ALMOST DIFFERENCE SETS AT SIXTEEN UNDETERMINED CELLS OF GORDON'S TABLE, AND THE STATUS OF $(61, 30, 14, 30)$

KOREA SUPERINTELLIGENCE LABS

Abstract. A (v, k, λ, t)-almost difference set is a k-element subset D of a group of order v in which t of the $v-1$ nonzero elements have exactly λ representations as a difference of two elements of D, and the remaining $v-1-t$ have exactly $\lambda+1$. Gordon's table of cyclic almost difference sets for $4 \le v \le 63$ marks 94 of its cells as undetermined: at those parameters the exhaustive search reported there did not run to completion. We exhibit almost difference sets at sixteen of them, namely at $(57, 27)$, $(58, 28)$, $(58, 29)$, $(60, 29)$, $(61, 22)$, $(61, 28)$, $(62, 19)$, $(62, 23)$, $(62, 27)$, $(62, 28)$, $(62, 29)$, $(63, 19)$, $(63, 21)$, $(63, 25)$, $(63, 26)$ and $(63, 27)$, each by an explicit witness printed in full, and at a seventeenth cell, $(63, 24)$, which turns out to be an instance of a product construction of Cai and Ding. Three of the sixteen are specializations of published constructions to cells the table leaves undetermined; for the other thirteen the recorded literature search matched the parameters to no published family, with the gaps in that search stated explicitly. We also record that the cell $(61, 30, 14, 30)$, named in the source as the first open case of an existence question of Arasu, Ding, Helleseth, Kumar and Martinsen, is realized by the quadratic residues modulo 61, and prove that for every odd modulus the question splits on v mod 4: at $v \equiv 3 \pmod 4$ every almost difference set with those parameters is a difference set, so nothing but difference-set existence survives there, while at $v \equiv 1 \pmod 4$ exactly one parameter tuple is admissible — the Paley shape, which the quadratic residues realize at every prime. Every theorem, proposition and corollary is machine-checked in Lean 4. No nonexistence is claimed anywhere.

1. Introduction

Let G be a finite abelian group of order v, written additively, and let $D \subseteq G$. For $x \in G$ put

$$d_D(x) \;=\; \#\{\, a \in D \;:\; a - x \in D \,\} \;=\; |D \cap (D + x)|,$$

the number of ordered pairs of elements of D with difference x. If every nonzero x has $d_D(x) = \lambda$ then D is a (v, k, λ)-difference set, $k = |D|$. Relaxing that by one unit gives the object of this paper, in the formulation of Gordon [1]: if t of the nonzero elements have $d_D(x) = \lambda$ and the remaining $v-1-t$ have $d_D(x) = \lambda + 1$, then D is a (v, k, λ, t)-*almost difference set* (ADS). The definition interpolates between two classical objects: $t = v - 1$ is a difference set, and $\lambda = 0$ is a modular Golomb ruler. Almost difference sets are the combinatorial form of binary sequences whose out-of-phase autocorrelation takes two values — three-level autocorrelation, counting the peak — which is where most of the published constructions come from [2, 5, 3]. Throughout, $G = \mathbb{Z}_v = \mathbb{Z}/v\mathbb{Z}$, the cyclic case that [1] tabulates.

The table and its undetermined cells. Figure 1 of [1] is a (v, k) grid for $4 \le v \le 63$ and $2 \le k \le 31$ in which each cell records the outcome of an exhaustive search over fixed-density necklaces: a cell is dark if a cyclic ADS with those parameters exists, white if none does, and dashed if, in the caption's words, the search "took too long to complete the exhaust". A dashed cell is therefore a report about a computation, not a statement about the mathematics: it records that one particular exhaustive search was abandoned, and nothing was claimed about whether a construction is known.

The figure is generated rather than typeset by hand, so it can be read exactly. The arXiv source of [1] builds it from a TikZ file of 930 rectangles, one per cell of the triangular grid $2 \le k \le \lfloor v/2 \rfloor$, $4 \le v \le 63$: 662 dark, 174 white and 94 dashed, every dashed one with $54 \le v \le 63$. Those counts are for arXiv versions v2 and v3, whose figure sources are byte-identical; v1 draws the same 930 cells but marks 112 of them dashed, a superset of the 94, so every cell called dashed here is dashed in all three. The cell-by-cell reading was checked against the figure as rendered from that source, row by row; against the inset $\hat{t} = \min(t, v-1-t)$ that each of the 174 white cells carries, recomputed from (v, k) by

Proposition 2.2 at all 174 with no mismatch; and against the text of [1], which names $(50, 18, 6, 37)$ and $(53, 17, 5, 40)$ as the white cells of largest $\hat{t}$, namely 12, and $(56, 17, 4, 3)$ as a dark cell of small positive $\hat{t}$ — all as read here.

The parameters of a dashed cell are not free. Section 2 recalls the counting identity behind this, but the effect is worth stating at once: at every cell of the grid the pair (λ, t) is determined by (v, k), so "the cell $(61, 30)$" and "the parameters $(61, 30, 14, 30)$" name the same thing.

The first open case. Section IV of [1] closes by quoting the existence question with which [2] ends — "It is an open question whether $(v, (v-1)/2, \lambda, t)$ almost difference sets exist for all odd v" — observing that the condition $t \neq v - 1$ should be added, since $(v, (v-1)/2, \lambda)$-difference sets are ruled out at $(39, 19, 9)$ and $(51, 25, 12)$ by the Mann test, and concluding: *the first open case is* $(61, 30, 14, 30)$. That sentence stands word for word in all three arXiv versions of [1] (Remark 3.4). The cell $(61, 30)$ is dashed in Figure 1, and it is the only dashed cell in the whole column $k = (v-1)/2$ — the only one among the thirty cells of that column, over the whole table.

That cell is realized by the Paley set of nonzero quadratic residues modulo 61 (Proposition 3.3). This is not new mathematics and we claim none: for a prime $p \equiv 1 \pmod 4$ the quadratic residues form a $\left(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{2}\right)$-ADS, which is Theorem 2(1) of [2] — the paper the question is quoted from — and, in its equivalent partial-difference-set form, Theorem 43 of the survey [3], going back to the order-2 cyclotomic numbers [11]. At $p = 61$ the parameters read $(61, 30, 14, 30)$ exactly. What Section 3 adds is the reason this closes the column and not just one cell: for *every* odd modulus the question splits on $v \bmod 4$, the half $v \equiv 3 \pmod 4$ containing no almost difference set that is not already a difference set, and the half $v \equiv 1 \pmod 4$ having exactly one admissible parameter tuple, which is the Paley shape.

