Relative difference sets partitioned by cosets

Peter J. Dukes[*]
Department of Mathematics and Statistics
University of Victoria
Victoria, Canada
dukes@uvic.ca

Alan C.H. Ling
Department of Computer Science
University of Vermont
Burlington, U.S.A.
aling@cems.uvm.edu

Submitted: Oct 16, 2015; Accepted: Sep 9, 2017; Published: Sep 22, 2017
Mathematics Subject Classifications: 05B10; 05B15; 05B25

Abstract

We explore classical (relative) difference sets intersected with the cosets of a subgroup of small index. The intersection sizes are governed by quadratic Diophantine equations. Developing the intersections in the subgroup yields an interesting class of group divisible designs. From this and the Bose-Shrikhande-Parker construction, we obtain some new sets of mutually orthogonal latin squares. We also briefly consider optical orthogonal codes and difference triangle systems.

Keywords: relative difference set; mutually orthogonal latin square; optical orthogonal code; difference triangle system

1 Introduction

A k-subset D of a group G of order v (which we often assume is abelian and written additively) is a (v, k, λ)-*difference set* if every non-zero element of G is realized exactly λ times as a difference of two elements in D. If, for the moment, we write G multiplicatively with identity e_G, its subsets correspond to elements of the group ring $\mathbb{Z}[G]$ with coefficients in $\{0, 1\}$; conveniently, D is a (v, k, λ)-difference set if and only if $\left(\sum_{d\in D} d\right)\left(\sum_{d\in D} d^{-1}\right) = k \cdot e_G + \lambda \cdot \left(\sum_{g\in G} g - e_G\right)$. This is naturally abbreviated as

$$D \cdot D^{(-1)} = k \cdot e_G + \lambda \cdot (G - e_G). \qquad (1)$$

Let N be a normal subgroup of G, where $|N| = n$ and $|G| = mn$. A k-subset R of G is an (m, n, k, λ)-*relative difference set* if every element of $G \setminus N$ is realized exactly λ

[*]Supported by NSERC grant 312595–2010.

times as a difference of elements in R, while no nonzero element of N is ever realized as such a difference. Back in the group ring language, this means that

$$R \cdot R^{(-1)} = k \cdot e_G + \lambda \cdot (G - N). \tag{2}$$

Relative difference sets were introduced over fifty years ago by Elliott and Butson in [7].

We review two important examples. Let q be a prime power and $\mathbb{F}_q$ the finite field of order q. If we take $G = \mathbb{F}_{q^3}^\times/\mathbb{F}_q^\times$ and $D = \{\alpha \in G : \mathrm{Tr}_{3/1}(\alpha) = 0\}$, then D is a $(q^2+q+1, q+1, 1)$-difference set. Extracting exponents of a generator yields an additive presentation, call it S_q, in the cyclic group $\mathbb{Z}/(q^2+q+1)\mathbb{Z}$. These are (a special case of) the 'Singer' difference sets. Next, a $(q+1, q-1, q, 1)$-relative difference set on $\mathbb{F}_q^\times \leqslant \mathbb{F}_{q^2}^\times$ is furnished by $R = \{\alpha : \mathrm{Tr}_{2/1}(\alpha) = 1\}$. We again have an additive presentation, call it $R_q \subseteq \mathbb{Z}/(q^2-1)\mathbb{Z}$ relative to the subgroup $\mathbb{Z}/(q-1)\mathbb{Z}$. These are often referred to as 'Bose' or 'affine' relative difference sets. These and other important examples of relative difference sets can be found in Alexander Pott's survey, [11].

It is well known that (v, k, λ)-difference sets, when acted on by their underlying group, develop into symmetric (v, k, λ)-designs. Indeed, the projective plane of order q arises from developing the Singer difference sets above. Similarly, relative difference sets develop into a generalized type of block design, defined next.

