JOURNAL OF ALGEBRA 6, 22-42 (1967)

Intersection Matrices for Finite Permutation Groups*

D. G. HIGMAN

Department of Mathematics, University of Michigan, Ann Arbor, Michigan

Communicated by Graham Higman

Received June 15, 1965

In this paper we study finite transitive groups G acting on a set Ω. The results, which are trivial for multiply-transitive groups, directly generalize parts of the discussion of rank-3 groups in [4] and [5]. There are close connections with Feit and Higman's paper [2].

For each $a \in \Omega$ let us choose a G_a-orbit $\Delta(a) \neq \{a\}$ so that $\Delta(a)^g = \Delta(a^g)$ for all $a \in \Omega$ and $g \in G$. Relative to Δ we introduce a *distance* in Ω based on taking the points of $\Delta(a)$ to be at distance 1 from a (see Section 1). The maximum distance we call the *diameter* of G. A necessary and sufficient condition for G to be primitive is that the diameter be finite with respect to every Δ. It is important to note, however, that finiteness of the diameter with respect to a single Δ does not imply primitivity.

We study the matrix M of *intersection numbers* of Δ (defined in Section 4). M is irreducible if and only if G has finite diameter with respect to Δ, and in this case the subdegrees and diameter are determined by M. The minimum polynomial of M is shown to coincide with that of the incidence matrix A of Δ, and it is shown how to compute the trace of A^q, $q \geqslant 0$, in terms of M. This means that if $\rho(x)$ is a polynomial such that $\rho(M) = 0$ and if θ is a root of $\rho(x)$, then the multiplicity of θ as an eigenvalue of A is determined by M. In case the minimum and characteristic polynomials of M coincide, we show that M has simple eigenvalues, from which it follows that the irreducible constituents of the permutation representation have multiplicity 1 and that the degrees of these constituents are determined by M. In this case there is a one-to-one correspondence between the eigenvalues of M and the irreducible constituents of the permutation representation, which preserves conjugacy.

The new simple group of order 750, 560 discovered by Janko [6] provides an example in which two of the constituents are conjugate even though the subdegrees are distinct.

* This research was supported in part by a National Science Foundation Research Grant.

Our considerations apply to groups G of maximal diameter, i.e., of diameter $r - 1$ with respect to a self-paired orbit, r being the rank, for in this case M is an irreducible tridiagonal matrix and so has simple (real) eigenvalues. As examples of such groups we mention that (1) any rank-3 group has diameter 2 with respect to one of the two nontrivial G_a-orbits, (2) in some cases the representation relative to a maximal parabolic subgroup of a group admitting a (B, N)-pair in the sense of Tits ([*8*], [*2*]) has maximal diameter with respect to a suitable orbit (this can already be decided by looking at the Weyl group; cf. [*1*]), and (3) Janko's new simple group refered to above has a representation as a primitive rank-5 group of degree 266 and diameter 4.

In a final section we consider two special possibilities for M closely related to the paper by Feit and Higman [*2*]. The extent to which ideas from [*2*] have been used in the present paper will be clear to the reader.

NOTATION. For the theory of finite permutation groups we refer the reader to Wielandt [*9*]. For the most part we adhere to the notation of that book.

We consider a transitive permutation group G on a set Ω and assume the *degree* $n = |\Omega|$ of G is finite. We denote the *rank* of G by r; this means that for each $a \in \Omega$, Ω decomposes into exactly r G_a-orbits,

$$\Omega = \Gamma_0(a) + \Gamma_1(a) + \cdots + \Gamma_{r-1}(a), \; \Gamma_0(a) = \{a\},$$

where G_a denotes the stabilizer of a. The notation is chosen so that

$$\Gamma_i(a)^g = \Gamma_i(a^g) \quad \text{for all} \quad a \in \Omega, \qquad g \in G, i = 0, 1,..., r-1.$$

It is convenient to define an *orbital* of G to be a mapping Δ from Ω into the subsets of Ω such that

(1) *$\Delta(a)$ is a G_a-orbit for $a \in \Omega$*, and

(2) *$\Delta(a)^g = \Delta(a^g)$ for all $a \in \Omega, g \in G$.*

The number $|\Delta(a)|$, which is clearly independent of $a \in \Omega$, we call the *length* $|\Delta|$ of Δ. In this terminology, $\Gamma_0, \Gamma_1,..., \Gamma_{r-1}$ are the orbitals of G. The lengths $l_i = |\Gamma_i|$, $i = 0, 1,..., r-1$ are called the *subdegrees* of G, their sum is the degree of G, $n = l_0 + l_1 + \cdots + l_{r-1}$.

Each orbital Δ of G has a mirror-image Δ' defined by

$$\Delta'(a) = \{a^{g^{-1}} \mid a^g \in \Delta(a)\} \qquad (a \in \Omega)$$

([*9*], Section 16). Δ' is again an orbital of G of the same length as Δ, and $\Delta'' = \Delta$. The correspondence $\Delta \leftrightarrow \Delta'$ is a pairing of the orbitals of G.

A necessary and sufficient condition for the existence of a self-paired orbital is that $|G|$ be even ([9], Theorem 16.5).

1. Distance

Relative to a particular orbital $\Delta \neq \Gamma_0$ we define a *path* of length q from a to b to be a sequence $x_0, x_1, \ldots, x_q$ of $q+1$ points of Ω such that $x_0 = a$, $x_q = b$ and $x_i \in \Delta(x_{i-1})$, $i = 1, \ldots, q$. We define

$$\rho(a, b) = \text{the length of the shortest path from } a \text{ to } b, \text{ or } \infty \text{ if there is no path from } a \text{ to } b.$$

Then we have at once that

$$\rho(a, b) = 0 \textit{ if and only if } a = b \tag{1.1}$$

and

$$\rho(a, b) + \rho(b, c) \geqslant \rho(a, c). \tag{1.2}$$

If we define ρ' in the same way as ρ, with Δ' in place of Δ, then

$$\rho(a, b) = \rho'(b, a). \tag{1.3}$$

This is because $a \in \Delta(b)$ implies $b \in \Delta'(a)$.

From the relation $\Delta(a)^g = \Delta(a^g)$ we see that G is a group of isometries of ρ, that is,

(1.4) $\rho(a^g, b^g) = \rho(a, b)$ *for* $g \in G$.

By (1.4), for any orbital Γ, if $a^g \in \Gamma(a)$, then

$$\rho(a, \Gamma(a)) = \rho(a, a^g) = \rho(a^{g^{-1}}, a) = \rho(\Gamma'(a), a),$$

that is,

$$\rho(a, \Gamma(a)) = \rho(\Gamma'(a), a). \tag{1.5}$$

Now put

$$\Lambda_q(a) = \{x \in \Omega \mid \rho(a, x) = q\}, \Lambda_q'(a) = \{x \in \Omega \mid \rho(x, a) = q\}.$$

These are the two types of *circles of radius* q *with center at* a. Clearly

(1.6) $\Lambda_q(a)^g = \Lambda_q(a^g)$ *and* $\Lambda_q'(a)^g = \Lambda_q'(a^g)$ *for* $g \in G$,

and

(1.7) *$\Lambda_q(a)$ is a union of G_a-orbits while $\Lambda_q'(a)$ is the union of the G_a-orbits paired with those in $\Lambda_q(a)$.*

Moreover,

$$\Lambda_{q+1}(a) \subseteq \sum_{x \in \Lambda_q(a)} \Delta(x) \subseteq \sum_{\alpha \leqslant q+1} \Lambda_\alpha(a) \tag{1.8}$$

and

$$\sum_{x \in \Lambda_q'(a)} \Delta(x) \subseteq \sum_{\alpha \geqslant q-1} \Lambda_\alpha'(a).$$

Proof. If $y \in \Lambda_{q+1}(a)$ then there is an $x \in \Lambda_q(a)$ such that $\rho(x, y) = 1$, i.e., such that $y \in \Delta(x)$. Thus $\Lambda_{q+1}(a) \subseteq \sum_{x \in \Lambda_q(a)} \Delta(x)$.

