AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **32** (2005), Pages 213–223

Cyclic difference covers

K.T. Arasu*

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

Surinder Sehgal

Department of Mathematics
Ohio State University
Columbus, Ohio 43210
U.S.A.

Abstract

A variation of the notion of the usual difference sets known as a "difference cover" is given and many constructions and nonexistence results are presented. The subtle difference in the new definition leads to very different results, although techniques employed mirror those used to investigate difference sets.

1 Introduction

Let G be any finite abelian group of order v. Let $D = (x_1, x_2, ..., x_k)$ be a multiset/list of elements from G (not neccessarily distinct elements). A difference of these elements is called nontrivial if and only if it is of the form $x_i - x_j$, for $i \neq j$, otherwise trivial. In particular the element 0 occurs exactly k times as a trivial difference but it can also be a nontrivial difference, if some of the elements of D are equal. With this convention we give the following definition:

Definition 1.1 *A multiset $D = (x_1, x_2, ..., x_k)$ is called a difference cover with parameters (v, k, λ) if and only if every element $z \in G$ (including the identity element) appears exactly λ times as a nontrivial difference i.e. $z = x_i - x_j$, (for $i \neq j$) of elements of D.*

The above notion of difference covers differs from that of difference sets or difference lists in the requirement that the nontrivial differences cover all the non identity

---

* Research partially suported by grants from NSA and NSF.

elements of G constant number of times in the difference sets or difference lists but in difference covers they cover all elements of G including identity constant number of times. (See (Beth, Jungnickel et al [3]) for difference sets and Arasu and Ray-Chaudhuri [1] for difference lists).

Definition 1.2 *If the group G is cyclic then we call the difference cover a cyclic difference cover.*

In the literature difference covers have been studied in a more general context, where the list of differences is simply required to cover all elements of G (not necessarily with constant number of times) e.g. See, ([7],[21],[9], [13], [10], [8], [14]). In these papers the main object was to find minimal size k covering all of G as a list of differences.

While our work is motivated by paper of (T. Bier [4]), in which the regularity condition was introduced (i.e. the parameter λ was introduced), we were pleasantly surprised when we came across the work of Buratti [5] in which he has introduced the notion of a 'difference multiset.' This concept coincides with what we call here 'difference cover.' We wish to promote our nomenclature. Our reasons are two-fold: (1) The words 'multiset' and 'list' are synonyms; hence the phrase 'difference multiset' seems to bear the same meaning as the phrase 'difference list.' But the latter phrase has an altogether different connotation, in the area of algebraic design theory. (2) The phrase 'difference cover' has been used by many authors earlier and the 'regularity' condition forcing the 'lambda' parameter as constant, naturally justifies our adopted terminology.

As discussed in Buratti [5], 'difference covers' and their 'family' analogs (so-called strong difference families) have applications in the construction of balanced incomplete block designs (BIBD's) and group divisible designs (GDD's). We also wish to mention, in passing, that some of our regular difference covers give rise to certain class of self-dual codes over 'small' prime fields and some classes of 'integer weighing matrices.' Thus, in addition to their interesting and rich mathematical properties, 'difference covers' have immediate applications to related areas in discrete mathematics. The overlap of our results with those of Buratti [5] is very minimal. Buratti's methods are completely combinatorial, but we adhere to the use of group rings, character theory, and representaion theory. On the surface, it may appear that our results follow directly from established results from the theory of difference sets; but there is a lot of 'subtlity' involved here - the slight change in the definition (from 'difference set' to 'difference cover') makes the construction methods and nonexistence results behave very differently in these two 'related' areas of study. We reiterate: although we utilize tools from the theory of difference sets, the end results are very different.

In this paper we give some new constructions of difference covers and prove several non-existence theorems. Our approach is using group rings and characters as in the theory of abelian difference sets. Most of our non-existence proofs 'mimic' those of difference sets. Difference covers can be studied for any finite groups but we restrict our discussions to abelian groups. Some of our results carry over to non-abelian groups as well.

