PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 11, November 2012, Pages 3769–3775
S 0002-9939(2012)11245-6
Article electronically published on March 14, 2012

RANKS OF p-GROUPS

INNA (KORCHAGINA) CAPDEBOSCQ

(Communicated by Jonathan I. Hall)

Abstract. The main results of this paper provide a lower bound on the p-rank of the finite p-groups.

1. Introduction

The main goal of this article is to provide a lower bound on the p-rank of the finite p-groups. Before we state the main result, let us give some reasons that motivated the author to investigate the value of such a bound.

In finite group theory there are certain problems that require identification and characterization of a group about which one knows very little to start with. These kinds of questions often arise in problems related to the second generation proof of the Classification of Finite Simple Groups, also known as the GLS-series, an ongoing project under the direction of Gorenstein, Lyons and Solomon, currently being published by the AMS (cf. [GLS1]).

Here is a typical situation arising in the project: given an unknown group G and few hypotheses about it, we must identify it or, in fact, show that such a group does not exist. In order to solve such a problem, we must try to find as much as possible about G. Usually this is done by studying the p-local subgroups of G for various primes p (i.e., the normalizers of non-trivial p-subgroups of G). Suppose that $N = N_G(P)$, P a non-trivial p-subgroup of G. Then we can try to answer various questions about N, e.g., what is $N_G(P)/P$? How big is P? The latter question can be asked in several ways; for example, how big is $|P|$? But more often, the question about "being big" really means, what is the p-rank $m_p(P)$ of P?

Let us consider the following definition.

Definition 1.1. For a finite p-group P, the p-rank of P, $m_p(P) := \log_p |P_0|$ where P_0 is the largest elementary abelian subgroup of P.

Notice that in the case $p = 2$, this is equivalent to P_0 being the largest subgroup of P of exponent 2.

How does one try to get an answer to this question? Suppose we know something about $N_G(P)/P$ acting on P; for example, suppose that we know that there exists a large cyclic subgroup $C \cong C_q$ of order co-prime to P acting faithfully on P. Then what we can evaluate is $n = m_p(P/\Phi(P))$, where $P/\Phi(P)$ is thought of as a vector space V of dimension n over $\mathbb{F}_p$ and C is acting on V faithfully. But if P is non-abelian, n still does not give us $m_p(P)$. So, what can we do now? This is

Received by the editors November 8, 2010 and, in revised form, March 1, 2011 and May 2, 2011.

2010 *Mathematics Subject Classification.* Primary 20D15.

precisely how we came across the question whose solution is the main result of this paper. Since the case $p = 2$ is of special importance, in this article we first provide the answer for $p = 2$.

Theorem 1.2. *Let P be a finite 2-group of class at most 2 and exponent 4. Suppose that $n := m_2(P/\Phi(P))$ and $l := m_2(\Phi(P))$. Then*

$$m_2(P) \geq [\frac{n}{l+1}] + l - 1.$$

The immediate consequence of the above result is a slightly rougher estimation of $m_2(P)$, but then only in terms of n.

Corollary 1.3. *Let P be a 2-group of class at most 2 and exponent 4 with $n := m_2(P/\Phi(P))$. Then*

$$m_2(P) \geq [2\sqrt{n} - 2].$$

At this moment, the reader might rightfully complain: why do we restrict ourselves to the result about P being of class at most 2 and exponent 4? This comes from the fact that every finite p-subgroup R contains a *critical* subgroup Q with the following properties (cf. [GLS2, Proposition 11.11]):

Theorem (J. G. Thompson)**.** *A p-group R possesses a characteristic subgroup Q with the following properties:*

1. *Every p'-group of automorphisms of R acts faithfully on Q.*
2. *Q has nilpotence class at most 2.*
3. *If Q is not abelian, then Q has exponent p or 4 according as p is odd or 2.*

Remark 1.4. Notice that the bound of Theorem 1.2 **cannot** be improved. For example, consider an extraspecial group $P = 2_-^{1+2m}$ (i.e., $P = D_8^{m-1} \circ Q_8$). Then $n = 2m$, $l = 1$ and according to Theorem 1.2,

$$m_2(P) \geq [\frac{2m}{1+1}] + 1 - 1 = m = m_2(P).$$

Another interesting example of 2-groups for which the estimates are sharp is Sylow 2-subgroups of unitary groups $PSU_3(2^m)$.

