# A SURVEY OF DIFFERENCE SETS[1]

MARSHALL HALL, JR.

1. **Introduction.** A set of $k$ distinct residues $d_1, d_2, \cdots, d_k$ modulo $v$ is called a difference set $D$ if every residue $b \not\equiv 0 \pmod{v}$ can be expressed in exactly $\lambda$ ways in the form $b \equiv d_i - d_j \pmod{v}$ with $d_i, d_j \in D$. The $v$ sets of residues $d_1+i, d_2+i, \cdots, d_k+i \pmod{v}$, $i=0, \cdots, v-1$, will form the blocks of a symmetric block design with parameters $v, k, \lambda$ satisfying $k(k-1)=\lambda(v-1)$. The mapping $x \to x+1 \pmod{v}$ is an automorphism of the block design which is cyclic and regular on both the elements and the blocks of the design, and conversely a symmetric design with such an automorphism may be represented by a difference set. Difference sets have been extensively studied and a partial bibliography is given at the end of this paper. If there is a residue $t$ modulo $v$ such that the mapping $x \to xt \pmod{v}$ is an automorphism of the design, then $t$ is called a multiplier of the difference set. The existence of multipliers has been one of the main tools in the construction and study of difference sets.

In an attempt to study a reasonably large number of combinatorial designs, a survey was made of all difference sets with parameters $v, k, \lambda$, with $k$ in the range $3 \leqq k \leqq 50$. The parameters must satisfy $k(k-1)=\lambda(v-1)$ and taking $k < v/2$ (as we may since the complement of a difference set is also a difference set) there were 268 choices of parameters. Of these choices 101 correspond to no design because of the criteria of Chowla and Ryser [2], and hence a fortiori to no difference set. Of the remaining 167, difference sets were found in 46 cases, and in only twelve cases does the existence of a difference set remain undecided.

This work involved a combination of theorems, some old and two new ones given here, hand calculations and calculations on SWAC, the digital computer at Numerical Analysis Research at the University of California in Los Angeles. The interplay of hand and machine calculations should be remarked upon. In the case of the four non-isomorphic solutions for $v=121$, $k=40$, $\lambda=13$ the machine found several solutions in three hours running time, finding a solution and others isomorphic to it. But it would have taken several hundred hours to complete the search at this rate. A careful study modulo 11

Received by the editors December 30, 1955.

[1] This research was supported by the National Science Foundation.

by hand led to 42 judiciously chosen starts which would eliminate most of the duplication and enormously shorten running time in other respects. Each of these 42 cases was so fast on the machine that the entire set was easily handled.

2. **Two theorems on difference sets.** The existence of multipliers is one of the main tools in constructing difference sets or showing that a difference set does not exist. The following theorem generalizes and includes the previously known theorems. As usual the parameters are $v$, $k$, $\lambda$, $n=k-\lambda$ where

$$k(k-1) = \lambda(v-1). \tag{2.1}$$

THEOREM 2.1. *Let $n_1$ be a divisor of $n=k-\lambda$ such that $(n_1, v)=1$ and $n_1>\lambda$. Also suppose that $t$ is an integer such that for each prime $p$ dividing $n_1$ there is a $j$ such that $p^j \equiv t \pmod{v}$. Then $t$ is a multiplier of a difference set $d_1, d_2, \cdots, d_k \pmod{v}$.*

PROOF. Note that with $n_1=p$, $t=p$ this includes Theorem 3.1 of [4]. It is also more general than the theorem enunciated there in Example 4 which corresponds to the present theorem in the special case in which $n_1$ is square-free. Also note that if $n_1=n$, then certainly $n_1>\lambda$. As in [4] we write

$$\theta(x) = x^{d_1} + x^{d_2} + \cdots + x^{d_k}$$

if $d_1, d_2, \cdots, d_k$ is a difference set modulo $v$. Then the properties of a difference set yield

