ON DIFFERENCE SETS WHOSE PARAMETERS SATISFY A CERTAIN RELATION

P. KESAVA MENON

1. **Introduction.** Let us denote, as usual, the parameters of a difference set by v, k, λ, n so that

$$k^2 = n + \lambda v, \tag{1.1}$$

$$k = n + \lambda. \tag{1.2}$$

We stipulate the further condition that

$$v = 4n. \tag{1.3}$$

Difference sets whose parameters satisfy (1.3) in addition to the necessary conditions (1.1) and (1.2) have certain remarkable properties. In the first place, since n is a divisor of v, there are no multipliers in the sense of Marshall Hall, Jr. for such a difference set. Secondly, the relation (1.3) enables us to express the parameters in terms of a single parameter l which may take all integral values. Lastly, the relation (1.3) is a necessary and sufficient condition for a certain composition of difference sets which produces other difference sets of the same kind.

2. **The values of parameters.** Let us suppose that the parameters satisfy (1.3). Then v is even so that, by the Chowla-Ryser condition, n must be a square, say,

$$n = l^2. \tag{2.1}$$

Substituting from (2.1) in (1.3) and (1.1) we get

$$v = 4l^2, \tag{2.2}$$

$$k^2 = l^2(1 + 4\lambda). \tag{2.3}$$

From (2.3) it follows at once that $1+4\lambda$ is a square, say,

$$1 + 4\lambda = (2t - 1)^2, \tag{2.4}$$

so that

$$\lambda = t(t - 1), \tag{2.5}$$

$$k = l(2t - 1). \tag{2.6}$$

Received by the editors March 20, 1961 and, in revised form, May 23, 1961.

Substituting from (2.1), (2.5) and (2.6) in (1.2) we get

$$l(2t-1) = l^2 + t(t-1)$$

so that

$$t = l \quad \text{or} \quad l+1.$$

Correspondingly we get the two sets of values for λ, k:

$$\lambda = l(l-1) \quad \text{or} \quad l(l+1),$$
$$k = l(2l-1) \quad \text{or} \quad l(2l+1).$$

Thus we get two sets of values for the parameters v, k, λ, n:

$$(2.7) \qquad v = 4l^2, \quad k = l(2l-1), \quad \lambda = l(l-1), \quad n = l^2,$$

$$(2.8) \qquad v = 4l^2, \quad k = l(2l+1), \quad \lambda = l(l+1), \quad n = l^2.$$

It is easily seen that if either of the sets (2.7) or (2.8) of parameters corresponds to a difference set then the other also corresponds to a difference set, namely, the complement of the former in the group in which it is defined. Moreover we note that by changing the sign of l we may reduce (2.8) to the form (2.7). Hence we have

THEOREM 1. *The values of the parameters of a difference set satisfying* (1.3) *are of the form* (2.7) *where l is a positive or negative integer, and two complementary difference sets of the kind have parameters which differ only by a change in the sign of l.*

3. **The composition theorem.** The following theorem is characteristic of difference sets whose parameters satisfy (1.3) and is a useful tool in the construction of such difference sets.

THEOREM 2. *Let S_1, S_2 be two difference sets in the groups G_1, G_2 respectively and $\overline{S}_1$, $\overline{S}_2$ their respective complements. Let $G = (G_1, G_2)$ be the direct product of G_1, G_2 and S the subset of G obtained as the union of the subsets (S_1, S_2) and $(\overline{S}_1, \overline{S}_2)$. Then S is a difference set in G if and only if the parameters of both S_1, S_2 satisfy* (1.3). *Moreover when S is a difference set its parameters will also satisfy* (1.3).