The following Theorems are due to Bier ([4])

Theorem 1.3 *For each positive integer m, there exits a difference cover with parameters $(m(m+1), m^2, m(m-1))$ in an abelian group.*

Theorem 1.4 *If there exits a cyclic $(v,k,2)$ difference cover, then $(v,k) = (3,3)$ or $(6,4)$.*

Remark: The construction of Theorem 1.3 is straightforward, but the proof of Theorem 1.4 is quite complicated.

We now give an example of a difference list which is not a difference cover. Take, for instance $G = Z_7 =< g >$ and $D = 2 + g + g^2 + g^4$. It is easy to check that D is a difference list, but not a difference cover.

2 Preliminaries

Let R be a commutative ring with unity 1 and G a group. We let RG denote the group ring of G over R. We identify each subset S of G with the group ring element $\sum_{x\in S} x$. For $A = \sum_{g\in G} a_g g \in RG$ and any integer t, we define $A^{(t)} = \sum_{g\in G} a_g g^t$. With these notations "the difference cover" condition for a multiset D of G becomes

$$DD^{(-1)} = ke + \lambda G \tag{1}$$

in ZG. Let G be a finite abelian group of exponent m. A character χ of G is a homomorphism of G into the multiplicative group of complex mth roots of unity. It is well known that the characters of G form a group G^* (called the character group of G) that is isomorphic to G. The identity element of G^* is the principal character χ_0 that maps each element of G to 1. The characters of G can be extended by linearity to the group ring $Z[G]$

$$\chi(\sum_{x\in G} a_x x) = \sum_{x\in G} a_x \chi(x).$$

Thus each character of G yields a ring homomorphism from $Z[G]$ into the ring of algebraic integers in the cyclotomic field obtained by adjoining a primitive mth root of unity to the field Q of rational numbers. We let ζ_m denote the complex mth root of unity $e^{2\pi i/m}$.

It is easy to show that D is a (v,k,λ) difference cover if and only if

$$|\chi(D)|^2 = \begin{cases} k^2 = k + \lambda v & \text{if } \chi = \chi_0 \\ k & \text{if } \chi \neq \chi_0. \end{cases} \tag{2}$$

Proposition 2.1 *If D is a (v,k,λ) difference cover in an abelian group then $k(k-1) = \lambda v$.*

Proof Apply χ_0 to both sides of equation (1) above.

Proposition 2.2 *Let D be a (v, k, λ) difference cover in an abelian group G. Let N be any subgroup of G of order n. Let $\sigma : G \rightarrow G/N$ be the canonical homomorphism. Then $\sigma(D)$ is a $(v/n, k, \lambda n)$ difference cover in G/N.*

Proof Apply σ to both sides of equation (1).

The following is a Bruck-Ryser-Chowla type theorem for difference covers. It follows from adapting the proof of Theorem 2.1 in Lander [16], for example.

Theorem 2.3 (Bruck-Ryser-Chowla) *Let D be a (v, k, λ) difference cover in an abelian group G.*

1. *If v is even then k is a perfect square.*
2. *If v is odd then there exist integers x, y, z not all zero such that $x^2 = ky^2 + (-1)^{(v-1)/2}\lambda z^2$.*

Remarks:

- Part 1 of Theorem 2.3 follows from equation (1) by applying a character of order 2.
- Part 2 is essentially contained in Hall and Ryser [11].

Let G be an abelian group of order v and N any subgroup of order n. Let $G/N = \{N_0, N_1, ..., N_{m-1}\}$ be all the cosets of N in G, where $m = v/n$. For any subset S of G define $s_i = |S \cap N_i|$ for $i = 0, 1, ..., m-1$. The numbers $(s_0, s_1, ..., s_{m-1})$ are called the intersection numbers of S relative to N.