$$\theta(x)\theta(x^{-1}) \equiv n + \lambda T(x) \pmod{x^v - 1} \tag{2.2}$$

where $T(x)=1+x+\cdots+x^{v-1}=(x^v-1)/(x-1)$. Let $T(x)=f_1(x)f_2(x)\cdots f_r(x)$ be the decomposition of $T(x)$ into irreducible factors over the rational field. Then the $f_i(x)$ are distinct and the roots of $f_i(x)$ are certain $v$th roots of unity. From the theory of cyclotomic fields if $f_i(x)$ is of degree $u$ and $\zeta$ is a root of $f_i(x)$, then $1, \zeta, \cdots, \zeta^{u-1}$ form an integral basis for the field $K(\zeta)$ whence we can associate the algebraic integers of $K(\zeta)$ with the residue classes of polynomials with rational integral coefficients modulo $f_i(x)$.

Writing $n=n_1n_2$ we have

$$\theta(x)\theta(x^{-1}) \equiv n_1n_2 \pmod{f_i(x)}, \tag{2.3}$$

which we may regard as a factorization of $n$ in $K(\zeta)$. Now if $\mathfrak{p}$ is a prime ideal divisor of $\theta(\zeta^{-1})$ and also the rational prime $p$ dividing $n_1$, then the automorphism of the field $K(\zeta)$ determined by $\zeta \to \zeta^p$ leaves $\mathfrak{p}$ unchanged. We note that this is an automorphism because

$(p, v)=1$. Also since $t\equiv p^i \pmod v$ and $\zeta^v=1$, it follows that $\zeta\to\zeta^t$ gives an automorphism of $K(\zeta)$ which takes $\mathfrak{p}$ into itself. Since this holds for every prime ideal divisor of $\theta(\zeta^{-1})$ and $n_1$ it will follow that, since $\theta(\zeta)\theta(\zeta^{-1})$ was divisible by $n_1$, $\theta(\zeta)\theta(\zeta^{-t})$ is also divisible by $n_1$. In terms of congruences this becomes

$$\theta(x)\theta(x^{-t}) \equiv n_1 S_i(x) \pmod{f_i(x)}. \tag{2.4}$$

There will be such a congruence for each irreducible factor of $T(x)$. We wish to deduce a similar congruence with $T(x)$ as a modulus. Suppose

$$\theta(x)\theta(x^{-t}) = n_1 R_j(x) + A(x)F_j(x), \tag{2.5}$$

where $F_j(x)=f_1(x)f_2(x)\cdots f_j(x)$. This is immediate for $j=1$ from (2.4). Also from (2.4) with $i=j+1$ we have

$$\theta(x)\theta(x^{-t}) = n_1 S_{j+1}(x) + B(x)f_{j+1}(x). \tag{2.6}$$

We will have for some integral polynomials $C(x)$ and $D(x)$

$$C(x)F_j(x) + D(x)f_{j+1}(x) = w, \tag{2.7}$$

where the integer $w$ is the resultant of $F_j(x)$ and $f_{j+1}(x)$. Now $w$ can be expressed as a product of factors $\alpha-\beta$ where $\alpha$ is a root of $F_j(x)$ and $\beta$ is a root of $f_{j+1}(x)$. But $\alpha$ and $\beta$ will be different $v$th roots of unity and if $\zeta$ is a primitive $v$th root of unity then for appropriate exponents $y, s$, $\alpha-\beta=\zeta^y(\zeta^s-1)$. Now $\zeta^y$ is a unit and $\zeta^s-1$ is a root of

$$[(z+1)^v - 1]/z = z^{v-1} + \cdots + v = 0, \tag{2.8}$$

and so $\zeta^s-1$ is a divisor of $v$. Hence $w$ will be a divisor of an appropriate power of $v$ and since $(n_1, v)=1$ by hypothesis then also $(n_1, w)=1$. Multiplying (2.5) by $D(x)f_{j+1}(x)$ and (2.6) by $C(x)F_j(x)$ and adding we have

$$w\theta(x)\theta(x^{-t}) = n_1 S(x) + G(x)F_{j+1}(x). \tag{2.9}$$

This may be combined with the trivial relation $n_1\theta(x)\theta(x^{-t})=n_1 H(x)$ using $(n_1, w)=1$ to yield

$$\theta(x)\theta(x^{-t}) = n_1 R_{j+1}(x) + A(x)F_{j+1}(x). \tag{2.10}$$

Continuing we find

$$\theta(x)\theta(x^{-t}) = n_1 R(x) + A(x)T(x). \tag{2.11}$$

From here on the argument is essentially the same as that in [4]. We take (2.11) modulo $x^v-1$ noting that $A(x)T(x)\equiv A(1)T(x)$ $\equiv AT(x) \pmod{x^v-1}$.

