PACIFIC JOURNAL OF MATHEMATICS
Vol. 15, No. 1, 1956

TRANSITIVE GROUPS OF COLLINEATIONS ON CERTAIN DESIGNS

RICHARD E. BLOCK

Let $M = (a_{ij})$ be an $m \times n$ matrix with entries in $\{1, -1\}$. Suppose that there is a positive integer d such that the inner product of every pair of distinct rows of M is $n - 2d$; this is equivalent to assuming that any two distinct rows have Hamming distance d, i.e. differ in exactly d places. The rows of M form the code words of a binary code; such a code is called a (binary) *constant-distance code*, of length n and distance d. Special cases of matrices which may be taken to be M are the Hadamard matrices, which are defined by the condition that $m = n = 2d$, and the incidence matrices (written with ± 1) of balanced incomplete block designs, which are characterized by the property that all column sums are equal and all row sums are equal.

Suppose that π is a permutation of $\{1, \cdots, n\}$ such that replacement, for $i = 1 \cdots, n$, of the $\pi(i)$th column of M by the ith column of M sends each row of M into a row of M. Then π induces a permutation of the rows of M. Call such a pair of permutations of the columns and of the rows a collineation of M, or of the code. We shall examine constant-distance codes with a group G of collineations which is transitive on the columns. We shall show that G has at most two orbits on the rows (just one orbit if and only if M comes from a balanced incomplete block design), and that if G is nilpotent then at most one of these orbits contains more than a constant row.

Moreover, it will be shown that this last conclusion need not hold if G is not assumed nilpotent; this will be done by giving an infinite class of Hadamard matrices with doubly transitive collineation groups.

One way of obtaining a constant-distance code with a transitive group on the columns is the following. Given a (cyclic) (v, k, λ) difference set, write a v-tuple of 1's and -1's with 1 in the k places which corresponds to elements of the difference set, and repeat this v-tuple s times to obtain a vs-tuple. The set of all cyclic permutations of this vs-tuple forms constant-distance code with v code words and distance $d = 2(k - \lambda)s$. Call such a code an *iterated difference set code*. The code is closed under the cyclic shift (the permutation $\pi = (1, 2, \cdots, vs)$ on the columns).

Our results imply that, conversely, any constant-distance code which is closed under the cyclic shift consists of repeated cyclic shifts of

Received December 20, 1963.

some single word, plus possibly a single constant word. The main part of the code is thus an iterated difference set code; the extra word can occur if and only if the parameters (v, k, λ) are of Hadamard type.

2. The number of orbits on the rows.

THEOREM 1. *Suppose that G is a group of collineations of a constant-distance code. If G is transitive on the columns then G has at most two orbits on the rows.*

Proof. Suppose that G has t orbits $T_1, \cdots, T_t$ on the rows. Then there are integers r_i such that each row in T_i has exactly r_i 1's, $i = 1, \cdots, t$. It follows that if α_i and α_j are rows and $\alpha_i \in T_i$, $\alpha_j \in T_j$, and if $c(\alpha_i, \alpha_j)$ is the number of places in which both α_i and α_j have 1, then $r_i + r_j = d + 2c(\alpha_i, \alpha_j)$, or $c(\alpha_i, \alpha_j) = (r_i + r_j - d)/2$. Let v_i denote the number of words in T_i. Since G is transitive on the columns, for each column there are the same number k_i of words in T_i with 1 in that place; we have $k_i = v_i r_i/n$, where n is the length of the words. Thus the words in T_i form the incidence matrix of a balanced incomplete block design with $\lambda = r_i - (d/2)$. Now suppose that $t \geqq 2$, that T_i and T_j are distinct orbits and that $\alpha \in T_j$. Counting in two ways the total number of times in which words in T_i have a 1 in the same place as a 1 in α, we have $v_i(r_i + r_j - d)/2 = r_j k_i$. Thus, since $k_i = v_i r_i/n$,

$$n\frac{(r_i + r_j - d)}{2} = r_i r_j \,. \tag{1}$$

Suppose that, $r_i \neq n$. Then for some prime p, with p^e and p^f the highest powers of p dividing n and r_i, respectively, one has $e > f$. Since $v_i r_i = nk_i$ and

