A FAMILY OF DIFFERENCE SETS

R. G. STANTON AND D. A. SPROTT

1. Introduction. A difference set $(\mathfrak{G},D)$ is defined in **(2)** as a subset D of k elements in a group $\mathfrak{G}$ of order v with the following properties:

(1) if $x \in \mathfrak{G}$, $x \neq 1$, there are exactly λ distinct ordered pairs (d_1, d_2) of elements of D such that $x = d_1^{-1}d_2$;

(2) if $x \in \mathfrak{G}$, $x \neq 1$, there are exactly λ distinct ordered pairs (d_3,d_4) of elements of D such that $x = d_3d_4^{-1}$.

If $\mathfrak{G}$ is abelian, the difference set $(\mathfrak{G},D)$ is said to be abelian; if $\mathfrak{G}$ is cyclic, $(\mathfrak{G},D)$ is said to be cyclic.

A cyclic difference set was earlier defined as a set of k distinct residues $d_1,d_2, \ldots, d_k$ (modulo v) with the property that all non-zero residues modulo v occur exactly λ times among the differences $d_i - d_j$ $(i \neq j)$. Such sets have been studied in detail **(3)**. Although the general difference set $(\mathfrak{G},D)$ was introduced in (2), the abelian difference set was used previously **(1)** to construct symmetrical balanced incomplete block designs. Thus, if $v = 4\lambda + 3 = p^n$, where p is prime, and if x is a primitive element of $GF(p^n)$, the set

$$(x^0,x^2,x^4, \ldots, x^{4\lambda})$$

is an abelian difference set. If $n = 1$, so that v is prime, then this becomes a cyclic difference set modulo v.

In **(3)**, a generalization of previous work on cyclic difference sets is presented, and a system of classification is given for sets in which $k < \frac{1}{2}v$ and $3 \leqslant k \leqslant 50$.

It is the purpose of this paper to prove the existence of the abelian difference set with parameters $v = p^n(p^n + 2)$, $k = \frac{1}{2}(v - 1)$, $\lambda = \frac{1}{4}(v - 3)$, where p^n and $q^m = p^n + 2$ are both prime powers. This includes the balanced incomplete block design $v = b = 63$, $r = k = 31$, $\lambda = 15$. If $n = m = 1$, the result is a family of cyclic difference sets including the case $v = 35$, $k = 17$, $\lambda = 8$, given in **(3)**. In what follows, p and q will always denote primes, and x and y will be primitive elements of $GF(p^n)$ and $GF(q^m)$ respectively; also, $q^m = p^n + 2$.

The difference set will be constructed by using the Galois Domain $GD(v)$, that is, the set of elements (α,β), where $\alpha \in GF(p^n)$ and $\beta \in GF(q^m)$. Addition and multiplication are defined by the relations

$$(\alpha_1,\beta_1) + (\alpha_2,\beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2),$$
$$(\alpha_1,\beta_1)\,(\alpha_2,\beta_2) = (\alpha_1\alpha_2, \beta_1\beta_2).$$

Received March 27, 1957

It will be convenient to name the elements of $GD(v)$ as follows:

$$z^i = (x^i,y^i), \quad w^i = (x^i,0), \quad u^i = (0,y^i), \quad 0 = (0,0).$$

In particular, $z^iz^j = z^{i+j}$.

The elements of $GD(v)$ form an additive abelian group; the subset of elements of the form z^i is a multiplicative abelian group of order $\frac{1}{2}(s^2 - 1)$. The method of counting differences between elements is similar to that used in (4) and (5).

2. Construction of the family. We prove the

THEOREM. *The elements*

$$(z^0,z,z^2, \ldots, z^{\frac{1}{2}(s^2-1)-1}, 0,w^0,w, \ldots, w^{s-2})$$

form a difference set with parameters $v = s(s + 2)$, $k = \frac{1}{2}(v - 1)$, $\lambda = \frac{1}{4}(v - 3)$, *where* $s = p^n$, $s + 2 = q^m$.

Proof. The differences are of three types:

(1) differences $w^i(w^j - 1)$ and $\pm w^i$;

(2) differences $\pm (z^i - w^j)$ and $\pm z^i$;

(3) differences $z^i(z^j - 1)$.

The differences of type (1) can be written in the form

$$(x^i(x^j - 1), 0) \text{ and } (\pm x^i, 0)$$

where i ranges from 0 to s-2, and j ranges from 1 to $s-2$. For j fixed, all elements of the form $(x^i,0) = w^i$ occur once among the differences $(x^i(x^j - 1), 0)$; hence, as j ranges, these elements occur $s-2$ times among such differences. Thus, the differences of type (1) produce each element w^i a total of $(s - 2) + 2 = s$ times.

