BLOCK, R. E.
Math. Zeitschr. 96, 33—49 (1967)

On the Orbits of Collineation Groups

RICHARD E. BLOCK*

Received May 2, 1966

1. Introduction

In this paper we consider some results on the orbits of groups of collineations, or, more generally, on the point and block classes of tactical decompositions, on symmetric balanced incomplete block designs (symmetric $BIBD=(v, k, \lambda)$-system = finite λ-plane), and we consider generalizations to (not necessarily symmetric) *BIBD* and other combinatorial designs. The results are about the number of point and block classes (or orbits, i.e. sets of transitivity) and the numbers of elements in these classes.

In Sections 2, 3 and 4 below we exhibit the key role of the rank of the incidence matrix of a design, while the remainder of the paper uses more specific properties of the incidence relations. Included in Section 2 is a simple new proof of the theorem of DEMBOWSKI [7] on the equality of the numbers of point and block classes for a tactical decomposition of a symmetric *BIBD* (for the orbits of a group of collineations the equality is a consequence of a result of BRAUER [*4*, p. 934], and was proved again by PARKER [*12*] and HUGHES [*10*]). Our proof generalizes the equality to a pair of inequalities for non-symmetric designs. In Section 3 we consider transitive groups of collineations, and in Section 4, cyclic groups.

We use an integral matrix congruence in Section 5 to prove a type of symmetry for tactical decompositions on symmetric designs. In particular for primes not dividing $n=k-\lambda$ we prove that such a decomposition is p-symmetric, i.e. the point and block classes can be paired so that paired classes have numbers of elements divisible by the same powers of p; this generalizes other results of DEMBOWSKI [7]. In Section 6 these results are used in conjunction with the theory of rational congruence of quadratic forms to obtain number-theoretic conditions on the numbers of elements in the point and block classes, generalizing the result of LENZ [*11*]. Finally, in Section 7 we generalize the result of Section 5 on p-symmetry to some inequalities for non-symmetric designs.

2. One-Sided Tactical Decompositions

For any (generalized) incidence structure, i.e. set of points and blocks with an incidence relation between points and blocks, a *tactical decomposition* is a partition of the points into point classes and of the blocks into block classes

* This work was supported in part by the U.S. National Aeronautics and Space Administration, under a Contract with the Jet Propulsion Laboratory of the California Institute of Technology.

such that the number of points in a point class which lie on a block depends only on the class in which the block lies, and similarly with point and block interchanged. A principle example is obtained by taking as the point and block classes the orbits of any collineation group. We extend the definition of a tactical decomposition in the following way.

Let $M=(m_{ij})$ be a $v\times b$ matrix with entries in a field F. Suppose that the set of row indices is the disjoint union of t nonempty subsets $R_1, \ldots, R_t$, and that the set of column indices is the disjoint union of t' nonempty subsets $C_1, \ldots, C_{t'}$. We shall say that M has a *right tactical decomposition*, with *row classes* R_i and *column classes* C_i, if for every i, j ($i=1, \ldots, t; j=1, \ldots, t'$) the submatrix (m_{hl}) ($h\in R_i$, $l\in C_j$) has constant column sums s_{ij}. The $t\times t'$ matrix $S=(s_{ij})=S_{cs}$ will be called the *associated matrix of column sums*. Similarly a *left tactical decomposition* and its *associated matrix* S_{rs} *of row sums* are defined by requiring the submatrices to have constant row sums.

We define a *tactical decomposition for a matrix* to be a partition of the row and column indices which is simultaneously a left *and* right tactical decomposition. Also, onesided tactical decompositions on incidence structures are defined by requiring only one of the two conditions on the point and block classes.

Thus a tactical decomposition on an incidence structure corresponds to a tactical decomposition on the incidence matrix, and similarly for right and left tactical decompositions.

Theorem 2.1. *Let M be a $v\times b$ matrix of rank ρ, having a right (resp., left) tactical decomposition with t row classes and t' column classes. Let ρ_{cs} (resp., ρ_{rs}) be the rank of the associated matrix of column (resp., row) sums. Then*

$$t-(v-\rho)\leqq\rho_{cs}(\textit{resp.}, t'-(b-\rho)\leqq\rho_{rs}). \tag{2.1}$$

In particular

$$t\leqq t'+v-\rho(\text{resp.}, t'\leqq t+b-\rho). \tag{2.2}$$

Proof. By symmetry, it suffices to give the proof for a right tactical decomposition. There is a set of ρ linearly independent rows, and the indices of the remaining $v-\rho$ rows lie in at most $v-\rho$ of the row classes. Hence there are $t-(v-\rho)$ row classes such that the rows of M indexed by the union of these classes are linearly independent. In the associated matrix of column sums, the rows corresponding to these $t-(v-\rho)$ classe must be linearly independent, since a dependence relation among them would give a dependence relation (with the same coefficients, only repeated) among a set of rows of M. Hence $t-(v-\rho)\leqq\rho_{cs}$, and the final result holds because $\rho_{cs}\leqq t'$.

There are a number of immediate consequences of this theorem. In the statement of these results, t will continue to denote the number of row or point classes (or orbits) and t' the number of column or block classes (or orbits).

Corollary 2.1. *If a nonsingular matrix has a tactical decomposition then $t=t'$. Moreover the associated matrices of row sums and of column sums are both nonsingular.*

This includes the corresponding results of DEMBOWSKI (Theorem 2 and Lemma 7 of [7]) for symmetric *BIBD*.

Corollary 2.2. *For a right tactical decomposition (or a group of collineations) on a BIBD,* $t \leqq t'$.

In fact this result holds for a wider class of designs, namely, for any design having an incidence matrix with linearly independent rows. In addition to *BIBD*, such designs include the group divisible designs which are regular (that is, for which $r > \lambda_1$ and $rk > v\lambda_2$) (see [3]) and other partially balanced incomplete block designs satisfying certain conditions on the parameters (see [6]).

A *BIBD* is called resolvable if the blocks are partitioned into classes such that each point is on exactly one block in each class. Thus a resolvable *BIBD* is an example of a *BIBD* with a tactical decomposition with $t=1$ and $t'=r$ (where v, b, r, k, λ as usual denote the parameters of a *BIBD*). By (2.2), $b-v \geqq r-1$. This inequality is part of a theorem of BOSE [2] which also says that equality holds if and only if pairs of blocks in distinct classes always have the same number of points in common. A resolvable *BIBD* satisfying this last condition is called affine. For these designs there is the following recent result of DEMBOWSKI [8, p. 164], which he has proved in a different way.

