SIGNED DIFFERENCE SETS FROM PERFECT NONLINEAR FUNCTIONS

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. A signed difference set in a finite abelian group G of order v is an element $D = \sum_g a_g\, g$ of $\mathbb{Z}[G]$ with $a_g \in \{0, \pm 1\}$, support size k, satisfying $DD^{(-1)} = (k-\lambda)\, 0_G + \lambda G$. He and Wu recently produced a $(125, 28, 3)$ signed difference set in C_5^3 out of quartic multiplicative characters of $\mathbb{F}_{25}$ and $\mathbb{F}_5$, together with quartic Jacobi sums. We show that their signed set is, verbatim, the graph of the norm map $\mathrm{N}\colon \mathbb{F}_{25} \to \mathbb{F}_5$ with the subgroup $\{0\} \times \mathbb{F}_5$ subtracted, so that no character theory is needed to see it. What that identity uses is only perfect nonlinearity: if $f\colon A \to B$ is a map of finite abelian groups with $|A| = n^2$, $|B| = n$ and every nonzero derivative of f balanced, then $\Gamma_f - (\{0\} \times B)$ is an $(n^3,\, n^2 + n - 2,\, n - 2)$ signed difference set. Binary quadratic forms of nonzero discriminant supply such an f over every finite field and in every characteristic, so there is a signed difference set with parameters $(q^3,\, q^2 + q - 2,\, q - 2)$ in the elementary abelian group of order q^3, for every prime power q; the He–Wu example is the case $q = 5$. Three members of the family — at $(27, 10, 1)$ in C_3^3, $(64, 18, 2)$ in C_2^6 and $(343, 54, 5)$ in C_7^3 — occupy cells recorded as open in Gordon's signed difference set database, and two further members are beyond its parameter range. We also exhibit two inequivalent $(125, 28, 3)$ signed difference sets in C_5^3, separated by an affine-covariant invariant, so the He–Wu set is one of at least two classes there. All statements are formally verified in Lean 4.

1. Introduction

1.1. **The objects.** Let G be a finite abelian group of order v, written additively, and identify a subset of G with the corresponding element of the integral group ring $\mathbb{Z}[G]$. A (v, k, λ) *difference set* is a k-subset $D \subset G$ with

$$DD^{(-1)} = n \cdot 0_G + \lambda G, \qquad n = k - \lambda, \tag{1}$$

in $\mathbb{Z}[G]$. Gordon [1] observed that (1) keeps its interest when the coefficients of D are allowed to be negative: writing $D = \sum_{g \in G} a_g\, g$ with $a_g \in \{0, +1, -1\}$, positive support $P = \{g : a_g = 1\}$, negative support $N = \{g : a_g = -1\}$ and *support size* $k = |P| + |N|$, he calls D a (v, k, λ) *signed difference set* (SDS) when (1) holds. Two familiar notions sit inside the definition as degenerate cases: $N = \varnothing$ gives an ordinary difference set, and $\lambda = 0$ gives a group-developed weighing matrix, circulant when G is cyclic. Note that λ may be negative and that k counts the whole support, not $|P|$.

Reading (1) coefficientwise is the form we work with throughout. The coefficient of t in $DD^{(-1)}$ is the periodic autocorrelation

$$C_a(t) \;=\; \sum_{h \in G} a_{t+h}\, a_h, \tag{2}$$

so (1) says exactly that $C_a(0) = k$ and $C_a(t) = \lambda$ for every $t \neq 0$. In the cyclic case this is the statement that the ternary sequence (a_g) has two-level periodic autocorrelation.

1.2. **The source and its open questions.** Existence for signed difference sets is organised by cells: a cell is a quadruple (v, k, λ, G) with G named by its invariant factors. Gordon maintains a database of cells [3]; the snapshot we downloaded on 2026-08-29 (5,193,480 bytes, md5 `3c0190930707d47740f0852d43580187`) has 70,543 keys, of which 87 are marked `Yes`, 59 `All`, 2,574 `No`, and 67,823 `Open`, the `Open` entries having v ranging over exactly $9 \le v \le 499$. The file is not merely what we happened to fetch on that day: it is byte-for-byte the blob of the last commit to touch `sds.json`, dated 2026-04-24, and was still the state of the default branch when we read it, so the snapshot is the database as it has stood since that date. He and Wu [5] attack that list. Their abstract reads, in part:

> "Applied cumulatively to the 67,823 open group-specific cases in the database with $9 \le v \le 499$, these criteria rule out 45,361 cases. For existence, we construct an infinite family from PCP-type regular partial difference sets arising from Desarguesian spreads and an explicit $(125, 28, 3)$-SDS in C_5^3 using quartic multiplicative characters. These constructions settle three further open cases."

The two counts they start from are exactly the two we reproduce from the file, which is what identifies it as the database they work against. We do *not* reproduce their elimination of 45,361 cases: their four obstructions — the self-conjugate prime criterion, the C_2-quotient, near-full-support and small-defect obstructions — are taken here as published, and nothing below depends on them.

