MATH. SCAND. 41 (1977), 218–224

ON MONOMIAL p^a-REPRESENTATIONS OF FINITE p-GROUPS

JØRN B. OLSSON

In his paper [2] D. L. Johnson studied minimal faithful permutation representations of finite groups. If G is a finite group, a homomorphism of G into a symmetric group is called a permutation representation, and we let $\mu(G)$ denote the smallest possible degree (dimension) of a faithful $(1-1)$ permutation representation of G.

In the present note we study a natural generalization of this, monomial p^a-representations. These were first studied by H.-P. Jacobs in his thesis [1], written at Universität Dortmund under the supervision of Professor R. Kochendörffer. This note also contains an apparently new description of the rank of a finite p-group (in terms of intersections of subgroups), which may be of some independent interest.

Let a be a nonnegative integer, p a prime integer and n a positive integer. If Sym (n) is the symmetric group on n letters and $\wr$ denotes wreath product, the group $\mathbf{Z}_{p^a} \wr \mathrm{Sym}\,(n)$ may be considered as the group of $n \times n$ complex monomial matrices, whose nonzero entries are p^ath roots of unity. If G is a finite group, a homomorphism M of G into $\mathbf{Z}_{p^a} \wr \mathrm{Sym}\,(n)$ is called a *monomial p^a-representation of G (of degree n)*. If M is $1-1$, it is called *faithful*. A faithful monomial p^a-representation of G is denoted briefly a FM (p^a) *of* G. A FM (p^a) of G of smallest possible degree is called *minimal* and is denoted briefly a FMM (p^a) *of* G. The degree of a FMM (p^a) of G is denoted $\mu(G, p^a)$. Thus $\mu(G, 1) = \mu(G)$ in Johnson's notation.

A monomial p^a-representation of G is in particular a monomial representation of G and is therefore a direct sum of transitive monomial p^a-representations of G. Any transitive monomial representation of G is similar to a representation T^G induced from a linear representation T of a subgroup H of G, and it is a monomial p^a-representation of G, if and only if, $H/\mathrm{Ker}\,T$ is cyclic of an order dividing p^a. (Since $H/\mathrm{Ker}\,T$ is isomorphic to a subgroup of $\mathbf{C}$, it is cyclic. Moreover the values $T(x)$, $x \in H$, occur as entries in the monomial matrices $M(g)$, $g \in G$, where $M = T^G$. Thus $T(x)$, $x \in H$, have to be p^ath roots of

Received March 3, 1976.

unity.) It is easily seen, the kernel of $M=T^G$ is just the G-core of $K=\operatorname{Ker} T$, that is, $\bigcap_{g\in G} K^g$.

For our purposes it is most convenient to describe an arbitrary monomial p^a-representation of G as a sequence

$$M = \{(H_1,K_1),\ldots,(H_r,K_r)\},$$

where for $1\leqq i\leqq r$, H_i and K_i are subgroups of G, $K_i \lhd H_i$, and H_i/K_i is cyclic of an order dividing p^a. This signifies that M is similar to $\sum_{i=1}^r T_i^G$, where T_i is a linear representation of H_i with kernel K_i. The *kernel of* M is then just the G-core of $\bigcap_{i=1}^r K_i$, and the *degree of* M is $\sum_{i=1}^r |G\colon H_i|$. We call r the *length of* M.

If G is a group of p'-order, then a monomial p^a-representation of G is just a permutation representation of G. Since we have in the definition of a monomial p^a-representation already chosen a prime p, we restrict our attention to the case where G is a finite p-group.

Let G be a finite p-group $\neq 1$. We let $d(G)$ denote the *rank* of G. An *intersection set for* G is a set of subgroups $\{L_1,L_2,\ldots,L_s\}$ of G such that

$$\bigcap_{i=1}^{s} L_i = 1, \quad \text{and for } 1\leqq j\leqq s \quad \bigcap_{\substack{i=1\\ i\neq j}}^{s} L_i \neq 1 .$$

(For $s=1$, this statement means just $L_1=1$.)