Corollary 2.3. *For a tactical decomposition on an affine resolvable BIBD,*

$$0 \leqq t' - t \leqq r-1$$

Proof. This follows immediately from (2.2) and the theorem of Bose.

A (binary) *constant-distance matrix* is a $v \times b$ matrix with entries chosen from two symbols such that any two rows differ in the same number d of columns, where $d > 0$. Examples include the Hadamard matrices and the incidence matrices of *BIBD*. An incidence structure is called a *constant-distance design* if its incidence matrix is a constant-distance matrix.

Corollary 2.4. *For a right tactical decomposition (or a group of collineations) on a* $v \times b$ *constant-distance matrix* M, $t \leqq t'+1$.

Proof. With the two symbols chosen as ± 1, the matrix MM' is a $v \times v$ matrix A with b on the main diagonal and $b-2d$ elsewhere. The determinant of A is $(2d)^{v-1}[2d+v(b-2d)]$. If the rank ρ of M is v then $t \leqq t'$ by (2.2). If $\rho < v$ then $\det A = 0$, so that $2d+v(b-2d)=0$. Deleting a row keeps b and d fixed but destroys this last equation. Hence $\rho = v-1$ and, by (2.2), $t \leqq t'+1$, which completes the proof.

In particular, a constant-distance matrix has $v \leqq b+1$. Corollary 2.3 generalizes a result in [1], in which it is shown that if $t'=1$ then $t \leqq 2$. Examples with $t=2$ and $t'=1$ were obtained from Hadamard matrices in [1] [1].

The following is a simpler proof and generalization of another result proved by DEMBOWSKI [7] (pp. 66–69) for symmetric *BIBD*.

[1] I would like to correct an error in the remarks in the last few lines of [1]: It may be shown that H itself is isomorphic to S_6; hence if $s=2$, G has order $16 \cdot 720$, and if $s>1$ then G contains a subgroup isomorphic to S_6 which fixes 4^{s-2} columns.

Corollary 2.5. *Let there be given two tactical decompositions of a nonsingular matrix. Then every row class of the second decomposition is contained in a row class of the first decomposition if and only if the same is true for the column classes.*

Proof. If a column class of the second decomposition contains members of distinct classes C_j and C_l of the first decomposition then the hypothesis on row classes implies the equality of columns j and l of S_{cs} of the first decomposition, contradicting Corollary 2.1.

We next consider a couple of results on the associated matrices of a tactical decomposition. We write $S_{cs}=S=(s_{ij})$ and $S_{rs}=A=(a_{ij})$; as before, ρ_{cs} and ρ_{rs} denote the ranks of these matrices.

Corollary 2.6. *Suppose there is given a tactical decomposition on a $v\times b$ matrix M of rank ρ over a field of characteristic 0. Then*

$$\max\{t-(v-\rho), t'-(b-\rho)\}\leqq\rho_{cs}=\rho_{rs}.$$

Proof. Let v_i and b_j denote the number of elements in R_i and C_j respectively. Then $v_i a_{ij}=s_{ij} b_j$, which gives the equality of ranks.

Theorem 2.2. *Let M be a $v\times b$ matrix over a field F, with a tactical decomposition. Then MM' is similar to a matrix having $(S_{cs}S'_{rs}, O_{t\times(v-t)})$ as its first t rows. In particular, the characteristic polynomial and the determinant of $S_{cs}S'_{rs}$ divide those of MM'.*

Proof. For $i=1,\ldots,t$(resp. t') let ζ_i(resp. η_i) denote the v-tuple (resp., b-tuple) having 1 in each place indexed by an element of R_i (resp. C_i) and 0 elsewhere. We have

$$\zeta_i M=\sum_{j=1}^{t'} s_{ij}\eta_j, \quad \eta_i M'=\sum_{j=1}^{t} a_{ji}\zeta_j.$$

Hence $\zeta_1,\ldots,\zeta_t$ are a basis of a space invariant under MM', and the matrix of MM' with respect to this basis is SA'. This gives the result.

3. Collineation Groups

Let $M=(m_{ij})$ be a $v\times b$ matrix with entries in a field F. A *collineation* x of M is a pair $\pi=\pi(x)$, $\sigma=\sigma(x)$ of permutations, π acting on the row indices and σ on the column indices, such that $m_{ij}=m_{\pi(i),\sigma(j)}$ for all i,j. With $\pi(x)$ and $\sigma(x)$ also denoting the corresponding permutation matrices, one has

$$M\sigma(x)=\pi(x)M. \tag{3.1}$$

A collineation, in the usual sense, of an incidence structure corresponds to a collineation of the incidence matrix of the structure.

If G is a group of collineations of M then π and σ give representations of the group algebra FG acting on the spaces of v-tuples and b-tuples, respectively, and right multiplication by M is an FG-module homomorphism. The isomorphism of the image and coimage gives the following.

Lemma 3.1. *For a group of collineations on a matrix of rank ρ, the matrix representation π has a constituent of degree ρ which is equivalent to a constituent of σ.*

The collineations of M are unchanged if the distinct entries of M are replaced by distinct elements in any set. The following lemma shows that in applications of (2.2) for orbits we may always assume that M is over the reals. For some M we will thus get a sharper inequality, since the rank may go up.

Lemma 3.2. *The distinct entries of a matrix of rank ρ over any field F may be replaced by distinct real numbers in such a way that the new matrix has rank at least ρ over the reals.*

Proof. There is a $\rho \times \rho$ submatrix of M with nonzero determinant. If this submatrix contains m distinct entries, we may regard its determinant as the value of a polynomial function of m variables with integer coefficients not all 0. Replacing the distinct entries of M by distinct real numbers in such a way that the m entries of the submatrix are replaced by real numbers algebraically independent over the rationals, we see that the new matrix has a $\rho \times \rho$ submatrix with nonzero determinant, and the proof is complete.

