Counterexamples to a rank analogue of the Shepherd–Leedham-Green–McKay theorem on finite p-groups of maximal class

Khukhro, E. I.

2013

MIMS EPrint: **2013.3**

ISSN 1749-9097

to appear in *Siberian Math. J.* **54**, no. 1

Counterexamples to a rank analogue of the Shepherd–Leedham-Green–McKay theorem on finite p-groups of maximal class

E. I. Khukhro
Sobolev Institute of Mathematics, Novosibirsk
khukhro@yahoo.co.uk

To Victor Danilovich Mazurov on the occasion of his 70th birthday

Abstract

By the Shepherd–Leedham-Green–McKay theorem on finite p-groups of maximal class, if a finite p-group of order p^n has nilpotency class $n-1$, then it has a subgroup of nilpotency class at most 2 with index bounded in terms of p. Counterexamples to a rank analogue of this theorem are constructed, which give a negative solution to Problem 16.103 in Kourovka Notebook. Moreover, it is shown that there are no functions $r(p)$ and $l(p)$ such that any 2-generator finite p-group all of whose factors of the lower central series, starting from the second, are cyclic would necessarily have a normal subgroup of derived length at most $l(p)$ with quotient of rank at most $r(p)$. The required examples of finite p-groups are constructed as quotients of torsion-free nilpotent groups, which are abstract 2-generator subgroups of nilpotent divisible torsion-free groups that are in the Mal'cev correspondence with "truncated" Witt algebras.

1 Introduction

A finite p-group P is said to have maximal class if it has order p^n and maximal possible nilpotency class $n-1$; this obviously means that $|P/\gamma_2(P)| = p^2$ and $|\gamma_i(P)/\gamma_{i+1}(P)| = p$ for all $i \geqslant 2$, where $\gamma_j(P)$ are terms of the lower central series. The theory of p-groups of maximal class was founded by Blackburn [1]. Alperin [2] proved that the derived length of a p-group of maximal class of bounded in terms of p only. A result that is in a sense best-possible was obtained (among other results) independently by Shepherd [3] and Leedham-Green and McKay [4]: a p-group of maximal class has a subgroup of nilpotency class at most 2 (even abelian for $p = 2$) with index bounded in terms of p only. As generalizations of finite p-groups of maximal class there appeared finite p-groups of given co-class, for which similar results were proved (by Donkin, Kiming, Leedham-Green, Mann, McKay, Newman, Plesken, Shalev, Zelmanov, et al.). Natural generalizations in terms of pro-p-groups were considered in parallel, for which certain definitive results were also obtained (mainly by the same authors).

I have posed Problem 16.103 in Kourovka Notebook [5] on the validity of a rank analogue of the Shepherd–Leedham-Green–McKay theorem: suppose that in a finite 2-generated p-group P all factors of the lower central series, starting from the second, are cyclic; must P have a normal subgroup of nilpotency class at most 2 with quotient of rank bounded in terms of p only?

The purpose of this note is a negative answer to this question. Moreover, one cannot even guarantee the existence of a normal subgroup of bounded derived length with quotient of bounded rank.

Theorem. *There are no functions $r(p)$ and $l(p)$ such that any finite 2-generator p-group all of whose factors of the lower central series, starting from the second, are cyclic would necessarily have a normal subgroup of derived length at most $l(p)$ with quotient of rank at most $r(p)$.*

The required examples of finite p-groups are constructed as quotients of torsion-free nilpotent groups, which are abstract 2-generator subgroups of nilpotent divisible torsion-free groups that are in the Mal'cev correspondence with "truncated" Witt algebras.

We point out that "truncated" Witt algebras were also used earlier [6, 7] for constructing examples of p-groups of maximal class with unbounded derived length — of course, for various values of p; therein algebras in characteristic p were used, and the Lazard correspondence, which works only for nilpotency class at most $p-1$. But our examples are "unbounded" for any fixed prime number p, and therefore their construction required an approach via torsion-free nilpotent groups and the Mal'cev correspondence.

It is interesting to compare the situation with related problems on p-automorphisms of finite p-groups with few fixed points. The theory of p-groups of maximal class is virtually equivalent to the theory of finite p-groups G admitting an automorphism φ of order p having exactly p fixed points, $|C_G(\varphi)| = p$. The so-called uncovered case of p-groups of given coclass has a strong relation to finite p-groups G admitting an automorphism φ of order p^n with $|C_G(\varphi)| = p$.

Now suppose that a finite p-group G admits an automorphism φ of order p^n with $|C_G(\varphi)| = p^m$. For $|\varphi| = p$ Alperin [2] proved that the derived length of G is (p, m)-bounded, and I proved in [8] that G has a subgroup of (p, m)-bounded index that has p-bounded nilpotency class (which, as noted by Makarenko [9], can even be bounded by $h(p)$, where $h(p)$ is Higman's function bounding the nilpotency class of a nilpotent group with a fixed-point-free automorphism of order p).

Henceforth we say for short that a certain quantity is, say, $(a, b, \dots)$-bounded if it is bounded above by some function depending only on $a, b, \dots$.

In the general case, Shalev [10] proved that the derived length of G is (p, n, m)-bounded, and I proved in [11] that G has a subgroup of (p, n, m)-bounded index that has derived length at most $2k(p^n)$, where $k(p^n)$ is Kreknin's function bounding the derived length of a Lie algebra with a fixed-point-free automorphism of order p^n. In an alternative direction, for $|\varphi| = p$ Medvedev [12] proved that G has a subgroup of (p, m)-bounded index that has m-bounded nilpotency class, and in the general case Jaikin-Zapirain [13] proved that G has a subgroup of (p, n, m)-bounded index that has m-bounded derived length.

These general results on p-automorphisms of finite p-groups have rather trivial rank analogues in the sense that if a finite p-group G admits an automorphism φ of order p^n with $C_G(\varphi)$ of rank m, then the rank of the whole group G is bounded in terms of p, n, and m. This result is well known in folklore; the proof is based on considering the Jordan normal form of φ as a linear transformation of any φ-invariant elementary abelian section. Since the number of fixed points in such a section is at most p^m, the number of Jordan blocks is at most m. Since the size of each block is at most $p^n \times p^n$, the rank of every such section is at most mp^n. Then one can apply the theory of powerful p-groups, or the fact that the rank of a p-group of automorphisms of an abelian p-group is bounded in terms of the rank of the latter.

Yet the examples in the present paper show that there is no rank analogue of the original Shepherd–Leedham-Green–McKay theorem, which corresponds to the case of $|\varphi| = |C_G(\varphi)| = p$ in terms of automorphisms, not even with a subgroup of p-bounded "co-rank" and p-bounded derived length.