The *intersection rank* of G is the maximal number of elements in an intersection set for G and is denoted $\tilde{d}(G)$. An intersection set for G with $\tilde{d}(G)$ elements is called *maximal*. As usual, $\Omega(G)$ is the subgroup of G generated by all elements of order p in G.

PROPOSITION 1. *Let G be a finite p-group. Then the intersection rank of G coincides with the* (*ordinary*) *rank, that is, $\tilde{d}(G)=d(G)$.*

PROOF. If A is an abelian subgroup of G of rank r, that is, $A=A_1\times\ldots\times A_r$, where $A_1,\ldots,A_r$ are cyclic, define for $1\leqq i\leqq r$

$$\hat{A}_i = A_1\times\ldots\times A_{i-1}\times A_{i+1}\times\ldots\times A_r .$$

It is easily seen that $\{\hat{A}_1,\ldots,\hat{A}_r\}$ is an intersection set for G. It follows that $d(G)\leqq\tilde{d}(G)$. On the other hand, let $\{L_1,\ldots,L_r\}$ be an intersection set for G. We show by induction on r, that G contains an abelian subgroup of rank r. This will prove $\tilde{d}(G)\leqq d(G)$. For $r=1$, the claim is trivially true. Since $L_1\cap\ldots\cap L_r=1$, there exists an i, $1\leqq i\leqq r$, such that $\Omega_1(Z(G))\nsubseteq L_i$, say $\Omega_1(Z(G))\nsubseteq L_1$.

(Here $Z(G)$ is the center of G.) From the definition of an intersection set it follows, that $\{L_1\cap L_2, L_1\cap L_3,\ldots,L_1\cap L_r\}$ is an intersection set for L_1. By the induction hypothesis L_1 contains an abelian subgroup A of rank $r-1$. Let

$z \in \Omega_1(Z(G))$, $z \notin L_1$. Then $|z| = p$ and $\langle z \rangle \cap A = \langle z \rangle \cap L_1 = 1$. Moreover $[\langle z \rangle, A] = 1$, because $z \in Z(G)$, so $\langle z \rangle$ and A form a direct product in G. Obviously $\langle z \rangle \times A$ has rank r. This proves Proposition 1.

Let us note the following trivial result.

LEMMA 2. *Let G be a finite p-group, $L \neq 1$ a subgroup and $L_1, \ldots, L_r$ subgroups of L. The following statements are equivalent*

I. *$\{L_1, \ldots, L_r\}$ is an intersection set for G*
II. *$\{L_1, \ldots, L_r\}$ is an intersection set for L*
III. *$\{L_1 \cap \Omega_1(G), \ldots, L_r \cap \Omega_1(G)\}$ is an intersection set for $\Omega_1(G)$.*

Now we return to monomial p^a-representations. As in Proposition 2 of [2] we of course have

LEMMA 3. *Let G and H be finite groups. Then*

$$\mu(G \times H, p^a) \leqq \mu(G, p^a) + \mu(H, p^a) .$$

In the rest of this work G *denotes a finite p-group* $\neq 1$.

LEMMA 4. *Let*

$$M = \{(H_1, K_1), (H_2, K_2), \ldots, (H_r, K_r)\}$$

be a FMM (p^a) *of G. Then $\{K_1 \cap Z(G), K_2 \cap Z(G), \ldots, K_r \cap Z(G)\}$ is an intersection set for $Z(G)$ and G is isomorphic to a subgroup of* $\prod_{i=1}^r G/(K_i \cap Z(G))$.