A *group divisible design* (GDD) is a triple $(V, \Pi, \mathcal{B})$, where V is a set of *points*, Π is a partition of V, and $\mathcal{B} \subseteq 2^V$ is a family of subsets of V called *blocks*, such that two elements from different parts of Π appear together in exactly one block, while two elements from the same part of Π never appear together in a blocks.

If the block sizes are in K, it is common to abbreviate this as a K-GDD. As with BIBDs, it is possible to replace 'exactly one' by 'exactly λ' above for a nonnegative integer λ; for our purposes, though, we assume $\lambda = 1$. The *type* of the GDD is the list of part sizes in Π. It is common to abbreviate this with exponential notation, so that, for instance, n^m represents m groups of size n.

A $(v, k, 1)$-BIBD is equivalent to a $\{k\}$-GDD of type 1^v. More generally, a *pairwise balanced design* $\mathrm{PBD}(v, K)$ is a K-GDD of type 1^v. In these cases, Π consists of v singleton parts. At the opposite extreme, a transversal design $\mathrm{TD}(k, n)$ is a $\{k\}$-GDD of type n^k. In this case the blocks are transversals of the partition Π. Recall that a $\mathrm{TD}(k, n)$ is equivalent to $k-2$ mutually orthogonal latin squares of order n, and also to k-factor orthogonal arrays of strength two. Therefore, GDDs provide a common generalization of the fundamental objects of interest in design theory. Richard Wilson was perhaps the first to consider GDDs in generality, starting in [13, §6]; this formed a key part of his existence theory for pairwise balanced designs.

Returning to relative difference sets, the group action develops such a set with parameters $(m, n, k, 1)$ into a $\{k\}$-GDD of type n^m. For instance, the Bose relative difference set in $\mathbb{F}_{q^2}^\times$ yields a $\{q\}$-GDD of type $(q-1)^{q+1}$, which is equivalent to an affine plane of order q with one point deleted.

Our primary observation is a straightforward extension of this. Since blocks are developed as cyclic shifts, subgroups of G induce smaller GDDs, potentially with a mixture of block sizes. This is similar in spirit to constructions in [2, 10, 12].

Theorem 1. *Let R be an $(m, n, k, 1)$-relative difference set on groups $N \leqslant G$. Let V be a subgroup of index d in G such that $G = NV$. Then R induces a GDD with points V, partition $\Pi = V/(N \cap V)$, and blocks $gR \cap V$, $g \in G$. The type of the GDD is $[n/d]^m$ and the block sizes are $|R \cap hV|$, where h ranges over a transversal of V in G.*

Proof. Let $x, y \in V$. Suppose they are in different cosets of Π. Then $xy^{-1} \in G \setminus N$. By the property of R being a relative difference set, it follows that $x, y \in gR$ for some (exactly one) $g \in G$. This is the condition for x, y to be covered by some (exactly one) block of the given form. Similarly, if $xy^{-1} \in N \setminus \{e_G\}$, then x, y are covered by no such block developed from R.

By assumption, we have $|V| = |G|/d = nm/d$ and, by the second isomorphism theorem, we have $|\Pi| = |G/N| = m$. This gives the GDD type. Finally, the size of a generic block is $|gR \cap V| = |R \cap g^{-1}V|$, which can be computed over coset representatives g for V in G. □

We comment on some additional structure. In a GDD with points V and blocks $\mathcal{B}$, a *symmetric class* of blocks is a subset $\mathcal{S} \subseteq \mathcal{B}$ such that each block in $\mathcal{S}$ has the same size, call it k, and every point of V is covered by exactly k elements of $\mathcal{S}$. For instance, developing a (relative) difference set of size k leads to one symmetric class $\mathcal{S} = \mathcal{B}$. We remark that the GDD of Theorem 1 induces d disjoint symmetric classes. In more detail, the blocks $gR \cap V$, $g \in G$, partition into classes according to the coset of g in V. That is, let $g_1, g_2, \ldots, g_d$ be a transversal of V in G and put $B_i = g_iR \cap V$. Then developing B_i in V gives symmetric block classes $\mathcal{S}_i = \{hB_i : h \in V\}$, $i = 1, \ldots, d$.