$$r_i(k_i - 1) = \left(r_i - \frac{d}{2}\right)(v_i - 1)\,, \tag{2}$$

$p \nmid (v_i - 1)$ and $p^f \mid r_i - (d/2)$. If $r_i = r_j$ then the left side of (1) is divisible by p^{e+f}, the right side only by p^{2f}, a contradiction. Hence $r_i \neq r_j$ if $i \neq j$. Also $r_i \neq n/2$, since otherwise, by (1), $r_i = n/2 = d$ and $k_i = v_i/2$, contradicting (2). Thus r_j is uniquely determined in terms of r_i by (1). It follows that $t \leqq 2$, and the theorem is proved.

If there is only one orbit, then, as shown in the above proof, M is the incidence matrix of a balanced incomplete block design. The next result is the converse.

THEOREM 2. *Suppose that G is a group of collineations of a balanced incomplete block design. If G is transitive on the blocks then G is also transitive on the points.*

Proof. The incidence matrix of the design is a constant-distance code with $d = 2(r - \lambda)$. If G had two orbits on the points, then $r_1 = r_2 = r$. But by the proof of Theorem 1, $r_1 \neq r_2$, a contradiction. This proves Theorem 2.

COROLLARY 1. *Let G be a group of collineations of a constant-distance code. Suppose that G fixes c columns and is transitive on the remaining columns. Let q be the number of different c-tuples in the rows of the submatrix formed by the c fixed columns. Then G has at most $2q$ orbits on the rows; if moreover the code corresponds to a balanced incomplete block design, then G has exactly q orbits on the rows (points).*

Proof. The set of rows with a given c-tuple in the fixed columns must be closed under G; deleting the fixed columns from these rows, one obtains a constant distance code with a transitive group of collineations. The result now follows immediately from Theorems 1 and 2.

These results are a partial generalization to nonsymmetric designs of a theorem proved by Dembowski [2], Hughes [3], and Parker [4], which says that for a symmetric design, the number of orbits on the points is the same as the number of orbits on the lines. However there are balanced incomplete block designs with a group of collineations which is transitive, even cyclic, on the points, but not transitive on the lines.

3. Codes with a nilpotent transitive group. In this section we assume that M is an $m \times n$ matrix whose rows form a constant-distance code with distance d, and that G is a group of collineations which is transitive on the columns. Let H denote the subgroup of G fixing the first column. We shall continue using the notation T_i, v_i, r_i and k_i introduced in the above proofs.

THEOREM 3. *Suppose that T_1 and T_2 are distinct orbits of G (on the rows). For $i = 1, 2$, take α_i in T_i and let S_i be the subgroup of G fixing α_i. Suppose that p is any prime such that the highest power p^j of p dividing n does not divide d. Then, either for $i = 1$ or 2, S_i contains the normalizer of a Sylow p-subgroup of G, $p \mid v_i - 1$, and $p^j \mid r_i$.*

Proof. If the orbit T_i is trivial (consists of a constant word) then $S_i = G$ and the conclusion is obvious. Thus suppose that both orbits are nontrivial. Take a prime p such that p^j, the highest power of p dividing n, does not divide d. Let p^e and p^f be the highest powers of p dividing r_1 and r_2, respectively; by choice of notation we may suppose that $e \leqq f$. By (1), $p^i \mid r_1 r_2$.

Suppose first that $p \nmid v_1 - 1$ and $p \nmid v_2 - 1$. Then by (2), $p^e \mid [r_1 - (d/2)]$ and $p^f \mid [r_2 - (d/2)]$, so that $p^f \mid (d/2)$ and $p^e \mid r_1 + r_2 - d$. If $p > 2$ then p^{j+e} divides the left side of (1) while p^{e+f} is the highest power of p dividing the right side; hence $f \geqq j$, so that $p^j \mid d$, a contradiction. If $p = 2$ then $p^{e-1} \mid [(r_1 + r_2 - d)/2]$ and p^{j+e-1} divides the left side of (1), so that $f \geqq i - 1$, $p^{j-1} \mid (d/2)$ and $p^j \mid d$, again a contradiction.