If $x \in \Lambda_q(a)$ and $b \in \Delta(x)$ then $\rho(x, b) = 1$ so

$$\rho(a, b) \leqslant \rho(a, x) + \rho(x, b) = q + 1.$$

That is, $\Delta(x) \subseteq \sum_{\alpha \leqslant q+1} \Lambda_\alpha(a)$.

If $x \in \Lambda_q'(a)$ and $b \in \Delta(x)$ then $q = \rho(x, a) \leqslant \rho(x, b) + \rho(b, a) = 1 + \rho(b, a)$ so $\rho(b, a) \geqslant q - 1$. That is $\Delta(x) \subseteq \sum_{\alpha \geqslant q-1} \Lambda_\alpha'(a)$.

We now define the *diameter of G relative to Δ to be*

$$\max \rho(a, b) = \max \rho'(a, b),$$

the maximum being taken over all $a, b \in \Omega$. Clearly if the diameter is finite it is just the number of circles of positive radius with a given center. Hence

(1.9) *If G has finite diameter then the diameter is at most $r - 1$. If G has diameter $r - 1$ then every G_a-orbit is a circle with center a.*

Now put $\Lambda(a) = \{x \in \Omega \mid \rho(a, x) < \infty\}$. Then $\Lambda(a)^g = \Lambda(a^g)$ for all $a \in \Omega$, $g \in G$, and if $x \in \Lambda(a)$ we have $\Lambda(x) \subseteq \Lambda(a)$ by (1.2) so that $\Lambda(x) = \Lambda(a)$ since $|\Lambda(x)| = |\Lambda(a)|$. Thus $\Lambda(a) \cap \Lambda(a)^g \neq \emptyset, g \in G$, implies $\Lambda(a) = \Lambda(a)^g$ so that $\Lambda(a)$ is a *block* for G in the terminology of Wielandt ([9], Section 6), and therefore $\Lambda(a) = a^H$ with H a subgroup of G containing G_a. In fact, $\Lambda(a)$ is the smallest block containing a and $\Delta(a)$ and H is the smallest subgroup of G containing G_a such that $a^H \cap \Delta(a) \neq \emptyset$. Writing

$$\Lambda'(a) = \{x \in \Omega \mid \rho'(a, x) < \infty\}$$

we have

(1.10) $\Lambda(a) = \Lambda'(a)$.

Proof. Since $\Delta(a) \subseteq \Lambda(a)$ there exists $h \in H$ such that $a^h \in \Delta(a)$. Then $a^{h^{-1}} \in \Delta'(a)$ and hence $\Delta'(a) \subseteq \Lambda(a)$. But this implies that

$$\Delta'(x) \subseteq \Lambda(x) = \Lambda(a)$$

for all $x \in \Lambda(a)$, and therefore $\Lambda'(a) \subseteq \Lambda(a)$. The reverse inclusion follows by symmetry.

(1.11) *The following conditions are equivalent.*

(1) *G has infinite diameter with respect to Δ.*

(2) *$\Lambda(a)$ is a system of imprimitivity for G.*

(3) *there exists a system Σ of imprimitivity for G such that $a \in \Sigma$ and $\Sigma \cap \Delta(a) \neq \emptyset$.*

(4) *there exists a subgroup H of G such that $G_a \leqslant H \neq G$ and $a^H \cap \Delta(a) \neq \emptyset$.*

Proof. (1) *implies* (2): The assumption that G be of infinite diameter means that $\Lambda(a) \neq \Omega$. Since $\Lambda(a)$ is a block and $|\Lambda(a)| > 1$ this means that $\Lambda(a)$ is a system of imprimitivity for G.

(2) *implies* (3) trivially.

(3) *implies* (4): This follows from the fact that if the systems of imprimitivity containing a are the sets of the form a^H with H a subgroup of G, $\neq G$, and properly containing G_a.

(4) *implies* (1): Suppose given a subgroup H as in (4). Then a^H is a system of imprimitivity for G and $\Delta(a) \leqslant a^H$. Consequently, $\Delta(x) \subseteq x^H = a^H$ for all $x \in a^H$, and therefore $\Lambda(a) \subseteq a^H$. This means that $\Lambda(a) \neq \Omega$, and hence that G has infinite diameter.

An immediate consequence of (1.11) is

(1.12) *G is primitive if and only if G has finite diameter with respect to every orbital $\neq \Gamma_0$.*

ρ is an actual metric precisely when Δ is self-paired, for by (1.3),

(1.13) *ρ is symmetric if and only if Δ is self-paired.*

In this case the circles $\Lambda_q(a)$ and $\Lambda_q'(a)$ coincide, so by (1.7) and (1.8),

(1.14) *If Δ is self-paired then the mirror-image of a G_a-orbit contained in $\Lambda_q(a)$ is contained in $\Lambda_q(a)$,*

and

(1.15) *If Δ is self-paired then*

$$\Lambda_{q+1}(a) \subsetneq \sum_{x \in \Lambda_q(a)} \Delta(x) \subseteq \Lambda_{q-1}(a) + \Lambda_q(a) + \Lambda_{q+1}(a).$$

Note also that, by (1.5) and (1.9),

(1.16) *If Δ is self-paired and G has maximal finite diameter* (i.e., *diameter* $r - 1$) *relative to Δ then every G_a-orbit is self-paired.*

2. Incidence Matrices and Incidence Structures

The incidence matrix $B_i = (\beta_{ab}^{(i)})$ for the orbital Γ_i of G is defined by

$$\beta_{ab}^{(i)} = \begin{matrix} 1 \text{ if } a \in \Gamma_i(b), \\ 0 \text{ otherwise.} \end{matrix}$$

The rows and columns of B_i are indexed by the points of Ω in some given order. Clearly

(2.1) $B_0 = I$ *and* $\sum_{i=0}^{r-1} B_i = F$ (*where* F *is the matrix with all entries* 1).

Moreover — cf. [9], Theorem (28.4) —

(2.2) $B_0, B_1, \ldots, B_{r-1}$ *is a basis for the commuting algebra of the permutation representation of* G,

and

(2.3) *If* $\Gamma_i' = \Gamma_{i'}$, *then* $B_i^t = B_{i'}$.

