KYUNGPOOK Math. J. 45(2005), 137-152

Regular Difference Covers

K. T. Arasu
Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435, U.S.A.
e-mail : karasu@math.wright.edu

Ashwani K. Bhandari
Centre for Advanced Study in Mathematics, Panjab University, Chandigarh - 160014, India
e-mail : akb@pu.ac.in

Siu-Lun Ma
Department of Mathematics, National University of Singapore, Singapore 119260, Republic of Singapore
e-mail : matmasl@nus.edu.sg

Surinder Sehgal
Department of Mathematics, Ohio State University, Columbus, Ohio 43210, U.S.A.
e-mail : sehgal@math.ohio-state.edu

Abstract. We introduce the concept of what we call "regular difference covers" and prove many nonexistence results and provide some new constructions. Although the techniques employed mirror those used to investigate difference sets, the end results in this new setting are quite different.

1. Introduction

Let G be any finite abelian group of order v. Let $D = \{x_1, \cdots, x_k\}$ be a multiset of elements from G (not all elements distinct). A difference of these elements is called non-trivial if and only if it is of the form $x_i - x_j$, for $i \neq j$, otherwise trivial. In particular the identity element 0 occurs exactly k times as a trivial difference but it can also be a non-trivial difference, if some of the elements of D are equal.

Definition 1.1. A multiset $D = \{x_1, \cdots, x_k\}$ is called a regular 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 non-trivial difference, i.e., $z = x_i - x_j$, $i \neq j$,

Received February 3, 2004, and, in revised form, April 6, 2004.
2000 Mathematics Subject Classification: 05B10.
Key words and phrases: difference set, difference cover.
Research supported by NSA and NSF grants.

of elements of D.

It may be observed that if the requirement "non-trivial" is omitted in the above definition, i.e., if every element $z \in G$ appears exactly λ times as a difference, i.e., $z = x_i - x_j$ for any i and j, of elements of G, then it follows from the orthogonality relations of characters of the group G that D must necessarily be a union (as multiset) of the whole group G a certain number of times. The above notion of regular difference covers differ from that of difference sets or difference lists in the requirement that the non-trivial differences cover all the non-identity elements of G a constant number of times in the difference sets or difference lists. However, in regular difference covers they cover all elements of G including the identity a constant number of times. For instance, for $G = \mathbb{Z}_7 = \langle g \rangle$, the list (multiset) $\{e, e, g, g^2, g^4\}$ can easily be checked to be a difference list but is not a regular difference cover. See, for example, [4] for difference sets and [1] for difference lists.

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) and the main object was to find minimal size of D covering all of G as a list of differences. See, for example, [7], [16], [9], [12], [11], [8], [13].

While this work is motivated by the work of T. Bier [5] and [3], 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 [6] in which he has introduced the notion of '1-difference multiset.' This concept coincides with what we call here 'regular difference cover.' We wish to promote our nomenclature. Our reasons are two-fold: (1) The phrases '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 [6], 'regular difference covers' and their 'family' analogs (so-called strong difference families) have applications in the construction of BIBD's and GDD's. We also wish to mention in passing that some of our regular difference sets 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, 'regular difference covers' have immediate applications to related areas in discrete mathematics. The overlap of our results with those of Burratti [6] is very minimal. His results focus mainly around objects of the type aD and $ae + bD$, for suitable choices of difference sets (or partial difference sets), but our go a step further and investigate objects of the type $aD + b(G - D)$, thereby producing new families. Buratti's methods are completely combinatorial, but we adhere to the use of group rings, character theory and representation 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' in here - the slight change in the definition (from 'difference set' to 'regular 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. (For example, the parameter λ in our study is necessarily even, in contrast to the difference sets. Proposition 2.10 has no "difference set" analog. Constructions in section 3 also look very different.)

In [3], the approach of using group rings and characters was followed and some basic properties of regular difference covers were established. In this paper we study multiplier theorems for regular difference covers, give their applications, characterize all possible regular difference covers with $\lambda = 2$ and also construct several new infinite families of regular difference covers.

We shall now give some preliminaries and also fix notations. Let R be a commutative ring with unity 1 and let G be a group. We let RG denote the group ring of G over R. We identify each multiset S of elements of G with the group ring element $\sum_{g\in G} s_g g$, where s_g denotes the multiplicity (possibly zero) with which the element g appears in S.

The homomorphism $\varepsilon : RG \to R$, given by $\varepsilon(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g$ is called the augmentation mapping of RG and its kernel, denoted by $\Delta_R(G)$, is called the augmentation ideal of RG. By [15, Proposition 3.2.10], the set $\{g-1 | g \in G, g \neq e\}$ is a basis of $\Delta_R(G)$ over R.

For $A = \sum_{g\in G} a_g g \in RG$ and for any integer t, we define $A^{(t)} = \sum_{g\in G} a_g g^{(t)}$. With these notations, it follows that a multiset D of G is a regular difference cover with parameters (v, k, λ) if and only if

$$DD^{(-1)} = ke + \lambda G \tag{1.1}$$

in $\mathbb{Z}G$.

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 m^{th} roots of unity. It is well known that the characters of G form a group 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 $\mathbb{Z}G$. Thus each character of G yields a ring homomorphism from $\mathbb{Z}G$ into the ring of algebraic integers in the cyclotomic field obtained by adjoining a primitive m^{th} root of unity to the field $\mathbb{Q}$ of rational numbers. We let ζ_m denote the complex m^{th} root of unity $e^{2\pi i/m}$.

It is easy to see that D is a (v, k, λ) regular difference cover in an abelian group G if and only if

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

and that if D is a (v, k, λ) regular difference cover, then $k(k-1) = \lambda v$.

Let G be a finite abelian group and let N be a normal subgroup of order n of G. Let $\sigma : G \to G/N$ be the natural homomorphism. Then applying σ on both sides of equation 1.1, we obtain the following Proposition, which will be used often.