$$\theta(x)\theta(x^{-t}) \equiv n_1 R(x) + AT(x) \pmod{x^v - 1}. \tag{2.12}$$

Putting $x=1$ in (2.12) we have

$$k^2 = n_1 R(1) + Av. \tag{2.13}$$

But $k^2-\lambda v = k-\lambda = n$ whence

$$k^2 \equiv Av \equiv \lambda v \pmod{n_1} \tag{2.14}$$

and so since $(n_1, v)=1$

$$A \equiv \lambda \pmod{n_1}. \tag{2.15}$$

Hence in (2.12) we may replace $A$ by $\lambda$ if we change $R(x)$ appropriately. We now have

$$\theta(x)\theta(x^{-t}) \equiv n_1 R(x) + \lambda T(x) \pmod{x^v - 1}. \tag{2.16}$$

From the left-hand side of this every coefficient is non-negative and from the right-hand side every coefficient is congruent to $\lambda$ modulo $n_1$. Since $n_1 > \lambda$ by hypothesis, every coefficient is therefore at least $\lambda$ and so in $R(x)$ all coefficients are non-negative. Since (2.16) is an identity we may replace $x$ by $x^{-1}$ to obtain

$$\theta(x^{-1})\theta(x^t) \equiv n_1 R(x^{-1}) + \lambda T(x) \pmod{x^v - 1}. \tag{2.17}$$

Now since $t$ is prime to $v$ we have both relations

$$\theta(x)\theta(x^{-1}) \equiv n_1 n_2 + \lambda T(x) \pmod{x^v - 1}, \tag{2.18}$$

$$\theta(x^t)\theta(x^{-t}) \equiv n_1 n_2 + \lambda T(x) \pmod{x^v - 1}. \tag{2.19}$$

With $x=1$ in (2.16) we have

$$k^2 = n_1 R(1) + \lambda v$$

whence since $k^2-\lambda v = n$ we have

$$R(1) = n_2. \tag{2.20}$$

The product of the left-hand sides of (2.16) and (2.17) is the same as that of (2.18) and (2.19). Equating the product of the right-hand sides, using (2.20) and simplifying we have

$$R(x)R(x^{-1}) \equiv n_2^2 \pmod{x^v - 1}. \tag{2.21}$$

But since $R(x)$ has non-negative coefficients this requires that $R(x)$ has only a single nonzero term and so for some power $x^{-s}$

$$R(x) \equiv n_2 x^{-s} \pmod{x^v - 1}. \tag{2.22}$$

Hence (2.17) becomes

$$\theta(x^{-1})\theta(x^t) \equiv nx^s + \lambda T(x) \pmod{x^v - 1}. \tag{2.23}$$

Multiplying by $\theta(x)$, using (2.2) and simplifying we have

$$\theta(x^t) \equiv x^s\theta(x) \pmod{x^v - 1} \tag{2.24}$$

and this says that $t$ is a multiplier of the difference set, saying that $td_1, td_2, \cdots, td_k$ are $d_{1s}, \cdots, d_{ks}$ in some order. This proves the theorem.