The open question the present paper addresses is the constructive one. The known constructions are sparse and shape-specific. Gordon [1] gives, among others, a $(4n-1, 2n, n-2)$ family from Paley difference sets, a quartic-residue family with parameters $\big(v, (v+3)/4, (v-13)/16\big)$ conditional on a Gauss-sum identity, and a prime-pair family $(4n-9, 2n-1, n-1)$ in $\mathrm{GF}(q) \oplus \mathrm{GF}(r)$. He, Chen and Ge [4] add families from partial difference sets, including $(3^{2m+1}, 3^{2m}+1, 1)$ — but their theorem opens "Let m be an even integer", so their smallest instance is $(243, 82, 1)$. He and Wu [5] add the Desarguesian-spread family and the single $(125, 28, 3)$ example. We have not found the parameter shape $(q^3,\ q^2+q-2,\ q-2)$ obtained below among any of them.

1.3. **What is settled here.** The starting point is an identification. He and Wu define their positive support by $P = \{(x, y) \in \mathbb{F}_{25}^* \times \mathbb{F}_5^* : \rho(x) = \sigma(y)\}$ for quartic characters ρ of $\mathbb{F}_{25}$ and σ of $\mathbb{F}_5$, and their negative support by $N = \{0\} \times \mathbb{F}_5^*$. Passing $\rho(x) = \sigma(y)$ through the discrete logarithm turns it into $\mathrm{N}_{25/5}(x) = y$ (Proposition 4.2). So their signed set is

$$D \;=\; \Gamma_{\mathrm{N}} - L, \qquad \Gamma_{\mathrm{N}} = \{(x, \mathrm{N}(x)) : x \in \mathbb{F}_{25}\}, \qquad L = \{0\} \times \mathbb{F}_5,$$

the graph of the norm map with a subgroup removed. Nothing in that description mentions $q = 5$, quartic characters, or Jacobi sums. What it uses is that Γ_{N} is a transversal of L and that every nonzero derivative of the norm is balanced. Section 3 proves the general statement:

- **Theorem 3.3.** If $f\colon A \to B$ has $|A| = n^2$, $|B| = n$ and every nonzero derivative $x \mapsto f(x+t) - f(x)$ balanced — equivalently, if Γ_f is a semiregular relative difference set in $A \times B$ relative to $\{0\} \times B$ — then $\Gamma_f - (\{0\} \times B)$ is an $(n^3,\ n^2+n-2,\ n-2)$ signed difference set.
- **Theorem 3.5.** Every binary quadratic form $aX^2 + bXY + cY^2$ of nonzero discriminant over a finite field $\mathbb{F}$ with $|\mathbb{F}| = q$ gives such an f, in every characteristic. Hence there is a $(q^3,\ q^2+q-2,\ q-2)$ signed difference set in the elementary abelian group $\mathbb{F} \times \mathbb{F} \times \mathbb{F}$, for every prime power q.
- **Theorem 3.9.** Five explicit members: $(27, 10, 1)$ in C_3^3, $(64, 18, 2)$ in C_2^6, $(343, 54, 5)$ in C_7^3, $(1331, 130, 9)$ in C_{11}^3 and $(2197, 180, 11)$ in C_{13}^3. The first three are cells recorded `Open` in the database snapshot above; the last two lie beyond its range $v \le 499$.
- **Theorem 6.2.** Over $\mathbb{F}_5$ the family produces both an elliptic and a hyperbolic member at $(125, 28, 3)$, and no affine map of C_5^3 carries one to the other or to its negative. So the He–Wu set is one of at least two equivalence classes at those parameters.

Two remarks on scope. First, the relative-difference-set route into signed difference sets appears to be new only in the sense that we have not found it: none of the three papers we know of on signed difference sets [1, 4, 5] mentions relative difference sets, perfect nonlinear or planar functions, semiregularity, or forbidden subgroups. The closest existing bridge we are aware of is Gordon's later use of relative difference sets to build circulant weighing matrices [2], which lands at $\lambda = 0$ by a different mechanism. Second, the smallest member of Theorem 3.5 is degenerate: at $q = 2$ the parameters are $(8, 4, 0)$, and a signed difference set with $\lambda = 0$ is a group-developed weighing matrix, so that case is classical. The content of the family is that the identity survives at $\lambda \neq 0$.

Section 4 records what we verified of [5] itself, Section 5 explains why the quartic choice there was forced, and Section 7 states carefully what is *not* proved here. Section 8 describes the formal verification and says exactly which claims rest on exhaustive computation.

2. Preliminaries

Definition 2.1. Let G be a finite abelian group with $|G| = v$. A *signed set* on G is a function $a\colon G \to \{0, 1, -1\}$; we write $P = \{g : a_g = 1\}$, $N = \{g : a_g = -1\}$, and $k = |P| + |N| = |\{g : a_g \neq 0\}|$ for its support size. With C_a as in (2), a is a (v, k, λ) *signed difference set* if

$$C_a(t) \;=\; \begin{cases} k, & t = 0, \\ \lambda, & t \neq 0. \end{cases}$$

That $C_a(0) = k$ is not an extra hypothesis but a normalisation: for a signed set, $\sum_h a_h a_h = \sum_h a_h^2$ counts the support. Everything in this paper is stated for abelian G.

The one general identity we need is the following, which is [1, Lemma 1.1] and [5, Eq. (2.3)]. He and Wu obtain it by applying the principal character to (1); Gordon obtains it by counting the nonzero differences and completing the square. The proof below works coefficientwise, which is what makes it convenient to verify.