In § 1 we recall the properties of the Mal'cev correspondence between divisible torsion-free nilpotent groups and nilpotent Lie algebras over $\mathbb{Q}$. In § 2 the Mal'cev correspondence is applied to "truncated" Witt algebras, which are nilpotent Lie algebras; these algebras and resulting groups G are considered for various values of the nilpotency class. Then abstract 2-generator subgroups F are chosen in the groups G in such a way that all factors of the lower central series of F, starting from the second, are infinite cyclic. In § 3 it is shown that finite p-groups that are quotients of F provide the required examples.

2 Mal'cev correspondence

In this section we recall the properties of the Mal'cev correspondence.

Let L be a nilpotent Lie algebra L over $\mathbb{Q}$ (for short, $\mathbb{Q}$-algebra). We denote Lie commutators (products) in L by parentheses, in order to distinguish them from group commutators, which will be defined on the same elements. The Baker–Campbell–Hausdorff formula defines the structure of a $\mathbb{Q}$-powered group (that is, a divisible, or radicable, group with unique roots, so that rational powers of elements are well defined). The group can be assumed to have the same underlying set $G = L$, so that the group operation is defined by a fixed formula in terms of the Lie algebra operations of L:

$$xy = x + y + \frac{1}{2}(x, y) + \frac{1}{12}((x, y), y) - \frac{1}{12}((x, y), x) - \frac{1}{24}(((x, y), x), y) + \cdots , \qquad (1)$$

where commutators on the right are Lie commutators in L depending on x and y. A commutator of two elements in G is also given by a fixed formula in terms of Lie algebra operations in L:

$$[x, y] = (x, y) + \cdots , \qquad (2)$$

where dots on the right-hand side denote a linear combination of Lie commutators in x and y of weight at least three.

The Lie operations in L can be reconstructed from the $\mathbb{Q}$-powered group operations in G by the inversions of the Baker–Campbell–Hausdorff formulae (1), (2). This correspondence between G and L is known as the *Mal'cev correspondence*. It is well known that this is an equivalence of categories of nilpotent Lie $\mathbb{Q}$-algebras and nilpotent $\mathbb{Q}$-powered groups.

In particular, the group G has the same nilpotency class as L; the terms the lower central series of G are $\mathbb{Q}$-powered subgroups and coincide as sets with the corresponding terms of the lower central series of the Lie algebra L. For any $\alpha \in \mathbb{Q}$ the αth power of $g \in G$ is equal to αg in L, and we shall freely write $g^\alpha = \alpha g$ for $g \in G = L$ and $\alpha \in \mathbb{Q}$. Note that $1 = 0$, where 1 is the identity elements of G and 0 is the zero element of L. For an abstract subgroup S of G (that is, S is a subgroup of G as an ordinary group) owe denote by $\sqrt{S}$ the set of all roots of elements of S; this is the $\mathbb{Q}$-powered subgroup generated by S; obviously, $\sqrt{S} = \mathbb{Q}S$ with multiplication by scalars in L on the right.

We shall need some technical properties of the Mal'cev correspondence, which are also known in folklore. However, in order to give precise references, it is convenient to cite some lemmas in [14].

Let $\mathscr{L}$ be a free nilpotent Lie $\mathbb{Q}$-algebra of nilpotency class c on free generators $x_1, x_2, \dots$. Then the $\mathbb{Q}$-powered group $\mathscr{G}$ that is in the Mal'cev correspondence with $\mathscr{L}$ as described above is a free nilpotent $\mathbb{Q}$-powered group of nilpotency class c on free generators $x_1, x_2, \dots$.

Lemma 1 ([14, Lemma 1]). *There is a c-bounded positive integer $d = d(c)$ such that any element of any abstract subgroup $\langle g_1, g_2, \dots \rangle$ of $\mathscr{G}$ is equal to a linear combination of Lie commutators in $g_1, g_2, \dots$ with rational coefficients whose denominators divide d.* □

(Henceforth "abstract" means generated as an ordinary group, without taking roots, that is, without fractional powers.)

Let $\mathscr{L}_0$ be the Lie ring ($\mathbb{Z}$-algebra) generated by the elements $x_1, x_2, \dots$ (so its additive group is generated by commutators in $x_1, x_2, \dots$). Let $\mathscr{G}_0$ be the abstract subgroup of $\mathscr{G}$ generated by $x_1, x_2, \dots$. Then $\mathscr{G}_0$ is an (abstract) free nilpotent group of nilpotency class c on free generators $x_1, x_2, \dots$. Lemma 1 is actually equivalent to the inclusion $\mathscr{G}_0 \subseteq d^{-1}\mathscr{L}_0$.

Lemma 2 ([14, Lemma 2]). *There is a c-bounded positive integer $D = D(c)$ such that for any positive integer k the subgroup $\mathscr{G}_0^k$ generated by all kth powers of elements of $\mathscr{G}_0$ is contained in $D^{-1}k\mathscr{L}_0$.* □

Although these lemmas are stated in terms of free nilpotent Lie $\mathbb{Q}$-algebras and $\mathbb{Q}$-powered groups, we shall be able to apply their consequences to other situations where the Mal'cev correspondence is applied.

3 Torsion-free groups

In this section first we construct torsion-free $\mathbb{Q}$-powered groups that are in the Mal'cev correspondence with certain nilpotent Lie $\mathbb{Q}$-algebras. Then we choose abstract 2-generator subgroups which have cyclic factors of the lower central series, starting from the second.

For $n \geqslant 2$, let $L = L(n)$ be a "truncated" Witt algebra over $\mathbb{Q}$ which is a Lie algebra with basis $e_1, \dots, e_n$ and structure constants

$$(e_i, e_j) = \begin{cases} (i-j)e_{i+j} & \text{for } i+j \leqslant n \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

Note that any Lie commutator in the e_i is a multiple of e_s, where s is the sum of indices of all elements involved in the commutator with account for multiplicities. For example, $(e_2, \underbrace{e_1, \dots, e_1}_{k-2}) = (k-2)! e_k$. Henceforth simple (left-normed) commutators are denoted as $(a_1, a_2, a_3, \dots, a_k) = (...((a_1, a_2), a_3), \dots, a_k)$.

Obviously, L is a nilpotent Lie algebra of nilpotency class $n-1$, with terms of the lower central series $\gamma_i(L) = \langle e_{i+1}, \dots, e_n \rangle$ for $i \geqslant 2$. It follows from the structure constants that $L/\gamma_i(L) \cong L(i)$ for every $i = 3, 4, \dots$, with the images of $e_1, \dots, e_i$ playing the role of the basis in the definition of $L(i)$.

