An explicit formal dual for every configuration $\Gamma(C, C^\perp)$ of Bierbrauer–Edel's definition, and formal isoduality of the packings in dimensions 18, 28 and 30

Antoine Olivier. 18 November 2026. This note follows an earlier note dated 9 November 2026, *Formal duals of the Bierbrauer–Edel and Vardy record packings in dimensions 18, 28 and 30* (personal communication [EN]; Cohn's table [ST] cites it in this form). The earlier note is not part of this deposit, and "the earlier note" below refers to it. Only its certificates of formal duality and its files of T rest on it alone: they are stated in [EN] and not proved here. The results of this note that mention it have a route inside this note (Theorem A, Proposition I, § 8.3, [CCV, § 5.1]), given first.

Summary

Results. Let C be a binary linear $[2k, k]$ code with $C \neq C^\perp$, and $\Gamma = \Gamma(C, C^\perp)$ the configuration of formula (1), the definition on p. 97 of Bierbrauer–Edel [BE]. **Theorem A** gives an explicit formal dual of Γ in the sense of [CKRS], in terms of C, $C^\perp$ and two auxiliary words. No hypothesis on minimum distance or parity is needed. The finite pair behind it has $|S| = |T| = 2^{r+1}$ in a group of order 2^{2r+2}, where $r = k - \dim R$ and $R = C \cap C^\perp$ is the hull of C.

Proposition I shows that this dual is an isometric copy of $\Gamma/8$. So Γ rescaled to unit density is formally isodual in the sense of [CKS]. A remark (§ 2.4) shows that it is formally self-dual exactly when $4 \mid n$ and the hull is doubly even. Hence the packings 18.1, 28.1 and 30.1 are formally isodual and not formally self-dual.

A further remark (§ 6) concerns codes with $\mathbf{1} \in R$ and $r = 4, 6, 8$. An $\mathbb{F}_2$-linear identification turns S into a graph $\{(x, F(x)) : x \in \mathbb{F}_{2^{r+1}}\}$ with F a permutation, formally self-dual under the trace pairing of Kölsch–Schüler [KS]. The same construction was also run for $r = 10, 12$: computed, not reviewed.

What it changes for Cohn's table of stealth radius records [ST]. The values in dimensions 18, 28 and 30 do not change. Only their description does. In this note, the dual given by the formula of Theorem A is an isometric copy of $\Gamma/8$ (Proposition I); its stealth radius at unit density is the packing's minimal distance $d_{\min}/(2\sqrt{2})$, that is $\sqrt{3}$, 2, 2, and the equality uses [CCV, § 5.1] and Theorem A, item 3. The duals of the earlier note [EN] are, at unit density, isometric copies of the packings 18.1, 28.1 and 30.1 themselves (checked by computer, § 8.3), with the same stealth radius; this radius also follows from the certificates of formal duality in [EN] together with [CCV, § 5.1]. Those certificates are stated in [EN] and not proved here.

Status. Theorem A, Proposition I and the remark on formal self-duality are proved on paper and were reviewed by model instances (three hostile reviews each for Proposition I and for the remark; two for items 1, 2 and 4 of Theorem A; for item 3, two, a third that took this step from them, and the GPT-6 Astra reviews; one for item 5; for the remark, the first review concerned an earlier version of the proof and covered the *if* direction only through Theorem A; details and reserves in § 7). §§ 3 to 5 give the proofs, and § 8.4 the proof of the distance lemma, all rewritten for this note; one model reviewer compared this text with the reviewed proofs, and Gemini 4 Carbon (Google) read it once as a hostile referee (§ 9). No person has checked them yet; Theorem A was also reviewed by GPT-6 Astra (§ 9). Astra and Gemini are the reviewers from other families of models. In the literature we searched (§ 10.2) we found neither statement; that search is not a proof of absence.

How to check quickly.

hexagon:2611.00626v1

- *Theorem A.* After the conventions of § 3.0, read §§ 3.3 to 3.5 (Gauss sums of the weight form, their Poisson relation, and the odd characters), then § 3.10 (differences of the two halves of T). The other lemmas are counts and congruences.
- *Proposition I.* Two congruences mod 4 (§ 4, steps 2 and 3) give $g(8Q) \subseteq \Gamma$; a count of residues (step 4) gives equality.
- *Self-duality.* § 5 tests the criterion of [CKRS, Cor. 2.7] at every residue mod 8, with closed forms. The witnesses for the *only if* direction are $z = 2\tilde{h}'$ with $h' \in R$ of weight $\equiv 2 \pmod 4$, and $z = \mathbf{1}$ (§ 5.4).
- *By hand.* The example for $n = 2$ (§ 2.5) applies formulas (1) to (5) literally.
- *Computer checks.* Their exact scope is in § 7 (summary table, then one entry per claim) and § 8.1; they check instances and do not replace a proof.

Why it matters. Formal duals of periodic non-lattice configurations were known for the family $D_n^+(\alpha)$, formally dual to $D_n^+(1/\alpha)$ when n is odd or a multiple of four and not a lattice for odd n, and for $\mathcal{P}_6$ [CKS]; for the TITO configuration, the family built from Gauss sums, and the configurations that [CKRS, Thm. 2.8] attaches to formally dual pairs in finite abelian groups, such as those of [LPS] and [KS]; and for Vardy's 20-dimensional packing [CCV, § 5]. What this note adds is a closed formula for a formal dual of $\Gamma(C, C^\perp)$ for every $[2k, k]$ code $C \neq C^\perp$, and the fact that this configuration is formally isodual.

Contents

Summary **1**

1. Notation and definitions **3**

2. Statements **4**

2.1 Theorem A: an explicit formal dual of $\Gamma(C, C^\perp)$ 4

2.2 Proposition I: $\Gamma(C, C^\perp)$ is formally isodual 5

2.3 Stealth radius 5

2.4 Remark on formal self-duality 5

2.5 A worked example: $n = 2$ 6

3. Proof of Theorem A **7**

3.0 Conventions and elementary facts 7

3.1 Lemma (periods and sizes) 8

3.2 Lemma (the two halves; even characters) 8

3.3 Lemma (Gauss sums of the weight form) 8

3.4 Lemma (Poisson relation) 9

3.5 Lemma (odd characters) 9

3.6 Lemma (the dual group) 10

3.7 Lemma (the target function) 10

3.8 Lemma (the set T) 11

3.9 Lemma (ν_T on even characters) 11

3.10 Lemma (ν_T on odd characters) . . . 11
3.11 Proof of items 1 and 2 . . . 12
3.12 Proof of item 3 . . . 12
3.13 Proof of item 4 . . . 12
3.14 Proof of item 5 . . . 13

4. Proof of Proposition I **13**

5. Proof of the remark on formal self-duality **15**
5.1 The criterion . . . 15
5.2 Residues z with $\bar{z} \notin \{0, \mathbf{1}\}$ . . . 15
5.3 Even residues $z = 2y$, $y \in (\mathbb{Z}/4)^n$ . . . 15
5.4 Odd residues $z = \mathbf{1} + 2y$, and conclusion . . . 16