Lemma 2.2 (Principal-character equation)**.** *Let a be a (v, k, λ) signed difference set on G. Then*

$$\bigl(|P| - |N|\bigr)^2 \;=\; k + \lambda\,(v - 1).$$

Proof. Summing (2) over $t \in G$ and exchanging the two sums, $\sum_t C_a(t) = \sum_h a_h \sum_t a_{t+h} = \bigl(\sum_g a_g\bigr)^2$, because $t \mapsto t + h$ is a bijection of G for each h. On the other hand the defining property evaluates the left side as $k + (v-1)\lambda$. Finally $\sum_g a_g = |P| - |N|$ for a signed set. ☐

Gordon uses Lemma 2.2 in the equivalent form $s = \sqrt{\lambda(v-1) + k} \in \mathbb{Z}$ with $|P| = (k+s)/2$ and $|N| = (k-s)/2$, under the normalising convention $|P| \geq |N|$; we do not adopt that convention, so the split is determined only up to interchange. Two consequences at the parameters of [5] are worth isolating, both immediate.

Proposition 2.3. *Every $(125, 28, 3)$ signed difference set in an abelian group satisfies $\{|P|, |N|\} = \{24, 4\}$.*

Proof. Lemma 2.2 gives $(|P| - |N|)^2 = 28 + 3 \cdot 124 = 400$, so $|P| - |N| = \pm 20$, and $|P| + |N| = 28$. ☐

He and Wu record $|P| = 24$, $|N| = 4$ as a property of their construction; by Proposition 2.3 no other split is available at these parameters.

Proposition 2.4. *No $(125, 28, 3)$ signed difference set has all coefficients nonnegative. Equivalently, the cell cannot be filled by an ordinary difference set, and every construction for it is genuinely signed.*

Proof. If $N = \varnothing$ then $|P| = k = 28$ and Lemma 2.2 reads $28^2 = 28 + 3 \cdot 124 = 400$, which is false. (This is the classical parameter equation $k(k-1) = \lambda(v-1)$ failing: $28 \cdot 27 = 756 \neq 372$.) ☐

The same one-line computation prices any exhaustive search at these cells; see Remark 7.1.

3. Signed difference sets from perfect nonlinear maps

3.1. **The construction.** Throughout this section A and B are finite abelian groups and $f\colon A \to B$ is any map. Write

$$\Gamma_f = \{(x, f(x)) : x \in A\} \subseteq A \times B, \qquad L = \{0\} \times B \subseteq A \times B,$$

and let $a^f = \mathbf{1}_{\Gamma_f} - \mathbf{1}_L$ be the corresponding coefficient function on $A \times B$. Since $\Gamma_f \cap L = \{(0, f(0))\}$, the function a^f takes values in $\{0, \pm 1\}$, with $P = \Gamma_f \setminus L$ and $N = L \setminus \Gamma_f$, so its support size is

$$k = \bigl(|A| - 1\bigr) + \bigl(|B| - 1\bigr) = |A| + |B| - 2, \tag{3}$$

whatever f is. We call L the *forbidden subgroup*, following the relative difference set literature.

Definition 3.1. f is *perfect nonlinear with balance* n if for every $t \in A$ with $t \neq 0$ and every $s \in B$,

$$\bigl|\{x \in A : f(x+t) - f(x) = s\}\bigr| = n.$$

Equivalently: every nonzero derivative of f is balanced. When $|A| = n^2$ and $|B| = n$ this says that Γ_f is a splitting semiregular (n^2, n, n^2, n) relative difference set in $A \times B$ relative to L. We use the standard conventions of [6], in the form recalled in [2, §1]: an (m, n, k, λ) relative difference set in a group G of order mn, relative to a subgroup N of order n, is a k-subset whose differences of distinct elements cover every element of $G \setminus N$ exactly λ times and no nonzero element of N; it is *splitting* when G is the direct product of N and G/N, and *semiregular* when $k = n\lambda$. Here $m = n^2$, $k = |\Gamma_f| = n^2$ and $\lambda = n$. The more familiar case $|A| = |B|$, where the balance is 1, is that of planar functions. This dictionary is a gloss; no proof below passes through it.

The whole computation is the following exact formula, which assumes nothing about f.

Lemma 3.2. *For every $f\colon A \to B$, every $t \in A$ and every $s \in B$,*

$$C_{a^f}(t,s) \;=\; \bigl|\{x \in A : f(x+t) - f(x) = s\}\bigr| \;-\; 2 \;+\; \begin{cases} |B|, & t = 0,\\ 0, & t \neq 0.\end{cases}$$

Proof. Expand $C_{a^f} = C_{\Gamma\Gamma} - C_{\Gamma L} - C_{L\Gamma} + C_{LL}$ by bilinearity of the correlation $(u, w) \mapsto \sum_h u\bigl((t,s)+h\bigr)w(h)$. The first term counts the points $(x, f(x)) \in \Gamma_f$ with $(x, f(x)) + (t, s) \in \Gamma_f$, i.e. the x with $f(x+t) - f(x) = s$, which is the displayed derivative count. The second counts the $(0, y) \in L$ with $(t, s+y) \in \Gamma_f$, i.e. the y with $s + y = f(t)$: exactly one. The third counts the $(x, f(x)) \in \Gamma_f$ with $(x+t,\, f(x)+s) \in L$, i.e. the x with $x = -t$: again exactly one. The fourth counts the $(0, y) \in L$ with $(t, s+y) \in L$, which needs $t = 0$ and then admits every $y \in B$, so it is $|B|$ at $t = 0$ and 0 otherwise. □

Theorem 3.3. *Let A, B be finite abelian groups with $|A| = n^2$ and $|B| = n$, and let $f\colon A \to B$ be perfect nonlinear with balance n. Then*

$$a^f = \mathbf{1}_{\Gamma_f} - \mathbf{1}_{\{0\}\times B}$$

is an $\bigl(n^3,\ n^2+n-2,\ n-2\bigr)$ signed difference set in $A \times B$.