When $n_1 = n$ a further property of algebraic numbers is relevant which does not depend on inequalities. This we note here although it adds nothing to the above proof since $n > \lambda$ always. Thus in (2.4) we have

$$\theta(x)\theta(x^{-t}) \equiv nS_i(x) \pmod{f_i(x)} \text{ where in } K(\zeta), \tag{2.25}$$

$S_i(\zeta)$ is a unit. Now

$$\theta(x^j)\theta(x^{-j}) \equiv n \pmod{f_i(x)} \tag{2.26}$$

for every $j$ prime to $v$. Thus as $\theta(\zeta^j)$ and $\theta(\zeta^{-j})$ are complex conjugates $|\theta(\zeta^j)| = n^{1/2}$. Hence in (2.25), $S_i(\zeta^j)$ is an algebraic integer of absolute value 1 for all $j$ prime to $v$. But an algebraic integer all of whose conjugates have absolute value 1 is a root of unity and in $K(\zeta)$ the roots of unity are of the form $\pm\zeta^s$. Hence (2.25) becomes

$$\theta(x)\theta(x^{-t}) \equiv \pm nx^s \pmod{f_i(x)}. \tag{2.27}$$

In several instances this method gave information not covered by the theorem. With $v = 221$, $k = 45$, $\lambda = 9$ we have $t = 16 \equiv 2^4 \equiv 3^{40} \pmod{221}$ as a multiplier, but applying the method to

$$\theta(x)\theta(x^{-1}) \equiv 36 + 117T_{17}(x) \pmod{x^{17} - 1}$$

we find that $2 \equiv 3^{14} \pmod{17}$ is a multiplier at least so far as the modulus 17 is concerned. Here if $\theta(x) \equiv \sum a_i x_i \pmod{x^{17} - 1}$ we have $a_1 = a_r$ if $r$ is a quadratic residue of 17 and $a_s = a_m$ if $m$ is a nonresidue. Here $a_0 + 8a_1 + 8a_3 = 45$, $a_0^2 + 8a_1^2 + 8a_3^2 = 153$. As these have no solution in non-negative integers no difference set exists.

In calculating difference sets of the Hadamard type with $v = 4t - 1$, $k = 2t - 1$, $\lambda = t - 1$ it was found that for $v = 31$ and $v = 43$ not only the quadratic residues but also residues with indices $\equiv 0, 1, 3 \pmod 6$ gave difference sets. On investigation these turned out to be instances of a general theorem.

THEOREM 2.2. *A set of residues forming a difference set modulo a prime $p = 6f + 1$ which includes the sextic residues as multipliers may consist of* (1) *the quadratic residues when* $p \equiv 3 \pmod 4$ *or* (2) *residues*

*with indices congruent to* 0, 1, *or* 3 *modulo* 6 *for an appropriate choice*[2] *of primitive root when* $p$ *is of the form* $p=4x^2+27$. *The only possibilities are equivalent to one of the above.*

PROOF. We note that the second case always duplicates the parameters $v$, $k$, $\lambda$ of the first so that if there are infinitely many primes of the form $p=4x^2+27$, this yields infinitely many cases of parameters with two distinct difference sets belonging to them.

Modulo a prime $p=6f+1$ the sextic residues form a cyclic group under multiplication. If $t$ is a generator of this group then since $(t-1, p)=1$ there is an equivalent difference set fixed by the multiplier $t$ and hence by all sextic residues. This set will consist of all residues whose indices are congruent to specified values modulo 6 and may also include in addition the residue 0. If $p\equiv 1 \pmod{12}$ then $-1$ is a sextic residue. In this case since $d_i-d_j\equiv(-d_j)-(-d_i)$, a residue modulo $p$ not of the form $2d_i$ will be given an even number of times as a difference and one of the form $2d_i$ an odd number of times. Hence we may assume $p\equiv 7 \pmod{12}$. For such primes the cyclotomic numbers $(i, j)$ are the number of solutions $x\equiv g^{6u+i}$, $y\equiv g^{6v+j} \pmod{p}$ of

$$g^{6u+i}+1\equiv g^{6v+j} \pmod{p} \tag{2.28}$$

where $g$ is a fixed primitive root of $p$. Following the methods of Dickson [3] Emma Lehmer found the values to depend on the quadratic representations

$$p=A^2+3B^2, \qquad 4p=L^2+27M^2=E^2+3F^2. \tag{2.29}$$

The numbers satisfy the relations

$$(i, j)=(j+3, i+3)=(6-i, j-i). \tag{2.30}$$

Thus with $i, j=0, \cdots, 5 \pmod{6}$ we have the following table expressing the 36 constants in terms of ten where $(i, j)$ is in row $i$ and column $j$.

$$\begin{array}{cccccc} 00 & 01 & 02 & 03 & 04 & 05 \\ 10 & 20 & 12 & 04 & 02 & 12 \\ 20 & 21 & 10 & 05 & 12 & 01 \\ 00 & 10 & 20 & 00 & 10 & 20 \\ 10 & 05 & 12 & 01 & 20 & 21 \\ 20 & 12 & 04 & 02 & 12 & 10 \end{array} \tag{2.31}$$

[2] This will be a choice which puts the residue 3 in the class with indices congruent to 1 modulo 6.

