Nonexistence of Some Difference Sets

K.T. Arasu*
Department of Mathematics and Statistics
Wright State University
Dayton, OH 45435

Surinder K. Sehgal
Department of Mathematics
Ohio State University
Columbus, OH 43210

ABSTRACT. We settle the existence status of some previously open cases of abelian difference sets. Our results fill ten missing entries in the recent table of López and Sánchez, all with answer 'No'.

1 Introduction

Let G be a multiplicatively written group of order v. A subset D of G of size k is said to be a (v, k, λ) difference set in G if each nonidentity element can be expressed in exactly λ ways as $d\left(d'\right)^{-1}$, where $d, d' \in D$. A (v, k, λ) difference set is said to be cyclic (resp. abelian) if the underlying group G is cyclic (resp. abelian). For more on difference sets, see Lander [3] or Jungnickel [1].

López and Sánchez [4] examined all possible triples (v, k, λ) for which an abelian difference set could possibly exist for k satisfying $100 < k \leq 150$. They report 16 open cases in their table as undecided cases. In this paper we settle four of these cases, all with a negative response, thereby filling ten missing entries as "no".

*Research partially supported by AFOSR grant F49620-96-1-0328 and by NSA grant MDA904-97-1-0012.

2 Preliminaries

In this section we state some well-known results on multipliers of a difference set.

Theorem 1. (First multiplier Theorem, see [3]) *Let D be a (v, k, λ) difference set in an abelian group G. Let p be a prime which divides n but does not divide v. (Here $n = k - \lambda$.) If $p > \lambda$, then p is a multiplier of D.*

Theorem 2. (McFarland and Rice [5]) *Let D be a (v, k, λ) difference set in an abelian group G. The group of numerical multipliers fixes at least one translate of D.*

Using the above two theorems, one can investigate the existence or nonexistence of a (v, k, λ) difference set. A hypothetical difference set D with parameters (v, k, λ), without loss of generality, can be assumed to be fixed by a known multiplier t of D. (Otherwise, D can be replaced by such a translate of D.) Then D must be the union of some of the orbits of G under $\langle x \mapsto tx \rangle$. By arguing carefully, one can either construct such D or prove that D cannot exist.

Theorem 3. (Jungnickel and Pott [2]) *Let D be a (v, k, λ)-difference set with $v > k$ in G. Furthermore, let $u \neq 1$ be a divisor of v, let U be a normal subgroup of index u of G, put $H = G/U$ and assume that H is abelian and has exponent u^*. Finally, let p be a prime not dividing u^* and assume that $tp^f \equiv -1 \mod u^*$ for some numerical G/U-multiplier t of D and a suitable non-negative integer f. Then the following hold:*

(i) *p does not divide the square-free part of $n = k - \lambda$, say $p^{2j} \parallel n$ (where $j \geq 0$);*

(ii) *$p^j \leq v/u$;*

(iii) *if $u > k$, then $p^j \mid k$.*

3 Main Results

Proposition 1. *There does not exist any (5085, 124, 3) difference sets in $C_3 \times C_3 \times C_5 \times C_{113}$.*

Proof: By Theorem 1, since $n = 124 - 3 = 11^2$, 11 is a multiplier of a putative (5085, 124, 3) difference set D in $G = C_3 \times C_3 \times C_5 \times C_{113}$. We shall work with the multiplier $t = 11^2 = 121$ of D. Since $t \equiv 1(\mod 15)$, t acts as identity on $C_3 \times C_3 \times C_5$. The orbits of 121 on C_{113} are of sizes 1, 28, 28, 28, 28; thus on G, the multiplier 121 has sizes 1 and 28. By Theorem 2, D is a union of some of these orbits (replacing D by a translate of it, if necessary). Let D consist of a orbits of size 1 and b orbits of size 28. Then

$a + 28b = 124$ and $0 \leq a \leq 45$. (Note: There are only 45 singleton orbits). Since $a \equiv 12(\mod 28)$, we must have $a = 12$ or $a = 40$.

The differences from each of the size 28 orbits all lie in C_{113}. Hence $28 \cdot 27 \cdot b \leq (113-1)3$, showing $b = 0$. But then $a = 124$, which is a contradiction.

Thus D cannot exist, proving Proposition 1.

Proposition 2. *There do not exist (1975, 141, 10) difference sets in $C_5 \times C_5 \times C_{79}$ or $C_{25} \times C_{79} = C_{1975}$.*

Proof: Let D be a hypothetical (1975, 141, 10) difference set in G, where $G = K \times C_{79}$, where $K = C_5 \times C_5$ or C_{25}. By Theorem 1, $t = 131$ is a multiplier of D. We work with the multiplier $t = 131^5$. Note: $131^5 \equiv 1$ (*mod* exponent of K), hence t is identity on K. Its orbits on C_{79} are: a single orbit of size 1 and 6 orbits of size 13. By Theorem 2, we may, without loss of generality, assume that D is a union of these orbits, say a orbits of size 1 and b of size 13.

Then

$$a + 13b = 141 \tag{1}$$

and $a \in [0, 25]$. Note that $a \equiv 11(\mod 13)$.