In this paper, we explore such GDDs for the affine relative difference sets.

Corollary 2. *Let $R_q \subset \mathbb{Z}/(q^2-1)\mathbb{Z}$ be the affine relative difference set and suppose $d \mid q-1$. Put $a_i = |R_q \cap (i + d\mathbb{Z})|$ for $i = 0, 1, \ldots, d-1$. Then there exists an $\{a_0, a_1, \ldots, a_{d-1}\}$-GDD of type $[(q-1)/d]^{q+1}$. Moreover, the blocks of this GDD partition into symmetric classes of block size a_i for $i = 0, 1, \ldots, d-1$.*

We investigate some special cases of these GDDs in the next section. As consequences, we obtain constructions of some new best-known sets of mutually orthogonal latin squares. The method appears to be useful for other difference problems, such as optical orthogonal codes and difference triangle systems.

2 Constraints on block sizes

Here we investigate the structure of the block sizes $a_0, a_1, \ldots, a_{d-1}$ of the GDD arising from Corollary 2. Since those block sizes are formed by intersecting R_q with cosets of $d\mathbb{Z}$, it follows that

$$\sum_{i=0}^{d-1} a_i = q. \tag{3}$$

Next, every difference which is 0 (mod d) must arise (exactly once) from a difference of elements of R_q in the same coset. Therefore,

$$\sum_{i=0}^{d-1} a_i(a_i - 1) = \frac{q(q-1)}{d}. \tag{4}$$

There exist other constraints (not all independent) by examining other types of differences. For the moment, we focus on the cases $d = 3, 4$.

Proposition 3. *Let $q = p \equiv 4n + 1$, a prime. Consider the GDD obtained by developing R_q in $\mathbb{Z}/(q^2 - 1)\mathbb{Z}$ using a subgroup of index $d = 4$. Its block sizes are*

$$\{a_0, a_1, a_2, a_3\} = \left\{n + \frac{a}{2}, n - \frac{a}{2}, n + \frac{1}{2} + \frac{b}{2}, n + \frac{1}{2} - \frac{b}{2}\right\},$$

where $p = a^2 + b^2$ is the unique decomposition of p as a sum of squares with a even.

Proof outline. From an easy counting argument, we can strengthen (3) in the case $d = 4$ to $a_0 + a_2 = 2n$, $a_1 + a_3 = 2n + 1$. With this, (4) becomes $a_0a_1 + a_1a_2 + a_2a_3 + a_3a_0 = 2n(2n + 1)$, after simplification. Letting a, b be defined as above, this is equivalent to Fermat's Diophantine equation $a^2 + b^2 = p$. □

Remark 4. Various explicit or algorithmic methods for computing a, b are known. For instance, it was known to Gauss that $a \equiv \frac{1}{2}\binom{2n}{n}$ and $b \equiv a(2k)!$ (mod p), where $|a|, |b| < p/2$. See [9] for a proof.

A similar explicit calculation of block sizes can be undertaken for $d = 3$.

Proposition 5. *Let $q = p \equiv 3n + 1$, a prime. Consider the GDD obtained by developing R_q in $\mathbb{Z}/(q^2 - 1)\mathbb{Z}$ using a subgroup of index $d = 3$. Its block sizes are*

$$\{a_0, a_1, a_2\} = \frac{1}{3}\binom{2n}{n}\{1, \omega, \omega^2\} \mod p,$$

where ω is a primitive cube root of unity in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Proof outline. Since by (3) we have $a_0 + a_1 + a_2 = p \equiv 1 \pmod 3$, we may assume (after re-indexing) that $a_0 \equiv a_1 \pmod 3$. Put $A := 3a_0 + 3a_1 - 2p$ and $B := (a_0 - a_1)/3$. After a calculation, we find that

$$A^2 + 27B^2 = 4p. \tag{5}$$

Since the Eisenstein integers $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ form a UFD, it follows that (5) has at most one solution in positive integers A, B. The formula given comes from a result of Jacobi (see, for instance, [9]), which explicitly solves (5). A few calculations are needed to switch back to variables a_0, a_1, a_2. □

In what follows, we let d be general and not assume q is prime. Let p be the characteristic of $\mathbb{F}_q$ and $\theta : x \mapsto x^p$ the Frobenius automorphism. Our next result controls the block sizes.

