L'Enseignement Mathématique, t. 40 (1994), p. 105-107

A NOTE ON TABLE I OF "BARKER SEQUENCES AND DIFFERENCE SETS"

by Wayne J. BROUGHTON

In Table I of [EK], S. Eliahou and M. Kervaire show the non-existence of cyclic difference sets with parameters $(2t(t+1)+1, t^2, t(t-1)/2)$, for $3 \leqslant t \leqslant 100$, $t \neq 50$, leaving the case $t = 50$ undecided. The purpose of this note is to fill this gap and to generalize the table to non-cyclic difference sets. See any of [EK], [L], or [J] for definitions and notation.

To handle the case $t = 50$ we make use of a multiplier theorem due to McFarland (see [L], Theorem 5.24, p. 218, or [J], Theorem 4.7, p. 254). It refers to a function $M(z)$ which has $M(1) = 1$, and (for $z \geqslant 5$) is defined recursively to be the product of the distinct prime factors of the numbers

$$z, M\left(\frac{z^2}{p^{2e}}\right), p - 1, p^2 - 1, \ldots, p^{u(z)} - 1 ,$$

where p is any prime dividing z with $p^e \| z$ and where $u(z) = (z^2 - z)/2$. (Note that the "definition" of M depends on the choice of p made for each z.)

PROPOSITION. *If D is an abelian (v, k, λ)-difference set in G, and m is a divisor of $n := k - \lambda$ such that $M(n/m)$ and v are co-prime, and if d is an integer co-prime with v such that for every prime $p \mid m$ there exists $f \geqslant 0$ with $p^f \equiv d$ $(\mathrm{mod}\, \exp(G))$, then d is a numerical multiplier of D.*

Now when $t = 50$ we have $v = 5101$, a prime, (so $G = \mathbf{Z}_{5101}$), and $n = 1275 = 3 \cdot 5^2 \cdot 17$. Let $m = 3 \cdot 17$. So $n/m = 5^2$, and $M(5^2)$ has as factors the prime factors of

$$5^2, M(1), 5 - 1, 5^2 - 1, \ldots, 5^{300} - 1 ,$$

since $u(25) = 300$. But the multiplicative order of 5 modulo 5101 is 425, so $M(25)$ is not divisible by $v = 5101$. Moreover,

$$3^{1088} \equiv 17^1 \quad (\mathrm{mod}\, 5101) ,$$

so by the proposition $d = 17$ is a multiplier of any (5101, 2500, 1225)-difference set.

But the non-trivial orbits of multiplication by 17 in $\mathbf{Z}_{5101}$ are all of size 75, so it is impossible for a union of orbits to have size 2500 and hence no such difference set exists.

The primary non-existence theorem used in Table I of [EK] to eliminate difference sets is what they call the Semi-Primitivity Theorem (see Theorem 4.5 of [L] or Theorem 7.1 of [J]). Since this theorem actually applies to abelian difference sets (not just cyclic ones), it can also be used to eliminate almost all of the abelian difference sets in the range $3 \leqslant t \leqslant 100$. The only (non-cyclic) abelian case to which the theorem does not apply is $t = 49$, where the parameters are (4901, 2401, 1176) and $n = 1225 = 35^2$. This is easily eliminated by Theorem 4.18 of [L]. Since $4901 = 13^2 \cdot 29$, we can (using Lander's notation) take a subgroup H in G of order $h = 29$, and let $m = 35$. So $m^2 \mid n$, and m is semi-primitive mod $|G/H| = 169$ since $5^{26} \equiv 7^{78} \equiv -1 \pmod{169}$; but by the theorem this implies $h \geqslant m$ (note the misprint in [L]), which is a contradiction.

Next, the only values of $t \in \{3, \ldots, 100\}$ for which there exists a *non-abelian* group of order $v = 2t(t + 1) + 1$ are $t = 26$, 28, 36, 41, 48, 51, 52, 66, 73, 76, 86, 88, 96, and 98. In every one of these cases we can apply Theorem 4.4 of [L] (Theorem 7.6 in [J]), using the semi-primitivity relations already listed in Table I of [EK].

So we conclude that there do not exist *any* $(2t(t + 1) + 1, t^2, t(t - 1)/2)$-difference sets for $3 \leqslant t \leqslant 100$.

We now point out a few misprints in Table I:

(i) At $t = 12$, v should be "313" (a prime), not "$3 \cdot 13$".

(ii) At $t = 17$, the semi-primitivity relation should read "$3^{51} \equiv -1 \pmod{613}$".

(iii) At $t = 28$, the factorization for n should read "$2 \cdot 7 \cdot 29$".

(iv) At $t = 61$, v should be "$5 \cdot 17 \cdot 89$".

S. Eliahou and M. Kervaire have also pointed out that on page 375 the polynomial $\theta_0(y)$ should read

$$y^3 + y^6 + y^7 + y^9 + y^{11} + y^{12} + y^{13} + y^{14}\,.$$

Finally, they also requested mention of the fact that at the time of writing [EK], they were not aware of the paper [C], which contains the complete classification of (255, 127, 63) cyclic difference sets and should have been included in their bibliography.

REFERENCES

[C] CHENG, U. Exhaustive Construction of (255, 127, 63)-Cyclic Difference Sets. *J. Comb. Theory., Ser. A 35* (1983), No. 2, 115-125.

[EK] ELIAHOU, S. and M. KERVAIRE. Barker Sequences and Difference Sets. *L'Ens. Math. 38* (1992), 345-382.

[J] JUNGNICKEL, D. Difference Sets. In *Contemporary Design Theory,* J. H. Dinitz and D. R. Stinson, Ed., Wiley-Interscience (1992), 241-324.

[L] LANDER, E. S. *Symmetric Designs: An Algebraic Approach.* London Math. Soc. Lecture Note Series 74, Cambridge University Press (1983).

(Reçu le 21 décembre 1993)

Wayne J. Broughton

Department of Mathematics
California Institute of Technology
Sloan 253-37
Pasadena, CA 91125
U.S.A.