PERFECT DIFFERENCE SETS

by H. HALBERSTAM and R. R. LAXTON

(Received 12 August, 1963)

1. Introduction. If the set K of $r+1$ distinct integers $k_0, k_1, \ldots, k_r$ has the property that the $(r+1)r$ differences $k_i - k_j$ $(0 \leqq i, j \leqq r, i \neq j)$ are distinct modulo r^2+r+1, K is called *a perfect difference set mod* r^2+r+1. The existence of perfect difference sets seems intuitively improbable, at any rate for large r, but in 1938 J. Singer [1] proved that, whenever r is a prime power, say $r = p^n$, a perfect difference set mod $p^{2n}+p^n+1$ exists. Since the appearance of Singer's paper several authors have succeeded in showing that for many kinds of number r perfect difference sets mod r^2+r+1 do not exist; but it remains an open question whether perfect difference sets exist *only* when r is a prime power (for a comprehensive survey see [2]).

In this note we shall be concerned solely with perfect difference (p.d.) sets mod $p^{2n}+p^n+1$, where p is prime. From now on (except in §2), let r denote p^n and write

$$q = r^2+r+1 = p^{2n}+p^n+1. \tag{1.1}$$

We shall lose no generality by assuming that $r > 7$.

If K is a p.d. set mod q and $K+s$ denotes the set $k_0+s, k_1+s, \ldots k_r+s$ then clearly $K+s$ is also a p.d. set mod q; since K contains two elements whose difference is congruent to $1 \pmod q$, there exists a translation $K+s$ which takes these two elements into 0 and 1. A p.d. set containing 0 and 1 is said to be *reduced*, and two p.d. sets mod q which can be translated to the same reduced set are said to be *equivalent*.

Singer arrived at his p.d. sets in the following way. Let G_3 and G_1 denote respectively the Galois fields $GF(p^{3n})$ and $GF(p^n)$, so that G_3 is a cubic extension of G_1. If ζ is a generator of G_3^*, the multiplicative cyclic group associated with G_3, ζ satisfies a monic cubic equation over G_1 irreducible in G_1, and every element of G_3 can be written in the form

$$a + b\zeta + c\zeta^2, \quad a, b, c \in G_1;$$

moreover, every element of G_3 other than 0 can also be expressed as a power of ζ. Consider then all the elements of G_3 of the form

$$a + b\zeta = \zeta^k \tag{1.2}$$

as a, b run independently through G_1 but are not both 0. We say that two such numbers are equivalent if there exists a number $c \neq 0$ in G_1 such that one is c times the other. The equivalence relation induces a partition of all numbers of the form (1.2) into $r+1$ equivalence classes; for there are, in all, $p^{2n}-1$ numbers of form (1.2) corresponding to the $p^{2n}-1$ choices for the pair a, b, and on the other hand there are $r-1$ choices for c. Let

$$a_i + b_i\zeta = \zeta^{k_i} \quad (i = 0, 1, \ldots, r)$$

be a representative set chosen from these equivalence classes. Then the system K of exponents is a p.d. set mod q (a simple proof is given in [3]; see also [4]). A p.d. set constructed in this way will be called a *Singer p.d. set*, or a *p.d. set of Singer type.*

N

Singer proposed the following two conjectures:

I. All p.d. sets mod $p^{2n}+p^n+1$ are of Singer type.

II. There exist exactly $\phi(q)/(3n)$ reduced Singer p.d. sets.

The chief aim of the present paper is to prove II (see Theorem 2 below). It may be that the method evolved below will be of help in a successful attack on the much more difficult conjecture I.

The main step in the proof of II is Theorem 1 (see §3), and two proofs of this theorem have appeared recently. One proof is implicit in the results of Bruck [5] and Higman and McLaughlin [6]; the other is Theorem 5 of Gordon, Mills and Welch [7]. The proof given below is different from either of these, and appears to us more elementary in conception.

We are indebted to Dr M. C. R. Butler for a valuable suggestion.