Proposition 6. *Consider the GDD obtained by developing by R_q in $\mathbb{Z}/(q^2-1)\mathbb{Z}$ using a subgroup of index d. Let $a_i := (i + d\mathbb{Z}) \cap R_q$ be the coset intersections with R_q, $i = 0, \ldots, d-1$. Then $a_i = a_{ip}$, where subscripts are read modulo d.*

Proof. The affine relative difference set in $\mathbb{F}_{q^2}$ is invariant under θ, and hence in the additive presentation we have $p \cdot R_q = R_q$ in $\mathbb{Z}/(q^2-1)\mathbb{Z}$. It follows that

$$a_{ip} = |(-ip + R_q) \cap d\mathbb{Z}| = |(-i + \overline{p}R_q) \cap d\mathbb{Z}| = |(-i + R_q) \cap d\mathbb{Z}| = a_i,$$

where $p\overline{p} = 1$ in $\mathbb{Z}/(q^2-1)\mathbb{Z}$ and where subscripts on the block sizes are interpreted modulo d. □

Remark 7. A similar invariance exists for the Singer difference sets S_q intersected with cosets of a subgroup of index d.

Corollary 8. *The number of different block sizes of the GDD arising from R_q and d is at most the number of orbits of multiplication by p on $\mathbb{Z}/d\mathbb{Z}$.*

The truth is sometimes better, since intersections from different orbits of θ might vanish or coincide.

Example 9. Let $q = 16$, $d = 5$ so that Corollary 2 gives an $\{a_0, a_1, \ldots, a_4\}$-GDD of type 3^{17}. Since $p = 2$ is a generator for $\mathbb{Z}/5\mathbb{Z}$, we have only two different block sizes: a_0 and $a_1 = a_2 = a_3 = a_4$. Substituting into (3) and (4), these necessary equations have only the solution $a_0 = 0$, $a_1 = 4$ in nonnegative integers. So, in fact, we obtain a $\{4\}$-GDD of type 3^{17}.

Extending this example, we have a class of two-block-size GDDs that occur in certain cases.

Corollary 10. *Suppose $q = p^{2t} \equiv 1 \pmod{d}$ is such that p generates $(\mathbb{Z}/d\mathbb{Z})^\times$. Then there exists a cyclic $\{\frac{q\mp\sqrt{q}}{d}, \frac{q\pm(d-1)\sqrt{q}}{d}\}$-GDD of type $[(q-1)/d]^{q+1}$, where the sign is chosen according to whether $\sqrt{q} \equiv \pm 1 \pmod{d}$.*

Proof. We have only two block sizes a_0 and $a_1 = \cdots = a_{d-1}$. Equations (3) and (4) reduce to

$$a_0 + (d-1)a_1 = q, \text{ and}$$
$$a_0^2 + (d-1)a_1^2 = \frac{q(q+d-1)}{d}.$$

Solving the quadratic equation gives $a_0 = \frac{q\mp\sqrt{q}}{d}$ and $a_1 = \frac{q\pm(d-1)\sqrt{q}}{d}$. □

We give a list of GDD types and block sizes for various small cases in Tables 1 and 2