PROOF. Let S_i, $\overline{S}_i$ have the parameters

$$v_i, k_i, \lambda_i, n_i; \qquad \bar{v}_i, \bar{k}_i, \bar{\lambda}_i, \bar{n}_i \ .$$

respectively so that we have the relations

$$(3.1) \qquad \bar{v}_i = v_i, \quad \bar{n}_i = n_i, \quad \lambda_i + \bar{\lambda}_i = v_i - 2n_i, \qquad (i = 1, 2).$$

Since S_i, $\overline{S}_i$ are difference sets we have

$$S_iS_i^{-1} = n_ie_i + \lambda_iG_i,$$
$$\bar{S}_i\bar{S}_i^{-1} = n_ie_i + \bar{\lambda}_iG_i,$$
$$S_i\bar{S}_i^{-1} = \bar{S}_iS_i^{-1} = n_i(G_i - e_i)$$

where e_i is the identity element of G_i. Hence

$$\begin{aligned} SS^{-1} &= (S_1S_1^{-1}, S_2S_2^{-1}) + (\bar{S}_1\bar{S}_1^{-1}, \bar{S}_2\bar{S}_2^{-1}) \\ &\quad + (S_1\bar{S}_1^{-1}, S_2\bar{S}_2^{-1}) + (\bar{S}_1\bar{S}_1^{-1}, \bar{S}_2\bar{S}_2^{-1}) \\ &= (n_1e_1 + \lambda_1G_1, n_2e_2 + \lambda_2G_2) + (n_1e_1 + \bar{\lambda}_1G_1, n_2e_2 + \bar{\lambda}_2G_2) \\ &\quad + 2(n_1G_1 - n_1e_1, n_2G_2 - n_2e_2) \\ &= 4n_1n_2(e_1, e_2) + n_1(\lambda_2 + \bar{\lambda}_2 - 2n_2)(e_1, G_2) \\ &\quad + n_2(\lambda_1 + \bar{\lambda}_1 - 2n_1)(G_1, e_2) + (\lambda_1\lambda_2 + \bar{\lambda}_1\bar{\lambda}_2 + 2n_1n_2)G. \end{aligned} \tag{3.2}$$

It follows that S will be a difference set in G if and only

$$\lambda_i + \bar{\lambda}_i = 2n_i$$

or, by (3.1),

$$v_i = 4n_i, \qquad (i = 1, 2). \tag{3.3}$$

Moreover when (3.3) are satisfied (3.2) reduces to

$$SS^{-1} = 4n_1n_2(e_1, e_2) + (\lambda_1\lambda_2 + \bar{\lambda}_1\bar{\lambda}_2 + 2n_1n_2)G. \tag{3.4}$$

It follows that if we denote the parameters of S by v, k, λ, n, then

$$v = v_1v_2 = 16n_1n_2,$$
$$n = 4n_1n_2,$$

so that $v = 4n$ which completes the proof of the theorem.

4. **Applications of the composition theorem.** If a single difference set with parameters of the form (2.7) is known we may take both S_1 and S_2 in Theorem 2 to be that set, or one of them to be that set and the other its complement. Then we get two new difference sets which are, of course complements of each other and which have for their parameter v the square of the corresponding parameter of the given difference set. Retaining the given difference as S_1 and taking either of the new difference sets as S_2 we get a difference set whose parameter v is the cube of the corresponding parameter of the given set. Proceeding by induction we get

THEOREM 3. *If there exists a difference set with parameters of the form* (2.7) *for a certain value l_0 of l then there exists a difference set with parameters corresponding to* $l = 2^{r-1}l_0^r$ $(r = 1, 2, \cdots)$.

The next theorem that we are going to prove may be called the duplication formula.

THEOREM 4. *If there exists a difference set corresponding to the value l_0 of l then there exists a difference set for $l=2l_0$.*

PROOF. Take G_2 in Theorem 2 to be either the cyclic group of order four, or Klein's four-group and S_2 to be any single one of its elements. Then S_2 has obviously the parameters

$$v = 4, \quad k = 1, \quad \lambda = 0, \quad n = 1 \tag{4.1}$$

which correspond to $l=1$ in (2.7). Taking for S_1 the given difference set we see at once that the composite of S_1 and S_2 corresponds to $l=2l_0$.

The next theorem provides a nontrivial example of difference sets of the kind.