Theorem 3.1. *Let G be a group of collineations of a $v \times b$ matrix M of rank v. Suppose that $\sigma(G)$ (and hence also $\pi(G)$) is transitive, and let u_π and u_σ denote the number of orbits of the subgroups of $\pi(G)$ and $\sigma(G)$, respectively, fixing one index. Then $u_\pi \leqq u_\sigma$, and there are at most u_σ distinct entries in M.*

Proof. By Lemma 3.2 we may assume that M is over the complex numbers. If

$$\sum_a c_a \chi^a$$

expresses the character χ_π of $\pi(G)$ as a sum of absolutely irreducible characters, and similarly for

$$\sum_a d_a \chi^a$$

as an expression of χ_σ, then $c_a \leqq d_a$ for all a, by Lemma 3.1. But by the orthogonality relations

$$\begin{aligned} u_\pi |G| = \sum_{x \in G} \chi_\pi^2(x) &= \sum_x \left[\sum_a c_a \chi^a(x)\right] \left[\sum_a c_a \overline{\chi^a(x)}\right] \\ &= |G| \sum_a c_a^2 \leqq |G| \sum_a d_a^2 = \sum_x \chi_\sigma^2(x) = u_\sigma |G|, \end{aligned}$$

so that $u_\pi \leqq u_\sigma$. If j is a given column index and $H = \{x \in G \mid \sigma(x) j = j\}$ then $\pi(H)$ has at least as many orbits as the number m_j of distinct entries in column j of M. But by (2.2), $\pi(H)$ has at most u_σ orbits, and so $m_j \leqq u_\sigma$. Since $\sigma(G)$ is transitive, all columns of M have the same set of entries, and so there are exactly m_j distinct entries in M. Thus the theorem is proved.

Corollary 3.1. *Let G be a group of collineations of a $v \times b$ matrix M of rank v where $v > 1$. If G is doubly transitive on the column indices then $v = b$, M is an* *incidence matrix of a symmetric BIBD, and G is doubly transitive on the row indices.*

Proof. Since $u_\pi > 1$, we have $u_\pi = u_\sigma = 2$, and G is doubly transitive on the row indices. Also by Theorem 3.1, there are at most two distinct entries in M, say α and β. By the transitivity of π and the double transitivity of σ, all rows of M have the same number of α's, and every pair of distinct columns has the same number of α's in common. This says that M' is the incidence matrix of a *BIBD*, with α and β in place of 1 and 0. Since $v = \text{rank}\, M \leqq b$, this *BIBD* is symmetric, and the proof is complete.

We can also obtain some information in the case in which the rows of M are not linearly independent.

Theorem 3.2. *Let G be a group of collineations of a $v \times b$ matrix M of rank $\rho > 1$. Suppose that $\sigma(G)$ is doubly transitive on the column indices. Then $\sigma(G)$ is equivalent (as a matrix representation) to a constituent of $\pi(G)$ (and in particular $v \geqq b$), and $\rho = b$ or $b-1$.*

Proof. Again by Lemma 3.2 we may assume that M is over the complex numbers. Let σ_1 be a constituent of σ which is equivalent to a constituent of degree ρ of π. Since $\sigma(G)$ is doubly transitive, it is equivalent to the sum of two absolutely irreducible constituents, one of them the identity. Therefore, since $\rho > 1$, σ_1 must have degree b or $b-1$. Since π contains the identity representation as a constituent and is completely reducible, the conclusions of the theorem hold.

That it can happen that $\rho = b-1$ is shown by the following example: take the *BIBD* with $2m$ points whose blocks consist of all sets of m of the points, and let M be the transpose of the incidence matrix, with 1 and -1 in place of 1 and 0. Here G acts as the symmetric group on the $2m$ column indices, and the row sums are zero, so that the rank is $b-1$. However we do have the following result.

Corollary 3.2. *Under the hypotheses of Theorem 3.2, if the entries of M are nonnegative real numbers then $\rho = b$.*

Proof. Suppose not. Then $\rho = b-1$, and the coefficients in a dependence relation among the columns are unique up to scalar multiple. It then follows from the double transitivity that all the coefficients are the same, that is, all row sums are zero. Then all entries are zero, contradicting $\rho > 1$, and the proof is complete.

In fact, if the entries are 1 and 0, and if all row sums are equal (which will be the case if π is transitive), then it is immediate that M is the transpose of the incidence matrix of a *BIBD*.

4. The Lengths of the Orbits

For left or right tactical decompositions we shall write v_i for the number of elements in a row class R_i, and b_i for the number of elements in a column class C_i. For any positive integer j we shall write a_j for the number of row classes R_i with $v_i = j$, and c_j for the number of column classes C_i with $b_i = j$. We have the following immediate consequence of Theorem 2.1.

Theorem 4.1. *Let M be a $v \times b$ matrix of rank ρ, with a left tactical decomposition. Suppose that $a_j \geqq c_j$ for every integer $j > 1$ except possibly one, say $j = m$. Then $a_m \leqq c_m + (v - \rho)/(m-1)$.*

Proof. By the second half of (2.2), $v - t \leqq b - t' + v - \rho$. Hence

$$\sum_j a_j(j-1) \leqq \sum_j c_j(j-1) + v - \rho,$$

whence the result.

Corollary 4.1. *Suppose there is a collineation of prime order p on a BIBD or on a constant-distance design (or matrix). Then the number of p-cycles on the blocks (columns) is at least the number of p-cycles on the points (rows).*

Proof. In this case $a_j = c_j = 0$ for $j > 1$ except for $j = p$. Moreover $v - \rho = 0$ except for the constant-distance designs, where $v - \rho \leqq 1$. The result then follows from the theorem except when $p = 2$ and $v - \rho = 1$ for a constant-distance design. In this case, in the notation of the proof of Corollary 2.4, $2d + v(b - 2d) = 0$, and the sum of the rows is orthogonal to each of the rows and so each column sum is 0. This implies that $\rho_{rs} < t$, and using (2.1) instead of (2.2) in the proof of Theorem 4.1 we get a strict inequality in that theorem, which gives the result.

Such a result holds for any collineation group in which every element of the group fixes the same set of points (rows) and blocks (columns), i.e. when each v_i and b_i is either 1 or the group order.

Corollary 4.1 is also a consequence of the next theorem, which generalizes the result of BRAUER [*4*] and PARKER [*12*] that says that a collineation on a symmetric *BIBD* (or a nonsingular matrix) has the same cycle lengths on the points as on the blocks.

Theorem 4.2. *Let x be a collineation of a $v \times b$ matrix M of rank ρ. For each positive integer j let a_j and c_j denote the number of j-cycles of x on the row indices and on the column indices, respectively. If m is a positive integer such that $a_n \geqq c_n$ for every proper multiple n of m then $a_m \leqq c_m + (v - \rho)/\varphi(m)$ (φ the Euler function).*

Proof. By Lemma 3.2 we may suppose that M is over the complex numbers. By Lemma 3.1 applied to the group generated by x, all except at most $v - \rho$ of the characteristic roots (counting multiplicity) of $\pi(x)$ are characteristic roots of $\sigma(x)$. Since an n-cycle contributes the n-th roots of unity to the characteristic roots of a permutation matrix, among the characteristic roots of $\pi(x)$ there are $\varphi(m)\, a_m$ which are primitive m-th roots of unity, in addition to those which come from cycles of length a proper multiple of m. Of these $\varphi(m)\, a_m$ roots, at least $\varphi(m)\, a_m - (v - \rho)$ give characteristic roots of $\sigma(x)$ which come from m-cycles, that is, $\varphi(m)\, a_m - (v - \rho) \leqq \varphi(m)\, c_m$, and the proof is complete.

