# Minimal faithful permutation degrees of finite groups

Neil Saunders*

**Abstract**

We calculate the minimal degree for a class of finite complex reflection groups $G(p, p, q)$, for $p$ and $q$ primes and establish relationships between minimal degrees when these groups are taken in a direct product.

## 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 $Sym(n)$. That is, $\mu(G)$ is the degree of the smallest faithful permutation representation of $G$, where a permutation representation is a group homomorphism from $G$ to $Sym(X)$ for some set $X$.

It is well known that when a group $G$ acts on a finite set $X$, the $G$-orbits induce an equivalence relation on $X$ and we can write

$$X = X_1 \sqcup \ldots \sqcup X_r,$$

where each $X_i$ represents a $G$-orbit.

The restriction of $G$ to one of its orbits on $X_i$ is *transitive* and we can easily verify that this action is equivalent to a right action on a set of cosets $G/G_i$ where $G_i$ is the stabiliser of a point in $X_i$.

Specifically, fix a point $x_i \in X_i$ and define a map $\theta$ from $X_i$ to $G/G_i$ by $\theta(x) = G_i h$ where $h \in G$ and $x_i h = x$. It is easy to see that Figure 1 commutes for all $x \in X_i$ and $g \in G$.

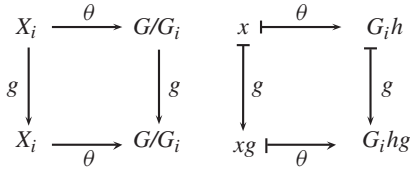


**Figure 1.**

Received 19 March 2008; accepted for publication 24 September 2008.
*School of Mathematics and Statistics, University of Sydney, NSW 2006.
E-mail: neils@maths.usyd.edu.au

Neil Saunders was joint winner of the B.H. Neumann Prize for best student talk (for his presentation of this paper) at the Annual Meeting of the AustMS, held in Melbourne in September 2007.

The kernel of the action of $G$ on $G/G_i$ is the subgroup $\bigcap_{g\in G} g^{-1}G_ig$ called the *core* of $G_i$, denoted by $\mathrm{core}(G_i)$. This is the largest normal subgroup of $G$ that is contained in $G_i$. We call $G_i$ *core-free* if $\mathrm{core}(G_i)$ is trivial.

Given that each permutation representation is a disjoint union of transitive representations which are equivalent to right actions on a set of cosets, we may abbreviate the information defining this permutation representation of $G$ on $X$ by the list $\{G_1,\dots,G_r\}$ where each $G_i$ represents the stabliser of a point in the orbit $X_i$. We will often denote such a collection of subgroups by $\mathcal{R}$ and refer to it as the representation of $G$. The elements of $\mathcal{R}$ are called *transitive constituents* and if $\mathcal{R}$ consists of just one subgroup $G_0$ say, then we say that $\mathcal{R}$ is transitive, in which case $G_0$ is core-free by faithfulness.

We may now restate the definition of the minimal faithful permutation degree of a finite group $G$.

$$\boxed{\begin{array}{l}\mu(G) \text{ is the smallest value of } \sum_{i=1}^{n} |G\colon G_i| \text{ for a collection of}\\ \text{subgroups } \mathcal{R} = \{G_1,\dots,G_n\} \text{ satisfying } \bigcap_{i=1}^{n} \mathrm{core}(G_i) = \{1\}\end{array}}$$

Thus the problem of finding the minimal permutation degree of a finite group presents a dichotomy relating to its lattice of subgroups. On the one hand we want to include as many subgroups in the collection so we can satisfy the condition that the intersection of their cores has to be trivial. On the other hand, we would like this collection to be as small as possible and the subgroups to be as large as possible so the the sum of their indices is minimised. If any member of $\mathcal{R}$ is core-free, then the other members of $\mathcal{R}$ are superfluous, so in fact $\mathcal{R}$ is then transitive.

The study of this topic dates back to Johnson [2] where he proved that one can construct a minimal faithful representation $\{G_1,\dots,G_n\}$ consisting entirely of so called *primitive* groups. These are groups which cannot be expressed as the intersection of groups that properly contain them.

We give a few examples of calculating the minimal degree when we have full access to the subgroup lattice.

*Example* 1. Let $G = C_{p^m}$ the cyclic group of order $p^m$ where $p$ is a prime number and $m$ an non-negative integer. Then the lattice of subgroups forms a chain so the identity subgroup is the only core-free subgroup of $G$. For example, the lattice of subgroups for $C_{p^3}$ is shown in Figure 2.

**Figure 2.** $\mathcal{L}(C_{p^3})$

It follows that the minimal faithful representation for any cyclic group of prime power order $p^m$ is given by the identity subgroup and so $\mu(G) = p^m$.