Proposition 2.4 *Let D be a difference cover with parameters (v, k, λ) in an abelian group G of order v. Suppose H is any normal subgroup of G of order n and index m. Let $H_1, H_2, ..., H_m$ be all the distinct cosets of H in G. Let $s_i = |D \cap H_i|$ then $\sum s_i = k$ and $\sum s_i^2 = k + \lambda|H|$.*

Proof Let $D = (a_1, a_2, ..., a_k)$ where all a_i need not be distinct. Let $\sigma : G \rightarrow G/H$ be the natural homomorphism. Let $\sigma(D) = \sum s_i g_i$ where all g_i's are distinct elements in the quotient group G/H. Then obviously $\sum s_i = k$ since D has size k. Also $\sigma(D).\sigma(D)^{-1} = ke + \lambda|H|G/H$. Now comparing the coefficients of identity in G/H we get $\sum s_i^2 = k + \lambda|H|$

Corollary 2.5 *If we take $H = \{e\}$ then we get the following result. If $D = \sum s_i g_i$ with all g_i's distinct then $\sum s_i = k$ and $\sum s_i^2 = k + \lambda$.*

Corollary 2.6 *Let D be a (v, k, λ) difference cover in an abelian group G, then λ must be even.*

Proof From Corollary 2.5 we get $\sum[s_i^2 - s_i] = \lambda$ and so λ is even.

Let p be a prime and w be an integer. Write $w = p^s w'$ where $s \geq 0$ and w' is co-prime to p. Then p is said to be *self conjugate modulo w* if there is an interger r

such that $p^r \equiv -1 \pmod{w'}$. An integer m is said to be self conjugate modulo w if all its prime divisors are. Self conjugacy is important because complex conjugation fixes all the ideals dividing the ideal (m) in the ring of integers of the cyclotomic field $Q(\zeta_w)$ if and only if m is self conjugate modulo w. This allows us to infer divisibility information about the algebraic integer $\chi(D)$ given similar information about the algebraic integer $\chi(D)\overline{\chi(D)}$.

The following is similar to Lemma 1.2 of Arasu and Sehgal [2].

Proposition 2.7 *Let D be a (v, k, λ) difference cover in an abelian group G. Assume there exists a prime p such that*

1. *$p^{2r} | k$ for some positive integer r, and*

2. *p is self conjugate modulo exponent of G*

Then $\chi(D) \equiv 0$ (mod p^r) for all nonprincipal characters of G.

3 New Constructions

Proposition 3.1 *There exists a difference cover with parameters $(m(m-1), m^2, m(m+1))$ in any abelian group of order $m(m-1)$.*

Proof Let $D = me + G$. We assert that D is a difference cover with the required parameters. We prove this statement using characters.

1. If χ is a non principal character of G, then $\chi(D) = m$

2. If χ_0 is the principal character then $\chi_0(D) = m + m^2 - m = m^2$.

The following is a different construction of a difference cover with the same parameters as in Proposition 3.1, when m is odd.

Proposition 3.2 *Let G be an abelian group of order $m(m-1)$ with m odd, then there exists a difference cover with parameters $(m(m-1), m^2, m(m+1))$ namely: Let P be a subgroup of G of order m, H a subgroup of G of order $m-1$, K a subgroup of H of order 2. Let K be generated by the involution k, then $D = me + 2Pk + P(H-K)$ is a difference cover with the above parameters.*

Proof If χ is the principal character of G then $\chi(D)$ = size of $D = m^2$. For χ a non-principal character of G, the following cases arise:

1. $\chi|P$ is non principal. Then $\chi(D) = m$

2. $\chi|P$ is principal.

    (a) If $\chi|K$ is non principal then $\chi(k) = -1, \chi(H) = 0, \chi(K) = 0$ so $\chi(D) = m - 2m = -m$

(b) $\chi|K$ is principal. Then χ cannot be principal on H. (For otherwise, χ will be principal on G). Hence $\chi(D) = m + 2m + m(0 - 2) = m$.