THEOREM 5. *There exist difference sets with parameters corresponding to $l=2^r$ $(r=1, 2, \cdots)$.*

PROOF. We start with a difference set with the parameters (4.1) and use the duplication formula to obtain a diffence set with parameters corresponding to $l=2$. Then the theorem follows by a repeated application of the duplication formula.

The existence of difference sets whose parameters correspond to $l=2^r$ has already been established by the author by different methods which are more or less analytical. The method given here, on the other hand, is purely combinatorial and leads to a result of even somewhat greater generality. It has the further advantage of giving rise to an infinity of difference sets of the kind as soon as a single one is known. We shall presently give another example of this method.

5. **A difference set with the parameters corresponding to $l=3$.** In attempting to discover difference sets corresponding to various values of l, the author has come across one corresponding to $l=3$. It was found almost by accident, by a happy choice of the basic group and a still luckier choice of the elements forming the difference set. The set in question may be defined as follows: Let D_3 be the dihedral group of order 6 whose elements may be expressed in the form

$$1, \ a, \ a^2, \ b, \ ab, \ a^2b$$

where

$$a^3 = b^2 = 1, \qquad ba = a^2b,$$

and let G_3 be the direct product of D_3 with itself so that G_3 is of order 36. It may be easily verified that the fifteen elements

$$\begin{array}{lll}
(1, 1), & (a, a^2), & (a^2, a) \\
(1, b), & (1, ab), & (1, a^2b) \\
(b, 1), & (ab, 1), & (a^2b, 1) \\
(b, ab), & (ab, a^2b), & (a^2b, b) \\
(ab, b), & (a^2b, ab), & (b, a^2b)
\end{array}$$

form a difference set in G_3 having the parameters

$$v = 36, \quad k = 15, \quad \lambda = 6, \quad n = 9.$$

The verification is left to the reader.

It may be observed that the basic group G_3 is noncommutative being the direct product of two noncommutative groups. This restriction is however not necessary. In fact we may obtain a difference set with the same parameters in the direct product of two cyclic groups of order 6. Thus taking G to be the set of 2-vectors (a, b) with addition mod 6 as the group operation we get the following difference set

$$\begin{array}{lll}
(0, 0), & (2, 4), & (4, 2) \\
(0, 1), & (0, 3), & (0, 5) \\
(1, 0), & (3, 0), & (5, 0) \\
(1, 3), & (3, 5), & (5, 1) \\
(3, 1), & (5, 3), & (1, 5)
\end{array}$$

in G. This is obtained from the previous example by replacing 1, a, a^2 by 0, 2, 4, and b, ab, a^2b by 1, 3, 5 respectively. The justification for this transition is left to the reader. Using the composition theorem we get at once

THEOREM 6. *There exist difference sets with parameters* (2.7) *corresponding to all values of l of the form* $2^s 3^r$, $s \geqq r-1 \geqq 0$.

6. Let us suppose that the basic group G of order $4l^2$ in which the difference set S with the parameters (2.7) is to be sought has a normal subgroup H of order l^2, and let

$$G = H + Ha_1 + Ha_2 + Ha_3 \tag{6.1}$$

be the decomposition of G into the cosets of H. The factor group G/H is either a cyclic group of order 4 or Klein's four-group. In either case we have

$$a_2a_3^{-1},\ a_3a_2^{-1} \in Ha_1,$$
$$(6.2) \qquad a_3a_1^{-1},\ a_1a_3^{-1} \in Ha_2,$$
$$a_1a_2^{-1},\ a_2a_1^{-1} \in Ha_3.$$

Suppose x_0, x_1, x_2, x_3 elements are chosen respectively from H, Ha_1, Ha_2, Ha_3 to form the difference set S. Then we have obviously

$$(6.3) \qquad x_0 + x_1 + x_2 + x_3 = l(2l - 1).$$

A "difference" of two elements of S will be contained in H if and only if both the elements belong to the same coset of H. Hence we have $x_0^2+x_1^2+x_2^2+x_3^2$ differences which are elements of H so that

$$(6.4) \qquad x_0^2 + x_1^2 + x_2^2 + x_3^2 = n + \lambda l^2 = l^2(l^2 - l + 1).$$