Let us consider a particular orbital $\Delta \neq \Gamma_0$, say $\Delta = \Gamma_1$, and put $A = B_1$, $\alpha_{ab} = \beta_{ab}^{(1)}$, so that

$$\alpha_{ab} = \begin{matrix} 1 \text{ if } a \in \Delta(b), \\ 0 \text{ otherwise.} \end{matrix}$$

A is the incidence matrix of the block design **A** whose points and blocks are both the elements of Ω, with a point a and a block b being incident if $a \in \Delta(b)$; the rows (resp. columns) of A are indexed by the elements of Ω regarded as the points (resp. blocks) of **A**. The group G is represented as a group of collineations of **A** according to the action of G on $\Omega \times \Omega$. The group $\mathfrak{G}$ of all permutations of Ω which induce collineations of **A** is just the group having Δ as an orbital, i.e., the isometries of ρ. The diameter of $\mathfrak{G}$ with respect to Δ is equal to that of G. The collineations induced by $\mathfrak{G}$ are those which commute with the correspondence $a \leftrightarrow a$ between points and blocks. $\mathfrak{G}$ is isomorphic with the group of all $n \times n$ permutation matrices which commute with A.

The assumption that Δ is self-paired is equivalent to the assumption that A is symmetric, and means precisely that the correspondence $a \leftrightarrow a$ is a polarity of **A**.

Assume now that Δ is self-paired. Given distinct points a and b we define the *line* $a + b$ joining them by

$$a + b = \bigcap_{a,b \in x} x^{\perp}, \quad \text{where} \quad x^{\perp} = \{x\} + \Delta(x).$$

Here we are concerned only with the *totally singular* lines, i.e., the lines

$a + b$ with $b \in \Delta(a)$. Clearly G_a is transitive on the set of totally singular lines through a and hence G is transitive on the set of all totally singular lines. Two totally singular lines have at most one point in common. For if $c \in a + b$, $c \neq a$, then $a + c$ is a totally singular line and $a + c \leqslant a + b$, whence $a + c = a + b$. It follows that G_{a+b} is doubly transitive on the points of $a + b$ unless $a + b = \{a, b\}$. If we put

$s + 1 =$ the number of points on a totally singular line, and
$t + 1 =$ the number of totally singular lines through a point,

then, since $\Delta(a)$ is the set of those points joined to a by totally singular lines, putting $k = |\Delta|$, we have

$$k = s(t + 1). \tag{2.4}$$

(Note that if G has rank 2 then $s = n - 1$, $t = 0$.)

We may consider the incidence structure **P** having as points the points of Ω and as lines the totally singular lines, with the obvious incidence. If P is an incidence matrix for **P** with the rows indexed by the points and the columns by the lines then $PP^t = A + (t + 1) I$. The structure **P** will be used in making explicit the connection between our discussion and that of [*2*].

3. A Bound for the Degree

Let us assume that G has finite diameter d with respect to a self-paired orbital $\Delta \neq \Gamma_0$. We observe that

$$|\Lambda_{q+1}(a)| \leqslant st\, |\Lambda_q(a)| \leqslant (k - 1) |\Lambda_q(a)|, \qquad q \geqslant 1. \tag{3.1}$$

In fact, if $x \in \Lambda_q(a)$, there exists a $y \in \Lambda_{q-1}(a)$ such that $x \in \Delta(y)$. Then

$$x + y \subseteq \{y\} + \Delta(y) \subseteq \Lambda_{q-2}(a) + \Lambda_{q-1}(a) + \Lambda_q(a)$$

by (1.15). Thus at most $s(t + 1) - s = st$ points of $\Delta(x)$ lie in $\Lambda_{q+1}(a)$ so the first inequality of (3.1) follows by (1.15). Since $k = s(t + 1) > st$ by (2.4), the second inequality is immediate.

Now $|\Lambda_1(a)| = |\Delta(a)| = s(t + 1)$, so (3.1) gives

$$|\Lambda_q(a)| \leqslant s^q t^{q-1}(t + 1)$$

from which we obtain a bound in the degree n of G, namely

(3.2) Theorem. *If G has finite diameter d with respect to the self-paired orbital $\Delta \neq \Gamma_0$ then*

$$n \leqslant 1 + s(t + 1)\frac{(st)^d - 1}{st - 1} \leqslant 1 + k\frac{(k - 1)^d - 1}{k - 2}.$$

Here $k = s(t + 1) = |\Delta|$, and s and t are as defined in Section 2.

If we drop the assumption that Δ is self-paired, then in place of (3.1) we have only that

$$|\Delta_{q+1}(a)| \leqslant k\,|\Delta_q(a)|;$$

so

$$n \leqslant \frac{k^{d+1}-1}{k-1}.$$

The remarks in this section include Theorem (17.4) of [9].

4. Intersection Matrices

The *intersection numbers* relative to an orbital Γ_α are defined by

$$\mu_{ij}^{(\alpha)} = |\Gamma_\alpha(b) \cap \Gamma_i(a)| \qquad [b \in \Gamma_j(a)].$$

It is evident that these numbers depend only on α, i, and j, and we see that

$$\sum_i \mu_{ij}^{(\alpha)} = l_\alpha, \sum_\alpha \mu_{ij}^{(\alpha)} = l_i, \mu_{ij}^{(\alpha)} = \mu_{\alpha j'}^{(i)},$$

and

$$\mu_{i0}^{(\alpha)} = \delta_{i\alpha} l_\alpha, \mu_{0i}^{(\alpha)} = \delta_{i\alpha'}, \tag{4.1}$$

(where $\Gamma_{\alpha'} = \Gamma_\alpha'$, the orbital paired with Γ_α). Moreover,[1]

(4.2) $l_j\mu_{ij}^{(\alpha)} = l_i\mu_{ji}^{(\alpha')}$ *and* $l_i\mu_{k'i}^{(j)} = l_j\mu_{i'j}^{(k)} = l_k\mu_{j'k}^{(i)}$.

Proof. A pair (b, c) is such that $b \in \Gamma_j(a)$ and $c \in \Gamma_\alpha(b) \cap \Gamma_i(a)$ if and only if $c \in \Gamma_i(a)$ and $b \in \Gamma_{\alpha'}(c) \cap \Gamma_j(a)$. Counting these pairs gives $l_j\mu_{ij}^{(\alpha)} = l_i\mu_{ji}^{(\alpha')}$, and combining this with $\mu_{ij}^{(\alpha)} = \mu_{\alpha j'}^{(i)}$ from (4.1) [or directly, counting the triplets (a, b, c) with $b \in \Gamma_i(a)$, $c \in \Gamma_j(b)$ and $a \in \Gamma_k(c)$] gives the rest of (4.2).

Included in (4.2) is Lemma 5 of [4] and part of a Theorem of Manning ([9], Theorem 17.7).

The $r \times r$ matrix $M_\alpha = (\mu_{ij}^{(\alpha)})_{i,j}$ will be called the *intersection matrix* of Γ_α. By (4.1) we have

(4.3) *M_α has column sum l_α. The matrices $M_0, M_1, \ldots, M_{r-1}$ are linearly independent and $\sum_\alpha M_\alpha = \hat{F}$, the matrix whose* ith *row is* $(l_i, l_i, \ldots, l_i)$, $i = 0, 1, \ldots, r-1$.

