COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA **11** (1) (1991) 1–8

SOME NON-EXISTENCE RESULTS ON DIVISIBLE DIFFERENCE SETS*

K. T. ARASU, JAMES DAVIS, DIETER JUNGNICKEL and ALEXANDER POTT

Received April 20, 1988

In this paper, we shall prove several non-existence results for divisible difference sets, using three approaches:

(i) character sum arguments similar to the work of Turyn [25] for ordinary difference sets,
(ii) involution arguments
and (iii) multipliers in conjunction with results on ordinary difference sets.

Among other results, we show that an abelian affine difference set of odd order s (s not a perfect square) in G can exist only if the Sylow 2-subgroup of G is cyclic. We also obtain a non-existence result for non-cyclic $(n, n, n, 1)$ relative difference sets of odd order n.

1. Introduction

A *divisible difference set* with parameters m, n, k, λ_1, λ_2 (for short, an $(m, n, k, \lambda_1, \lambda_2)$ – DDS) in a group G of order mn relative to a normal subgroup N of order n is a k-subset D of G such that every element $g \in G \setminus N$ has exavtly λ_2 representations as $g = d - d'$ with d, $d' \in D$ and every $g \neq 1$ in N has exactly λ_1 such representations (here we write G additively). We say that G is *splitting* if in fact $G = N \oplus H$ for some subgroup H of G. D is called abelian or cyclic or splitting if G has the respective property. In case $\lambda_1 = 0$, D is called a *relative difference set* (for short, an (m, n, k, λ_2) – RDS). Finally, an *affine difference set* of order s is an $(s+1, s-1, s, 1)$ – RDS, since there is a natural way of constructing an affine plane of order s from D. For more on divisible difference sets (including a detailed bibliography), see [17] and [21]. (We warn the readers that various authors, including [17], use somewhat different terminology than the one introduced above). Relative difference sets were introduced by Elliott and Butson [9], and affine difference sets have been extensively studied since the pioneering papers of Bose [7] and Hoffman [12]. We mention [3], [4], [18], [20], [21], [23] as recent examples. Note that a DDS with $\lambda_1 = \lambda_2$ or with $n = 1$ is just an ordinary difference set (see [6] for background on these).

We shall need one more concept: An integer t is called a *multiplier* of an abelian $(m, n, k, \lambda_1, \lambda_2)$ – DDS D, if $\varphi : x \mapsto tx$ is an automorphism of both G and the

AMS subject classification (1980): 05 B 10 (primary), 05 B 20 (secondary)

*The first author's research was partially supported by NSA Grant #MDA 904–87–H–2018. The second and fourth authors gratefully acknowledge the hospitality of Wright State University during the time of this research. The last two authors thank the University of Waterloo for its hospitality, and the third author also acknowledges the financial support of NSERC under Grant #IS–0367.

divisible design $\mathrm{dev}D = (G, \{D + x \mid x \in G\}, \in)$ naturally associated with D (see e.g. [17]). In other words, we require $(t, mn) = 1$ and $tD = \{td : d \in D\} = D + g$ for a suitable $g \in G$. (Actually, one may assume $g = 0$ in this definition, but we will not make use of this fact).

In this paper we shall prove several non-existence results for divisible difference sets, using three approaches:

(i) character sum arguments similar to the work of Turyn [25] for ordinary difference sets,

(ii) involution arguments

and (iii) multipliers in conjunction with results on ordinary difference sets.

Among other results, we show that an abelian affine difference set of odd order s (s not a perfect square) in G can only exist if the Sylow 2-subgroup of G is cyclic. We also obtain a non-existence result for non-cyclic $(n, n, n, 1)$ – RDS's of odd order n.