Proposition 3.3 *Let E be a (v, k, λ) difference set in an abelian group G. Suppose $k - \lambda$ divides k. Let $a = \frac{k}{k-\lambda}$. Then $D = aE$ is a $(v, ak, a^2\lambda)$ difference cover in G.*

Proof

$$\begin{aligned} DD^{(-1)} &= a^2EE^{-1} \\ &= a^2[(k-\lambda) + \lambda G] \\ &= a^2[k/a + \lambda G] \\ &= ak + \lambda a^2 G \end{aligned}$$

Since $\chi_0(D) = ak$, the result follows.

Corollary 3.4 *Let E be any $(4t-1, 2t, t)$ difference set in an abelian group G, then $D = 2E$ is a difference cover in G with parameters $(4t-1, 4t, 4t)$.*

Proof Follows immediately from Proposition 3.3.

Remarks: Corollary 3.4 provides many examples of difference covers since the required difference sets with Paley parameters $(4t-1, 2t, t)$ exist in abundance e.g. see Beth et al. [3].

Proposition 3.5 *If p^n is congruent to 3 mod 4 and D is a skew Hadamard difference set with parameters $(p^n, (p^n-1)/2, (p^n-3)/4)$ then $E = 1 + 2D$ is a difference cover with parameters $(p^n, p^n, p^n - 1)$*

Note: D is a skew Hadamard means $D + D^{(-1)} + 1 = G$ in $Z[G]$.

Proof

$$\begin{aligned} (1+2D)(1+2D)^{-1} &= 1 + 2(D + D^{-1}) + 4DD^{-1} \\ &= 1 + 2(G-1) + 4[(p^n+1)/2 + (p^n-3)/4G] \\ &= p^n + G(p^n - 1). \end{aligned}$$

Since $\chi_0(E) = 1 + 2\chi_0(D) = p^n$, the result follows.

Remark: The above construction works only for Skew Hadmard Payley difference sets; as we can see from its proof, D must satisfy $D + D^{(-1)} = G - 1$. These have been classified by Camion and Mann [6].

Remark: If D is a Payley difference set with parameters $(p^n, (p^n-1)/2, (p^n-3)/4)$ with p^n is congruent to 3 mod 4 then $E = (a + bD)$ is a difference cover ifand only if $a = 1$ and $b = 2$.

Proof

$$\begin{aligned} EE^{(-1)} &= (a+bD)(a+bD^{(-1)}) \\ &= a^2+ab(G-1)+b^2[(p^n+1)/4+((p^n-3)/4)G] \end{aligned}$$

E is a difference cover if and only if $EE^{(-1)} = (a+b(\frac{p^n-1}{2}))+\mu G$ for some integer μ. Now compare the above two expressions of $EE^{(-1)}$ and obtain:

$$a+b(p^n-1)/2 = a^2-ab+b^2(p^n+1)/4$$
$$a-b/2+p^n(b/2-b^2/4) = a^2-ab+b^2/4 = (a-b/2)^2.$$
$$x^2-x = p^n(\frac{b}{2}-\frac{b^2}{4}), \text{ where } x = a-\frac{b}{2}$$

1. If $b=1$ then we get
$$a-\frac{1}{2}+p^n(\frac{1}{4}) = (a-\frac{1}{2})^2$$
$$4a-2+p^n = 4a^2-4a+1$$
$$p^n = 4a^2-8a+3 = (2a-1)(2a-3)$$
$$\Rightarrow 2a-3 = 1 \Rightarrow a = 2 \text{ and } b = 1$$

2. If $b \geq 2$ then $x^2-x \leq 0 \Rightarrow x(x-1) < 0 \Rightarrow 0 \leq x \leq 1 \Rightarrow 0 \leq a-\frac{b}{2} \leq 1 \Rightarrow$
$$2a-b = \begin{cases} 0 \\ 1 \\ 2 \end{cases}$$

If $2a-b=0$, we get $x=0$ and hence $\frac{b}{2}=\frac{b^2}{4}$, showing $b=2$ and hence $a=1$. If $2a-b=1$ the equation $p^n(\frac{b}{2}-\frac{b^2}{4}) = \frac{-1}{4}p^n(2b-b^2) = -1$, a contradiction . If $2a-b=2$, then $x=1$ and hence $\frac{b}{2}=\frac{b^2}{4}$, showing $b=0$ and $a=1$ (on $b=2$ and $a=0$).