Proposition 1.2. *Let D be a (v, k, λ) regular difference cover in an abelian group G. Then $\sigma(D)$ is a $(v/n, k, n\lambda)$ regular difference cover in G/N.*

Remark 1.3. Let $D = \sum_{i=1}^{v} s_i\, g_i,\ s_i \geq 0$, be a regular difference cover with parameters (v, k, λ) in an abelian group $G = \{g_1 = e,\ g_2, \cdots, g_v\}$. Then $\sum_{i=1}^{v} s_i = k$. Also, the identity element e is represented as a non-trivial difference exactly $\sum_{i=1}^{v} s_i(s_i - 1)$ times. It follows that $\sum_{i=1}^{v} s_i(s_i - 1) = \lambda$ and hence $\sum_{i=1}^{v} s_i^2 = k + \lambda$. These conditions will be used later.

2. Multiplier theorems

Multipliers for regular difference covers can be defined as in the case of difference sets, namely:

Definition 2.1. Let D be a (v, k, λ) regular difference cover in an abelian group G. An automorphism σ of G is said to be a multiplier of D if $\sigma(D) = D + g$, for some $g \in G$. An integer t, relatively prime to the order of G, is said to be a numerical multiplier, if the automorphism $\sigma : x \mapsto tx$ is a multiplier of D.

We now prove a multiplier theorem for regular difference covers. The proof is similar to the proof of Theorem VI.4.6 of [4], which we give below for the sake of completeness.

Theorem 2.2. *Let D be a (v, k, λ) regular difference cover in an abelian group G such that $(v, k) = 1$. Let t be an integer such that $t \equiv p^f \pmod{v^*}$ for some f, for every prime divisor p of k, where v^* is the exponent of G. Then t is a numerical multiplier for D (it follows that $(t, v) = 1$).*

Proof. We first claim that $D^{(t)}D^{(-1)} \equiv \lambda G \pmod{k}$. For this, it is sufficient to show that $D^{(t)}.D^{(-1)} \equiv \lambda G \pmod{q^a}$, for every prime divisor q of k such that $k = q^a k'$, $(k', q) = 1$. Suppose not; then $D^{(t)}.D^{(-1)} - \lambda G = q^b.B$, where $B \in \mathbb{Z}G$, $B \not\equiv 0 \pmod{q}$ and $b < a$. Suppose that e is the smallest positive integer such that $t^e \equiv 1 \pmod{v^*}$. Now $D^{(t^e)} = D$ and hence

$$\begin{aligned} & (D^{(t)}D^{(-1)} - \lambda G)(D^{(t^2)}D^{(-t)} - \lambda G^{(t)}) \cdots (D^{(t^e)}D^{(-t^{e-1})} - \lambda G^{(t^{e-1})}) \\ \equiv\ & (DD^{(-1)})(D^{(t)}D^{(-t)}) \cdots (D^{(t^{e-1})}D^{(-t^{e-1})}) \pmod{G} \\ \equiv\ & k^e \pmod{G}, \end{aligned}$$

as $(D^{(t^r)}D^{(-t^r)}) = ke + \lambda G$, and $0 \leq r \leq e-1$. Thus $(D^{(t)}D^{(-1)} - \lambda G)(D^{(t^2)}D^{(-t)} - \lambda G^{(t)}) \cdots (D^{(t^e)}D^{(-t^{e-1})} - \lambda G^{(t^{e-1})}) = k^e + \beta G = k^e + \alpha G$, where $\beta \in \mathbb{Z}G$, $\alpha \in \mathbb{Z}$. Also, $\varepsilon(D^{(t)}D^{(-1)} - \lambda G) = k^2 - \lambda v = k$, where $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ is the augmentation homomorphism. Hence, from above, $k^e = k^e + \alpha v$, so that $\alpha = 0$. Thus

$$(D^{(t)}D^{(-1)} - \lambda G)(D^{(t^2)}D^{(-t)} - \lambda G^{(t)}) \cdots (D^{(t^e)}D^{(-t^{e-1})} - \lambda G^{(t^{e-1})}) = k^e.$$

Hence

$$q^{eb}B.B^{(t)}\cdots B^{(t^{e-1})} = k^e = q^{ea}(k^{'})^e$$

implies that $B.B^{(t)}\cdots B^{(t^{e-1})} \equiv 0 \pmod{q}$. But $t \equiv q^f \pmod{v^*}$, implies that $B^{(t^r)} = B^{(q^{fr})} \equiv B^{q^{fr}} \pmod{q}$, by [4, Lemma VI.3.7]. Thus, $B.B^{q^f}\cdots B^{qf(e-1)} = B^{1+q^f+\cdots+q^{f(e-1)}} \equiv 0 \pmod{q}$ and hence $B \equiv 0 \pmod{q}$, by [4, Lemma 6.3.7], which is a contradiction. Thus $D^{(t)}D^{(-1)} = kQ + \lambda G$, $Q \in \mathbb{Z}G$. Multiplying both sides by D, we get $D^{(t)}(ke + \lambda G) = kQD + \lambda GD$, so that

$$D^{(t)} = DQ, \tag{2.1}$$

as $GD = GD^{(t)} = kG$. Taking augmentation on both sides, $k = \varepsilon(D^{(t)}) = k\varepsilon(q)$, so that $\varepsilon(Q) = 1$ and hence $Q-1 \in \Delta_{\mathbb{Z}}(G)$. It follows that $(Q-1)G = 0$, i.e., $QG = G$ and also $Q^{-1}G = G$. By (2.1), $D^{(-t)} = D^{(-1)}Q^{(-1)}$ and on multiplying $D^{(t)}$ and $D^{(-t)}$, we get $ke + \lambda G = (ke + \lambda G)QQ^{(-1)}$, i.e., $ke = kQQ^{(-1)}$, i.e., $QQ^{(-1)} = e$. If $Q = \sum_{g\in G} q_g g$, then $e = QQ^{(-1)}$ implies that $\sum_{g\in G} q_g^2 = 1$ and hence $Q = g$ for some $g \in G$. Thus, $D^{(t)} = D.g$, $g \in G$, so that t is a multiplier. □

Remark 2.3. In fact one can show that if D is a regular difference cover with parameters (v, k, λ) and if p is a prime divisor of k such that $(p, v) = 1$ and $p > \lambda$, then p is a multiplier for D. However, if $k = p^a k^{'}$, $(p, k^{'}) = 1$, then $\lambda = p^a k^{'}(p^a k^{'} - 1)/v$ and hence $\lambda \geq p^a$. Thus, such a p does not exist. Also, it is possible to prove a multiplier theorem for regular difference covers, similar to McFarland's multiplier theorem for difference sets ([4, Theorem VI.4.10]), but Theorem 2.2 above is most suitable for applications.