2. The reduction lemma. We begin with a completely elementary result which will provide an essential step in the main argument below (see §3).

For the purpose of this section we may drop the restriction that r is a prime power.

We say that an integer is written *in standard form mod* r^2+r+1 when it is expressed modulo r^2+r+1 as

$$u+vr \quad \text{or} \quad u+r^2 \quad \text{or} \quad r+r^2 \tag{2.1}$$

with integers u, v satisfying

$$0 \leqq u < r, \quad 0 \leqq v < r. \tag{2.2}$$

We say that an integer t is of *reduced type mod* r^2+r+1 if

$$t \equiv u+vr \pmod{r^2+r+1},$$

where u, v satisfy (2.2) and also

$$0 < u+v \leqq r. \tag{2.3}$$

Then

LEMMA 1. *Let r be a fixed integer greater than* 1. *Then every integer t greater than* 1 *and coprime to r^2+r+1 has the property that t, tr or tr^2 is of reduced type mod r^2+r+1.*

Proof. If $t \equiv u+r^2 \pmod q$, $0 \leqq u < r$, then $tr \equiv ur+1 \pmod q$ and $0 < u+1 \leqq r$. If $t \equiv r+r^2$, then $tr^2 \equiv 1+r$ and $0 < 2 \leqq r$. Thus in the first case tr, and in the second tr^2, are of reduced type mod q.

It remains to consider the case $t \equiv u+vr \pmod q$, $0 \leqq u$, $v < r$ and

$$u+v > r. \tag{2.4}$$

From (2.4) $u+v \geqq r+1$, whence $u = 0, 1$ is impossible; hence $u \geqq 2$ and similarly $v \geqq 2$.

(i) Suppose that $u = v$. Then $t \equiv u(1+r) \equiv -ur^2$; therefore $tr \equiv -u \equiv (r-u)-r$ and $tr^2 \equiv (r-u)r-r^2 \equiv (r-u)r+1+r \equiv (r-u+1)r+1$. Hence $tr^2 \equiv u'+v'r \pmod q$, with $u' = 1$, $v' = r-u+1$, $0 \leqq u'$, $v' < r$ and $u'+v' = r-u+2 \leqq r$, since $u \geqq 2$. Therefore tr^2 is of reduced type.

(ii) Suppose that $u > v$. Then $u \geqq v+1$ and

$$tr \equiv ur+vr^2 \equiv (u-v)r-v = (u-v-1)r+(r-v) \equiv u'+v'r \pmod q,$$

with $u' = r-v$, $v' = u-v-1$ and $0 \leqq u'$, $v' < r$.

https://doi.org/10.1017/S2040618500034985 Published online by Cambridge University Press

If $u'+v' \leqq r$, then tr is of reduced type. If $u'+v' > r$, then $r+u-2v-1 > r$, that is, $u > 2v+1$. In this case

$$tr^2 \equiv ur^2+v \equiv (v-u)-ur \equiv (v-u)-ur+r^2+r+1 \equiv (r+v+1-u)+(r-u)r \equiv u''+v''r \pmod{q},$$

with $u'' = r+v+1-u$ and $v'' = r-u$. Since $u > 2v+1$, we have $0 < u''$, $v'' < r$. Now $u''+v'' = 2r+v+1-2u > r$ if and only if $r+1+v > 2u$. However, if $u > 2v+1$, then

$$2u > 2v+u+1 = (v+1)+(v+u) > v+1+r.$$

It follows that $u''+v'' \leqq r$ and hence tr^2 is of reduced type.

(iii) Suppose that $v > u$. Then $v \geqq u+1$ and

$$tr \equiv ur+vr^2 \equiv (u-v)r-v \equiv (u-v)r-v+r^2+r+1 \equiv (r-v+u)r+(r-v+1) \equiv u'+v'r \pmod{q},$$

with $u' = r-v+1$, $v' = r-v+u$, $0 \leqq u'$, $v' < r$ and $u'+v' = 2r-2v+u+1$.

