ON p-GROUPS WITH A MAXIMAL ELEMENTARY ABELIAN NORMAL SUBGROUP OF RANK k

ZOLTÁN HALASI, KÁROLY PODOSKI, LÁSZLÓ PYBER, AND ENDRE SZABÓ

Abstract. There are several results in the literature concerning p-groups G with a maximal elementary abelian normal subgroup of rank k due to Thompson, Mann and others. Following an idea of Sambale we obtain bounds for the number of generators etc. of a 2-group G in terms of k, which were previously known only for $p > 2$. We also prove a theorem that is new even for odd primes. Namely, we show that if G has a maximal elementary abelian normal subgroup of rank k, then for any abelian subgroup A the Frattini subgroup $\Phi(A)$ can be generated by $2k$ elements ($3k$ when $p = 2$). The proof of this rests upon the following result of independent interest: If V is an n-dimensional vector space, then any commutative subalgebra of $\mathrm{End}(V)$ contains a zero algebra of codimension at most n.

1. Introduction

For a finite p-group G we denote by $d(G)$ the size of (any) minimal set of generators for G. Then the p-rank of G (denoted by $r(G)$), the normal p-rank of G (denoted by $nr(G)$) and the sectional p-rank of G (denoted by $sr(G)$) are defined as

$$r(G) = \max\{d(A) \,|\, A \leq G,\ A \text{ is abelian}\},$$
$$nr(G) = \max\{d(A) \,|\, A \lhd G,\ A \text{ is an abelian}\},$$
$$sr(G) = \max\{d(H/K) \,|\, K \lhd H \leq G,\ H/K \text{ is abelian}\}.$$

Note that $sr(G)$ equals the maximum of the generator numbers of all the subgroups of G.

These parameters were much investigated in the past. The results of Blackburn and MacWilliams (see [4], [5], [21]) concerning p-groups of very low rank played an important role in the proof of the Classification Theorem of Finite Simple Groups (see also Janko [18]). A natural question that arises is that knowing $r(G)$ or $nr(G)$ what can be said about $sr(G)$. By a classical result of Thompson if p is odd and $nr(G)$ is at most k then any subgroup of G can be generated by at most $\frac{k(k+1)}{2}$ elements. Thompson's result has been later improved by MacWilliams and an analogous bound has been obtained by Mann for $p = 2$.

In fact, the following, much stronger results were proved.

Theorem 1.1. *Let G be a finite p-group and let E be a maximal elementary abelian normal subgroup of G. If $d(E) = k$, then*

Date: September 21, 2023.

This work on the project leading to this application has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 741420). The first and the third authors were partly supported by the National Research, Development and Innovation Office (NKFIH) Grant No. K138596.

(1) $sr(G) \leq \frac{k(k+1)}{2}$ *for* p *odd (Thompson* [16, III, 12.3 Satz]*);*
(2) $sr(G) \leq \frac{k(k+4)}{4}$ *for* p *odd (MacWilliams* [20, Theorem B]*);*
(3) $sr(G) \leq k^2 + \frac{k(k+1)}{2}$ *for* $p = 2$ *(Mann* [22, Theorem B]*).*

Remark 1.2. The above cited theorems are formed with the stronger assumption "each normal abelian subgroups of G can be generated by k elements" (i.e. that $nr(G) \leq k$), but it can be easily checked that the proofs of [16, III, 12.3 Satz]), [20, Theorem B] and of [22, Theorem B] only use the existence of an $A \leq G$ which is maximal among the normal abelian subgroups of exponent p or 4 such that $d(A) \leq k$.

In particular, under the hypothesis of this theorem, every abelian subgroup $A \leq G$ is the product of at most $O(k^2)$ many cyclic groups. Note that apart from the implied constant multiple this is the best possible bound for $d(A)$ as the following example shows.

Example 1.3. Let V be a $k = 2m$ dimensional vector space over $\mathbb{F}_p$ and let $V_1 \leq V$ be an m-dimensional subspace of V. Let us define

$$H = \{\varphi \in GL(V) \,|\, \varphi_{V_1} = \mathrm{id}_{V_1},\ \varphi_{V/V_1} = \mathrm{id}_{V/V_1}\} \quad \text{and} \quad G = V \rtimes H,$$

with the natural action of H on V. Then both V and $V_1 \times H$ are maximal normal abelian subgroups of G with $d(V) = k$ and $d(V_1 \times H) = \frac{k^2}{4} + \frac{k}{2}$.

The significant part of MacWilliams' improvement was to show that if p is an odd prime and P is any p-subgroup of $GL(n,p)$, then $d(P) \leq \frac{n^2}{4}$ holds, see [20, Theorem A]. (Note that Thompson's argument only uses the trivial bound $d(P) \leq \frac{n(n-1)}{2}$.)

By a modification of her proof, the same result can be achieved for $p = 2$, as well.

Theorem 1.4. *Let G be any 2-subgroup of $GL(n,2)$. Then G can be generated by at most $\frac{n^2}{4}$ elements.*

This result allow us to give a nearly optimal bound for the maximum of the generating numbers of all subgroups of $GL(n,p)$. On the one hand, results of Lucchini [19, Theorem 1] and Guralnick [14, Theorem A] say that if G is a finite group and for every prime $r \mid |G|$ the Sylow r-subgroups of G can be generated by d elements then G can be generated by $d+1$ elements. On the other hand, it was proved by Isaacs [17, Theorem A] that if $r \geq 3$ is a prime different from the characteristic of a field K, then any finite r-subgroup of $GL(n,K)$ can be generated by n elements. Combining these results with Theorem 1.4, we obtain the following.