For *BIBD* and also for constant-distance designs the conclusion of the theorem says that $a_m \leqq c_m$, and $a_n = c_n$ for every proper multiple n of m (in the case of a constant-distance design when $m=2$ and $v-\rho=1$, the characteristic root that is deleted by the above use of Lemma 3.1 has the value 1, since in this case the row vector $(1, \ldots, 1)$ spans the null space of M).

5. A Matrix Congruence and an Application to Symmetric Designs

We now begin proving results which depend on more specific features of an incidence matrix than its rank. For any positive integer m, let I_m and J_m denote respectively the $m\times m$ unit matrix and the $m\times m$ matrix with all entries 1. For a right or left tactical decomposition of a matrix (or of an incidence structure) we continue to write $v_i (i=1, \ldots, t)$ and b_j $(j=1, \ldots, t')$ for the cardinalities of the i-th row class and j-th column class, respectively, and we write V for the $t\times t$ diagonal matrix $\mathrm{diag}(v_1, \ldots, v_t)$ and B for the $t'\times t'$ diagonal matrix $\mathrm{diag}(b_1, \ldots, b_{t'})$. Also S denotes the associated matrix of column or row sums.

Lemma 5.1. *Suppose there is a right tactical decomposition of a $v\times b$ matrix $M=(m_{ij})$ over a field F, and suppose there are elements $\alpha \neq 0$ and β in F such that $MM'=\alpha I_v+\beta J_v$. Then*

$$SBS'=\alpha V I_t+\beta V J_t V. \tag{5.1}$$

The determinant of the right side W of (5.1) *is*

$$\left(\prod_{i=1}^{t} v_i\right) \alpha^{t-1}(\alpha+\beta v).$$

Moreover S has rank at least $t-1$, and rank exactly t provided $\alpha+\beta v\neq 0$. If the entries of M are integers and if $t=t'$ then

$$\alpha^{t-1}(\alpha+\beta v)\prod_{i=1}^{t}(v_i/b_i)=\det S^2 \tag{5.2}$$

and so is the square of an integer.

Proof. Counting

$$\sum_{l=1}^{b}\Big(\sum_{k\in R_i} m_{kl}\Big)\Big(\sum_{k\in R_j} m_{kl}\Big)$$

in two ways, one gets

$$\sum_{q=1}^{t'} b_q s_{iq} s_{jq}=v_i v_j \beta+\delta_{ij} v_i \alpha,$$

so that (5.1) holds. The determinant of W can be computed by subtracting v_j/v_1 times the first column from the j-th column, $j=2, \ldots, t$, and then adding to the first row the rows after the first, thus making a triangular matrix with diagonal entries $\alpha v_1+\beta v v_1, \alpha v_2, \ldots, \alpha v_t$. Since $\det MM'=\alpha^{v-1}(\alpha+\beta v)$, if $\alpha+v\beta\neq 0$ then the rank ρ of M is v, while if $\alpha+v\beta=0$ then (as in the proof of Corollary 2.4) $\rho=v-1$. The statements about the rank of S then follow from Theorem 2.1. The final statement of the lemma follows immediately from the first two conclusions.

Suppose that the hypotheses of Lemma 5.1 hold and that $\alpha+v\beta\neq 0$. Then S has rank t, and $t\leqq t'$. Take any t linearly independent columns of S; by reordering they may be assumed to be the first t columns. Let S_1 and S_2 denote the submatrices of S consisting respectively of these first t columns and of the remaining $t'-t$ columns of S. Define $t'\times t'$ matrices S_0 and W_0 by

$$S_0=\begin{bmatrix} S_1 & S_2 \\ 0 & I_{t'-t} \end{bmatrix}, \qquad W_0=\begin{bmatrix} W & S_2 B_4 \\ B_4' S_2' & B_4 \end{bmatrix}$$

where B_4 is the $(t'-t)\times(t'-t)$ diagonal matrix $\operatorname{diag}(b_{t+1}, \ldots, b_{t'})$.

Theorem 5.1. *Under the hypotheses of Lemma 5.1, if* $\alpha+v\beta\neq 0$ *and* S_0 *and* W_0 *are constructed as above, then*

$$S_0 B S_0' = W_0 \tag{5.3}$$

and S_0 *is nonsingular.*

Proof. The nonsingularity of S_0 follows from its construction, and (5.3) follows from (5.1) by inspection.

For a *BIBD* with the discrete tactical decomposition, i.e. with all v_i and b_j equal to 1, (5.3) becomes the congruence studied by Connor [5].

For any prime p and any positive integer a, define $\varphi_p(a)$ by writing

$$a=p^{\varphi_p(a)}\,a^*,$$

where a^* is an integer prime to p.

Lemma 5.2. *Suppose that the hypotheses of Lemma 5.1 hold for an integral matrix* M, *and that* $t=t'$. *If* p *is a prime not dividing* $\alpha(\alpha+\beta v)$ *then* $p\nmid\det S$, *and if an entry* s_{ij} *of* S *is not divisible by* p *then* $\varphi_p(b_j)\geqq\varphi_p(v_i)$.

Proof. Let M_p and S_p be the matrices obtained from M and S by taking residues of the entries modulo p. Since $\alpha(\alpha+\beta v)\not\equiv 0 \bmod p$, by Lemma 5.1 S_p has rank t and hence $p\nmid\det S$. Therefore $(S')^{-1}$ exists and is a rational matrix with denominators prime to p. By (5.1),

$$S\,B=(\alpha\,V\,I+\beta\,V\,J\,V)\,(S')^{-1}.$$

If $p^a\mid v_i$ then each entry of the i-th row of the right side, and so of SB, is divisible by p^a. In particular $p^a\mid s_{ij}\,b_j$, so that $p^a\mid b_j$. This gives the conclusion of the lemma.

For any set P of primes, two sequences $v_1, \ldots, v_t$ and $b_1, \ldots, b_t$ of positive integers will be called *P-symmetric* (*p-symmetric* if $P=\{p\}$) if the sequences can be reordered so that $\varphi_p(v_i)=\varphi_p(b_i)$ for $i=1, \ldots, t$ and for every p in P. A right or left tactical decomposition with $t=t'$ will be called P-symmetric if P-symmetry holds for the corresponding sequences $v_1, \ldots, v_t$ and $b_1, \ldots, b_t$. The decomposition is called *symmetric* if it is P-symmetric for all P, that is, if $t=t'$ and the b_i's and v_i's can be reordered so that $b_i=v_i$, $i=1, \ldots, t$.