If $u'+v' \leqq r$, then tr is of reduced type. If $u'+v' > r$, then $r+u+1 > 2v$. In this case,

$$tr^2 \equiv ur^2+v \equiv (v-u)-ur \equiv (v-u)-ur+r^2+r+1 \equiv (r-u+1)r+(v-u+1) \equiv u''+v''r \pmod{q},$$

with $u'' = v-u+1$, $v'' = r-u+1$, $0 \leqq u''$, $v'' < r$ and $u''+v'' = r+v-2u+2$.

If $u''+v'' \leqq r$, then tr^2 is of reduced type. There remains the case when both $u'+v' > r$ and $u''+v'' > r$, that is, when $r+u+1 > 2v$ and $v+2 > 2u$. The first inequality implies that $r+2u+1 \geqq 2v+u+1 = v+1+(v+u) > v+1+r$, i.e. $2u \geqq v+1$. This, together with the second inequality, shows that $2u = v+1$ is the only possibility. Now if $2u = v+1$ and

$$r+u+1 > 2v = 4u-2,$$

then $r+3 > 3u$. Also $3u = u+v+1 > r+1$ and so we are left with the one case $3u = r+2$ to consider. But then $3v = 6u-3 = 2r+4-3 = 2r+1$ and therefore

$$3t \equiv 3u+3vr \equiv (r+2)+(2r+1)r = 2(r^2+r+1) \equiv 0 \pmod{q};$$

whence $(t, q) > 1$.

3. Multipliers. We need to introduce the notion of a multiplier of a p.d. set (see [**2**]). Let tK denote the set of integers $tk_0, tk_1, \ldots, tk_r$. If $(t, q) = 1$, it is evident that tK is also a p.d. set; we say that t is a *multiplier* of K if K and tK are equivalent. Clearly, if t_1 and t_2 are multipliers, then so is $t_1 t_2$. Singer himself showed in [**1**] that if t is congruent mod q to a power of p, t is a multiplier of any p.d. set of Singer type. (This also follows at once from Lemma 3 in §4.) The object in this section is to prove the converse (see Theorem 1 below).

We observe that t is a multiplier of K if and only if there exists an integer s such that tK and $K+s$ are identical modulo q, i.e. such that for every element k_i of K there exists an element k_j of K such that

$$tk_i \equiv k_j+s \pmod{q}.$$

Bearing in mind the construction of Singer p.d. sets described in §1, an equivalent necessary and sufficient condition for t to be a multiplier of the p.d. set of Singer type generated by ζ is:

https://doi.org/10.1017/S2040618500034985 Published online by Cambridge University Press

Condition C. *There exists an integer s with the following two properties: for every $a \in G_1$, there exist elements b, c of G_1 such that*

$$(a+\zeta)^t = \zeta^s(b+c\zeta); \tag{3.1}$$

also, there exist elements b_1, c_1 of G_1 such that $\zeta^{-s} = b_1 + c_1\zeta$.

We prove

Lemma 2. *Let $t > 1$ be an integer of reduced type mod q. Then t does not satisfy condition C unless t is congruent mod q to a power of p. In particular, t does not satisfy C if $t \equiv u+vr$ and $u+v=r$.*

Proof. We may clearly suppose without loss of generality that

$$1 < t < q.$$

Let†

$$F(x) = F(x,\zeta) = \prod_{a \in G_1}(x-\zeta-a) = x^r - x - (\zeta^r - \zeta).$$

Then we have, modulo $F(x)$, that

$$x^r \equiv x+\zeta^r-\zeta \quad \text{and} \quad x^{r^2} \equiv x+\zeta^{r^2}-\zeta. \tag{3.2}$$