PROOF. Let $N_i = K_i \cap Z(G)$, $1 \leqq i \leqq r$. Now M is faithful if and only if the G-core of $K_1 \cap K_2 \cap \ldots \cap K_r$ is 1 and this is obviously equivalent to

$$K_1 \cap K_2 \cap \ldots \cap K_r \cap Z(G) = 1 .$$

(If $K_1 \cap K_2 \cap \ldots \cap K_r$ contains a nontrivial normal subgroup of G, this normal subgroup has a nontrivial intersection with $Z(G)$.) So as M is faithful, $N_1 \cap N_2 \cap \ldots \cap N_r = 1$. If for some i, $1 \leqq i \leqq r$,

$$N_1 \cap N_2 \cap \ldots \cap N_{i-1} \cap N_{i+1} \cap \ldots \cap N_r = 1 ,$$

then $\{(H_1, K_1), (H_2, K_2), \ldots, (H_{i-1}, K_{i-1}), (H_{i+1}, K_{i+1}), \ldots, (H_r, K_r)\}$ is a FM (p^a) of G. This contradicts that M is minimal. So $\{N_1, \ldots, N_r\}$ is an intersection set for $Z(G)$. Since $N_1 \cap \ldots \cap N_r = 1$, the homomorphism $x \mapsto (xN_1, \ldots, xN_r)$ from G to $\prod_{i=1}^r G/N_i$ is $1-1$.

As an extension of Theorem 3 of [2] and Hauptsatz 6 of [1] we offer the following:

THEOREM 5. *Let $a \geqq 1$. The length of a* FMM (p^a) *of G is at most $d(Z(G))$. If p is odd, it equals $d(Z(G))$, and if $p=2$, there exists a* FMM (2^a) *of G of length $d(Z(G))$.*

PROOF. Let $M=\{(H_1,K_1),(H_2,K_2),\ldots,(H_r,K_r)\}$ be a FMM (p^a) of G, let $\Omega=\Omega_1(Z(G))$, and define $L_i=\Omega\cap K_i$, $1\leqq i\leqq r$. By Lemma 4 and Lemma 2 $\{L_1,L_2,\ldots,L_r\}$ is an intersection set for Ω. Thus by Proposition 1, $r\leqq d(\Omega)=d(Z(G))$, proving the first statement of Theorem 5. Since $\{L_1,L_2,\ldots,L_r\}$ is an intersection set for Ω, $L_i\nsubseteq\Omega$ for $1\leqq i\leqq r$. Suppose $|\Omega\colon L_i|=p$ for all i, $1\leqq i\leqq r$. Then in the chain

$$\Omega \supset L_1 \supset L_1\cap L_2 \supset \ldots \supset L_1\cap L_2\cap\ldots\cap L_r = 1$$

each subgroup has index exactly p in the preceding. It follows, that $|\Omega|=p^r$. This means that $d(Z(G))=r$, so we have done in this case.

Suppose now $|\Omega\colon L_i|>p$ for some i, say $|\Omega\colon L_1|>p$.

Let $\hat{H}_1=\Omega\cdot H_1$. As $\Omega\subseteqq Z(G)$, we have for the commutator groups

$$[\hat{H}_1,\hat{H}_1] = [H_1,H_1] \subseteqq K_1 .$$

It follows that $K_1\lhd\hat{H}_1$, and that $\hat{H}_1/K_1$ is abelian. Moreover, by an isomorphism theorem

$$\hat{H}_1/K_1 = \Omega H_1/K_1 \supseteqq \Omega K_1/K_1 \cong \Omega/\Omega\cap K_1 = \Omega/L_1 .$$

Now Ω/L_1 is elementary abelian of order at least p^2, so $\hat{H}_1/K_1$ is not cyclic. By the theory of finite abelian groups we can choose a subgroup $\tilde{H}_1\subseteqq\hat{H}_1$, such that

$$\tilde{H}_1/K_1 \cong H_1/K_1\times A/K_1 ,$$

where $|A\colon K_1|=p$. Then obviously $H_1\cap A=K_1$, so

$$\tilde{M} = \{(\tilde{H}_1,H_1),(\tilde{H}_1,A),(H_2,K_2),(H_3,K_3),\ldots,(H_r,K_r)\}$$

is a FM (p^a) of G. Thus the degree of $\tilde{M}$ is greater than the degree of M, i.e.,

$$2\cdot|G\colon\tilde{H}_1| \geqq |G\colon H_1| .$$

This is impossible when p is odd. When $p=2$, equality is possible, so that $\tilde{M}$ and M have the same degree. But the length of $\tilde{M}$ is greater than the length of M. By repeating the above argument we can eventually get a FMM (2^a) of G of length $d(Z(G))$. This proves Theorem 5.