Let $G = G(n)$ be the nilpotent group in the Mal'cev correspondence with $L = L(n)$. As described in § 2, we assume that G has the same underlying set $G = L$ with the group operations defined in terms of the Lie algebra operations of L by the Baker–Campbell–Hausdorff formulae (1) and (2) for products and commutators. Note that $G/\gamma_i(G) \cong G(i)$ for every $i = 3, 4, \dots$ in accordance with the above-mentioned property of L.

Lemma 3. *Any (repeated) group commutator in elements* $e_i^{c_i}$, $c_i \in \mathbb{Q}$, *is equal to a linear combination of Lie commutators in the same elements* $e_i^{c_i} = c_i e_i$ *each having at least the same multiplicity of occurrence of each element* $c_j e_j$ *as the original group commutator.*

Proof. This follows directly from the repeated application of the commutator formula (2). □

Every element of L (and therefore of G) is a linear combination of the basis elements e_i. The first term with nonzero coefficient, with the least index, is called the *leading term*: if $g = c_i e_i + c_{i+1} e_{i+1} + \cdots$ with $c_i \neq 0$, then the leading term of g is $c_i e_i$. Writing $g = c_i e_i + \cdots$ we shall always mean that $c_i e_i$ is the leading term of g.

Lemma 4. *If* $g = c_i e_i + \cdots$ *and* $h = d_j e_j + \cdots$ *for* $i \neq j$, *then*

$$[g, h] = \begin{cases} (i-j) c_i d_j e_{i+j} + \cdots & \text{if } i + j \leqslant n, \text{ and} \\ 1 = 0 & \text{if } i + j > n. \end{cases}$$

Proof. This immediately follows from the structure constants (3) and the commutator formula (2). □

We now consider certain abstract 2-generator subgroups of G.

Proposition 1. *There is an* n*-bounded positive integer* $M(n)$ *such that for any positive integer* M *divisible by* $M(n)$ *the group* $F = F(M)$ *generated as an abstract group by* e_1 *and* e_2^M *has the following properties:*

(a) *the factors* $\gamma_i(F)/\gamma_{i+1}(F)$ *are infinite cyclic for all* $i \geqslant 2$;

(b) $\gamma_i(F) = F \cap \gamma_i(G)$ *for every* $i = 1, 2, \dots$;

(c) $\gamma_i(F)/\gamma_{i+1}(F)$ *is generated by the image of* $[e_2^M, \underbrace{e_1, \dots, e_1}_{i-1}]$ *for every* $i \geqslant 2$.

(We shall actually need just one $M(n)$ for each n, but in the proof of the proposition by induction on n it is convenient to have the formally stronger assertion with divisibility.)

Proof. By Lemma 4 and structure constants formulae (3),

$$[e_2^M, \underbrace{e_1, \ldots, e_1}_{i-1}] = (Me_2, \underbrace{e_1, \ldots, e_1}_{i-1}) + \cdots = M(i-1)! e_{i+1} + \cdots,$$

so that clearly the $\mathbb{Q}$-linear span of these elements together with e_1 and $e_2^M = Me_2$ coincides with L. In other words, $\sqrt{F} = G$ is the Mal'cev completion of F. Hence, $\sqrt{\gamma_i(F)} = \gamma_i(G)$. Therefore, $\sqrt{\gamma_i(F)}/\sqrt{\gamma_{i+1}(F)} \cong \mathbb{Q}$ for $i \geqslant 2$. Since the $\gamma_i(F)$ are finitely generated, part (a) will follow if we show that $\gamma_i(F)/\gamma_{i+1}(F)$ is torsion-free for $i \geqslant 2$. Since $G/\gamma_{i+1}(G)$ are torsion-free, it suffices to prove part (b), that is, $\gamma_i(F) = F \cap \gamma_i(G)$ for all $i = 1, 2, \ldots$. We proceed by induction simultaneously proving part (c) and constructing the required positive integer $M(n)$ in the process. The key lemma deals with $\gamma_{n-1}(F)$.

Lemma 5. *There is an n-bounded positive integer $N(n)$ such that for any N divisible by $N(n)$ the group F generated as an abstract group by e_1 and e_2^N has torsion-free quotient $F/\gamma_{n-1}(F)$ and, moreover, $\gamma_{n-1}(F) = F \cap \gamma_{n-1}(G) = \langle [e_2^N, \underbrace{e_1, \ldots, e_1}_{n-2}] \rangle$.*

Proof. Since $G/\gamma_{n-1}(G)$ is torsion-free, we only need to prove the second assertion. From the structure constants (3) and Lemma 3 it is clear that

$$\gamma_{n-1}(F) = \langle [e_2^N, \underbrace{e_1, \ldots, e_1}_{n-2}] \rangle = \langle (n-2)! N e_n \rangle$$

(where angle brackets denote subgroups generated as abstract groups). Since $\sqrt{\gamma_{n-1}(F)} = \gamma_{n-1}(G) = \mathbb{Q}\langle e_n \rangle$, it is also clear that we simply need to find $N(n)$ such that for any N divisible by $N(n)$ the following holds: for any element $\alpha e_n \in F$ the coefficient α is an integer divisible by $(n-2)!N$.

By the usual collecting process arguments, such an element $\alpha e_n \in F$ is a product of (integer) powers of (basic) commutators in the generators e_1 and e_2^N in some order compatible with the increase of the weight:

$$\alpha e_n = e_1^{k_1} (e_2^N)^{k_2} [e_2^N, e_1]^{k_3} [e_2^N, e_1, e_1]^{k_4} [e_2^N, e_1, e_2^N]^{k_5} \cdots [e_2^N, e_1, \ldots, e_1]^{k_z}, \tag{4}$$

where $k_i \in \mathbb{Z}$.

We transform the right-hand side into a linear combination of Lie commutators in e_1 and $e_2^N = Ne_2$. First we expand the (repeated) group commutators by repeatedly using the commutator formula (2), and then we apply the product formula (1). As a result, the right-hand side of (4) becomes a linear combination of Lie commutators in $e_2^N = Ne_2$ and e_1,

$$\alpha e_n = k_1 e_1 + k_2 N e_2 + \sum_{i=1}^{n-2} \lambda_i (Ne_2, \underbrace{e_1, \ldots, e_1}_{i}) + \sum_i \mu_i \varkappa_i, \tag{5}$$

where, apart from the "linear part" $k_1 e_1 + k_2 e_2$, we also distinguished the commutators $(Ne_2, \underbrace{e_1, \ldots, e_1}_{i})$ with exactly one occurrence of Ne_2, while the $\varkappa_i$ are other Lie commutators in Ne_2 and e_1 containing at least two occurrences of Ne_2. It does not matter for us whether the coefficients of the $\varkappa_i$ are collected or not, as long as this expansion arose from applying the commutator and product formulae to the right-hand side of (4), — as we shall see soon enough the $\varkappa_i$ can be easily dealt with.