Remark 2.4. Let $G = \langle g \rangle$ be the cyclic group of order 11. Then $D = 2e + 2g^2 + 2g^6 + 2g^7 + 2g^8 + 2g^{10}$ is easily seen to be a regular difference cover in G with parameters $(11, 12, 12)$. One can check that 3 is a multiplier for D but the prime 2 is not a multiplier for D. However, $(11, 12) = 1$ and $2|12$. Thus, every prime divisor of k need not be a multiplier for regular difference covers with parameters (v, k, λ). Therefore, a conjecture like the "multiplier conjecture for difference sets" is not feasible for regular difference covers.

Let G be a finite abelian group of order v. Recall that G is a basis of $\mathbb{Z}G$ over $\mathbb{Z}$. We enumerate the elements of G in some order : $G = \{e = g_1, \cdots, g_v\}$. The regular representation $\varrho : G \to GL(\mathbb{Z}G)$ is defined by assigning for every $g \in G$, the linear mapping ϱ_g which acts on the above basis by multiplication, i.e., $\varrho_g(g_i) = gg_i$. The matrix corresponding to ϱ_g with respect to the above fixed basis is a permutation matrix and hence the matrix corresponding to $\varrho_{g^{-1}}$ is the transpose of the matrix corresponding to ϱ_g. We thus get a homomorphism $\varrho : G \to GL(v, \mathbb{Z})$. Extending ϱ by linearity to $\mathbb{Z}G$, we get the regular representation $\varrho : \mathbb{Z}G \to M_{v\times v}(\mathbb{Z})$.

Definition 2.5. Let D be a (v, k, λ) regular difference cover in an abelian group G. Let M be the matrix of the regular representation of $D \in \mathbb{Z}G$ (having fixed the enumeration $G = \{e = g_1, \cdots, g_v\}$ of elements of G). We shall call M to be an

"incidence matrix" of D.

Remark 2.6. Since the inverse of a permutation matrix is its transpose, from the identity $DD^{(-1)} = ke + \lambda G$, it follows that $MM^T = kI_{v\times v} + \lambda J$, where $I_{v\times v}$ is the identity matrix of size v and J is the $v \times v$ matrix with all entries 1.

As in the proof of Lemma II. 2.3 of [4], it follows that MM^T has one eigenvalue k^2 and $v-1$ eigenvalues k. Thus $\det MM^T = k^{v+1}$ and that M is non - singular.

Let t be a numerical multiplier of a regular (v, k, λ) difference cover D in an abelian group G. Then $D^{(t)} = Dg_i$ for some $g_i \in G$ and $\varrho(D^{(t)}) = \varrho(Dg_i) = \varrho(D)\varrho(g_i) = MQ$, where Q the permutation matrix $\varrho(g_i)$. On the other hand, for any $g_j \in G$, $(Dg_j)^{(t)} = D^{(t)}g_j^t = Dg_ig_j^t$. Since $g \mapsto g^t$ is an automorphism of G, it follows that this automorphism permutes the translates $D = Dg_1, Dg_2, \cdots, Dg_v$ (as $g \mapsto g_ig$ permutes elements of G). Thus, $\varrho(D^{(t)}) = PM$, for some permutation matrix P, and hence $M = P^{-1}MQ$. The number of fixed rows (respectively columns) of M, on multiplication by P^{-1} and Q respectively is the trace of P^{-1} (respectively the trace of Q). As M is non - singular, $Q = M^{-1}PM$ and trace Q = trace P = trace P^T = trace P^{-1}.Thus, the number of elements of G fixed by the automorphism $g \mapsto g^t$ is same as the number of translates Dg_i of D fixed by $g \mapsto g^t$. Since e is fixed, it follows that there exists at least one translate Dg_i which is fixed by the automorphism $g \mapsto g^t$. We have thus proved:

Proposition 2.7. *Let t be a numerical multiplier of an abelian (v, k, λ) regular difference cover D. Then there exists at least one translate Dg_i of D which is fixed by the automorphism $g \mapsto g^t$ of G, i.e., $(Dg_i)^{(t)} = Dg_i$.*

Remark 2.8. Using regular representations, one can prove the analogue of the result of McFarland and Rice for regular difference covers, on the lines of the proof of Theorem VI.2.6 of [4].

Remark 2.9. When considering a hypothetical abelian (v, k, λ) - regular difference cover, Proposition 2.7 and Remark 2.8 allow us to assume that D is fixed by every numerical multiplier. Hence D must then be the union (as a multiset) of (several copies of) orbits on G under any group $\mathcal{M}$ (usually a cyclic group) of numerical multipliers.

We shall now give some applications of the multiplier theorem for regular difference covers. However, we first Characterize all cyclic regular difference covers with parameters $(k(k-1)/2, k, 2)$, which, as claimed by Bier [5], exist if and only if $k = 3$ or $k = 4$. We have not been able to verify the details of his proof.