Further, let

$$H(x) = H(x,\zeta) = \prod_{b,\, c \in G_1}(x-b\zeta^s-c\zeta^{s+1})$$

$$= x^{r^2} - x^r\zeta^{r(r-1)s} - (x^r - x\zeta^{(r-1)s})(\zeta^{r(s+1)} - \zeta^{rs+1})^{r-1},$$

so that

$$H(x^t) = x^{r^2t} - x^{rt}\zeta^{r(r-1)s} - (x^{rt} - x^t\zeta^{(r-1)s})(\zeta^{r(s+1)} - \zeta^{rs+1})^{r-1} \tag{3.3}$$

is the polynomial having as its zeros the tth roots of all the linear forms $\zeta^s b + \zeta^{s+1}c$. Then, by (3.1), t can satisfy the condition C for some s only if

$$H(x^t) \equiv 0 \pmod{F(x)}.$$

By (3.2) and (3.3) we have

$$H(x^t) \equiv (x+\zeta^{r^2}-\zeta)^t - A(x+\zeta^r-\zeta)^t + Bx^t \pmod{F(x)}, \tag{3.4}$$

where

$$A = \zeta^{r(r-1)s} + (\zeta^{r(s+1)} - \zeta^{rs+1})^{r-1} = \zeta^{r(r-1)s}(1+(\zeta^r-\zeta)^{r-1}), \tag{3.5}$$

so that $A \neq 0$, and

$$B = \zeta^{(r-1)s}(\zeta^{r(s+1)} - \zeta^{rs+1})^{r-1} = \zeta^{(r^2-1)s}(\zeta^r-\zeta)^{r-1}. \tag{3.6}$$

† In the calculations below we make repeated use of the facts that $(x+y)^p = x^p + y^p$ for $x, y \in G_3$, and that $\prod_{a \in G_1}(y-a) = y^r - y$.

https://doi.org/10.1017/S2040618500034985 Published online by Cambridge University Press

Since t is of reduced type and $t < q$, we may substitute $u+vr$ for t in (3.4) and obtain, after applying (3.2),

$$0 \equiv H(x^t) = H(x^{u+vr})$$
$$\equiv (x+\zeta^{r^2}-\zeta)^u x^v - A(x+\zeta^r-\zeta)^u(x+\zeta^{r^2}-\zeta)^v + Bx^u(x+\zeta^r-\zeta)^v \pmod{F(x)}. \quad (3.7)$$

The polynomial on the right has degree less than or equal to $u+v$ and so less than or equal to r, and the degree of F is r. Accordingly, if $u+v = r$, this polynomial and F are essentially the same, and, if $u+v < r$, all the coefficients of the polynomial vanish. This is the situation which we now proceed to exploit. Since $1 < u+vr$ and $u+v \leqq r$, we have to consider the following three cases: (i) $u = 0$ or $v = 0$; (ii) $u > 0$, $v > 0$, $u+v < r$; (iii) $u > 0$, $v > 0$, $u+v = r$.

Case (i). The proof of the lemma in this case has been given in [**3**]. It can also be proved independently by the methods used below. To be precise, the main result of [**3**] is that if $t \equiv u$, $0 < u < r$, then t cannot satisfy C unless it is congruent mod q to a power of p; and this result also settles the case $t \equiv vr$, $0 < v < r$.

Case (ii). Since both u and v are positive and $u+v < r$, the constant term in the polynomial on the right of (3.7) must vanish, that is, $A(\zeta^r-\zeta)^u(\zeta^{r^2}-\zeta)^v = 0$. Since none of A, $\zeta^r-\zeta$ and $\zeta^{r^2}-\zeta$ is 0, this is impossible. Hence t cannot, in this case, satisfy condition C.