Note that for the moment we keep the coefficient N of e_2 "inside" the Lie commutators, regarding both group commutators in (4) and Lie commutators in (5) as commutators in these two elements $e_2^N = Ne_2$ and e_1.

Of course, each Lie commutator in (5) is equal to a multiple of one of the basis elements e_i by the structure constants (3), where the index i is equal to the sum of indices of all the entries of the commutator. For example, $(Ne_2, e_1, e_1, e_1, Ne_2) = 18N^2 e_7$. After collecting terms in the resulting linear combination of $e_1, \dots, e_n$, we must of course have all coefficients of e_i become zero for $i < n$, and the coefficient of e_n become equal to α. Therefore all terms in (5) with sums of indices less than n must cancel out.

We observe straight away that when the structure constants formulae (3) are applied to the right-hand side of (5), the only contribution to the coefficients of e_1 and e_2 is $k_1 e_1 + k_2 N e_2$. Since $n \geqslant 3$ in our construction, we must have $k_1 = 0$ and $k_2 = 0$.

Our task is to show that after application of the structure constant formulae and collecting all terms — which must result in a multiple of e_n — the resulting coefficient α of e_n is an integer divisible by $(n-2)!N$, as long as N is divisible by a certain positive integer $N(n)$, which we shall determine in the course of the proof. We shall do this step by step, by analysing separately the coefficients λ_i and μ_i, with λ_i being the difficult part, and the μ_i being easier to handle.

We should bear in mind that the coefficients of the Lie commutators in (5) are, generally speaking, rational numbers rather than integers. However, the denominators of these coefficients are bounded. This fact is not quite obvious, since the product and commutator formulae (1), (2) are applied repeatedly; we derive it here from Lemma 1, which was stated for free nilpotent Lie $\mathbb{Q}$-algebra and $\mathbb{Q}$-powered group.

Lemma 6. *There is an n-bounded positive integer $d = d(n)$ such that any element of any abstract subgroup $\langle g_1, g_2, \dots \rangle$ of G is equal to a linear combination of Lie commutators in $g_1, g_2, \dots$ with rational coefficients whose denominators divide d.*

Proof. We apply Lemma 1 to the abstract subgroup $\mathscr{G}_0$ of $\mathscr{G}$ generated by $x_1, x_2, \dots$ with $c = n-1$. This subgroup is an abstract free nilpotent group of class $n-1$. The same number $d = d(n)$ given by that lemma has the required property, in view of the homomorphism of $\mathscr{L}$ into L extending the mapping $x_i \to g_i$, which is also a homomorphism of $\mathscr{G}$ into G. □

Let $\varkappa = \varkappa_i$ be one of the Lie commutators in Ne_2 and e_1 in (5) with at least two occurrences of Ne_2. By Lemma 6, the coefficient $\mu = \mu_i$ of $\varkappa$ is equal to a/d for some $a \in \mathbb{Z}$. Indeed, this term $\mu\varkappa$ appeared in the expansion of the right-hand side of (4), an element of the abstract group generated by Ne_2 and e_1.

Using the linearity of $\varkappa$ and two occurrences of Ne_2 in it, we see that

$$\mu\varkappa = \frac{bN^2}{d} e_s \quad \text{for some } b \in \mathbb{Z}, \tag{6}$$

where s is the sum of indices of the entries of $\varkappa$, because the structure constants are integers. In particular, if N is divisible by $(n-2)!d$, then after application of structure constant formulae all contributions of the $\varkappa_i$ to the coefficient of e_n will be integers divisible by $(n-2)!N$, which is what we need.

It remains to consider the coefficient λ_{n-2} of the Lie commutator $(Ne_2, \underbrace{e_1, \dots, e_1}_{n-2})$, to which contributions are made not only by the power of the same group commutator $[e_2^N, \underbrace{e_1, \dots, e_1}_{n-2}]$ in (4) (which, of course, causes no problems as it contributes $(n-2)!Nk_z e_n$), but also by the "tails" of other powers of group commutators. Here, by the *tail* of a power of a group commutator of some weight we mean the linear combination of Lie commutators of greater weight appearing in the expansion by repeated application of the commutator formula (2). We approach λ_{n-2} by induction analysing the properties of all λ_i in (5).

Changing notation, let s_m be the integer exponent of $[e_2^N, \underbrace{e_1, \dots, e_1}_{m}]$ in (4), so that $[e_2^N, \underbrace{e_1, \dots, e_1}_{m}]^{s_m}$ is the corresponding factor in (4).

Lemma 7. *The coefficient λ_m of the commutator $(Ne_2, \underbrace{e_1, \dots, e_1}_{m})$ in* (5) *is equal to the sum of s_m and the coefficients of this commutator in the tails of $[e_2^N, \underbrace{e_1, \dots, e_1}_{i}]^{s_i}$ for $i < m$.*

Proof. When the commutator formula (2) is (repeatedly) applied to every factor in (4), by Lemma 3 it is only commutators $[e_2^N, \underbrace{e_1, \dots, e_1}_{j}]^{s_i}$ for $i \leqslant m$ that have $(Ne_2, \underbrace{e_1, \dots, e_1}_{m})$ in their decompositions. By the same lemma, the corresponding term in the decomposition of $[e_2^N, \underbrace{e_1, \dots, e_1}_{m}]^{s_m}$ is $s_m(Ne_2, \underbrace{e_1, \dots, e_1}_{m})$.

Since $k_1 = k_2 = 0$, we are dealing only with commutators in x_1 and $Ne_2 = e_2^N$, which all involve e_2, so that any commutator in such commutators involves at least two occurrences of Ne_2. Therefore subsequent application of the product formula (1) obviously only sums up contributions to the coefficient of $(Ne_2, \underbrace{e_1, \dots, e_1}_{m})$. $\square$

We claim that these exponents s_m must be "almost divisible" by N, since only then the cancellations will be possible that are necessary for the coefficients of e_{m+2} for $m+2 < n$ to become zero after application of the structure constants formulae.

Lemma 8. *For $m+2 < n$ the exponent s_m can be written in the form*

$$s_m = \frac{u_m N}{m! d^{m-3}} \qquad \textit{for some } u_m \in \mathbb{Z},$$

where d is the positive integer in Lemma 6.

(Of course, the s_m are integers, but we need the factor N to appear in the numerator of a fraction with denominator bounded in terms of n.)