Theorem 1.5. *Every subgroup of $GL(n,2)$ can be generated by at most $\frac{n^2}{4} + 1$ elements.*

For p odd, the same result for $GL(n,p)$ already appears in [26, p. 199].

In [3, Remark 2.7], Babai and Goodman claim that if $|G| = p^n$ and H is any p-subgroup of $\mathrm{Aut}(G)$, then $d(H) \leq \frac{1}{3}n^2$ follows from the result of MacWilliams for $p > 2$ and remark that they do not know whether such an estimate also holds for $p = 2$. As another consequence of Theorem 1.4 we show that it does indeed hold. In fact, almost the same estimate can be verified for any subgroup of $\mathrm{Aut}(G)$.

Corollary 1.6. *If G is any p-group of order p^n, then $sr(\mathrm{Aut}(G)) \leq \frac{1}{3}n^2 + 1$. Furthermore, every p-subgroup of $\mathrm{Aut}(G)$ can be generated by at most $\frac{1}{3}n^2$ elements.*

Proof. Let H be any subgroup of $\mathrm{Aut}(G)$. The action of H on G induces and action of H on the $\mathbb{F}_p$-vector space $G/\Phi(G)$. Let $\tau : H \to \mathrm{Aut}(G/\Phi(G))$ be the associated homomorphism and $K = \ker(\tau) \lhd H$. Let k be the dimension of $G/\Phi(G)$. Then $\tau(H)$ embeds into $GL(k,p)$ so $d(H/K) = d(\tau(H)) \leq \frac{1}{4}k^2 + 1$ by [26, p. 199] and by Theorem 1.5.

On the other hand, by a result of Hall ([15, Section 1.3, p. 37-38.], [28, Chapter 2, Theorem 1.17]), K is a p-group of order at most $p^{(n-k)k}$, so we have $d(K) \leq k(n-k)$. Thus,

$$\text{(Eq. 1)}\quad d(H) \leq d(H/K) + d(K) \leq k^2/4 + 1 + k(n-k) = nk - \frac{3}{4}k^2 + 1 \leq \frac{1}{3}n^2 + 1.$$

Therefore, $sr(\mathrm{Aut}(G)) \leq \frac{1}{3}n^2 + 1$, as claimed.

If H is a p-subgroup of $\mathrm{Aut}(G)$, then we can use [20, Theorem A] and Theorem 1.4 to bound $d(H/K)$ in Eq. 1 by $k^2/4$. □

Using Theorem 1.4 for $p = 2$ and other results of this paper, we improve Theorem 1.1(3) as follows.

Theorem 1.7. *Let G be a finite 2-group and let E be a maximal elementary abelian normal subgroup of G. If $d(E) = k$, and H is any subgroup of G, then $d(H) \leq 2k + \frac{1}{4}k^2$.*

Note that by Example 1.3 this bound is almost optimal.

By an old result of Mann and Su [24], if M is a compact manifold, then any elementary abelian p-group acting faithfully on M by homeomorphisms has rank at most $f(M)$, where $f(M)$ depends only on M (and does not depend on the prime p). In the work of the third and fourth authors with Csikós [8] the following consequence of the above results is used.

Corollary 1.8. *If every elementary abelian subgroup of a finite group G has rank at most k, then each subgroup H of G can be generated by at most $\frac{1}{4}k^2 + 2k + 1$ elements.*

This result is the starting point for obtaining a structural description of finite groups acting on compact manifolds.

Note that Ol'shanskii [25] has given a probabilistic construction of p-groups G of nilpotency class 2 with $r(G) = k$ and $d(G) \geq (k^2 - 9)/8$. In section 3 we will use his method to show the following:

Theorem 1.9. *For any prime number p and positive integers r, n, k with $k(k-1) > 2n$ there is a p-group G and $G' \leq N \leq Z(G)$ such that $G/N \simeq C_{p^r}^n$ and G does not contain a subgroup isomorphic to $C_{p^r}^{2k}$.*

For the remainder, for any natural number t, we use the notation

$$\Omega_t(G) = \langle x \in G \,|\, x^{p^t} = 1\rangle \text{ and } \mho_t(G) = \langle x^{p^t} \,|\, x \in G\rangle.$$

Note that if G is abelian, then

$$\Omega_t(G) = \{x \in G \,|\, x^{p^t} = 1\} \text{ and } \mho_t(G) = \{x^{p^t} \,|\, x \in G\}.$$

Furthermore, in this case $G/\Omega_t(G) \simeq \mho_t(G)$, and $\mho_t(G)$ equals the t-th term of the Frattini series of G.

We improve another related result of Mann [23, Theorem 3] as follows

Theorem 1.10. *Let G be a 2-group and let E be a maximal normal elementary abelian subgroup of G. If $d(E) = k$, then $|G : \mho_1(G)| \leq 2^{\frac{k(k+5)}{2}}$.*

Knowing $d(E)$ for a maximal normal elementary abelian subgroup $E \lhd G$ not only gives restrictions on $d(H)$ for subgroups H of G, but on the structure of subgroups of G more deeply. A particularly interesting question could be that what can be said about the cyclic decomposition of an abelian subgroup A of G if such an information is known. In this paper we prove that under the same assumption as of Theorem 1.1, the number of factors in the cyclic decomposition of A which are larger than C_p is more restricted.