Now consider the differences of type (2), in particular, the differences with negative signs

$$(x^i(x^{j-i} - 1), - y^i), - (x^i,y^i).$$

Elements of the form $w^i = (x^i,0)$ and $0 = (0,0)$ do not occur at all among these differences. For each value of i, j may range from 0 to $s-2$; hence the term $x^i(x^{j-i} - 1)$ takes on $s-1$ distinct values. As i ranges from 0 to s, the total number of distinct elements occurring among these negative type (2) differences is

$$(s - 1)(s + 1) + (s + 1) = s(s + 1).$$

Thus all elements not of the form $(a,0)$ occur once. Taking into account the plus and minus signs, and allowing i to range from 0 to $\frac{1}{2}(s^2 - 1) - 1$, we see that all elements not of the form $(a,0)$ occur among the type (2) differences a total of $(s^2 - 1)/(s + 1) = s - 1$ times.

Finally, consider the type (3) differences $z^i(z^j - 1)$. These are elements of the form

$$(x^i(x^j - 1), y^i(y^j - 1)).$$

If $j = c(s - 1)$, where $c = 1,2, \ldots, \frac{1}{2}(s - 1)$, these elements have the form

$$(0, y^i(y^{c(s-1)} - 1)).$$

For a given c, all elements $(0,b)$ occur $\frac{1}{2}(s^2 - 1)/(s + 1) = \frac{1}{2}(s - 1)$ times; as c ranges, such elements occur $\frac{1}{4}(s - 1)^2$ times. Since they occurred $s - 1$ times among the differences of type (2), they must occur $\frac{1}{4}(s^2 + 2s - 3)$ times in all.

Similarly, if $j = d(s + 1)$, where $d = 1,2, \ldots, \frac{1}{2}(s - 3)$, the type (3) differences are of the form

$$(x^i(x^{d(s+1)} - 1), 0).$$

For d fixed, all elements of the form $(a,0)$ occur $\frac{1}{2}(s + 1)$ times; as d ranges, they occur $\frac{1}{4}(s + 1)(s - 3)$ times. But they occurred s times among the differences of type (1); so they must occur $\frac{1}{4}(s^2 + 2s - 3)$ times in all.

If j does not have the form $c(s - 1)$ nor the form $d(s + 1)$, then, for j fixed, the differences

$$(x^i(x^j - 1), y^i(y^j - 1))$$

range over half of the $s^2 - 1$ elements of the form (a,b); for the same j, the differences

$$-(x^i(x^j - 1), y^i(y^j - 1)) = (x^r(x^j - 1), y^t(y^j - 1))$$

range over the other half of the elements of the form (a,b). For, if this were not so, we should have

$$i + \tfrac{1}{2}(s - 1) \equiv r \pmod{s - 1},$$
$$i + \tfrac{1}{2}(s + 1) \equiv r \pmod{s + 1}.$$

Writing these congruences as equations, and subtracting, we find

$$k_1(s - 1) - k_2(s + 1) + 1 = 0,$$

where both k_1 and k_2 are integers. This is impossible, since 2 is a divisor of $s - 1$ and $s + 1$.

Thus we conclude that, for j fixed, the differences

$$\pm (x^i(x^j - 1), y^i(y^j - 1))$$

range once over all elements of the form (a,b). As j ranges, these elements will occur a total of $\frac{1}{2}\{\frac{1}{2}(s^2 - 1) - 1 - \frac{1}{2}(s - 3) - \frac{1}{2}(s - 1)\} = \frac{1}{4}(s^2 - 2s + 1)$ times. Since they occurred $s - 1$ times among the differences of type (2), they will occur $\frac{1}{4}(s^2 + 2s - 3)$ times in all. This completes the theorem: all non-zero elements $(a,0)$, $(0,b)$, and (a,b) occur $\lambda = \frac{1}{4}(s^2 + 2s - 3)$ times.

3. Example. Take $p = 7$, $p + 2 = 3^2$. To construct $GF(9)$, we use the irreducible polynomial $f(x) = x^2 + 2x + 2$; then x is a primitive element, and the field is made up of elements

$$x^0 = 1, x, x^2 = x + 1, x^3 = 2x + 1, x^4 = 2, x^5 = 2x, x^6 = 2x + 2, x^7 = x + 2,$$

together with 0. Since 3 is a primitive root modulo 7, we take $z = (3,x)$, $w = (3,0)$, $0 = (0,0)$. The difference set is

$$(z^0, z, z^2, \ldots, z^{23}, 0, w^0, w, w^2, \ldots, w^5),$$

with parameters $v = 63$, $k = 31$, $\lambda = 15$. Two cyclic difference sets with these parameters are given in **(3)**.