2. Preliminaries on character sums

In this section we write G multiplicatively and consider the group ring ZG of G over the integers. By abuse of notation, we will identify each subset S of G with $\sum_{x \in S} x \in ZG$. As usual, we shall define

$$A^{(t)} = \sum_{g \in G} a_g g^t \qquad \text{for} \quad A = \sum_{g \in G} a_g g \in ZG,$$

where t is an arbitrary integer. With these notations, a subset D of G is an $(m, n, k, \lambda_1, \lambda_2)$ – DDS in G relative to N if and only if D satisfies the identity:

$$\mathrm{DD}^{(-1)} = k - \lambda_1 + \lambda_1 N + \lambda_2 (G - N). \tag{1}$$

Assume that G is abelian and that χ is a nonprincipal character of G which is also nonprincipal on N (see Huppert [14] for background from group theory). Thus, χ is a homomorphism from G into $Z[\omega]$ where ω is a primitive e^{th} root of unity (with e the exponent of G). We may extend χ to a ring homomorphism from ZG to $Z[\omega]$ (by linearity) which will again be denoted by χ. Applying χ to equation (1) yields

$$\chi(D)\chi(D^{(-1)}) = k - \lambda_1 \tag{2}$$

since $\chi(N) = \chi(G) = 0$ by the orthogonality relations. Note that $\chi(D^{(-1)}) = \chi^{-1}(D) = \overline{\chi}(D)$, where $\overline{\ }$ denotes complex conjugation. Thus (2) implies the following result:

Lemma 2.1. *Let D be an abelian $(m, n, k, \lambda_1, \lambda_2)$ – DDS in G (relative to N). If χ is any character of G which is non-principal on N, then one has*

$$|\chi(D)|^2 = k - \lambda_1. \tag{3}$$ ∎

We shall next derive a similar result for splitting divisible difference sets. Thus assume that $G = N \oplus H$ and denote by $\underline{A}$ the image of $A \in ZG$ under the canonical epimorphism $\gamma : ZG \to Z(G/H) \cong ZN$. Applying γ to equation (1) gives

$$\underline{D}\underline{D}^{(-1)} = k - \lambda_1 + (\lambda_1 + \lambda_2(m-1))N. \tag{4}$$

Assume furthermore that N is abelian and that χ is a non-principal character of N. Then an analogous argument as the one given above shows the following:

Lemma 2.2. *Let D be a splitting $(m, n, k, \lambda_1, \lambda_2) - \mathrm{DDS}$ in $G = N \oplus H$, where N is abelian. If χ is non-principal character on N, then one has*

$$|\chi(D)|^2 = k - \lambda_1. \tag{5}$$

∎

We close this section by stating the following Lemma due to Turyn [25]:

Lemma 2.3. *Let η be an algebraic integer in the m^{th} cyclotomic field Q_m and suppose that $|\eta|^2 = n$. Let p be a prime divisor of n which is semi-primitive modulo m (i.e., there exists a non-negative integer f with $p^f \equiv -1 \pmod{m}$). Then p divides n to an even power, say $p^{2b} || n$ and $p^b || \eta$ (here we write $p^a || x$ if $p^a | x$ but $p^{a+1} \nmid x$).* ∎

It is clear that Lemma 2.3 applies to $\chi(D)$ in the situation of either Lemma 2.1 or Lemma 2.2.

3. Abelian Divisible Difference Sets

We begin with the following application of Lemma 2.1:

Theorem 3.1. *Let D be an abelian $(m, n, k, \lambda_1, \lambda_2) - \mathrm{DDS}$ in G relative to N and suppose $m \equiv 2 \bmod 4$. Then the Sylow 2-subgroup of G is cyclic or $k - \lambda_1$ is a perfect square.*

Proof. We may assume that the Sylow 2-subgroup S of G is not cyclic. As $m \equiv 2 \bmod 4$ this implies that n is even. Thus $|S| = 2^d$ for some $d \geq 2$ and $|N \cap S| = 2^{d-1}$. Consider the Frattini subgroup $\Phi(S)$ of S (see Huppert [14] for the properties of $\Phi(S)$ which we shall use). Since S is not cyclic, we have $|\Phi(S)| \leq 2^{d-2} < |N \cap S|$. Thus we may choose an element $g \in (N \cap S) \setminus \Phi(S)$. Then g is contained in a minimal generating set (i.e. in a basis) of S, and therefore g is also contained in a basis B of G. Let χ be the character of G which maps g to -1 and every other element of B to $+1$. Then χ has order 2 and is non-principal on N. Hence $\chi = \overline{\chi} = \overline{\chi}^{-1}$ and thus Lemma 2.1 shows that $\chi(D)^2 = k - \lambda_1$ is a perfect square. ∎

Corollary 3.2. *Let D be an abelian affine difference set of order $s \equiv 1 \pmod 4$ in G. Then the Sylow 2-subgroup of G is cyclic or s is a perfect square.* ∎

We next state a simple Lemma which will allow us to deal also with abelian affine difference sets of order $s \equiv 3 \pmod 4$.