We would like to mention that this short result (Theorem 1.2) turned out to be a small yet useful contribution to the GLS-project and was most recently used in the paper of Franchi, Mainardis and Solomon [FMS].

1.1. **Odd case and related questions.** The natural questions to ask, of course, would be whether a relation between the p-rank of a p-group and the number of its generators has been investigated before and what types of results hold for odd primes p. Let us say a few words about it and also mention some related questions.

It is only appropriate to start with a work of W. Burnside [B], who has shown that a p-group P of order p^a (p is an arbitrary prime) has normal abelian subgroups of order p^b where b is such that $a \leq \frac{b(b-1)}{2}$. Later J.G. Thompson showed that if p is an odd prime and every normal abelian subgroup of P can be generated by k elements, then any subgroup of P (and in particular, P) can be generated by $\frac{k(k+1)}{2}$ elements (cf. p. 343 of [Hu]). His result was then improved by A. (MacWilliams) Patterson [McW2], who showed that under the same hypotheses any subgroup of P can be generated by $\frac{k(k+4)}{4}$ elements.

On the other hand, A. Ol′shanskii [Ol] established that if f (correspondingly F) is the smallest function such that every finite p-group (any prime p), all of whose abelian subgroups are generated by at most n elements (all of whose abelian subgroups have orders at most p^n), has at most $f(n)$ generators (has order not exceeding $p^{F(n)}$), then $f(n) \geq \frac{n^2-9}{8}$ and $F(n) \geq \frac{n^2+4n-8}{8}$. His results were then further improved for odd p in [BGH] (see p. 275). There the authors showed that for each odd prime p and a positive integer a there is a group G of order p^a whose largest abelian subgroups have order at most p^d where $d = [\sqrt{8a+9}] - 3$.

Thus it might be of some interest to investigate whether our main result also holds (and in fact can be slightly improved) in the case when p is odd. Analogous to $p = 2$, we resolve the question for p-groups of class 2 and exponent p to obtain the following conclusion.

Theorem 1.5. *Let p be an odd prime, and let P be a finite p-group of class at most 2 and exponent p. Suppose that $n := m_p(P/\Phi(P))$ and $l := m_p(\Phi(P))$. Then*

$$m_p(P) \geq [\frac{n}{l+1}] + l.$$

In particular,

$$m_p(P) \geq [2\sqrt{n} - 1].$$

Now we go on with the proof.

2. Proof of the main result for $p = 2$

Recall that P is a 2-group of class at most 2 and exponent at most 4, $n := m_2(P/\Phi(P))$ and $l := m_2(\Phi(P))$. It follows immediately that n is the number of generators of P and l is the number of generators of $\Phi(P)$. Also, notice that the following is true.

Lemma 2.1. *If P is a 2-group of class at most 2 and exponent 4, then $\Phi(P) \leq Z(P)$ and $\Phi(P)$ is elementary abelian.*

Proof. For $x, y \in P$, let $[x, y] := xyx^{-1}y^{-1}$.

Recall that as P is a finite 2-group, $\Phi(P) = [P,P]P^2$ where $P^2 = \langle x^2 \mid x \in P\rangle$. Since $cl(P) = 2$, $P/Z(P)$ is abelian and so $[P,P] \leq Z(P)$. Thus we need to show that $P^2 \leq Z(P)$. Assume the contrary. Then there exists $t \in P$ such that $t^2 \notin Z(P)$. Hence, we may find $x \in P$ such that $[t^2, x] \neq 1$. Recall that for all $a, b \in P$ we have

$$(*) \qquad [a^i, b^j] = [a,b]^{ij} \text{ and } (ab)^2 = [b,a]a^2b^2$$

(cf. Lemma 2.2.2 of [G]). Thus $[t,x]^2 = [t^2, x] \neq 1$. Since $exp(P) = 4$, it follows immediately that $o([t,x]) = 4$.

On the other hand, using $(*)$ above we obtain that $[t,x] = (xt)^2t^2x^2$ and $[a^2, b^2] = [a,b]^4 = 1$ for all $a, b \in P$. Since $[x^2, t^2] = [x,t]^4 = 1$, $[(xt)^2, x^2] = [xt, x]^4 = 1$ and $[(xt)^2, t^2] = [xt, t]^4 = 1$ (i.e., $(xt)^2$, x^2 and t^2 are pairwise commuting elements), we have that

$$[t,x]^2 = ((xt)^2t^2x^2)^2 = (xt)^4t^4x^4 = 1,$$

i.e., $o([t,x]) = 2$, an obvious contradiction proving that $\Phi(P) \leq Z(P)$.