Let us note, that in the case G is abelian we have the following trivial Corollary to Theorem 5:

COROLLARY 6. *Suppose G is abelian, $a \geqq 1$. If there exists a subgroup H of G, such that $\{(H, 1)\}$ is an* FMM (p^a) *of G of maximal length, then $G = Z(G)$ is cyclic.*

(When p is odd one can drop the condition on maximal length in Corollary 6, but not for $p = 2$. See Satz 10 in [1].)

A subgroup H of G is called *primitive*, if there does not exist two subgroups L, N of G with $L \neq H$, $N \neq H$ and $L \cap N = H$. Since we are assuming that G is a p-group, $H \subseteqq G$ is primitive, if and only if, $d(N_G(H)/H) = 1$. This is fairly easy to show. It can for instance be proved by using Proposition 1.

If $M = \{(H_1, K_1), (H_2, K_2), \ldots, (H_r, K_r)\}$ is a FMM (p^a) of G, one may ask whether the subgroups $K_1, \ldots, K_r$ of G are primitive. For $a = 0, 1$, this is true by results of Johnson and Jacobs. However, for $a \geqq 2$, it is generally false, as the following simple example shows. Let

$$D = \langle x, y \mid x^4 = y^2 = 1,\ y^{-1}xy = x^{-1} \rangle$$

be the dihedral group of order 8. As $Z(D) = \langle x^2 \rangle$ is cyclic, a FMM (2^a) of D has length 1 by Theorem 5. If it is $\{(H, K)\}$, then $K \cap Z(D) = 1$, so $K \cap \langle x \rangle = 1$. Now $\{(\langle y, x^2 \rangle, \langle y \rangle)\}$ and $\{(\langle x \rangle, 1)\}$ are both FMM (2^a)'s of D if $a \geqq 2$. But 1 is not a primitive subgroup of D. A similar example exists for odd p. (Take a group of order p^3 and exponent p^2).

However, we can prove the following result for all $a \geqq 1$, which puts some restriction on the K_i's of a FMM (p^a) of G.

PROPOSITION 7. *Let $M = \{(H_1, K_1), (H_2, K_2), \ldots, (H_r, K_r)\}$ be a* FMM (p^a) *of G of maximal length, $a \geqq 1$. Let $1 \leqq i \leqq r$. If $N_i = N_G(K_i)$ and $\tilde{N}_i$ is a subgroup of N_i containing $H_i \cdot Z(G)$, then $\{(H_i/K_i, 1)\}$ is a* FMM (p^a) *of $\tilde{N}_i/K_i$ of maximal length. The center of $\tilde{N}_i/K_i$ is cyclic. In particular, if N_i/K_i is abelian, it is cyclic.*

PROOF. We assume $i = 1$. Suppose that $\{(H_1/K_1, 1)\}$ is not a FMM (p^a) of $\tilde{N}_1/K_1$. It is obviously a FM (p^a). Let

$$\bar{M} = \{(\bar{R}_1, \bar{S}_1), (\bar{R}_2, \bar{S}_2), \ldots, (\bar{R}_t, \bar{S}_t)\}$$

be a FMM (p^a) of $\tilde{N}_1/K_1$. If Z_1 is defined by $Z_1/K_1 = Z(\tilde{N}_1/K_1)$ and R_j, S_j by

$$R_j/K_1 = \bar{R}_j, \quad S_j/K_1 = \bar{S}_j, \quad 1 \leqq j \leqq t,$$

then $Z(G) \subseteqq Z_1$, (since $Z(G) \subseteqq \tilde{N}_j$ by assumption), and

$$(*) \qquad Z_1 \cap S_1 \cap S_2 \cap \ldots \cap S_t = K_1 ,$$

(since $\bar{M}$ is faithful).