Theorem 5.2. *A tactical decomposition of a symmetric BIBD is $\{p\}\cup Q$-symmetric for any prime p not dividing $n=k-\lambda$ and any set Q of primes each greater than k.*

Proof. The incidence matrix satisfies the hypotheses of Lemma 5.1, with $\alpha=n$ and $\beta=\lambda$, so that $\alpha+\beta v=k^2$. First suppose $p\nmid\det S$. Hence there is a transversal of S of entries not divisible by p, and by reordering the classes we may suppose that this is the diagonal, that is, $p\nmid s_{ii}$, $i=1, \ldots, t$. Then $q\nmid s_{ii}$ for any q in Q since $1\leqq s_{ii}\leqq k$. Write $P=\{p\}\cup Q$. For each a in P and for $i=1, \ldots, t$, $\varphi_a(b_i)\geqq\varphi_a(v_i)$ by Lemma 5.2, and hence $\varphi_a(b_i)=\varphi_a(v_i)$ by (5.2). This gives P-symmetry in this case.

Next suppose that $p\mid k$ but that $p\nmid n$. The complementary design has parameters v, $k'=v-k$, $\lambda'=v-2k+\lambda$, and $n'=k'-\lambda'=k-\lambda=n$, and its incidence matrix has a tactical decomposition with the same row and column classes and with $s'_{ij}=v_i-s_{ij}$. Also $p\nmid n'k'$ since otherwise $p\mid v-k, p\mid v, p\mid\lambda$ since $p\mid k(k-1)=\lambda(v-1)$, and $p\mid k-\lambda=n$, a contradiction (this already proves p-symmetry). Therefore we may as before assume that $p\nmid s'_{ii}$, $i=1, \ldots, t$. If j is such that $p\mid v_j$ then $p\nmid s_{jj}=v_j-s'_{jj}$ and $s_{jj}\neq 0$, so that no q in Q divides s_{jj}. Thus by Lemma 5.2 if a is any power of an element of P then

$$\{i: a\mid v_i \text{ and } p\mid v_i\}\subseteq\{i: a\mid b_i \text{ and } p\mid b_i\}.$$

Consideration of the left as well as the right version of the tactical decomposition then shows that these two sets have the same number of elements and so are equal. Thus P-symmetry and hence also Q-symmetry hold for the subsequences of those v_i and those b_i which are divisible by p. By the first case of the proof the decomposition is Q-symmetric, and so Q-symmetry holds for the complements of the above subsequences. This gives P-symmetry for the decomposition, and the proof is complete.

This theorem generalizes results of DEMBOWSKI [7] who proved that if p is a prime not dividing nk then the sets $\{i: p\mid v_i\}$ and $\{i: p\mid b_i\}$ have the same cardinality, and that for a p-group of collineations if $p\nmid n$ and $\lambda=1$ then the group fixes the same number of points and lines. The theorem is also related to a work of ROTH [*13*] which shows that on certain planes of order n solvable collineation groups of order prime to n fix the same number of points and lines.

The result of Theorem 5.2 does not hold without the restriction on p dividing n — in fact the four-group acts in a non-symmetric manner on the projective plane of order 2.

Corollary 5.1. *Let G be a group of collineations on a symmetric BIBD, p a prime not dividing n, Q a set of primes each greater than k, and H a normal subgroup of G all of whose orbits have the same number m of elements. Then m divides each v_i and b_i and the sequences $v_1/m, \ldots, v_t/m$ and $b_1/m, \ldots, b_t/m$ are $\{p\}\cup Q$-symmetric. In particular, the orbits of G give a tactical decomposition which is symmetric if every prime dividing the order of G/H is in $\{p\}\cup Q$.*

Proof. Let S_H be the associated matrix of column sums for the tactical decomposition into orbits for H. Then S_H has degree v/m, and by (5.1),

$S_H S'_H = \alpha I + \beta J$ where $\alpha = n$ and $\beta = m\lambda$. Note that $\alpha + \beta(v/m) = n + \lambda v = k^2$. Since H is a normal subgroup, the elements of G permute the orbits of H and thus there is induced a tactical decomposition on S_H corresponding to a group of collineations which is a homomorphic image of G/H. An associated matrix of column or row sums for this decomposition is also an associated matrix for the decomposition induced by G on the original incidence matrix, and the orbits of this latter decomposition have length m times that of the orbits of G on S_H. The proof of Theorem 5.2 now goes through when applied to the decomposition on S_H provided one changes b_i to b_i/m and v_i to v_i/m except in the equations $s'_{ij} = v_i - s_{ij}$. This gives the result on $\{p\} \cup Q$-symmetry. Finally since each v_i/m and b_i/m divides $|G/H|$, the last conclusion holds.

Corollary 5.2. *Let S be the associated matrix of column sums of a tactical decomposition on the incidence matrix M of a symmetric BIBD. Then* $(\det S)/k$ *is an integer of which every prime factor divides n, and*

$$n^{t-1} \prod_{i=1}^{t} (v_i/b_i) = (\det S)^2/k^2$$

and so is the square of an integer. If $t \leqq (v+1)/2$ then $\det S \mid \det M$.

Proof. Since the column sums of S are k, k is a characteristic root of S and $k \mid \det S$. The first two conclusions then follow from (5.2) and the p-symmetry of the decomposition for every prime p not dividing n. Write

$$\gamma = \prod_{i=1}^{t} (v_i/b_i).$$

Then $n^{t-1}\gamma$ is an integer, and consideration of the matrix of row sums instead of column sums shows that n^{t-1}/γ is an integer also. Hence $n^{t-1}\gamma \mid n^{2(t-1)}$ and if $t \leqq (v+1)/2$ then

$$(\det S)^2 = n^{t-1}\gamma k^2 \mid n^{v-1} k^2 = (\det M)^2,$$

which completes the proof.

The first part of the proof of Theorem 5.2 actually establishes the following.