Theorem 1.11. *Let G be a finite p-group and let E be a maximal normal elementary abelian subgroup of G. If $d(E) = k$, and A is any abelian subgroup of G, then*

(1) $d(\Phi(A)) \leq 2k$ *for* $p > 2$,
(2) $d(\Phi(A)) \leq 3k$ *for* $p = 2$.

It seems quite possible that if the stronger condition $nr(G) \leq k$ holds, then the number of generators of any abelian subgroup A is at most linear in k (see Question 3.9). By Theorem 1.11, such a bound holds for the generating number of the Frattini subgroup of any abelian subgroup of G. As another piece of evidence let us quote the following:

Theorem 1.12 (Alperin, Glauberman [2])**.** *Let G be a finite p-group satisfying one of the following conditions.*

(1) *p is odd and $p > 4r(G) - 7$;*
(2) *G has nilpotency class at most p;*

Then $nr(G) = r(G)$.

In contrast, examples of Alperin [16, Exercise 31, p. 349] and Glauberman [10] shows that $nr(G)$ can be strictly smaller than $r(G)$.

A key result in this paper (which is essential for the proof of Theorem 1.11) says that a commutative subalgebra $\mathcal{A} \leq \mathrm{Hom}(V)$ is "close to being a zero algebra" in the following sense.

Theorem 1.13. *Let V be an n-dimensional vector space over the field K and let $\mathcal{A} \leq \mathrm{Hom}(V)$ be a commutative algebra. Then there exists a zero algebra $\mathcal{B} \leq \mathcal{A}$ satisfying $\mathrm{codim}(\mathcal{B}, \mathcal{A}) \leq n$.*

As a consequence of Theorem 1.13 we have the following

Theorem 1.14. *Let $A \leq GL(n,p)$ be an abelian subgroup. Then $|A : \Omega_1(O_p(A))| \leq p^n$. In particular, if $A \leq GL(n,p)$ is an abelian p-subgroup then there are at most n many factors in the cyclic decomposition of A, which are larger than C_p. In other words, $d(\Phi(A)) \leq n$ for any abelian p-subgroup $A \leq GL(n,p)$.*

Remark 1.15. Let $k = n/(p+1)$ and $V = V_1 \oplus \ldots \oplus V_k$ with $\dim(V_i) = p + 1$ for each i. Furthermore, let $g_1, \ldots, g_k \in GL(V)$ be such that $g_i|_{V_j} = \mathrm{id}_{V_j}$ for $i \neq j$ while $g_i|_{V_i}$ corresponds to a unipotent Jordan-block for each i. Then $o(g_i) = p^2$ and $\langle g_1, \ldots, g_k\rangle = \langle g_1\rangle \times \langle g_2\rangle \times \ldots \times \langle g_k\rangle \simeq C_{p^2}^k$, so the upper bound in Theorem 1.14 is essentially the best possible.

An immediate consequence is that $|A| \le p^n - 1$ holds for any abelian p'-subgroup of $GL(n,p)$. Previously, we only knew of a proof for this fact which depends on Maschke's theorem. (Note that a subgroup of $GL(n,p)$ generated by a Singer cycle has order exactly $p^n - 1$, so this bound is the best possible.)

2. Proofs

Let V be an n dimensional vector space over a field K and let $\mathcal{A} \le \mathrm{Hom}(V)$ be a commutative subalgebra in the full endomorphism algebra $\mathrm{Hom}(V)$ of V. We use the notation $\mathcal{A}^2$ for the subalgebra of $\mathcal{A}$ generated by all products $\{xy \,|\, x, y \in \mathcal{A}\}$. Furthermore, let $\ker(\mathcal{A}) := \cap_{a\in\mathcal{A}} \ker(a) = \{v \in V \,|\, a(v) = 0 \ \forall a \in \mathcal{A}\}$. Clearly, $\mathcal{A}$ is a zero algebra if and only if $\ker(\mathcal{A}^2) = V$. In what follows, for two subspaces $U \le W$, the codimension of U in W is denoted by $\mathrm{codim}(U,W) := \dim(W) - \dim(U)$. First, we prove the following stronger theorem than Theorem 1.13. Note that in our terminology the property "ideal" also implies "K-subspace".

Theorem 2.1. *Let V be an n dimensional vector space over the field K and let $\mathcal{A} \le \mathrm{Hom}(V)$ be a commutative algebra with $\dim(\ker(\mathcal{A})) = k$. Then there is an ideal $\mathcal{B}$ of $\mathcal{A}$ satisfying $\mathrm{codim}(\mathcal{B},\mathcal{A}) \le n-k$ and $\mathcal{B}^2 = 0$.*

Proof. We define a series of integers $0 = l_0 < l_1 < \ldots \le n-k$ and ideals $\mathcal{A} = \mathcal{A}_0 > \mathcal{A}_1 > \ldots$ of $\mathcal{A}$ such that $\mathrm{codim}(\mathcal{A}_i,\mathcal{A}) = l_i$ and $\dim(\ker(\mathcal{A}_i)) \ge l_i + k$ holds for every i. For $i = 0$, the pair $l_0 = 0$, $\mathcal{A}_0 = \mathcal{A}$ clearly satisfies both conditions. Let us assume that we found the pair $l_i, \mathcal{A}_i$ for some i. Now, if $\ker(\mathcal{A}_i^2) = V$, then statement of the Theorem holds for $\mathcal{B} := \mathcal{A}_i$.

