PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 41, Number 1, November 1973

VARIANTS OF CYCLIC DIFFERENCE SETS[1]

H. J. RYSER

ABSTRACT. This paper is an exploratory study of certain rare and intriguing configurations that are "almost" cyclic difference sets. The variants are of two types. We give precise definitions of the variants and then establish some nonexistence theorems. Only a few examples of the variants are known to us and their complete structure is far from understood.

1. **Introduction.** Let v, k, and λ be positive integers. Suppose that $D=\{d_1, \cdots, d_k\}$ is a set of k residues modulo v with the property that for any residue $a\not\equiv 0 \pmod{v}$ the congruence

$$d_i - d_j \equiv a \pmod{v} \tag{1.1}$$

has exactly λ solution pairs (d_i, d_j) with d_i and d_j in D. Such a residue set is called a *cyclic difference set*. The terms *difference set* and (v, k, λ)-*difference set* are also in standard usage.

It follows at once that

$$k(k-1) = \lambda(v-1). \tag{1.2}$$

It is customary to write

$$n = k - \lambda \tag{1.3}$$

and we usually assume that $n\geqq 2$ so that all of the degenerate difference sets are excluded. We let C denote the permutation matrix of order v with 1's in positions $(1, 2)$, $(2, 3)$, $\cdots$, $(v-1, v)$, $(v, 1)$ and 0's in all other positions. Then the *incidence matrix*

$$A = C^{d_1} + \cdots + C^{d_k} \tag{1.4}$$

Received by the editors February 20, 1973.

AMS (MOS) subject classifications (1970). Primary 05B10, 05B20, 05B25; Secondary 05B05, 15A24.

Key words and phrases. Circulant, cyclic difference set, finite projective plane, group divisible design, incidence matrix, planar difference set, symmetric block design.

[1] This research was supported in part by the Army Research Office-Durham under Grant DA-ARO-D-31-124-72-G171 and the National Science Foundation under Grant GP-36230X.

of the difference set D satisfies the matrix equation

$$(1.5) \qquad AA^{\mathrm{T}} = nI + \lambda J \equiv B,$$

where A^{T} is the transpose of the matrix A, I is the identity matrix of order v, and J is the matrix of 1's of order v.

Difference sets on the parameters

$$(1.6) \qquad v = n^2 + n + 1, \qquad k = n + 1, \qquad \lambda = 1$$

are called *planar* of *order n*. Singer has constructed planar difference sets for every prime power order and all known planar difference sets are of the Singer type. The extensive literature on difference sets is well summarized in the recent text by Baumert [**1**].

2. **Near difference sets of type 1.** We are now ready to define the first of two variants of the difference set D. Let $v \geqq 4$ be an even integer and let k and λ be positive integers. Suppose that $D_1 = \{d_1, \cdots, d_k\}$ is a set of k residues modulo v with the property that for any residue $a \not\equiv 0$, $v/2 \pmod v$ the congruence

$$(2.1) \qquad d_i - d_j \equiv a \pmod v$$

has exactly λ solution pairs (d_i, d_j) with d_i and d_j in D_1 and no solution pairs for the residue $a \equiv v/2 \pmod v$. Then we call D_1 a *near difference set* and we say that D_1 is of *type* 1.

It follows that

$$(2.2) \qquad k(k-1) = \lambda(v-2)$$

and we write

$$(2.3) \qquad n = k - \lambda.$$

Then the *incidence matrix*

$$(2.4) \qquad A = C^{d_1} + \cdots + C^{d_k}$$

of the near difference set D_1 of type 1 satisfies the matrix equation

$$(2.5) \qquad AA^{\mathrm{T}} = nI + \lambda J - \lambda C^{v/2} \equiv B_1.$$

We now prove a nonexistence theorem for near difference sets of type 1. The first portion of the theorem follows from known results on group divisible designs [**2**]. But we keep the discussion self-contained.