Focusing attention on a particular orbital $\Delta \neq \Gamma_0$, say $\Delta = \Gamma_1$, we put $M = M_1$ and write $\mu_{ij} = \mu_{ij}^{(1)}$. As before we put $k = l_1$ and $A = B_1$.

---

[1] The author is indebted to M. Suzuki for pointing out this improvement of his original statement.

Arrange the G_a-orbits into circles of increasing radius about a (with respect to Δ) and number the orbitals accordingly, so that

$$\Lambda_q(a) = \sum_{c_q \leqslant i < c_{q+1}} \Gamma_i(a) \qquad (1 \leqslant q \leqslant m) \tag{4.4}$$

and $\rho(a, \Gamma_i(a)) = \infty$ for $i \geqslant c_{m+1}$. Recall that

$$\Lambda(a) = \sum_{q=0}^{m} \Lambda_q(a)$$

is a system of imprimitivity for G unless G has finite diameter with respect to Δ [by (1.11)].

(4.5) *With respect to the described arrangement of the G_a-orbits, M takes the form $M = \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix}$ with $X = (\lambda_{ij})_{1 \leqslant i,j \leqslant m}$ and*

$$\lambda_{ij} = (\mu_{\alpha\beta})_{c_i \leqslant c < c_{i+1}; c_j \leqslant \beta < c_{j+1}}$$

such that

(a) $\lambda_{ij} = 0$ *if* $i > j + 1$,

(b) λ_{ii} *is a square matrix,* $0 \leqslant i \leqslant m$, *and*

(c) *every row of* λ_{i+1i} *contains a nonzero entry.*

Proof. It follows at once from the definitions that M takes the form $M = \begin{pmatrix} X & Z \\ 0 & Y \end{pmatrix}$ where X has the described form. By (1.10) we know that $\Lambda(a) = \Lambda'(a)$, and this means that the intersection matrix for Δ' takes the form $\begin{pmatrix} U & W \\ 0 & V \end{pmatrix}$ (with respect to the given arrangement of the orbitals) with U an $m \times m$ block. Therefore, by (4.2), $Z = 0$.

Conversely, we have

(4.6) *If by simultaneous row and column permutations applied to the last $r - 2$ rows and columns M is brought to the form $\begin{pmatrix} X & Z \\ 0 & Y \end{pmatrix}$ with $X = (\lambda_{ij})$ satisfying* (a), (b) *and* (c) *of* (4.5), *then, renumbering the orbitals accordingly we have that the circles of finite radius about a are given by* (4.4) (*and hence by* (4.5) *that* $Z = 0$).

In particular,

(4.7) *G has finite diameter with respect to Δ if and only if M is irreducible; in this case the diameter of G is one less than the number of diagonal blocks λ_{ii} in the form* (4.5).

By (1.10) this implies

(4.8) *G is primitive if and only if M_α is irreducible for all* $\alpha = 1, 2,..., r - 1$.

The intersection matrix M_α can be obtained from the incidence matrix B_α in the following way. Arrange the points of Ω according to the G_a-orbits and consider the corresponding blocking of B_α. Each block has constant column sum, and we see that in fact the matrix $\hat{B}_\alpha$ obtained from B_α by replacing each block by its column sum is precisely M_α. Putting $L = (l_0, l_1, ..., l_{r-1})^t$, we have as a first consequence

(4.9) $M_\alpha L = l_\alpha L$, i.e., *M_α has L as an eigenvalue corresponding to the eigenvalue l_α. If G has finite diameter with respect to Γ_α then the subdegrees are uniquely determined by this equation.*

Proof. We have $B_\alpha X = l_\alpha X$, $X = (1, 1, ..., 1)^t$, so $\hat{B}_\alpha \hat{X} = l_\alpha \hat{X}$, and $M_\alpha = \hat{B}_\alpha$, $L = \hat{X}$ (the notation being self-explanatory). If G has finite diameter with respect to Γ_α then M_α is irreducible by (4.7), so L is uniquely determined as the positive eigenvector with first component 1 corresponding to the maximal eigenvalue l_α (by the Perron–Frobenius theory).

Each matrix X in the commuting algebra C of the permutation representation of G has its rows and columns indexed by the points of Ω and so has a blocking according to the arrangement of the points of Ω into G_α-orbits. The blocks have constant column sum, and denoting by $\hat{X}$ the $r \times r$ matrix obtained by replacing each block by its column sum, we obtain an algebra homomorphism of C onto a subalgebra $\hat{C}$ of the algebra of all $r \times r$ matrices. (Here we are applying an unpublished theorem of Wielandt. For completeness a proof of Wielandt's theorem is indicated in an appendix at the end of this paper.) But by (4.3) the matrices $M_\alpha = \hat{B}_\alpha$, $\alpha = 0, 1, ..., r-1$, are linearly independent. Hence by (2.2) the homomorphism is an isomorphism

$$C = \langle B_0, B_1, ..., B_{r-1} \rangle \approx \hat{C} = \langle M_0, M_1, ..., M_{r-1} \rangle.$$

As a first consequence we have

(4.10) *The matrices $M_0, M_1, ..., M_{r-1}$ span an algebra $\hat{C}$, which is commutative if and only if the irreducible constituents of the permutation representation are inequivalent.*

Proof. $\hat{C}$ is commutative if and only if C is commutative, and commutativity of C is equivalent to the inequivalence of the irreducible constituents of the permutation representation (cf. [9], Theorem 29.3).

A second important consequence is

(4.11) *M_α and B_α have the same minimum polynomial*, $\alpha = 0, 1, ..., r-1$.
Now we can prove that

(4.12) *The following are equivalent:*

(a) *the minimum polynomial of M has degree r.*

(b) *the powers of M span $\hat{C}$.*

(c) *the powers of A span C.*

(d) *the eigenvalues of M are simple.*

Proof. We prove that (a) implies (d). The implications (d) $\Rightarrow$ (c) $\Rightarrow$ (b) $\Rightarrow$ (a) are immediate using (4.11).

If the minimum polynomial of M has degree r then by (4.11),

$$C = \langle I, A, A^2, \ldots, A^{r-1} \rangle.$$

Since C is commutative we know that the permutation representation Δ has r inequivalent irreducible constituents $\Delta_0 = 1, \Delta_1, \ldots, \Delta_{r-1}$. Choose a nonsingular matrix P such that

$$P^{-1}\Delta P = \mathrm{diag}\{\Delta_0, \Delta_1, \ldots, \Delta_{r-1}\}.$$

Then

$$P^{-1}AP = \mathrm{diag}\{\theta_0, \theta_1 I_{f_1}, \ldots, \theta_{r-1} I_{f_{r-1}}\},$$

where f_i is the degree of Δ_i and $\theta_0 = k, \theta_1, \ldots, \theta_{r-1}$, as eigenvalues of A, are eigenvalues of M. If now k_α is the αth class sum of G then $\Delta_i(k_\alpha) = \omega_i(k_\alpha) I_{f_i}$ where ω_i is the linear representation of the center of the group algebra of G corresponding to Δ_i. Thus

$$P^{-1}\Delta(k^\alpha) P = \mathrm{diag}\{\omega_0(k_\alpha), \omega_1(k_\alpha) I_{f_1}, \ldots, \omega_{r-1}(k_\alpha) I_{f_{r-1}}\}.$$

Now $\Delta(k_\alpha) \in C$ so

$$\Delta(k_\alpha) = \sum_{q=0}^{r-1} x_{\alpha q} A^q$$

where the $x_{\alpha q}$ are uniquely determined rational numbers. Hence we have $\omega_i(k_\alpha) = \sum x_{\alpha q} \theta_i^q$ which means that for each i, ω_i is determined by θ_i. But the ω_i are distinct since the Δ_i are inequivalent. Hence the θ_i are distinct.