Otherwise, let us choose an $x \in V$ such that $x \notin \ker(\mathcal{A}_i^2)$. This means that $V_i = \mathcal{A}_i(x) := \{a(x) \,|\, a \in \mathcal{A}_i\}$ is not contained in $U_i := \ker(\mathcal{A}_i)$. Since $\mathcal{A}_i$ is an ideal of $\mathcal{A}$, both U_i and V_i are $\mathcal{A}$-invariant, so $U_i \cap V_i$ is also $\mathcal{A}$-invariant. Now, let

$$\mathcal{A}_{i+1} = \{a \in \mathcal{A}_i \,|\, a(x) \in U_i \cap V_i\},\ m_i := \mathrm{codim}(U_i \cap V_i, V_i) > 0,\ l_{i+1} := l_i + m_i.$$

Since $\varphi_x : a \mapsto a(x)$ defines a surjective linear map $\varphi_x : \mathcal{A}_i \mapsto V_i$ and $\mathcal{A}_{i+1} = \varphi_x^{-1}(U_i \cap V_i)$ it readily follows that $\mathrm{codim}(\mathcal{A}_{i+1},\mathcal{A}_i) = m_i > 0$, so $\mathrm{codim}(\mathcal{A}_{i+1},\mathcal{A}) = l_{i+1} > l_i$. Furthermore, the $\mathcal{A}$-invariance of $U_i \cap V_i$ and $\mathcal{A}_i \lhd \mathcal{A}$ implies that $\mathcal{A}_{i+1} \lhd \mathcal{A}$.

It remains to prove that $\dim(\ker(\mathcal{A}_{i+1})) \ge l_{i+1} + k$. (Thus, $l_{i+1} \le n-k$ also holds!) For any $y \in V_i$ we have $y \in \mathcal{A}_i(x)$, so $\mathcal{A}_{i+1}(y) \subset \mathcal{A}_{i+1}(\mathcal{A}_i(x)) = \mathcal{A}_i(\mathcal{A}_{i+1}(x)) \subset \mathcal{A}_i(U_i) = 0$ by using the commutativity of $\mathcal{A}$ and the definition of $\mathcal{A}_{i+1}$ and U_i. Therefore, $V_i \le \ker(\mathcal{A}_{i+1})$. On the other hand, $U_i = \ker(\mathcal{A}_i) \le \ker(\mathcal{A}_{i+1})$, so $\dim(\ker(\mathcal{A}_{i+1})) \ge \dim(U_i + V_i) = \dim(U_i) + \mathrm{codim}(U_i \cap V_i, V_i) \ge l_i + k + m_i = l_{i+1} + k$ also holds.

Trivially, the series $0 = l_0 < l_1 < \ldots \le n-k$ has length at most $n-k+1$, so we find a sufficient ideal $\mathcal{B} = \mathcal{A}_i$ for some i in at most $n-k+1$ many steps. □

Proof of Theorem 1.14. We only need to prove the first statement, since the second statement is just a special case of the first.

Let V be an n dimensional vector space over $\mathbb{F}_p$, so we can view A as a subgroup of $GL(V)$. If $A \le B \le GL(V)$ and B is also an abelian subgroup, then $\Omega_1(O_p(A)) = A \cap \Omega_1(O_p(B))$, so $|A : \Omega_1(O_p(A))| \le |B : \Omega_1(O_p(B))|$. Thus, we can assume that $A \le GL(V)$ is maximal among the abelian subgroups of $GL(V)$. Let $\mathcal{A} \le \mathrm{Hom}(V)$ be the subalgebra of $\mathrm{Hom}(V)$ generated by A. Then $\mathcal{A}$ is commutative and $A = U(\mathcal{A})$ is the unit group of $\mathcal{A}$. By Theorem 1.13, there is a zero algebra $\mathcal{B} \le \mathcal{A}$ with

$\operatorname{codim}(\mathcal{B},\mathcal{A}) \le n$. Then $1+\mathcal{B} \le A$ is an elementary abelian p-subgroup of A, so $1+\mathcal{B} \le \Omega_1(O_p(A))$. Therefore,

$$|A : \Omega_1(O_p(A))| \le \frac{|A|}{|1+\mathcal{B}|} \le \frac{|\mathcal{A}|}{|\mathcal{B}|} = p^{\operatorname{codim}(\mathcal{B},\mathcal{A})} \le p^n,$$

and the claim follows. □

Before the proof of Theorem 1.11, we summarise an idea of Sambale, which can be found in the proof of [27, Theorem 1.3]). This idea will also be used in the proofs of Theorem 1.7 and Theorem 1.10.

Let G be a finite 2-group and let E be a maximal elementary abelian normal subgroup of G with $d(E) = k$. Let $C = C_G(E)$. Choose a maximal abelian normal subgroup A of exponent at most 4 which contains E. Then obviously $C_G(A) \le C$. By a result of Alperin [1, Theorem] (see also [16, III, 12.1 Satz]), $\Omega_2(C_G(A)) = A \le Z(C_G(A))$, that is, $C_G(A)$ is 2-central. (For the definition and basic properties of p-central groups see [7] and [23].) Sambale observed that $C/C_G(A)$ is elementary abelian. Furthermore, by using a theorem of MacWilliams (see [6, Theorem 37.1]), he showed that $|C : \Phi(C)| \le 2^{2k}$. We note that Sambale's argument can be used without modification to prove that $|H : \Phi(H)| \le 2^{2k}$ holds for any subgroup H satisfying $E \le H \le C$.