THEOREM 2.1. *Let $D_1 = \{d_1, \cdots, d_k\}$ be a near difference set of type* 1 *on the parameters v, k, and λ. Then $v \equiv 0$* (mod 4) *implies that $k - 2\lambda$ is a square and $v \equiv 2$* (mod 4) *implies that k is a square. Moreover, the existence* *of D_1 implies the existence of a cyclic difference set (possibly degenerate) on the parameters $v/2$, k, and 2λ.*

Proof. Equation (2.5) tells us that the determinant of the matrix B_1 must be a square. We write B_1 in the form

$$B_1 = \begin{bmatrix} nI + \lambda J & -\lambda I + \lambda J \\ -\lambda I + \lambda J & nI + \lambda J \end{bmatrix}, \tag{2.6}$$

where I and J are both of order $v/2$. If we subtract appropriate rows and then add appropriate columns we transform B_1 into

$$\begin{bmatrix} kI & -kI \\ -\lambda I + \lambda J & nI + \lambda J \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} kI & 0 \\ -\lambda I + \lambda J & (k - 2\lambda)I + 2\lambda J \end{bmatrix}, \tag{2.7}$$

respectively, where 0 is the zero matrix of order $v/2$. Hence

$$\det(B_1) = k^{v/2}(k - 2\lambda)^{(v-2)/2}(k + \lambda(v - 2)), \tag{2.8}$$

and by (2.2) we have

$$\det(B_1) = k^{(v+4)/2}(k - 2\lambda)^{(v-2)/2}. \tag{2.9}$$

We note that $k=2\lambda$ is possible only for $v\equiv 0 \pmod 4$, again by (2.2); thus (2.9) gives us our first conclusion.

Two distinct elements d_i and d_j of the near difference set $D_1 = \{d_1, \cdots, d_k\}$ of type 1 cannot satisfy $d_i \equiv d_j \pmod{v/2}$ because this implies $d_i - d_j \equiv v/2 \pmod v$, contrary to hypothesis. We now regard D_1 as a set of k residues modulo $v/2$. Then for any residue $a \not\equiv 0 \pmod{v/2}$ the congruence $d_i - d_j \equiv a \pmod{v/2}$ has exactly 2λ solution pairs (d_i, d_j) with d_i and d_j in D_1. Thus D_1 becomes a cyclic difference set on the parameters $v/2$, k, and 2λ.

Near difference sets of type 1 on the parameters

$$v = n^2 + n + 2, \qquad k = n + 1, \qquad \lambda = 1 \tag{2.10}$$

are called *planar* of *order n*. The following are planar near difference sets of type 1 of orders $n=1$, 2, and 3, respectively:

$$D_1 = \{0, 1\} \pmod 4,$$
$$D_1 = \{0, 1, 3\} \pmod 8,$$
$$D_1 = \{0, 1, 4, 6\} \pmod{14}.$$

These are the only orders of planar near difference sets of type 1 known to us.

The following is an example of a near difference set of type 1 on the parameters $v=12$, $k=5$, and $\lambda=2$: $D_1 = \{0, 1, 2, 4, 9\} \pmod{12}$.

3. **Near difference sets of type 2.** Our second variant of the difference set D is defined as follows. Let $v \geqq 4$, k, and λ be positive integers. Suppose that $D_2 = \{d_1, \cdots, d_k\}$ is a set of k residues modulo v with the property that for any residue $a \not\equiv 0, \pm 1 \pmod{v}$ the congruence

$$d_i - d_j \equiv a \pmod{v} \tag{3.1}$$

has exactly λ solution pairs (d_i, d_j) with d_i and d_j in D_2 and no solution pairs for the residues $a \equiv \pm 1 \pmod{v}$. Then we also call D_2 a *near difference set* and we say that D_2 is of *type* 2.

It follows that

$$k(k-1) = \lambda(v-3) \tag{3.2}$$

and we write

$$n = k - \lambda. \tag{3.3}$$

Then the *incidence matrix*

$$A = C^{d_1} + \cdots + C^{d_k} \tag{3.4}$$

of the near difference set D_2 of type 2 satisfies the matrix equation

$$AA^{\mathrm{T}} = nI + \lambda J - \lambda(C + C^{-1}) \equiv B_2. \tag{3.5}$$

The following nonexistence theorem for near difference sets of type 2 uses certain ideas developed earlier in [4] for cyclic difference sets.

THEOREM 3.1. *Let $D_2 = \{d_1, \cdots, d_k\}$ be a near difference set of type 2 on the parameters v, k, and λ. Suppose that $v = 3m$, where m is a positive integer. Then the Diophantine equation*

$$x^2 = ky^2 - \lambda(m-1)z^2 \tag{3.6}$$

has a solution in integers x, y, and z, not all zero.