What this paper settles. The dashed region is larger than one cell, and the searches described in Section 5 reach sixteen more of it. Theorem 4.1 and Theorem 4.2 exhibit almost difference sets at sixteen dashed cells; Proposition 4.3 adds a seventeenth, $(63, 24, 8, 6)$, which is a published construction evaluated at a cell the table leaves undetermined. Every witness is listed in full in Appendix A, so every one of these existence statements can be checked by hand.

Of the sixteen, three — $(58, 28, 13, 42)$, $(58, 29, 14, 43)$ and $(60, 29, 13, 14)$ — are specializations of constructions of [2], and only their application to these cells is new. For the remaining thirteen the literature search recorded in Section 6 identified no published family reaching those parameters. That is a statement about a search, not about the literature: the gaps in it are named in Section 6, and "not found" is not "new".

Nothing here is a nonexistence statement. A cell we do not settle is a cell where the searches of Section 5 found nothing, which is evidence about the searches and not about the cell; 76 of the 94 remain undetermined.

Verification. Every theorem, proposition and corollary below has been checked in Lean 4 against *Mathlib*. The remarks are not part of the formal development, and say so where it matters. Section 8 says precisely which statements are proved by argument in the kernel and which are delegated to compiled evaluation of a finite check, and reports the negative controls that keep the formal definition honest.

2. Preliminaries

Definition 2.1. Let $v \geq 2$, let $D \subseteq \mathbb{Z}_v$ and let $k, \lambda, t \in \mathbb{N}$. Then D is a (v, k, λ, t)-*almost difference set* if

(1) $|D| = k$;
(2) $d_D(x) \in \{\lambda, \lambda + 1\}$ for every $x \neq 0$; and
(3) $\#\{x \neq 0 : d_D(x) = \lambda\} = t$.

Both of the last two conditions belong in the definition. Dropping (3) would leave t out of the predicate altogether, so every t would qualify — even though, by Proposition 2.2 below, (1) and (2) already determine the true count; dropping (2) would say nothing about the remaining $v - 1 - t$ multiplicities. Here t counts the elements attaining the *smaller* multiplicity, as in [1] and [2, §I]; $t = v-1$

is the degenerate case of a difference set. We will use twice, without comment, that $d_D(-x) = d_D(x)$, which holds because $a \mapsto a - x$ is a bijection from $D \cap (D + x)$ onto $D \cap (D - x)$.

Proposition 2.2 (Double counting and the parameter identity)**.** *For every $D \subseteq \mathbb{Z}_v$,*

$$\sum_{x \in \mathbb{Z}_v} d_D(x) \;=\; |D|^2.$$

Consequently, if D is a (v, k, λ, t)-almost difference set then

$$\lambda t + (\lambda + 1)(v - 1 - t) + k \;=\; k^2, \qquad \text{equivalently} \qquad (\lambda + 1)(v - 1) - t \;=\; k(k - 1). \tag{1}$$

In particular $t \leq v - 1$ always, and t is determined by v, k and λ: two almost difference sets in $\mathbb{Z}_v$ with the same k and the same λ have the same t.

Proof. Summing $d_D(x) = \#\{a \in D : a - x \in D\}$ over all x counts each ordered pair $(a, b) \in D \times D$ once, at $x = a - b$; the reindexing $x \mapsto a - x$ shows that for each fixed a the number of x with $a - x \in D$ is $|D|$. Splitting off the term $x = 0$, where $d_D(0) = |D|$, and evaluating the remaining sum by Definition 2.1(2)–(3) gives (1). The second form follows from the first by expanding, and it exhibits t as a function of v, k, λ alone. □

Identity (1) is the reason a cell of the table is a pair and not a quadruple. Since $0 \leq t \leq v - 1$, the integer $\lambda + 1$ is confined to the interval $[q, q + 1]$ with $q = k(k - 1)/(v - 1)$, and when $(v - 1) \nmid k(k - 1)$ that interval contains exactly one integer, so (λ, t) is forced. (When $(v - 1) \mid k(k - 1)$ the two solutions are $t = v - 1$ and $t = 0$, which are the two ways of naming a difference set; that degeneracy is the subject of Theorem 3.1(a).) We record the forced tuples at the cells this paper settles.

Proposition 2.3 (Rigidity of the tuple)**.** *Let (v, k) be one of the thirteen pairs*

$$\begin{array}{lllll} (61, 22), & (61, 28), & (62, 19), & (62, 23), & \\ (62, 27), & (62, 28), & (62, 29), & (63, 19), & \\ (63, 21), & (63, 24), & (63, 25), & (63, 26), & (63, 27), \end{array}$$

and suppose $D \subseteq \mathbb{Z}_v$ is a (v, k, λ, t)-almost difference set. Then (λ, t) is the pair listed for (v, k) in Table 1.

Proof. Each case is (1) together with $0 \leq t \leq v - 1$, which leaves a single pair of nonnegative integers; for instance at $(63, 26)$ one has $k(k - 1) = 650$ and $v - 1 = 62$, so $(\lambda + 1) \cdot 62 - t = 650$ with $0 \leq t \leq 62$ forces $\lambda = 10$, $t = 32$. No search is involved. □

Remark 2.4. The same one-line computation forces the tuple at every other cell of Table 1 as well — $(v - 1) \nmid k(k - 1)$ at all of them. The instances at $(57, 27)$, $(58, 28)$, $(58, 29)$ and $(60, 29)$ are not part of the formal development; the instance at $(61, 30)$ is (Corollary 3.2).

The last general fact we need is complementation, which is why Figure 1 of [1] is drawn only for $k \leq \lfloor v/2 \rfloor$.

Proposition 2.5 (Complementation)**.** *For every $D \subseteq \mathbb{Z}_v$ and every $x \in \mathbb{Z}_v$,*

$$d_{D^c}(x) + 2|D| \;=\; v + d_D(x). \tag{2}$$

Consequently, if D is a (v, k, λ, t)-almost difference set and $2k \leq v + \lambda$, then D^c is a $(v,\ v - k,\ v + \lambda - 2k,\ t)$-almost difference set. The fourth parameter is unchanged.

Proof. Summing the indicator identity $[a \in D^c][a - x \in D^c] = 1 - [a \in D] - [a - x \in D] + [a \in D][a - x \in D]$ over $a \in \mathbb{Z}_v$ gives (2), the two middle sums each contributing $|D|$. So every multiplicity shifts by the same constant $v - 2|D|$; the value condition transports, and the set of x at which the smaller value is attained is literally the same set, so t is preserved. □

Corollary 2.6. *There is a $(63, 37, 21, 32)$-almost difference set in $\mathbb{Z}_{63}$, namely the complement of the witness $W_{63,26}$ of Appendix A.*

Proof. Proposition 2.5 applied to Theorem 4.2 at $(63, 26, 10, 32)$, with $2k = 52 \leq 73 = v + \lambda$. □

Cells with $k > 31$ are outside the range of Figure 1, so Proposition 2.5 carries each witness of Section 4 to a parameter set the table does not draw.