6. Remark: formally self-dual graphs over $\mathbb{F}_{2^m}$ for $m = 5, 7, 9$, and computed instances for $m = 11, 13$ **17**
6.1 Explicit tables for the remark of § 6 . . . 17

7. Status **18**

8. Computations, comparison with known pairs, and the configurations of the earlier note **20**
8.1 What is computed . . . 20
8.2 Position with respect to known finite pairs . . . 21
8.3 What it means for the configurations of the earlier note . . . 21
8.4 Minimal distances . . . 21
8.5 Formal self-duality, as opposed to isoduality . . . 22
8.6 Context: the densest packings and formal duality . . . 22

9. Tool and computational resource disclosure **22**

10. Limits **23**
10.1 Two readings of Bierbrauer–Edel 2000 . . . 23
10.2 Prior art . . . 23
10.3 What this note does not claim . . . 24

References **24**

1. Notation and definitions

Notation. $n = 2k$. For a binary word b, $\tilde{b} \in \{0,1\}^n \subset \mathbb{Z}^n$ is its 0/1 lift; $\mathbf{1}$ is the all-ones vector; e_1 the first unit vector; $\zeta = e^{2\pi i/8}$; for $y \in \mathbb{Z}^n$, $\chi_y(x) = \zeta^{\langle x,y\rangle}$. For a code C: $R = C \cap C^\perp$ (hull), $h = \dim R$, $r = k - h$, and $\lambda(x) = \mathrm{wt}(x)/2 \bmod 2$ for $x \in R$. For X in a finite abelian group, $\nu_X(g) = \#\{(a,b) \in X^2 : a - b = g\}$. Following Bierbrauer–Edel [BE, p. 97] (two readings of [BE];

for $\mathbf{1} \notin R$ the configuration (1) may differ from the packing of the p. 98 reading: §§ 10.1 and 10.3), for binary linear codes C_2, C_2' of the same length,

$$\begin{aligned} &\Gamma(C_2, C_2') = \Gamma_8 + 8\mathbb{Z}^n, \\ &\Gamma_8 = \{-2\tilde{b} + 4\tilde{c} : \ b \in \mathbf{1} + C_2, \ \text{wt}\, c \text{ even}\} \\ &\qquad \cup \ \{\mathbf{1} - 2\tilde{b} + 4\tilde{c} : \ b \in C_2', \ \text{wt}\, c \text{ odd}\} \pmod 8 \end{aligned} \tag{1}$$

Formal duality: [CKRS, Def. 2.1] for periodic configurations in $\mathbb{R}^n$; [CKRS, Def. 2.9 and Thm. 2.8] for subsets $S \subset H$, $T \subset \hat{H}$ of a finite abelian group: $|T|\,|\hat{S}(\chi)|^2 = |S|^2\,\nu_T(\chi)$ for every χ, and the symmetric identity.

2. Statements

2.1 Theorem A: an explicit formal dual of $\Gamma(C, C^\perp)$

Theorem A. Let $C \subset \mathbb{F}_2^n$ be a binary linear $[n, k]$ code, $n = 2k$, with $C \neq C^\perp$, and $\Gamma = \Gamma(C, C^\perp)$. Choose

- $u \in \mathbb{F}_2^n$ with $u \cdot x = \lambda(x)$ for every $x \in R$;
- $w \in C$ with $w \cdot c \equiv \text{wt}(c) \pmod 2$ for every $c \in C$ ($w = 0$ if C is even);
- $\varepsilon \equiv n/2 + 1 \pmod 2$.

Let $L' = 8\mathbb{Z}^n + \sum_j \mathbb{Z}\, 4(e_1 + e_j) + \sum_{x \in R} \mathbb{Z}\, 2\tilde{x}$, $A = \langle \Gamma - \Gamma \rangle$, $H' = A/L'$, $x_0 \in \Gamma$, $S = (\Gamma - x_0)/L' \subset H'$, and

$$T = \{2\tilde{c} + 4(u \cdot c)e_1 : \ c \in C\} \ \cup \ \{\mathbf{1} + 2\widetilde{(u + w)} + 2\tilde{d} + 4(\varepsilon + u \cdot d)e_1 : \ d \in C^\perp\}, \tag{2}$$

each vector y being read as the character χ_y of H'. Then:

1. L' is a lattice of periods of Γ; $|S| = 2^{r+1}$, $|H'| = 2^{2r+2}$, and T is a set of 2^{r+1} distinct characters of H' (the two halves of (2) have disjoint images, and within each half every class of its image has exactly 2^h preimages).
2. $S \subset H'$ and $T \subset \widehat{H'}$ are formally dual (both identities, for every character and every group element).
3. Hence Γ and $Q = A^* + T/8$ are formally dual in $\mathbb{R}^n$ [CKRS, Thm. 2.8 with $\Lambda = L'$, equivalently Cor. 2.7; the lattice of Q is A^*, and $y \in \mathbb{Z}^n$ stands for the character $y/8 + A^*$ of L'^*/A^*], where

$$A^* = \tfrac{1}{4}\{z \in \mathbb{Z}^n : \ z \bmod 2 \in R, \ \textstyle\sum_i z_i \equiv 0 \pmod 4\}. \tag{3}$$

4. ν_T takes the value 2^{r+1} once (at 0), 2^{r-1} on a family of $4(2^r - 1)$ characters, 2 on a disjoint family of 2^{2r} characters, and 0 elsewhere; for $r = 2$ the two values coincide, so $\nu_T = 2$ on 28 characters. $\widehat{H'}$ is elementary abelian if and only if $\mathbf{1} \in R$.
5. The pair (S, T) is primitive in the sense of Kölsch–Schüler [KS]: neither set lies in a coset of a proper subgroup, and neither is a union of cosets of a non-trivial subgroup.

If $\mathbf{1} \in R$, the dot product is alternating on C/R, so r is even.

2.2 Proposition I: $\Gamma(C, C^\perp)$ is formally isodual

Proposition I. Keep the hypotheses and notation of Theorem A, with (u, w) admissible (chosen as in Theorem A). Let $f \in R^\perp = C + C^\perp$ with $\mathrm{wt}(u + f) \equiv n/2 \pmod 2$; write $f = c_0 + e$ with $c_0 \in C$, $e \in C^\perp$ (any decomposition); put $D = u + f$, choose $v \in \mathbb{F}_2^n$ with $\mathrm{wt}\, v \equiv \mathrm{wt}\, c_0 \pmod 2$, and set

$$\tau = 2(\tilde{\mathbf{1}} - \tilde{c}_0) + 4\tilde{v}, \qquad g(x) = \sigma_D\, x + \tau, \tag{4}$$

where σ_D changes the sign of the coordinates in $\operatorname{supp} D$.

1. $g(8Q) = \Gamma$, as subsets of $\mathbb{R}^n$.
2. Such an f exists for every admissible (C, u, w): if $\mathbf{1} \in R$ every f works (for instance $f = 0$ with $c_0 = v = 0$, which gives $g(x) = \sigma_u x + 2 \cdot \mathbf{1}$); if $\mathbf{1} \notin R$, $R^\perp$ contains odd-weight words.
3. Hence $Q = \sigma_D(\Gamma - \tau)/8$ is isometric to $\Gamma/8$, and $P = \Gamma/(2\sqrt{2})$, which has density 1, is formally dual to the isometric copy $\sigma_D\big(P - \tau/(2\sqrt{2})\big)$ of itself: P is formally isodual in the sense of Cohn–Kumar–Schürmann [CKS].