Theorem 3.6 *Let p^n be any prime power congruent to 1 mod 4, then there exists a difference cover with parameters (p^n, p^n, p^n-1)*

Proof Let E(resp. $E^{'}$) be the set of all nonzero squares (resp. nonsquares) in the finite field of order p^n. Let $D = 1+2E$, then we assert that D is a difference cover with parameters (p^n, p^n, p^n-1). We know that E is a partial difference set (for more on partial difference sets, see Ma [17]) with parameters $(p^n, (p^n-1)/2, (p^n-5)/4, (p^n-1)/4)$ and $E = E^{(-1)}$. So

$$\begin{aligned} DD^{(-1)} &= 1+4E^2+4E \\ &= 1+4[(p^n-1)/2+((p^n-5)/4)E+((p^n-1)/4)E^{'}]+4E \\ &= 1+4[(p^n-1)/2+(p^n-1)/4E+((p^n-1)/4)E^{'}] \\ &= 1+2(p^n-1)+(p^n-1)[E+E^{'}] \\ &= 2p^n-2+1+(p^n-1)[E+E^{'}] = p^n+(p^n-1)G \end{aligned}$$

Remark: If p is a prime congruent to 1 mod 4 and D is any difference cover with parameters $(p, p, p-1)$ then D must be as in the above construction. We use the following well-known result to prove this remark.

Result 3.7 (Ireland, Rosen [12], Chapter 6) *Let p be a prime and $A \in X[H]$ be an element in the integral group ring over the cyclic group $H =< h >$ of order p. Then $\chi(A)\overline{\chi(A)} = p$ for all complex characters $\chi \neq \chi_0$ if and only if there exists a suitable translate Ag of A with*

$$Ag = xH + \sum_{i=0}^{p-1} (\frac{i}{p}) h^i$$

for some integer x. The integer x can be determined from the principal character value $\chi_0(A)$ (we have $\chi_0(A) = xp$). (Here $(\frac{i}{p})$ is the so called ***Legendre symbol****: It is 0, 1 or -1 depending on whether i is 0, a square or a non-square modulo p.)*

Theorem 3.8 *If p is a prime, $p \equiv 1$ mod 4 and D is any-difference cover with parameters $(p, p, p-1)$, then D must be equal to $1 + 2E$ where E is the set of all quadratic residues mod p. (See constructions as in Theorem 3.6)*

Proof Let $D = \sum_{i=0}^{p-1} s_i g^i$; then

$$\sum_{i=0}^{p-1} s_i = p$$

$$DD^{(-1)} = p + (p-1)G$$

$$\chi(DD^{(-1)}) = p \; \forall \; \chi \neq \chi_0$$

so by result 3.7, we see that

$$s_i = \begin{cases} x & \text{when } i = 0 \\ x+1 & \text{when } (\frac{i}{p}) = 1 \\ x-1 & \text{when } (\frac{i}{p}) = -1 \end{cases} \tag{3}$$

Thus $x + (\frac{p-1}{2})(x-1) + (\frac{p-1}{2})(x+1) = \sum_{i=0}^{p-1} s_i = p$ showing $x = 1$ and $D = 1 + 2E$ as asserted.

Lemma 3.9 *If D is a (v, k, λ) difference cover in an abelian group G and $E = G - D$ is a difference cover in G then $v = 2k$.*

Proof

$$EE^{(-1)} = (G - D)(G - D^{(-1)}) = vG - 2kG + k + \lambda G \tag{4}$$

By definition of difference cover,

$$EE^{(-1)} = (v - k) + \lambda G \tag{5}$$

Compare (4) and (5) to get the result.

