A Strict Inequality for a Minimal Degree of a Direct Product

Neil Saunders

August 7, 2007

Abstract

The minimal faithful permutation degree $\mu(G)$ of a finite group G is the least non-negative integer n such that G embeds in the symmetric group $Sym(n)$. Work of Johnson and Wright in the 1970's established conditions for when $\mu(H \times K) = \mu(H) + \mu(K)$, for finite groups H and K. Wright asked whether this is true for all finite groups. A counter-example of degree 15 was provided by the referee and was added as an addendum in Wright's paper. Here we provide a counter-example of degree 12.

1 Introduction

The minimal faithful permutation degree $\mu(G)$ of a finite group G is the least non-negative integer n such that G embeds in the symmetric group $Sym(n)$. It is well known that $\mu(G)$ is the smallest value of $\sum_{i=1}^{n} |G : G_i|$ for a collection of subgroups $\{G_1, \ldots, G_n\}$ satisfying $\bigcap_{i=1}^{n} \operatorname{core}(G_i) = \{1\}$, where $\operatorname{core}(G_i) = \bigcap_{g \in G} G_i^g$.

We first give a theorem due to Karpilovsky [2] which will be needed later. The proof of it can be found in [3] or [6].

Theorem 1.1. *Let A be a non-trivial finite abelian group and let $A \cong A_1 \times \ldots \times A_n$ be its direct product decomposition into non-trivial cyclic groups of prime power order. Then*

$$\mu(A) = a_1 + \ldots + a_n,$$

where $|A_i| = a_i$ *for each* i.

One of the themes of Johnson and Wright's work was to establish conditions for when

$$\mu(H \times K) = \mu(H) + \mu(K) \tag{1}$$

for finite groups H and K. The next result is due to Wright [8].

Theorem 1.2. *Let* G *and* H *be non-trivial nilpotent groups. Then* $\mu(G \times H) = \mu(G) + \mu(H)$.

Further in [8], Wright constructed a class of groups $\mathscr{C}$ with the property that for all $G \in \mathscr{C}$, there exists a nilpotent subgroup G_1 of G such that $\mu(G_1) = \mu(G)$. It is a consequence of Thereom (1.2) that $\mathscr{C}$ is closed under direct products and so (1) holds for any two groups $H, K \in \mathscr{C}$. Wright proved that $\mathscr{C}$ contains all nilpotent, symmetric, alternating and dihedral groups, however the extent of it is still an open problem. In [1], Easdown and Praeger showed that (1) holds for all finite simple groups.

The counter-example to (1) was provided by the referee in Wright's paper [8] and involved subgroups of the standard wreath product $C_5 \wr Sym(3)$, specifically the group $G(5, 5, 3)$ which is a member of a class of unitary reflection groups. We give a brief exposition on these groups now.

Let m and n be positive integers, let C_m be the cyclic group of order m and $B = C_m \times \ldots \times C_m$ be the product of n copies of C_m. For each divisor p of m define the group $A(m, p, n)$ by

$$A(m, p, n) = \{(\theta_1, \theta_2, \ldots, \theta_n) \in B \mid (\theta_1\theta_2 \ldots \theta_n)^{m/p} = 1\}.$$

It follows that $A(m, p, n)$ is a subgroup of index p in B and the symmetric group $Sym(n)$ acts naturally on $A(m, p, n)$ by permuting the coordinates.

$G(m, p, n)$ is defined to be the semidirect product of $A(m, p, n)$ by $Sym(n)$. It follows that $G(m, p, n)$ is a normal subgroup of index p in $C_m \wr Sym(n)$ and thus has order $m^n n!/p$.

It is well known that these groups can be realized as finite subgroups of $GL_n(\mathbb{C})$, specifically as $n \times n$ matrices with exactly one non-zero entry, which is a complex mth root of unity, in each row and column such that the product of the entries is a complex (m/p)th root of unity. Thus the groups $G(m, p, n)$

are sometimes referred to as monomial reflection groups. For more details on the groups $G(m, p, n)$, see [4].

2 Calculation of $\mu(G(4,4,3))$

Recall that $G(4,4,3) = A(4,4,3) \rtimes Sym(3)$, where

$$A(4,4,3) = \{(\theta_1, \theta_2, \theta_3) \in C_4 \times C_4 \times C_4 \mid \theta_1\theta_2\theta_3 = 1\}$$

which is isomorphic to a product of two copies of the cyclic group of order 4. Hence

$$G(4,4,3) \cong (C_4 \times C_4) \rtimes Sym(3).$$

From now on, we will let G denote $G(4,4,3)$. A presentation for this group can be given thus

$$G = \langle x, y, a, b | x^4 = y^4 = b^3 = a^2 = 1, xy = yx, x^a = y, x^b = y, y^b = x^{-1}y^{-1}, b^a = b^{-1}\rangle.$$

Since $\langle x, y\rangle \cong C_4 \times C_4$ is a proper subgroup of G we have by Theorem 1.1, that $8 = \mu(\langle x, y\rangle) \leq \mu(G)$. Moreover since G is a proper subgroup of the wreath product $W := C_4 \wr Sym(3)$, for which $\mu(W) = 12$, we have the inequalities

$$8 \leq \mu(G) \leq 12.$$

We will prove that in fact $\mu(G) = 12$ by a sequence of lemmas.