We first show:

Proposition 2.10. *Suppose that D is a cyclic regular difference cover with parameters $(v, k, 2)$. Then k is not divisible by square of any odd prime.*

Proof. Suppose that p is an odd prime such that $p^2|k$. As $v = \frac{k(k-1)}{2}$, $p|v$. Let S be the Sylow $p-$ subgroup of G of order p^a. Let $G = ST$ for some subgroup T of G. By Proposition 1.2, $E = \sigma(D)$, the image of D under $\sigma : G \to G/T$ is a

$(p^a, k, 2v/p^a)$ regular difference cover in S. Since p is self conjugate modulo $|S|$, by a result similar to Lemma 1.2 of [2], it follows that $\chi(E) \equiv 0 \pmod{p}$, for every non-principal character χ of S (as $p^2|k$). So, by Ma's Lemma, $E = pX + \langle g \rangle Y$, where order of g is p, $g \in S$ and $X, Y \in \mathbb{Z}S$. It follows that $EE^{(-1)} \equiv 0 \pmod{p}$ and as $EE^{(-1)} = ke + \frac{2v}{p^a}$, $p|\frac{2v}{p^a}$, which is not possible. Hence k is not divisible by the square of any odd prime. □

If v is even, applying the (real valued) character of order 2 to the equation $DD^{(-1)} = ke + \lambda G$, it follows that $k = (\chi(D))^2$ must be a perfect square. Thus, it follows that if D is a regular cyclic difference cover with parameters $(v, k, 2)$ and if v is odd, then k is a product of distinct primes. Also, in case v is even, k has to ve a perfect square and Proposition 2.10 implies that $k = 2^{2n}$ and $v = 2^{2n-1}(2^{2n} - 1)$.

A proof similar to that of Theorem VI.15.11 of [4] yields the following exponent bounds.

Theorem 2.11 (Turyn's Exponent Bound)**.** *Assume the existence of a (v, k, λ)-regular difference cover $D = \sum_{g \in G} s_g g$ in an abelian group G. Suppose that $T = \max_{g \in G} s_g$. Let p be a prime divisor of v and denote the Sylow $p-$subgroup of G by S. Let U be any subgroup of G with $U \cap S = \{e\}$ and assume that p^{2a} divides k for some $a \geq 1$. If p is self conjugate modulo the exponent of G/U, then exp $S \leq \frac{|U|}{p^a}|S|T$.*

Applying the above result to hypothetical cyclic regular difference cover with parameters $(2^{2n-1}(2^{2n} - 1), 2^{2n}, 2)$, one observes that as $\lambda = 2$, Remark 1.3 yields that $T = 2$. Hence, taking $U = \{e\}$, $2^{2n-1} \leq \frac{1}{2^n}.2^{2n-1}.2$, i.e., $2^{2n-1} \leq 2^n$, so that $n \leq 1$. Hence the only difference cover of this type would have parameters $(6, 4, 2)$. Combining all the above observations, we have:

Proposition 2.12. *If D is a regular difference cover with parameters (v, k, λ), then either $v = 6$, $k = 4$ or k is a product of different primes.*

In order to characterize all regular difference covers with parameters $(v, k, 2)$, we first prove:

Lemma 2.13. *Let $G = P \times H$ be an abelian group of order $v = pw$, where $P = \langle \alpha \rangle$, $o(\alpha) = p$, $|H| = w$, p is a prime and w is a positive integer relatively prime to p. Let t be an integer such that $t \equiv 1 \pmod{w}$ and $t \equiv 0 \pmod{p}$. Suppose there exists $D \in \mathbb{Z}G$ such that*

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

with $p|n$ and $p|\varepsilon(D)$. Then

$$D^{(t)}D^{(-1)} = pX$$

where $X \in \mathbb{Z}G$ satisfies $PX = \frac{n}{p}P + \lambda G$.

Proof. Note that $t \equiv p^j \bmod pw$ for some positive integer j. So

$$D^{(t)}D^{(-1)} \equiv D^{p^j}D^{(-1)} \equiv nD^{p^j-1} + \lambda\chi_0(D)^{p^j-1}G \equiv 0 \pmod{p},$$

i.e., $D^{(t)}D^{(-1)} = pX$ for some $X \in \mathbb{Z}G$.

Let $\rho : G \to H$ be the projection such that $\rho(\alpha) = 1$ and $\rho(h) = h$ for all $h \in H$. Since $\rho(D) = D^{(t)} = \rho(D^{(t)})$,

$$n + \lambda pH = \rho(D)\rho(D)^{(-1)} = \rho(D^{(t)}D^{(-1)}) = p\rho(X).$$

Thus $PX = \frac{n}{p}P + \lambda G$. □

Lemma 2.14. *With the notation and conditions of Lemma 2.13 above, suppose in addition that* $0 < \lambda < p$. *Then*

$$v \leq \frac{(n^2 + \lambda np)(p-1)}{\lambda p(p-\lambda)} + p.$$

Proof. Let $X = \sum_{i=0}^{p-1} \sum_{g \in H} a_{\alpha^i g} \alpha^i g$ where $a_{\alpha^i g}$ are integers. Since

$$p^2 X X^{(-1)} = D^{(t)}D^{(-t)}DD^{(-1)} = (n + \lambda pH)(n + \lambda G) = n^2 + \lambda npH + (\lambda n + \lambda^2 v)G,$$

we have

$$\sum_{i=0}^{p-1} \sum_{g \in H} a_{\alpha^i g}^2 = \frac{n^2 + \lambda np + \lambda n + \lambda^2 v}{p^2}.$$

By $PX = \frac{n}{p}P + \lambda G$, we have

$$\sum_{i=0}^{p-1} a_{\alpha^i g} = \begin{cases} \lambda & \text{if} g \neq 1 \\ \frac{n+\lambda p}{p} & \text{if} g = 1. \end{cases}$$

Note that

$$\sum_{i=0}^{p-1} a_{\alpha^i}^2 \geq \left(\frac{n + \lambda p}{p^2}\right)^2 p = \frac{n^2 + 2\lambda np + \lambda^2 p^2}{p^3}$$

and since $0 < \lambda < p$, for $g \neq 1$,

$$\sum_{i=0}^{p-1} a_{\alpha^i g}^2 \geq \lambda.$$

So

$$\lambda\left(\frac{v}{p} - 1\right) + \frac{n^2 + 2\lambda np + \lambda^2 p^2}{p^3} \leq \frac{n^2 + \lambda np + \lambda n + \lambda^2 v}{p^2}$$

and the lemma follows. □

We are now ready to show :

Theorem 2.15. *Cyclic* $(v, k, 2)$ *regular difference covers exist if and only if* $(v, k) = (3, 3)$ *or* $(6, 4)$.