Items 1 and 2 use no external result; item 3 rests on Theorem A, item 3, and on [CKRS, Lemma 2.4] with $\varphi = I/(2\sqrt{2})$.

2.3 Stealth radius

By [CCV, § 5.1], when two configurations of density 1 are formally dual, the stealth radius of one (in the sense of [CCV, § 2], for the stationary process obtained by a random translation, no factor 2π) equals the minimal distance of the other. With Proposition I, the stealth radius at unit density of the dual is the minimal distance of the packing at unit density:

$$\mathrm{stealth}(Q_{\text{unit density}}) = d_{\min}(P) = \frac{d_{\min}(\Gamma)}{2\sqrt{2}}. \tag{5}$$

2.4 Remark on formal self-duality

Remark (formal self-duality). *Status: proved on paper; both directions passed three hostile reviews.* Call R doubly even if every word of R has weight divisible by 4. With $P = \Gamma/(2\sqrt{2})$ as in Proposition I, P is formally self-dual in the sense of [CKS] (formally dual to itself, equivalently to a translate of P or of $-P$) if and only if $4 \mid n$ and R is doubly even. The *only if* direction does not use Theorem A. The *if* direction is the case $D = 0$ of Proposition I; it was reviewed in that form, which uses Theorem A, item 3, by all three reviews (conditionally on Theorem A, item 3, and Proposition I, item 1), and in a direct proof that does not use Theorem A by the second and third; the third review redid both directions without Theorem A, and its argument does not use $C \neq C^\perp$. A related pattern in n mod 4 appears in Cohn, Kumar and Schürmann's result for the two-coset structure D_n^+, which is formally self-dual when n is odd or a multiple of four and formally isodual when $n \equiv 2 \pmod 4$ [CKS, § 6, Proposition 1; lines 621–623 of the source of arXiv:0911.2169v2]. For the codes of 18.1, 28.1 and 30.1 the hulls have weight sets $\{0, 18\}$, $\{0, 14, 28\}$ and $\{0, 10, 20, 30\}$, none doubly even, and $n/2$ is odd for $n = 18, 30$. These three packings are therefore formally isodual and not formally self-dual. This last step uses the codes extracted from the coordinates of the packings of `recordpackings.toml` [RP] by two independent programs (§ 8.3), which give the same hull weights.

2.5 A worked example: $n = 2$

Take $k = 1$ and $C = \{00, 10\}$, so $C^\perp = \{00, 01\}$, $R = \{00\}$, $h = 0$, $r = 1$, and $\mathbf{1} \notin R$. Every $u \in \mathbb{F}_2^2$ is admissible because $R = 0$; we take $u = 11$, so that no term of (2) vanishes. The only $w \in C$ with $w \cdot c \equiv \mathrm{wt}(c)$ is $w = 10$. Here $\varepsilon \equiv n/2 + 1 \equiv 0$. Everything below was computed by an exact script (integers and $\mathbb{Z}[\zeta_8]$) that applies (1) to (5) as written, and every identity was also run for the four values of u.

The configuration. By (1), with 0/1 lifts, Γ_8 has $8 = 2^{n+k}$ points mod 8. The even half ($b \in \{11, 01\}$, $\mathrm{wt}\, c$ even) is $(0,6), (2,2), (4,2), (6,6)$. The odd half ($b \in C^\perp$, $\mathrm{wt}\, c$ odd) is $(1,3), (1,5), (5,1), (5,7)$.

The finite group. L' is generated by $(8,0)$ and $(4,4)$, and $A = \langle \Gamma - \Gamma \rangle = \{x \in \mathbb{Z}^2 : x_1 \equiv x_2 \bmod 2\}$ has basis $a_1 = (2,0)$, $a_2 = (1,1)$. The coordinates $(c_1, c_2) = ((x_1 - x_2)/2,\ x_2)$ identify $H' = A/L'$ with $\mathbb{Z}_4^2$, of order $16 = 2^{2r+2}$ (not elementary abelian, as $\mathbf{1} \notin R$). With $x_0 = (0,6)$ we get $S = \{(0,0), (1,3), (2,1), (3,0)\}$, so $|S| = 4 = 2^{r+1}$.

The set T. A vector y with $y_1 + y_2$ even is the character $\chi(c_1, c_2) = i^{ac_1 + bc_2}$ with $a \equiv y_1$, $b \equiv (y_1 + y_2)/2 \pmod 4$ (our labelling). In (2), $2\widetilde{(u + w)}$ lifts the sum $u + w = 01$, so it equals $(0,2)$, not $2\tilde{u} + 2\tilde{w} = (4,2)$. The other reading breaks both identities (checked); here it gives the same set T as flipping ε. We get

$$T = \{(0,0), (6,0)\} \cup \{(1,3), (5,5)\},$$

that is the characters $(a,b) = (0,0), (2,3), (1,2), (1,1)$, which are distinct.

Both identities. Here $|T|\,|\hat{S}(\chi)|^2 = 4|\hat{S}(\chi)|^2$ and $|S|^2 \nu_T(\chi) = 16\,\nu_T(\chi)$. The 16 characters fall into four classes.

ν_T	**characters** (a,b)	**number**	$\lvert\hat{S}\rvert^2$
4	$(0,0)$	1	16
2	$(1,1), (1,2), (3,2), (3,3)$	4	8
1	$(0,1), (0,3), (2,1), (2,3)$	4	4
0	the other 7	7	0

So $4|\hat{S}|^2 = 16\,\nu_T$ in every class. For $r = 1$ item 4 predicts $2^{r+1} = 4$ once, $2^{r-1} = 1$ on $4(2^r - 1) = 4$ characters and 2 on $2^{2r} = 4$ characters: this is what we see, and the values 1 and 2 do not coincide here. The symmetric identity $|S|\,|\hat{T}(x)|^2 = |T|^2 \nu_S(x)$ holds on all 16 elements: $|\hat{T}(x)|^2 = 16, 8, 4, 0$ on $1, 4, 4, 7$ elements, and $\nu_S = 4, 2, 1, 0$ on the same elements. With $\varepsilon = 1$ instead, the first identity fails on 8 of the 16 characters.