Proof of Theorem 1.11. First, we consider the case $p > 2$. In accordance with the assumption, let E be a maximal elementary abelian normal subgroup of G with $d(E) = k$. Let C be the centraliser of E in G. Then $\Omega_1(C) \le E$ by [1, Theorem]. If $A \le G$ is any abelian subgroup, then $d(A \cap C) = d(\Omega_1(A \cap C)) \le d(E) = k$ holds. The action of A on E defines an injection $A/A \cap C \mapsto \operatorname{Aut}(E) \simeq GL(k,p)$, so $d(\Phi(A/A \cap C)) \le k$ by Theorem 1.14. Therefore,

$$d(\Phi(A)) \le d(\Phi(A)(A \cap C)) \le d(\Phi(A/A \cap C)) + d(A \cap C) \le 2k.$$

Now, we turn to the case $p = 2$. Let E be a maximal elementary abelian normal subgroup of G with $d(E) = k$ and $C = C_G(E)$. Furthermore, let $A \le G$ be any abelian subgroup. Using the aforementioned result of Sambale we get $d(A \cap C) \le d((A \cap C)E) \le 2k$. On the other hand, the same argument as in case $p > 2$ proves that $d(\Phi(A/A \cap C)) \le k$. Therefore,

$$d(\Phi(A)) \le d(\Phi(A/A \cap C)) + d(A \cap C) \le k + 2k = 3k.$$

□

Now, we show that MacWilliams' Theorem [20, Theorem A] can be extended for $p = 2$, as well.

Proof of Theorem 1.4. We only point out, how MacWilliams' argument must be modified to hold also for $p = 2$. MacWilliams proof can be divided into two parts.

(1) First, she proves that if p is an odd prime and G is a p-group, then there is a subgroup $H \le G$ of nilpotency class at most two satisfying $d(G) \le d(H)$.
(2) Second, starting from a p-subgroup $G \le GL(n,p)$ of nilpotency class at most two, she modify it to get a $\tilde{G} \le GL(n,p)$ with $d(G) \le d(\tilde{G})$ such that $d(\tilde{G})$ can easily be calculated.

It turns out that part (2) of MacWilliams' proof works also for the case $p = 2$, but the claim in part (1) is not valid for $p = 2$. However, there is a similar statement which also follows for $p = 2$. Let $w = x^{p^2}[y,z] \in F_3$ be a word, i.e. an element of the free group $F_3 = \langle x, y, z\rangle$. For any p-group P, let $w(P) = \langle w(g_1, g_2, g_3) \mid g_1, g_2, g_3 \in P\rangle$ be the verbal subgroup of P defined by w. Thus, $s(P) := |P : w(P)|$ equals the order of the largest abelian quotient of P with exponent at most p^2. Now, results of González-Sánchez and Klopsch ([13, Lemma 3.1] and [13, Theorem 3.3]) imply that there is a subgroup $G_1 \leq G \leq GL(n, p)$ of nilpotency class ≤ 2 such that $s(G_1) = s(G)$. Now, the initial step of MacWilliams' modifying argument can be used to find a $G_2 = N \rtimes H \leq GL(n, p)$ of nilpotency class ≤ 2 such that $|G_2| = |G_1|$, furthermore $N \lhd G_1$ and $\Phi(G_2) = G_2' = [N, G_2] = [N, G_1] \leq G_1'$. (For details, see [20, page 135].) Therefore,

$$s(G) = s(G_1) \leq |G_1 : G_1'| \leq |G_2 : G_2'| = |G_2 : \Phi(G_2)| = p^{d(G_2)}.$$

Now, $d(G_2) \leq \frac{1}{4}n^2$ by MacWilliams' argument, so $s(G) \leq p^{\frac{1}{4}n^2}$ which readily implies $d(G) \leq \frac{1}{4}n^2$. □

Proof of Theorem 1.7. Let $C = C_G(E)$ be the centraliser of E and let $H \leq G$ be any subgroup of G. Using Sambale's result to the group $(H \cap C)E$ we get that $d(H \cap C) \leq d((H \cap C)E) \leq 2k$. On the other hand, $H/(H \cap C)$ is included in $\mathrm{Aut}(E) \simeq GL(k, 2)$, so $d(H/(H \cap C)) \leq \frac{1}{4}k^2$ by Theorem 1.4. Therefore, $d(H) \leq d(H \cap C) + d(H/(H \cap C)) \leq 2k + \frac{1}{4}k^2$, as claimed. □

Proof of Theorem 1.10. Let E be a maximal elementary abelian normal subgroup of G with $d(E) = k$ and let $C = C_G(E)$. Then G/C is a subgroup of $\mathrm{Aut}(E) \simeq GL(k, 2)$, so $|G : C| \leq 2^{\binom{k}{2}}$. As in Sambale's argument (see the paragraph preceding the proof of Theorem 1.11) choose a maximal abelian normal subgroup A of exponent at most 4 which contains E. Then $C/C_G(A)$ is elementary abelian, and $|C : \Phi(C)| \leq 2^{2k}$, so $|C : C_G(A)| \leq |C : \Phi(C)| \leq 2^{2k}$. Furthermore, $C_G(A)$ is p-central, so, by using [23, Proposition 4], we get that $|C_G(A) : \mho_1(C_G(A))| \leq |\Omega_1(C_G(A))| = |E| = 2^k$. Therefore,

$$\begin{aligned}|G : \mho_1(G)| &\leq |G : \mho_1(C_G(A))| = |G : C| \cdot |C : C_G(A)| \cdot |C_G(A) : \mho_1(C_G(A))| \\ &\leq 2^{\binom{k}{2}+2k+k} = 2^{\frac{k(k+5)}{2}}.\end{aligned}$$

□

3. Related problems

In this section we pose some problems related to the above results. A positive answer to the following question would be a generalization of Theorem 1.14.