*Example* 2. Let $G = D_4$ the dihedral group of order 8. Then its lattice of subgroups is as shown in Figure 3, where the normal subgroups are represented by filled dots and each edge represents a subgroup of index two.

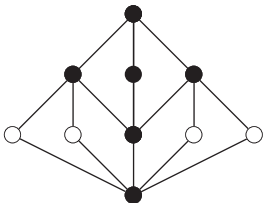

**Figure 3.** $\mathcal{L}(D_4)$

Suppose $\mathcal{R}$ is a minimal faithful collection of subgroups of $D_4$. By examining the lattice of subgroups, if $\mathcal{R}$ contained a normal subgroup and $\mathcal{R}$ did not contain the trivial subgroup, then it would also have to contain a non-normal subgroup. All non-normal subgroups are core-free of index 4 and so $\mathcal{R}$ is transitive. Therefore $\mu(D_4) = 4$.

*Example* 3. Let $G = Q_8 = \langle x, y \mid x^4 = 1, x^2 = y^2, x^y = x^{-1} \rangle$, the quaternion group of order 8. Its lattice of subgroups is shown in Figure 4 and all subgroups are normal.

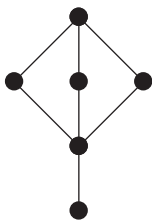

**Figure 4.** $\mathcal{L}(Q_8)$

Thus $Q_8$, like cyclic groups of prime power order, has a unique minimal normal non-trivial subgroup. Hence, any minimal faithful collection of subgroups for $Q_8$ must consist of only one subgroup, namely the identity. Therefore $\mu(Q_8) = 8$.

Examples 1 and 3 are scenarios where the minimal faithful degree of the group $G$ is given by the *Cayley* or *regular* representation; that is, representing the group $G$ acting on itself by right multiplication. Johnson [2, Theorem 1] classifies all cases where this occurs. Note that the four-group also has a minimal faithful representation which is not transitive.

**Theorem 1.** *The regular representation of a group $G$ is minimal if and only if $G$ is*

- *cyclic group of prime power order,*
- *a generalised quaternion two-group, or*
- *the four-group.*

## The groups $G(m,p,n)$

In this section we follow the notation of [6].

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 direct 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 the wreath product $C_m \wr Sym(n) = \underbrace{(C_m \times \cdots \times C_m)}_{n \text{ times}} \rtimes Sym(n)$ and thus has order $m^n n!/p$.

It is well known that these groups can be realised as finite subgroups of $GL_n(\mathbb{C})$, specifically as $n \times n$ matrices with exactly one non-zero entry, which is a complex $m$-th root of unity, in each row and column such that the product of the non-zero 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 [3], [1].

## Direct products

The primary motivation for the author studying these monomial reflection groups is due to one of the central themes of Johnson [2] and Wright [7]. While it is clear that for any two finite groups $G$ and $H$,

$$\mu(G \times H) \leq \mu(G) + \mu(H), \tag{1}$$

Johnson and Wright investigated under what conditions equality holds in (1). Johnson [2] proved that equality in (1) holds whenever $G$ and $H$ have coprime orders and Wright [7] proved that equality holds whenever $G$ and $H$ are $p$-groups and hence nilpotent groups.

Wright went further with this investigation constructing a class of finite groups $\mathcal{C}$ with the property that for any group $G \in \mathcal{C}$, $G$ has a nilpotent subgroup $G_1$ such that $\mu(G_1) = \mu(G)$. It can easily be seen that $\mathcal{C}$ is closed under taking direct products and so any two groups in $\mathcal{C}$ yield an equality in (1). For if $G$ and $H$ are elements of $\mathcal{C}$, then

$$\mu(G) + \mu(H) = \mu(G_1) + \mu(H_1) = \mu(G_1 \times H_1) \leq \mu(G \times H),$$

and so $\mu(G \times H) = \mu(G) + \mu(H)$ and we can take $(G \times H)_1 = G_1 \times H_1$.

Wright proved that this class $\mathcal{C}$ contains all nilpotent, symmetric, alternating and dihedral groups, however the extent of this class is still unknown. At the end of his paper and in Johnson's paper, they both pose the question:

| When is $\mu(G \times H) < \mu(G) + \mu(H)$ for two finite groups $G$ and $H$? |
|---|

Wright even asks whether equality is true for all finite groups. The referee to Wright's paper provided an example of when strict inequality holds and attached it as an addendum. The example was of degree 15 and involved the group $G(5,5,3)$, though this group was simply given in terms of permutations on a set of 15 letters.

It was observed by the referee that $G(5,5,3)$ has minimal degree 15 and moreover possesses a non-trivial centraliser in $Sym(15)$ which is isomorphic to $C_5$ and intersects trivially with it. Therefore

$$\mu(G(5,5,3)) = \mu(G(5,5,3) \times C_{Sym(15)}(G(5,5,3))) = 15$$

and so we immediately have a strict inequality to (1) by taking $G$ and $H$ to be $G(5,5,3)$ and $C_{Sym(15)}(G(5,5,3))$ respectively.