4 Nonexistence Results

Theorem 4.1 *Suppose that there exists a (v, k, λ) difference cover D in an abelian group G. Assume that $p^2|k$ for some prime p. If $p|v$ and if the sylow p-subgroup of G is cyclic, then $p|\lambda$.*

Proof Suppose that $p|v$ and let S be the sylow p-subgroup of G of order p^α, write $G = ST$ for some subgroup T of G. By Proposition 2.2, $E = D^\sigma$, the image of D under $\sigma : G \to G/T$ is the canonical homomorphism, is a $(p^\alpha, k, v/p^\alpha\lambda)$ difference cover in S. Since p is self conjugate modulo $|S|$, by Proposition 3.4, it follows that $\chi(E) \equiv 0 \pmod p$, (since $p^2|k$) for all nonprincipal characters χ of S. So by Ma's Lemma, $E = px + < g > y$, where $o(g) = p$, $g \in S$ and x, $y \in ZS$. Therefore $E(1 - g) \equiv 0 \pmod p$. Thus the coefficients of E satisfy:

$$a_{h^j} \equiv a_{h^j g^i} \text{ (mod p) for all } i = 0, ..., p-1 \;\&\; j = 0, 1, ..., p^\alpha - 1 \tag{6}$$

where $E = \sum_{j=0}^{p^\alpha} a_{h^j} h^j$, $S = \langle h \rangle$. We have

$$\sum_j a_{h^j} = k \text{ and } \sum_j a_{h^j}^2 = k + (v/p^\alpha)\lambda \tag{7}$$

Use of (6) and (7) imply that $p \mid \frac{v}{p^\alpha}\lambda$ and hence $p \mid \lambda$.

Proposition 4.2 *If there exists a $(m, m, m-1)$ difference cover in a cyclic group of odd order m, then $(\frac{(-1)^{\frac{(m-1)}{2}}(m-1)}{p}) = 1$ for all primes p.*

Proof In view of Theorem 4.1, we can assume that m is squarefree, now we apply Bruck-Ryser theorem to conclude that there exist integers x, y, z, not all zero, such that

$$x^2 = my^2 + (-1)^{\frac{(m-1)}{2}}(m-1)z^2 \tag{8}$$

Now let p be any prime dividing m, we can assume without loss of generality, that p not divides x (and hence p not divides z). So, (8) when read modulo p, gives $(\frac{(-1)^{\frac{(m-1)}{2}}(m-1)}{p}) = 1$,as desired.

Remarks: Proposition 4.2 also holds in general abelian groups, if we assume that for the prime p in question, the Sylow p-subgroup is cyclic.
Application: $(21, 21, 20)$ difference covers do not exist.

Proof Follows from Proposition 4.2, by taking $p = 3$, since $(\frac{(-1)^{\frac{(m-1)}{2}}(m-1)}{3}) = \frac{20}{3} = -1$.

Corollary 4.3 *Cyclic difference covers with parameters $(m^2(m \pm 1), m^2, m \mp 1)$ do not exist.*

Proof Immediate from Theorem 4.1.

Corollary 4.4 (m^2, m^2, m^2-1) *difference covers do not exist.*

Proof Follows from Theorem 4.1.

Corollary 4.5 $(\frac{m^2(m+1)}{t}, m^2, t(m-1))$ *cyclic difference covers do not exist for all* t *dividing* $(m+1)$.

Proof Follows from Theorem 4.1.

Remarks: Corollary 4.5 shows that the cyclic difference covers $(m(m+1), m^2, m(m-1))$, in Theorem 1.3, do not extend to parameters as given in corollary 4.5.