$q=3n+1$	type	a_0,a_1,a_2	$q=4n+1$	type	a_0,a_1,a_2,a_3
4	1^5	$0,2,2$	5	1^6	$2,2,1,0$
7	2^8	$2,4,1$	9	2^{10}	$1,2,4,2$
13	4^{14}	$6,5,2$	13	3^{14}	$2,4,5,2$
16	5^{17}	$8,4,4$	17	4^{18}	$5,2,4,6$
19	6^{20}	$4,9,6$	25	6^{26}	$5,8,8,4$
25	8^{26}	$5,10,10$	29	7^{30}	$10,8,5,6$
31	10^{32}	$9,8,14$	37	9^{38}	$10,6,9,12$
37	12^{38}	$16,9,12$	41	10^{42}	$13,8,8,12$
43	14^{44}	$17,10,16$	49	12^{50}	$9,12,16,12$
49	16^{50}	$12,17,20$	53	13^{54}	$10,14,17,12$
61	20^{62}	$20,25,16$	61	15^{62}	$18,12,13,18$
64	21^{65}	$16,24,24$	73	18^{74}	$17,14,20,22$
67	22^{68}	$24,17,26$	81	20^{82}	$25,20,16,20$
73	24^{74}	$22,30,21$	89	22^{90}	$25,18,20,26$
79	26^{80}	$32,25,22$	97	24^{98}	$29,26,20,22$
97	32^{98}	$26,37,34$	101	25^{102}	$26,30,25,20$
103	34^{104}	$30,32,41$	109	27^{110}	$26,32,29,22$
109	36^{110}	$37,42,30$	113	28^{114}	$25,24,32,32$
121	40^{122}	$33,44,44$	121	30^{122}	$25,30,36,30$
127	42^{128}	$49,36,42$	125	31^{126}	$26,30,37,32$
139	46^{140}	$54,41,44$	137	34^{138}	$29,32,40,36$
151	50^{152}	$44,49,58$	149	37^{150}	$34,42,41,32$
157	52^{158}	$57,56,44$	157	39^{158}	$34,36,45,42$
163	54^{164}	$46,57,60$	169	42^{170}	$45,36,40,48$
169	56^{170}	$56,64,49$	173	43^{174}	$50,44,37,42$
181	60^{182}	$58,69,54$	181	45^{182}	$50,50,41,40$
193	64^{194}	$72,65,56$	193	48^{194}	$45,42,52,54$
199	66^{200}	$70,57,72$	197	49^{198}	$50,42,49,56$

Table 1: Block sizes and types for $q = 3n+1$ and $4n+1$

3 Some new MOLS, IMOLS and HMOLS

Following [2, 8], we can use the GDDs of Corollary 2 to construct mutually orthogonal latin squares via the Bose-Shrikhande-Parker construction, [1]. We cite the relevant construction below, simplified somewhat for our use. The usual statement involves 'incomplete transversal designs' $\mathrm{TD}(k,n) - \sum_{i=1}^{t} \mathrm{TD}(k,m_i)$, which are equivalent to $k-2$ mutually orthogonal 'holey' latin squares of size n missing t disjoint subsquares of size m_i. In the case where all $m_i = 1$ and $t = n$, this can be regarded as a family of mutually orthogonal idempotent latin squares of size n. See [5] for a formal definition.

Theorem 11 (see [1, 5])**.** *Let $(V, \Pi, \mathcal{B})$ be a K-GDD with $|V| = v$ and $\Pi = \{V_1, \ldots, V_t\}$. Suppose $\mathcal{B}$ partitions into symmetric classes $\mathcal{S}_1, \ldots, \mathcal{S}_s$, where $\mathcal{S}_j$ has block size α_j. Let*

$q=5n+1$	type	a_0,a_1,a_2,a_3,a_4
11	2^{12}	$2,0,4,3,2$
16	3^{17}	$0,4,4,4,4$
31	6^{32}	$4,10,7,4,6$
41	8^{42}	$10,6,8,5,12$
61	12^{62}	$12,12,18,9,10$
71	14^{72}	$18,8,14,15,16$
81	16^{82}	$9,18,18,18,18$
101	20^{102}	$26,22,14,21,18$
121	24^{122}	$28,25,28,16,24$
131	26^{132}	$24,30,32,19,26$
151	30^{152}	$31,34,28,22,36$
181	36^{182}	$34,46,34,37,30$
191	38^{192}	$30,38,47,36,40$
211	42^{212}	$42,36,46,51,36$
241	48^{242}	$45,48,42,46,60$