The dual configuration. By (3), $A^* = \frac{1}{4}\{z : z \text{ even},\ z_1 + z_2 \equiv 0 \bmod 4\} = \frac{1}{2}D_2$, which contains $\mathbb{Z}^2$. Hence $8Q = 8A^* + T$ is $8\mathbb{Z}^2$-periodic, with residues mod 8

$$(0,0), (6,0), (1,3), (5,5), (4,4), (2,4), (5,7), (1,1).$$

Proposition I. Take $f = 10 = c_0 + e$ with $c_0 = 10$, $e = 00$, so $D = u + f = 01$ has weight $1 \equiv n/2$. Take $v = 10$. Then $\tau = 2(\tilde{\mathbf{1}} - \tilde{c}_0) + 4\tilde{v} = (0,2) + (4,0) = (4,2)$ and $g(x_1, x_2) = (x_1 + 4,\ 2 - x_2)$. The eight residues above go to

$$(4,2), (2,2), (5,7), (1,5), (0,6), (6,6), (1,3), (5,1),$$

which is exactly Γ_8. Since $8Q$ is $8\mathbb{Z}^2$-periodic, $g(8Q) = \Gamma$ as subsets of $\mathbb{R}^2$. Also Γ has density $8/8^2 = 1/8$, and $(2\sqrt{2})^2 = 8$, so $P = \Gamma/(2\sqrt{2})$ has density 1. The minimal squared distance of Γ

is 2 (for instance $(0,6)$ and $(1,5)$), so by (5) the stealth radius at unit density is $\sqrt{2/8} = 1/2$. As $4 \nmid n$, the remark of § 2.4 says that P is formally isodual and not formally self-dual.

What it shows. The finite pair of Theorem A and the map g of Proposition I can be checked by hand in dimension 2, including the readings of the lifts. For $r = 1$ the finite pair is equivalent to a product of two TITO pairs, see § 8.2 and Row 5 of § 7, so this example illustrates the formulas and is not a new object.

3. Proof of Theorem A

The hypotheses used are $n = 2k$, $C_2' = C^\perp$ and $h < k$ (that is, $C \neq C^\perp$); nothing else. The proof computes the Fourier transform of Γ (§ 3.1 to § 3.5), identifies the dual group (§ 3.6), and compares the result with the pair counts of T (§ 3.7 to § 3.11). Items 3, 4 and 5 follow in § 3.12 to § 3.14. The heart of the proof is § 3.5 (odd characters) and § 3.10 (the differences between the two halves of T).

3.0 Conventions and elementary facts

For a statement P, $[P]$ is 1 if P holds and 0 otherwise. L'^* and A^* denote dual lattices. The function $\lambda(x) = \mathrm{wt}(x)/2 \bmod 2$ is defined on any word of even weight. Binary words are read in $\mathbb{F}_2^n$, and in sums and weights also through their 0/1 lift. For $y \in \mathbb{Z}^n$ write $\bar{y} = y \bmod 2 \in \mathbb{F}_2^n$ and $\Sigma y = \sum_i y_i$. For $z \in (\mathbb{Z}/4)^n$ write $z = \bar{z} + 2z_1$ digitwise, with $z_1 \in \mathbb{F}_2^n$; then $\Sigma z \equiv \mathrm{wt}\,\bar{z} + 2\,\mathrm{wt}\,z_1 \pmod 4$. We write Γ_8 for the set of residues of Γ mod 8, E for its even half and O for its odd half, so $\Gamma_8 = E \cup O$ with

$$E = \{-2\tilde{b} + 4\tilde{c} :\ b \in \mathbf{1} + C,\ \mathrm{wt}\,c \text{ even}\}, \qquad O = \{\mathbf{1} - 2\tilde{a} + 4\tilde{c} :\ a \in C^\perp,\ \mathrm{wt}\,c \text{ odd}\}.$$

The characters of $(\mathbb{Z}/8)^n$ are the χ_y, $y \in (\mathbb{Z}/8)^n$, and $\hat{S}_8(y) = \sum_{x \in \Gamma_8} \chi_y(x)$.

(F1) For binary words a, b: $\mathrm{wt}(a+b) = \mathrm{wt}\,a + \mathrm{wt}\,b - 2|a \cap b|$, hence $\mathrm{wt}(a+b) \equiv \mathrm{wt}\,a + \mathrm{wt}\,b + 2\,a \cdot b \pmod 4$. For several words, apply this repeatedly.

(F2) The hull $R = C \cap C^\perp$ is self-orthogonal, so its words are even ($x \cdot x \equiv \mathrm{wt}\,x$). By (F1), $\mathrm{wt}(x + x') \equiv \mathrm{wt}\,x + \mathrm{wt}\,x' \pmod 4$ for $x, x' \in R$, so λ is linear on R, and $\mathrm{wt}\,x \equiv 2\lambda(x) \pmod 4$ for $x \in R$. Also $R^\perp = C + C^\perp$ and $\mathbf{1} \in R^\perp$.

(F3) The words u and w of Theorem A exist. A linear form on R is $x \mapsto u \cdot x$ for some u, which gives u. For w: write $\mathbf{1} = w + w'$ with $w \in C$, $w' \in C^\perp$; for $c \in C$, $w \cdot c = \mathbf{1} \cdot c = \mathrm{wt}\,c \pmod 2$. The admissible w form a coset of R. If C is even they are exactly the elements of R, since $w \cdot c = 0$ on C means $w \in C^\perp$. Two consequences used below: $\mathbf{1} + w \in C^\perp$, and $w \cdot x = 0$ for $x \in R$.

(F4) The maps $(b, c) \mapsto -2\tilde{b} + 4\tilde{c}$ and $(a, c) \mapsto \mathbf{1} - 2\tilde{a} + 4\tilde{c}$ are injective mod 8 (the four values of (b_i, c_i) give four distinct residues mod 8, and likewise for (a_i, c_i)), and E, O are disjoint (parity of the coordinates). So $|E| = |O| = 2^k 2^{n-1}$ and $|\Gamma_8| = 2^{n+k} = 2^{3k}$. Equivalently, writing a point as $2y$ or $\mathbf{1} + 2y$ with $y \in (\mathbb{Z}/4)^n$,

$$E = \{2y :\ \bar{y} \in \mathbf{1} + C,\ \Sigma y \equiv -\mathrm{wt}\,\bar{y}\}, \qquad O = \{\mathbf{1} + 2y :\ \bar{y} \in C^\perp,\ \Sigma y \equiv 2 - \mathrm{wt}\,\bar{y}\} \pmod 4$$

(take $y = -\tilde{b} + 2\tilde{c}$, resp. $-\tilde{a} + 2\tilde{c}$, and note that $\mathrm{wt}\,c$ is even, resp. odd, exactly when $\Sigma y \equiv -\mathrm{wt}\,b$, resp. $2 - \mathrm{wt}\,a$).

