BULL. AUSTRAL. MATH. SOC. 94A10, 05B10, 05B20, 05A17
VOL. 16 (1977), 361-369.

On circulant codes with prescribed distances

M. Deza and Peter Eades

Necessary and sufficient conditions are given for a square matrix to be the matrix of distances of a circulant code. These conditions are used to obtain some inequalities for cyclic difference sets, and a necessary condition for the existence of circulant weighing matrices.

1. Preliminaries

Throughout this paper, a *circulant code* C of length m shall mean a set of m $(0, 1)$ codewords of length m, with the property that successive codewords differ by a cyclic shift. Thus if $(x_1, x_2, \ldots, x_m)$ is the first codeword, then $(x_{m-j+2}, x_{m-j+3}, \ldots, x_{m-j+1})$ is the jth codeword, for $2 \le j \le m$. We can write these codewords as the rows of a circulant $(0, 1)$ matrix X. The matrix $2(J-X)X^t$ is called the *matrix of distances* of the code C. (J is the $m \times m$ matrix with every entry 1.) Clearly the (i, j)th entry of $2(J-X)X^t$ is the (Hamming) distance between the ith and jth codewords. A matrix of the form $2(J-X)X^t$, where X is a $(0, 1)$ circulant matrix, is called *realizable*, and the circulant code whose codewords are the rows of X is called the *realization* of $2(J-X)X^t$.

The problem of finding a code with prescribed distances has received attention from both coding theorists and combinatorialists. In Section 2, the realizability of an $m \times m$ matrix is shown to be equivalent to the

Received 5 January 1977. Communicated by Jennifer R. Seberry.

existence of a partition of m with appropriate properties. Firstly, however, we require some definitions.

Let $x = (x_1, x_2, \ldots, x_m)$ be a $(0, 1)$ codeword. For Sections 1 and 2, we will use the convention that $x_1 = 1$ and $x_m = 0$. If $x_{i-1} \neq x_i = x_{i+1} = \ldots = x_j \neq x_{j+1}$, we call $B = (i, i+1, \ldots, j)$ a *block* of x. The blocks of x are numbered $B_1, B_2, \ldots, B_t$ from left to right as they appear in x. Note that since $x_1 \neq x_m$, t is even. Let X denote the circulant with first row x, and let b_i denote $|B_i|$, the length of the ith block. We say that the sequence $(b_1, b_2, \ldots, b_t)$ *describes* X.

Note that $m = b_1 + b_2 + \ldots + b_t$ is an ordered partition of m. Consider all the series $b_j + b_{j+1} + \ldots + b_k$. (If $j > k$, the sum is defined cyclically, that is,

$$b_j + b_{j+1} + \ldots + b_k = b_j + b_{j+1} + \ldots + b_t + b_1 + \ldots + b_k .)$$

For each $1 \leq i \leq [m/2]$, let f_i be the number of such series that have sum i and an odd number of terms, less the number of series that have sum i and an even number of terms. Let f_0 be t; then the sequence $(f_i : 0 \leq i \leq [m/2])$ is called the *structure* of the ordered partition $m = b_1 + b_2 + \ldots + b_t$.

For example, $(2, 3, 5, 2, 1, 4)$ describes a circulant code with first codeword (1100011111 and blocks $B_1 = (1, 2)$, $B_2 = (3, 4, 5)$, $B_3 = (6, 7, 8, 9, 10)$, $B_4 = (11, 12)$, $B_5 = (13)$, and $B_6 = (14, 15, 16, 17)$. The structure of $17 = 2 + 3 + 5 + 2 + 1 + 4$ is $(6, 1, 2, 0, 1, -1, -1, 1, 0)$.