Corollary 5.3. *Let there be given a right tactical decomposition with $t = t'$ on an integral $v \times b$ matrix M such that $MM' = \alpha I + \beta J$. If p is a prime not dividing $\alpha(\alpha + \beta v)$ then the decomposition is p-symmetric. If P is a set of primes none of which divide $\alpha(\alpha + \beta v)$ and if there is a transversal $s_{1j_1}, \ldots, s_{tj_t}$ of the associated matrix S such that each s_{ij_i} is prime to every element of P, then the decomposition is P-symmetric.*

This applies in particular to *BIBD*. For a *BIBD* with parameters v, b, r, k, λ, the incidence matrix M satisfies $MM' = \alpha I + \beta J$ with $\alpha = n = r - \lambda$, $\beta = \lambda$ and $\alpha + \beta v = r - \lambda + v\lambda = rk$. Replacing 1 and 0 in M by γ and δ respectively, one obtains a matrix A such that

$$AA' = (r' - \lambda')I + \lambda' J \quad \text{where} \quad r' = r\gamma^2 + (b-r)\delta^2$$

and

$$\lambda' = \lambda\gamma^2 + 2(r-\lambda)\gamma\delta + (b-2r+\lambda)\delta^2.$$

A straightforward computation shows that $r'-\lambda' = n(\gamma-\delta)^2$ and

$$r'-\lambda'+v\lambda' = [k\gamma+(v-k)\delta]\,[r\gamma+(b-r)\delta].$$

Corollary 5.4. *Suppose there is given a right tactical decomposition with $t=t'$ on a BIBD, and a prime p not dividing $r-\lambda$. If $p \nmid (r,b)\,(k,v)$ or, in case $p=2$, if $p \nmid (rk, (b-r)\,(v-k))$, then the decomposition is p-symmetric. If $p \nmid rk$ and if Q is a set of primes such that for every q in Q, $q>k$ and $q \nmid (r-\lambda)r$ then the decomposition is $\{p\} \cup Q$-symmetric.*

Proof. When (γ, δ) has the value $(1,0)$, $(0,1)$ or $(-1,1)$, then $r'-\lambda'+v\lambda'$ has the value rk, $(b-r)\,(v-k)$, or $(b-2r)\,(v-2k)$, respectively. The conditions on the *g.c.d.*'s guarantee that one of these three integers is not divisible by p (the stronger condition when $p=2$ is needed because p must not divide $(r-\lambda)$ $(\gamma-\delta)^2$, so that then (γ,δ) must not be $(-1,1)$). The first conclusion then follows from Corollary 5.3. As in the proof of Theorem 5.2, the hypotheses of the final statement of the corollary imply those of the last statement of Corollary 5.3, which then gives the present result.

6. An Application of the Theory of Quadratic Forms

Consider a symmetric *BIBD* with a tactical decomposition. Eq. (5.1) says that B and $V(\lambda J)\,V + nV$ are rationally congruent. Using this fact, HUGHES [9], [10] (see also DEMBOWSKI [7]) applied the Hasse-Minkowski theory of rational congruence of quadratic forms to obtain number-theoretic conditions on the v_i's (or b_i's) for certain special symmetric decompositions. LENZ [11] gave a simple proof that the above congruence implies the rational congruence of the $(t+1)\times(t+1)$ diagonal matrices $(b_1, \ldots, b_t, n\lambda)$ and $(nv_1, \ldots, nv_t, \lambda)$ (actually Lenz only stated this for projective planes) and used this in the case of symmetric decompositions to obtain a generalization of the results of HUGHES and DEMBOWSKI. In the following, an application of the Hasse-Minkowski theory to the congruence of LENZ and of the symmetry results of the preceding section gives an extension to number-theoretic conditions for non-symmetric decompositions. The symbols $(a,c)_p$ and (n/p) denote the Hilbert norm residue and the Legendre symbols.

Theorem 6.1. *Suppose there is given a tactical decomposition on a symmetric BIBD. For every prime p, if t is odd then*

$$\left((-1)^{(t-1)/2}\lambda\prod_{i=1}^{t} b_i, n\right)_p \prod_{1\leq j<l\leq t} (v_j, v_l)_p (b_j, b_l)_p = 1; \tag{6.1}$$

if t is even then

$$((-1)^{(t/2)+1}\lambda, n)_p \prod_{1\leq j<l\leq t} (v_j, v_l)_p (b_j, b_l)_p = 1. \tag{6.2}$$

If $p \nmid n$ these both reduce to

$$\left(\frac{n}{p}\right)^a \prod_{\{j \mid \varphi_p(v_j) \text{ odd}\}} (p, v_j)_p \prod_{\{j \mid \varphi_p(b_j) \text{ odd}\}} (p, b_j)_p = 1, \tag{6.3}$$

where a is 1 or 0 according as $\{j \mid \varphi_p(v_j)$ odd$\}$ (or $\{j \mid \varphi_p(b_j)$ odd$\}$) has an odd or even number of elements.

Proof. For an m by m matrix with i-th principle minors D_i, $i=1, \ldots, m$, the Hasse invariant c_p has the value

$$(-1, -D_m)_p \prod_{i=1}^{m-1} (D_i, -D_{i+1})_p,$$

and this invariant must have the same value for $\operatorname{diag}(b_1, \ldots, b_t, \lambda n)$ and $\operatorname{diag}(nv_1, \ldots, nv_t, \lambda)$ (where $m=t+1$). In computing c_p, we drop the subscript p from the Hilbert symbols. Write

$$\gamma_i = \prod_{j=1}^{i} b_j, \qquad i=1, \ldots, t.$$

Then

$$(\gamma_i, -\gamma_{i+1}) = (\gamma_i, -\gamma_i)(\gamma_i, b_{i+1}) = (\gamma_i, b_{i+1}) \qquad \text{for } i=1, \ldots, t-1,$$

since $(\gamma, -\gamma)=1$ for any integer γ. Hence

$$\prod_{i=1}^{t-1} (\gamma_i, -\gamma_{i+1}) = \prod_{1 \leqq j < l \leqq t} (b_j, b_l),$$

and therefore

$$c_p(\operatorname{diag}(b_1, \ldots, b_t, \lambda n)) = (-1, \gamma_t \lambda n)(\gamma_t, \lambda n) \prod_{1 \leqq j < l \leqq t} (b_j, b_l).$$

Next write

$$\delta_i = \prod_{j=1}^{i} v_j, \qquad i=1, \ldots, t,$$

and consider $\operatorname{diag}(nv_1, \ldots, nv_t, \lambda)$. Here $(D_t, -D_{t+1}) = (n^t \delta_t, \lambda)$, which equals $(n\delta_t, \lambda)$ if t is odd and (δ_t, λ) if t is even. For $i=1, \ldots, t-1$,

$$(D_i, -D_{i+1}) = (n^i, -n^{i+1})(n^i, \delta_{i+1})(\delta_i, n^{i+1})(\delta_i, -\delta_{i+1}).$$