Proof. The ambient group has order $|A|\,|B| = n^3$ and, by (3), $k = n^2+n-2$. Apply Lemma 3.2. At $(t, s) = (0, 0)$ the derivative count is $|A| = n^2$ and the correction is n, giving $C_{a^f}(0,0) = n^2+n-2 = k$. At $t = 0$ and $s \neq 0$ the derivative count is 0 and the correction is n, giving $n-2$. At $t \neq 0$ perfect nonlinearity makes the derivative count n and there is no correction, giving $n-2$ again. So C_{a^f} takes the value k at the identity and $\lambda = n-2$ at every other point. □

The three cases of the proof are exactly the three ways the value $n-2$ can arise, and they collapse only because $|B| = n$: this is where the hypothesis $|A| = |B|^2$ enters.

3.2. **Quadratic forms, and the family.** Perfect nonlinear maps with $|A| = |B|^2$ are supplied in every characteristic by binary quadratic forms.

Lemma 3.4. *Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = q$ and let $f(X,Y) = aX^2 + bXY + cY^2$ with $b^2 - 4ac \neq 0$. Then $f\colon \mathbb{F}^2 \to \mathbb{F}$ is perfect nonlinear with balance q.*

Proof. For $t = (t_1, t_2)$ the derivative is affine in $x = (x_1, x_2)$:

$$f(x+t) - f(x) = (2at_1 + bt_2)\,x_1 + (bt_1 + 2ct_2)\,x_2 + f(t).$$

Its linear part vanishes identically only if $2at_1 + bt_2 = 0$ and $bt_1 + 2ct_2 = 0$; eliminating,

$$2c(2at_1 + bt_2) - b(bt_1 + 2ct_2) = (4ac - b^2)\,t_1, \qquad 2a(bt_1 + 2ct_2) - b(2at_1 + bt_2) = (4ac - b^2)\,t_2,$$

so $b^2 - 4ac \neq 0$ forces $t = 0$. For $t \neq 0$ the derivative is therefore a nonzero affine form on $\mathbb{F}^2$, and a nonzero linear form on $\mathbb{F}^2$ takes each value exactly q times. The elimination is valid in every characteristic; in characteristic 2 the condition $b^2-4ac \neq 0$ degenerates to $b \neq 0$, which is the correct nondegeneracy condition for the polarisation there. □

Theorem 3.5. *Let $\mathbb{F}$ be a finite field with $|\mathbb{F}| = q = p^m$ and let $f(X,Y) = aX^2 + bXY + cY^2$ with $b^2 - 4ac \neq 0$. Then*

$$\Gamma_f - \big(\{0\} \times \mathbb{F}\big)$$

is a $\big(q^3,\ q^2+q-2,\ q-2\big)$ signed difference set in the elementary abelian group $\mathbb{F} \times \mathbb{F} \times \mathbb{F} \cong C_p^{3m}$.

Proof. Lemma 3.4 and Theorem 3.3 with $A = \mathbb{F}^2$, $B = \mathbb{F}$, $n = q$. □

Remark 3.6. The discriminant hypothesis is the only hypothesis, and it does not distinguish elliptic from hyperbolic forms; both give signed difference sets with the same parameters. When r is a non-square, $X^2 - rY^2$ is the norm form of $\mathbb{F}_{q^2}/\mathbb{F}_q$ and Γ_f is the graph of the norm map, which is the shape of the He–Wu example. Section 6 shows the two shapes are genuinely different as signed difference sets.

Remark 3.7. At $q = 2$ the parameters read $(8,4,0)$ in C_2^3. A signed difference set with $\lambda = 0$ is a group-developed weighing matrix [1], so this member is classical. The interest of Theorem 3.5 is that the same identity survives at $\lambda \neq 0$.

3.3. **Cells.** The member at $q = 5$ is the one the source produced.

Corollary 3.8. *Over $\mathbb{F}_5$ the form $X^2 - 2Y^2$ — which, in the coordinates $\mathbb{F}_{25} = \mathbb{F}_5[\alpha]$ with $\alpha^2 = 2$, is the norm form of $\mathbb{F}_{25}/\mathbb{F}_5$ — gives a $(125, 28, 3)$ signed difference set in C_5^3.*

Proof. The discriminant is $0^2 - 4 \cdot 1 \cdot (-2) = 8 = 3 \neq 0$ in $\mathbb{F}_5$; apply Theorem 3.5 at $q = 5$. □

Existence at this cell is [5, Theorem 5.6], and by Proposition 4.2 the signed set of Corollary 3.8 is literally theirs; the derivation above is a second, character-free one. The remaining members of the family fall on other cells; see Remark 3.10.