3. The column $k = (v-1)/2$, and the cell $(61, 30, 14, 30)$

The question quoted in Section 1 concerns a single column of the table. It splits, uniformly in the modulus, on $v \bmod 4$.

Theorem 3.1. *Let $D \subseteq \mathbb{Z}_v$ be a (v, k, λ, t)-almost difference set.*

(a) *If $v = 4m + 3$ and $k = 2m + 1 = \frac{v-1}{2}$, then $t \in \{0, v-1\}$, and in either case all $v - 1$ nonzero multiplicities $d_D(x)$ are equal, so D is a difference set.*

(b) *If $v = 4m + 1$ with $m \geq 1$ and $k = 2m = \frac{v-1}{2}$, then $\lambda = m - 1 = \frac{v-5}{4}$ and $t = 2m = \frac{v-1}{2}$.*

Proof. Both parts are (1) with $t \leq v - 1$. In (a) the identity reads $(\lambda + 1)(4m + 2) - t = (2m + 1)2m$, i.e. $(m - \lambda)(4m + 2) = (4m + 2) - t$; the bounds $0 \leq (4m + 2) - t \leq 4m + 2$ force $m - \lambda \in \{0, 1\}$ and hence $t \in \{0, 4m + 2\}$. If $t = v - 1$ every nonzero multiplicity equals λ; if $t = 0$ every one equals $\lambda + 1$. In (b) the identity reads $(\lambda + 1) \cdot 4m - t = 2m(2m - 1)$, and $0 \leq t \leq 4m$ forces $\lambda + 1 = m$ and then $t = 2m$. $\square$

Part (a) is the sharp form of the remark of [1] that $t \neq v-1$ should be added to the question. On the half $v \equiv 3 \pmod 4$ that condition does not do the work it is meant to do: the two admissible values of t are $v-1$ and 0, and at $t = 0$ every nonzero multiplicity equals $\lambda+1$, so D is a difference set there as well. Whatever the naming of t, an almost difference set at those parameters has all its nonzero multiplicities equal, and the surviving content on that half is difference-set existence — which is exactly where the Mann test on $(39, 19, 9)$ and $(51, 25, 12)$ lives. Part (b) says that on the other half the question is never degenerate: $t = \frac{v-1}{2} \neq v - 1$ automatically, and the admissible tuple is $\left(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{2}\right)$, which is the Paley shape.

Corollary 3.2. *If $D \subseteq \mathbb{Z}_{61}$ is a $(61, 30, \lambda, t)$-almost difference set then $\lambda = 14$ and $t = 30$.*

So $(61, 30, 14, 30)$ is not merely *a* parameter tuple at that cell; it is the only one.

Proposition 3.3. *Let $Q \subseteq \mathbb{Z}_{61}$ be the set of 30 nonzero quadratic residues modulo 61. Then Q is a $(61, 30, 14, 30)$-almost difference set, and Q^c, the non-residues together with 0, is a $(61, 31, 15, 30)$-almost difference set. The set $W'_{61,30}$ of Appendix A, a union of cosets of the subgroup $\{1, 13, 47\}$ of $\mathbb{Z}_{61}^{\times}$, is a second $(61, 30, 14, 30)$-almost difference set, and $W'_{61,30} \neq Q$.*

The first assertion is classical: it is Theorem 2(1) of [2] at $q = 61$, listed there as "$D_0^{(2,q)}$ with parameters $\left(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{2}\right)$, where $q \equiv 1 \pmod 4$", and it rests on the order-2 cyclotomic numbers $(0,0)_2 = \frac{p-5}{4}$, $(1,1)_2 = \frac{p-1}{4}$ of [11]. The same set is Theorem 43 of [3], recorded there as a *partial* difference set with parameters $\left(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4}\right)$ — whose last entry is the second multiplicity and not the count t — from which that survey's own remark, that a (v, k, λ, μ)-partial difference set with $|\lambda - \mu| = 1$ is an almost difference set, returns the tuple above. *We claim no novelty for it.* Its interest here is one of placement: the cell $(61, 30)$ is dashed in Figure 1 of [1] and is named there as the first open case of the question of [2], while the construction that settles it is a theorem of [2] itself. The survey [3] has the same gap independently: its concluding problem (2) asks, verbatim, to "Find $\left(n, \frac{n-1}{2}, \frac{n-5}{4}, \frac{n-1}{2}\right)$-ADSs in $\mathbb{Z}_n$", which its own Theorem 43 supplies for every prime $n \equiv 1 \pmod 4$. The second witness is recorded because it shows the cell does not depend on one algebraic coincidence; it was found by the search of Section 5 and, like Q, is invariant under multiplication by 13.

Remark 3.4 (Which text is cited). All quotations from [1], and the reading of its Figure 1, are from the arXiv source. The sentence naming $(61, 30, 14, 30)$ as the first open case is byte-identical in versions v1 (2024-08-29), v2 (2025-03-06) and v3 (2025-04-11), and in each of them it stands in the fourth section, "Computational Results for general ADS". The published version, IEEE Trans. Inform. Theory **71** (2025) 5737–5743, was *not* read: as of 2026-08-28 no open-access or repository copy of it is indexed and the publisher's text is behind a paywall, so nothing here is a claim about its wording. Theorem and problem numbers cited from [3] are those of arXiv:1409.0114v1, its only version.

cell (v, k, λ, t)	u	where	construction
$(57, 27, 12, 26)$	7	Thm. 4.1	search; no published family identified
$(58, 28, 13, 42)$	—	Thm. 4.1	Ding–Helleseth–Martinsen, $\mathbb{Z}_2 \times \mathbb{Z}_{29}$ [2, Thm. 5]
$(58, 29, 14, 43)$	—	Thm. 4.1	the same with 0 adjoined [2, Thm. 6]
$(60, 29, 13, 14)$	—	Thm. 4.1	from a $(15, 7, 3)$ difference set [2, Cor. 1]
$(61, 22, 7, 18)$	13	Thm. 4.2	search; no published family identified
$(61, 28, 12, 24)$	13	Thm. 4.2	search; no published family identified
$(62, 19, 5, 24)$	5	Thm. 4.2	search; no published family identified
$(62, 23, 8, 43)$	5	Thm. 4.2	search; no published family identified
$(62, 27, 11, 30)$	5	Thm. 4.2	search; no published family identified
$(62, 28, 12, 37)$	5	Thm. 4.2	search; no published family identified
$(62, 29, 13, 42)$	5	Thm. 4.2	search; no published family identified
$(63, 19, 5, 30)$	4	Thm. 4.2	search; no published family identified
$(63, 21, 6, 14)$	2	Thm. 4.2	search; no published family identified
$(63, 24, 8, 6)$	2	Prop. 4.3	Cai–Ding product at $m = 6$ [4, Thm. 7.1]
$(63, 25, 9, 20)$	4	Thm. 4.2	search; no published family identified
$(63, 26, 10, 32)$	25	Thm. 4.2	search; no published family identified
$(63, 27, 11, 42)$	4	Thm. 4.2	search; no published family identified
$(61, 30, 14, 30)$	13	Prop. 3.3	Paley; quadratic residues [2, Thm. 2(1)]

TABLE 1. The eighteen cells of Figure 1 of [1] that are dashed there and carry a witness here. The column u gives a multiplier of the witness listed in Appendix A: $uW = W$ in $\mathbb{Z}_v$. The last column records the provenance of the *construction*, not of the cell; see Section 6 for the search behind the entries marked "no published family identified".