Since $(n^i, -n^{i+1})=1$ or $(n, -1)$ according as i is even or odd,

$$\prod_{i=1}^{t-1} (n^i, -n^{i+1}) = (n, -1)^{(t-1)/2} \quad \text{or} \quad (n, -1)^{t/2}$$

according as t is odd or even. Also

$$\begin{aligned}\prod_{i=1}^{t-1} (n^i, \delta_{i+1})(\delta_i, n^{i+1}) &= \prod_{i=1}^{t-1} (n^i, \delta_i)(n^i, v_{i+1})(n^i, \delta_i)(n, \delta_i) \\ &= \prod_{i=1}^{t-1} (n, \delta_i)(n^i, v_{i+1}) = \prod_{m=1}^{(t-1)/2} (n, \delta_{2m})^2 = 1\end{aligned}$$

if t is odd, while if t is even there is a remaining factor (n, δ_t). Finally

$$\prod (\delta_i, -\delta_{i+1}) = \prod_{j<l} (v_j, v_l)$$

just as for the b_j. Hence

$$c_p(\operatorname{diag}(n v_1, \ldots, n v_t \lambda)) = \begin{cases} (-1, \delta_t \lambda n)(n \delta_t, \lambda)(n, -1)^{(t-1)/2} \prod_{j<l} (v_j, v_l) \; (t \text{ odd}) \\ (-1, \delta_t \lambda)(\delta_t, \lambda)(n, -1)^{t/2} (n, \delta_t) \prod_{j<l} (v_j, v_l) \; (t \text{ even}). \end{cases}$$

By (5.2), if t is odd then $\gamma_t \delta_t$ is a square, so that $(\gamma, \gamma_t) = (\gamma, \delta_t)$ for any γ; if t is even then $n \gamma_t \delta_t$ is a square, and $(\lambda n, \gamma_t \delta_t) = (\lambda n, n) = (\lambda, n)(n, -1)$. Comparison of the two values of c_p now gives (6.1) and (6.2).

Finally suppose $p \nmid n$. Then $(\lambda, n) = 1$ (if $p \mid \lambda$ then $(\lambda, n) = (\lambda, n + v\lambda) = (\lambda, k^2) = 1$) and $(-1, n) = 1$. Since the decomposition is p-symmetric, the v_i's and b_i's can be ordered so that $\varphi_p(v_j)$ and $\varphi_p(b_j)$ have the same value, say d_j, $j = 1, \ldots, t$. Write $v_j = p^{d_j} v_j'$ and similarly for b_j. Then

$$\prod_{j<l} (v_j, v_l)(b_j, b_l) = \prod_{j<l} (p^{d_j}, p^{d_l})^2 (p^{d_j}, v_l' b_l')(v_j' b_j', p^{d_l})$$
$$= \prod_j (p^{d_j}, \prod_l v_l b_l)(p^{d_j}, v_j b_j).$$

When t is odd

$$\prod_l v_l b_l$$

is a square and when t is even

$$\prod_j (p^{d_j}, \prod_l v_l b_l) = \prod_j (p^{d_j}, n) = (p, n)^a = \left(\frac{n}{p}\right)^a$$

where a is the number of odd d_j. Also

$$(\prod_i b_i, n) = (p, n)^a.$$

Collecting these simplifications gives the final result of the theorem.

Corollary 6.1. *Let G be a group of collineations on a symmetric BIBD and p a prime such that $p \nmid n$ and $(n/p) = -1$. If $p \leqq k$ (respectively, $p > k$) suppose that $(q/p) = 1$ for every prime divisor $q \neq p$ of $|G|$ such that $q \leqq k$ (respectively, such that $q \mid n$). Then $\varphi_p(v_i)$ is odd for an even number of point orbits.*

Proof. By P-symmetry the orbits may be ordered so that $\varphi_p(v_j) = \varphi_p(b_j)$ and $\varphi_q(v_j) = \varphi_q(b_j)$ for all $q > k$ and all j. The quadratic residue condition on the q then implies that $(p, v_j b_j)_p = 1$ for all j. Hence the exponent a of (6.3) must be 0 and the conclusion holds when $p \leqq k$. Similarly by $\{p, q\}$ symmetry for each q not dividing n the conclusion holds when $p > k$.

The hypothesis that $(q/p) = 1$ is only needed for those primes q such that the decomposition is not $\{p, q\}$-symmetric.

7. A Generalization of p-Symmetry to Nonsymmetric Designs

Suppose there is given a right tactical decomposition of a matrix, with as usual row classes with $v_1, \ldots, v_t$ elements and column classes with $b_1, \ldots, b_{t'}$ elements. In this section, for any prime p and nonnegative integer j we write p_j for the number of i with $\varphi_p(v_i)=j$, and p'_j for the number of i with $\varphi_p(b_i)=j$. Thus p-symmetry says exactly that $p_j=p'_j$ for all j.

Theorem 7.1. *Let there be given a right tactical decomposition of a $v\times b$ integral matrix M, where $MM'=\alpha I+\beta J$, and a prime p not dividing α. For any i, if $p\nmid\alpha+\beta v$ then*

$$0\leqq(i+1)(p'_0-p_0)+i(p'_1-p_1)+\cdots+(p'_i-p_i) \tag{7.1}$$

while if $p\mid\alpha+\beta v$ then

$$-(i+1)\leqq(i+1)(p'_0-p_0)+i(p'_1-p_1)+\cdots+(p'_i-p_i). \tag{7.2}$$

Proof. For any matrix A and any row indices $i_1, \ldots, i_m$ and column indices $j_1, \ldots, j_m$ let $A(i_1, \ldots, i_m; j_1, \ldots, j_m)$ denote the $m\times m$ submatrix of A formed from the given rows and columns. By the elementary expresion for the determinant of the product of an $m\times l$ and an $l\times m$ matrix as a sum of products of $m\times m$ minors, (5.1) implies that

$$\sum_{1\leqq j_1<j_2<\cdots<j_m\leqq t'} b_{j_1}\ldots b_{j_m}(\det S(i_1, \ldots, i_m; j_1, \ldots, j_m))^2 = \det W(i_1, \ldots, i_m; i_1, \ldots, i_m)$$

for any $i_1, \ldots, i_m$ with $1\leqq i_1<i_2<\cdots<i_m\leqq t$. A calculation just like that of det W shows that the right side equals

$$v_{i_1}\ldots v_{i_m}\alpha^{m-1}[\alpha+\beta(v_{i_1}+\cdots+v_{i_m})]. \tag{7.3}$$