At the same time we see that

(4.13) *If the minimum polynomial of M has degree r then there is a one-to-one correspondence between the eigenvalues of M and the irreducible constituents of the permutation representation, preserving conjugacey, and the multiplicity of an eigenvalue of M as an eigenvalue of A is the degree of the corresponding irreducible constituent.*

We remark that in case the minimum polynomial of M has degree r, so that M has simple eigenvalues, C is the full commuting algebra of M. Hence in this case we can determine the M_α, $\alpha = 0, 1, \ldots, r-1$, from M as the unique matrices commuting with M whose first rows contain only a single nonzero entry 1. At the same time we will, of course, determine the subdegrees and the pairing of the orbitals.

5. Multiplicities of the Eigenvalues of A

Define vectors $\eta_q = (\eta_{q0}, \eta_{q1}, ..., \eta_{qr-1})$, $q \geqslant 0$, by

$$\eta_0 = (1, 0, ..., 0), \eta_{q+1} = \eta_q M. \tag{5.1}$$

(5.2) Theorem. trace $A^q = n\eta_{q0}$, $q \geqslant 0$, *where n is the degree of G.*

Proof. Write $A^q = \sum \lambda_{qj} B_j$, then trace $A^q = n\lambda_{q0}$, and $M^q = \sum \lambda_{qj} M_j$. Now $M_j M = \sum \mu_{j'\alpha'} M_\alpha$ since the first row of M_j has all entries 0 except for a 1 in the j'-position. Hence $M^{q+1} = \sum \lambda_{qj}\mu_{j'\alpha'} M_\alpha$ and therefore $\lambda_{q+1i} = \sum \lambda_{qj}\mu_{j'i'}$. This can be written as $\lambda_{q+1} = \lambda_q PMP$ where $\lambda_\alpha = (\lambda_{\alpha 0}, \lambda_{\alpha 1}, ...)$ and P is the permutation matrix representing the pairing of the orbitals. Then $\lambda_{q+1}P = \lambda_q PM$ so that $\eta_q = \lambda_q P$, giving $\eta_{q0} = \lambda_{q0}$.

If now $\rho(x)$ is a polynomial such that $\rho(M) = 0$ then we know that $\rho(A) = 0$ by (4.11). If θ is a root of $\rho(x)$ of multiplicity m then the multiplicity of θ as an eigenvalue of A is

$$\text{trace } \rho_0(A)/\rho_0(\theta), \tag{5.3}$$

where $\rho_0(x) = \rho(x)/(x - \theta)^m$ (cf. [2], Lemma 3.4). Since the trace of $\rho_0(A)$ can be computed from M by (5.2), we have

(5.4) *If θ is a root of a polynomial $\rho(x)$ such that $\rho(M) = 0$, then the multiplicity of θ as an eigenvalue of A is determined by M according to* (5.3) *and* (5.2).

Combining this with (4.14) we get

(5.5) Theorem. *If M has simple eigenvalues $\theta_0 = k, \theta_1, ..., \theta_{r-1}$, then the degrees $x_0 = 1, x_1, ..., x_{r-1}$ of the irreducible constituents of the permutation representation of G are determined by M, namely, they are given by*

$$x_i = \text{trace } f_i(A)/f_i(\theta_i), \qquad i = 0, 1, ..., r-1,$$

where $f_i(x) = f(x)/(x - \theta_i)$, $f(x)$ being the characteristic polynomial of M.

Putting $N = (\eta_{ij}) = (\eta_0, \eta_1, ...)^t$, the recursion (5.1) can be written as

$$SN = NM \qquad \text{with} \qquad S = \begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & \ddots \\ & & & \ddots \end{pmatrix}. \tag{5.6}$$

Taking N_0 to be the $r \times r$ matrix consisting of the first r rows of N we have

(5.7) *$N_0 M = CN_0$ where C is the companion matrix of the characteristic polynomial $f(x)$ of M.*

From (5.7) we have $M(adjN_0) = (adjN_0)\,C$, and hence, since M has column sum k, $k(XadjN_0) = (XadjN_0)\,C$ where $X = (1, 1, \ldots, 1)$. Writing $adjN_0 = (\eta_{ij}^*)$ and putting

$$g(x) = \sum_{j=0}^{r-1} \sigma_j x^j, \qquad \sigma_j = \sum_{i=0}^{r-1} \eta_{ij}^*,$$

it follows that

$$(x - k)\, g(x) = \sigma_{r-1} f(x). \tag{5.8}$$

Note that N_0 is nonsingular if and only if the minimum polynomial of M has degree r, and in this case we have

$$M_{i'} = \sum \eta^{ij} M^j, \qquad N_0^{-1} = (\eta^{ij}).$$

6. Groups of Maximal Diameter

We now assume that $\Delta = \Gamma_1$ is self-paired, and write $k = l_1$ as before. We shall say that G is a group of *maximal diameter* (with respect to Δ) if G has the largest possible finite diameter with respect to Δ, namely $r - 1$. In this case the G_a-orbits coincide with the circles with center a and all are self-paired. By (4.5) and (4.6) we have

(6.1) Theorem. *G is of maximal diameter if and only if by simultaneous row and column permutations applied to the last $r - 2$ rows and columns M can be put in tridiagonal form with all super- and subdiagonal entries $\neq 0$. Putting M into this form is equivalent to renumbering the orbitals so that $\Gamma_q(a) = \Delta_q(a)$, $q = 1, 2, \ldots, r - 1$.*

Suppose now that G is a group of maximal diameter with respect to Δ and assume that the orbitals have been arranged in accordance with (6.1). Then M is a tridiagonal matrix

$$M = \begin{pmatrix} 0 & 1 & & & & \\ k & z_1 & x_2 & & & \\ & y_1 & z_2 & \cdot & & \\ & & y_2 & \cdot & \cdot & \\ & & & \cdot & \cdot & x_{r-1} \\ & & & & y_{r-2} & z_{r-1} \end{pmatrix}$$

with $x_{i+1} y_i \neq 0$, $1 \leqslant i \leqslant r - 1$. By (4.2), $x_{q+1} l_{q+1} = y_q l_q$, $q \geqslant 1$, and hence

$$l_q = \frac{y_{q-1} y_{q-2} \cdots y_1}{x_q x_{q-1} \cdots x_2} k, \; q \geqslant 1. \tag{6.2}$$

By (3.1),

$$y_q \leqslant stx_{q+1}\,,\ q \geqslant 1. \tag{6.3}$$

From the well-known recursion for the characteristic polynomial $f(x)$ of the tridiagonal matrix M it is deduced that M has r distinct eigenvalues (all of which are real). Hence (4.13) and (5.5) are immediately applicable, giving, in particular, that the irreducible constituents of the permutation representation are of multiplicity 1 and that their degrees are given by (5.5).