Corollary 3.5. *There is no* $(61, 30, 14, 31)$*-almost difference set and no* $(61, 30, 14)$*-difference set in* $\mathbb{Z}_{61}$*; and for no* t *whatsoever is there a* $(61, 30, 13, t)$*- or a* $(61, 30, 15, t)$*-almost difference set.*

Proof. Corollary 3.2. A $(61, 30, 14)$-difference set would be the case $t = v - 1 = 60$. □

Corollary 3.5 is not a result about the mathematics but a control on the formal statement: it says that the tuple in Proposition 3.3 cannot be strengthened in either remaining coordinate, so the witness is not being credited to a weaker claim than intended. Combining Theorem 3.1 with the Paley construction accounts for all thirty entries of the column $k = (v - 1)/2$ of Figure 1 with $v \leq 63$: the fifteen entries with $v \equiv 3 \pmod 4$ are degenerate by (a), so what is being asked there is difference-set existence and not an almost-difference-set question at all; the eight primes $5, 13, 17, 29, 37, 41, 53, 61$ carry Paley sets; and the seven composite $v \equiv 1 \pmod 4$ entries $9, 21, 25, 33, 45, 49, 57$ are already dark in the figure. The first cell of that column not reached by this argument is $v = 65$, past the right-hand edge of the table.

4. Sixteen dashed cells

Theorem 4.1. *There exist almost difference sets in* $\mathbb{Z}_v$ *with parameters*

$$(57, 27, 12, 26), \qquad (58, 28, 13, 42), \qquad (58, 29, 14, 43), \qquad (60, 29, 13, 14).$$

Explicit witnesses are $W_{57,27}$*,* $W_{58,28}$*,* $W_{58,29}$ *and* $W_{60,29}$ *of Appendix A. All four cells are dashed in Figure 1 of* [1].

Theorem 4.2. *There exist almost difference sets in* $\mathbb{Z}_v$ *with parameters*

$$\begin{array}{llll} (61, 22, 7, 18), & (61, 28, 12, 24), & (62, 19, 5, 24), & (62, 23, 8, 43), \\ (62, 27, 11, 30), & (62, 28, 12, 37), & (62, 29, 13, 42), & (63, 19, 5, 30), \\ (63, 21, 6, 14), & (63, 25, 9, 20), & (63, 26, 10, 32), & (63, 27, 11, 42). \end{array}$$

Explicit witnesses are the corresponding sets $W_{v,k}$ *of Appendix A; each is a union of orbits of* $x \mapsto ux$ *for the unit* u *listed in Table 1. All twelve cells are dashed in Figure 1 of* [1].

Proposition 4.3. *There is a* $(63, 24, 8, 6)$*-almost difference set in* $\mathbb{Z}_{63}$*, namely* $W_{63,24}$ *of Appendix A; the cell* $(63, 24)$ *is dashed in Figure 1 of* [1]*. These parameters are those of the product construction of Cai and Ding* [4, Thm. 7.1] *at* $m = 6$*: for even* m*, with* $R_1 = \{x \in \mathrm{GF}(2^m) : \mathrm{Tr}_{2^m/2^{m/2}}(x) = 1\}$ *and* R_2 *a* $\bigl(2^{m/2} - 1,\, 2^{(m-2)/2} - 1,\, 2^{(m-4)/2} - 1\bigr)$*-difference set in* $\mathrm{GF}(2^{m/2})^\times$*, the product* $R = \{r_1 r_2 : r_1 \in R_1,\ r_2 \in R_2\}$ *is a* $\bigl(2^m - 1,\, 2^{m-1} - 2^{m/2},\, 2^{m-2} - 2^{m/2},\, 2^{m/2} - 2\bigr)$*-almost difference set in* $\mathrm{GF}(2^m)^\times$*, a cyclic group of order* $2^m - 1$*; at* $m = 6$ *the tuple reads* $(63, 24, 8, 6)$ *and the group is* $\mathbb{Z}_{63}$*. Only the application to a cell the table leaves undetermined is new.*

Proof of Theorems 4.1 and 4.2 and Proposition 4.3. Each statement asserts that one explicit finite set has a prescribed difference spectrum, so each is a finite evaluation and nothing more. For a set $W \subseteq \mathbb{Z}_v$ with $v \le 63$ one computes the $v - 1$ numbers $d_W(x)$ — at most 31 of them, since $d_W(-x) = d_W(x)$ — and checks that they take only the values λ and $\lambda + 1$ and that the value λ occurs t times. With the witnesses printed in Appendix A this is a computation a reader can carry out by hand at any single cell. In the formal development each of these checks is a single Boolean evaluated by the compiler; see Section 8.

Nothing in these three statements depends on the searches of Section 5: the searches produced the witnesses, and the witnesses are now data. For the same reason the correctness of the search program is irrelevant to the theorems.