Now consider

$$M' = \{(R_1, S_1), (R_2, S_2), \ldots, (R_t, S_t), (H_2, K_2), (H_3, K_3), \ldots, (H_r, K_r)\}$$

as a monomial p^a-representation of G. By (*)

$$\begin{aligned}(S_1 \cap \ldots \cap S_t) \cap (K_2 \cap \ldots \cap K_r) \cap Z(G) \\ &= ((S_1 \cap \ldots \cap S_t \cap Z_1) \cap Z(G)) \cap (K_2 \cap \ldots \cap K_r) \\ &= K_1 \cap K_2 \cap \ldots \cap K_r \cap Z(G) \\ &= 1 ,\end{aligned}$$

because M is faithful. Thus M' is faithful. Moreover, since $\bar{M}$ is a FMM (p^a) of $\tilde{N}_1/K_1$,

$$|\tilde{N}_1 \colon H_1| > |\tilde{N}_1 \colon R_1| + |\tilde{N}_2 \colon R_2| + \ldots + |\tilde{N}_2 \colon R_t| ,$$

so multiplying by $|G \colon \tilde{N}_1|$ gives

$$|G \colon H_1| > |G \colon R_1| + |G \colon R_2| + \ldots + |G \colon R_t| .$$

We now have a contradiction to the assumption, that M is minimal. Thus $\{(H_1/K_1), 1\}$ is a FMM (p^a) of $\tilde{N}_1/K_1$. A similar argument shows, that since M is of maximal length, the same is true for $\{(H_1/K_1, 1)\}$. We can now apply Theorem 5 to get the rest of the statements of Proposition 7.

If $i \in \mathbf{Z}$ we define

$$\{p^i\} = \begin{cases} p^i, & \text{if } i \geqq 0 \\ 1, & \text{if } i \leqq 0 . \end{cases}$$

We finish this note by computing $\mu(G, p^a)$, if G is abelian. (In [1], this was done for $d(G) = 2$ or $a = 1$).

THEOREM 8. *If $a \geqq 1$ and G is abelian of type $(p^{a_1}, \ldots, p^{a_r})$, then*

$$\mu(G, p^a) = \sum_{j=1}^{r} \{p^{a_j - a}\} .$$

PROOF. Let $M = \{H_1, K_1), (H_2, K_2), \ldots, (H_r, K_r)\}$ be a FMM (p^a) of G of maximal length (cf. Theorem 5!). Let $1 \leqq i \leqq r$. Since G is abelian, $N_G(K_i) = G$, and therefore G/K_i is cyclic by Proposition 7. It is easy to see, that

$$|G: H_i| = \left\{\frac{|G: K_i|}{p^a}\right\}.$$

By Lemma 4 we may consider G as a subgroup of $\prod_{j=1}^{r} G/K_j$. By a well-known theorem on abelian group we get, that after possibly reordering the a_j's, we have $p^{a_i} \mid |G: K_i|$, $1 \leqq i \leqq r$. Thus

$$\{p^{a_i - a}\} \leqq \left\{\frac{|G: K_i|}{p^a}\right\}, \qquad 1 \leqq i \leqq r.$$

By assumption M is minimal, so

$$\mu(G, p^a) = \sum_{j=1}^{r} |G: H_j| = \sum_{j=1}^{r} \left\{\frac{|G: K_j|}{p^a}\right\} \geqq \sum_{j=1}^{r} \{p^{a_i - a}\}$$

proving one inequality. The other inequality is trivial for $r=1$, and for arbitrary r it then follows from Lemma 3.

One final remark: It is easy to prove that for an arbitrary finite group G and $a \geqq 0$

$$p^a \mu(G, p^a) \geqq \mu(G) \geqq \mu(G, p^a)$$

and that these bounds are the best possible.

REFERENCES

1. H.-P. Jacobs, *Minimale monomiale Darstellungen endlicher Gruppen*, Dissertation, Universität Dortmund, 1975.
2. D. L. Johnson, *Minimal permutation representations of finite groups*, Amer. J. Math. 93 (1971), 857–866.

ABTEILUNG MATHEMATIK
UNIVERSITÄT DORTMUND
W. GERMANY