The following result is a straight forward generalitation of the so-called Mann's test (See **Jungnickel and Pott [15]**), for instance,

Theorem 4.6 (Jungnickel and Pott) *Let* D *be a* (v, k, λ)*-difference cover 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* $tp^f \equiv -1 \bmod u^*$ *for some numerical* G/U*-multiplier* t *of* D *and a suitable non-negative integer* f*. Then the following hold:*

1. p does not divide the square-free part of k, say $p^{2j} \parallel k$ (where $j \geq 0$);
2. $p^j \leq v/u$.

Application: $(105, 21, 4)$ difference covers do not exist.

Proof Take $p = 3, |U| = 15, H = Z_7, u^* = 7, t = 1, f = 3$ in Theorem 4.6.

We finally wish to mention that Schmidt's results in his recent work([18], [19]) (also see Chapter 6 of [3]), carry over to difference covers in a very straightforward manner.

References

[1] K.T. Arasu and D.K. Ray-Chaudhuri, Multiplier theorem for a difference list, *Ars Combin.* **22** (1986), 119–137.

[2] K.T. Arasu and S.K. Sehgal, Difference sets in abelian groups of p-rank two, *Designs, Codes Crypt.* **5** (1995), 5–12.

[3] T. Beth, D. Jungnickel and H. Lenz, *Design theory (2nd edition)*, Cambrige University Press (1999).

[4] T. Bier(Personal Communication)

[5] M. Buratti, Old and new designs via difference multisets and strong difference families, *J. Combin. Des.* **7** (1999), 406–425.

[6] P. Camion and H.B. Mann, Antisymmetric difference sets, *J. Number Th.* **4** (1972), 266–268.

[7] C.J. Colbourn and A.C.H. Ling, Quorums from difference covers, *Inform. Process. Lett.* **75** (2000), 9–12.

[8] D. Connolly, Integer difference covers which are not k-sum covers, for $k = 6, 7$, *Proc. Cambridge Philos. Soc.* **74** (1973), 17–28.

[9] D.M. Connolly and J.H. Williamson, Difference-covers that are not k-sum-covers II, *Proc. Cambridge Philos. Soc.* **75** (1974), 63–73.

[10] J.A. Haight, Difference covers which have small k-sums for any k, *Mathematika* **20** (1973), 109–118.

[11] M. Hall and H.J. Ryser, Cyclic Incidence Matrices, *Canadian J. Math.* **3** (1951), 495–502.

[12] K. Ireland and M. Rosen, "A Classical Introduction to Modern Number Theory", Springer, New York (1982).

[13] T.H. Jackson and F. Rehman, Note on difference-covers that are not k-sum-covers, *Mathematika* **21** (1974), 107–109.

[14] T.H. Jackson, J.H. Williamson and D.R. Woodall, Difference-covers that are not k-sum-covers I, *Proc. Cambridge Philos. Soc.* **72** (1972), 425–438.

[15] D. Jungnickel and A. Pott, Two results on difference sets, *Coll. Math. Soc. Janos Bolyai* **52** (1988), 325–330.

[16] E.S. Lander, *Symmetric Designs: An algebraic approach*, Cambridge University Press, Cambridge, 1983.

[17] S.L. Ma, *Polynomial addition sets*, Ph.D. Thesis, University of Hong Kong, 1985.

[18] B. Schmidt, Cyclotomic integers of prescribed absolute value and the class group, *J. Number Theory* **72** (1998), 269–281.

[19] B. Schmidt, Cyclotomic intergers and finite geometry, *J. Amer. Math. Soc.* **12** (1999), 929–952.

[20] R.J. Turyn, Character sums and difference sets, *Pacific J.Math.* **15** (1965), 319–346.

[21] D. Wiedemann, Cyclic difference covers through 133, Proc. Twenty-third Southeastern Internat. Conf. Combinatorics, Graph Theory, and Computing (Boca Raton, FL, 1992). *Congr. Numerantium* **90** (1992), 181–185.

(Received 28 Sep 2003; revised 23 Apr 2004)