Theorem 3.9. *The following signed difference sets exist, each as a member of the family of Theorem 3.5:*

$$\begin{array}{ll}
(27,10,1) \text{ in } C_3^3, & f = X^2 - 2Y^2 \text{ over } \mathbb{F}_3,\\
(64,18,2) \text{ in } C_2^6, & f = \text{the norm form of } \mathbb{F}_{16}/\mathbb{F}_4,\\
(343,54,5) \text{ in } C_7^3, & f = X^2 - 3Y^2 \text{ over } \mathbb{F}_7,\\
(1331,130,9) \text{ in } C_{11}^3, & f = X^2 - 2Y^2 \text{ over } \mathbb{F}_{11},\\
(2197,180,11) \text{ in } C_{13}^3, & f = X^2 - 2Y^2 \text{ over } \mathbb{F}_{13}.
\end{array}$$

Proof. In each of the four prime cases the discriminant of f is $-4c \neq 0$ in $\mathbb{F}_q$, so Theorem 3.5 applies; the parameters are $(q^3, q^2+q-2, q-2)$ at $q = 3, 7, 11, 13$. In each case the constant $r \in \{2,3\}$ chosen is a non-square modulo q, so the form is in fact anisotropic, though Theorem 3.5 does not require this. For $q = 4$ we use $\mathbb{F}_4 = \mathbb{F}_2[\theta]$ with $\theta^2 = \theta + 1$ and the norm form $\mathrm{N}(u + w\beta) = u^2 + uw + \theta w^2$ of $\mathbb{F}_{16} = \mathbb{F}_4[\beta]$, $\beta^2 = \beta + \theta$; its perfect nonlinearity with balance 4 is checked directly from Definition 3.1 — 60 pairs (t,s) with $t \neq 0$, each a count over 16 field elements — and Theorem 3.3 then applies with $n = 4$. □

Remark 3.10. In the database snapshot of Section 1 the three keys

`SDS(27,10,1,[3,3,3])`, `SDS(64,18,2,[2,2,2,2,2,2])`, `SDS(343,54,5,[7,7,7])`

all carry `"status": "Open"`; so do all eleven abelian groups of order 64 at $(64,18,2)$ and all three of order 343 at $(343,54,5)$. The cyclic entry `SDS(27,10,1,[27])` is already `"No"`, which is consistent with the construction being elementary abelian only. We state this as a fact about the snapshot; a database snapshot is a record of what was recorded, not a literature search, and we make no stronger priority claim than that we have not found these parameters elsewhere. The cells at $q = 11, 13$ lie past the range $v \leq 499$ covered by the file.

Remark 3.11. The $q = 3$ member deserves a comparison. He, Chen and Ge [4] construct signed difference sets with parameters $(3^{2m+1}, 3^{2m}+1, 1)$ in C_3^{2m+1}, which at $m = 1$ would read $(27, 10, 1)$ in C_3^3 — the same cell, in the same group. Their theorem, however, opens "Let m be an even integer", because the Paley partial difference set it is built on carries parameters $\big(3^m, (3^m-1)/2, (3^m-5)/4, (3^m-1)/4\big)$ and so needs $3^m \equiv 1 \pmod 4$; their smallest instance is $(243, 82, 1)$. The $q = 3$ member of Theorem 3.5 is the first case their parity condition excludes.

3.4. **Controls.** The following finite checks confirm that the hypothesis of Theorem 3.5 is load-bearing and that the resulting parameters are not accidental. Write a^{ell} for the signed set of Theorem 3.5 over $\mathbb{F}_5$ with $f = X^2 - 2Y^2$.

Proposition 3.12. (1) *(Sharpness.) For the degenerate form $f = X^2$ over $\mathbb{F}_5$, which has $b^2 - 4ac = 0$, the signed set $\Gamma_f - L$ is not a signed difference set for* any *parameter triple: its autocorrelation is* 23 *at one nonzero shift and* 3 *at another.*

(2) *(Too large, too small.) Adjoining 0_G to the support of a^{ell}, or deleting one point of its positive support, destroys the property for every parameter triple.*

(3) *(Parameters pinned.) If a^{ell} is a (v, k, λ) signed difference set then $v = 125$, $k = 28$ and $\lambda = 3$.*

Item (1) is the sharp one. By (3) the degenerate form gives a signed set of the *same* support size $k = 28$, so nothing about the count of points detects the failure; what fails is the two-level property, and it fails badly. All three items are exhaustive evaluations of (2) on a group of order 125.

4. The He–Wu construction

This section records what we verified of [5] itself. Nothing in it is new mathematics; it is stated because the identification of Proposition 4.2 is what produced Section 3, and because the identification is only meaningful against the source's own normalisations.

Their setup: the polynomial $x^2 + 3$ is irreducible over $\mathbb{F}_5$, α is a root, so $\alpha^2 = -3 = 2$ and $\mathbb{F}_{25} = \mathbb{F}_5[\alpha]$; $\gamma = 1 + 2\alpha$ has multiplicative order 24; $\rho\colon \mathbb{F}_{25}^* \to \{1, i, -1, -i\}$ is the quartic character with $\rho(\gamma) = i$; and $\sigma\colon \mathbb{F}_5^* \to \{1, i, -1, -i\}$ is the quartic character with $\sigma(2) = -i$. All of this we check rather than assume: the irreducibility, the value of α^2, the order of γ, and the multiplicativity of ρ and of σ, each on all pairs of nonzero arguments of its own field.