Lemma 3.3. *Let D be an $(m, n, k, \lambda_1, \lambda_2) - \mathrm{DDS}$ in G relative to N (where G is not necessarily abelian). If λ_1 is odd, then all involutions of G are contained in $G \setminus N$. If λ_2 is odd, then all involutions of G are contained in N.*

Proof. Assume that λ_1 is odd. If possible, pick an involution $x \in N$. Whenever $x = d - d'$ with $d, d' \in D$, then also $x = -x = d' - d$. Thus the number of difference representations of x from D has to be even, a contradiction. The proof of the second assertion is similar. ∎

Corollary 3.4. *Let D be an affine difference set of order $s \equiv 3 \pmod 4$ in G. Then the Sylow 2-subgroup of G is cyclic.*

Proof. As $n = s - 1 \equiv 2 \pmod 4$, the Sylow 2-subgroup of N is isomorphic to Z_2. Thus N contains a unique involution. If the Sylow 2-subgroup of G if not cyclic, we have to have an involution outside N, contradicting 3.3. ∎

Combining 3.2 and 3.4, we obtain:

Theorem 3.5. *Let D be an abelian affine difference set of odd order s in G. Then the Sylow 2-subgroup of G is cyclic or s is a perfect square.* ∎

4. Splitting divisible difference sets

We begin with an application of Lemma 2.2 which gives the following analogue of Theorem 3.1:

Theorem 4.1. *If there exists a splitting $(m, n, k, \lambda_1, \lambda_2) - \mathrm{DDS}$ in $G = N \oplus H$ where N is an abelian group of even order, then $k - \lambda_1$ is a perfect square.*

Proof. Since $|N|$ is even, there exists a non-principal character χ of order 2. Apply Lemma 2.2. ∎

Specializing 4.1 to affine difference sets is not too interesting since one can obtain a stronger result from Lemma 3.3:

Lemma 4.2. *There exists no splitting affine difference set of odd order s.*

Proof. Note that here $m = s + 1$ and $n = s - 1$ are both even. If D is a splitting affine difference set of order s in $N \oplus H$, then clearly H contains an involution, contradicting Lemma 3.3. ∎

Combining 4.2 with results of Arasu and Jungnickel [4] we obtain:

Theorem 4.3. *Assume the existence of a splitting affine difference set D of order s. Then $s = 2$ or s is divisible by 4. If D is abelian, then s is divisible by 8 (unless $s = 2$ or 4). Moreover, the following two conditions have to be satisfied:*

(i) There exists a Hadamard difference set in N which admits every prime divisor of s as a multiplier.

(ii) Either s is a square, or we have $\left(\frac{p}{q}\right) = 1$ for each prime p dividing s and each prime q dividing $s - 1$. (Here $\left(\frac{p}{q}\right)$ denotes the Legendre symbol.) ∎

A weaker version of 4.3 (in particular containing the abelian case) was obtained by Jungnickel [20]. We now use 3.3 to strengthen another result of [20]:

Theorem 4.4. *Let H and N be arbitrary groups and assume the existence of a splitting $(n\lambda + 2, n, n\lambda + 1, \lambda) - \mathrm{RDS}$ in $G = H \oplus N$. Then one has one of the following cases:*

(i) n and λ are even, $n\lambda + 1$ is a perfect square and H is non-abelian.

(ii) $n \equiv 0 \bmod 4$, λ is even and N is not solvable.

(iii) $n \equiv 3 \bmod 4$ and λ is odd.

(iv) n is odd and λ is even.