Lemma 2.1. *$\langle x^2, y^2\rangle$ is the unique minimal normal subgroup of G.*

Proof. Observe by the conjugation action of a and b on x^2 and y^2 that $M = \langle x^2, y^2\rangle$ is indeed normal in G. Let N be a non-trivial normal subgroup of G so there exists an

$$\alpha = x^i y^j b^k a^l$$

in N where $i, j \in \{0, 1, 2, 3\}$, $k \in \{0, 1, 2\}$, $l \in \{0, 1\}$ are not all zero. It remains to show that M is contained in N.

Case (a): $k = l = 0$.
Subcase (i): $i = j$ so $\alpha = x^i y^i$.

Then $\alpha\alpha^b = x^i y^i y^i x^{-i} y^{-i} = y^i \in N$, so $y^{-i}\alpha = x^i \in N$. But $i \neq 0$, so $M \subseteq \langle x^i, y^i\rangle$. Hence $M \subseteq N$, as required.

Subcase (ii): $i + j \not\equiv 0 \bmod 4$.

Then $\alpha\alpha^a = x^{i+j}y^{i+j}$ and we are back in Subcase (i).

Subcase (iii): $i + j \equiv 0 \bmod 4$.

Then $\alpha\alpha^b = x^{i-j}y^i$. If $2i - j \not\equiv 0 \bmod 4$, then we are back in Subcase (ii), so suppose $2i \equiv j \bmod 4$. Then together with $i + j \equiv 0 \bmod 4$ it follows that $i = 0$. Therefore j is zero and α is trivial. This completes case (a).

Case (b): $k \neq 0$ or $l \neq 0$.
Subcase (i): $l = 0$ so $k \neq 0$

Then $\alpha\alpha^{-b} = x^iy^jb^k(x^{-j}y^{i-j}b^k)^{-1} = x^{i+j}y^{2j-i}$. If $i + j \not\equiv 0$ or $2j - i \not\equiv 0 \bmod 4$, then we are back in Case (a) so suppose $i + j \equiv 2j - i \equiv 0 \bmod 4$. Solving gives $i = j = 0$ and so $\alpha = b^k$, whence $\langle b \rangle \in N$. Hence

$$b^{-1}b^x = b^{-1}x^{-1}bx = y^{-1}x \in N$$

and we are back in Case (a).

Subcase (ii): $l \neq 0$ and $k \neq 0$.

Then $\alpha\alpha^{-a} = x^iy^jb^ka^l(x^jy^ib^{-k}a^l)^{-1} = x^iy^jb^ka^la^{-l}b^kx^{-j}y^{-i} = x^py^qb^{2k}$ where $p, q \in \{0, 1, 2, 3\}$ and we are back in Subcase (i), replacing k by $2k$.

Subcase (iii): $k = 0$ so $l = 1$
Then

$$\alpha\alpha^{-b} = x^iy^ja(x^iy^ja)^{-b} = x^py^qb^2$$

for some $p, q \in \{0, 1, 2, 3\}$ and again we are back in Subcase (i).

This completes the proof. □

It is worth observing at this point that Lemma 2.1 tells us that any minimal faithful representation of G is necessarily transitive. That is, any minimal faithful collection of subgroups $\{G_1, \ldots, G_n\}$ is just a single core-free subroup.

Lemma 2.2. *Elements of $\langle x, y \rangle b$ and $\langle x, y \rangle b^2$ have order 3. All other elements of G have order dividing by 8.*

Proof. It is a routine calculation to show that any element of the form $\alpha = x^i y^j b^k$ for k nonzero has order three. Now suppose $\alpha = x^i y^j b^k a^l$ where l is nonzero. Then $l = 1$ and we have

$$\alpha^2 = x^p y^q (b^k a)^2 = x^p y^q,$$

for some p, q, which has order dividing 4. Therefore α has order dividing 8. □

It is an immediate consequence that G does not contain any element of order 6.

Lemma 2.3. *If L is a core-free subgroup of G then $|G : L| \geq 12$.*

Proof. Suppose for a contradiction that $\text{core}(L) = \{1\}$ and $|G : L| < 12$. Since $|G| = 96$, $|L| > 8$. However, if $|L| > 12$ then $|G : L| < 8$ and so $\mu(G) < 8$ contradicting that $\mu(G) \geq 8$. Therefore $|L| = 12$ and so by the classification of groups of order 12, see [5], L is isomorphic to one of the following groups

$$L \cong \begin{cases} C_{12} \\ C_6 \times C_2 \\ A_4 \\ D_6 \\ T = \langle s, t \mid s^6 = 1, s^3 = t^2, sts = s \rangle \end{cases}$$

Notice that the groups $C_{12}, C_6 \times C_2, D_6$ and T each contain an element of order 6 and so cannot be isomorphic to L by Lemma 2.2.