Lemma 4.1 ([5, Lemma 5.5])**.** *With these normalisations the multiplicity tables of $\rho(x)\rho(1-x)$ over $\mathbb{F}_{25}$ and of $\sigma(x)\sigma(1-x)$ over $\mathbb{F}_5$, listed at $z = 0, 1, -1, i, -i$, are $(2, 7, 4, 8, 4)$ and $(2, 0, 1, 2, 0)$. Consequently $J(\rho, \rho) = 3 + 4i$, $J(\sigma, \sigma) = -1 + 2i$ and $J(\rho, \rho)\overline{J(\sigma, \sigma)} = 5 - 10i$.*

Every entry here is printed in [5, §5.2]; we reproduced them by enumeration over the 25 and 5 field elements respectively, from the source's own normalisations, and then formed the two Jacobi sums and their product. The Gaussian integers are handled as pairs, so no transcendental input enters.

Proposition 4.2. *Let $P = \{(x, y) \in \mathbb{F}_{25}^* \times \mathbb{F}_5^* : \rho(x) = \sigma(y)\}$ and $N = \{0\} \times \mathbb{F}_5^*$ be as in* [5, §5.2], *and let $\mathrm{N}\colon \mathbb{F}_{25} \to \mathbb{F}_5$ be the norm. Then, as signed sets on $(\mathbb{F}_{25}, +) \times (\mathbb{F}_5, +)$,*

$$\mathbf{1}_P - \mathbf{1}_N \;=\; \mathbf{1}_{\Gamma_{\mathrm{N}}} - \mathbf{1}_{\{0\}\times\mathbb{F}_5}.$$

In the coordinates $\mathbb{F}_{25} = \mathbb{F}_5[\alpha]$ the norm is the binary quadratic form $\mathrm{N}(u + w\alpha) = u^2 - 2w^2$, so the He–Wu signed set is the member of Theorem 3.5 at $q = 5$.

The reason is short. Write $x = \gamma^u$ and $y = 2^t$. Then $\rho(x) = \sigma(y)$ reads $i^u = (-i)^t$, i.e. $u \equiv -t \pmod 4$. Since $\mathrm{N}(\gamma^u) = \gamma^{6u}$ and γ^6 generates $\mathbb{F}_5^*$, the condition is $\mathrm{N}(x) = y^c$ for some c coprime to 4; the normalisations $\rho(\gamma) = i$ and $\sigma(2) = -i$ make $c = 1$. We record it as a proposition rather than a lemma because it is not stated in [5], and we verify it as what it is: an equality of two functions on a 125-element group, checked pointwise.

Theorem 4.3 ([5, Theorem 5.6]). *The signed set $D = P - N$ above is a $(125, 28, 3)$ signed difference set in $G \cong C_5^3$, with $|P| = 24$ and $|N| = 4$.*

Priority for this cell is entirely theirs. We obtain it twice: once by direct evaluation of (2) at all 125 shifts, independently of the source's own computation, and once as the case $q = 5$ of Theorem 3.5 through Proposition 4.2 — the route the formal proof takes, so that the $(125, 28, 3)$ statement inherits the general argument rather than a search. The split $|P| = 24$, $|N| = 4$ is their closing remark, and Proposition 2.3 shows it was forced.

Theorem 4.4 ([5, Example 5.4]). *The two Desarguesian-spread instances of* [5, Theorem 5.3] *exist with the parameters printed in* [5, Example 5.4]*:* $\mathrm{SDS}(64, 22, 6)$ *in* C_2^6 *and* $\mathrm{SDS}(256, 106, 42)$ *in* C_2^8*; their support splits are* $(|P|, |N|) = (21, 1)$ *and* $(105, 1)$ *respectively.*

Here $V = \mathbb{F}_{2^m}^2$ carries its Desarguesian m-spread $\mathcal{S}$, one takes $\mathcal{A} \subseteq \mathcal{S}$ with $|\mathcal{A}| = \ell = 2^{m-1} - 1$, sets $P = \bigcup_{U \in \mathcal{A}} (U \setminus \{0\})$ and $D = P - 0_G$; we instantiate $m = 3$ and $m = 4$ with $\mathcal{A}$ the first ℓ members U_a, over $\mathbb{F}_8 = \mathbb{F}_2[\theta]/(\theta^3 + \theta + 1)$ and $\mathbb{F}_{16} = \mathbb{F}_2[\theta]/(\theta^4 + \theta + 1)$. We verify the two witnesses only: the general theorem [5, Theorem 5.3] behind them is taken as published. Note that $\mathrm{SDS}(64, 22, 6)$ lives in the same group C_2^6 as the $q = 4$ member of Theorem 3.9, at a different cell.

5. Why the quartic choice was forced

Proposition 4.2 raises a question about [5]: was the quartic order a choice among many? It was not. Run their ansatz with characters ρ of $\mathbb{F}_{q^2}^*$ and σ of $\mathbb{F}_q^*$ of a common order $e \mid q - 1$, keeping $P = \{(x, y) : \rho(x) = \sigma(y)\}$ and $N = \{0\} \times \mathbb{F}_q^*$, and write $q = ed + 1$. Their Case 1 and Case 2 computations, carried out for general e, give

$$\Theta_{0,b}(D) = -d(q + 1) + 1, \qquad \Theta_{a,0}(D) = -d(e + 1),$$

for the additive characters $\Theta_{a,b}$ of G with $(a, b) \neq (0, 0)$; the fibres of ρ have size $(q^2 - 1)/e = d(q+1)$ and those of σ have size d, which is all that enters. A signed difference set forces $|\Theta_{a,b}(D)|$ to be constant over nonprincipal characters, hence $d(q + 1) = d(e + 1) + 1$. That equation is rigid.