$q=6n+1$	type	a_0,a_1,a_2,a_3,a_4,a_5
7	1^{8}	$0,2,1,2,2,0$
13	2^{14}	$2,2,2,4,3,0$
19	3^{20}	$2,6,4,2,3,2$
25	4^{26}	$1,4,6,4,6,4$
31	5^{32}	$5,6,8,4,2,6$
37	6^{38}	$8,6,8,8,3,4$
43	7^{44}	$7,6,10,10,4,6$
49	8^{50}	$8,8,8,4,9,12$
61	10^{62}	$8,10,8,12,15,8$
67	11^{68}	$10,6,12,14,11,14$
73	12^{74}	$14,16,9,8,14,12$
79	13^{80}	$18,12,8,14,13,14$
97	16^{98}	$14,16,14,12,21,20$
103	17^{104}	$16,14,17,14,18,24$
109	18^{110}	$19,24,18,18,18,12$

Table 2: Block sizes and types for $q=5n+1$ and $6n+1$

$\epsilon_j \in \{0,1\}$, *and suppose there exist*

$$\mathrm{TD}(k,\alpha_j+\epsilon_j)-\sum_{i=1}^{\alpha_j+\epsilon_j}\mathrm{TD}(k,1),$$

i.e. $k-2$ *mutually orthogonal idempotent latin squares of size* $\alpha_j+\epsilon_j$, *for all* $j=1,\ldots,s$. *Let* $\sigma=\sum_{j=1}^{s}\epsilon_j\alpha_j$. *Then there exists a*

$$\mathrm{TD}(k,v+\sigma)-\mathrm{TD}(k,\sigma)-\sum_{i=1}^{t}\mathrm{TD}(k,|V_i|),$$

i.e. $k-2$ *mutually orthogonal holey latin squares with hole sizes as indicated.*

Remark 12. A more general form with similar notation is [5, Theorem 3.23]; an even more general version of the construction appears as [3, Theorem 3.7].

If, in Theorem 11, we also have the existence of $\mathrm{TD}(k,\sigma)$ and $\mathrm{TD}(k,|V_i|)$, then we can 'fill holes' to get a $\mathrm{TD}(k,v+\sigma)$. Likewise, assuming the existence of $\mathrm{TD}(k,\sigma+1)$ and $\mathrm{TD}(k,|V_i|+1)$, we obtain a $\mathrm{TD}(k,v+\sigma+1)$.

A good set of MOLS is possible under the (strange) hypothesis that our intersection sizes $a_0,\ldots,a_{d-1}$ of Section 2 be prime powers, or one less than prime powers. We give two examples improving known lower bounds on $N(n)$, the maximum number MOLS, in [6, Table III.3.87], which in recent years has become fairly static.

Example 13. Let $q = 79$, $d = 3$. We compute from Corollary 2 a $\{22, 25, 32\}$-GDD of type 26^{80} having symmetric classes of each block size. By Theorem 11, we obtain a TD$(23, 2102)-$TD$(23, 22) - 80\times$TD$(23, 26)$, where we have incremented 22 to 23 using ϵ_1, say. For this, we have used the existence of $q - 2$ mutually orthogonal idempotent latin squares for prime powers q. Add 1 to the hole sizes and fill them, producing a TD$(23, 2103)$. It follows that $N(2103) \geqslant 21$; compare with $N(2103) \geqslant 15$ in [6].

