Bull. Aust. Math. Soc. **79** (2009), 23–30
doi:10.1017/S0004972708000956

STRICT INEQUALITIES FOR MINIMAL DEGREES OF DIRECT PRODUCTS

NEIL SAUNDERS

(Received 17 March 2008)

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 $\mathrm{Sym}(n)$. Work of Johnson and Wright in the 1970s 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 two counter-examples; one of degree 12 and the other of degree 10.

2000 *Mathematics subject classification*: primary 20B35; secondary 51F15.

Keywords and phrases: faithful permutation representations, complex reflection groups, monomial reflection groups.

1. Introduction

The minimal faithful permutation degree $\mu(G)$ of a finite group G is the least nonnegative integer n such that G embeds in the symmetric group $\mathrm{Sym}(n)$. 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 $\bigcap_{i=1}^{n} \mathrm{core}(G_i) = \{1\}$, where $\mathrm{core}(G_i) = \bigcap_{g \in G} G_i^g$.

We first give a theorem due to Karpilovsky [3] which will be needed later. Its proof can be found in [2] or [7].

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

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

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

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

$$\mu(H \times K) = \mu(H) + \mu(K) \tag{1.1}$$

for finite groups H and K. The next result is due to Wright [9].

THEOREM 1.2. *Let G and H be nontrivial nilpotent groups. Then* $\mu(G \times H) = \mu(G) + \mu(H)$.

Wright [9] 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 Theorem 1.2 that $\mathscr{C}$ is closed under direct products and so (1.1) 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 (1.1) holds for all finite simple groups.

The counter-example to (1.1) was provided by the referee in Wright's paper [9] and involved subgroups of the standard wreath product $C_5 \wr \mathrm{Sym}(3)$, specifically the group $G(5, 5, 3)$ which is a member of a class of unitary reflection groups. We now give a brief exposition on these groups.

Let m and n be positive integers, let C_m be the cyclic group of order m and $B = C_m \times \cdots \times C_m$ 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 $\mathrm{Sym}(n)$ acts naturally on $A(m, p, n)$ by permuting the coordinates.

The group $G(m, p, n)$ is defined to be the semidirect product of $A(m, p, n)$ by $\mathrm{Sym}(n)$. It follows that $G(m, p, n)$ is a normal subgroup of index p in $C_m \wr \mathrm{Sym}(n)$ 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 [5].

1.1. A note on cyclotomic polynomials The following definition and result is taken from [4].

DEFINITION 1.3. For r a prime number, the polynomial

$$Q_r(x) = 1 + x + x^2 + \cdots + x^{r-1}$$

is called the rth *cyclotomic polynomial*. The roots of this polynomial are nontrivial rth roots of unity.

THEOREM 1.4. *Let $\mathbb{F}_q$ be a finite field of q elements and let n be a positive integer coprime to q. Then the polynomial $Q_n(x)$ factors into $(\phi(n))/d$ distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree d, where d is the least positive integer such that $q^d \equiv 1 \bmod n$ and ϕ is the Euler's phi function.*

Thus for r a prime, $Q_r(x)$ splits into $(r-1)/d$ monic irreducible factors, where d is the multiplicative order of r in the group of units $(\mathbb{Z}/n\mathbb{Z})^*$.

https://doi.org/10.1017/S0004972708000956 Published online by Cambridge University Press

We shall use this result in the next section when we calculate the minimal degree of $G(2, 2, 5)$.

2. Calculation of minimal degrees

2.1. Calculation of $\mu(G(4, 4, 3))$ Recall that $G(4, 4, 3) = A(4, 4, 3) \rtimes \mathrm{Sym}(3)$, 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

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

From now on, we shall 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, then, by Theorem 1.1, $8 = \mu(\langle x, y\rangle) \leq \mu(G)$. Moreover, since G is a proper subgroup of the wreath product $W := C_4 \wr \mathrm{Sym}(3)$, for which $\mu(W) = 12$, then we have the inequalities

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

We shall 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 nontrivial 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 that $2i \equiv j \bmod 4$. Then, together with $i + j \equiv 0 \bmod 4$, it follows that $i = 0$. Therefore j is zero and α is trivial, a contradiction. This completes case (a).

https://doi.org/10.1017/S0004972708000956 Published online by Cambridge University Press