To show that the difference set constructed in this example is not isomorphic to either of these cyclic difference sets, we consider incidence relations among the blocks of the corresponding balanced incomplete block designs. We first note that if, in any one of these three designs, there exist seven blocks with seven common elements, then these seven common elements must differ by an element of additive period seven. It follows at once that the 2 cyclic designs of **(3)** have the property that 0,9,18,27,36,45,54 all occur in seven blocks, and they are the only elements with this property; in the design constructed in this example, the elements (0,0), (1,0), (2,0), (3,0), (4,0), (5,0), and (6,0) all occur in seven blocks, and they are the only elements with this property. Consequently, if the design under consideration is to be isomorphic to either of the designs in **(3)**, then the elements (0,0), . . . , (6,0) must correspond to the elements 0, . . . , 54 in some order.

Now both the cyclic designs have one property in common; if any pair of the elements 0,9,18,27,36,45,54 occurs in a block, then a third determined element occurs in that block, that is, any triplet of these numbers either does not occur in any block, or it occurs in 15 blocks. In the case of the projective design, this follows from the fact that any two points determine a line, and any 4-space through the line must contain the third point on that line; in the case of the other cyclic design, it is clear that the triplet (0,9,45) occurs 15 times and hence, by addition, so do the triplets (9,18,54), (18,27,0), (27,36,9), (36,45,18), (45,54,27), (54,0,36); since this accounts for all 21 possible doublets of these elements, no other triplets can occur.

On the other hand, the triplet structure of the present design is quite different; consider, for example, the pair of elements (0,0) and (1,0). They occur together in 15 blocks, of which seven blocks contain the other elements (2,0), (3,0), (4,0), (5,0) and (6,0). But an elementary discussion of congruences shows that the other 8 blocks containing (0,0) and (1,0) can contain, in each case, only one element of the form $(a,0)$. For 4 of these blocks, it is (3,0); for the other 4, it is (5,0). Thus, in this design, the triplets (0,0), (1,0), (3,0) and (0,0), (1,0), (5,0) occur exactly 11 times. This completes the demonstration that we do not have either of Hall's cyclic designs.

If $n = m = 1$, the result is the family of cyclic difference sets with $v = p(p + 2)$, $k = \frac{1}{2}(v - 1)$, $\lambda = \frac{1}{4}(v - 3)$. In this case, the pairs (x,y) and $(x,0)$ can be replaced by the residues z and w modulo v defined by

$$z \equiv x \pmod{p}, \qquad z \equiv y \pmod{p + 2};$$
$$w \equiv x \pmod{p}, \qquad w \equiv 0 \pmod{p + 2}.$$

4. Two further examples. (i) Suppose $p = 3$, $p + 2 = 5$; then $v = 15$, $k = 7$, $\lambda = 3$. Since 2 is a primitive root mod 3 and mod 5, we can take $z = 2$, $w = 5$, thus generating the difference set

$$(2^0, 2, 2^2, 2^3, 0, 5, 5^2) = (1,2,4,8,0,5,10).$$

Of course, this set could also have been obtained from a projective geometry.

(ii) Suppose $p = 5$, $p + 2 = 7$; then $v = 35$, $k = 17$, $\lambda = 8$. Here 3 is a primitive root mod 5 and mod 7; so $z = 3$, $w = 28$. The set is

$$(3^0, 3, 3^2, \ldots, 3^{11}, 0, 28, 28^2, 28^3, 28^4),$$

or

$$(1,3,9,27,11,33,29,17,16,13,4,12,0,28,14,7,21),$$

as given in **(3)**. Since 2 and 3 are primitive roots mod 5 and mod 7 respectively, $z = 17$ and $w = 7$ could also have been used to generate this difference set.

References

1. R. C. Bose, *On the construction of balanced incomplete block designs*, Ann. Eugenics, *9* (1939), 353–399.
2. R. H. Bruck, *Difference sets in a finite group*, Trans. Amer. Math. Soc., *73* (1955), 464–481.
3. Marshall Hall, *A survey of difference sets*, Proc. Amer. Math. Soc., *7* (1956), 975–986.
4. D. A. Sprott, *A Note on balanced incomplete block designs*, Can. J. Math., *6* (1954), 341–346.
5. D. A. Sprott, *Some series of balanced incomplete block designs*, Sankhyā, *17* (1956), 185–192.

University of Toronto