PROOF. Let $\varepsilon \neq 1$ be a vth root of unity. Then following [4] we let

$$\theta(\varepsilon) = \varepsilon^{d_1} + \cdots + \varepsilon^{d_k}. \tag{3.7}$$

Since D_2 is a near difference set of type 2 we have

$$\theta(\varepsilon)\theta(\varepsilon^{-1}) = n - \lambda(\varepsilon + \varepsilon^{-1}). \tag{3.8}$$

Now let ε be a primitive 3rd root of unity. Then (3.8) reduces to

$$\theta(\varepsilon)\theta(\varepsilon^{-1}) = k. \tag{3.9}$$

Let e_i of the roots $\varepsilon^{d_1}, \cdots, \varepsilon^{d_k}$ be equal to ε^i $(i = 0, 1, 2)$. Then

$$e_0 + e_1 + e_2 = k \tag{3.10}$$

and we may write $\theta(\varepsilon)$ in the form

$$\theta(\varepsilon) = e_0 + e_1\varepsilon + e_2\varepsilon^2. \tag{3.11}$$

Equation (3.9) implies

$$e_0^2 + e_1^2 + e_2^2 - k = e_0e_1 + e_1e_2 + e_2e_0. \tag{3.12}$$

We square (3.10) and use (3.2) and (3.12) to obtain

$$e_0^2 + e_1^2 + e_2^2 = k + \lambda(m - 1) \tag{3.13}$$

and

$$e_0e_1 + e_1e_2 + e_2e_0 = \lambda(m - 1). \tag{3.14}$$

We now define the circulant

$$E = \begin{bmatrix} e_0 & e_1 & e_2 \\ e_2 & e_0 & e_1 \\ e_1 & e_2 & e_0 \end{bmatrix}. \tag{3.15}$$

Then it follows from (3.13) and (3.14) that

$$EE^{\mathrm{T}} = kI + \lambda(m - 1)J. \tag{3.16}$$

Hence by the basic nonexistence criterion for symmetric block designs we have that the Diophantine equation (3.6) has a solution in integers x, y, and z, not all zero. (Our precise situation is covered by the lemma on rational congruences in [**4**].)

Near difference sets of type 2 on the parameters

$$v = n^2 + n + 3, \qquad k = n + 1, \qquad \lambda = 1 \tag{3.17}$$

are called *planar* of *order n*. The following are planar near difference sets of type 2 of orders $n=1, 2, 3$, and 4, respectively:

$$D_2 = \{0, 2\} \pmod 5, \qquad D_2 = \{0, 2, 6\} \pmod 9,$$
$$D_2 = \{0, 2, 5, 9\} \pmod{15}, \qquad D_2 = \{0, 2, 7, 10, 19\} \pmod{23}.$$

These are the only orders of planar near difference sets of type 2 known to us. We remark that Theorem 3.1 excludes orders 5 and 9.

There is very great interest in the problem of the existence of a finite projective plane of order 10. This is the smallest undecided order. However, it has been known for a long time that there does not exist a planar difference set of order 10 [**3**]. Theorem 2.1 implies that there does not exist a planar near difference set of type 1 of order 10 because there does not exist a difference set on the parameters $v=56$, $k=11$, and $\lambda=2$. However, we have not excluded the possibility of the existence of a planar near difference set of type 2 of order 10. But its existence appears unlikely.

REFERENCES

1. L. D. Baumert, *Cyclic difference sets*, Lecture Notes in Math., vol. 182, Springer-Verlag, New York, 1971. MR **44** #97.

2. R. C. Bose and W. S. Connor, *Combinatorial properties of group divisible incomplete block designs*, Ann. Math. Statist. **23** (1952), 367–383. MR **14**, 124.

3. M. Hall, Jr., *Cyclic projective planes*, Duke Math. J. **14** (1947), 1079–1090. MR **9**, 370.

4. M. Hall, Jr. and H. J. Ryser, *Cyclic incidence matrices*, Canad. J. Math. **3** (1951), 495–502. MR **13**, 312.

DEPARTMENT OF MATHEMATICS, CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CALIFORNIA 91109