Proof. Since $k_1 = k_2 = 0$, the only contribution to the coefficient of e_3 when the structure constants formulae (3) are applied to (5) comes from the leading term of the factor

$[e_2^N, e_1]^{k_3}$ in (4), and this contribution is Nk_3e_3. Henceforth we apply repeatedly Lemmas 3 and 4 without special references. Hence, $s_1 = k_3 = 0$, too (unless $n \leqslant 3$, when there is nothing to prove about s_1).

Next, it follows that the only contribution to the coefficient of e_4 after the structure constants formulae are applied to the right-hand side of (5) comes from the leading term of the factor $[e_2^N, e_1, e_1]^{k_4}$ in (4), and this contribution is $2Nk_4e_4$. By Lemma 7 we also have a contribution from the tail of $[e_2^N, e_1]^{s_1}$, but we already know that $s_1 = 0$. Hence, $s_2 = k_4 = 0$ (unless $n \leqslant 4$, when there is nothing to prove about s_2).

The situation becomes different starting from the coefficient of e_5. After the structure constants formulae are applied to the right-hand side of (5), the coefficient of e_5 is equal to the sum of $3!s_3N$, which is the contribution of the summand $s_3(Ne_2, e_1, e_1, e_1)$, the leading term of the factor $[e_2^N, e_1, e_1, e_1]^{s_3}$ in (4), and the only other contribution of $k_5(Ne_2, e_1, Ne_2) = k_5N^2(e_2, e_1, e_2) = k_5N^2e_5$ arising as the leading term of $[e_2^N, e_1, e_2^N]^{k_5}$ in (4). (By Lemma 7 we would also need to consider the tails of $[e_2^N, e_1]^{s_1}$ and $[e_2^N, e_1, e_1]^{s_2}$, but we already know that $s_1 = s_2 = 0$.) Thus, assuming that $n > 5$, we must have $3!s_3N + k_5N^2 = 0$, whence

$$s_3 = \frac{-k_5N}{3!} = \frac{u_3N}{3!d^{3-3}} \tag{7}$$

with $u_3 = -k_5 \in \mathbb{Z}$, as required.

We make one more step before proving the step of induction on m. After the structure constants formulae are applied to the right-hand side of (5), the coefficient of e_6 is the sum of $\lambda_4 4!N$ and the coefficients resulting from some Lie commutators with at least two occurrences of Ne_2. The latter together contribute b_4N^2/d for $b_4 \in \mathbb{Z}$ by (6). By Lemma 7, we have $\lambda_4 = s_4 + c_{43}s_3$, where $c_{43}(Ne_2, e_1, e_1, e_1, e_1)$ is a summand in the tail of $[e_2^N, e_1, e_1, e_1]$ (while s_3 is the exponent of the factor $[e_2^N, e_1, e_1, e_1]^{s_3}$ in (4)). By Lemma 6 we have $c_{43} = t_{43}/d$ for $t_{43} \in \mathbb{Z}$. Assuming that $n > 6$ we must have the coefficient of e_6 be zero. Therefore, using the previous formula (7), we obtain

$$(s_4 + c_{43}s_3)4!N + \frac{b_4N^2}{d} = \Big(s_4 + \frac{t_{43}u_3N}{3!d}\Big)4!N + \frac{b_4N^2}{d} = 0,$$

whence

$$s_4 = -\frac{b_4N}{4!d} - \frac{t_{43}u_3N}{3!d} = \frac{u_4N}{4!d}$$

for $u_4 \in \mathbb{Z}$, as required.

We now prove the step of induction on m. After the structure constants formulae are applied to the right-hand side of (5), the coefficient of e_{m+2} is the sum of $\lambda_m m!N$ and the coefficients resulting from some Lie commutators with at least two occurrences of Ne_2. The latter together contribute b_mN^2/d for $b_m \in \mathbb{Z}$ by (6).

By Lemma 7,

$$\lambda_m = s_m + \sum_{i=1}^{m-1} c_{mi}s_i,$$

where $c_{mi}(Ne_2, \underbrace{e_1, \dots, e_1}_{m})$ is a summand in the tail of the commutator $[e_2^N, \underbrace{e_1, \dots, e_1}_{i}]$ (while s_i is the exponent of the factor $[e_2^N, \underbrace{e_1, \dots, e_1}_{i}]^{s_i}$ in (4)). By Lemma 6, we have

$c_{mi} = t_{mi}/d$ for $t_{mi} \in \mathbb{Z}$, and by the induction hypothesis, $s_i = u_i N/i!d^{i-3}$ for $u_i \in \mathbb{Z}$. Since the coefficient of e_{m+2} on the left of (5) is zero (unless $m+2 = n$, when there is nothing to prove), we must have

$$\Big(s_m + \sum_{i=1}^{m-1} c_{mi} s_i\Big) m!N + \frac{b_m N^2}{d} = \Big(s_m + \sum_{i=1}^{m-1} \frac{t_{mi} u_i N}{i!d^{i-2}}\Big) m!N + \frac{b_m N^2}{d} = 0,$$

whence

$$s_m = -\frac{b_m N}{m!d} - \sum_{i=1}^{m-1} \frac{t_{mi} u_i N}{i!d^{i-2}} = \frac{u_m N}{m!d^{m-3}}$$

for $u_m \in \mathbb{Z}$, as required. $\square$

We now finish the proof of Lemma 5. We already saw that if N is divisible by $(n-2)!d$, then $(n-2)!N$ divides the contribution to the coefficient of e_n given by the terms $\mu_j \varkappa_j$ in (5), where Lie commutators $\varkappa_i$ in Ne_2 and e_1 have at least two occurrences of Ne_2.

It remains to consider λ_{n-2}. By Lemma 7,

$$\lambda_{n-2} = s_{n-2} + \sum_{i=1}^{n-3} c_i s_i,$$

where $c_i(Ne_2, \underbrace{e_1, \dots, e_1}_{m})$ is a summand in the tail of the commutator $[e_2^N, \underbrace{e_1, \dots, e_1}_{i}]$ (while s_i is the exponent of the factor $[e_2^N, \underbrace{e_1, \dots, e_1}_{i}]^{s_i}$ in (4)). By Lemma 6 we have $c_i = t_i/d$ for $t_i \in \mathbb{Z}$, and by Lemma 8 we have $s_i = u_i N/i!d^{i-3}$ for $u_i \in \mathbb{Z}$. Therefore,

$$\begin{aligned} \lambda_{n-2}(Ne_2, \underbrace{e_1, \dots, e_1}_{n-2}) &= \Big(s_{n-2} + \sum_{i=1}^{n-3} c_i s_i\Big)(n-2)!Ne_n \\ &= \Big(s_{n-2} + \sum_{i=1}^{n-3} \frac{t_i u_i N}{i!d^{i-2}}\Big)(n-2)!Ne_n \\ &= \Big(s_{n-2}(n-2)!N + \frac{uN}{(n-3)!d^{n-5}}(n-2)!N\Big) e_n, \end{aligned}$$

where $u \in \mathbb{Z}$. Hence this contribution to the coefficient of e_n will be divisible by $(n-2)!N$ if N is divisible by $(n-3)!d^{n-5}$. Thus, as long as N is divisible by $(n-3)!d^{n-5}$ and by $(n-2)!d$, the coefficient α in (5) is divisible by $(n-2)!N$, as required. $\square$

To finish the proof of Proposition 1 we set $M(n)$ to be the product of the numbers $N(3), N(4), \dots, N(n)$ given by Lemma 5. We use induction on n to prove that this number $M(n)$ has the required properties. Let M be any positive integer divisible by $M(n)$.