The following determination of the characteristic polynomial of M is convenient for some applications. In our present case N_0 is nonsingular so we have $MN_0^{-1} = N_0^{-1}C$. For $0 \leqslant m \leqslant r - 1$ define

$$g_m(x) = \sum_{j=0}^{m} \sigma_j^{(m)} x^j, \qquad \sigma_j^{(m)} = \sum_{i=0}^{m} \eta^{ij},$$

where $N_0^{-1} = (\eta^{ij})$. Then $g_0(x) = 1$, $g_1(x) = x + 1$ and $(\det N_0)\, g_{r-1}(x) = g(x)$. Put

$$X_m = (\underbrace{1, 1,\ldots, 1}_{m}, 0,\ldots, 0);$$

then

$$X_m M = (\underbrace{k, k,\ldots, k}_{m-1}, \alpha, \beta, 0,\ldots, 0)$$

with $\alpha = x_{m-1} - z_{m-1}$ and $\beta = x_m$. Hence the jth entry in the vector $X_m M N_0^{-1}$ is

$$k\sigma_j^{(m-2)} + \alpha\eta^{m-1j} + \beta\eta^{mj} = \sigma_j^{(m)} + (k-1)\,\sigma_j^{(m-2)} + (\alpha - 1)\,\eta^{m-1j} + (\beta - 1)\,\eta^{mj}.$$

On the other hand, the jth entry of $X_m N_0^{-1} C$ is $\sigma_{j-1}^{(m-1)}$. (Since M is tridiagonal, N_0 is lower triangular and hence so is N_0^{-1}.) Equating, multiplying by x^j, and summing over j, we get

$$g_m + (k-1)\,g_{m-2} + (\alpha - 1)(g_{m-1} - g_{m-2}) + (\beta - 1)(g_m - g_{m-1}) = xg_{m-1}$$

since $\sum_j \eta^{vj} x^j = g_v - g_{v-1}\,,\ v = 1, 2,\ldots$. Hence, since $k - \alpha = y_{m-1}$, we have

$$x_m g_m(x) = (x + \alpha_m)\, g_{m-1}(x) - y_{m-1} g_{m-2}(x), \qquad m \geqslant 2,$$

with $\alpha_m = x_m - z_{m-1} - x_{m-1}$. Therefore, putting

$$G_m(x) = x_m x_{m-1} \cdots x_1 g_m(x),$$

we have

(6.6) $G_m(x) = (x + \alpha_m) G_{m-1}(x) - x_{m-1}y_{m-1}G_{m-2}(x)$, $m \geqslant 2$, *with* $\alpha_m = x_m - z_{m-1} - x_{m-1}$ *and* $G_0(x) = 1$, $G_1(x) = x + 1$. And by (5.8), since $G_m(x)$ is monic,

(6.7) *The characteristic polynomial of* M *is*

$$f(x) = (x - k) G_{r-1}(x).$$

Note that $f_{m+1}(x) = (x - k) G_m(x)$ is the characteristic polynomial of the matrix obtained by truncating M after $m + 1$ rows and columns and replacing z_m by $z_m + y_m$ to make the column sum k. Also, it is easily seen directly that $G(A) = F$ and hence that $f(A) = 0$.

As a first illustration we consider the symmetric group $S = S^{\Omega}$ on Ω, $|\Omega| = n \geqslant 2$, which (for each k, $1 \leqslant k \leqslant n$) acts faithfully and transitively on the set $\Omega(k) = \{A \subseteq \Omega \mid |A| = k\}$. Since the action of S on $\Omega(k)$ is equivalent to that on $\Omega(n - k)$ we assume that $1 \leqslant k \leqslant n/2$.

For $A \in \Omega(k)$ and $1 \leqslant k \leqslant l \leqslant n/2$, the number of S_A-orbits in $\Omega(l)$ is $k + 1$. Namely, for each t, $0 \leqslant t \leqslant k$, the sets $B \in \Omega(l)$ such that $|B \cap A| = t$ constitute an S_A-orbit, and all are accounted for in this way. Hence if $\pi_k = \sum e_\lambda \zeta_\lambda$ and $\pi_l = \sum f_\lambda \zeta_\lambda$ are the permutation characters of S acting on $\Omega(k)$ and $\Omega(l)$, respectively, the sums being over the irreducible characters ζ_λ of S, a well-known result on the theory of permutation representations (see, e.g., [3]) gives

$$\sum e_\lambda f_\lambda = k + 1.$$

Taking $k = l$ we see that S has rank $k + 1$ as a permutation group on $\Omega(k)$, the S_A-orbits for $A \in \Omega(k)$ being

$$\Gamma_i(A) = \{B \in \Omega(k) \mid |B \cap A| = k - i\} \qquad (i = 0, 1, \ldots, k)$$

Each of these orbits is self-paired since $B \in \Gamma_i(A)$ implies $A \in \Gamma_i(B)$. If $1 \leqslant i \leqslant k - 1$ and $B \in \Gamma_i(A)$, we see easily that $\Gamma_1(B) \cap \Gamma_{i+1}(A) \neq \emptyset$ and that $\Gamma_1(B) \subseteq \Gamma_{i-1}(A) + \Gamma_i(A) + \Gamma_{i+1}(A)$. Hence S has maximal diameter with respect to $\Gamma_1(A)$, $\Gamma_j(A)$ being the circle of radius j about A, $j = 1, 2, \ldots, k$. [Note, however, that S is not primitive on $\Omega(n/2)$, n even.]

Now it follows by (4.13) and the paragraph following (6.3) that each $e_\lambda = 0$ or 1, and that $\sum e_\lambda = k + 1$. Taking $1 \leqslant k < l \leqslant n/2$ we have, therefore, that $e_\lambda = 1$ implies $f_\lambda = 1$. Hence

(6.9) THEOREM ([7], Lemma 3). *There exist distinct nontrivial irreducible characters* $\zeta_1, \ldots, \zeta_{[n/2]}$ *of* S *such that* $\pi_k = 1 + \zeta_1 + \cdots + \zeta_k$, $1 \leqslant k \leqslant [n/2]$.

An interesting example is provided by Janko's new simple group [*6*] of order 175, 560. According to [*6*], this group (let us denote it by J) has a maximal subgroup of order 660 isomorphic with $L_2(11)$. It can be seen, using results in [*6*], that the corresponding representation of J as a primitive group of degree 266 has rank 5 and subdegrees 1, 11, 110, 132, and 12. The matrix M of intersection numbers with respect to the orbital of length 11 is already determined by the subdegrees. For the given arrangement of the subdegrees we get, using (4.2) and (4.9), that

$$M = \begin{matrix} 0 & 1 & 0 & 0 & 0 \\ 11 & 0 & 1 & 0 & 0 \\ 0 & 10 & 4 & 5 & 0 \\ 0 & 0 & 6 & 5 & 11 \\ 0 & 0 & 0 & 1 & 0, \end{matrix}$$

hence J is of maximal diameter. The characteristic polynomial of M is

$$\begin{aligned} f(x) &= (x - 11)(x^4 + 2x^3 - 20x^2 - 27x + 44) \\ &= (x - 11)(x - 1)(x - 4)(x^2 + 7x + 11) \end{aligned}$$

with roots

$$\theta_0 = 11, \theta_1 = 1, \theta_2 = 4, \begin{Bmatrix}\theta_3 \\ \theta_4\end{Bmatrix} = \frac{-7 \pm 5^{1/2}}{2}.$$