Proof. Except for the assertion that λ is even in (i) and (ii), this is Theorem 4.3 of [20]. Note that the assumption that λ is odd yields a contradiction as in the proof of 4.2. ∎

5. Characters of prime order

In this section we shall apply Lemmas 2.2 and 2.3 to characters of prime order to obtain the following result:

Theorem 5.1. *Let D be a splitting $(m, n, k, \lambda_1, \lambda_2)$ – DDS in $G = N \oplus H$, where N is abelian. Moreover, let p be a prime dividing the square-free part of $k - \lambda_1$, and let $q \neq p$ be any prime divisor of n. Then p is a quadratic residue modulo q.*

Proof. Since q divides n, we may choose a (non-principal) character χ of order q on N. By Lemma 2.2, the algebraic integer $\chi(D)$ (in the q^{th} cyclotomic field) satisfies $|\chi(D)|^2 = k - \lambda_1 \in Z$. Thus Lemma 2.3 shows that p cannot have even order mod q (since otherwise $p^f \equiv -1 \bmod q$) for a suitable f, contradicting the fact that p divides $k - \lambda_1$ to an odd power, by hypothesis). Thus p has odd order mod q which implies that p is a quadratic residue mod q. ∎

We note that Theorem 5.1 is equivalent to Theorem 8.1 of Elliott and Butson [9] under the additional assumptions that q does not divide m and that H is abelian. Our result is stronger, as it also rules out certain non-abelian groups. Even more important is the removal of the assumption that q does not divide m, since this enables us to obtain a non-existence result for splitting $(n, n, n, 1)$ – RDS's of odd order n:

Theorem 5.2. *Let D be a splitting $(n, n, n, 1)$ – RDS in $G = N \oplus H$, where N is abelian. Moreover, let p be an odd prime dividing the square-free part of n. Then p is a quadratic residue modulo q for every prime divisor $q \neq p$ of n.* ∎

We give two sample applications:

Corollary 5.3. *Let D be a splitting $(n, n, n, 1)$ – RDS in $G = N \oplus H$, where N is abelian. Then the square-free part of n has at most one prime divisor $\equiv 3$ modulo 4.*

Proof. Otherwise let p and q be distinct prime divisors of n which are $\equiv 3$ modulo 4. Thus $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = 1$ by 5.2 (where $\left(\frac{x}{y}\right)$ denotes the Legendre symbol). But quadratic reciprocity gives $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ for $p, q \equiv 3 \pmod 4$, a contradiction. ∎

Corollary 5.4. *Let D be a splitting $(n, n, n, 1)$ – RDS in $G = N \oplus H$, where N is abelian. If 3 divides the square-free part of n, then every other prime divisor q of n satisfies either $q \equiv 1 \bmod 12$ or $q \equiv -1 \bmod 12$. In the second case, q divides n to an even power.*

Proof. By 5.2, $\left(\frac{3}{q}\right) = 1$ and thus $q \equiv \pm 1 \bmod 12$. If $q \equiv -1 \bmod 12$, then $q \equiv 3 \bmod 4$ and so q does not divide the square-free part of n by 5.3. ∎

We remark that the structure of abelian $(n,n,n,1)$ – RDS's of even order is completely settled; in particular, n is a power of 2, then, and G does *not* split (see Ganley [10] and, for a simpler proof, Jungnickel [19]). Thus 5.2 is only interesting if n is odd. In this case, every affine plane of order n over a commutative semifield gives rise to an abelian $(n,n,n,1)$ – RDS. Thus n is a prime power, then; moreover, G is known to be elementary abelian (see, e.g., Jungnickel [17] for a proof of this result which basically goes back to Hughes [13]). In particular, for all known abelian examples of odd order, the RDS is splitting. Thus this assumption on Theorem 5.2 seems reasonable. We note also that no cyclic $(n,n,n,1)$ – RDS with $n \geq 3$ exists, see Elliott and Butson [9].

In view of Theorem 4.3, an application of 5.1 to affine difference sets can only be interesting if the order s is even. We then obtain the following result:

Theorem 5.5. *Let D be a splitting affine difference set (of even order s) in $G = N \oplus H$, where N is abelian. If p is a prime dividing the square-free part of s and if q is any prime divisor of $s-1$, then $\left(\frac{p}{q}\right) = 1$.*

If G is abelian, a somewhat stronger result than 5.5. holds, (cf. Theorem 4.3). We note that 5.2 can also be derived from a result due to de Launey who used the notion of "generalized Hadamard matrices", see [8].