Question 3.1. *Let $G \leq GL(n, p)$ be a p-group and let H/K be an abelian section of G, that is, $K \lhd H \leq G$ with H/K abelian. Is is true that there are at most n many factors in the cyclic decomposition of H/K, which are larger than C_p? Or, at least, is the number of such factors bounded by $O(n)$?*

Another possible generalisation of Theorem 1.14 is

Question 3.2. *Let $G \leq GL(n, p)$ be p-central. Is it true that $|\Omega_2(G)/\Omega_1(G)| \leq p^n$?*

By [23, Lemma C], the p-central assumption implies that $\Omega_2(G)$ is of exponent p^2 and of nilpotency class 2. Furthermore, $|\Omega_{i+1}(G)/\Omega_i(G)| \leq |\Omega_2(G)/\Omega_1(G)|$ for every $i \geq 2$ in a p-central group.

Note that if $G \leq GL(n, p)$ is a p-Sylow subgroup of $GL(n, p)$, then $d(\Phi(G)) = 2n - 5$, so the final conclusion in Theorem 1.14 does not remain valid if the abelian condition for G is dropped. In fact, the below example shows that there exists a p-group $G \le GL(n,p)$ such that $d(\Phi(G))$ is roughly $n^2/4$.

Example 3.3. Let $\{E_{ij} \mid 1 \le i,j \le n\}$ be the usual basis of the vector space of $n \times n$ matrices over $\mathbb{F}_p$ and let 1 denote the $n \times n$ identity matrix. Let

$$G = \Big\{ 1 + \sum_{i<j} a_{ij} E_{ij} \,\Big|\, a_{ij} = 0 \text{ if } j < \lceil n/2 \rceil \text{ or } i > \lceil n/2 \rceil \Big\} \le GL(n,p).$$

Then

$$\Phi(G) = G' = Z(G) = \Big\{ 1 + \sum_{i<j} a_{ij} E_{ij} \,\Big|\, a_{ij} = 0 \text{ if } j \le \lceil n/2 \rceil \text{ or } i \ge \lceil n/2 \rceil \Big\}$$

has rank $\lfloor n/2 \rfloor \cdot (\lceil n/2 \rceil - 1)$.

Maybe the abelian condition in Theorem 1.14 can be weakened to several important classes of p-groups. We ask

Question 3.4. *Let $G \le GL(n,p)$ be a p-central, powerful or regular p-group. Is it true that $d(\Phi(G)) \le n$ (or $O(n)$)?*

The next problem is similar to Theorem 1.13. It might be useful to answer Question 3.1.

Question 3.5. *Let V be an n dimensional vector space over the field K and let $A \le \mathrm{Hom}(V)$ be a nilpotent algebra. Does there exist a subalgebra $B \le A$ of codimension at most n (or $O(n)$) such that $B^2 \le [B,B]$ (or, at least, $B^2 \le [A,A]$)?*

One might think that Question 3.1 could be reduced to Theorem 1.14 by showing that if a finite p-group has a quotient isomorphic to $(C_{p^r})^n$ for some r and n, then it always contains a subgroup isomorphic to $(C_{p^r})^n$ (or, at least $(C_{p^r})^{\varepsilon n}$ for some absolute constant $\varepsilon > 0$). However, this is not the case; For $r = 1$, this has been proved by Ol'shanskii [25]. Using his result, we now prove Theorem 1.9, which is a generalisation of the above statement for any $r \ge 1$.

First we prove a lemma.

Lemma 3.6. *Let R be a commutative ring, $A = R^n$, $B = R^k$ and let $\varphi : A \times A \mapsto B$ be an alternating R-bilinear map. Then there is a 2-nilpotent group G and $G' \le N \le Z(G)$ such that $G/N \simeq A$, $N \simeq B$ as abelian groups and the commutator map $[.\,,.] : G/N \times G/N \mapsto N$, $(xN, yN) \mapsto [x,y]$ agrees with φ under these isomorphisms.*

Proof. First, if S is any ring with $S^3 = 0$, then $G := 1 + S$ is a 2-nilpotent group with group operation $(1+s)(1+t) := 1 + s + t + st$ satisfying $G' \le 1 + S^2 \le Z(G)$. Furthermore, $[1+s, 1+t] = (1 - s + s^2)(1 - t + t^2)(1+s)(1+t) = 1 + st - ts$ holds for every $s, t \in S$.