2. The structure theorem

THEOREM 1 (Structure Theorem). *An* $m \times m$ *matrix* H *with first row* $(h_1, h_2, \ldots, h_m)$ *is realizable if and only if*

https://doi.org/10.1017/S0004972700023467 Published online by Cambridge University Press

(i) *H is a symmetric circulant matrix with zero diagonal;*

(ii) *the entries of H are even, non-negative integers; and*

(iii) *there is an ordered partition $m = b_1 + b_2 + \ldots + b_t$ with structure (f_i) satisfying $f_0 = h_2$ and $f_i = \frac{1}{2}(2h_{i+1}-h_i-h_{i+2})$ for $1 \le i \le [m/2]$.*

Proof. Suppose H is realized by a circulant code whose codewords are the rows of a circulant $(0, 1)$ matrix X . Let $(b_1, b_2, \ldots, b_t)$ denote the sequence that describes the first row of X , and let (f_i) be the structure of $m = b_1 + b_2 + \ldots + b_t$. Clearly *(i)* and *(ii)* follow, and $h_2 = f_0$. Now

$$h_i = 2 \sum_{q=1}^{m} \left(x_q - x_q x_{q+i-1}\right) ,$$

and we can deduce

$$\tfrac{1}{2}\left(2h_{i+1}-h_i-h_{i+2}\right) = \sum_{q=1}^{m} t_{iq}$$

where $t_{iq} = \left(x_q-x_{q-1}\right)\left(x_{q+i-1}-x_{q+i}\right)$.

But t_{iq} is non-zero only when $x_q \ne x_{q-1}$ and $x_{q+i-1} \ne x_{q+i}$. In this case, q must be the first element of some block B_k , and $q + i$ must be the last element of some block B_l . Hence if $t_{iq} \ne 0$, then $b_k + b_{k+1} + \ldots + b_l = i$. But $t_{iq} = 1$ if $l - k + 1$ is odd, and $t_{iq} = -1$ if $l - k + 1$ is even. So $f_i = \frac{1}{2}(2h_{i+1}-h_i-h_{i+2})$, for $i \ge 1$.

Conversely, suppose that H is a symmetric circulant of even non-negative integers, and suppose the partition $m = b_1 + b_2 + \ldots + b_t$ has structure (f_i) satisfying $f_0 = h_2$ and $f_i = \frac{1}{2}(2h_{i+1}-h_i-h_{i+2})$, for $i \ge 1$. We claim that H is the matrix of distances of a circulant code with first codeword described by $(b_1, b_2, \ldots, b_t)$. Let X be the $(0, 1)$ circulant with first row described by $(b_1, b_2, \ldots, b_t)$. If

https://doi.org/10.1017/S0004972700023467 Published online by Cambridge University Press

$(h_1', h_2', \ldots, h_m')$ is the first row of $2(J-X)X^t$, then by the argument above,

$$h_2 = h_2' = f_0 ,$$

and

$$2h_{i+1} - h_i - h_{i+2} = 2f_i = 2h_{i+1}' - h_i' - h_{i+2}' \quad \text{for} \quad i \geq 1 .$$

Since $h_1' = h_1 = 0$, these equations suffice to ensure that $h_i = h_i'$ for $1 \leq i \leq m$.

3. Applications

From the structure theorem, a cyclic difference set (see [1]) with parameters (v, k, λ) exists if and only if there is an ordered partition of v with structure (f_i) satisfying $f_0 = 2(k-\lambda)$, $f_1 = k - \lambda$, and $f_i = 0$ for $2 \leq i \leq [v/2]$. We can prove some inequalities for partitions with these properties.

PROPOSITION 2. *Suppose there is an ordered partition* $v = b_1 + b_2 + \ldots + b_t$ *with structure* (f_i) *satisfying* $f_0 = 2n$, $f_1 = n$, *and* $f_2 = f_3 = 0$. *Let* p_i *be the number of times that* i *occurs in* $(b_1, b_2, \ldots, b_t)$. *Then, whenever* $v > 11n/3$ *and* $n \geq 4$,

(1) $$p_1 = \tfrac{1}{2}t = n ,$$

(2) $$\max(0, 4n+1-v, n-[(v-n)/4]) \leq p_2 \leq [3n/4] ,$$

and

(3) $$\max(0, 5n-v-2p_2) \leq p_3 \leq \min(n-p_2-1, 2p_2, 3n-4p_2) .$$

Proof. By definition, $f_0 = 2n = t$; and f_1 is the number of ones in $\{b_1, b_2, \ldots, b_t\}$, hence we have (1).