The matrix N_0 is

$$\begin{matrix} 1 & & & & \\ 0 & 1 & & & \\ 11 & 0 & 1 & & \\ 0 & 21 & 4 & 5 & \\ 231 & 40 & 67 & 45 & 55. \end{matrix}$$

Applying (5.5) to find the degrees $x_0 = 1, x_2, x_3, x_4$ of the irreducible constituents of the permutation representation we find

$$f_1(x) = f(x)/(x - 1) = x^4 - 8x^3 - 50x^2 + 143x + 484;$$

so by (5.4), trace $f_1(A) = 266\ [231 - 50\ 11 + 484] = 266 \cdot 165$, and $f_1(1) = 570$. Hence $x_1 = 77$. In the same way we get $x_2 = 76$, $x_3 = x_4 = 56$. This is consistent with the character table of [*5*]. From (4.13) we see that the two characters of degree 56 must be conjugate, settling a question raised in Section 30 of [*9*]. As has been noted by several people, this also gives a counter example to Frame's conjecture (cf. [*9*], Section 30) since

$$266^3 \frac{11 \cdot 110 \cdot 132 \cdot 12}{77 \cdot 76 \cdot 56 \cdot 56}$$

is not a square.

Using the remark at the end of Section 4 we find for M_2, M_3, and M_4, respectively,

$$\begin{array}{ccccc|c} 0 & 1 & 0 & 0 & 0 & 1 \\ 110 & 45 & 40 & 45 & 55 & 110 \\ 0 & 4 & 10 & 5 & 0 & 11 \\ 0 & 54 & 60 & 55 & 55 & 132 \\ 0 & 6 & 0 & 5 & 0 & 12 \end{array} \qquad \begin{array}{ccccc|c} 0 & 1 & 0 & 0 & 0 & 1 \\ 132 & 66 & 66 & 60 & 55 & 132 \\ 0 & 55 & 54 & 60 & 55 & 110 \\ 0 & 5 & 6 & 0 & 11 & 11 \\ 0 & 5 & 6 & 12 & 11 & 12 \end{array}$$

$$\begin{array}{ccccc|c} 0 & 1 & 0 & 0 & 0 & 1 \\ 12 & 0 & 1 & 0 & 0 & 12 \\ 0 & 11 & 5 & 6 & 12 & 132 \\ 0 & 0 & 5 & 6 & 0 & 110 \\ 0 & 0 & 1 & 0 & 0 & 11. \end{array}$$

The columns after the vertical lines indicate the arrangements of the J_a-orbits into circles. The diameters are, respectively, 2, 2, 3.

7. Some Applications

For the applications to be given in this section we need to consider the partial difference equation

$$h_m(x) = (x - (u + v))\, h_{m-1}(x) - uvh_{m-2}(x), \qquad m \geqslant 2 \tag{7.1}$$

with

$$h_0(x) = 1,\ h_1(x) = x - v.$$

The solution can be written in terms of the polynomials $k_m(x)$ defined by

$$\left.\begin{aligned} k_{2h}(x + 2 + x^{-1}) &= \frac{x^{2h} - 1}{x^{h-1}(x^2 - 1)} \\ k_{2h+1}(x + 2 + x^{-1}) &= \frac{x^{2h+1} - 1}{x^h(x - 1)} \end{aligned}\right\} \quad (h \geqslant 0).$$

First observe that

$$\left.\begin{aligned} k_{2h}(x) &= k_{2h-1}(x) - k_{2h-2}(x) \\ \text{and} \quad k_{2h+1}(x) &= xk_{2h}(x) - k_{2h-1}(x) \end{aligned}\right\} \quad (h \geqslant 1). \tag{7.2}$$

Now define polynomials $\gamma_m(x) = \gamma_m(x, u, v)$ by

$$\left.\begin{aligned} \gamma_{2h}(x) &= x(x - (u + v))(uv)^{h-1}\, k_{2h}\left(\frac{(x - (u + v))^2}{uv}\right) \\ \gamma_{2h+1}(x) &= x(uv)^h\, k_{2h+1}\left(\frac{(x - (u + v))^2}{uv}\right) \end{aligned}\right\} \quad (h \geqslant 0). \tag{7.3}$$

Using (7.2) we can verify that

$$\gamma_m(x) = (x - (u + v))\,\gamma_{m-1}(x) - uv\gamma_{m-2}(x), \qquad m \geqslant 2. \tag{7.4}$$

Thus the $\gamma_m(x)$ satisfy the recursion (7.1) but not the initial conditions, for $\gamma_0(x) = 0$, $\gamma_1(x) = x$. Define polynomials $h_m(x) = h_m(x, u, v)$ by

$$\begin{aligned} h_0(x) &= 1, \\ h_m(x) &= \gamma_m(x) - vh_{m-1}(x), \qquad m \geqslant 1. \end{aligned} \tag{7.5}$$

so that $h_1(x) = x - v$. Now we verify at once by induction that

$$\gamma_m(x) = (x - u)\,h_{m-1}(x) - uvh_{m-2}(x), \qquad m \geqslant 2, \tag{7.6}$$

from which it follows that the $h_m(x)$ solve (7.1).

Observe finally that

$$h_m(x, u, u) = u^m k_{2m+1}\left(\frac{x}{u}\right), \qquad m \geqslant 0. \tag{7.7}$$

For when $u = v$, it is easily verified using (7.2) that the polynomials defined by (7.7) solve (7.1)

We now return to the consideration of a transitive group G of rank r and put $\Delta = \Gamma_1$. Let us look at the case in which M has form

$$\begin{pmatrix} 0 & 1 & & & & \\ u(v+1) & u-1 & \ddots & & & \\ & uv & \ddots & 1 & & \\ & & \ddots & u-1 & 1 & \\ & & & uv & u(v+1)-1 \end{pmatrix}.$$

Put $\tilde{A} = A + (v + 1)\,I$, then the entry in the (a, b)-position of A^q is

$$\tilde{\eta}_{qj} = \sum_{q=0}^{j} (v + 1)^{q-j}\,\eta_{qj}\,, \tilde{\eta}_{0j} = \delta_{0j}\,.$$

Putting $\tilde{N} = (\tilde{\eta}_{qj})$ and $T = (\binom{q}{j}(v + 1)^{q-j})_{q,j}$, we have $\tilde{N} = TN$, so by (5.2), $\tilde{N}\tilde{M} = S\tilde{N}$ with $\tilde{M} = M + (v + 1)\,I$. But this is the recursion considered in Lemma 2.5 of [*2*], so, in the notation of [*2*],

$$\tilde{\eta}_{qj} = [(1 + u)^{q-1}\,(1 + v)^q\,(1 - uv)]^{q-j}_{-1}, \qquad 0 \leqslant q \leqslant 2r - 2 - j.$$

In particular,

$$\text{trace } \tilde{A}^q = n[(1 + u)^{q-1}\,(1 + v)^q\,(1 - uv)]^{q-1}_{-1}, \quad 0 \leqslant q \leqslant 2r - 2. \quad (7.8.)$$

Now put $H_m(x) = G_m(x - (v + 1))$ where the $G_m(x)$ solve the recursion (6.6) corresponding to our given matrix M. Then the $H_m(x)$ solve (7.1), so $H_m(x) = h_m(x, u, v)$ as defined in (7.5). By (6.7),

(7.9) *The characteristic polynomial* $\rho(x)$ *of* $\tilde{A}$ *is*

$$\rho(x) = (x - (u + v)(v + 1))\, h_{r-1}(x, u, v).$$

(7.10) THEOREM. *If the intersection matrix* M *has the form*

$$\begin{pmatrix} 0 & 1 & & & & \\ u(u+1) & u-1 & 1 & & & \\ & u^2 & u-1 & \ddots & & \\ & & u^2 & \ddots & 1 & \\ & & & \ddots & u-1 & 1 \\ & & & & u^2 & u^2+u-1 \end{pmatrix}$$

with $u > 1$ *then* $r = 2$, i.e., G *is doubly transitive* (*of degree* $u^2 + u + 1$).