Example 14. For $q = 127$, $d = 3$ we similarly have a $\{36, 42, 49\}$-GDD of type 42^{128} with symmetric classes. Taking $\epsilon_1 = \epsilon_2 = 1$ in Theorem 11 (corresponding to classes of block size 36 and 42) leads to $N(42 \times 128 + 36 + 42 + 1) = N(5455) \geqslant 35$; compare with $N(5455) \geqslant 15$ in [6].

Next, we have an improved set of incomplete MOLS. Following the standard notation, let the maximum number of incomplete MOLS of size n missing a common subsquare of size m be denoted $N(n; m)$.

Example 15. With $q = 41$ and $d = 4$, we get a $\{8, 8, 12, 13\}$-GDD of type 10^{42}. So $N(449; 29) \geqslant 7$; compare with $N(449; 29) \geqslant 6$ in [6].

Finally, we have some noteworthy holey MOLS with a uniform partition into holes. Let $N(h^m)$ denote the maximum number of holey MOLS of size hm missing m disjoint holes of size h.

Example 16. With $q = 37$ and $d = 3$, we get a $\{9, 12, 16\}$-GDD of type 12^{38}. So $N(12^{39}) \geqslant 7$; compare with $N(12^{39}) \geqslant 4$ in [6]

Example 17. With $q = 61$ and $d = 3$, we get a $\{16, 20, 25\}$-GDD of type 20^{62}. So $N(20^{63}) \geqslant 15$, and this is the second largest number of HMOLS known (of any type) for the challenging case of group size 20.

Example 18. With $q = 49$ and $d = 4$, we get a $\{9, 12, 12, 16\}$-GDD of type 12^{50}, with two symmetric classes of block size 12. So $N(12^{52}) \geqslant 7$, and this is again a reasonable lower bound for a difficult group size.

This general technique can produce many interesting non-uniform HMOLS, although there is no table for comparison.

4 Optical orthogonal codes and difference triangle sets

An (n, w, λ) *optical orthogonal code* (OOC) is a family of cyclic binary sequences of length n, constant weight w, and such that any two sequences from different cycles has at most λ ones in common positions. In other words, all 'Hamming correlations' between different sequences are at most λ. As a cyclic binary code, the minimum distance of such an OOC is at least $2(w - \lambda)$.

If we extract the supports of binary sequences in an $(n, w, 1)$ OOC, the result is a family of sets of size w in $\mathbb{Z}/n\mathbb{Z}$ which form a 'difference packing', that is, such that any nonzero element in the group occurs as a difference in one of the sets at most once. The converse relationship is also clear.

We propose the cyclic GDD of Corollary 10, with blocks of size a_0 discarded, as an infinite class of (sometimes very good) difference packings.

Proposition 19. *Suppose $q = p^{2t}$ with $\sqrt{q} \equiv 1 \pmod{d}$. Let $d \geqslant 3$ be an integer such that p generates $(\mathbb{Z}/d\mathbb{Z})^\times$. Then there exists a $(q^2-1, \frac{q+(d-1)\sqrt{q}}{d}, 1)$ OOC of size $d-1$.*

An (n,k)-*difference triangle set* (abbreviated DΔS) is a set $\{X_1, X_2, \dots, X_n\}$ of $(k+1)$-subsets of integers such that the $nk(k+1)/2$ (unsigned) differences between two elements in some X_i are distinct and nonzero. The case $n=1$ reduces to a 'Golomb ruler' with $k+1$ marks or, equivalently, a 'Sidon set' of size $k+1$.

For example, a $(2,2)$-DΔS is given by $\{\{0,1,4\},\{0,2,7\}\}$. As illustrated in this example, we can assume by translation that each set X_i has minimum element 0; in this case, the difference triangle set is called *normalized*. Similar to Golomb rulers, it is of interest to find normalized (n,k)-DΔS such that the maximum integer in any of its sets, called the *scope*, is as small as possible. The $(2,2)$-DΔS above has scope 7, which is best possible. A table of known upper and lower bounds on minimum scopes of (n,k)-DΔS for small n,k can be found in [6, §VI.19].

