THE NONEXISTENCE OF SEVEN DIFFERENCE SETS[1]

BY
RICHARD TURYN

In a recent paper [2] Mann considered the existence of difference sets in elementary abelian groups. The only known difference sets in such groups are the squares in $GF(q)$, $q \equiv -1 \pmod 4$, and some difference sets for which $v = 4^s$, $n = 4^{s-1}$. In [2], Mann showed that no others exist for other values of $v < 2500$ with the possible exception of nine sets of values of (v, k, λ) unless the group is cyclic. It is shown here that no such sets exist for seven of these sets of values of (v, k, λ). Of particular interest in the second set ($v = 121$, $n = 27$) in that there exist four nonisomorphic cyclic difference sets with these parameters [1]. This is unlike the case in which $(n, v) > 1$, where a difference set is more likely to exist if the group has no characters of relatively large order: for $v = 16$, $n = 4$, there is a difference set in every abelian group except the cyclic one, and for $v = 36$, $n = 9$, there is a difference set in the two abelian groups with no characters of order 9. The method here is that of [3]: The possible values of the character sums are first determined, and used to determine the structure (here nonexistence) of the difference set. Here these are the integers of absolute value $\sqrt{n}$ in the field of p^{th} roots of 1, $v = p^m$.

We use the notations of [2] and [3]. G denotes the elementary abelian group of order v, D the difference set whose existence is disproved. If $g \in G$, $y_g = 1$ if $g \in D$, $y_g = 0$ if $g \notin D$. If χ is a nonprincipal character, $\chi(D) = \sum_D \chi(g) = \sum_G y_g \chi(g)$; if ζ is a fixed p^{th} root of 1, Y_i is the number of elements g in D such that $\chi(g) = \zeta^i$. $\hat{G}$, the character group of G is also an elementary abelian group; if χ is a nonprincipal character of G, we refer to the set of $\{\chi^i\}$, $i \not\equiv 0$ as a line of $\hat{G}$.

We recall the inversion formula

$$y_g = \frac{1}{v} \sum_{\chi} \chi(D)\bar{\chi}(g) \tag{1}$$

$$= \frac{1}{p^m}\left(k + \sum_j \sum_{i=1}^{p-1} \chi_j^i(D)\chi_j^{-i}(g)\right) \tag{2}$$

where in (2) $v = p^m$ and χ_j runs over a set of representatives of the lines of $\hat{G}$ (G is elementary abelian). We also recall that if σ is a multiplier of D, an automorphism σ such that $\sigma(D) = D + a$, then D may be replaced by a translate D' such that $\sigma D' = D'$. We also note that in (2) $\sum_1^{p-1} \chi^i(D)\chi^{-i}(g)$ is the trace of the algebraic integer $\chi(D)\bar{\chi}(g)$ from $Q(\zeta)$ to Q. w denotes an arbitrary root of 1 ($w = \pm\zeta^a$).

Received April 3, 1964.

[1] This paper was partially supported by a contract with the Air Force Cambridge Research Laboratory.

I. *There is no difference set with* $v = 3^4$, $k = 16$, $n = 13$.

Proof. In $Q(\omega)$ $(\omega^2 + \omega + 1 = 0)$, $13 = (4 + \omega)(4 + \omega^2)$ and therefore each character sum $= (4 + \omega)w$ or $(4 + \omega^2)w$, $16 \equiv -5 \pmod 3$ implies $w = -\omega^a$; if χ is any nonprincipal character Y_0, Y_1, Y_2 must be 3, 6, 7 in some order (whether $(\chi(D)) = (4 + \omega)$ or $(4 + \omega^2)$); i.e., the number of elements of D in any three parallel hyperplanes is 3, 6, 7.

The following argument is due to A. Gleason: translating D if necessary, we may assume $0 \in D$ and that 0 belongs to a hyperplane which contains only three points of D. These three points belong to a two-dimensional subspace. There are four hyperplanes which contain this two-dimensional subspace, one of which contains no additional points of D. However, together the four hyperplanes contain 13 $(= 16 - 3)$ other points of D, so one of them will contain at least 5 additional points of D $(\frac{13}{3} > 4)$ and hence one hyperplane will contain at least 8 points of D, which is impossible.