The parameter tuple attached to each cell is not a choice: at the thirteen cells with $v \ge 61$ it is forced by Proposition 2.3, and at the remaining four by the identical computation (Remark 2.4). Finally, the three cells $(58, 28, 13, 42)$, $(58, 29, 14, 43)$ and $(60, 29, 13, 14)$ also arise from published constructions. Theorems 5 and 6 of [2] — the Ding–Helleseth–Martinsen classes, as [2] attributes them — give almost difference sets of $\mathrm{GF}(2) \times \mathrm{GF}(q)$ with parameters $\bigl(n, \frac{n-2}{2}, \frac{n-6}{4}, \frac{3n-6}{4}\bigr)$ and $\bigl(n, \frac{n}{2}, \frac{n-2}{4}, \frac{3n-2}{4}\bigr)$, $n = 2q$, for $q \equiv 5 \pmod 8$ with quadratic partition $q = s^2 + 4b^2$, $s \equiv \pm 1 \pmod 4$; at $q = 29 = 5^2 + 4 \cdot 1^2$, where $b = 1$ and the first index alternative of each theorem applies, $n = 58$ and the two tuples read $(58, 28, 13, 42)$ and $(58, 29, 14, 43)$, transported through $\mathbb{Z}_2 \times \mathbb{Z}_{29} \cong \mathbb{Z}_{58}$. Corollary 1 of [2] — which that paper derives not from its interleaving construction, its Theorem 17, but from a theorem of Jungnickel on divisible designs — turns an ordinary $\bigl(l, \frac{l-1}{2}, \frac{l-3}{4}\bigr)$-difference set into a $(4l,\, 2l - 1,\, l - 2,\, l - 1)$-almost difference set of $\mathbb{Z}_4 \times \mathbb{Z}_l$; at $l = 15$, applied to $\{0, 1, 2, 4, 5, 8, 10\}$ through $\mathbb{Z}_4 \times \mathbb{Z}_{15} \cong \mathbb{Z}_{60}$, that is $(60, 29, 13, 14)$. The witnesses given here were obtained independently by both routes, which agree. ☐

Remark 4.4 (Autocorrelation). Reading $D \subseteq \mathbb{Z}_v$ as the support of a binary sequence of period v and passing to the ± 1 form, the periodic autocorrelation at shift $x \ne 0$ is $C(x) = v - 4\bigl(k - d_D(x)\bigr)$. So a (v, k, λ, t)-almost difference set has exactly two out-of-phase autocorrelation values, $v - 4(k - \lambda)$ and $v - 4(k - \lambda) + 4$. For the witness at $(61, 28, 12, 24)$ these are $\{1, -3\}$, and for the three witnesses at $(62, 27, 11, 30)$, $(62, 28, 12, 37)$ and $(62, 29, 13, 42)$ they are $\{2, -2\}$. These are exactly the value sets that [2, §V] and [4, §1] call *optimal* autocorrelation at periods $n \equiv 1$ and $n \equiv 2 \pmod 4$, with the asymmetry that [4, §1] is explicit about: at $n \equiv 2 \pmod 4$ the bound $\max_{w \ne 0} |C(w)| \ge 2$ is a theorem, so $\{2, -2\}$ is optimal outright, whereas at $n \equiv 1 \pmod 4$ the value 3 is the accepted optimum only because $\max_{w \ne 0} |C(w)| = 1$ is believed impossible for $n > 13$.

All four are attained here away from the balanced weight. Of the constructions catalogued for these two period classes in [4, §§5–6], those of period $n \equiv 2 \pmod 4$ produce weight $n/2$ (Sidelnikov–Lempel–Cohn–Eastman) or $n/2 - 1$ and $n/2$ (Ding–Helleseth–Martinsen), and the Legendre and Ding–Helleseth–Lam families of period $n \equiv 1 \pmod 4$ produce weight $(n - 1)/2$; the one remaining family there, from generalized cyclotomy, has composite period $p(p + 4)$ and so cannot have period 61 at all. At $v = 61$ and $v = 62$ those weights are 30 and $\{30, 31\}$, whereas the witnesses here sit at 28 and at $27, 28, 29$. These four are the cells where we would look first, in either direction, before treating the provenance question of Section 6 as settled.

5. The search

This section describes the computation that produced the witnesses. It supports no statement in the paper — the theorems of Section 4 are evaluations of explicit data — but it is what a reader would need in order to repeat or extend the work, and it is the reason the cells were reached at all.

Why an algebraic class, and not local search. Local search is the wrong instrument here, and that was measured rather than assumed. For $D \subseteq \mathbb{Z}_v$ of fixed size the energy $E(D) = \sum_{x\neq 0} d_D(x)^2$ has fixed sum $\sum_{x\neq 0} d_D(x) = k(k-1)$ by Proposition 2.2, so E is minimized exactly on the ADS spectrum, and its minimum at $(61, 30)$ is $30 \cdot 14^2 + 30 \cdot 15^2 = 12630$. A tabu search over the 30-subsets of $\mathbb{Z}_{61}$ — full swap neighbourhood of size $30 \cdot 31 = 930$ scanned at every step, aspiration on the global best, randomized tenure, restarts on stagnation — ran 250 000 moves in 60 seconds and never reached a solution, plateauing at $E = 12634$; an earlier simulated annealer stalled at the same value. Since $(61, 30)$ is a cell where solutions demonstrably exist (Proposition 3.3), this is a calibration failure of the method and not evidence about any cell. The explanation is that the solutions are algebraically rigid — unions of cyclotomic classes, isolated in the swap landscape. The search therefore looked where such objects live, and every witness in Table 1 was found in at most 0.02 seconds of wall clock.

The multiplier class. The class searched is: all $D \subseteq \mathbb{Z}_v$ invariant under some affine map $\sigma(x) = ux+c$ with $u \in \mathbb{Z}_v^\times$ and $\sigma \neq \mathrm{id}$. Three reductions make its enumeration exhaustive rather than heuristic. A set invariant under a nontrivial group of such maps is invariant under a cyclic subgroup, so it suffices to enumerate the cycles of a single σ. A quasi-multiplier ($uD = D + s$, the form that occurs when a set has no honest multiplier) is invariance under $x \mapsto u^{-1}x - u^{-1}s$ and is already in the class. And conjugating σ by $x \mapsto x + d$ replaces c by $c + d(1-u)$, so c matters only modulo $(1-u)\mathbb{Z}_v$ and finitely many c per u exhaust it. For each σ the orbits partition $\mathbb{Z}_v$ and the candidates are the unions of orbits of total size k, enumerated by depth-first search with prefix-sum pruning, partitions deduplicated and tried coarsest first. Because $v \leq 63$, a subset is a single 64-bit word and $d_D(x)$ is the population count of $D \wedge \mathrm{rot}_v(D, x)$, so a candidate costs on the order of ten nanoseconds; that is what makes the enumeration a statement about a class rather than a sample from it.

All 94 dashed cells were run through this enumeration. Two affine maps were skipped as too expensive to enumerate, both of the "fix a large subgroup pointwise" kind: $x \mapsto 29x$ on $\mathbb{Z}_{56}$ (42 orbits) and $x \mapsto 31x$ on $\mathbb{Z}_{60}$ (45 orbits); no other map at any $v \in \{54, \ldots, 63\}$ exceeded 40 orbits. At 39 of the 76 cells that remain undetermined, the enumeration of this class ran to completion without a witness — at the one of those 39 with $v = 56$, namely $(56, 20)$, "to completion" means apart from the skipped map, and no cell of the 39 has $v = 60$. *That is a statement about the class, not about the cell*: it says that a construction of the kind used here does not exist there, so more cyclotomy will not help, and it says nothing about existence. No nonexistence is asserted anywhere in this paper.