In the basis of induction for $n = 3$ all three parts follow from Lemma 5.

For $n > 3$ the quotient of the $\mathbb{Q}$-powered group G by $\gamma_{n-1}(G) = \mathbb{Q}e_n$ is isomorphic to $G(n-1)$ and is in the Mal'cev correspondence with $L(n-1) \cong L(n)/\gamma_i(L(n)) = L(n)/\mathbb{Q}e_n$. Let the bar denote images in $G/\gamma_{n-1}(G)$. Since M is also divisible by $M(n-1)$, by induction the abstract group $\bar F = \langle \bar e_1, \bar e_2^M\rangle$ has infinite cyclic factors of the lower central series starting from the second. These factors are isomorphic to the lower central factors $\gamma_i(F)/\gamma_{i+1}(F)$ of F for $i = 1,\dots,n-2$, since $F\cap\gamma_{n-1}(G) = \gamma_{n-1}(F)$ by Lemma 5. Furthermore, $\gamma_{n-1}(F)$ is also infinite cyclic by the same lemma. Thus, part (a) is proved.

Furthermore, by induction $\gamma_i(\bar F) = \bar F\cap\gamma_i(\bar G)$, which is equivalent to

$$\gamma_i(F)\gamma_{n-1}(G) = (F\cap\gamma_i(G))\gamma_{n-1}(G) \tag{8}$$

because $\gamma_i(G)\geqslant\gamma_{n-1}(G)$. Since $F\cap\gamma_{n-1}(G) = \gamma_{n-1}(F)$ by Lemma 5, this implies that $\gamma_i(F) = F\cap\gamma_i(G)$. Indeed, we only need to prove that $\gamma_i(F)\geqslant F\cap\gamma_i(G)$. For any $f\in F\cap\gamma_i(G)$ by (8) there is $z\in\gamma_{n-1}(G)$ and $g\in\gamma_i(F)$ such that $gz = f$, whence $z = g^{-1}f\in F\cap\gamma_{n-1}(G) = \gamma_{n-1}(F)\leqslant\gamma_i(F)$ by Lemma 5, so that $f = gz\in\gamma_i(F)$. This proves (b).

Finally, part (c) follows from part (b) and the induction hypothesis for $\gamma_i(F)/\gamma_{i+1}(F)$ for $2\leqslant i<n-1$, and from Lemma 5 for $\gamma_{n-1}(F)$. □

4 Finite p-groups

In the preceding section we proved that the abstract subgroup $F = \langle e_1, e_2^M\rangle$ of the $\mathbb{Q}$-powered group $G = G(n)$ for any M divisible by a certain n-bounded number $M(n)$ is a 2-generator torsion-free nilpotent group of class $n-1$ with cyclic factors of the lower central series starting from the second. In this section for any given prime number p we consider finite p-groups that are quotients of these groups F (for various n). These quotients form a family of required examples of 2-generator finite p-groups with cyclic factors of the lower central series, stating from the second, that do not have a subgroup of p-bounded derived length with quotient of p-bounded rank.

In what follows, for a given n we choose a positive integer $M = M(n)$ satisfying Proposition 1. It is also easy to make sure that $M(n)$ is divisible by $M(i)$ for all $i\leqslant n$, for example, by setting $M(n) = \prod_{i=3}^n N(i)$ for the $N(i)$ given by Lemma 5. Then $M(n)$ will also satisfy Proposition 1 applied to the quotient $G/\gamma_i(G)$ identified with the group $G(i)$, for any $i\leqslant n$.

As quotients of F that are the required finite p-groups we take the groups $P = P(k) = F/F^{p^k}$ for positive integers k, which will be chosen to be large enough in the proofs. Since F is 2-generator and has cyclic factors of the lower central series, starting from the second, the same properties are enjoyed by the groups P.

We shall be using the Lie algebra L for controlling subgroups and sections of P and of F, which, recall, is the abstract subgroup of the $\mathbb{Q}$-powered group G, which is in the Mal'cev correspondence with the Lie $\mathbb{Q}$-algebra L. For example, a section of P can be viewed as a section Q/R of the abstract group G, and if R is contained as a subset in some subset $S\subseteq L$ and we manage to show in L that $Q\not\subseteq S$, then we can conclude that $Q/R\neq 1$ in P, even if S is not contained in F, say.

It is convenient to introduce also the Lie ring ($\mathbb{Z}$-algebra) L_0 generated by the basis elements $e_1,\dots,e_n$. In particular, since all the structure constants (3) are integers, the additive group of L_0 is a free abelian group of rank n with basis $e_1,\dots,e_n$.

Lemma 9. *There is an n-bounded positive integer $D = D(n)$ such that for any positive integer k the subgroup F^k generated by all kth powers of elements of F is contained in $D^{-1}kL_0$.*

Proof. This fact follows from Lemma 2 for the free nilpotent Lie $\mathbb{Q}$-algebra $\mathscr{L}$ and $\mathbb{Q}$-powered group $\mathscr{G}$ with nilpotency class $c = n - 1$. Recall that $\mathscr{G}_0$ is the abstract free nilpotent group of class $n-1$ on free generators $x_1, x_2, \dots$. Let $D = D(n)$ be the number given by that lemma, so that

$$\mathscr{G}_0^k \subseteq D^{-1}k\mathscr{L}_0 \tag{9}$$

for any positive integer k. The map $x_1 \to e_1$, $x_2 \to e_2^M = Me_2$, $x_i \to 1 = 0$ for $i \geqslant 3$ extends to a homomorphism of $\mathscr{G}_0$ onto F, of $\mathscr{G}$ into G, of $\mathscr{L}_0$ into L_0, and of $\mathscr{L}$ into L, and all these homomorphisms agree on common parts of domains of definition. Applying these homomorphisms to (9) we obtain $F^k \subseteq D^{-1}kL_0$, as required. (In fact, the image of $\mathscr{L}_0$ under that homomorphism is somewhat smaller than L_0, but we use L_0 for simplicity.) □

It is more convenient for us to have a consequence of Lemma 9 in terms of divisibility by a given prime p. Let $\mathbb{Q}_{p'}$ denote the ring of all rational numbers with denominators coprime to p.