3.1 Lemma (periods and sizes)

(a) $\Gamma + L' = \Gamma$ *and* $L' \subseteq A$. *(b)* $|L'/8\mathbb{Z}^n| = 2^{n-1+h}$ *and* $|S| = 2^{r+1}$. *(c) Let* $L'^{\perp} = \{y \in (\mathbb{Z}/8)^n : \chi_y = 1 \text{ on } L'\}$. *Then*

$$L'^{\perp} = \{p\mathbf{1} + 2z : \ p \in \{0,1\},\ z \in (\mathbb{Z}/4)^n,\ \bar{z}\cdot x = p\,\lambda(x)\ \forall x \in R\}, \qquad |L'^{\perp}| = 2^{2n+1-h}.$$

Proof. (a) The lattice $8\mathbb{Z}^n$ fixes Γ by definition. Adding $4(e_1+e_j)$ to $-2\tilde{b}+4\tilde{c}$ gives $-2\tilde{b}+4(\widetilde{c+e_1+e_j})$ mod 8, and e_1+e_j has even weight, so the parity of $\operatorname{wt} c$ is kept; the same holds on O. Let $x \in R$. Coordinatewise one checks $-2\tilde{b}+2\tilde{x} \equiv -2(\widetilde{b+x}) + 4(\widetilde{x\wedge\neg b}) \pmod 8$. Hence adding $2\tilde{x}$ to a point of E replaces b by $b+x$ and c by $c+x\wedge\neg b$. Here $b+x \in \mathbf{1}+C$ because $x \in C$. Moreover $\operatorname{wt}(x\wedge\neg b) = \operatorname{wt} x - |x\cap b|$ is even, because $\operatorname{wt} x$ is even and $|x\cap b| \equiv x\cdot b = x\cdot\mathbf{1} + x\cdot(b+\mathbf{1}) = 0$ (as $x \in C^{\perp}$ and $b+\mathbf{1} \in C$). On O: $\mathbf{1} - 2\tilde{a} + 2\tilde{x} \equiv \mathbf{1} - 2(\widetilde{a+x}) + 4(\widetilde{x\wedge\neg a})$ with $a+x \in C^{\perp}$ ($x \in R \subseteq C^{\perp}$), and $x\wedge\neg a$ has even weight since $x\cdot a = 0$ ($x \in C$). So each generator of L' maps Γ into Γ; as translation is injective and Γ_8 is finite, $\Gamma + g = \Gamma$ for each generator g, hence $\Gamma + L' = \Gamma$. Then every $g \in L'$ is a difference of two points of Γ, so $L' \subseteq A$, $H' = A/L'$ is defined, and $S = (\Gamma - x_0)/L' \subseteq H'$.

(c) χ_y is trivial on $8e_i$ for every y. It is trivial on $4(e_1+e_j)$ iff $y_1 \equiv y_j \pmod 2$; so $y \equiv p\mathbf{1} \pmod 2$ for some $p \in \{0,1\}$, that is $y = p\mathbf{1} + 2z$. It is trivial on $2\tilde{x}$ ($x \in R$) iff $\sum_{i\in x} y_i \equiv 0 \pmod 4$. Now $\sum_{i\in x} y_i = p\operatorname{wt} x + 2\sum_{i\in x} z_i \equiv 2p\lambda(x) + 2\,\bar{z}\cdot x \pmod 4$ by (F2), which vanishes iff $\bar{z}\cdot x = p\lambda(x)$. Both sides are linear in x, so it suffices to impose the condition on a basis of R: h independent affine conditions on $\bar{z}$. This leaves 2^{n-h} words $\bar{z}$, each with 2^n lifts to $(\mathbb{Z}/4)^n$, for each p; hence $|L'^{\perp}| = 2\cdot 2^{n-h}\cdot 2^n$.

(b) The characters of $(\mathbb{Z}/8)^n$ trivial on the subgroup $L'/8\mathbb{Z}^n$ form a group of order $8^n/|L'/8\mathbb{Z}^n|$; so $|L'/8\mathbb{Z}^n| = 2^{3n-(2n+1-h)} = 2^{n-1+h}$. The set Γ_8 is a union of cosets of $L'/8\mathbb{Z}^n$, and S is the set of these cosets: $|S| = 2^{n+k}/2^{n-1+h} = 2^{k-h+1} = 2^{r+1}$. □

3.2 Lemma (the two halves; even characters)

For $y \in \mathbb{Z}^n$, $\hat{S}_8(y) = 0$ *unless* $\bar{y} \in \{0,\mathbf{1}\}$, *and* $\hat{S}_8(y) = 0$ *for* $y \notin L'^{\perp}$. *For* $y = 2z$ *(write* $z_0 = \bar{z}$*):*

$$\hat{S}_8(2z) = 2^{n-1+k}\Big((-1)^{\operatorname{wt} z_0}[z_0 \in C^{\perp}] + i^{\Sigma z}[z_0 \in C]\Big). \tag{3.2.1}$$

Proof. On the two halves, $\chi_y(-2\tilde{b}+4\tilde{c}) = i^{-\langle\tilde{b},y\rangle}(-1)^{c\cdot y}$ and $\chi_y(\mathbf{1}-2\tilde{a}+4\tilde{c}) = \zeta^{\Sigma y} i^{-\langle\tilde{a},y\rangle}(-1)^{c\cdot y}$. Summing over all c gives $2^n[\bar{y}=0]$, and summing $(-1)^{\operatorname{wt} c + c\cdot y}$ gives $2^n[\bar{y}=\mathbf{1}]$. Hence

$$\sum_{\operatorname{wt} c \text{ even}} (-1)^{c\cdot y} = 2^{n-1}([\bar{y}=0] + [\bar{y}=\mathbf{1}]), \qquad \sum_{\operatorname{wt} c \text{ odd}} (-1)^{c\cdot y} = 2^{n-1}([\bar{y}=0] - [\bar{y}=\mathbf{1}]).$$

So $\hat{S}_8(y) = 0$ unless $\bar{y} \in \{0,\mathbf{1}\}$. Since Γ_8 is L'-periodic (Lemma 3.1), $\hat{S}_8(y) = \chi_y(g)\hat{S}_8(y)$ for $g \in L'$, so $\hat{S}_8$ vanishes off $L'^{\perp}$. For $y = 2z$ we have $i^{-\langle\tilde{b},2z\rangle} = (-1)^{b\cdot z_0}$ and $\zeta^{\Sigma y} = i^{\Sigma z}$; the even half contributes $2^{n-1}\sum_{b\in\mathbf{1}+C}(-1)^{b\cdot z_0} = 2^{n-1+k}(-1)^{\operatorname{wt} z_0}[z_0 \in C^{\perp}]$, and the odd half $2^{n-1}i^{\Sigma z}\sum_{a\in C^{\perp}}(-1)^{a\cdot z_0} = 2^{n-1+k}i^{\Sigma z}[z_0 \in C]$. □

3.3 Lemma (Gauss sums of the weight form)

For a binary linear code K and $v \in \mathbb{F}_2^n$ put $G_K(v) = \sum_{c\in K} i^{\operatorname{wt} c}(-1)^{c\cdot v}$.

Then $|G_K(v)|^2 = |K|\sum_{\rho\in K\cap K^{\perp}}(-1)^{\lambda(\rho)+\rho\cdot v}$. *In particular* $|G_K(v)|^2 = |K|\,2^{\dim(K\cap K^{\perp})}\,[\,v\cdot\rho = \lambda(\rho)\ \forall\rho \in K\cap K^{\perp}\,]$.