CASE (b): $k \neq 0$ or $l \neq 0$.
Subcase (i): $l = 0$ so $k \neq 0$. Then $\alpha\alpha^{-b} = x^i y^j b^k (x^{-j} y^{i-j} b^k)^{-1} = x^{i+j} y^{2j-i}$. If $i + j \not\equiv 0$ or $2j - i \not\equiv 0$ mod 4, then we are back in case (a) so suppose that $i + j \equiv 2j - i \equiv 0$ mod 4. Solving gives $i = j = 0$ and so $\alpha = b^k$, whence $\langle b \rangle \in N$. Hence

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

and we are back in case (a).
Subcase (ii): $l \neq 0$ and $k \neq 0$. Then

$$\alpha\alpha^{-a} = x^i y^j b^k a^l (x^j y^i b^{-k} a^l)^{-1} = x^i y^j b^k a^l a^{-l} b^k x^{-j} y^{-i} = x^p y^q b^{2k}$$

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

$$\alpha\alpha^{-b} = x^i y^j a (x^i y^j a)^{-b} = x^p y^q b^2$$

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 representation is given by just a single core-free subgroup.

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* 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 3. Now suppose that $\alpha = x^i y^j b^k a^l$, where l is nonzero. Then $l = 1$ and

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

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 $\mathrm{core}(L) = \{1\}$ and $|G : L| < 12$. Since $|G| = 96$, $|L| > 8$. However, if $|L| > 12$ then $|G : L| < 8$ and so $\mu(G) < 8$, contradicting the fact that $\mu(G) \geq 8$. Therefore $|L| = 12$ and so, by the classification of groups of order 12 (see [6]), L is isomorphic to one of the following groups:

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

https://doi.org/10.1017/S0004972708000956 Published online by Cambridge University Press

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 noncommuting elements $\alpha = x^i y^j b^k$ and $\beta = x^s y^t b^r$ of order 3 that generate it such that $\alpha\beta$ has order 2. 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, we get three possibilities:

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

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

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

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

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, $12 \le \mu(G)$. But $\mu(G) \le 12$, so we have proved the following.

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

2.2. Calculation of $\mu(G(2, 2, 5))$ In this section, let G and A denote the groups $G(2, 2, 5)$ and $A(2, 2, 5)$ respectively. Let c_1, c_2, c_3, c_4 be the generators of the base group A and let $b = (1\,2\,3\,4\,5)$ be the 5-cycle in $\mathrm{Sym}(5)$. Define a subgroup H of G by

$$H := \langle c_1, c_2, c_3, c_4, b \rangle = A \rtimes \langle b \rangle.$$

Then it can easily be proved that H is isomorphic to

$$(C_2 \times C_2 \times C_2 \times C_2) \rtimes C_5$$

and, furthermore, we may treat A as a four-dimensional $\langle b \rangle$-module over the finite field $\mathbb{F}_2$. The element b acts on the generators of the base group thus:

$$c_1^b = c_2, \quad c_2^b = c_3, \quad c_3^b = c_4, \quad c_4^b = c_1 c_2 c_3 c_4.$$

The matrix of this action with respect to this basis is the companion matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

and so the minimal polynomial for this action is the cyclotomic polynomial $Q_5(\lambda) = 1 + \lambda + \lambda^2 + \lambda^3 + \lambda^4$. By Theorem 1.4, $Q_5(\lambda)$ splits into $(\phi(5))/d$ monic irreducible polynomials of degree d, where d is the multiplicative order of 2 mod 5. So in this particular case, since $\phi(5) = d = 4$, $Q_5(\lambda)$ is irreducible over $\mathbb{F}_2$. This shows that A is a minimal normal subgroup of H, and we prove below that it is the unique minimal normal subgroup of H.

PROPOSITION 2.5. *A is the unique minimal normal subgroup of H.*

PROOF. It suffices to show that A is contained in every nontrivial normal subgroup of H. Let N be a nontrivial normal subgroup of H and suppose that N does not contain A. Then, by normality, the group AN is the internal direct product of A with N. Since A is maximal in H, we must have that $AN = H$ and so every nontrivial element not contained in A centralizes A. But b is not contained in A and we have $c_1 b = c_2 b$, a contradiction. □

It is immediate from this proposition that every minimal faithful representation of H is transitive and thus given by a single core-free subgroup.

PROPOSITION 2.6. *If L is a nontrivial core-free subgroup of H, then $|H : L| \geq 10$.*

PROOF. Suppose that L is a core-free subgroup of H whose index is strictly less than 10. Since $8 \leq \mu(H) \leq 10$,

$$8 \leq |H : L| < 10.$$

Moreover, since $|H| = 2^4.5$, we can deduce that $|L| = 10$ and this forces L to be either the cyclic group or the dihedral group of order 10.