Two further classes, as controls. Two other searches were run and produced nothing new, which is itself information about where the remaining witnesses can live. *Interleaving*: for composite $v = ab$ with $\gcd(a, b) = 1$, sets of the form $\bigcup_{i\in\mathbb{Z}_a} \{i\} \times (S_i + c_i)$ through $\mathbb{Z}_v \cong \mathbb{Z}_a \times \mathbb{Z}_b$, with each S_i a union of cyclotomic classes of $\mathbb{Z}_b$ and independent shifts c_i (normalizing $c_0 = 0$); this is the shape of the $(60, 29, 13, 14)$ witness and it lies outside the multiplier class. It was run on 86 (cell, factorization) pairs over the 57 open cells admitting a coprime splitting, and was truncated by its time budget at $a \in \{7, 8\}$. *One point off a multiplier*: unions of orbits of size $k \mp 1$ with one element added or removed, over partitions into at most 18 orbits; 152 (cell, direction) probes, all completed within that restriction.

Calibration. No search here is trusted on its own word. The multiplier enumeration re-finds all five cells that had been settled before it was written — $(57, 27)$, $(58, 28)$, $(58, 29)$, $(60, 29)$ and $(61, 30)$ — and at $(57, 27)$ returns the same witness element for element. The interleaving search independently re-finds $(58, 28, 13, 42)$ and $(60, 29, 13, 14)$, and the $\mathbb{Z}_{58}$ witnesses were also built directly from the order-4 cyclotomic classes of $\mathbb{Z}_{29}$; the two routes agree, which is what checks the transport through the Chinese-remainder isomorphism. Finally every witness is re-checked against an independent implementation of Definition 2.1 in Lean (Section 8): a fault in the search program would have to be mirrored there to survive.

6. Which published families reach these cells

Thirteen of the sixteen cells of Theorems 4.1 and 4.2 — all twelve of Theorem 4.2, and $(57, 27, 12, 26)$ — were not matched to any published construction. This section records what was searched and, in the same breath, what was not; the conclusion is "not found", which is weaker than "new" and is offered as such.

Read in full text: [2] (its Theorem 2, the cyclotomic catalogue of orders 2, 4 and 8; Theorem 4, Lempel–Cohn–Eastman and Sidelnikov; Theorems 5 and 6, Ding–Helleseth–Martinsen; Theorem 9, Davis; Theorems 21 and 22, the period-4ℓ families); [5], including its Table V, "Known cyclotomic almost difference sets of $\mathbb{Z}_N$"; [6]; [4], including §§5–6, which enumerate the known optimal-autocorrelation families at each period class; [7]; the survey [3] in full; and [1] including its Theorems 3–5 and Table II. Where those families stop, at the four moduli that matter here:

- $v = 57 = 3 \cdot 19$: here $57 \equiv 1 \pmod 4$, and none of the three families that [4, §6] lists for that period class applies — the Legendre and Ding–Helleseth–Lam families need the period to be prime, and the generalized-cyclotomy family needs it to be $p(p + 4)$, which 57 is not. The cyclotomic catalogues of [2, Thm. 2] and [5, Table V] are stated in $\mathrm{GF}(q)$ and in $\mathbb{Z}_N$ for N prime respectively, and 57 is neither a prime power nor prime; Theorem 4 of [2] needs $v = q-1$, and 58 is not a prime power.
- $v = 61$: among the cyclotomic families listed in Theorem 2 of [2] and in Table V of [5], those whose hypotheses hold at $N = 61$ are Theorem 2(1) of [2] ($q \equiv 1 \pmod 4$), giving $(61, 30, 14, 30)$, and its Theorem 2(2) ($q = 25 + 4y^2$, here $y = 3$), giving $(61, 15, 3, 30)$, together with one sporadic order-6 entry of [5, Table V] at $N = 61$, again a set of size 30. Every one of them has $k \in \{15, 30\}$, and nothing in either catalogue reaches $k = 22$ or $k = 28$. Both witnesses at those cells are unions of cyclotomic classes of order 20 together with 0; the published work on order-20 classes that the search reached is about difference sets, not almost difference sets [10]. One further route to $(61, 22, 7, 18)$ is closed by [1] itself: Theorem 3 there would produce that tuple by adding one element to a $(61, 21, 7)$-difference set, and the cell $(61, 21)$ is white in Figure 1, reported there as carrying no almost difference set at all.
- $v = 62 = 2 \cdot 31$: [4, §5] enumerates the known families of period $N \equiv 2 \pmod 4$ as Sidelnikov–Lempel–Cohn–Eastman ($N = q - 1$ with $q \equiv 3 \pmod 4$ a power of an odd prime, which would need $q = 63$), Ding–Helleseth–Martinsen ($N = 2q$ with $q \equiv 5 \pmod 8$ prime, but $31 \equiv 7$), and the families of period $p^m - 1$ of [9], which would need $p^m = 63$. None applies.
- $v = 63$: the catalogued sets are the cyclic difference sets with Singer parameters $(63, 31, 15)$ — [4, §3.2] lists the Singer, hyperoval, five-people, Dillon–Dobbertin and Gordon–Mills–Welch constructions — together with the Cai–Ding set of Proposition 4.3. Theorems 3–5 of [1] add or remove one element of a (v, k, λ)-difference set to get a $(v, k+1, \lambda, v-1-2k)$- or a $(v, k-1, \lambda-1, 2(k-1))$-almost difference set; on any cyclic $(63, 31, 15)$-difference set that is $(63, 32, 15, 0)$ and $(63, 30, 14, 60)$, not the tuples here. Theorem 2 of [2] needs v a prime power and its Theorem 4 needs $v = q - 1$ with q a power of an odd prime, so $v = 63$ is outside both.

Remark 6.1 ($(63, 26, 10, 32)$ and the $\mathrm{GF}(64)$ route). At one cell the exclusion is sharper, by a computation carried out outside the formal development. The witness $W_{63,26}$ has multiplier group exactly $\{1, 25, 58\}$, and 2 is not a multiplier of it even up to translation; moreover no union of 2-cyclotomic cosets modulo 63 of size 26 is an almost difference set at all — there are 13 such cosets, so this is an exhaustive check over 2^{13} unions. Hence no Frobenius-invariant construction in $\mathrm{GF}(64)$ — which is the shape of every family listed above at $v = 63$, the Singer-parameter difference sets and the Cai–Ding set alike — reaches $(63, 26)$. This is a statement about that class of constructions, not a nonexistence statement about the cell, and it is not part of the formal development.

