zbl 0625.12001 MR 0868860

[G] W. Gaschütz, Zu einem von B. H. und H. Neumann gestellten Problem. *Math. Nachr.* **14** (1955), 249–252. Zbl 0071.25202 MR 0083993

[JZ] A. Jaikin-Zapirain, On the verbal width of finitely generated pro-p groups. *Rev. Mat. Iberoamericana* **24** (2008), 617–630. Zbl 1158.20012 MR 2459206

[MZ] C. Martinez and E. Zelmanov, Products of powers in finite simple groups. *Israel J. Math.* **96** (1996), 469–479. Zbl 0890.20013 MR 1433702

[NS] N. Nikolov and D. Segal, On finitely generated profinite groups, I: strong completeness and uniform bounds. *Ann. of Math.* (2) **165** (2007), 171–238. Zbl 1126.20018 MR 2276769

[SW] J. Saxl and J. S. Wilson, A note on powers in simple groups. *Math. Proc. Cambridge Philos. Soc.* **122** (1997), 91–94. Zbl 0890.20014 MR 1443588

[S] D. Segal, Closed subgroups of profinite groups. *Proc. London Math. Soc.* (3) **81** (2000), 29–54. Zbl 1030.20017 MR 1756331

[W] D. Segal, *Words: notes on verbal width in groups*. London Math. Soc. Lecture Note Ser. 361, Cambridge University Press, Cambridge 2009. Zbl 1198.20001 MR 2547644

[Z1] E. I. Zel′manov, Solution of the restricted Burnside problem for groups of odd exponent. *Izv. Akad. Nauk SSSR Ser. Mat.* **54** (1990), 42–59; English transl. *Math. USSR-Izv.* **36** (1991), 41–60. Zbl 0704.20030 MR 1044047

[Z2] E. I. Zel′manov, A solution of the restricted Burnside problem for 2-groups. *Mat. Sb.* **182** (1991), 568–592; English transl. *Math. USSR-Sb.* **72** (1992), 543–565. Zbl 0752.20017 MR 1119009

Received September 21, 2009

N. Nikolov, Department of Mathematics, Imperial College, London SW7 2AZ, UK
E-mail: n.nikolov@imperial.ac.uk

D. Segal, All Souls College, Oxford OX1 4AL, UK
E-mail: dan.segal@all-souls.ox.ac.uk