Now, starting from A, B, φ we construct a ring S with underlying abelian group $A \oplus B$. Let $e_1, \dots, e_n$ be the canonical basis of A. We define the multiplication on S as

$$BS = SB = 0, \; e_i e_j = \begin{cases} \varphi(e_i, e_j) & \text{if } i < j, \\ 0 & \text{if } i \ge j \end{cases}$$

and we extend it to the whole S in a distributive way. Then S is a ring with $S^3 = 0$, so $G = 1 + S$ is a group and $N = 1 + B$ satisfies $G' \le 1 + S^2 \le N \le Z(G)$. Furthermore, the maps $(1+a)N \mapsto a$ and $1 + b \mapsto b$ $(a \in A,\ b \in B)$ define isomorphisms $G/N \mapsto A$ and $N \mapsto B$, respectively. Finally, for every $1 \le i, j \le n$ we have

$$[(1+e_i)N, (1+e_j)N] = 1 + e_ie_j - e_je_i = 1 + \varphi(e_i, e_j).$$

Thus the commutator map $[.\,,.] : G/N \times G/N \mapsto N$ agrees with φ on the set of generators $\{(1+e_i)N \,|\, 1 \le i \le n\}$ under the above isomorphisms, so it agrees with φ on the whole G/N. □

Remark 3.7.

(1) The above construction also works in the more general case if A is any (not necessarily finite dimensional) free R-module and B is any R-module.
(2) If there is a half of every element in B (for example, when R is a K-algebra over a field K of characteristic different from 2), then the multiplication $A \times A \mapsto B$ can be defined in a more natural way by choosing $a_1a_2 := \frac{1}{2}\varphi(a_1, a_2)$. In that case the exponent of G always agrees with the exponent of R as an additive group.

Proof of Theorem 1.9. Let $\tilde{A} := \mathbb{Z}_p^n,\ \tilde{B} := \mathbb{Z}_p^k$ and let $\tilde{\varphi} : \tilde{A} \times \tilde{A} \mapsto \tilde{B}$ be an alternating bilinear map such that there is no k-dimensional completely isotropic subspace of A with respect to $\tilde{\varphi}$. (Since $2n < k(k-1)$, such a map exists by [25, Lemma 2.].) Let $M_{\tilde{\varphi}} \in (\tilde{B})^{n\times n}$ be the matrix form of $\tilde{\varphi}$ with respect to the natural basis of $\tilde{A} = \mathbb{Z}_p^n$ so $M_{\tilde{\varphi}}$ is an alternating matrix over $\tilde{B}$.

Let us choose $R = \mathbb{Z}_{p^r},\ A = R^n,\ B = R^k$, so $A \simeq C_{p^r}^n$ and $B \simeq C_{p^r}^k$ as abelian groups. Let $M_\varphi \in B^{n\times n}$ be an alternating matrix over B such that the natural homomorphism $\pmod p : \mathbb{Z}_{p^r} \mapsto \mathbb{Z}_p$ maps M_φ to $M_{\tilde{\varphi}}$ and let $\varphi : A \times A \mapsto B$ be the alternating map whose matrix is M_φ with respect to the natural basis of A.

By Lemma 3.6 and its proof, there are p-groups $G = G(A, B, \varphi)$ and $\tilde{G} = G(\tilde{A}, \tilde{B}, \tilde{\varphi})$ of the form $G = 1+S$ and $\tilde{G} = 1+\tilde{S}$. By construction, the $\pmod p$-map extends to a surjective ring homomorphism $S \mapsto \tilde{S}$, so it also defines a surjective group homomorphism $\rho : G \mapsto \tilde{G}$ whose kernel is $K = 1 + pS$. Now, for any $s \in S$ we have $(1+ps)^{p^{r-1}} = 1 + p^rs + \binom{p^{r-1}}{2} \cdot p^2s^2 = 1$, so the exponent of K is p^{r-1}.

It remains to prove that G does not contain any abelian subgroup isomorphic to $C_{p^r}^{2k}$. Assuming the converse, let $H \le G$ be such a subgroup. Then $\rho(H) \simeq H/H\cap K$ is an abelian subgroup of $\tilde{G}$ such that $d(\rho(H)) = 2k$. Therefore, the image of $\rho(H)$ under the natural map $\tilde{G} \mapsto \tilde{G}/\tilde{B} \simeq \tilde{A}$ is a completely isotropic subspace with respect to the form φ whose dimension is at least k, which is a contradiction. □

Some results from [13] suggest that Question 3.1 might be reduced to p-groups of nilpotency class 2 as follows.

Question 3.8. *Let G be a finite p-group such that G has a quotient isomorphic to $(C_{p^r})^l$ for some positive integers l and $r > 1$. Is it true that G contains a subgroup of nilpotency class at most 2 with this property?*

By Example 1.3, if we only assume that G contains a maximal abelian normal subgroup A with $d(A) = k$, then $O(k^2)$ is the smallest general upper bound to $r(G)$. On the other hand, if we assume that $d(A) \le k$ for *every* maximal abelian normal subgroup A of G (i.e. we assume that $nr(G) \le k$), then we do not know any similar example. So we may ask:

Question 3.9. *Let G be a p-group and let us assume that $nr(G) \leq k$, that is, $d(A) \leq k$ for every abelian normal subgroup A of G. Is it true that $r(G) \leq 2k$, that is, $d(B) \leq 2k$ holds for every abelian subgroup B of G ?*

Remark 3.10. The k-term direct power D_{16}^k (where D_{16} is the dihedral group of order 16) shows that this bound is the best possible.

One can ask a similar question, but using the order of abelian subgroups instead of their rank.