If $exp(\Phi(P)) > 2$, we could find $x \in \Phi(P)$ with $o(x) = 4$. Clearly, $exp(P^2) \leq 2$. Thus there would exist $a, b \in P$ with $o([a,b]) = 4$. Then $1 \neq [a,b]^2 = [a^2, b] = 1$ (as $a^2 \in \Phi(P) \leq Z(P)$), a contradiction which finishes the proof. $\square$

An immediate consequence of Lemma 2.1 is $|P| = 2^{n+l}$. Notice that $l = 0$ is equivalent to P being an elementary abelian group. Note that our main result obviously holds for such groups.

We shall now proceed with a proof by induction on n. If $n = 1$, P is cyclic and the result trivially holds. Suppose that $n = 2$. If $l = 1$, then $[n/(l+1)] + l - 1 = 1 \leq m_2(P)$. If $l \geq 2$, $m_2(P) \geq l$ and so

$$[n/(l+1)] + l - 1 = l - 1 \leq l \leq m_2(P),$$

which proves the result.

Suppose now that the statement of Theorem 1.2 is correct for all $n < m$. Let $n = m$.

Assume first that $P - \Phi(P)$ does not contain an involution; i.e., all the elements of order two lie in $\Phi(P)$. In particular, $m_2(P) = l$. Therefore we now have to show that $l \geq [m/(l+1)] + l - 1$. In order to do that, let us combine the following two statements:

Proposition (I. M. Isaacs, [Is, 4.6])**.** *Let G be a group with exactly f involutions. Then*

$$1 + f = \Sigma_{\chi \in Irr(G)} \nu_2(\chi)\chi(1)$$

where $\nu_2(\chi) = 0$ if $\chi \neq \bar{\chi}$ and $\nu_2(\chi) = \pm 1$ if $\chi = \bar{\chi}$.

Lemma (A. MacWilliams, [McW1])**.** *Let G be a 2-group with $|G : \Phi(G)| \geq 2^{2k+1}$. Then*

$$\Sigma_{\chi \in Irr(G)} \nu_2(\chi)\chi(1) \equiv 0 \pmod{2^{k+1}}.$$

As a result we obtain that if $k \in \mathbb{N}$ is such that $m \geq (2k+1)$, then $k + 1 \leq l$. If m is odd, take $k = \frac{m-1}{2}$. This implies that $m \leq 2l - 1 < 2(l+1)$. If m is even, take $k = \frac{m-2}{2}$. Since $k + 1 \leq l$, obviously, $k < l$. Therefore again $m < 2(l+1)$. Dividing both sides of this inequality by $(l+1)$, we obtain that $m/(l+1) < 2$, and so $[m/(l+1)] \leq 1$. Hence, we obtain that

$$[m/(l+1)] + l - 1 \leq 1 + l - 1 = l,$$

which finishes the proof in the case when $P - \Phi(P)$ does not contain an involution.

Therefore we may now assume that there exists an involution $t \in P - \Phi(P)$. Let $\overline{P} := P/\Phi(P)$. Then $1 \neq \bar{t} \in \overline{P}$ and so we may choose a generating set of m elements of P in such a way that t is one of the generators. Now, $\overline{P}$ is abelian. In particular, it follows that $\langle t \rangle \Phi(P) \triangleleft P$. Hence, $t^P \subseteq \langle t \rangle \Phi(P) - \Phi(P)$, which implies that t has at most 2^l conjugates in P. Thus $|P : C_P(t)| \leq 2^l$ and $|C_P(t)| \geq 2^m$. Consider $C_P(t)$. Since $t \in Z(C_P(t))$, there exists $R_0 \leq C_P(t)$ such that $C_P(t) = \langle t \rangle \times R_0$. Moreover, as $\Phi(P) \leq Z(P)$, $\Phi(P) \leq C_P(t)$. There are now two cases to consider.