6. Some results involving multipliers

In this section, D will always be an abelian (m,n,k,λ) – RDS in G relative to N. If K is any subgroup of order t of N, then the image of D in G/K is an $(m,n/t,k,\lambda t)$ – RDS relative to N/K; this well-known result is due to Elliott and Butson [9]. In particular, we obtain an ordinary $(m,k,\lambda n)$-difference set $\overline{D}$ in G/N. This allows us to use non-existence results for difference sets to obtain some new results for relative difference sets. The first of these strengthens a result of Arasu and Pott [5]:

Theorem 6.1. *Let D be an abelian (m,n,k,λ) – RDS in G with multiplier 2, and assume that $k - n\lambda$ is odd. Then D is a $(k+1,(k-1)/\lambda,k,\lambda)$ – RDS.*

Proof. By assumption, the order $k - n\lambda$ of the associated $(m,k,n\lambda)$-difference set $\overline{D}$ is odd. Clearly, 2 is a multiplier of $\overline{D}$, as it is a multiplier of D. This is possible only if $\overline{D}$ is a trivial difference set, i.e. $k - n\lambda \leq 1$, by a result of Pott [24]. Since $k - n\lambda$ is odd, we have $k = n\lambda + 1$. The trivial equation $\lambda n(m-1) = k(k-1)$ gives the assertion. ∎

Similarly, one also gets the following result:

Theorem 6.2. *Let D be an abelian (m,n,k,λ) – RDS with multiplier 3, where 3 does not divide $k - \lambda n$. If there is no $(m,k,n\lambda)$-difference set with multiplier -1, then R is a $(k+1,(k-1)/\lambda,k,\lambda)$ – RDS.*

Proof. Here $\overline{D}$ is an abelian $(m,k,n\lambda)$-difference set with multiplier 3, where 3 does not divide the order $k - n\lambda$ of $\overline{D}$. Again by [24], -1 is a multiplier of $\overline{D}$ or $\overline{D}$ is trivial. By hypothesis $\overline{D}$ is trivial and the assertion follows. ∎

Note that there are many known non-existence results for abelian difference sets with multiplier -1, see [6], [11], [15], [16], [24]. Thus our hypothesis will be satisfied quite often. We note that examples for 6.1 and 6.2 are provided by the cyclic affine difference sets of orders 2^a and 3^a, respectively, and their homomorphic images. The case $\lambda = 1$ of 6.1 and 6.2 is of particular interest when combined with Hoffman's multiplier Theorem [12]:

Corollary 6.3. *Let D be an abelian $(m, n, k, 1)$ – RDS. Then one has the following:*

(i) If $k - n$ is odd then 2 is a multiplier of D if D is an affine difference set of even order k.

(ii) If 3 is a multiplier of D and if 3 divides k, then D is an affine difference set of order k or there exists an (m, k, n)-difference with multiplier -1. In the latter case, m is even and $k - n$ a perfect square.

Our final result is as follows:

Theorem 6.4. *Let D be an abelian (m, n, k, λ)–RDS with multiplier 2, where $k–n\lambda \equiv 2 \pmod 4$. Then D is a $(4t–1, (t-1)/\lambda, 2t-1, \lambda)$ – RDS or a $(4t-1, t/\lambda, 2t, \lambda)$ – RDS.*

Proof. Now $\overline{D}$ is a $(m, k, n\lambda)$-difference set with multiplier 2 and order $k - n\lambda \equiv 2 \pmod 4$. By results of Arasu [1], [2], D has to be a $(4t-1, 2t-1, t-1)$-difference set or the complementary $(4t-1, 2t, t)$-difference set. ∎

The only examples of RDS's with the parameters of Theorem 6.4 known to us are cyclic $(7, 2, 4, 1)$ — and $(31, 2, 16, 4)$ – RDS's, see Lam [22]. Since $n = 2$, here, these examples of course do not admit 2 as a multiplier. Note that all the theorems of this section remain true under the possibly weaker assumption that the image $\overline{D}$ of D admits the multipliers in question (even if D itself does not). Indeed, this is true for the two examples mentioned above.