II. *There is no difference set with* $v = 121$, $k = 40$, $n = 27$.

Proof. Let ζ be a primitive 11^{th} root of 1, $\eta = \sum \zeta^r$ (r denotes arbitrary quadratic residues mod 11). Then $3 = \eta\bar{\eta}$ and, for $\chi \neq \chi_0$, $\chi(D)$ or $\bar{\chi}(D)$ is $3\eta w$ or $\eta^3 w$, $w = \pm\zeta^a$. Then $\chi(D) = 3\eta w$ implies $\chi(D) = -3\eta\zeta^a$; $\chi(D) = \eta^3 w$ implies $\chi(D) = (2\eta - 3)\zeta^a$, since $\eta^2 + \eta + 3 = 0$, $\eta^3 = -2\eta + 3$.

We now compute $\sum_{i=1}^{10} \chi^i(D)$, the trace of χ, for $\chi \neq \chi_0$.

$\chi(D) =$	$\sum \chi^i(D) =$
-3η	$15\ (=5\cdot(-3)\cdot(-1))$
$-3\eta\zeta^{-r}$	-18
$-3\eta\zeta^{r}$	15
$2\eta - 3$	-40
$(2\eta - 3)\zeta^{-r}$	15
$(2\eta - 3)\zeta^{r}$	$-7.$

Since all the quadratic residues are multipliers of D, we may assume D translated so that it is invariant under all σ_r $(\sigma_r(g) = g^r)$. Then for each χ, $\chi(D)$ or $\bar{\chi}(D)$ must be $2\eta - 3$ or -3η, and $\sum \chi^i(D) = -40$ or 15. Let A be the number of lines in $\hat{G}$ in which there is a χ such that $\chi(D) = 2\eta - 3$. Then by (2)

$$121y_e = 40 + (-40)A + (12 - A)15.$$

Thus $55A = 220 - (0 \text{ or } 121)$, and $A = 4$. Now $k = 40$, $\chi(D) = 2\eta - 3$ (for any χ) implies $Y_0 = 0$, $Y_r = 5$, $Y_{-r} = 3$.

Let χ_∞, χ_{11} be two independent characters such that $\chi(D) = 2\eta - 3$. Express the group in terms of the dual basis. $\chi_\infty(a, b) = \zeta^b$, $\chi_{11}(a, b) = \zeta^a$, $a, b \bmod 11$. Let $\chi_j = \chi_{11}\chi_\infty^j$. Then $\chi_j(a, b) = \zeta^{a+jb}$.

$y_{r,0} = 0$ (since the number of g in D with $\chi_{00}(g) = 1$ is 0). Thus, by (2)

$$0 = 40 - 40 + 15 + (-7, 15) + (-7, 15) + 15A + (8 - A)(-18)$$

where $(-7, 15)$ means -7 or 15 and the terms correspond to χ_0, χ_∞, χ_{11}, the two characters with $\chi(D)$ or $\bar{\chi}(D) = 2\eta - 3$, and the others, successively. The two terms $(-7, 15)$ must be 15, and $A = 3$. Thus the two χ_j such that $\chi_j(D) = 2\eta - 3$ or $2\bar{\eta} - 3$ must be such that $\chi_j(D) = 2\eta - 3$.

Now $y_{0,r} = 0$. Using this for a similar computation, we conclude that the trace of $(2\eta - 3)\zeta^{-jr}$ must be 15 for these two characters, and thus both values of j are residues mod 11. By taking an automorphism of G of the form $\sigma(x, y) = (x, ry)$ and replacing D by σD, we may assume that $\chi_1(D) = 2\eta - 3$. $\chi_1(-a, a) = 1$; compute $y_{-r,r}$ which must again be 0.

$$0 = 40 - 40 - 7 + 15 + (-7, 15) + 15B + (8 - B)(-18),$$

the terms corresponding to χ_0, χ_1, χ_{11}, χ_∞, the other character such that $\chi(D) = 2\eta - 3$, and the others. But this equation has no integer solution for B.