The values will depend on the cubic character of 2.

(2.32)

| | 2 cubic residue<br>$L=2A$,<br>$E=2A$,<br>$F=-2B$,<br>$3M=2B$ | Ind $2\equiv 2 \pmod 3$<br>$3B=E+A$,<br>$F=A+B$,<br>$L=A+3B$,<br>$3M=A-B$ | Ind $2\equiv 1 \pmod 3$<br>$3B=-(E+A)$,<br>$F=-A+B$,<br>$L=A-3B$,<br>$3M=-(A+B)$ |
|---|---|---|---|
| 36 (00) | $p-11-8A$ | $p-11-2A$ | $p-11-2A$ |
| 36 (01) | $p+1-2A+12B$ | $p+1-2A-12B$ | $p+1+4A$ |
| 36 (02) | $p+1-2A+12B$ | $p+1-8A+12B$ | $p+1-2A+12B$ |
| 36 (03) | $p+1+16A$ | $p+1+10A+12B$ | $p+1+10A-12B$ |
| 36 (04) | $p+1-2A-12B$ | $p+1-2A-12B$ | $p+1-8A-12B$ |
| 36 (05) | $p+1-2A-12B$ | $p+1+4A$ | $p+1-2A+12B$ |
| 36 (10) | $p-5+4A+6B$ | $p-5+4A+6B$ | $p-5-2A+6B$ |
| 36 (20) | $p-5+4A-6B$ | $p-5-2A-6B$ | $p-5+4A-6B$ |
| 36 (12) | $p+1-2A$ | $p+1+4A$ | $p+1+4A$ |
| 36 (21) | $p+1-2A$ | $p+1-8A+12B$ | $p+1-8A-12B$ |

From (2.28) we see that $(i, j)$ is the number of solutions of

$$y - x \equiv 1 \pmod p \tag{2.33}$$

with $y$ in class $j$ and $x$ in class $i$. Multiplying by $d$ in class $s$ we have

$$y_1 - x_1 \equiv d \pmod p \tag{2.34}$$

with $y_1$ in class $j+s$ and $x_1$ in class $i+s$. Thus

$$y - x \equiv d \pmod p \tag{2.35}$$

has for a fixed $d$ in class $s$ $(i-s, j-s)$ solutions with $y$ in class $j$ and $x$ in class $i$. This enables us to tell how often each difference arises from sets composed of classes of given sextic character. With a set whose characters are 0, 1, 3 we find that for $y-x\equiv d \pmod p$ with $d$ in class $s$ the number of solutions is

$$\begin{aligned} N_s = {} & (-s, -s) + (1-s, -s) + (-s, 1-s) + (1-s, 1-s) \\ & + (-s, 3-s) + (3-s, -s) + (1-s, 3-s) \\ & + (3-s, 1-s) + (3-s, 3-s). \end{aligned} \tag{2.36}$$

The values for $s=3, 4, 5$ will repeat those for $s=0, 1, 2$. Using (2.31) and (2.32) we find in the three cases.