If we interpret a cyclic difference set over the integers (i.e. ignoring the modulus), the result is a Golomb ruler. In a similar way, the second author in [10] used relative difference sets to obtain record-breaking scopes for various (n,k)-DΔS.

To illustrate another application of our coset technique, we offer one example improvement on the table mentioned above.

Example 20. Let $q = 81$ and consider the Singer difference set S_q of size $q+1$ in $\mathbb{Z}/(q^2+q+1)\mathbb{Z}$. Project S_q onto $d=7$ cosets, and compute that $|S \cap 7\mathbb{Z}| = 4$, while $|S \cap (i+7\mathbb{Z})| = 13$ for all nonzero $i \in \mathbb{Z}/7\mathbb{Z}$. Retain the six 'full' cosets and translate each to include zero. All internal differences are distinct multiples of 7, so we divide and normalize again, this time searching for an optimal scaling and translation to minimize the scope. We obtain a $(6,12)$-DΔS of scope 786, which improves on 797 found in [6, Table VI.19.37]:

$$\begin{aligned}\{&\{0,36,57,89,102,229,293,374,499,619,702,716,774\},\\ &\{0,160,161,350,356,461,532,576,587,638,663,755,786\},\\ &\{0,29,70,178,241,243,278,320,337,376,494,618,757\},\\ &\{0,43,48,152,273,303,353,357,431,439,491,500,538\},\\ &\{0,24,112,180,207,321,475,565,605,715,727,734,749\},\\ &\{0,132,165,302,318,393,403,421,669,736,762,782,785\}\}.\end{aligned}$$

We have not undertaken an exhaustive analysis of other cases. Qualitatively, it seems that this technique for constructing difference triangle systems has too much waste unless the (relative) difference set admits a very favorable partition by cosets.

References

[1] R.C. Bose, S.S. Shrikhande and E.T. Parker, Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture. *Canad. J. Math.* 12 (1960), 189–203.

[2] A.E. Brouwer, A series of separable designs with application to pairwise orthogonal Latin squares. *European J. Combin.* 1 (1980), 39–41.

[3] A.E. Brouwer and G.H.J. van Rees, More mutually orthogonal latin squares. *Discrete Math.* 39 (1982), 263–281.

[4] S. Chowla, P. Erdős, and E.G. Strauss, On the maximal number of pairwise orthogonal latin squres of a given order. *Canad. J. Math.* 12 (1960), 204–208.

[5] C.J. Colbourn and J.H. Dinitz, Making the MOLS table. *Computational and constructive design theory*, 67–134, Math. Appl., 368, Kluwer, Dordrecht, 1996.

[6] C.J. Colbourn and J.H. Dinitz, eds., The CRC Handbook of Combinatorial Designs, 2nd edition, CRC Press, Boca Raton, 2006.

[7] J.E.H. Elliott and A.T. Butson, Relative difference sets. *Illinois J. Math.* 10 (1966), 517–531.

[8] M. Greig, Designs from projective planes and PBD bases. *J. Combin. Des.* 7 (1999), 341–374.

[9] F. Lemmermeyer, Reciprocity laws: from Euler to Eisenstein. Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[10] A.C.H. Ling, Difference triangle sets from affine planes. *IEEE Trans. Inform. Theory* 48 (2002), 2399–2401.

[11] A. Pott, A survey on relative difference sets. *Groups, difference sets, and the Monster* (Columbus, OH, 1993), 195–232, Ohio State Univ. Math. Res. Inst. Publ., 4, de Gruyter, Berlin, 1996.

[12] A. Pott, Two applications of relative difference sets: Difference triangles and negaperiodic autocorrelation functions. *Discrete Math.* 308 (2008), 2854–2861.

[13] R.M. Wilson, An existence theory for pairwise balanced designs I: Composition theorems and morphisms. *J. Combin. Theory Ser. A* 13 (1972), 220–245.