In [4], the author proved that a similar result occurs with the groups $G(4,4,3)$ and $G(2,2,5)$, that is $\mu(G(4,4,3)) = \mu(G(4,4,3) \times C_{Sym(12)}(G(4,4,3))) = 12$ and $\mu(G(2,2,5)) = \mu(G(2,2,5) \times C_{Sym(10)}(G(2,2,5))) = 10$, and so we obtain two more examples of strict inequality in (1). The author does not know whether 10 is the smallest degree for which strict inequality occurs.

Further, in [5] the author proved that for $p$ and $q$ distinct odd primes

$$\mu(G(p,p,q)) = \mu(G(p,p,q) \times C_{Sym(pq)}(G(p,p,q))) = pq$$

except when $p \equiv 1 \bmod 3$, thus demonstrating that the groups $G(p,p,q)$ provide an infinite family of examples for when strict inequality holds in (1). In the next section, we give a brief outline to the proof of this result; for more details and explicit proofs, see [5].

## $\mu(G(p,p,q))$ for $p > q$

In this section we denote $G(p,p,q)$ by $G$ and $A(p,p,q)$ by $A$ throughout. We assume $p$ and $q$ are odd primes such that $p > q$ and exploit the action of $Sym(q)$ on $A$ to prove that every minimal faithful representation of $G$ is given by a core-free subgroup.

Observe that we may treat $A$ as a semi-simple $Sym(q)$-module of dimension $q-1$ over the finite field $\mathbb{F}_p$ since $p$ does not divide the order of $Sym(q)$. The following is a well-known result from modular representation theory.

**Proposition 1.** *$Sym(q)$ acts irreducibly and faithfully on $A$.*

*Proof.* We show that the submodule generated by an arbitrary non-trivial element is the whole of $A$. Let $w = \prod_{i=1}^{q} \theta_i^{\lambda_i}$ be a non-trivial element of $A$ so that $\sum_{i=1}^{q} \lambda_i = 0$. It is enough to prove that we can obtain the basis elements $c_1 = \theta_1\theta_2^{-1}, \ldots, c_{q-1} = \theta_{q-1}\theta_q^{-1}$ of $A$ via the action of $Sym(q)$ on $w$.

Fix a non-zero $\lambda_i$. There is another non-zero $\lambda_j$ such that $\lambda_i - \lambda_j \neq 0$. For suppose $\lambda_i = \lambda_k$ for all non-zero $\lambda_k$. Then

$$w = \left(\prod_{j \in I} \theta_j\right)^{\lambda_i},$$

where $I$ is a subset of $\{1, 2, \ldots, q\}$. So $\sum_{j \in I} \lambda_i = |I|\lambda_i = 0$ in $\mathbb{F}_p$. However since $p > q$, this implies that $\lambda_i = 0$, a contradiction.

Choose two non-zero $\lambda_i$ and $\lambda_j$ with $\lambda_i - \lambda_j \neq 0$. Then applying the transposition $(i\ j)$ to $w$ we have

$$w^{(i\ j)} = \theta_1^{\lambda_1} \ldots \theta_i^{\lambda_j} \ldots \theta_j^{\lambda_i} \ldots \theta_q^{\lambda_q},$$

so

$$w(w^{(i\ j)})^{-1} = \theta_i^{\lambda_i - \lambda_j} \theta_j^{\lambda_j - \lambda_i} = (\theta_i \theta_j^{-1})^{\lambda_i - \lambda_j}.$$

Therefore, $\theta_i \theta_j^{-1}$ is contained in $A$ and by applying the appropriate permutation to it, we can obtain all the basis elements $c_1, \ldots, c_{q-1}$ as required. So $Sym(q)$ acts irreducibly on $A$.

Now suppose that the action of $Sym(q)$ on $A$ has a kernel. This kernel must be a normal subgroup of $Sym(q)$ and since $q \neq 4$, the only possibility is the alternating group $Alt(q)$. However, it can easily be verified that the $q$-cycle $b = (1\ 2\ \ldots\ q)$, which is an even permutation, does not commute with any non-trivial element of $A$. Therefore $Sym(q)$ acts faithfully on $A$.

**Corollary 1.** *$A$ is the unique minimal normal subgroup of $G$.*

*Proof.* Certainly $A$ is a normal subgroup of $G$ and since $Sym(q)$ acts irreducibly on it, it is a minimal normal subgroup.

Suppose $N$ is a non-trivial normal subgroup of $G$ which does not contain $A$. By minimality of $A$ we must have $A \cap N = \{1\}$. It follows that $AN = A \times N$, that is $AN$ is the internal direct product of $A$ and $N$.