A *one-run* A in the sequence $b = (b_1, b_2, \ldots, b_t)$ is a subsequence $A = (b_i, b_{i+1}, \ldots, b_j)$ where $b_i = 1 = b_{i+1} = \ldots = b_j$. Of course, we define one-runs cyclically: if $j < i$, then

$$A = (b_i, b_{i+1}, \ldots, b_t, b_1, \ldots, b_j) .$$

Let u be the number of one-runs of b, and let w be the number of one-runs with precisely one entry. Then the number of times $(1, 1)$ occurs in b is $\sum (|A|-1)$, where the sum runs over all the one-runs A of b.

But

$$\begin{aligned}\sum (|A|-1) &= \left(\sum |A|\right) - u \\ &= p_1 - u \\ &= n - u .\end{aligned}$$

Thus, since $f_2 = 0$, we obtain

(4) $$p_2 = n - u .$$

Now the number of times that $(1, 1, 1)$ occurs in b is $\sum (|A|-2)$, where the sum runs over all one-runs of b with more than one entry. But

(5) $$\begin{aligned}\sum (|A|-2) &= (n-w) - 2(u-w) \\ &= 2p_2 + w - n .\end{aligned}$$

Hence

(6) $$w \geq \max\{0, n-2p_2\} .$$

Now let x_1 and x_2 be the number of times $(1, 2)$ and $(2, 1)$ occur in b respectively. Then, for $i = 1, 2$, $x_i \leq u$ and $x_i \leq p_2$.

Hence

(7) $$\begin{aligned}x_1 + x_2 &\leq 2 \min\{u, p_2\} \\ &= 2 \min\{n-p_2, p_2\} .\end{aligned}$$

Using $f_3 = 0$ and (5), we obtain

$$p_3 + (2p_2-n+w) \leq 2 \min\{n-p_2, p_2\} .$$

This, together with (6) implies

https://doi.org/10.1017/S0004972700023467 Published online by Cambridge University Press

(8) $$p_3 \leq 2 \min\{n-p_2, p_2\} + n - 2p_2 - \max\{0, n-2p_2\}$$
$$= \min\{3n-4p_2, 2p_2\} .$$

Let $C = \{b_i : b_i \neq 1, 2, \text{or } 3\}$. Since $p_1 = n = \frac{1}{2}t$, $|C| = n - p_2 - p_3$. We show that $|C| > 0$. For if $|C| = 0$, then $n - p_2 = p_3$; so by (8), $n - p_2 \leq 2p_2$, so $p_2 \geq n/3$. But $v = p_1 + 2p_2 + 3p_3 = 4n - p_2$; hence $p_2 = 4n - v$. But this implies $4n - v \geq n/3$, and thus $v \leq 11n/3$, contrary to our assumptions.

Hence $|C| = n - p_2 - p_3 \geq 1$. So

(9) $$p_3 \leq n - p_2 - 1 .$$

Also, $\sum_{c \in C} c \geq 4|C|$, since $c \geq 4$ for all $c \in C$. This gives $v - p_1+2p_2+3p_3 \geq 4\ n-p_2-p_3$, and by (1) we have

(10) $$p_3 \geq 5n - 2p_2 - v .$$

Now (8), (9), and (10) together give (3). From (3) we obtain $\max(0, 4n+1-v, (5n-v)/4) \leq p_2 \leq [3n/4]$. But since $n \geq 4$, this is the same as (2). This completes the proof of Proposition 2.

Using Baumert's list of known difference sets [1], one can check that the inequalities (2) and (3) are sharp; that is, for each inequality in (2) and (3), there is a difference set for which equality holds.

A *circulant Hadamard matrix* is a circulant $(1, -1)$ matrix whose rows are mutually orthogonal. Konvalina and Kosloski [3] have defined a circulant quasi-Hadamard matrix to be a circulant $(-1, 1)$ matrix whose first row is orthogonal to all but possibly one of the succeeding rows. Let p_i be the number of blocks of length i in the first row of a circulant quasi-Hadamard matrix of order $4n \geq 16$. Konvalina and Kosloski noted that $p_1 = n$; from Proposition 2 we can also deduce

$$n/4 \leq p_2 \leq 3n/4 ,$$

and

https://doi.org/10.1017/S0004972700023467 Published online by Cambridge University Press

$$\max\{0,\ n-2p_2\} \le p_3 \le \min\{n-p_2-1,\ 2p_2,\ 3n-4p_2\}\ .$$

Since a circulant Hadamard matrix is a circulant quasi-Hadamard matrix, this gives bounds on the length of blocks in the first row of a circulant Hadamard matrix.