Proof. By (7.9) and (7.7) the characteristic polynomial for $\tilde{M}$ is

$$\rho(x) = (x - (u + 1)^2)\, u^{r-1} k_{2r-3}\left(\frac{x}{u}\right).$$

Hence, since we have the formula (7.8) for the trace of $\tilde{A}^q$ the analysis of ([2], Section IV) is directly applicable, giving $2r - 1 = 3$ or $r = 2$.

It can be shown that for $r \geqslant 3$, M has the form of (7.10) with $u = s = t$ if and only if $\mathbf{P}$ (as defined in Section 2) is a nondegenerate $(2r - 1) -$ gon. Then Theorem 1 of [2] can be directly applied, but of course (7.10) is a stronger result in our context.

A curious consequence of (7.10) is

(7.11) COROLLARY. *Let* G *be a transitive permutation group of rank* r *with subdegrees* $1, u^{2\alpha-1}(u + 1), \alpha = 1, 2, \ldots, r - 1, u > 1$. *Then* G *is doubly transitive.*

Proof. Using (4.2) and (4.9) it is easily seen that in this case M has the form of (7.10).

(7.12) THEOREM. *If* M *has the form*

$$M = \begin{pmatrix} 0 & 1 & & & & \\ u(v+1) & u-1 & 1 & & & \\ & uv & \ddots & \ddots & & \\ & & \ddots & \ddots & 1 & \\ & & & \ddots & u-1 & v+1 \\ & & & & uv & (u-1)(v+1) \end{pmatrix}$$

then $r = 2, 3, 4, 5$ *or* 7, *and if* $u > 1$ *and* $v > 1$ *then* $r \neq 7$.

Proof. We may assume that $r \geqslant 3$. Again we work with

$$\tilde{A} = A + (v + 1) I$$

and $\tilde{M} = M + (v + 1) I$, and obtain from Lemma 2.5 of [2] that

$$\operatorname{trace} \tilde{A}^q = [(1 - u)^{q-1} (1 - v)^q (1 - uv)]_{-1}^q \qquad (0 \leqslant q \leqslant 2r - 3).$$

By (5.7) and (6.6) we find that the characteristic polynomial $\rho(x)$ for $\tilde{M}$ is given by $(x - (u + 1)(v + 1))\, h(x)$ where

$$h(x) = (x - u)\, h_{r-2}(x) - uvh_{r-3}(x),$$

$h_m(x) = h_m(x, u, v)$ as defined in (7.5). Hence by (7.6)

$$\rho(x) = (x - (u + 1)(v + 1))\, \gamma_{r-1}(x),$$

where $\gamma_m(x)$ is defined by (7.3). Now the analysis of ([2], Sections V–VII) is directly applicable, giving $2r - 2 = 4$, 6, 8, or 12 with $2r - 2 \neq 12$ if $u > 1$ and $v > 1$.

Actually the analysis of [2] gives more, namely, in case $r = 4$, uv is a square, while if $r = 5$, $2uv$ is a square (cf. Theorem 1 of [2]).

If $r \geqslant 3$, it can be shown that M has the form of (7.12) with $u = s$, $v = t$, if and only if $\mathbf{P}$ is a generalized $(2r - 2) -$ gon.

The analog of (7.11), proved in the same way, is

(7.13) Corollary. *If G is a transitive permutation group of rank r with subdegrees* $1, u^\alpha v^{\alpha-1}(v + 1), \alpha = 1, 2,..., r - 2)$, *and* $u^{r-1}v^{r-2}$, *then the conclusions of* (7.12) *hold.*

Appendix

We indicate here a proof of a simple but very useful result due to Wielandt (unpublished), essential use of which was made in Section 4.

Let H be an intransitive group of permutations on a finite set Ω. Let D be the permutation representation and let C be the commuting algebra of D. Arrange the points of Ω according to the H-orbits, so that, if there are t of these, $D(x)$ takes the form

$$D(x) = \operatorname{diag}\{D_1(x), D_2(x),..., D_t(x)\}$$

for $x \in H$. If $X = (X_{ij})_{1 \leqslant i,j \leqslant t}$ is the corresponding blocking of $X \in C$, then

$$X_{ij} D_j(x) = D_i(x)\, X_{ij} \qquad (1 \leqslant i, j \leqslant t),$$

from which it follows that X_{ij} has constant column sum. Moreover, there exists a nonsingular matrix P such that

$$P^{-1}XP = \begin{pmatrix} \hat{X} & 0 \\ 0 & * \end{pmatrix}$$

where $\hat{X}$ is obtained from X by replacing each block X_{ij} by its column sum. We see this by reducing D to irreducible constituents and suitably rearranging these. Now it follows that

The mapping $X \to \hat{X}$ is an algebra homomorphism of C onto a subalgebra $\hat{C}$ of the algebra of all $t \times t$ matrices.[2]

Acknowledgments

The author is indebted to T. Bickel and J. E. McLaughlin for substantial help in the development of the material of this paper.

References

1. Bickel, T. Some properties of groups admitting (B, N)-pairs (Ph.D. Thesis, University of Michigan, 1965).
2. Feit, W. and Higman, G. The nonexistence of certain generalized polygons. *J. Algebra* 1 (1964), 114-131.
3. Frame, J. S. Double coset matrices and group characters. *Bull. Am. Math. Soc.* **49** (1943), 81-92.
4. Higman, D. G. Finite permutation groups of rank 3. *Math. Z.* **86** (1964), 145-156.
5. Higman, D. G. Primitive rank 3 groups with a prime subdegree. *Math. Z.* **91** (1966), 70-86.
6. Janko, Z. A new finite simple group with abelian 2-Sylow subgroups and its characterization. *J. Algebra* 3 (1966), 147-186.
7. Livingstone, D. and Wagner, A. Transitivity of unordered sets. *Math. Z.* **90** (1965), 393-403.
8. Tits, J. Algebraic and abstract simple groups. *Ann. Math.* **80** (1964), 313-329.
9. Wielandt, H. "Finite Permutation Groups." Academic Press, New York, 1964.

[2] This is one of the results presented to the Conference on Finite Groups held in East Lansing and Ann Arbor in March of 1964.