Lemma 10. *There is an n-bounded positive integer $\varepsilon = \varepsilon(n)$ such that for any positive integer k the subgroup F^{p^k} generated by all p^kth powers of elements of F is contained in $p^{k-\varepsilon}\mathbb{Q}_{p'}L_0$.* □

To lighten the notation we introduce the elements $g_i = [e_2^M, \underbrace{e_1, \dots, e_1}_{i-2}]$ for $i \geqslant 3$. The leading term of g_i, in terms of L, is $M(e_2, \underbrace{e_1, \dots, e_1}_{i-2}) = (i-2)!Me_i$. By Proposition 1 the image of g_i generates $\gamma_{i-1}(F)/\gamma_i(F)$.

Proposition 2. *Let s be a positive integer such that $s \leqslant n/2$.*

(a) *The section $\gamma_s(F)/\gamma_{2s}(F)$ is a free abelian group of rank s freely generated by the images of $g_{s+1}, \dots, g_{2s}$.*

(b) *There is an s-bounded positive integer $k_0(s)$ such that for any positive integer $k \geqslant k_0(s)$ the section $\gamma_s(P)/\gamma_{2s}(P)$ of $P = F/F^{p^k}$ is an abelian p-group of rank exactly s generated by the images of $g_{s+1}, \dots, g_{2s}$.*

Proof. (a) Since $\gamma_{2s}(F) = F \cap \gamma_{2s}(G)$ by Proposition 1, we can simply assume that $\gamma_{2s}(G) = 1$, which is equivalent to $\gamma_{2s}(L) = 0$, or $n = 2s$. Then the elements $g_{s+1}, \dots, g_{2s}$ clearly commute by Lemma 4. Considering the leading terms of $g_i = (i-2)!Me_i + \cdots$ we see that the $s \times s$ matrix of the coefficients of $g_{s+1}, \dots, g_{2s}$ with respect to the basis $e_{s+1}, \dots, e_{2s}$ is triangular with nonzero elements on the diagonal. Therefore the elements $g_{s+1}, \dots, g_{2s}$ are linearly independent (in L, regarded as a vector space over $\mathbb{Q}$). This in turn of course means that the additive subgroup of L generated by $g_{s+1}, \dots, g_{2s}$ is free abelian on these free generators. It remains to use the fact that for commuting elements the group multiplication in G coincides with the addition in L (see (1)).

(b) Since our section

$$\gamma_s(P)/\gamma_{2s}(P) = \gamma_s(F)F^{p^k}/\gamma_{2s}(F)F^{p^k} \cong \gamma_s(F)/(\gamma_s(F) \cap \gamma_{2s}(F)F^{p^k})$$

is abelian by (a), it is sufficient to prove that its image in $G/\gamma_{2s}(G)$ has the required property. Therefore we can again assume that $\gamma_{2s}(G) = 1$, which is equivalent to $\gamma_{2s}(L) = 0$, or $n = 2s$. Then our section becomes isomorphic to $\gamma_s(F)/(\gamma_s(F) \cap F^{p^k})$, since $\gamma_{2s}(F) = F \cap \gamma_{2s}(G)$ by Proposition 1. We know that $\gamma_s(F) = \langle g_{s+1}\rangle \times \cdots \times \langle g_{2s}\rangle$ is free abelian by part (a). The assertion will be proved if we show that $\gamma_s(F) \cap F^{p^k} \leqslant \gamma_s(F)^p$. As we saw in the proof of part (a), the elements $g_{s+1}, \dots, g_{2s}$ form a basis of the vector subspace $\gamma_s(L)$ of L, which is spanned by $e_{s+1}, \dots, e_{2s}$. In addition, the elements $g_{s+1}, \dots, g_{2s}$ are expressed in terms of $e_{s+1}, \dots, e_{2s}$ by certain formulae depending only on $n = 2s$. Hence there is an s-bounded positive integer $m = m(s)$ such that

$$p^m E \subseteq \mathbb{Q}_{p'}\gamma_s(F)^p, \tag{10}$$

where E is the additive subgroup of L generated by $e_{s+1}, \dots, e_{2s}$.

On the other hand, by Lemma 10 we have $F^{p^k} \subseteq p^{k-\varepsilon}\mathbb{Q}_{p'}L_0$, whence by Proposition 1(b)

$$F^{p^k} \cap \gamma_s(F) = F^{p^k} \cap \gamma_s(G) = F^{p^k} \cap \gamma_s(L) \subseteq p^{k-\varepsilon}\mathbb{Q}_{p'}L_0 \cap \gamma_s(L) = p^{k-\varepsilon}\mathbb{Q}_{p'}E.$$

Combining this with (10) we obtain that if $k - \varepsilon \geqslant m$, that is, $k \geqslant \varepsilon + m$, then

$$F^{p^k} \cap \gamma_s(F) \subseteq p^{k-\varepsilon}\mathbb{Q}_{p'}E \subseteq p^m\mathbb{Q}_{p'}E \subseteq \mathbb{Q}_{p'}\gamma_s(F)^p.$$

Then, in fact, $F^{p^k} \cap \gamma_s(F) \leqslant \gamma_s(F)^p$, as required, since the finite p-group $\gamma_s(F)/\gamma_s(F)^p$ has no nontrivial p'-elements. □

We are now ready to show that the groups P, for varying n and k, provide required examples, by using them in the proof of the main theorem.

Proof of the Theorem. We argue by contradiction: suppose that there are functions $r(p)$ and $l(p)$ such that any finite 2-generator p-group all of whose factors of the lower central series, starting from the second, are cyclic necessarily contains a normal subgroup of derived length at most $l(p)$ with quotient of rank at most $r(p)$.