Hence $p \mid v_i - 1$ for some i, with $i = 1$ or 2. Then since $p \mid ([G : S_i] - 1)$, $p \nmid [G : S_i]$ and S_i contains a Sylow p-subgroup of G. Suppose that K is any subgroup of G, and consider the orbits of K when K is regarded as a permutation group on the columns. For each of these orbits there is an x in G such that the number of elements in the orbit is $[K : K \cap xHx^{-1}]$. If p^l is the highest power of p dividing $|H|$ then p^{j+l} is the highest power of p dividing $|G|$. Hence if K contains a Sylow p-subgroup of G then $p^j \mid [K : K \cap xHx^{-1}]$ for any x. Taking $K = S_i$ we see that $p^j \mid r_i$, since the set of places where α_i has 1 is a union of orbits of S_1 (on the columns). If $g \in G$ and $g \notin S_i$ then $g\alpha_i \neq \alpha_i$, and gS_ig^{-1} is the subgroup of G fixing $g\alpha_i$. If moreover gS_ig^{-1} contains a Sylow p-subgroup of S_i, then p^j divides the number of elements in each orbit (on the columns) of $S_i \cap gS_ig^{-1}$. But the set of places where α_i and $g\alpha_i$ disagree is a union of orbits of $S_i \cap gS_ig^{-1}$, so that $p^j \mid d$, a contradiction. Therefore no Sylow p-subgroup of S_i is contained in a conjugate of S_i. Suppose that P is a Sylow p-subgroup of S_i (and so also of G), and that $x \in N_G(P)$, the normalizer of P. If $x \notin S_i$ then $xS_1x^{-1} \neq S_i$ but $P = xPx^{-1} \subseteqq xS_ix^{-1}$, a a contradiction. Hence $N_G(P) \subseteqq S_i$, and the theorem is proved.

COROLLARY 2. *If G is a nilpotent group of collineations of M which is transitive on the columns, then either G is transitive on the rows or one of the two orbits of G on the rows consists of one trivial row.*

Proof. Unless M has only the two trivial rows, there is a prime p such that the highest power of p dividing n does not divide d. Since a Sylow p-subgroup of a nilpotent group is normal, if G is not transitive on the rows then by Theorem 3, G fixes a row. This proves the result.

Now suppose the constant distance code is closed under the cyclic shift $\pi = (1, 2, \cdots, n)$. If α is a code word with r ones, then α must be periodic of (minimal) period v, a divisor of n; write $v = n/s$.

A single period of α gives a (v, k, λ) difference set with $k = r/s$ and $\lambda = [r - (d/2)]/s$. Thus the set of cyclic shifts $\pi^i\alpha$ or α forms an s-times iterated (v, k, λ)-difference set code; solving $k(k-1) = \lambda(v-1)$ for s, one has $s = n + [2r(r-n)/d]$. By Corollary a, either this set is the entire code or there is one more word, with all 1's or all -1's. If the extra word has all -1's then $r = d$, $\lambda = d/2s$, and from $k(k-1) = \lambda(v-1)$ one obtains $n/s = 2d/s$. Hence, with $d/2s = u$, one would have $v = 4u - 1$, $k = 2u$ and $\lambda = u$. If on the other hand the extra word has all 1's, then we have the complement of a code of the above type, and $v = 4u - 1$, $k = 2u - 1$ and $\lambda = u - 1$.

The above characterization of constant-distance code closed under the cyclic shift was conjectured by the writer and proved independently at the same time by the writer [1] and R.C. Titsworth [5]. Titsworth's proof uses arguments on polynominals dividing $x^n - 1$.

3. Hadamard matrices and codes with two orbits. In this section we give a class of Hadamard matrices with doubly transitive collineation groups, and use these matrices to obtain a class of constant-distance codes with a transitive group on the columns for which the conclusion of Corollary 2 does not hold.

Let A be the Hadamard matrix of order 4 with 1 on the diagonal, -1 elsewhere, and let $B = B(s)$ be the tensor product of s copies of A.