Hence L is isomorphic to A_4 and so we can find two non-commuting elements $\alpha = x^i y^j b^k$ and $\beta = x^s y^t b^r$ of order three that generate it such that $\alpha\beta$ has order two. Now

$$\alpha\beta = x^p y^q b^{k+r}$$

for some $p, q \in \{0, 1, 2, 3\}$ and so $k + r \equiv 0 \bmod 3$ by Lemma 2.2. Without loss of generality let $k = 1$. Now

$$\alpha\beta = \begin{cases} x^2 \\ y^2 \\ x^2 y^2 \end{cases}$$

and upon conjugation by $\alpha = x^i y^j b$, we get respectively,

$$(\alpha\beta)^\alpha = \begin{cases} y^2 \\ x^2y^2 \\ x^2. \end{cases}$$

So in each case we get $\langle x^2, y^2\rangle \subseteq L$, contradicting that L is core-free. $\square$

Combining the above lemmas we find that any minimal faithful representation of G is necessarily transitive and that any faithful transitive representation has degree at least 12. Therefore we have $12 \le \mu(G)$. But $\mu(G) \le 12$. Therefore we have proved the following:

Theorem 2.4. *The minimal faithful permutation degree of $G(4,4,3)$ is 12.*

3 G(4,4,3) forms a Counter-Example of Degree 12

Let $W = C_4 \wr Sym(3)$ be the wreath product of the cyclic group of order 4 by the symmetric group on 3 letters. Observe at this point that since the base group of W is $C_4 \times C_4 \times C_4$, and $\mu(C_4 \times C_4 \times C_4) = 12$ by Theorem 1.1, $\mu(W) = 12$. Let $\gamma_1, \gamma_2, \gamma_3$ be generators for the base group of W and let $a = (23), b = (123)$ be generators for $Sym(3)$ acting coordinate-wise on the base group. It follows that $\gamma := \gamma_1\gamma_2\gamma_3$ commutes with a and b and thus lies in the centre of W. Let $H = \langle\gamma\rangle$, so $\mu(H) = 4$.

Set $x = \gamma_1^{-1}\gamma_2^2\gamma_3^{-1}$ and $y = \gamma_1^{-1}\gamma_2^{-1}\gamma_3^2$. Then it readily follows that

$$x^a = x^b = y,\ y^a = x,\ y^b = x^{-1}y^{-1},$$

so that $G = \langle x, y, a, b\rangle$ is isomorphic to $G(4,4,3)$. Moreover with a little calculation, it can be shown that $G \cap H = \{1\}$.

It now follows that W is an internal direct product of G and H. Therefore by Theorem 2.4, we have

$$12 = \mu(G \times H) < \mu(G) + \mu(H) = 16$$

and so G and H form a counter-example to (1) of degree 12.

Finally, we remark that using the result from [7] that $\mu(G(p,p,p)) = p^2$ for p a prime, it follows that $\mu(G(3,3,3)) = 9$. However the centralizer, $C_{Sym(9)}(G(3,3,3))$ in $Sym(9)$ is a proper subgroup of $G(3,3,3)$. So it is not possible to get a counter-example to (1) of degree 9 in this case, by this method.

Similarly by realizing $G(2,2,3)$ as $Sym(4)$, it is immediate that $\mu(G(2,2,3)) = 4$ and again a counter-example to (1) of degree 4 is impossible by this method.

References

[1] D. Easdown and C.E Praeger. On minimal faithful permutation representations of finite groups. *Bull. Austral. Math. Soc.*, 38:207–220, 1988.

[2] Karpilovsky G.I. The least degree of a faithful representation of abelian groups. *Vestnik Khar'kov Gos. Univ*, 53:107–115, 1970.

[3] D.L. Johnson. Minimal permutation representations of finite groups. *Amer. J. Math.*, 93:857–866, 1971.

[4] Peter Orlik and Hiroaki Terao. *Arrangements and Hyperplanes*. Springer-Verlag, 1992.

[5] John Pedersen. *Groups of Small Order*. University of South Florida, Online Notes, http://www.math.usf.edu/ eclark/algctlg/small_groups.html, 2005.

[6] N. Saunders. *Minimal Faithful Permutation Representations of Finite Groups*. (Honours Thesis), University of Sydney, 2005.

[7] Neil Saunders. *The Minimal Degree for a Class of Finite Complex Reflection Groups*. Preprint, 2007.

[8] D. Wright. Degrees of minimal embeddings of some direct products. *Amer. J. Math.*, 97:897–903, 1975.