Proof. Write $|G_K(v)|^2 = \sum_{c,c' \in K} i^{\mathrm{wt}\, c - \mathrm{wt}\, c'} (-1)^{(c+c')\cdot v}$ and put $c' = c + e$, $e \in K$. By (F1), $i^{\mathrm{wt}\, c - \mathrm{wt}\, c'} = i^{-\mathrm{wt}\, e}(-1)^{c\cdot e}$. So $|G_K(v)|^2 = \sum_{e\in K} i^{-\mathrm{wt}\, e}(-1)^{e\cdot v} \sum_{c\in K}(-1)^{c\cdot e}$, and the inner sum is $|K|\,[e \in K^\perp]$. For $e \in K \cap K^\perp$, $\mathrm{wt}\, e \equiv 2\lambda(e) \pmod 4$ (F2), so $i^{-\mathrm{wt}\, e} = (-1)^{\lambda(e)}$. The map $e \mapsto \lambda(e) + e\cdot v$ is linear on $K \cap K^\perp$, so the character sum equals $|K \cap K^\perp|$ if it vanishes identically and 0 otherwise. □

For $K = C$ and $K = C^\perp$ the intersection $K \cap K^\perp$ is R.

3.4 Lemma (Poisson relation)

If $|C| = 2^{n/2}$, then $G_C(v) = \zeta^n\, i^{-\mathrm{wt}\, v}\, \overline{G_{C^\perp}(v)}$ for every $v \in \mathbb{F}_2^n$.

Proof. Poisson summation on $\mathbb{F}_2^n$ reads $\sum_{c\in C} f(c) = |C|\, 2^{-n} \sum_{e\in C^\perp} \hat f(e)$ with $\hat f(e) = \sum_x f(x)(-1)^{x\cdot e}$. For $f(x) = i^{\mathrm{wt}\, x}(-1)^{x\cdot v}$,

$$\hat f(e) = \prod_{j=1}^{n} \bigl(1 + i(-1)^{v_j + e_j}\bigr) = (1+i)^n (-i)^{\mathrm{wt}(v+e)},$$

because $1 + i = \sqrt{2}\,\zeta$ and $1 - i = (1+i)(-i)$. Here $(1+i)^n = 2^{n/2}\zeta^n$ and $|C|2^{-n} = 2^{-n/2}$, so $G_C(v) = \zeta^n \sum_{e\in C^\perp} i^{-\mathrm{wt}(v+e)}$. By (F1), $i^{-\mathrm{wt}(v+e)} = i^{-\mathrm{wt}\, v}\, i^{-\mathrm{wt}\, e}(-1)^{v\cdot e}$, and $\sum_{e\in C^\perp} i^{-\mathrm{wt}\, e}(-1)^{e\cdot v} = \overline{G_{C^\perp}(v)}$. □

3.5 Lemma (odd characters)

Let $y = \mathbf{1} + 2z$ with $z \in (\mathbb{Z}/4)^n$, $z_0 = \bar z$, $z = z_0 + 2z_1$ digitwise, and $G' = G_{C^\perp}(z_0)$. Then

$$\hat S_8(\mathbf{1} + 2z) = 2^{n-1}\zeta^{-n}\, i^{\mathrm{wt}\, z_0}\, \overline{G'}\, \Bigl(1 - (-1)^{k + \mathrm{wt}\, z_1}\Bigr). \tag{3.5.1}$$

If moreover $\mathbf{1} + 2z \in L'^\perp$, then

$$|\hat S_8(\mathbf{1} + 2z)|^2 = 2^{2n+k+h}\, [\, \mathrm{wt}\, z_1 \equiv n/2 + 1 \pmod 2\,]. \tag{3.5.2}$$

Proof. Let $\hat E$ and $\hat O$ be the contributions of E and O. Here $\bar y = \mathbf{1}$, so by Lemma 3.2 the sum over c is $+2^{n-1}$ on E and -2^{n-1} on O. We have $\langle \tilde b, y\rangle = \mathrm{wt}\, b + 2\langle \tilde b, z\rangle \equiv \mathrm{wt}\, b + 2\, b\cdot z_0 \pmod 4$. For $b = \mathbf{1} + p$, $p \in C$: $\mathrm{wt}\, b = n - \mathrm{wt}\, p$ and $b\cdot z_0 = \mathrm{wt}\, z_0 + p\cdot z_0$. Therefore

$$\hat E = 2^{n-1} i^{-n} (-1)^{\mathrm{wt}\, z_0} G_C(z_0), \qquad \hat O = -2^{n-1}\zeta^{\Sigma y}\, \overline{G'}, \quad \Sigma y = n + 2\Sigma z.$$

By Lemma 3.4 (here $|C| = 2^{n/2}$ is used), $G_C(z_0) = \zeta^n i^{-\mathrm{wt}\, z_0}\overline{G'}$; with $i^{-n}\zeta^n = \zeta^{-n}$ and $(-1)^{\mathrm{wt}\, z_0} i^{-\mathrm{wt}\, z_0} = i^{\mathrm{wt}\, z_0}$ this gives $\hat E = 2^{n-1}\zeta^{-n} i^{\mathrm{wt}\, z_0}\overline{G'}$. Also $\zeta^{\Sigma y} = \zeta^n i^{\Sigma z}$, so

$$\hat O / \hat E = -\zeta^{2n}\, i^{\Sigma z - \mathrm{wt}\, z_0} = -i^n\, i^{2\,\mathrm{wt}\, z_1} = -(-1)^{k + \mathrm{wt}\, z_1} \qquad (\text{when } \hat E \neq 0).$$

So $\hat S_8 = \hat E + \hat O = \hat E\,(1 - (-1)^{k+\mathrm{wt}\, z_1})$, which is (3.5.1). Hence $\hat S_8$ is either 0 or $2\hat E$, according as $\mathrm{wt}\, z_1 \equiv k$ or $k+1$. If $\mathbf{1} + 2z \in L'^\perp$ then $z_0 \cdot x = \lambda(x)$ for all $x \in R$ (Lemma 3.1, $p = 1$), and Lemma 3.3 with $K = C^\perp$ gives $|G'|^2 = 2^k 2^h$. Then $|\hat S_8|^2 = 4 \cdot 2^{2n-2} \cdot 2^{k+h}$ in the second case ($\mathrm{wt}\, z_1 \equiv k+1$), and 0 in the first, which is (3.5.2) since $k = n/2$. □

3.6 Lemma (the dual group)

(a) Every character of $H' = A/L'$ is $\chi_y|_A$ for some $y \in L'^{\perp}$, and $\chi_y = \chi_{y'}$ on H' iff $y - y' \in A^{\perp} := \{y : \chi_y = 1 \text{ on } A\}$. So $\widehat{H'} \cong L'^{\perp}/A^{\perp}$. (b) $A^{\perp} = \{2z : z \in (\mathbb{Z}/4)^n,\ \bar{z} \in R,\ \Sigma z \equiv 0 \pmod 4\}$. It has 2^{h+n-1} elements, and $|H'| = 2^{2r+2}$. (c) $A^* = \frac{1}{4}\{z \in \mathbb{Z}^n : z \bmod 2 \in R,\ \sum z_i \equiv 0 \pmod 4\}$, which is (3). The map $y/8 + A^* \mapsto \chi_y|_{H'}$ is an isomorphism $L'^*/A^* \to \widehat{H'}$, compatible with the pairing $\langle x + L', y/8 + A^*\rangle = e^{2\pi i\langle x,y\rangle/8} = \chi_y(x)$. (d) Let $\mathcal{E} = \{2z \in L'^{\perp}\}$ be the even characters, $z \in (\mathbb{Z}/4)^n$ with $\bar{z} \in R^{\perp}$. The map $\psi(2z) = (\bar{z} + R,\ \Sigma z \bmod 4) \in (R^{\perp}/R) \times \mathbb{Z}/4$ is a homomorphism with kernel $A^{\perp}$ and image $\{(v + R, s) : s \equiv \operatorname{wt} v \pmod 2\}$. So $|\mathcal{E}/A^{\perp}| = 2^{2r+1}$, and $\mathcal{E}/A^{\perp}$ has index 2 in $\widehat{H'}$. (e) $\widehat{H'}$ is elementary abelian if and only if $\mathbf{1} \in R$.