Proof. By Proposition 2.12, either $v = 6$, $k = 4$ or k is a product of distinct primes. Suppose there exists a cyclic $(v, k, 2)$ difference cover with $k \geq 10$. Then $v = (k^2 - k)/2$. Let p be the largest prime divisor of k. Note that $p \geq 5$. By Lemma 2.14,

$$\begin{aligned} \frac{k^2 - k}{2} &\leq \frac{(k^2 + 2kp)(p-1)}{2p(p-2)} + p \qquad (*) \\ &< \frac{k^2 + 2kp}{2(p-2)} + p. \end{aligned}$$

This implies that

$$k < \frac{3p-2}{p-3} + \frac{2p(p-2)}{k(p-3)} \leq \frac{3p-2}{p-3} + \frac{2(p-2)}{p-3} = 5 + \frac{9}{p-3} \leq 9.5\ ,$$

which contradicts the assumption $k \geq 10$.

However, if $(v, k, 2)$ regular difference cover exists, then $k \leq 9$. Now, regular difference covers with parameters $(10, 5, 2)$ does not exist (5 is not a square) and one with parameters $(15, 6, 2)$ does not exist because the one with parameters $(3, 6, 10)$ does not exist (not possible to find s_i's with $s_1 + s_2 + s_3 = 6$, $s_1^2 + s_2^2 + s_3^2 = 16$). Also, $k = p = 7$, does not satisfy the inequality (*) above. Regular difference covers with parameters $(28, 8, 2)$ and $(36, 9, 2)$ do not exist as 8 is not a square and by Proposition 2.11 respectively. Thus, only choices left are $(3, 3, 2)$ and $(6, 4, 2)$ and one checks easily that regular difference covers with these parameters exist ($D = 1 + 2g$ for $(3, 3, 2)$ and $D = 2 + h + h^4$ for $(6, 4, 2)$). This completes the proof of Theorem 2.15. □

Having investigated regular difference covers with parameters $(k(k-1)/2, k, 2)$, we now turn to regular difference covers with parameters $((k-1)/2, k, 2k)$ and apply multiplier theorem. The multiplier Theorem 2.2 does not yield any any significant information about regular difference covers with parameters $((p-1)/2, p, 2p)$, where p is a prime; as even though p is a multiplier for the regular difference cover with parameters $((p-1)/2, p, 2p)$, but $p \equiv 1 \pmod{(p-1)/2}$ and hence orbits on G by the automorphism group generated by the mulpilier p are of length 1. We thus investigate the regular difference covers with parameters $((pq-1)/2, pq, 2pq)$, where p and q are distinct primes.

If D is a regular difference cover with parameters (v, k, λ) and if $M = \varrho(D)$ is the matrix of D in the regular representation, then as observed earlier $MM^T = kI_{v\times v} + \lambda J_{v\times v}$. Working exactly as in the proof of Lemma II.4.5 of [4], it follows that Bruck-Ryser-Chowla type result holds for regular difference covers. Namely, if there exists a regular difference cover with parameters (v, k, λ), with v odd, then the Diophantine equation

$$x^2 = ky^2 + (-1)^{\frac{v-1}{2}}\lambda z^2$$

has a non-trivial solution in integers.

For distinct primes p and q, if a cyclic regular difference cover with parameters $(\frac{pq-1}{2}, pq, 2pq)$ exists then a simple application of the above result yields that in case p and q are odd, then either $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$ or $p \equiv 1 \pmod 8$, $q \equiv 7 \pmod 8$ and in both cases p is a square modulo q. For instance $p = 73$, $q = 23$ is one such pair. We show:

Example 2.16. The regular difference cover with parameters $(839, 73 \times 23, 2 \times 73 \times 23)$ does not exist. From Theorem 2.2, it follows that both 73 and 23 are multipliers for D and hence D must be a union of orbits of the automorphism induced by either 23 or 73 in the cyclic group of order 839. The order of either of 23 or 73 modulo 839 is 419. There is one orbit of length 1 and two of length 419, say, C_1 and C_2 for the automorphism induced by the prime 23 in the group of order 839. Suppose that $D = a.e + b.C_1 + c.C_2$, where $a, b, c \geq 0$. Then by Remark 1.3,

$$a + 419b + 419c = 73 \times 23 = 1679$$

$$a^2 + 419b^2 + 419c^2 = 73 \times 23 + 2 \times 73 \times 23 = 3 \times 1679 \, .$$

One checks easily that as $0 \leq b \leq 3$ and $0 \leq c \leq 3$, there is no solution to the above equations. Thus regular difference covers with parameters $(839, 73 \times 23, 2 \times 23 \times 73)$ does not exist.

Example 2.17. The regular difference covers with parameters $(33, 34, 34)$ do not exist. As, by Theorem 2.2, 17 is a multiplier. The order of 17 modulo 33 is 10. There are one orbit of size 1, one orbit of size 2 and three orbits of size 10. Since the hypothetical difference cover has to be a union of orbits, there must exist non-negative integers a, b, c, d, e satisfying

$$a + 2b + 10c + 10d + 10e = 17 \times 2 = 34$$

$$a^2 + 2b^2 + 10c^2 + 10d^2 + 10e^2 = 34 + 34 = 68$$

or, after setting $a = 2a_1$

$$a_1 + b + 5c + 5d + 5e = 17$$

$$2a_1^2 + b^2 + 5c^2 + 5d^2 + 5e^2 = 34 \, .$$

It follows that $0 \leq c, d, e \leq 2$ and $a_1 + b \equiv 2 \pmod 5$ and $2a_1^2 + b^2 \equiv 4 \pmod 5$. Thus either $a_1 \equiv 0 \pmod 5$ and $b \equiv 2 \pmod 5$ or $a_1 \equiv 3 \pmod 5$ and $b \equiv 4 \pmod 5$. For $a_1 = 3$ and $b = 4$ and also for $a_1 = 0$ and $b = 2$, one checks easily that the above equations have no solutions. Hence the required regular difference covers do not exist.