Proposition 5.1. *Let $e, d \geq 1$ be integers with $d\big((ed + 1) + 1\big) = d(e + 1) + 1$. Then $d = 1$.*

Proof. The equation rearranges to $(d - 1)(ed + 1) = 0$, and $ed + 1 > 0$. □

So $d = 1$, i.e. $e = q - 1$: the characters must have the *full* order $q - 1$. Then $\rho(x) = \sigma(y)$ says $\mathrm{N}_{q^2/q}(x) = y^c$ for a c coprime to $q - 1$, and one is on the graph of the norm. At $q = 5$ the full order is 4, which is why the quartic characters of [5] are the only ones their ansatz admits. We emphasise what is proved and what is read: Proposition 5.1 is the arithmetic step; the character computation that produces the two displayed values for general e is our extension of the source's Case 1 and Case 2, which are stated there only at $q = 5$, $e = 4$. As a numerical cross-check, over all prime powers $q \leq 200$ and all $e \mid q - 1$ with $e \neq q - 1$, integrality of λ alone already fails, with no exceptions.

6. Two inequivalent signed difference sets at $(125, 28, 3)$

By Remark 3.6, Theorem 3.5 over $\mathbb{F}_5$ produces a signed difference set $\Gamma_f - L$ for each $f = X^2 - rY^2$ with $r \neq 0$; the values $r = 2, 3$ are non-squares and give anisotropic forms — at $r = 2$ this is the norm form of $\mathbb{F}_{25}/\mathbb{F}_5$, hence the He–Wu set itself by Proposition 4.2 — while $r = 1, 4$ are squares and give hyperbolic forms. Write a^{ell} and a^{hyp} for the members at $r = 2$ and $r = 1$.

Call two signed sets a_1, a_2 on G *equivalent* if $a_2(Ag + t) = \varepsilon\, a_1(g)$ for all g, for some $A \in \mathrm{Aut}(G)$, some $t \in G$ and a single sign $\varepsilon \in \{+1, -1\}$; this is the usual equivalence for difference sets, extended by the negation $D \mapsto -D$, which preserves (1). The first ingredient removes the invertibility hypothesis one would otherwise carry.

Lemma 6.1. *Let a_1 be a (v,k,λ) signed difference set on a finite abelian group G with $k \neq \lambda$, let $A\colon G \to G$ be an additive endomorphism and $t \in G$, and suppose $a_2(Ag+t) = a_1(g)$ for all g. Then A is injective.*

Proof. If $Aw = 0$ with $w \neq 0$ then $a_1(w+g) = a_2(A(w+g)+t) = a_2(Ag+t) = a_1(g)$ for all g, so a_1 is invariant under translation by w; hence $C_{a_1}(w) = C_{a_1}(0)$, i.e. $\lambda = k$. □

The separating invariant is elementary and affine-covariant. For a signed set a on G and $c \in G$ put

$$\mathrm{sp}(a,c) \;=\; \bigl|\{g \in G :\; a(g) = 1 \text{ and } a(2g-c) = 1\}\bigr|.$$

If $a_2(Ag+t) = a_1(g)$ with A injective, then $g \mapsto Ag+t$ carries the pair $(g, 2g)$ to $(h, 2h-t)$ with $h = Ag+t$, so it injects the set counted by $\mathrm{sp}(a_1, 0)$ into the set counted by $\mathrm{sp}(a_2, t)$, giving

$$\mathrm{sp}(a_1,0) \;\le\; \mathrm{sp}(a_2,t). \tag{4}$$

For a signed set of the form $\Gamma_f - L$ over a field of odd characteristic the invariant at $c = 0$ has a geometric reading. Here $a(g) = 1$ and $a(2g) = 1$ say that $g = (x, f(x))$ with $x \neq 0$ and $f(2x) = 2f(x)$; since f is a quadratic form, $f(2x) = 4f(x)$, so the condition is $2f(x) = 0$, that is $f(x) = 0$. Thus $\mathrm{sp}(a,0)$ counts the nonzero points of the conic $f = 0$, which is 0 for an anisotropic form and $2(q-1) = 8$ for a hyperbolic one over $\mathbb{F}_5$.

Theorem 6.2. *There is no additive endomorphism A of C_5^3 and no $t \in C_5^3$ with $a^{\mathrm{ell}}(Ag+t) = a^{\mathrm{hyp}}(g)$ for all g, and none with $a^{\mathrm{ell}}(Ag+t) = -a^{\mathrm{hyp}}(g)$ for all g. Consequently a^{ell} and a^{hyp} are two inequivalent $(125,28,3)$ signed difference sets in C_5^3, and the construction of* [5] *reaches one of at least two equivalence classes at these parameters.*

Proof sketch. Both signed sets are $(125,28,3)$ signed difference sets by Theorem 3.5, and $k = 28 \neq 3 = \lambda$, so Lemma 6.1 makes any matching A injective. For the unsigned case, (4) would give $\mathrm{sp}(a^{\mathrm{hyp}},0) \le \mathrm{sp}(a^{\mathrm{ell}},t)$, whereas exhaustive evaluation gives $\mathrm{sp}(a^{\mathrm{hyp}},0) = 8$ and $\mathrm{sp}(a^{\mathrm{ell}},c) \le 6$ for *every* one of the 125 values of c. For the signed case, an affine matching of a^{hyp} with $-a^{\mathrm{ell}}$ injects the positive support of a^{hyp} into the negative support of a^{ell}, which is impossible: a direct count gives 24 and 4 for the two sizes, and by Proposition 2.3 no $(125,28,3)$ signed difference set can do better. Since an automorphism of C_5^3 is in particular an additive endomorphism, this excludes every equivalence in the sense above. □

Remark 6.3. Outside the formal development, and recorded here only for orientation, a direct enumeration of $\mathrm{GL}(3,5)$ gives stabiliser orders 48 for a^{ell} and 32 for a^{hyp} and no linear map carrying one to the other; the negative support of each sums to 0, so the translation part is forced to vanish independently. These numbers are not part of the verified development and are not used above.