Proof. (a) A character of the subgroup A/L' of the finite abelian group $\mathbb{Z}^n/L'$ extends to $\mathbb{Z}^n/L'$. The characters of $\mathbb{Z}^n/L'$ are the χ_y with $y \in L'^{\perp}$ (as $8\mathbb{Z}^n \subseteq L'$). Two such characters agree on A iff $y - y' \in A^{\perp}$.

(b) By the triangle inequality, $y \in A^{\perp}$ iff χ_y is constant on Γ_8 iff $|\hat{S}_8(y)| = |\Gamma_8| = 2^{n+k}$. Characters with $\bar{y} \notin \{0, \mathbf{1}\}$ have $\hat{S}_8 = 0$. For $\bar{y} = \mathbf{1}$, (3.5.2) and Lemma 3.2 give $|\hat{S}_8|^2 \le 2^{2n+k+h} < 2^{2n+2k}$, because $h < k$. For $y = 2z$, formula (3.2.1) has modulus 2^{n+k} iff both terms are present and equal, i.e. $\bar{z} \in C \cap C^{\perp} = R$ and $i^{\Sigma z} = (-1)^{\operatorname{wt}\bar{z}} = 1$ (the words of R are even). This is the stated set. Count: 2^h words $\bar{z}$, 2^n lifts, half of which satisfy $\Sigma z \equiv 0 \pmod 4$ (since $\operatorname{wt}\bar{z}$ is even): 2^{h+n-1}. Hence $|H'| = |L'^{\perp}|/|A^{\perp}| = 2^{2n+1-h}/2^{h+n-1} = 2^{n+2-2h} = 2^{2r+2}$.

(c) Since $8\mathbb{Z}^n \subseteq L' \subseteq A \subseteq \mathbb{Z}^n$, we have $A^* \subseteq \frac{1}{8}\mathbb{Z}^n$ and, for $y \in \mathbb{Z}^n$: $y/8 \in A^*$ iff $\langle a, y\rangle \in 8\mathbb{Z}$ for all $a \in A$ iff $y \bmod 8 \in A^{\perp}$. By (b), $A^* = \frac{1}{8} \cdot 2\{z \in \mathbb{Z}^n : \bar{z} \in R,\ \Sigma z \equiv 0\ (4)\}$, which is (3). In the same way $L'^* = \frac{1}{8}\{y \in \mathbb{Z}^n : y \bmod 8 \in L'^{\perp}\}$, and $y/8 + A^* \mapsto (y \bmod 8) + A^{\perp}$ is an isomorphism $L'^*/A^* \to L'^{\perp}/A^{\perp} \cong \widehat{H'}$ that matches the pairing.

(d) ψ is a homomorphism because $z \mapsto \bar{z}$ and $z \mapsto \Sigma z \bmod 4$ are additive. Its kernel is $\{\bar{z} \in R,\ \Sigma z \equiv 0\} = A^{\perp}$ by (b). Since $\Sigma z \equiv \operatorname{wt}\bar{z} \pmod 2$, the image lies in $\{(v + R, s) : s \equiv \operatorname{wt} v\}$ (well defined because R is even). Conversely, for such $(v + R, s)$ take $z = \tilde{v} + 2\tilde{t}$ with $\operatorname{wt} v + 2\operatorname{wt} t \equiv s \pmod 4$. The image has $2^{n-2h} \cdot 2 = 2^{2r+1}$ elements ($n - 2h = 2r$). The even characters are those with $p = 0$ in Lemma 3.1(c), which is a subgroup of index 2 of $L'^{\perp}$.

(e) We ask whether $2y \in A^{\perp}$ for every $y \in L'^{\perp}$. Suppose $\mathbf{1} \in R$. For $y = 2z$ with $\bar{z} \in R^{\perp}$: $2y = 2z'$ with $z' = 2z$, $\bar{z}' = 0$, and $\Sigma z' = 2\Sigma z \equiv 2\operatorname{wt}\bar{z} \equiv 0$ since $\bar{z} \perp \mathbf{1}$. For $y = \mathbf{1} + 2z$: $2y = 2z'$ with $z' = \mathbf{1} + 2z$, so $\bar{z}' = \mathbf{1} \in R$, and $\Sigma z' = n + 2\Sigma z$. The condition of Lemma 3.1(c) at $x = \mathbf{1}$ gives $\operatorname{wt}\bar{z} \equiv n/2 \pmod 2$, so $2\Sigma z \equiv n \pmod 4$ and $\Sigma z' \equiv 2n \equiv 0$. Hence $2y \in A^{\perp}$. Suppose $\mathbf{1} \notin R$. As $R = (R^{\perp})^{\perp}$, some $z_0 \in R^{\perp}$ has odd weight. For $y = 2\tilde{z}_0 \in \mathcal{E}$: $2y = 2z'$ with $z' = 2\tilde{z}_0$, $\bar{z}' = 0$, $\Sigma z' = 2\operatorname{wt} z_0 \equiv 2$, so $2y \notin A^{\perp}$: the character has order 4. □

3.7 Lemma (the target function)

Put $|T| = 2^{r+1}$ (proved in § 3.8) and, for $\chi = \chi_y$ with $y \in L'^{\perp}$, $\nu^*(\chi) = |T|\,|\hat{S}_H(\chi)|^2/|S|^2$, where $\hat{S}_H(\chi) = \sum_{s\in S}\chi(s)$. Then:

- *for odd $y = \mathbf{1} + 2z$: $\nu^* = 2\,[\operatorname{wt} z_1 \equiv n/2 + 1\ (2)\,]$;*
- *for even $y = 2z$: $\nu^* = 2^{r-1}\left|(-1)^{\operatorname{wt}\bar{z}}[\bar{z} \in C^{\perp}] + i^{\Sigma z}[\bar{z} \in C]\right|^2$. In ψ-coordinates of Lemma 3.6(d): $\nu^* = 2^{r+1}$ at $(0,0)$; $\nu^* = 0$ at $(0,2)$; $\nu^* = 2^{r-1}$ at the $4(2^r - 1)$ classes $(v + R, s)$ with $v \in (C \cup C^{\perp}) \setminus R$; $\nu^* = 0$ elsewhere.*