The number of elements of Ha_1 among the differences is easily seen to be $2(x_0x_1+x_2x_3)$ so that we have

$$(6.5) \qquad \alpha = 2(x_0x_1 + x_2x_3) = \lambda l^2 = l^3(l - 1),$$

and likewise,

$$(6.6) \qquad \beta = 2(x_0x_2 + x_1x_3) = l^3(l - 1),$$

and

$$(6.7) \qquad \gamma = 2(x_0x_3 + x_1x_2) = l^3(l - 1).$$

The equations (6.3) to (6.7) are easily seen to be consistent. From them we get

$$(6.8) \qquad \sum \alpha = 2 \sum x_0x_1 = 3l^3(l - 1),$$

$$(6.9) \qquad \begin{aligned} \sum \alpha\beta &= 4 \sum x_0 \sum x_0x_1x_2 - 16x_0x_1x_2x_3 \\ &= 3l^6(l - 1)^2, \end{aligned}$$

$$(6.10) \qquad \begin{aligned} \alpha\beta\gamma &= 8x_0x_1x_2x_3 \sum x_0^2 + 8 \sum x_0^2x_1^2x_2^2 \\ &= 8x_0x_1x_2x_3\left(\sum x_0^2 - 2 \sum x_0x_1\right) + 8\left(\sum x_0x_1x_2\right)^2 \\ &= l^9(l - 1)^3. \end{aligned}$$

Denoting $\sum x_0x_1x_2$, $x_0x_1x_2x_3$ by s, t respectively we may write (6.9) and (6.10) as

$$4l(2l - 1)s - 16t = 3l^6(l - 1)^2$$
$$8s^2 - 8tl^2(2l^2 - 2l - 1) = l^9(l - 1)^3$$

which have the two solutions

$$(6.11) \qquad 4s = l^5(2l-3), \qquad 16t = l^7(l-2)$$

and

$$(6.12) \qquad 4s = l^3(l-1)^2(2l+1), \quad 16t = l^4(l-1)^3(l+1).$$

Accordingly we see that x_0, x_1, x_2, x_3 may be the roots of either of the equations

$$16x^4 - 16l(2l-1)x^3 + 24l^3(l-1)x^2 - 4l^5(2l-3)x + l^7(l-2) = 0$$

or

$$16x^4 - 16l(2l-1)x^3 + 24l^3(l-1)x^2 - 4l^3(l-1)^2(2l+1)x + l^4(l-1)^3(l+1) = 0.$$

It is easily seen that these equations may be written in the forms

$$(2x-l^2)^3\{2x-l(l-2)\} = 0,$$
$$\{2x-l(l-1)\}^3\{2x-l(l+1)\} = 0,$$

respectively. Thus we get two possible sets of values for x_0, x_1, x_2, x_3, namely,

$$(6.13) \qquad \frac{l^2}{2}, \quad \frac{l^2}{2}, \quad \frac{l^2}{2}, \quad \frac{l(l-2)}{2},$$

and

$$(6.14) \qquad \frac{l(l-1)}{2}, \quad \frac{l(l-1)}{2}, \quad \frac{l(l-1)}{2}, \quad \frac{l(l+1)}{2},$$

in some order. Of these the set (6.13) is admissible only if l is even, whereas (6.14) may hold for all l. Thus we have

THEOREM 7. *If the group G of order $4l^2$ having a normal subgroup H of order l^2 contains a difference set S with parameters* (2.7) *then the number of elements to be chosen from the cosets of H to form S is given by either* (6.13) *or* (6.14), *the former holding only when l is even.*

REFERENCE

1. P. Kesava Menon, *Difference sets in abelian groups*, Proc. Amer. Math. Soc. **11** (1960), 368–376.

NEW DELHI, INDIA