Acknowledgement. The authors thank Dr. John F. Dillon for a helpful discussion.

References

[1] K. T. ARASU: "On Wilbrink's theorem", *J. Comb. Th. Ser.* A **44**, (1987) 156–158.

[2] K. T. ARASU: "Another variation of Wilbrink's theorem", *Ars Combinatoria*, **25** (1988), 107–109.

[3] K. T. ARASU: "Cyclic affine planes of even order", *Disc. Math.*, **76** (1989), 177–181.

[4] K. T. ARASU, and D. JUNGNICKEL: "Affine difference sets of even order", *J. Comb. Th. A.* **52** (1989), 188–196.

[5] K. T. ARASU, and A. POTT: "Relative difference sets with multipliers 2", *Ars Combinatoria*, **27**, (1989), 139–142.

[6] T. BETH, D. JUNGNICKEL, and H. LENZ: *Design Theory*, Bibliographisches Institut, Mannheim (1985), and Cambridge University Press, Cambridge (1986).

[7] R. C. BOSE: "An affine analogue of Singer's theorem", *J. Ind. Math. Soc.* **6** (1942), 1–15.

[8] W. DE LAUNEY: "On the non-existence of generalized weighing matrices", *Ars Combinatoria* **17A** (1984), 117–132.

[9] J. E. H. ELLIOTT, and A. T. BUTSO: "Relative difference sets", *Illinois J. Math.* **10** (1966), 517–531.
[10] M. J. GANELY: "On a paper of Dembowski and Ostrom", *Arch. Math.* **27** (1976), 93–98.
[11] D. GHINELLI-SMIT: "A new result on difference sets with -1 as a multiplier", *Geom. Ded.* **23** (1987), 309–317.
[12] A. J. HOFFMAN: "Cyclic affine planes", *Can. J. Math.* **4** (1952), 295–301.
[13] D. R. HUGHES: "Partial difference sets", *Amer. J. Math.* **78** (1956), 650–674.
[14] B. HUPPERT: *Endliche Gruppen I*, Springer-Verlag, Berlin–Heidelberg–New York, 1967.
[15] E. C. JOHNSEN: "The inverse multiplier for abelian group difference sets", *Can. J. Math.* **16** (1964), 787–796.
[16] D. JUNGNICKEL: "Difference sets with multiplier -1", *Arch. Math.* **38** (1982), 511–512.
[17] D. JUNGNMICKEL: "On automorphism groups of divisible designs", *Can. J. Math.* **34** (1982), 257–297.
[18] D. JUNGNICKEL: "A note on affine difference sets", *Arch. Math.* **47** (1986), 279–280.
[19] D. JUNGNICKEL: "On a theorem of Ganley", *Graphs and Comb.* **3** (1987), 141–143.
[20] D. JUNGNICKEL: "On automorphism groups of divisible designs, II: Group invariant generalized conference matrices", *Arch. Math.* **54** (1990), 200–208.
[21] H. P. KO, and D. K. RAY-CHAUDHURI: "Multiplier theorems", *J. Comb. Th. A* **30** (1981), 134–157.
[22] C. W. H. LAM: "On relative difference sets", Proc. 7th Manitoba conference on numerical math. and computing, (1977), 445–474.
[23] A. POTT: "Affine analogue of Wilbrink's theorem", *J. Comb. Th.* A. **55** (1990), 313–315.
[24] A. POTT: "On abelian difference sets with multiplier -1, *Arch. Math.* **53** (1989), 510–512.
[25] R. J. TURYN: "Character sums and difference sets", *Pacific J. Math.* **15** (1965), 319–346.

K. T. Arasu

Department of Mathematics and Statistics
Wright State University
Dayton, Ohio 45435, U.S.A.

James Davis

Dept. of Mathematics and Computer Science
University of Richmond
Richmond, Virginia 23173, U.S.A.

Dieter Jungnickel and Alexander Pott

Mathematisches Institut,
Justus-Liebig-Universität Giessen
Arndtstr. 2, D-6300 Giessen, F. R. Germany