The limits of the search, stated plainly. [8] was not read: as of 2026-08-28 the publisher's text is behind a paywall and no open copy of it is indexed, so its range $v \le 50$ is taken on the authority of [1], and 50 is below every modulus in Table 1. [9] and [10] *were* read in full text — the former in an author-hosted reprint, the latter in the publisher's open-access copy. [9] restricts itself to periods $p^m - 1$ with p an odd prime, which excludes 62 (since 63 is not a prime power) and 63 (since $64 = 2^6$); [10] constructs difference sets, not almost difference sets, from unions of cyclotomic classes of orders 12, 20 and 24 in $\mathrm{GF}(q)$ for $q < 10^5$. The companion papers of that series, on cyclotomic classes of other orders, were not read. Of the reviewing databases, zbMATH was searched and returned nothing at these parameters — it has no full-text index, so the tuples themselves cannot be queried there, only titles, abstracts and reviews — and MathSciNet could not be reached. Under those limits, the thirteen cells are recorded as witnesses whose parameters were not matched to a published family, and not as new objects.

7. Validation against published data

Three independent checks of the formal definition against published values were run. All three agree with the published data; no discrepancy was found.

Proposition 7.1. (a) *The five sets listed in Table II of* [1] *— the almost difference sets there reported as missed by the earlier table of* [8] *— are almost difference sets with the parameters assigned to them there, namely* $(39, 17, 7, 32)$*,* $(48, 17, 5, 10)$*,* $(48, 22, 9, 8)$*,* $(48, 23, 10, 11)$ *and* $(50, 20, 7, 12)$*.*

(b) *For every prime* $p \equiv 1 \pmod 4$ *with* $p \le 113$*, that is for*

$$p \in \{5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113\},$$

the nonzero quadratic residues modulo p *form a* $\left(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{2}\right)$*-almost difference set.*

(c) *At* $p = 59 \equiv 3 \pmod 4$ *the nonzero quadratic residues form a* $(59, 29, 14, 58)$*-almost difference set, that is a* $(59, 29, 14)$*-difference set, and they are not a* $(59, 29, 14, 29)$*-almost difference set.*

Part (a) exercises Definition 2.1 at moduli and tuples far from the Paley family — t as small as 8 — so it tests the definition on the unbalanced side, and it reproduces published data exactly. In part (b) the eight primes up to 61 reproduce the column $k = (v-1)/2$ of Figure 1 of [1] and the other six extend it past the right-hand edge of that figure. Part (c) is the boundary case: it is Theorem 3.1(a) in one instance, and it is why the hypothesis $p \equiv 1 \pmod 4$ is needed in Proposition 3.3.

8. Verification

Every theorem, proposition and corollary of this paper has been formally verified in Lean 4 against *Mathlib*; the development is free of `sorry`, and the repository reference is to be added at submission. The remarks are outside it: the computation behind Remark 6.1, the four instances named in Remark 2.4, the autocorrelation arithmetic of Remark 4.4 and the bibliographic statements of Remark 3.4 are not formalized. The split between what is proved and what is evaluated is exactly the split between the counting layer and the witnesses.

Kernel-checked by argument, with no appeal to computation and uniformly in the modulus: the double-counting identity and the parameter identity of Proposition 2.2; the determination of t by (v, k, λ); the rigidity statements of Proposition 2.3 and Corollary 3.2; both parts of Theorem 3.1; the complement identity and complementation theorem of Proposition 2.5; and the negative statements of Corollary 3.5, which are arithmetic and not searches. These depend on no axioms beyond `propext`, `Classical.choice` and `Quot.sound`. Corollary 2.6 is proved by the same argument, but from Theorem 4.2 as input, so it inherits that theorem's evaluation and adds no computation of its own.

Delegated to compiled evaluation, through Lean's `native_decide`: every witness statement, i.e. Theorems 4.1 and 4.2, Propositions 3.3 and 4.3, the fourteen multiplier identities $uW = W$ of Table 1 for the witnesses of Theorem 4.2, Proposition 4.3 and the cell $(57, 27)$, and the checks of Section 7. (The invariance under 13 of the two witnesses at $(61, 30)$ is recorded in Table 1 but not separately formalized; for the Paley set it is immediate, 13 being a quadratic residue modulo 61.) Each of these is one Boolean: the decision procedure for Definition 2.1 applied to a set given by explicit data. Such a statement carries the corresponding native-evaluation axiom, and each of them is small enough that a reader can confirm it independently from Appendix A.

Two families of controls keep the definition honest. On the too-strong side, Corollary 3.5 and Proposition 2.3 refute every neighbouring tuple at their cells by argument, so a witness cannot be credited with more than it shows. On the too-weak side, each witness of Theorems 4.1 and 4.2, of Proposition 4.3 and the Paley set is re-tested at the neighbouring value of t and rejected, so the counting clause of Definition 2.1 is doing work in every case; in addition, at $(61, 30)$ the Paley witness with one residue exchanged for a non-residue, an interval of 30 consecutive residues, the empty set and the whole group are all rejected. Finally, the witnesses were produced by an implementation in C and the formal statements were written against its output afterwards, so the two implementations of Definition 2.1 are independent.

Appendix A. The witnesses

Each set below is a subset of $\mathbb{Z}_v$ for the v of its cell, written with representatives in $\{0, 1, \ldots, v-1\}$. The column u repeats the multiplier of Table 1: $uW = W$ in $\mathbb{Z}_v$, so the set is a union of orbits of $x \mapsto ux$ and can be reconstructed from a few representatives. The set $W'_{61,30}$ is the second witness of Proposition 3.3; $W_{61,30}$ is the set of nonzero quadratic residues.