THEOREM 4. *For any s, the group G of collineations of $B(s)$ is doubly transitive on the columns (and also on the rows).*

Proof. Denote the rows and columns of B by s-tuples, so that

$$b_{i_1} \cdots, i_s; j_1, \cdots, j_s = a_{i_1, j_1} a_{i_2, j_2} \cdots a_{i_s, j_s} .$$

The result is obvious when $s = 1$. Suppose $s = 2$. We shall show that the subgroup H of G fixing the column $(1, 1)$ is transitive on the remaining columns. If τ_1 and τ_2 are any permutations on four letters then the permutation of columns sending (i_1, i_2) to $(\tau_1(i_1), \tau_2(i_2))$ is a collineation of B, sending row (i_1, i_2) to row $(\tau_1(i_1), \tau_2(i_2))$; denote this collineation by (τ_1, τ_2). It can be verified that the product of four transpositions of columns $\sigma = ((1, 4)\,(2, 3))((4, 1)\,(3, 2))((1, 3)\,(2, 4))((3, 1)\,(4, 2))$ is a collineation of B; also, $\sigma \in H$. Taking σ and its products with various (τ_1, τ_2), we see that all columns other than $(1, 1)$ form a single orbit of H. Moreover some (τ_1, τ_2) moves column $(1, 1)$, so that G is transitive, and hence doubly transitive. Now suppose that $s > 2$. If τ is a collineation of $B(2)$ and if a set of two column coordinates of $B(s)$ is given, then a collineation of $B(s)$ is obtained by applying τ to the given column coordinates while keeping the remaining ones fixed. Using this type of collineation, we see that the subgroup of G fixing column $(1, \cdots, 1)$ is transitive on the remaining columns. Hence G is always doubly transitive on the columns, and, by symmetry, also on the rows. This completes the proof.

COROLLARY 3. *For every power 4^s of $4 (s > 1)$, there is a constant-distance code with 4^s words of length $4^s - 1$, such that the group of collineations is transitive on the columns but has two nontrivial orbits on the rows.*

Proof. The matrix $B(s)$ is Hadamard, and hence its rows form a constant-distance code. Complement the rows with $a + 1$ in column $(1, \cdots, 1)$ and then delete this column. What remains is still a constant-distance code; call it C. The subgroup of G fixing $(1, \cdots, 1)$ clearly gives a group of collineations of C which is transitive on the columns. Moreover the set of uncomplemented rows is closed under the group, so the group has two nontrivial orbits. This completes the proof.

Let G and H continue to have the same meanings as in Theorem 4. It follows from Corollary 2 and the proof of Corollary 3 that H is not nilpotent. However it can actually be shown that the subgroup K of H fixing column $(1, 2)$ is isomorphic to S_6, being generated by σ and certain (τ_1, τ_2)'s. Hence when $s = 2$, G has order $16 \cdot 15 \cdot 720$. Also it follows that if $s > 1$ then G contains a subgroup isomorphic to S_6 which fixes $2 \cdot 4^{s-2}$ columns.

REFERENCES

1. R.E. Block, *Difference sets, block designs, and constant distance codes*, Space Programs Summary No. 37-22, Vol. IV, Jet Propulsion Laboratory, California Institute of Technology, August 31, (1963), 137-138.

2. P. Dembowski, *Verallgemeinerungen von Transitivitätsklassen endlicher projektiver Ebenen*, Math. Zeit. **69** (1958), 59-89.

3. D.R. Hughes, *Collineations and generalized incidence matrixes*, Trans. Amer. Math. Soc. **86** (1957), 284-286.

4. E.T. Parker, *On collineations of symmetric designs*, Proc. Amer. Math. Soc. **8** (1957), 350-351.

5. R.C. Titsworth, *Binary cyclic constant-distance codes*, Space Programs Summary No. 37-22, Vol. IV, Jet Propulsion Laboratory, California Institute of Technology, August 31, (1963), 147, 152-153.

CALIFORNIA INSTITUTE OF TECHNOLOGY