Let $a \in A$ and $n = a'\sigma \in N \setminus A$, where $a' \in A$ and $\sigma \in Sym(q)$. Then $n = a^{-1}na$ so $a'\sigma = a^{-1}a'\sigma a = a'a^{-1}\sigma a$, and so $\sigma = a^{-1}\sigma a$. That is, $\sigma$ commutes with $a$. But $a$ is arbitrary so $\sigma$ is contained in the kernel of the action of $Sym(q)$ on $A$. Therefore $\sigma$ is trivial and $n = a'$ contradicting that $n \notin A$.

Therefore $A$ is contained in every non-trivial normal subgroup of $G$ and is thus the unique minimal normal subgroup of $G$.

It follows now that any minimal faithful representation of $G$ must be transitive, that is, given by a single core-free subgroup. We use this fact to prove the minimal degree of $G$ is $pq$.

Let $L$ be a core-free subgroup of $G$ such that $|G\colon L| = \mu(G)$. Since $A$ is an elementary Abelian $p$-group of rank $q-1$, $\mu(A) = p(q-1)$ and since $G$ is a proper subgroup of the wreath product $C_p \wr Sym(q)$ which has minimal degree $pq$, we have the upper and lower bounds

$$p(q-1) \leq \mu(G) \leq pq.$$

Via some arguments in linear representation theory involving duality, (see [5]) we can in fact prove (for $p \not\equiv 1 \bmod 3$) that any core-free subgroup of $G$ has index at least $pq$ and so $\mu(G) = pq$.

For the case $q = 3$ and $p \equiv 1 \bmod 3$ the calculation is easier. Observe that in this case, the group $G(= G(p, p, 3))$ is isomorphic to $(C_p \times C_p) \rtimes Sym(3)$. Let $c_1, c_2$

generate the base group $A$ and $a = (1\ 2), b = (1\ 2\ 3)$ generate $Sym(3)$. Then $b$ and $a$ act on the base group $A$ as follows:

$$c_1^a = c_1^{-1}, \quad c_2^a = c_1c_2, \quad c_1^b = c_2, \quad c_2^b = c_1^{-1}c_2^{-1},$$

and this action induces a two dimensional $Sym(3)$-module structure on $A$. It is well known that when $p \equiv 1 \bmod 3$, there is a cube root of unity $\zeta_3$ in the field $\mathbb{F}_p$. Observe that $\zeta_3^2 + \zeta_3 + 1 = 0$. Consider the element $c_1c_2^{-\zeta_3}$. We have

$$(c_1c_2^{-\zeta_3})^b = c_1^{\zeta_3}c_2^{\zeta_3+1} = (c_1c_2^{-\zeta_3})^{\zeta_3},$$

so $c_1c_2^{-\zeta_3}$ is an eigenvector for $b$ with eigenvalue $\zeta_3$. It is easily verified that $c_1c_2^{-\zeta_3}$ is not an eigenvector for $a$ and so the subgroup $L = \langle c_1c_2^{-\zeta_3}, b\rangle$ forms a core-free subgroup of $G$ of order $3p$. Since $G$ has order $6p^2$, we have $|G\colon L| = 2p$, so $\mu(G) = 2p$.

Combining this with the previous arguments we have proved:

**Theorem 2.** *Let $p$ and $q$ be odd primes with $p > q$. Then*

$$\mu(G(p,p,q)) = \begin{cases} pq & \text{if } q \geq 5, \text{ or } q = 3 \text{ and } p \equiv 2 \bmod 3 \\ 2p & \text{if } q = 3 \text{ and } p \equiv 1 \bmod 3. \end{cases}$$

## Acknowledgements

The author thanks his supervisor David Easdown and his associated supervisor Anthony Henderson for many helpful discussion regarding reflection groups and finite groups.

## References

[1] Cohen, A.M. (1976). Finite complex reflection groups. *Ann. Sci. École Norm.* Sup. (4) **9,** 379–436.
[2] Johnson, D.L. (1971). Minimal permutation representations of finite groups. *Amer. J. Math.* **93,** 857–866.
[3] Orlik, P. and Hiroaki, T. (1992). *Arrangements and Hyperplanes*. Springer.
[4] Saunders, N. (2007). *A Strict Inequality for a Minimal Degree of a Direct Product*. Preprint.
[5] Saunders, N. (2008). *The Minimal Degree for a Class of Finite Complex Reflection Groups*. Preprint.
[6] Taylor, D.E. and Lehrer, G.I. (2007). *Unitary Reflection Groups*. Cambridge University Press. To appear.
[7] Wright, D. (1975). Degrees of minimal embeddings of some direct products. *Amer. J. Math.* **97,** 897–903.