III. *There is no difference set with* $v = 19^2$, $k = 136$, $n = 85$.

The proof is almost the same as the preceding. The integers of absolute value $\sqrt{85} = \sqrt{5.17}$ in the field of 19^{th} roots of 1 are $(3\eta - 5)w$ and $(4\eta + 5)w$, $\eta = \sum \zeta^r$. $\chi(D) = \pm(3\eta - 5)$, $k = 136$ implies the sign is $+$ and $Y_0 = 1$, $Y_r = 9$, $Y_{-r} = 6$. As before, we compute $\sum_1^{18} \chi^i(D)$ for $\chi \neq \chi_0$.

$\chi(D) =$	$\sum \chi^i(D) =$
$3\eta - 5$	-117
$(3\eta - 5)\zeta^r$	-22
$(3\eta - 5)\zeta^{-r}$	35
$4\eta + 5$	54
$(4\eta + 5)\zeta^r$	-41
$(4\eta + 5)\zeta^{-r}$	35.

Assume D is fixed by all the σ_r. Now each $\chi(D)$, $\chi \neq \chi_0$, must be $3\eta - 5$ or $4\eta + 5$. By (2)

$$19^2 y_e = (136 - 117A + 54(20 - A))$$

or

$$171A = 1216 - (0, 19^2).$$

Thus $y_e = 1$, $A = 5$. There are five independent characters such that $\chi(D)$ or $\chi^{-1}(D) = 3\eta - 5$. We pick two independent ones for which $\chi(D) = 3\eta - 5$ and express the group in terms of the dual basis. Since $y_e = 1$ and $Y_0 = 1$ for each of these five independent characters, there are no elements g of D other than e for which $\chi(g) = 1$ for χ any one of these five characters.

As before, let $\chi_{19}(a, b) = \zeta^a$, $\chi_\infty(a, b) = \zeta^b$, $\chi_j(a, b) = \zeta^{a+bj}$. Since

$$19^2 y_{a,b} = 136 + \sum_j \sum_{i=1}^{18} (\chi_j^i(D)\chi_j^{-i}(a, b)) \quad \text{and} \quad y_{-r,0} = 0,$$

we have

$$0 = 136 - 117 - 22 + (-22, 35) + (-22, 35) + (-22, 35) - 41B + 35(15 - B)$$

where the terms correspond successively to χ_0, χ_∞, χ_{19}, the other three characters χ_j for which $\chi(D) = 3\eta - 5$ or $3\bar{\eta} - 5$, and the other 15 characters. It is easy to see that the only solution with B integral is $B = 6$, with the three doubtful terms all -22. Thus $\chi_j(D) = 3\eta - 5$ for all five of these χ_j.

Since $y_{0,-r} = 0$, we get

$$0 = 136 - 117 - 22 + (-22, 35) + (-22, 35) + (-22, 35) - 41B + 35(15 - B)$$

the second and third terms corresponding to χ_{19}, χ_∞. As before we must have $B = 6$ and the three terms all -22, which shows the three χ_j with $\chi_j(D) = 3\eta - 5$ all occur for j a quadratic residue mod 19. We may again assume that $\chi_1(D) = 3\eta - 5$. Since $\chi_1(r, -r) = 1$ and $y_{r,-r} = 0$, we get

$$0 = 136 - 117 + 35 - 22 + (22, -35) - 41B + 35(15 - B)$$

the second, third, and fourth terms corresponding to χ_1, χ_{19}, χ_∞, respectively. But this is impossible with B integral.

IV. *There is no difference set with* $v = 29^2$, $k = 120$, $n = 103$.

Proof. Let η_i be the fourth power periods, say $\eta_i = \sum_{j=1}^{7} \zeta^{24j+i}$, ζ a fixed primitive 29^{th} root of 1. Then $(\eta_0 - 2)(\eta_2 - 2) = 11 + \eta_1 + \eta_3 = 11 + \sum \zeta^{2r}$. Since $\bar{\eta}_0 = \eta_2$, it follows that the integers $w(\eta_i - 2)(\eta_{i+1} - 2)$ are all the integers of absolute value $\sqrt{103}$ in $Q(\zeta)$. If D is fixed under the fourth power multipliers, we must have for each $\chi \neq \chi_0$, $\chi(D) = -(\eta_i - 2) \cdot (\eta_{i+1} - 2)$ for some i, since $(\eta_i - 2)(\eta_{i+1} - 2) \equiv -k \pmod{1 - \zeta}$. Now the trace of $\chi(D)$ is -91 for each χ, and by (2)

$$29^2 y_e = 120 + 30(-91)$$

which is impossible.