Case 1. $\Phi(P) = \Phi(R_0)$. Then $C_P(t)$ has at least $m - l$ generators. Choose them so that t is one of them. Then R_0 has at least $m - l - 1$ generators. By induction, $m_2(R_0) \geq [(m-l-1)/(l+1)] + l - 1$, and so

$$m_2(P) \geq m_2(C_P(t)) \geq 1 + [(m-l-1)/(l+1)] + l - 1 = [m/(l+1)] + l - 1,$$

which proves the result. This leads us to the second case.

Case 2. $\Phi(P) > \Phi(R_0)$. Now $R_0 = R_1 \times R_2$, where R_2 is an elementary abelian subgroup of $\Phi(P)$ of order $2^{l-m_2(\Phi(R_0))}$, while R_1 is a subgroup of R_0 with $\Phi(R_0) = \Phi(R_1)$ and R_1 is generated by at least $m - l - 1$ elements. Now,

$$m_2(R_0) = m_2(R_1) + m_2(R_2) = m_2(R_1) + l - m_2(\Phi(R_0)).$$

As $m_2(R_1/\Phi(R_1)) < m$, we may apply induction to obtain

$$m_2(R_1) \geq [(m - l - 1)/(m_2(\Phi(R_0)) + 1)] + m_2(\Phi(R_0)) - 1$$

and so

$$\begin{aligned} m_2(P) &\geq m_2(C_P(t)) = 1 + m_2(R_0) \\ &\geq 1 + [(m - l - 1)/(m_2(\Phi(R_0)) + 1)] + m_2(\Phi(R_0)) - 1 + l - m_2(\Phi(R_0)) \\ &= [(m - l - 1)/(m_2(\Phi(R_0))+1)]+l \geq [(m - l - 1)/(l + 1)] + l = [m/(l + 1)] + l - 1, \end{aligned}$$

which proves the result.

3. Case of odd p

This time P is a p-group of class at most 2 and exponent p, $n := m_p(P/\Phi(P))$ and $l := m_p(\Phi(P))$. Since $exp(P) = p$, it follows immediately that $\Phi(P) \leq Z(P)$ for $P^p = \langle x^p \mid x \in P\rangle = \{1_P\}$ while $[P, P] \leq Z(P)$ as $cl(P) = 2$. Thus $\Phi(P)$ is obviously an elementary abelian group, $|\Phi(P)| = p^l$ and $|P| = p^{n+l}$. As in the case $p = 2$ notice that $l = 0$ is equivalent to P being an elementary abelian group and that our result obviously holds for such groups.

We shall again proceed with a proof by induction on n. Note that our proof is pretty much a repetition of the proof for the case $p = 2$ adjusted to the odd case and that it is considerably easier than the "even" one.

If $n = 1$, $P \cong C_p$, a cyclic group of order p and the result trivially holds. Suppose that $n = 2$. If $l = 1$, then P is a group of order p^3 and exponent p. In particular, P is an extraspecial group and $m_p(P) = 2$. Since $[n/(l + 1)] + l = [2/2] + 1 = 2$, the result obviously holds. If $l \geq 2$, $m_p(P) \geq l$ and so $[n/(l+1)]+l = [2/(l+1)]+l = l \leq m_p(P)$, again proving the result.

Suppose now that the statement of Theorem 1.5 is correct for all $n < m$. Let $n = m$. Since $exp(P) = p$, every element of $P - \Phi(P)$ has order p (and so we do not need to worry as we did in the case $p = 2$). Let $t \in P - \Phi(P)$ be of order p. Let $\overline{P} := P/\Phi(P)$. Then $1 \neq \overline{t} \in \overline{P}$ and so we may choose a generating set of m elements of P in such a way that t is one of the generators. Now, $\overline{P}$ is abelian. In particular, it follows that $\langle t\rangle\Phi(P) \triangleleft P$. Hence, $t^P \subseteq \langle t\rangle\Phi(P) - \Phi(P)$ and so $|t^P| \leq p|\Phi(P)| - |\Phi(P)| = (p - 1)p^l$. Since the length of a conjugacy class in a p-group is a power of p, we may conclude that t has at most p^l conjugates in P.

Thus $|P : C_P(t)| \leq p^l$ and $|C_P(t)| \geq p^m$. Consider $C_P(t)$. Since $t \in Z(C_P(t))$, there exists $R_0 \leq C_P(t)$ such that $C_P(t) = \langle t\rangle \times R_0$. Moreover, as $\Phi(P) \leq Z(P)$, $\Phi(P) \leq C_P(t)$. There are now two cases to consider.