Hence if s denotes the value of φ_p of this expression then $\varphi_p(b_{j_1}\ldots b_{j_m})\leqq s$ for some choice of $j_1, \ldots, j_m$. Applying this fact to the $m=p_0+\cdots+p_i$ of the row indices l with $\varphi_p(v_l)\leqq i$, one sees that if γ is defined by

$$\gamma+\sum_{j=0}^{i} p'_j=\sum_{j=0}^{i} p_j$$

then

$$(i+1)\gamma+\sum_{j=0}^{i} j\,p'_j\leqq\sum_{j=0}^{i} j\,p_j+\varphi_p(\alpha)\left(-1+\sum_{j=0}^{i} p_j\right)+\varphi_p\Big(\alpha+\beta\sum_{\varphi_p(v_j)\leqq i} v_j\Big). \tag{7.4}$$

By hypothesis $\varphi_p(\alpha)=0$. Moreover the last term vanishes if $p\nmid\alpha+\beta v$ because $p\mid\beta\sum v_j$ where the sum is over those j such that $\varphi_p(v_j)>i$. Hence multiplying the equation defining γ by $i+1$ and then subtracting (7.4), one gets (7.1).

Next suppose that $p|\alpha+\beta v$. Then $p\nmid v\beta$ since $p\nmid\alpha$. Suppose the last term of (7.4) does not vanish. Pick an index l such that $\varphi_p(v_l)=0$ (such exists since $p\nmid v$) and apply the above argument this time to the $p_0+\cdots+p_i-1$ indices j such that $\varphi_p(v_j)\leqq i, j\neq l$. Then p_0 is replaced by p_0-1, and the term corresponding to the last term of (7.4) now vanishes, since $p\nmid\beta v_l$. Hence (7.2) holds, and the proof is complete.

This theorem gives a second proof of the p-symmetry of a tactical decomposition of a symmetric *BIBD* when $p\nmid n$.

For a right tactical decomposition and any integer a, let g_a denote the number of i for which $a|b_i$, and l_a the number of i for which $a|v_i$. Thus

$$g_{p^j}=\sum_{i\geqq j}p'_i,\qquad l_{p^j}=\sum_{i\geqq j}p_i,\qquad g_{p^j}-l_{p^j}=t'-t-\sum_{i=0}^{j-1}(p'_i-p_i).$$

Theorem 7.2. *Let M be a $v\times b$ matrix over the integers such that $MM'=\alpha I+\beta J$. Suppose that M has a right tactical decomposition and that p is a prime not dividing α. Suppose that $j\geqq 0$ is such that $g_{p^j}=t'$. Then* (a) *if $p\nmid\alpha+\beta v$ then*

$$(7.5)\qquad |g_{p^{j+1}}-l_{p^{j+1}}|\leqq t'-t,\quad \textit{and}\quad l_{p^j}=t;$$

(b) *if $p|(\alpha+\beta v)$ then $|g_{p^{j+1}}-l_{p^{j+1}}|\leqq t'-t+1$, $l_{p^j}=t$ (when $j=0$) or $t-1$ (when $j>0$), and $p^j|\alpha+\beta v$.*

(In the most significant case $j=0$ and the conditions $g_1=t'$ and $l_1=t$ are automatically satisfied).

Proof. Suppose first that $p\nmid\alpha+\beta v$ and that $j=0$. Reduction of (5.1) modulo p gives $S_p B_p S'_p=W_p$ for the matrices of residue classes. The rank of S_p is t (by Lemma 5.2), the rank of B_p is $t'-g_p$, and the rank of W_p is $t-l_p$ as may be seen using (7.3). Since rank $B_p\geqq$rank W_p=rank $S_p B_p S'_p$, one has $t'-g_p\geqq t-l_p\geqq t-g_p-(t'-t)$, and (a) follows in this case ($j=0$). Next suppose that $j>0$ and that p^j divides all v_i (as well as all b_i). Then $p^{-j}B$ and $p^{-j}W$ are integral. The analogue of the above argument for the case $j=0$, applied to the equation $S_p(p^{-j}B)_p S'_p=(p^{-j}W)_p$, yields the inequality of (a). This inequality and induction then show that p^j divides all v_i whenever it divides all b_i, which completes the proof of (a).

The proof of (b) is obtained by modifying the proof of (a), in particular noting that $(p^{-j}W)_p$ has rank $t-l_{p^{j+1}}-1$; we omit the details.

Half of the inequality of (a), as well as of (b) when $j=0$, also follows from Theorem 7.1.

The following holds by the reasoning of Corollary 5.4.

Corollary 7.1. *Suppose there is given a right tactical decomposition on a BIBD, and a prime p such that $p\nmid(r-\lambda)(r,b)(k,v)$, or, in case $p=2$, $p\nmid(r-\lambda)(rk,(b-r)(v-k))$. Then* (7.1) *holds, and if $g_{p^j}=t'$ then* (7.5) *holds.*

References

[1] BLOCK, R.E.: Transitive groups of collineations on certain designs. Pacific J. Math. **15**, 13–18 (1965).
[2] BOSE, R.C.: A note on the resolvability of balanced incomplete block designs. Sankhya **6**, 105–110 (1942).
[3] —, and W.S. CONNOR: Combinatorial properties of group divisible incomplete block designs. Annals Math. Stat. **23**, 367–383 (1952).
[4] BRAUER, R.: On the connection between the ordinary and the modular characters of groups of finite order. Annals of Math. **42**, 926–935 (1941).
[5] CONNOR, W.S.: On the structure of balanced incomplete block designs. Annals Math. Stat. **23**, 57–71 (1952).
[6] —, and W.H. CLATWORTHY: Some theorems for partially balanced designs. Annals Math. Stat. **25**, 100–112 (1954).
[7] DEMBOWSKI, P.: Verallgemeinerungen von Transitivitätsklassen endlicher projektiver Ebenen. Math. Z. **69**, 59–89 (1958).
[8] — Kombinatorik. Vorlesung Frankfurt 1965.
[9] HUGHES, D.R.: Regular collineation groups. Proc. Amer. Math. Soc. **8**, 165–168 (1957).
[10] — Collineations and generalized incidence matrices. Trans. Amer. Math. Soc. **86**, 284–296 (1957).
[11] LENZ, H.: Quadratische Formen und Kollineationsgruppen. Arch. Math. **13**, 110–119 (1962).
[12] PARKER, E.T.: On collineations of symmetric designs. Proc. Amer. Math. Soc. **8**, 350–351 (1957).
[13] ROTH, R.: Collineation groups of finite projective planes. Math. Z. **83**, 409–421 (1964).

University of Illinois, Urbana, Ill., USA