Case (iii). Here both u and v are positive and $u+v = r$. If the coefficient of x^{u+v} $(= x^r)$ is zero, we refer back to case (ii). If the coefficient of x^r is non-zero, the polynomial on the right of (3.7) must be a constant multiple of F, and the ratios of the pairs of corresponding coefficients are equal. Since $r > 7$ (by hypothesis—see §1) at least one of u, v exceeds 2; suppose first that both do. Equating the ratios of the coefficients of x and the constant term, we obtain

$$\frac{1}{a_1} = \frac{v}{a_2} + \frac{u}{a_1},$$

where $a_1 = \zeta^r - \zeta$ and $a_2 = \zeta^{r^2} - \zeta$. It follows that

$$a_1 = a_2^r \quad \text{and} \quad va_2^{(r-1)} = (u-1). \quad (3.8)$$

Since $a_2 \neq 0$, $u \equiv 1 \pmod p$ if and only if $v \equiv 0 \pmod p$, and $u+v \equiv 1 \pmod p$ contradicts $u+v = r$. Hence $u \not\equiv 1 \pmod p$, $v \not\equiv 0 \pmod p$ and $p \neq 2$.

We consider the coefficient of x^2 in (3.7). The coefficient is zero in F since $r > 7$; and since $u \geqq 3$, $v \geqq 3$, $a_1 \neq 0$, $a_2 \neq 0$, $p \neq 2$, we have

$$a_2^2 u(u-1) + 2a_1 a_2 uv + a_1^2 v(v-1) = 0.$$

Applying (3.8), we see that this reduces to $a_2^{2(r-1)} v(v-1) = u(u-1)$, and a second application of (3.8) gives $(u-1)((u-1)(v-1)-uv) = 0$. But $u \not\equiv 1 \pmod p$; hence

$$0 \equiv (v-1)(u-1) - uv = uv - u - v + 1 - uv = -(u+v-1) \pmod p.$$

Since $u+v = r \equiv 0 \pmod p$, we have arrived at a contradiction.

It remains to consider the special possibilities

$$u = 1, v = r-1; \; u = 2, v = r-2; \; u = r-1, v = 1 \quad \text{and} \quad u = r-2, v = 2.$$

If $u+vr$ is a multiplier, then so is $r(u+vr)$. In the first case

$$r(u+vr) = r(1+(r-1)r) = r^3-r^2+r \equiv 2+2r \pmod q,$$

and in the second

$$r(u+vr) = r(2+(r-2)r) = r^3-2r^2+2r \equiv 3+4r \pmod q.$$

But from case (ii) above, neither $2+2r$ nor $3+4r$ is a multiplier (we recall that $r > 7$) and so the same can be said of $1+(r-1)r$ and $2+(r-2)r$. If $u+vr$ is a multiplier, then so is $r^2(u+vr)$. In the third case

$$r^2(u+vr) = r^2((r-1)+r) = 2r^3-r^2 \equiv 2-r^2 \equiv 3+r \pmod q,$$

and in the fourth case

$$r^2(u+vr) = r^2((r-2)+2r) = 3r^3-2r^2 \equiv 3-2r^2 \equiv 5+2r \pmod q.$$

Again, by case (ii), neither $3+r$ nor $5+2r$ is a multiplier if $r > 7$ and so the same can be said of $(r-1)+r$ and $(r-2)+2r$.

Hence t cannot, in case (iii), satisfy condition C. Thus, to sum up, t can satisfy C only in case (i), and then only when one of u, v is zero and the other is a power of p. The proof of the lemma is thus complete.

We are now in a position to prove

THEOREM 1. *The only multipliers of perfect difference sets mod q of Singer type are the powers of p (mod q).*

Proof. It suffices to prove that if t is a multiplier of a p.d. set of Singer type, then t is congruent mod q to a power of p. By Lemma 2 this is certainly true if t is of reduced type mod q. Moreover, if t is a multiplier, so is each of tr, tr^2; and by Lemma 1, if t is not of reduced type, then at least one of these two must be. The theorem follows at once on appealing again to Lemma 2.