First: 2 is a cubic residue

$$\begin{array}{ll} & N_s \\ s=0 & (9p-45+6B)/36 \\ s=1 & (9p-27)/36 \\ s=2 & (9p-9-6B)/36. \end{array} \tag{2.37}$$

Second: Ind $2 \equiv 2 \pmod 3$

$$\begin{aligned} s &= 0 \quad (9p - 45 + 6A - 6B)/36 \\ s &= 1 \quad (9p - 27 - 6A - 12B)/36 \\ s &= 2 \quad (9p - 9 + 18B)/36. \end{aligned} \tag{2.38}$$

Third: Ind $2 \equiv 1 \pmod 3$

$$\begin{aligned} s &= 0 \quad (9p - 45 - 18B)/36 \\ s &= 1 \quad (9p - 27 - 6A + 12B)/36 \\ s &= 2 \quad (9p - 9 + 6A + 6B)/36. \end{aligned} \tag{2.39}$$

For the first case the three values will be equal when $B=3$. For the second case we need $A=2$, $B=-1$ which gives $p=7$. For the third we must have $A=-2$, $B=-1$ which again gives $p=7$. Modulo 7 the residues 1, 5, 6 satisfy these requirements but these are equivalent to the quadratic residues 1, 2, 4.

In the first case with $B=3$ we have $p=A^2+27$, and $A$ must be even $A=2x$ and so $p=4x^2+27$. For such a prime 2 is a cubic residue and also $p \equiv 7 \pmod{12}$ and (2.31) and (2.32) apply. If $B=-3$ classes 0, 5, 3 form a difference set, but this differs from the previous case only in the choice of primitive root. Since the cubic class of the residue 3 is given by $M \pmod 3$ and since 3 is a quadratic nonresidue of $p$, in either case the difference set will consist of cubic residues and the sextic class including 3.

The remaining combinations of sextic classes when calculated as above fail to yield difference sets.

3. **Known difference sets.** With $k<v/2$, and in the range $3 \leqq k \leqq 50$, there are 268 choices of $v$, $k$, $\lambda$ satisfying

$$k(k-1) = \lambda(v-1). \tag{3.1}$$

Of these choices 101 do not satisfy the conditions of Chowla and Ryser [2] which are:

(3.2.1) If $v$ is even, $n=k-\lambda$ is a square.

(3.2.2) If $v$ is odd, $z^2=nx^2+(-1)(v-1)/2y^2$ has integer solutions $x$, $y$, $z$ not all zero. Of the remaining 167 choices, difference sets have been found in 46 cases. Of these 46 cases, in three there are two nonisomorphic solutions and in one case, $v=121$, $k=40$, $\lambda=13$, there are four nonisomorphic solutions. In 109 cases it has been established that no difference set exists, and in 12 cases it remains undecided whether or not one exists.

In all known difference sets every divisor of $n=k-\lambda$ is a multiplier.

Emma Lehmer [6] has shown that this is true for the residue difference sets and for those given by Theorem 2.2 above. When every divisor of $n$ is also a divisor of $v$, there are no logical candidates for multipliers. But by the methods of Theorem 2.1 we can sometimes find a multiplier modulo some divisor of $v$. Thus for $v=177$, $k=33$, $\lambda=6$ we have $n=27$ and find that 3 is a multiplier modulo 59. From this it readily follows that no difference set exists. The 12 undecided cases are given by the following parameters:

(3.3)

| $v$ | $k$ | $\lambda$ | $n$ |
|---|---|---|---|
| 45 | 12 | 3 | 9 |
| 36 | 15 | 6 | 9 |
| 96 | 20 | 4 | 16 |
| 64 | 28 | 12 | 16 |
| 175 | 30 | 5 | 25 |
| 171 | 35 | 7 | 28 |
| 120 | 35 | 10 | 25 |
| 288 | 42 | 6 | 36 |
| 100 | 45 | 20 | 25 |
| 208 | 46 | 10 | 36 |
| 189 | 48 | 12 | 36 |
| 176 | 50 | 14 | 36 |

In the range surveyed there are exactly two instances in which Theorem 2.2 applies. These difference sets are

$$v = 31, \quad k = 15, \quad \lambda = 7, \quad n = 8,$$

1, 2, 3, 4, 6, 8, 12, 15, 16, 17, 23, 24, 27, 29, 30 (mod 31)

$$v = 43, \quad k = 21, \quad \lambda = 10, \quad n = 11,$$

1, 2, 3, 4, 5, 8, 11, 12, 16, 19, 20, 21, 22, 27, 32, 33, 35, 37, 39, 41, 42 (mod 43).

For these parameters the quadratic residues in each case yield the only other solution.