We can also calculate p_i for partitions with more general structure.

PROPOSITION 3. *Let* p_i *be the number of times that* i *occurs in the ordered partition* $m = b_1 + b_2 + \ldots + b_t$. *For* $i \ge 2$, *let*

$$m_i = m - \sum_{j=1}^{i-1} jp_j$$

and

$$t_i = t - \sum_{j=1}^{i-1} p_j\ .$$

Then $m_i \ge it_i$, *and*

(i) *if* $m_i = it_i$, *then* $p_i = t_i$; *and*

(ii) *if* $m_i > it_i$, *then* $p_i \le t_i-1$.

Proof. Note that t_i is the number of summands b_j which are greater than or equal to i ; m_i is their sum. Thus $m_i \ge it_i$ is immediate, and if $m_i = it_i$, then each b_j which is greater than $i - 1$ must be i ; thus $p_i = t_i$. And if $m_i > it_i$, then $p_i < t_i$; that is, $p_i \le t_i-1$.

Finally, the structure theorem gives a necessary condition for the existence of circulant weighing matrices. An $m \times m$ $(0, \pm 1)$ matrix satisfying $WW^t = kI_m$ is called a weighing matrix of weight k and order m . The problem of determining for which k and m a circulant weighing matrix of weight k and order m exists is discussed in [2].

Suppose X and Y are $(0, 1)$ circulants described by $b = (b_1, b_2, \ldots, b_n)$ and $c = (c_1, c_2, \ldots, c_u)$ respectively. Let

$x = (x_1, x_2, \ldots, x_m)$ and $y = (y_1, y_2, \ldots, y_m)$ be the first rows of x and y respectively. We will assume that $x_1 = 1$ and $x_m = 0$, but we will allow $y_1 = y_m$. If X and Y are disjoint, that is, $x_i = 1$ implies $y_i \neq 1$, then we say the *sum* of b and c is the sequence which describes $X + Y$.

COROLLARY 4. *Suppose there is a circulant weighing matrix W of weight k and order m . Then there are partitions $m = b_1 + b_2 + \ldots + b_n$ and $m = c_1 + c_2 + \ldots + c_u$ with sum $m = d_1 + d_2 + \ldots + d_v$ with the following properties:*

(i) $b_1 + b_3 + \ldots + b_{n-1} = (k+\sqrt{k})/2$;

(ii) $c_2 + c_4 + \ldots + c_u = (k-\sqrt{k})/2$;

(iii) $d_1 + d_3 + \ldots + d_v = k$;

and if (f_i), (g_i), and (h_i) are the structures of the partitions $m = b_1 + b_2 + \ldots + b_n$, $m = c_1 + c_2 + \ldots + c_u$, and $m = d_1 + d_2 + \ldots + d_v$, respectively, then

(iv) $2f_0 + 2g_0 - h_0 = 2k$;

(v) $2f_1 + 2g_1 - h_1 = k$;

(vi) $2f_i + 2g_i - h_i = 0$, *for* $i \geq 2$.

Proof. Write W as $X - Y$, where X and Y are $(0, 1)$ circulants. Since $WW^t = 2XX^t + 2YY^t - (X+Y)(X+Y)^t$, the corollary follows from the structure theorem.

References

[1] Leonard D. Baumert, *Cyclic difference sets* (Lecture Notes in Mathematics, 182. Springer-Verlag, Berlin, Heidelberg, New York, 1971).

https://doi.org/10.1017/S0004972700023467 Published online by Cambridge University Press

[2] Peter Eades and Richard M. Hain, "On circulant weighing matrices", *Ars Combinatoria* (to appear).

[3] John Konvalina and Rodney H. Kosloski, "Cyclic quasi-Hadamard matrices", *Utilitas Math.* (to appear).

Centre National des Recherches Scientifiques,
Université de Paris VII,
Paris,
France;

Department of Pure Mathematics,
School of General Studies,
Australian National University,
Canberra, ACT.