V. *There is no difference set with* $v = 11^3$, $k = 210$, $n = 177$.

Proof. If η is the quadratic period in the field of eleventh roots of 1, then $|\eta| = 3$, and $(3 - 7\eta)w$ and $(-3 - 8\eta)w$ are the only integers in the field of eleventh roots of 1 (up to conjugation) of absolute value 177; $3 - 7\eta$ and $-3 - 8\eta \equiv 210 \pmod{1 - \eta}$. $\sum_{j=1}^{10} \chi^j(D)$ is 65 if $\chi(D) = 3 - 7\eta$, 10 if $\chi(D) = -3 - 8\eta$. If D is fixed by all σ_r then by (2)

$$11^3 y_e = 210 + 65A + (133 - A)10.$$

But $y_e \leq 1$ implies $A < 0$, which is impossible. (This proof, shorter than my original proof, is due to Mann.)

VI. *There is no difference set with* $v = 11^3$, $k = 266$, $n = 213$.

Proof. $n = 213 = 3 \cdot 71$; since $11 \cdot 5^2 + 3^2 = 4 \cdot 71$, $-\eta - 5$, $11 - 4\eta$ are the possible values for $\chi(D)$ (up to conjugation) if D is invariant under σ_r. The traces are -145, 130, respectively, and we conclude that $0 \in D$, and there are 59 lines in $\hat{G}$ of the type $-\eta - 15$, 74 of the second type. We now com-

pute m, the number of points of D in a subgroup H of order p of G. There are 11^2 characters in $\hat{G}$ such that $\sum_H \chi(g) = 11$; for all other χ $\sum_H \chi(g) = 0$.

Thus by (2)

$$11^3 m = 11^3 \sum_H y_g = (11k + \sum_{\chi \neq \chi_0} \chi(D)(\sum_H \bar{\chi}(g)))$$
$$= 11 \cdot 266 + 11(-145A + 130(12 - A))$$
$$25A = 166 - 11m.$$

Thus $m \equiv 1 \pmod 5$, $m = 1$, 6 or 11. $m = 1$, 11 lead to fractional values of A. Thus $m = 6$ for any subgroup of order 11 of G; but this implies there are at least $5 \cdot 133 + 1 > 266 = k$ points in D, which is impossible.

VII. *There is no difference set with* $v = 13^3$, $k = 793$, $n = 507 = 3 \cdot 13^2$.

Proof. Let η be any fourth power period ($\eta = \zeta^i + \zeta^{3i} + \zeta^{9i}$, $i \not\equiv 0 \pmod{13}$). It is easily verified that $|1 + \eta| = 3$ and that $w(1 + \eta)$ are the only integers of absolute value 3 in the field $Q(\zeta)$. We take D invariant under all the fourth power multipliers, so that $\chi(D) = \pm 13(1 + \eta)$ for each $\chi \neq \chi_0$ (and one of four η's). The trace of $\chi(D)$ is clearly $\pm 13 \cdot 9$. Now by (2)

$$13^3 y_e = 793 + 13 \cdot 9(A - B)$$

where $A + B = (13^3 - 1)/12 = 183$. Since $9 \mid (13^2 y_e - 61)13$, we must have $y_e = 1$, and

$$A - B = 183 - 2B = 12$$

which leads to a fractional value of B.

The only sets of values of (v, k, λ, n) left from [2] are

$$31^2, 256, 68, 188 = 4 \cdot 47$$

and

$$3^6, 273, 102, 171 = 9 \cdot 19.$$

References

1. Marshall Hall, Jr., *A survey of difference sets*, Proc. Amer. Math. Soc., vol. 7 (1956), pp. 975–986.
2. H. B. Mann, *Difference sets in elementary abelian groups*, Illinois J. Math., vol. 9 (1965), pp. 212–219.
3. Richard Turyn, *Character sums and difference sets*, Pacific J. Math., vol. 15 (1965), pp. 319–346.

Sylvania Electronic Systems
Waltham, Massachusetts