Further classes of difference sets are given by certain residues modulo $p$. These were treated by Emma Lehmer [5] and include

(1) Quadratic residues of primes $p \equiv 3 \pmod 4$ when we will have $v=p=4t-1$, $k=2t-1$, $\lambda=t-1$. In this search the values of $v$ covered were 7, 11, 19, 23, 31, 43, 59, 67, 71, 79, 83 and these were the unique

solutions for the parameters except for $v=31$ and 43 which had also the solutions above as cases of Theorem 2.2.

(2) Biquadratic residues of primes $p=4x^2+1$, $x$ odd. Here $v=p=4x^2+1$, $k=x^2$, $\lambda=(x^2-1)/4$. $v=37$, 101, 197 were covered in this search, and solutions for these parameters were unique.

(3) Biquadratic residues and zero for primes $p=4x^2+9$, $x$ odd. Here $v=4x^2+9$, $k=x^2+3$, $\lambda=(x^2+3)/4$. Here $v=13$ and 109 were included and gave unique solutions for the parameters.

(4) Octic residues of primes $p=8a^2+1=64b^2+9$, with $a$, $b$ odd. Here $v=p$, $k=a^2$, $\lambda=b^2$. The only case arising was $v=73$, $k=9$, $\lambda=1$ and the solution was unique for these parameters.

(5) Octic residues and zero for primes $p=8a^2+49=64b^2+441$, $a$ odd, $b$ even. Here $v=p$, $k=a^2+6$, $\lambda=b^2+7$. No cases arose in the range studied.

By the results of Singer [9], finite Desarguesian projective geometries have collineations which are cyclic on the points and hyperplanes. The points of a hyperplane will form a difference set. We will have for an $s$-dimensional space $v=(t^{s+1}-1)/(t-1)$, $k=(t^s-1)/(t-1)$, $\lambda=(t^{s-1}-1)/(t-1)$. When $s=2$ a solution will yield a plane and whenever $t=p^r$ a prime power there is certainly the Desarguesian plane with coordinates from the field with $p^r$ elements. There are conceivably non-Desarguesian cyclic planes but so far none has been found [4; 7; 8]. Here with $n=t=2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 25, 27, 32$ the solution is unique and so of course Desarguesian.

For $s>3$ if the solution is a geometry then the geometry is surely Desarguesian but some solutions were found for the above parameters which are not geometries. The survey covered the following:

PLANES IN 3 SPACES. Solutions unique $v=15$, $k=7$, $\lambda=3$.

0, 1, 2, 4, 5, 8, 10 (mod 15).

$$v = 40, \qquad k = 13, \qquad \lambda = 4,$$

1, 2, 3, 5, 6, 9, 14, 15, 18, 20, 25, 27, 35 (mod 40).

$$v = 85, \qquad k = 21, \qquad \lambda = 5,$$

0, 1, 2, 4, 7, 8, 14, 16, 17, 23, 27, 28, 32, 34, 43, 46, 51, 54, 56, 64, 68 (mod 85).

$$v = 156, \qquad k = 31, \qquad \lambda = 6,$$

0, 1, 5, 11, 13, 25, 28, 39, 46, 55, 58, 65, 68, 74, 76, 86, 87, 91, 111, 117, 118, 119, 122, 123, 125, 127, 134, 140, 142, 143, 147 (mod 156).

3 spaces in 4 spaces.

$$v = 31, \qquad k = 15, \qquad \lambda = 7.$$

We have already noted the only two solutions for these parameters. The geometry is given by the example above arising from Theorem 2.2. The quadratic residues do not yield the geometry. This is easily seen since if $r_i$ are the quadratic residues modulo 31 the sets $\{r_i\}$, $\{r_i+1\}$, $\{r_i+3\}$ intersect in the four values 5, 8, 10, 19, while in the geometry there is no subspace with exactly 4 points. This shows incidentally that not only are the difference sets nonisomorphic but that the designs which they define are nonisomorphic.

$$v = 121, \qquad k = 40, \qquad \lambda = 13$$

(1) 1, 3, 4, 7, 9, 11, 12, 13, 21, 25, 27, 33, 34, 36, 39, 44, 55, 63, 64, 67, 68, 70, 71, 75, 80, 81, 82, 83, 85, 89, 92, 99, 102, 103, 104, 108, 109, 115, 117, 119.