7. What is not proved here

It is worth being explicit about the boundaries of the above.

1. The nonexistence half of [5] — the four obstructions and the elimination of 45,361 of the 67,823 open cells — is taken as published and is not re-derived. We reproduce only the input count 67,823 and its range $9 \le v \le 499$, from the database file itself.
2. The general Desarguesian-spread theorem [5, Theorem 5.3] is not re-derived either; Theorem 4.4 covers its two printed instances.
3. Theorem 6.2 is a lower bound of 2 on the number of equivalence classes at $(125,28,3)$ in C_5^3. The exact number is not determined here.

Remark 7.1. Nothing above is an existence search, and there is a reason. Lemma 2.2 pins the split before any search begins: at $(27,10,1)$ one has $s^2 = 10 + 26 = 36$, so $(|P|,|N|) = (8,2)$. Even with that reduction a naive exhaustive search over the smallest open cell runs over $\binom{27}{8}\binom{19}{2} =$ 2,220,075 $\cdot$ 171 $=$ 379,632,825 signed sets, each needing a 27×27 autocorrelation check: about 2.8×10^{11} elementary operations before any multiplier or orbit pruning. Every other open cell has larger v, up to 499. Deciding these cells is a per-cell campaign, not a single computation, which is why constructions of the kind given here are the practical instrument.

8. Verification

Every theorem, proposition, lemma and corollary above has been formally verified in Lean 4 against *Mathlib*; the development contains no `sorry`, and the setup of Section 4 is checked rather than assumed. The repository is private at the time of writing; a repository reference is to be added at submission. The general results carry no computational content at all: Lemma 2.2, Propositions 2.3, 2.4, 5.1, Lemma 3.2, Theorem 3.3, Lemma 3.4, Theorem 3.5, Corollary 3.8, the four prime cells of Theorem 3.9, and Lemma 6.1 all reduce to `propext`, `Classical.choice` and `Quot.sound`, so the infinite family and its prime members rest on no evaluation. The $q = 4$ cell of Theorem 3.9 is likewise free of compiled evaluation: its perfect nonlinearity is decided by the kernel over the 60 pairs (t, s) with $t \neq 0$. What is delegated to compiled evaluation, through Lean's `native_decide`, is exactly the finite searches over concrete groups: the three items of Proposition 3.12 (autocorrelations of explicit functions on a group of order 125 at named shifts, and the support count); the multiplicity tables and Jacobi sums of Lemma 4.1 and the multiplicativity of ρ (over all $24 \cdot 24$ pairs of nonzero arguments of $\mathbb{F}_{25}$); the 125-point function equality of Proposition 4.2, from which Theorem 4.3 follows with no further evaluation; the two witnesses of Theorem 4.4 (autocorrelation at all shifts of groups of order 64 and 256, and their support splits); and, for Theorem 6.2, the values $\mathrm{sp}(a^{\mathrm{hyp}}, 0) = 8$, $\mathrm{sp}(a^{\mathrm{ell}}, c) \leq 6$ for all 125 values of c, and the two support counts 24 and 4. Every numerical value quoted was first produced by an independent implementation in Python, written from the definitions rather than from the sources' code, and the formal statement was then written against it; the database counts of Section 1 were computed from the downloaded file, whose size and md5 are recorded there.

References

[1] D. M. Gordon, *Signed difference sets*, Des. Codes Cryptogr. **91** (2023), no. 5, 2107–2115; MR4578178. Preprint: arXiv:2212.10630v1, whose numbering is the one used in the citations above.

[2] D. M. Gordon, *Cyclic relative difference sets and circulant weighing matrices*, J. Algebraic Combin. **63** (2026), no. 2, Paper No. 24, 14 pp. Preprint: arXiv:2501.14924v2, whose sectioning is the one used in the citation above.

[3] D. M. Gordon, *Signed difference set database*, `https://github.com/dmgordo/signed-difference-sets`; file `sds.json`, downloaded 2026-08-29, 5,193,480 bytes, md5 `3c0190930707d47740f0852d43580187`, byte-identical to the blob of commit `e3bf810` of 2026-04-24, the last commit to that file, and to the default branch as of the download.

[4] Z. He, T. Chen and G. Ge, *New constructions of signed difference sets*, Des. Codes Cryptogr. **92** (2024), no. 8, 2323–2340. Preprint: arXiv:2306.05631v1, the version quoted above.

[5] Z. He and J. Wu, *Nonexistence Results and Constructions for Signed Difference Sets*, arXiv:2608.22936 (submitted 2026-08-24; version v1 used throughout).

[6] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics, vol. 1601, Springer-Verlag, Berlin, 1995.