cell	u	witness
$(57, 27, 12, 26)$	7	{1, 2, 3, 4, 5, 6, 7, 9, 11, 14, 16, 17, 20, 21, 25, 26, 28, 29, 32, 33, 35, 41, 42, 43, 49, 53, 55}
$(58, 28, 13, 42)$	—	{1, 2, 5, 7, 9, 13, 14, 16, 20, 23, 24, 25, 30, 32, 33, 35, 36, 40, 45, 46, 48, 49, 50, 51, 52, 53, 54, 57}
$(58, 29, 14, 43)$	—	{0, 1, 2, 5, 7, 9, 13, 14, 16, 20, 23, 24, 25, 30, 32, 33, 35, 36, 40, 45, 46, 48, 49, 50, 51, 52, 53, 54, 57}
$(60, 29, 13, 14)$	—	{1, 2, 5, 10, 12, 15, 17, 19, 23, 24, 25, 28, 30, 31, 34, 35, 36, 38, 44, 45, 46, 47, 48, 49, 50, 52, 53, 55, 56}
$(61, 22, 7, 18)$	13	{0, 1, 2, 6, 7, 13, 16, 17, 20, 24, 25, 26, 28, 30, 33, 35, 36, 38, 41, 45, 47, 59}
$(61, 28, 12, 24)$	13	{0, 1, 2, 3, 4, 5, 8, 10, 13, 14, 19, 22, 26, 28, 32, 33, 35, 39, 40, 42, 43, 47, 48, 50, 52, 58, 59, 60}
$(62, 19, 5, 24)$	5	{1, 2, 4, 5, 10, 20, 21, 25, 29, 31, 32, 34, 36, 38, 43, 44, 46, 50, 56}
$(62, 23, 8, 43)$	5	{0, 1, 2, 4, 5, 7, 10, 11, 12, 20, 25, 27, 31, 34, 35, 38, 44, 46, 50, 51, 52, 55, 60}
$(62, 27, 11, 30)$	5	{1, 2, 3, 5, 7, 10, 12, 13, 15, 16, 18, 25, 28, 32, 34, 35, 36, 37, 44, 46, 50, 51, 52, 56, 57, 60, 61}
$(62, 28, 12, 37)$	5	{0, 1, 2, 3, 4, 5, 7, 10, 13, 15, 16, 18, 20, 24, 25, 28, 34, 35, 37, 38, 42, 44, 46, 50, 51, 57, 58, 61}
$(62, 29, 13, 42)$	5	{0, 1, 2, 3, 5, 7, 8, 10, 11, 13, 14, 15, 16, 18, 25, 27, 28, 31, 32, 34, 35, 36, 40, 44, 46, 50, 51, 55, 56}
$(63, 19, 5, 30)$	4	{0, 1, 2, 4, 5, 7, 8, 11, 16, 17, 20, 28, 30, 32, 39, 44, 49, 50, 57}
$(63, 21, 6, 14)$	2	{0, 1, 2, 3, 4, 6, 8, 12, 13, 16, 19, 21, 24, 26, 32, 33, 38, 41, 42, 48, 52}
$(63, 24, 8, 6)$	2	{1, 2, 3, 4, 5, 6, 8, 10, 12, 16, 17, 20, 23, 24, 29, 32, 33, 34, 40, 43, 46, 48, 53, 58}
$(63, 25, 9, 20)$	4	{1, 2, 3, 4, 8, 9, 11, 12, 13, 16, 18, 19, 30, 31, 32, 36, 39, 42, 44, 48, 50, 52, 55, 57, 61}
$(63, 26, 10, 32)$	25	{0, 1, 2, 3, 4, 5, 10, 12, 13, 19, 21, 25, 27, 31, 34, 37, 38, 43, 45, 48, 50, 53, 54, 58, 61, 62}
$(63, 27, 11, 42)$	4	{0, 1, 2, 4, 5, 7, 8, 10, 16, 17, 20, 21, 27, 28, 31, 32, 34, 40, 42, 45, 47, 49, 54, 55, 59, 61, 62}
$(61, 30, 14, 30)$	13	{1, 3, 4, 5, 9, 12, 13, 14, 15, 16, 19, 20, 22, 25, 27, 34, 36, 39, 41, 42, 45, 46, 47, 48, 49, 52, 56, 57, 58, 60}
$(61, 30, 14, 30)'$	13	{1, 2, 3, 9, 12, 13, 15, 19, 22, 26, 27, 28, 31, 33, 34, 35, 36, 37, 39, 41, 42, 45, 46, 47, 49, 54, 56, 57, 58, 59}

Three of the sets have a shorter description. Modulo 63, writing $C_s = \{s2^i\}$ for the 2-cyclotomic cosets, $W_{63,21} = C_0 \cup C_1 \cup C_3 \cup C_{13} \cup C_{21}$ and $W_{63,24} = C_1 \cup C_3 \cup C_5 \cup C_{23}$; and $W_{61,30}$ is the group of nonzero squares modulo 61. At $v = 61$ the multiplier 13 generates the subgroup $\{1, 13, 47\}$ of order 3, whose cosets are the twenty cyclotomic classes of order 20; at $v = 62$ the unit 5 also has order 3 and corresponds to $(1, 5)$ under $\mathbb{Z}_{62} \cong \mathbb{Z}_2 \times \mathbb{Z}_{31}$, where $\langle 5 \rangle$ has index 10 in $\mathbb{Z}_{31}^{\times}$; at $v = 63$ the units 2, 4 and 25 have orders 6, 3 and 3.

References

[1] D. M. Gordon, *Modular Golomb rulers and almost difference sets*, arXiv:2408.16721; published as IEEE Trans. Inform. Theory **71** (2025), no. 7, 5737–5743, doi:10.1109/TIT.2025.3566655. Citations here are to the arXiv source; see Remark 3.4.

[2] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar and H. M. Martinsen, *Almost difference sets and their sequences with optimal autocorrelation*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 2934–2943, doi:10.1109/18.959271.

[3] K. Nowak, *A survey on almost difference sets*, arXiv:1409.0114v1.

[4] Y. Cai and C. Ding, *Binary sequences with optimal autocorrelation*, Theoret. Comput. Sci. **410** (2009), no. 24–25, 2316–2322, doi:10.1016/j.tcs.2009.02.021.

[5] C. Ding, T. Helleseth and K. Y. Lam, *Several classes of binary sequences with three-level autocorrelation*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2606–2612, doi:10.1109/18.796414.

[6] C. Ding, T. Helleseth and H. Martinsen, *New families of binary sequences with optimal three-level autocorrelation*, IEEE Trans. Inform. Theory **47** (2001), no. 1, 428–433, doi:10.1109/18.904555.

[7] C. Ding, A. Pott and Q. Wang, *Constructions of almost difference sets from finite fields*, Des. Codes Cryptogr. **72** (2014), no. 3, 581–592, doi:10.1007/s10623-012-9789-9.

[8] Y. Zhang, J. G. Lei and S. P. Zhang, *A new family of almost difference sets and some necessary conditions*, IEEE Trans. Inform. Theory **52** (2006), no. 5, 2052–2061, doi:10.1109/TIT.2006.872969.

[9] J.-S. No, H. Chung, H.-Y. Song, K. Yang, J.-D. Lee and T. Helleseth, *New construction for binary sequences of period* $p^m - 1$ *with optimal autocorrelation using* $(z+1)^d + az^d + b$, IEEE Trans. Inform. Theory **47** (2001), no. 4, 1638–1644, doi:10.1109/18.923752.

[10] J. M. P. Balmaceda and B. M. Estrella, *Difference sets from unions of cyclotomic classes of orders* 12*,* 20*, and* 24, Philipp. J. Sci. **150** (2021), no. 6B, 1803–1810, doi:10.56899/150.6b.16.

[11] T. Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics **2**, Markham Publishing Company, Chicago, 1967.