If L is the dihedral group, then there is an element of order 2 which normalizes and hence inverts the element of order 5. Observe that any element of order 5 has the form ab^j, where $a \in A$ and $1 \leq j \leq 4$. Since H is the semidirect product of A with $\langle b \rangle$, all elements of order 2 are contained in A, of which none can invert b.

Suppose now that L is the cyclic group of order 10. Then there is an element of order 5 commuting with an element of order 2. We may treat this element of order 2 as a 1-eigenvector for the element b. However, this contradicts that fact that 1 is not a solution to $Q_5(\lambda)$ in $\mathbb{F}_2$. Therefore no such L can exist and we have proved the proposition. □

The above results immediately prove the following.

THEOREM 2.7. *The minimal faithful permutation degree of $G(2, 2, 5)$ is* 10.

3. G(4,4,3) forms a counter-example of degree 12

As above, let $W = C_4 \wr \mathrm{Sym}(3)$ be the wreath product. 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 $a = (2\ 3)$, $b = (1\ 2\ 3)$ be generators for $\mathrm{Sym}(3)$ acting coordinatewise 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

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

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,

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

and so G and H form a counter-example to (1.1) of degree 12.

4. G(2,2,5) forms a counter-example of degree 10

In this section, we let U be the wreath product $C_2 \wr \mathrm{Sym}(5)$. Let $\theta_1, \theta_2, \theta_3, \theta_4, \theta_5$ generate the base group of U and let $a = (1\ 2)$ and $b = (1\ 2\ 3\ 4\ 5)$ be generators for $\mathrm{Sym}(5)$ action coordinatewise on the base group. Let

$$c_1 = \theta_1\theta_2, \quad c_2 = \theta_2\theta_3, \quad c_3 = \theta_3\theta_4, \quad c_4 = \theta_4\theta_5.$$

Then it can be easily proved that $G := \langle c_1, c_2, c_3, c_4, b, a \rangle$ is isomorphic to the group $G(2, 2, 5)$. Let $\theta = \theta_1\theta_2\theta_3\theta_4\theta_5$ and set $K := \langle \theta \rangle$. Then with a little calculation it can be shown that $G \cap K = \{1\}$ and that G and K centralize each other in U. So U is the internal direct product of G with K and so by Theorem 2.7,

$$10 = \mu(G \times K) < \mu(G) + \mu(K) = 10 + 2 = 12$$

and we get a counter-example of degree 10.

Finally, we remark that using the result from [8] that $\mu(G(p, p, p)) = p^2$ for p a prime, it follows that $\mu(G(3, 3, 3)) = 9$. However, the centralizer $C_{\mathrm{Sym}(9)}(G(3, 3, 3))$ in $\mathrm{Sym}(9)$ is a proper subgroup of $G(3, 3, 3)$. So it is not possible to get a counter-example to (1.1) of degree 9 in this case, by this method.

Similarly, by realizing $G(2, 2, 3)$ as $\mathrm{Sym}(4)$, it is immediate that $\mu(G(2, 2, 3)) = 4$ and again a counter-example to (1.1) of degree 4 is impossible by this method.

The author does not know whether 10 is the minimal degree of any counter-example. Furthermore, the author is not aware of any examples where, for two groups G and H,

$$\min\{\mu(G), \mu(H)\} < \mu(G \times H) < \mu(G) + \mu(H).$$

https://doi.org/10.1017/S0004972708000956 Published online by Cambridge University Press

References

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

[2] D. L. Johnson, 'Minimal permutation representations of finite groups', *Amer. J. Math.* **93** (1971), 857–866.

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

[4] R. Lidl and H. Niederreiter, *Finite Fields* (Cambridge University Press, Cambridge, 1997).

[5] P. Orlik and H. Terao, *Arrangements of Hyperplanes* (Springer, Berlin, 1992).

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

[7] N. Saunders, 'Minimal faithful permutation representations of finite groups', Honours Thesis, University of Sydney, 2005.

[8] ———, 'The minimal degree for a class of finite complex reflection groups', Preprint, 2008.

[9] D. Wright, 'Degrees of minimal embeddings of some direct products', *Amer. J. Math.* **97** (1975), 897–903.

NEIL SAUNDERS, School of Mathematics and Statistics, University of Sydney,
NSW 2006, Australia
e-mail: neils@maths.usyd.edu.au

https://doi.org/10.1017/S0004972708000956 Published online by Cambridge University Press