Case 1. $\Phi(P) = \Phi(R_0)$. Then $C_P(t)$ has at least $m - l$ generators. Choose them so that t is one of them. Then R_0 has at least $m - l - 1$ generators. By induction, $m_p(R_0) \geq [(m - l - 1)/(l + 1)] + l$, and so

$$m_p(P) \geq m_p(C_P(t)) \geq 1 + [(m - l - 1)/(l + 1)] + l = [m/(l + 1)] + l,$$

which proves the result. This leads us to the second case.

Case 2. $\Phi(P) > \Phi(R_0)$. Now $R_0 = R_1 \times R_2$, where R_2 is an elementary abelian subgroup of $\Phi(P)$ of order $p^{l-m_p(\Phi(R_0))}$, while R_1 is a subgroup of R_0 with $\Phi(R_0) = \Phi(R_1)$ and R_1 is generated by at least $m-l-1$ elements. Now,

$$m_p(R_0) = m_p(R_1) + m_p(R_2) = m_p(R_1) + l - m_p(\Phi(R_0)).$$

By induction,

$$m_p(R_1) \geq [(m-l-1)/(m_p(\Phi(R_0)) + 1)] + m_p(\Phi(R_0))$$

and so

$$\begin{aligned} m_p(P) \geq m_p(C_P(t)) &= 1 + m_p(R_0) \\ &\geq 1 + [(m-l-1)/(m_p(\Phi(R_0)) + 1)] + m_p(\Phi(R_0)) + l - m_p(\Phi(R_0)) \\ &= 1 + [(m-l-1)/(m_p(\Phi(R_0)) + 1)] + l \\ &\geq 1 + [(m-l-1)/(l+1)] + l = [m/(l+1)] + l, \end{aligned}$$

which finishes the proof.

Acknowledgements

The author is deeply indebted to George Glauberman for the information about the history of the subject and for the suggestion to extend the investigation to the case of odd p. The author would like to thank an anonymous referee who also suggested extending the investigation of the problem to the case of odd p and whose comments helped to improve the exposition of this article. The author is grateful to Ron Solomon for fruitful discussions and for his constant support.

This work was completed during the author's stay at the IAS (Princeton). This material is based upon work supported by the National Science Foundation under agreement No. DMS-0635607. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

References

[B] W. Burnside. On some properties of groups whose orders are powers of primes. Proc. London Math. Soc. (2), ii (1912), 225–245.

[BGH] J. Buhler, R. Gupta, J. Harris. Isotropic subspaces for skewforms and maximal abelian subgroups of p-groups. J. Algebra **108**, no. 1 (1987), 269–279. MR887208 (88d:15034)

[FMS] C. Franchi, M. Mainardis, R. Solomon. A characterization of HN. J. Group Theory **11** (2008), no. 3, 357–369; and **13** (2010), no. 1, 151–153. MR2419006 (2009d:20027); MR2604854 (2011c:20026)

[G] D. Gorenstein. Finite groups, Second edition. Chelsea Publishing Co., New York, 1980. MR569209 (81b:20002)

[GLS1] D. Gorenstein, R. Lyons, R. Solomon. The Classification of the Finite Simple Groups, Number 1. Amer. Math. Soc. Surveys and Monographs **40**, #**1** (1994). MR1303592 (95m:20014)

[GLS2] D. Gorenstein, R. Lyons, R. Solomon. The Classification of the Finite Simple Groups, Number 1. Amer. Math. Soc. Surveys and Monographs **40**, #**2** (1996). MR1358135 (96h:20032)

[Hu] B. Huppert. Endliche Gruppen. I. Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin-New York, 1967. MR0224703 (37:302)

[Is] I. Martin Isaacs. Character Theory of Finite Groups. Academic Press, New York (1976). MR0460423 (57:417)

[McW1] 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. MR0276324 (43:2071)

[McW2] A. R. (MacWilliams) Patterson. The minimal number of generators for p-subgroups of $GL(n, p)$. J. Algebra **32**, Issue 1 (1974), 132-140. MR0369522 (51:5755)

[Ol] A. Ju. Ol′shanskii. On the question of the orders and the number of generators of abelian subgroups of finite p-groups. Mat. Zametki **23**, no. 3 (1978), 337–341. MR0480736 (58:888)

Department of Mathematics, University of Warwick, Coventry, CV4 7AL England