Hence

$$a = 11 \text{ or } 24 \tag{2}$$

The b orbits of size 13 yield $13 \cdot 12 \cdot b$ differences of D all of which lie in C_{79}.

Hence $13 \cdot 12 \cdot b \leq (79-1)10$,using $\lambda = 10$ so

$$b \leq 5 \tag{3}$$

(2) and (3) contradict (1). Hence D cannot exist proving Proposition 2.

Proposition 3. *There do not exist any (1161, 145, 18) difference sets in $G = K \times C_{43}$, where K is any abelian group of order 27.*

Proof: If possible, let D be such a difference set. By Theorem 1, 127 is a multiplier of D. We work with the multiplier $t = 127^3$, noting that $t \equiv 1(\mod 27)$, thus $t \equiv 1(\mod \text{ exponent of } K)$; so t acts as identity on K. The orbit of t on C_{43} are: one singleton orbit and 6 orbits of size 7. Thus the orbits of t on G are of sizes 1 and 7. Assume that D is comprised of a orbits of size 1 and b orbits of size 7.

Then

$$a + 7b = 145 \tag{4}$$

and

$$a \in [0, 27] \tag{5}$$

Note that

$$a \equiv 5(\mod 7) \tag{6}$$

Counting differences as in Proposition 2 yields $7 \cdot 6 \cdot b \leq 42 \cdot 18$ showing $b \leq 18$. Hence by (4), $a \geq 19$.

So from (5) and (6), we conclude $a = 19$ or 26.

Case 1. $a = 26$.

All the singleton orbits are of the form (i, e), where e is the identity element of C_{43} (where i is any element of K).

Hence the differences of these 26 elements all lie in K. So we must have:

$$26 \cdot 25 \leq (|K| - 1).\lambda = 26 \cdot 18,$$

a contradiction.

Case 2. $a = 19$, so $b = 18$.

The subgroup C_{43} has index 27 in G. Since D uses 19+18=37 orbits (37 > 27), there exist at least one coset K' of C_{43} containing more than 7 elements of D, say $|D \cap K'| \geq 8$. Thus $8 \cdot 7 + 7 \cdot 6 \cdot 17 \leq 18 \cdot 42$. Which is a contradiction. Hence D cannot exist.

Proposition 4. *There do not exist (448, 150, 50) difference sets in (i) $G = C_4 \times C_2^4 \times C_7$ (or) (ii) $G = C_4 \times C_4 \times \times C_2^2 \times C_7$ (or) (iii) $G = C_8 \times C_2 \times \times C_2 \times C_2 \times C_7$.*

Proof: We apply Theorem 3 with $p = 5$;

$$U = \begin{cases} C_2 & \text{in (i)} \\ C_2 \times C_2 & \text{in (ii)} \\ C_4 & \text{in (iii)} \end{cases}$$

so that G/U has exponent 14.

We take $t = 1$ in Theorem 3 and use the fact $5^3 \equiv -1(\mod 14)$.

By (ii) of Theorem 3, we have

$$5 \leq \frac{v}{\text{index of } U}$$

i.e. $5 \leq 4$, a contradiction, proving Proposition 4.

Proposition 5. *There does not exist any* $(16513, 129, 1)$ *difference set in* $C_7 \times C_7 \times C_{337}$.

Proof: By Theorem 1, since $n = 129 - 1 = 2^7$, 2 is a multiplier of a hypothetical $(16513, 129, 1)$ difference set D in $G = C_7 \times C_7 \times C_{337}$. We shall work with the multiplier $t = 2^3 = 8$ of D. Since $t \equiv 1 \pmod{7}$, t acts as identity on $C_7 \times C_7$. The orbits of 8 on C_{337} are 1 and 7: a singleton orbit and 48 orbits of size 7. Thus the orbits on G are also of sizes 1 and 7. By Theorem 2, replacing D by a translate, if necessary, we may assume that D is a union of some of these orbits. Let D consist of a orbits of size 1 and b orbits of size 7. Then

$$a + 7b = 129 \tag{7}$$

The differences from the a elements of the singleton orbits all lie in $C_7 \times C_7$. Hence $a\,(a - 1) \leq (49 - 1)\,1$, showing

$$a \leq 7 \tag{8}$$

The differences from each of the size 7 orbits yield elements of C_{337}. Hence $7 \cdot 6 \cdot b \leq (337 - 1)\,1$, giving

$$b \leq 8 \tag{9}$$

(8) and (9) contradict (7). Hence D cannot exist.

References

[1] D. Jungnickel, Difference Sets, In: *Contemporary Design Theory* (Ed: Dinitz & Stinson), Wiley (1992), 241–324.

[2] D. Jungnickel & A. Pott, Two Results on Difference sets, *Colloquia Math. Societatis János Bolyai* **52** *Combinatorics, Eger*, (1987), 325–330.

[3] E.S. Lander, Symmetric designs: An algebraic approach, Cambridge Univ. Press (1983).

[4] A.V. López and M.A.G. Sánchez, On the existence of Abelian Difference Sets with $100 < k \leq 150$ *JCMCC* **23** (1997), 97–112.

[5] R.L. McFarland and B.F. Rice, Translates and multipliers of abelian difference sets, *Proc. AMS* **68** (1978), 375–379.