Question 3.11. *Let G be a p-group and let us assume that $|A| \leq p^m$ for every abelian normal subgroup A of G. Is is true that $|B| \leq p^{2m}$ holds for every abelian subgroup B of G?*

Remark 3.12. Examples of Alperin and Glauberman [16, Exercise 31, p. 349], [12] show that there exists a p-group G for which $\max\{|B| \mid B \leq G \text{ is abelian}\}$ is strictly larger than $\max\{|A| \mid A \lhd G \text{ is abelian}\}$. Moreover, if $p \geq 5$, then there exists a group of exponent p with this property.

On the other hand, under various conditions (for example when G is metabelian [9] or it has nilpotency class at most $p-1$ [11]) there is a normal abelian subgroup among the abelian subgroups of maximal order.

References

[1] J. L. Alperin, Centralizers of abelian normal subgroups of p-groups, *J. Algebra* **1** (1964) 110–113.

[2] J. L. Alperin and G. Glauberman, Limits of abelian Subgroups of Finite p-Groups, *J. Algebra* **203** (1998) 533–566.

[3] L. Babai and A. J. Goodman, Subdirectly reducible groups and edge-minimal graphs with given automorphism group, *J. London Math. Soc. (2)* **47** (1993), 417–432.

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

[5] N. Blackburn, Generalizations of certain elementary theorems on p-groups, *Proc. London Math. Soc. (3)* **11** (1961), 1–22.

[6] Y. Berkovich, *Groups of prime power order. Vol. 1*, de Gruyter Expositions in Mathematics, **46**, Walter de Gruyter GmbH & Co. KG, Berlin, 2008.

[7] D. Bubbolini, G. Corsi Tani, p-groups with some regularity properties, *Ricerche Mat.* **49** (2000) 327–339.

[8] B. Csikós, L. Pyber, E. Szabó, Finite subgroups of the homeomorphism group of a compact manifold are almost nilpotent, in preparation.

[9] J. D. Gillam, A note on finite metabelian p-groups, *Proc. Amer. Math. Soc.* **25** (1970), 189–190.

[10] G. Glauberman, Large abelian Subgroups of Groups of Prime Exponent, *J. Algebra* **237** (2001) 735–768.

[11] G. Glauberman, Large subgroups of small class in finite p-groups, *J. Algebra* **272** (2004) 128–153.

[12] G. Glauberman, A p-group with no normal large abelian subgroup, Character theory of finite groups, 61–65. *Contemp. Math.*, **524** American Mathematical Society, Providence, RI, 2010

[13] J. González-Sánchez and B. Klopsch, On w-maximal groups, *J. Algebra* **328** (2011) 155–166.

[14] R. M. Guralnick, On the number of generators of a finite group. *Arch. Math. (Basel)* **53** (1989), 521–523.

[15] P. Hall, A contribution to the theory of groups of prime-power order, *Proc. London Math. Soc.* **36** (1934) 29–95.

[16] B. Huppert, *Endliche Gruppen. I.* Springer-Verlag, Berlin-New York 1967.

[17] I. M. Isaacs, The number of generators of a linear p-group. *Canadian J. Math.* **24** (1972), 851–858.

[18] Z. Janko, Finite 2-groups with no normal elementary abelian subgroups of order 8. *J. Algebra* **246** (2001), 951–961.

[19] A. Lucchini, A bound on the number of generators of a finite group. *Arch. Math. (Basel)* **53** (1989), 313–317.
[20] A. R. (MacWilliams) Patterson, The minimal number of generators for p-subgroups of $GL(n,p)$, *J. Algebra* **32** (1974), 132–140.
[21] A. R. MacWilliams, On 2-groups with no normal abelian subgroups of rank 3, and their occurrence as Sylow 2-subgroups of finite simple groups. *Trans. Amer. Math. Soc.* **150** (1970), 345–408.
[22] A. Mann, Generators of 2-groups, *Israel J. Math.* **10** (1971) 158–159.
[23] A. Mann, The power structure of p-groups. II. *J. Algebra* **318** (2007), 953–956.
[24] L. N. Mann, J. C. Su, Actions of elementary p-groups on manifolds, *Trans. Amer. Math. Soc.* **106** (1963), 115–126.
[25] A. Yu. Ol'shanskii, The number of generators and orders of abelian subgroups of finite p-groups, *Math. Notes*, **23**(3) (1978) 183–185.
[26] L. Pyber, Asymptotic results for permutation groups, Groups and computation (New Brunswick, NJ, 1991), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, RI, (1993) 197–219.
[27] B. Sambale, Exponent and p-rank of finite p-groups and applications. *Arch. Math.* (Basel) **103** (2014) 11–20.
[28] M. Suzuki, *Group theory I.* Springer-Verlag, Berlin-New York, 1982.
[29] M. Suzuki, *Group theory II.* Springer-Verlag, New York, 1986.

Department of Algebra and Number Theory, Eötvös University, Pázmány Péter sétány 1/c, H-1117, Budapest, Hungary and Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary
ORCID: https://orcid.org/0000-0002-1305-5380
Email address: zhalasi@caesar.elte.hu and halasi.zoltan@renyi.hu

Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary
Email address: podoski.karoly@renyi.hu

Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary
Email address: pyber.laszlo@renyi.hu

Alfréd Rényi Institute of Mathematics, Reáltanoda utca 13-15, H-1053, Budapest, Hungary
Email address: szabo.endre@renyi.hu