4. Proof of conjecture II. It remains to prove our main result and, incidentally, to establish another conjecture given in [**1**], namely, that any two Singer p.d. sets (mod q) are *connected*, i.e. that if K_1, K_2 are two such sets, there exists an integer t such that K_1 and tK_2 are equivalent. We require

LEMMA 3. *Given a generator ζ of G_3^*, then, for any integer t coprime with q, there exists an integer s such that, for every pair $a, b \in G_1$, there exists a pair $c, d \in G_1$ such that*

$$a+b\zeta^t = \zeta^s(c+d\zeta). \tag{4.1}$$

Proof. Let

$$\zeta^m = \alpha_m\zeta^2+\beta_m\zeta+\gamma_m, \quad \alpha_m, \beta_m, \gamma_m \in G_1 \quad (m = 1, 2, \ldots),$$

and write α, β, γ for α_3, β_3, γ_3 respectively, so that $\zeta^3-\alpha\zeta^2-\beta\zeta-\gamma = 0$ is the irreducible cubic satisfied by ζ (see introduction). The α's, β's and γ's satisfy the following recurrence relations

$$\alpha_{m+1} = \alpha\alpha_m+\beta_m, \quad \beta_{m+1} = \beta\alpha_m+\gamma_m, \quad \gamma_{m+1} = \gamma\alpha_m.$$

We write (4.1) in the form

$$a+b(\alpha_t\zeta^2+\beta_t\zeta+\gamma_t) = c(\alpha_s\zeta^2+\beta_s\zeta+\gamma_s)+d(\alpha_{s+1}\zeta^2+\beta_{s+1}\zeta+\gamma_{s+1}),$$

and note that this relation is equivalent to the three simultaneous equations

$$\begin{aligned} b\alpha_t &= c\alpha_s+d\alpha_{s+1}, \\ b\beta_t &= c\beta_s+d\beta_{s+1}, \\ a+b\gamma_t &= c\gamma_s+d\gamma_{s+1}. \end{aligned}$$

For given a, b, these equations are soluble if and only if

$$\begin{vmatrix} \alpha_s & \alpha_{s+1} & b\alpha_t \\ \beta_s & \beta_{s+1} & b\beta_t \\ \gamma_s & \gamma_{s+1} & b\gamma_t+a \end{vmatrix} = 0,$$

and if a, b now vary over G_1, this is true only if

$$\begin{vmatrix} \alpha_s & \alpha_{s+1} & \alpha_t \\ \beta_s & \beta_{s+1} & \beta_t \\ \gamma_s & \gamma_{s+1} & \gamma_t \end{vmatrix} = 0 \quad \text{and} \quad \alpha_s\beta_{s+1}-\alpha_{s+1}\beta_s = 0;$$

and it is easy to check that these two relations determine ζ^s uniquely to within a factor from G_1.

LEMMA 4.† *If K is a Singer p.d. set mod q, and $(t, q) = 1$, then tK is also a Singer p.d. set mod q.*

Proof. Suppose that K is generated by ξ, a generator of G_3^*, so that

$$a+b\xi = \xi^k \quad (k \in K), \tag{4.2}$$

for any pair $a, b \in G_1 ((a, b) \neq (0, 0))$. Now solve $\zeta^t = \xi$ for ζ, giving another generator of G_3^*. (There is no loss in generality in assuming that $(t, r^3-1) = 1$, for $(t, q) = 1$ and so $(t+mq, r-1) = 1$ for some positive integer m (by Dirichlet's theorem on primes in an arithmetic progression), so that we use $t+mq$ in place of t if $(t, r-1) > 1$.) Then (4.2) now reads

$$a+b\zeta^t = \zeta^{tk} \quad (k \in K),$$

and by Lemma 3 it follows that there exists s such that, for given $a, b \in G_1$, there exist $c, d \in G_1$ such that $a+b\zeta^t = \zeta^s(c+d\zeta)$, i.e. we have

$$\zeta^{tk} = \zeta^s(c+d\zeta).$$

But, on varying c, d over G_1, this means that $tK-s$ is the p.d. set generated by ζ, i.e. tK is a p.d. set of Singer type.

We mention in passing that Lemma 3 also implies the result to which we referred earlier, namely that every number congruent mod q to a power of p is a multiplier of Singer p.d. sets mod q. To see this we have only to note that if $t \equiv p^m \pmod q$, (3.1) of condition C reads

† This result is proved in [4] using the theory of projective planes.

$$a'+\zeta^t = \zeta^s(b+c\zeta),$$

the relation discussed in Lemma 3.