Example 2.18. Regular difference covers with parameters $(81, 82, 82)$ does not exist. As before, 41 is a multiplier. The orbit lengths are $1, 2, 6, 18$ and 54. If the hypothetical regular difference cover exists, there should exist non-negative integers a, b, c, d, e such that

$$a + 2b + 6c + 18d + 54e = 82$$

$$a^2 + 2b^2 + 6c^2 + 18d^2 + 54e^2 = 164 .$$

The above two equations have a unique solution $a = 6,\ b = 5,\ c = 2,\ d = 0,\ e = 1$. Thus D should be

$$D = 6e + 5(g^{27} + g^{54}) + 2(g^9 + g^{18} + g^{36} + g^{72} + g^{63} + g^{45}) + (g + g^2 + \cdots).$$

Checking the character values using Mathematika on the computer shows that D is not a regular difference cover. Hence regular difference covers with parameters $(81, 82, 82)$ do not exist.

In a similar manner, Theorem 2.2 can be used to show the non-existence of regular difference covers with parameters $(109, 73 \times 3, 2 \times 73 \times 3)$ and many more.

3. Constructions of new regular difference covers

In this section we shall construct several new families of regular difference covers. In [3], regular difference covers with parameters $(m(m-1),\ m^2,\ m(m+1))$ and regular difference covers with parameters $(p^n,\ p^n,\ p^{n-1})$ (p an odd prime) of the form $E = e + 2D$ were constructed, where for $p^n \equiv 3 \pmod 4$, D is a difference set with parameters $(p^n,\ (p^n-1)/2,\ (p^n-3)/4)$ and for $p^n \equiv 1 \pmod 4$, D is a partial difference set with parameters $(p^n,\ (p^n-1)/2,\ (p^n-5)/4,\ (p^n-1)/4)$.

For several families of difference sets D, it is possible (though not easy) to choose positive integers a and b such that $E = aD + b(G - D)$ is a regular difference cover with suitable parameters. A significant feature of this construction is that for a chosen abelian group G, it is possible to construct infinitely many regular difference covers in G with size and regularity parameter (i.e., the number of times it covers G) as large as desired.

Suppose that D is a difference set in a group G with parameters $(v,\ k,\ \lambda)$ and let $E = aD + b(G - D)$, where a and b are positive integers. Then for any non-principal character χ of G, $\chi(E) = a\chi(D) + b\chi(G - D) = (a - b)\chi(D)$ and hence

$$\chi(E)\overline{\chi(E)} = (a-b)\chi(D)\overline{\chi(D)} = (a-b)^2(k-\lambda) .$$

Thus E will be a regular difference cover in G if and only if $(a - b)^2(k - \lambda) = \chi(E)\overline{\chi(E)} = |E| = ak + b(v - k)$.

For further use we record this observation as:

Lemma 3.1. *Let D be a difference set with parameters (v, k, λ) in an abelian group G. Then, for positive integers a and b, $E = aD + b(G - D)$ is a regular difference cover in G with parameters $(v, ak + b(v - k), (ak + b(v - k))(ak + b(v - k) - 1)/v)$ if and only if $(a - b)^2(k - \lambda) = ak + b(v - k)$.*

We now have:

Theorem 3.2.

(a) (Planar Regular Difference Covers).
Let D be a planar difference set with parameters $(n^2 + n + 1, n + 1, 1)$. Then

$$E = (4n^3 + 6n^2 + 4n)D + (4n^3 + 8n^2 + 7n + 2)(G - D)$$

is a regular difference cover with parameters $(n^2+n+1,\ 4n^5+12n^4+17n^3+12n^2+4n,\ (4n^5+12n^4+17n^3+12n^2+4n)(4n^3+8n^2+5n-1))$.

(b) (Paley Regular Difference Covers).
Let D be a Paley difference set with parameters $(q,(q-1)/2,(q-3)/4)$, where q is a prime power, $q \equiv 3 \pmod 4$. Then

$$E = (16q^2 + 12q - 4)D + (16q^2 + 20q - 4)(G - D)$$

is a regular difference cover with parameters $(q, 16q^2(q+1), 16q(q+1)(16q^3+16q^2-1))$.

(c) (Menon-Hadamard Regular Difference Covers).
Let D be a Menon - Hadamard difference set with parameters $(4u^2,\ 2u^2-u,\ u^2-u)$. Then

$$E = (4u^2 - 2u - 1)D + (4u^2 + 2u - 1)(G - D)$$

is a regular difference cover with parameters $(4u^2, 16u^4, 4u^2(4u-1)(4u+1))$.

(d) (Singer Regular Difference Covers).
Let D be a Singer difference set with parameters $\left(\frac{q^{d+1}-1}{q-1},\ \frac{q^d-1}{q-1},\ \frac{q^{d-1}-1}{q-1}\right)$, $d \geq 2$, q a prime power. Then

$$\begin{aligned} E &= \left(2q^d + 4q^{d-1}.\frac{q^{d+1}-1}{q-1}\right) D \\ &\quad + \left(q(1+2q^{d-1}) + (2+4q^{d-1})\left(\frac{q^{d+1}-1}{q-1}\right)\right)(G-D) \end{aligned}$$

is a regular difference cover with parameters $\left(\frac{q^{d+1}-1}{q-1}, K, \frac{K(K-1)(q-1)}{q^{d+1}-1}\right)$, *where* $K = q^{d-1}[4q^{2d+2} + 4q^{d+3} - 4q^{d+2} - 8q^{d+1} + q^4 - 2q^3 - 3q^2 + 4q + 4]/(q-1)^2$.