There are however three further solutions which are not geometries.

(2) 1, 3, 4, 5, 9, 12, 13, 14, 15, 16, 17, 22, 23, 27, 32, 34, 36, 39, 42, 45, 46, 48, 51, 64, 66, 69, 71, 77, 81, 82, 85, 86, 88, 92, 96, 102, 108, 109, 110, 117.

(3) 1, 3, 4, 7, 8, 9, 12, 21, 24, 25, 26, 27, 34, 36, 40, 43, 49, 63, 64, 68, 70, 71, 72, 75, 78, 81, 82, 83, 89, 92, 94, 95, 97, 102, 104, 108, 112, 113, 118, 120.

(4) 1, 3, 4, 5, 7, 9, 12, 14, 15, 17, 21, 27, 32, 36, 38, 42, 45, 46, 51, 53, 58, 63, 67, 68, 76, 79, 80, 81, 82, 83, 96, 100, 103, 106, 107, 108, 114, 115, 116, 119.

These are all the difference sets with these parameters.

4 spaces in 5 spaces

$$k = t^4 + t^3 + t^2 + t + 1, \qquad \lambda = t^3 + t^2 + t + 1,$$
$$v = t^5 + t^4 + t^3 + t^2 + t + 1.$$
$$k = 31, \qquad \lambda = 15, \qquad v = 63$$

There are two solutions.

The geometry:

(1) 0, 1, 2, 3, 4, 6, 7, 8, 9, 12, 13, 14, 16, 18, 19, 24, 26, 27, 28, 32, 33, 35, 35, 38, 41, 45, 48, 49, 52, 54, 56 (mod 63).

A second solution:

(2) 0, 1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 16, 17, 18, 20, 23, 24, 27, 29, 32, 33, 34, 36, 40, 43, 45, 46, 48, 53, 54, 58 (mod 63).

The author has found only two instances of difference sets which do not have parameters belonging to the categories listed. The first is:

$$k = 17, \qquad \lambda = 8, \qquad v = 35$$

0, 1, 3, 4, 7, 9, 11, 12, 13, 14, 16, 17, 21, 27, 28, 29, 33 (mod 35).

This belongs to the general category of Hadamard designs with parameters $v = 4m - 1$, $k = 2m - 1$, $\lambda = m - 1$, as do those of the second and seventh classes. The other difference set found still defies classification:

$$k = 33, \qquad \lambda = 8, \qquad v = 133$$

1, 4, 5, 14, 16, 19, 20, 21, 25, 38, 54, 56, 57, 64, 66, 70, 76, 80, 83, 84, 91, 93, 95, 98, 100, 101, 105, 106, 114, 123, 125, 126, 131 (mod 133).

## BIBLIOGRAPHY

1. R. H. Bruck, *Difference sets in a finite group*, Trans. Amer. Math. Soc. vol. 78 (1955) pp. 464–481.

2. S. Chowla and H. J. Ryser, *Combinatorial problems*, Canadian Journal of Mathematics vol. 2 (1950) pp. 93–99.

3. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. vol. 57 (1935) pp. 391–424.

4. Marshall Hall and H. J. Ryser, *Cyclic incidence matrices*, Canadian Journal of Mathematics vol. 3 (1951) pp. 495–502.

5. Emma Lehmer, *On residue difference sets*, Canadian Journal of Mathematics vol. 5 (1953) pp. 425–432.

6. ———, *Period equations applied to difference sets*, Proc. Amer. Math. Soc. vol. 6 (1955) pp. 433–442.

7. H. B. Mann, *Some theorems on difference sets*, Canadian Journal of Mathematics vol. 4 (1952) pp. 222–226.

8. H. B. Mann and T. A. Evans, *On simple difference sets*, Sankhya, vol. 11 (1951) pp. 357–364.

9. James Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. vol. 43 (1938) pp. 377–385.

THE OHIO STATE UNIVERSITY