Let K denote a fixed Singer p.d. set mod q, and let t run through a reduced set of residues mod q, thereby giving rise to $\phi(q)$ p.d. sets tK, each of Singer type by Lemma 4. By Theorem 1, these $\phi(q)$ sets fall into $\phi(q)/3n$ non-overlapping classes, with t_1K, t_2K belonging to the same class if and only if $t_1 \equiv p^m t_2 \pmod q$ for some m; two of these sets are equivalent or not according as they belong to the same or to different classes. Hence it follows that there exist *at least* $\phi(q)/3n$ non-equivalent p.d. sets mod q of Singer type.

In the opposite direction, any Singer p.d. set mod q is generated by some generator ζ of G_3^*, and there exist in all $\phi(p^{3n}-1)$ distinct generators of G_3^* which can be written as ζ^t with t running through a reduced set of residues mod $(p^{3n}-1)$. However, if ζ^{t_1} and ζ^{t_2} are generators of G_3^* with $t_1 \equiv t_2 \pmod q$, ζ^{t_1} and ζ^{t_2} evidently give rise to the same p.d. set; hence we need concern ourselves only with $\phi(q)$ generators ζ^t, any two having exponents non-equivalent mod q. However, if ζ^{t_1} and ζ^{t_2} are two of these generators and $t_1 \equiv t_2 p^m \pmod q$, then ζ^{t_1} and ζ^{t_2} generate equivalent p.d. sets; for if $a+b\zeta^{t_1} = \zeta^{t_1 k}$,

$$\zeta^{t_1 k} = a+b'\zeta^{t_2 p^m} = (a''+b''\zeta^{t_2})^{p^m} = (\zeta^{t_2 l})^{p^m},$$

where l runs through the p.d. set generated by ζ^{t_2}, and so $\zeta^{t_1 k} = \zeta^{t_1 l+dq}$—in other words, $\{k\}$ and $\{l\}$ are equivalent sets. Hence there exist *at most* $\phi(q)/3n$ non-equivalent Singer p.d. sets mod q. It follows from the previous paragraph that there exist *precisely* $\phi(q)/3n$ non-equivalent Singer p.d. sets mod q and that any two of these are connected. We have proved

THEOREM 2. *There exist precisely* $\phi(q)/3n$ *reduced Singer p.d. sets mod q, any two of which are connected. Two generators* ζ *and* ζ^t *of* $GF^*(p^{3n})$ *give rise to equivalent p.d. sets if and only if t is congruent mod q to a power of p.*

We remark in conclusion that the reduction lemma (Lemma 1) is relevant to the study of multipliers of p.d. sets mod r^2+r+1 even when r is not a prime power; in testing whether or not a given t is a multiplier, we know that tr or tr^2 possesses the same multiplier properties as t and one of t, tr, tr^2 is of reduced type mod r^2+r+1.

REFERENCES

1. J. Singer, A theorem of finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938), 377–385.

2. M. Hall, Jr, A survey of difference sets, *Proc. Amer. Math. Soc.* **7** (1956), 975–986.

3. H. Halberstam and R. R. Laxton, On perfect difference sets, *Quart. J. Oxford Ser.* (2) **14** (1963), 86–90.

4. G. Berman, Finite projective plane geometries and difference sets, *Trans. Amer. Math. Soc.* **74** (1953), 492–499.

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

6. D. G. Higman and J. E. McLaughlin, Geometric *ABA*-groups, *Illinois J. Math.* **5** (1961), 382–397.

7. B. Gordon, W. H. Mills and L. R. Welch, Some new difference sets, *Canad. J. Math.* **14** (1962), 614–625.

TRINITY COLLEGE, DUBLIN
UNIVERSITY OF MICHIGAN and UNIVERSITY OF SUSSEX

https://doi.org/10.1017/S2040618500034985 Published online by Cambridge University Press