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 $\{\chi^i\}$, $i \neq 0$ as a line of $\hat{G}$.

We recall the inversion formula

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

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

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.