(e) (McFarland Regular Difference Covers).
Let D be a McFarland difference set with parameters $\left(q^{d+1}\left(1+\frac{q^{d+1}-1}{q-1}\right),\ q^d\left(\frac{q^{d+1}-1}{q-1}\right),\ q^d\left(\frac{q^d-1}{q-1}\right)\right)$, *where q is a prime power and d is a positive integer. Then*

$$\begin{aligned} E &= (4q^d(2q + q^2 + \cdots + q^{d+1}) + 2(q^{d+1} + q - 1))D \\ &\quad + (4q^d(2q + q^2 + \cdots + q^{d+1}) - 2(1 + q + \cdots q^d))(G - D) \end{aligned}$$

is a regular difference cover with parameters $\left(v = q^{d+1}(1+\frac{q^{d+1}-1}{q-1}), K, \frac{K(K-1)}{v}\right)$, *where* $K = 4q^{2d}(2q + q^2 + \cdots + q^{d+1})^2$.

Proof. For each of the families in (a), (b), (c), (d) and (e), using Lemma 3.1, it is enough to check that for the given choice of 'a' and 'b', $(a-b)^2(k-\lambda) = ak+b(v-k)$, where D is the difference set under consideration with parameters (v,k,λ). □

Example 3.3 Let $D = g+g^2+g^4$ be the $(7,3,1)$ difference set in the cyclic group $G = \langle g\rangle$ of order 7. Then $E = 64(g+g^2+g^4)+80(e+g^3+g^5+g^6)$ is a $(7,512,37376)$ regular difference cover. Also, let $D = g+g^3+g^4+g^5+g^9$ be the difference set with parameters $(11,5,2)$ in the cyclic group $G = \langle g\rangle$ of order 11. Then $E = (16\times 11^2 + 12\times 11-4)(g+g^3+g^4+g^5+g^9)+(16\times 11^2+20\times 11-4)(e+g^2+g^6+g^7+g^8+g^{10})$ is a $(11,23232,49063872)$ regular difference cover.

Remark 3.4. Usually, for a (v,k,λ) difference set D in an abelian group G, there are infinitely many choices for a and b such that $E = aD+b(G-D)$ is a regular difference cover. In fact, if a and b are such that $E = aD+b(G-D)$ is a regular difference cover with parameters $(v, ak+b(v-k), (ak+b(v-k))(ak+b(v-k)-1)/v)$, then for

$$\begin{aligned} c &= (4(k-\lambda)+2)v + 4(a-b)(k-\lambda) - 2k \\ d &= 4(k-\lambda)v + 4(a-b)(k-\lambda) - 2k, \end{aligned}$$

$E' = (a+c)D+(b+d)(G-D)$ is also a regular difference cover in G with parameters $(v,(a+c)k+(b+d)(v-k),((a+c)k+(b+d)(v-k))((a+c)k+(b+d)(v-k)-1)/v)$. Indeed, one checks that

$$\begin{aligned} \chi(E')\overline{\chi(E')} &= ((a-b)+(c-d))^2(k-\lambda) \\ &= ak+b(v-k)+4v^2(k-\lambda)+4(a-b)v(k-\lambda) \\ &= (a+c)k+(b+d)(v-k). \end{aligned}$$

Remark 3.5. In general, for a partial difference set D with parameters (v,k,λ,μ), it is not possible to choose positive integers a and b such that $E = aD+b(G-D)$ is a regular difference cover. Indeed, proceeding as in Lemma 3.1, E will be a regular difference cover if and only if for any non-principal character χ of G,

$$\chi(E)\overline{\chi(E)} = (a-b)^2\chi(D)\overline{\chi(D)} = ak+b(v-k)$$

i.e., if and only if

$$|\chi(D)|^2 = \frac{ak+b(v-k)}{(a-b)^2}\ .$$

The right hand side of the above is a fixed number, whereas, usually, for partial difference sets, non-principal characters take two different values $\frac{\lambda-\mu\pm\sqrt{(\lambda-\mu)^2+4\gamma}}{2}$, where $\gamma = k-\mu$, if $e\notin D$ and $\gamma = k-\lambda$ if $e\in D$ (see [10] or [14]).

As partial difference sets D do not yield regular difference covers of type $E = aD+b(G-D)$, we now examine whether it is possible to construct regular difference covers of type $ae+bD$ from partial difference sets. We observe:

Lemma 3.6. *Let D be a (v, k, λ, μ) partial difference set with $D = D^{(-1)}$ and $e \notin D$. Then $E = ae + bD$ will be a $(v, a + bk, b^2\mu)$ regular difference cover if and only if $\mu - \lambda > 0$, and either $b(\mu - \lambda) = 2a$ and $a^2 + b^2(k - \mu) = a + bk$ or $\mu - \lambda = 2ab$ and $a^2 + k - \mu = a + bk$.*

Proof. Using properties of partial difference sets, as given in [10] or [14], it follows that

$$\begin{aligned} EE^{(-1)} &= a^2 + 2abD + b^2D^2 \\ &= a^2 + 2abD + b^2(\lambda D + \mu(G - D) + (k - \mu)e) \\ &= (a^2 + (k - \mu)b^2)e + (2ab + b^2\lambda)D + b^2\mu(G - D). \end{aligned}$$

Hence $EE^{(-1)} = (a+bk)e+\alpha G$, for some positive integer α if and only if $2ab+b^2\lambda = b^2\mu$ and $a^2 + (k - \mu)b^2 = a + bk$.

Also, writing $EE^{(-1)}$ differently, we get

$$\begin{aligned} EE^{(-1)} &= a^2 + 2abD + b^2(\mu G + (\lambda - \mu)D + (k - \mu)e) \\ &= (a^2 + k - \mu) + b^2\mu G + (2ab + (\lambda - \mu))D. \end{aligned}$$

Thus, $EE^{(-1)} = (a+bk)e+\alpha G$ if and only if $a^2+k-\mu = a+bk$ and $2ab+(\lambda-\mu) = 0$. □

J. Davis in [10] has constructed partial difference sets in $\mathbb{Z}_{p^2}^2$ with parameters $(p^4, (t+fp)(p^2-1), p^2+(t+fp)^2-3(t+fp), (t+fp)^2-(t+fp))$, $3 \le t \le p+1, 1 \le f \le p-1$ (Theorem 3.3 of [10]). Using these partial difference sets, we observe:

Proposition 3.7. *Let D be the partial difference set as above. Then $E = ae + bD$ is a regular difference cover if and only if $t = \frac{p+1}{2}$, $f = \frac{p-1}{2}$ and hence D is a partial difference set with Paley parameters $(p^4, \frac{p^4-1}{2}, \frac{p^4-5}{4}, \frac{p^4-1}{4})$.*

Proof. For the above partial difference set $v = p^4$, $k = (t + fp)(p^2 - 1)$, $\lambda = p^2 + (t + fp)^2 - 3(t + fp)$, $\mu = (t + fp)^2 - (t + fp)$. Hence $\mu - \lambda = 2(t + fp) - p^2$. As $\mu - \lambda$ is odd, we will never get $\mu - \lambda = 2ab$, for any a, b. Thus, we have to find positive integers a and b such that

$$b(\mu - \lambda) = 2a \quad \text{and} \quad a^2 + b^2(k - \mu) = a + bk.$$

Substituting the values of k, $\mu - \lambda$ and $b - \mu$ and eliminating a, we get

$$b = \frac{2[(\mu - \lambda) + 2k]}{(\mu - \lambda)^2 + 4(k - \mu)} = \frac{2(2t + 2fp - 1)}{p^2}.$$

Thus, $p^2|2t+2fp-1$, where $3 \le t \le p+1$ and $1 \le f \le p-1$. So $2t+2fp-1 \equiv 0 \pmod p$ implies that $2t \equiv 1 \pmod p$ and hence $t = (p+1)/2$ and $f = (p-1)/2$. Thus D is the partial difference set with parameters $(p^4, (p^4-1)/2, (p^4-5)/4, (p^4-1)/4)$ and $b = 2$, $a = 1$ is the only solution, i.e., $E = e + 2D$ is the only regular difference cover of this type. □

Using Theorem 3.4 and Corollary 3.2 of [10], we immediately get:

Corollary 3.8. *Let D be either the partial difference set in $\mathbb{Z}_{p^2}^r$ with parameters $(p^{2r},\ (p^{2r}-1)/2,\ (p^{2r}-5)/4,\ (p^{2r}-1)/4)$ or the partial difference set in $\mathbb{Z}_{p^2}^{4a}\times\mathbb{Z}_p^{4b}$, with $a+b$ a power of 2 and with parameters $(p^{4a+4b},\ (p^{4a+4b}-1)/2,\ (p^{4a+4b}-5)/4,\ (p^{4a+4b}-1)/4)$. Then $E=e+2D$ is a regular difference cover with parameters $(p^{2r},p^{2r},p^{2r}-1)$ in $\mathbb{Z}_{p^2}^r$ or with parameters $(p^{4a+4b},p^{4a+4b},p^{4a+4b}-1)$ in $\mathbb{Z}_{p^2}^{4a}\times\mathbb{Z}_p^{4b}$.*

Remark 3.9. We finally note that it is not possible either to construct regular difference covers of the form $E = ae + bD$ from the partial difference sets D, constructed in [14] with parameters $(p^{2t}, r_2(p^t-1), p^t+r_2^2-3r_2, r_2^2-r_2)$, $r_2 = lp^{t-s}$, $1 \le l \le p^s$, s is a positive divisor of t, $s < t$, for any prime $p > 2$. Indeed, using Lemma 3.6, we need to find positive integers a and b such that $b(\mu-\lambda) = 2a$ and $a^2 + b^2(k-\mu) = a + bk$. It follows that $b = 2(2lp^{t-s}-1)/p^t$. As $s|t$ and $1 \le s \le t$, it is not possible to choose any integer b satisfying the above requirements, for any odd prime p.

We close this paper by making a final remark on how regular difference covers lead to certain self-dual codes, with a small example.

Example 3.10. Let D be the difference cover with parameters $(9, 19, 38)$ given by $D = 4g^2 + 2g^3 + 4g^4 + 2g^5 + 2g^6 + 2g^7 + 3g^8$ where $G = \langle g \rangle$ is the cyclic group of order 9. Define $E = D - G$. Then $EE^{(-1)} = 19 + 9G$. Let M be the 9×9 circulant matrix whose first row is given by the coefficients of E. Then MM^T has all its diagonal entries 28 and off-diagonal entries 9. Let N be the 10×10 matrix obtained from M where the first row of N is $(0, 1, 1, 1, \cdots, 1)$ and its first column is $(0, 1, 1, 1, \cdots, 1)^T$. Then NN^T is the matrix having $(9, 29, 29, \cdots, 29)$ as its diagonal and all of whose off-diagonal entries being 10. It is easy to see that $[I_{10}|N]$ is the generator matrix of a self-dual code over $\mathbb{Z}_5$.

Remark 3.11. The above example has an obvious generalization to other classes of self-dual codes over small prime fields.

References

[1] K. T. Arasu and D. K. Ray-Chaudhuri, *Multiplier theorem for a difference list*, Ars Comb., **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] K. T. Arasu and S. K. Sehgal, *Cyclic difference covers*, to appear in Australasian J. Combinatorics.

[4] T. Beth, D. Jungnickel and H. Lenz, Design Theory (2nd edition), Cambridge University Press, (1999).

[5] T. Bier, personal communication.

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

[7] Charles J. Colbourn, Alan 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 Phil. Soc., **74**(1973), 17-28.

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

[10] J. A. Davis, *Partial difference sets in p-groups*, Archiv der Math., **63**(1994), 103-110.

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

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

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

[14] D. K. Ray-Chaudhuri, Yu Qing Chen and Qing Xiang, *Construction of partial difference sets and relative difference sets using Galois rings II*, J. Comb. Theory Ser A, **76**(1996), 179-196.

[15] Cesaro Polcino Milies and Sudarshan K. Sehgal, An Introduction to Group Rings, Kluwer Acad. Publishers, Dordrecht, (2000).

[16] Dong Wiedemann, *Cyclic difference covers through 133*, Proceedings of the twenty-third South Eastern International Conference on Combinatorics, Graph Theory and Computing (Boca Raton, FL, 1992), Congr. Number, **90**(1992), 181-185.