Suppose that n and $s \leqslant n/2$ are large enough so that $s \geqslant r(p) + 1$. Suppose also that k is large enough in the sense of Proposition 2(b). As we know, the group $P = F/F^{p^k}$ constructed above is a 2-generator finite p-group with cyclic factors of the lower central series starting from the second. By our assumption, the group P has a normal subgroup H such that P/H has rank at most $r(p) < s$. By Proposition 2, the group $\gamma_{s+1}(P)/\gamma_{2s}(P)$ is an abelian p-group of rank s generated by the images $\bar{g}_{s+1}, \dots, \bar{g}_{2s}$ of $g_{s+1}, \dots, g_{2s}$. Therefore the image of H in $P/\gamma_{2s}(P)$ must contain at least one element outside the Frattini subgroup of $\gamma_s(P)/\gamma_{2s}(P)$. This implies that H covers at least one of the cyclic factors $\gamma_t(P)/\gamma_{t+1}(P)$ for $s \leqslant t \leqslant 2s-1$. Indeed, choose minimal t such that $s \leqslant t \leqslant 2s-1$ and

$$\bar{g}_{t+1}^{\alpha_{t+1}}\bar{g}_{t+2}^{\alpha_{t+2}} \cdots \in H\gamma_{2s}(P)/\gamma_{2s}(P) \qquad \text{for } p \nmid \alpha_{t+1}.$$

Then $\bar{g}_{t+1} \in H\gamma_{t+1}(P)/\gamma_{2s}(P)$, and, since $\gamma_t(P)/\gamma_{t+1}(P)$ is generated by the image of g_{t+1} by Proposition 1(c), we obtain $\gamma_t(P) \leqslant H\gamma_{t+1}(P)$. Hence, $\gamma_t(P) \leqslant H$, since H is a normal subgroup of the nilpotent group P. But the derived length of $\gamma_t(P)$ can be made larger than $l(p)$ by appropriate choice of n, t, and k, which will bring us to a contradiction.

We use the standard commutator words that define solubility of given derived length: $\delta_1(x_1, x_2) = [x_1, x_2]$ and by induction

$$\delta_{i+1}(x_1, x_2, \dots, x_{2^{i+1}}) = \big[\delta_i(x_1, \dots, x_{2^i}),\ \delta_i(x_{2^i+1}, \dots, x_{2^{i+1}})\big].$$

By our assumption the subgroup H is soluble of derived length at most $l(p)$, which is equivalent to the equality $\delta_{l(p)}(h_1, \dots, h_{2^{l(p)}}) = 1$ for any $h_i \in H$.

On the other hand, in F the elements g_i have leading terms $(i-2)!Me_i$. By Lemma 4, if n is large enough, then the value of the commutator $\delta_{l(p)}$ on $g_t, g_{t+1}, \dots, g_{t+2^{l(p)}-1}$ will have leading term ζe_w with $e_w \neq 0$, where the index w is the sum of indices $w = \sum_{i=t}^{i=t+2^{l(p)}-1} i$ and the coefficient ζ is equal to the product of the coefficients $(i-2)!M(n)$ multiplied by those differences of indices that appear by the structure constants (3) provided that $n \geqslant w = \sum_{i=t}^{i=t+2^{l(p)}-1} i$, because the indices of leading terms in the subcommutators arising in the inductive calculation of $\delta_{l(p)}(g_t, g_{t+1}, \dots, g_{t+2^{l(p)}-1})$ are all different. Clearly, the coefficient $\zeta = \zeta(n, t, l(p))$ is a positive integer bounded in terms of n, t, and $l(p)$.

If, in addition to the condition $k \geqslant k_0(s)$ in Proposition 2(b), the number k is also large enough so that $p^{k-\varepsilon}$ does not divide the coefficient ζ, then the image of $\delta_{l(p)}(g_t, g_{t+1}, \dots, g_{t+2^{l(p)}-1}) = \zeta e_w + \cdots$ is nontrivial in $P = F/F^{p^k}$, since $F^{p^k} \subseteq p^{k-\varepsilon}\mathbb{Q}_{p'}L_0$ by Lemma 10.

As a result, we arrive at a contradiction, provided

- $n/2 \geqslant s > r(p)$,
- $n \geqslant \sum_{i=2s}^{i=2s+2^{l(p)}-1} i \geqslant \sum_{i=t}^{i=t+2^{l(p)}-1} i$ for any $t \leqslant 2s$, and
- k is large enough in the sense of Proposition 2(b), that is, $k \geqslant k_0(s)$, and $p^{k-\varepsilon(n)}$ does not divide the coefficient $\zeta(n, t, l(p))$.

Clearly, these conditions can be satisfied simultaneously: first choose $s = r(p) + 1$, then $n \geqslant \sum_{i=2s}^{i=2s+2^{l(p)}-1} i$ (which also implies $n \geqslant 2s$), and then large enough k. □

References

[1] N. Blackburn, On a special class of p-groups, *Acta Math.* **100** (1958) 45–92.

[2] J. L. Alperin, Automorphisms of solvable groups, *Proc. Amer. Math. Soc.* **13** (1962), 175–180.

[3] R. Shepherd, p-Groups of maximal class, *Ph. D. Thesis*, Univ. of Chicago, 1971.

[4] C. R. Leedham-Green and S. McKay, On p-groups of maximal class. I, *Quart. J. Math. Oxford Ser.* (2) **27** (1976), 297–311.

[5] *Unsolved Problems in Group Theory. The Kourovka Notebook*, no. 16, Institute of Mathematics, Novosibirsk, 2006.

[6] B. A. Panfërov, Nilpotent groups with lower central factors of minimal ranks, *Algebra Logika* **19** (1980), 701–706; English transl., *Algebra Logic* **19** (1980), 455–458.

[7] L. G. Kovács and C. R. Leedham-Green, Some normally monomial p-groups of maximal class and large derived length, *Quart. J. Math.* (2) **37** (1986), 49–54.

[8] E. I. Khukhro, Finite p-groups admitting an automorphism of order p with a small number of fixed points, *Mat. Zametki* **38** (1985), 652–657; English transl., *Math. Notes.* **38** (1986), 867–870.

[9] N. Yu. Makarenko, On almost regular automorphisms of prime order, *Sibirsk. Matem. Zh.* **33**, no. 5 (1992), 206–208; English transl., *Siberian. Math. J.* **33** (1992), 932–934.

[10] A. Shalev, On almost fixed point free automorphisms, *J. Algebra* **157** (1993), 271–282.

[11] E. I. Khukhro, Finite p-groups admitting p-automorphisms with few fixed points, *Mat. Sb.* **184**, no. 12 (1993), 53–64; English transl., *Russ. Acad. Sci.*, *Sb.*, *Math.* **80** (1995), 435–444.

[12] Yu. Medvedev, p-Divided Lie rings and p-groups, *J. London Math. Soc.* (2) **59** (1999), 787–798.

[13] A. Jaikin-Zapirain, On almost regular automorphisms of finite p-groups, *Adv. Math.* **153** (2000), 391–402.

[14] A. Jaikin-Zapirain and E. I. Khukhro, A connection between nilpotent groups and Lie rings, *Sibirsk. Mat. Zh.* **41** (2000), 1203–1218; English transl., *Siberian Math. J.* **41** (2000), 994–1004.