Proof. Since χ_y is trivial on L', each of the $|S|$ cosets of L' in $\Gamma - x_0$ contributes $|L'/8\mathbb{Z}^n|$ equal terms: $|\hat{S}_8(y)| = |L'/8\mathbb{Z}^n|\,|\hat{S}_H(\chi_y)|$. With $|\Gamma_8| = |S|\,|L'/8\mathbb{Z}^n|$ this gives $|\hat{S}_H|^2/|S|^2 = |\hat{S}_8|^2/|\Gamma_8|^2$. For odd y, (3.5.2) gives $\nu^* = 2^{r+1}2^{2n+k+h}/2^{2n+2k}\,[\cdots] = 2^{r+1-(k-h)}[\cdots] = 2[\cdots]$. For even y,

(3.2.1) gives $\nu^* = 2^{r+1} \cdot 2^{2n-2+2k}/2^{2n+2k} \,|\cdots|^2 = 2^{r-1}|\cdots|^2$. For $\bar{z} \in R$ the bracket is $|1 + i^{\Sigma z}|^2$, equal to 4 if $\Sigma z \equiv 0$ and to 0 if $\Sigma z \equiv 2$ (Σz is even). For $\bar{z} \in (C \cup C^\perp) \setminus R$ exactly one term is present and the modulus is 1. Otherwise it is 0. Finally $R^\perp/R = C/R \oplus C^\perp/R$ (as $R^\perp = C + C^\perp$ and $C \cap C^\perp = R$); each of $C/R \setminus 0$ and $C^\perp/R \setminus 0$ has $2^r - 1$ elements, and each v carries two classes $s \equiv \operatorname{wt} v \pmod 2$. □

3.8 Lemma (the set T)

Put $a(c) = 2\tilde{c} + 4(u \cdot c)e_1$ for $c \in C$, $a_2(d) = 2\tilde{d} + 4(u \cdot d)e_1$ for $d \in C^\perp$, and $y^* = \mathbf{1} + 2\widetilde{(u+w)} + 4\varepsilon e_1$. Then $T = X_1 \cup (y^* + X_2)$ with $X_1 = \{a(c)\}$, $X_2 = \{a_2(d)\}$, and: (i) every element of T lies in $L'^\perp$; (ii) $\psi(a(c)) = (c + R, F_1(c))$ with $F_1(c) = \operatorname{wt} c + 2\,u \cdot c \pmod 4$, which depends only on $c + R$; likewise $\psi(a_2(d)) = (d + R, F_2(d))$ with $F_2(d) = \operatorname{wt} d + 2\,u \cdot d$ on $C^\perp/R$; (iii) as a set of characters of H', X_1 is the graph of F_1 over C/R and X_2 the graph of F_2 over $C^\perp/R$: each has 2^r elements, and each element has 2^h preimages. The two halves X_1 and $y^* + X_2$ are disjoint (even versus odd), so $|T| = 2^{r+1}$.

Proof. The second half of (2) is $y^* + a_2(d)$. (i) For $a(c)$: $z = \tilde{c} + 2(u \cdot c)e_1$ has $\bar{z} = c \in C \subseteq R^\perp$. For $a_2(d)$: $\bar{z} = d \in C^\perp \subseteq R^\perp$ (as $R \subseteq C$). For y^*: $p = 1$, $\bar{z} = u + w$, and $(u + w) \cdot x = \lambda(x) + 0$ for $x \in R$ by (F3). (ii) $\Sigma z = \operatorname{wt} c + 2\,u \cdot c$. For $x \in R$ and $c \in C$ we have $c \cdot x = 0$, so by (F1), (F2): $F_1(c + x) = \operatorname{wt} c + 2\lambda(x) + 2\,u \cdot c + 2\lambda(x) = F_1(c)$; the same for F_2 using $d \cdot x = 0$ for $d \in C^\perp$, $x \in R \subseteq C$. (iii) follows from (ii): ψ separates distinct classes $c + R$ by its first coordinate, and elements with the same image differ by an element of $A^\perp$, hence are the same character. □

3.9 Lemma (ν_T on even characters)

On $\mathcal{E}/A^\perp$, $\nu_T = \nu^*$.

Proof. A difference of two elements of T is even iff both lie in the same half. So $\nu_T = \nu_{X_1} + \nu_{X_2}$ on even characters ($y^* + X_2$ has the same differences as X_2). In ψ-coordinates $X_1 = \{(c + R, F_1(c))\}$. For $v \in C/R$, (F1) gives $F_1(c + v) - F_1(c) = F_1(v) + 2\,c \cdot v \pmod 4$. The form $c \mapsto c \cdot v$ on C/R is well defined ($v \in C \subseteq R^\perp$), and it is non-zero iff $v \notin R$, because the radical of the dot product on C is $C \cap C^\perp = R$. So for $v \neq 0$ in C/R the differences $(v, F_1(v))$ and $(v, F_1(v) + 2)$ each occur 2^{r-1} times; for $v = 0$ the difference $(0, 0)$ occurs 2^r times and $(0, 2)$ never; no other class occurs. Thus $\nu_{X_1} = 2^r$ at $(0, 0)$, 2^{r-1} at both classes over each $v \in C/R \setminus 0$, and 0 elsewhere. The same holds for X_2 over $C^\perp/R$. The supports of the two halves over $v \neq 0$ are disjoint ($C/R \cap C^\perp/R = 0$), so ν_T is 2^{r+1} at $(0, 0)$, 0 at $(0, 2)$, 2^{r-1} over $(C \cup C^\perp) \setminus R$, and 0 elsewhere: this is ν^* (Lemma 3.7). When C is even, $F_1(c)/2 = \operatorname{wt}(c)/2 + u \cdot c \pmod 2$ is a non-degenerate quadratic form on C/R with polar form $c \cdot c'$, i.e. a bent function. □

3.10 Lemma (ν_T on odd characters)

For odd characters x, $\nu_T(x) = \nu^*(x)$. Moreover the odd characters with $\nu^* = 2$ are exactly the 2^{2r} characters $g(c, d) = y^* + a_2(d) - a(c)$, $(c, d) \in C/R \times C^\perp/R$.

Proof. A pair $(t, t') \in T^2$ with odd difference has one element in each half. So $\nu_T(x) = N(x) + N(-x)$ with $N(x) = \#\{(c, d) \in C/R \times C^\perp/R :\ g(c, d) = x\}$.

(i) *The 2^{2r} characters $g(c, d)$ are distinct.* If $g(c, d) = g(c', d')$, then $a_2(d) - a_2(d') - a(c) + a(c') \in A^\perp$, so its ψ-image has zero first coordinate: $c + c' + d + d' \in R$. Then $c + c' \in C \cap (C^\perp + R) = C \cap C^\perp = R$, so $c \equiv c'$, and then $d \equiv d'$ modulo R.

(ii) $\nu^*(g(c, d)) = 2$. The vector $g(c, d)$ is $\mathbf{1} + 2z$ with $z = \widetilde{(u+w)} + \tilde{d} - \tilde{c} + 2(\varepsilon + u \cdot d - u \cdot c)e_1$, so $\bar{z} = u + w + c + d$. We compute $\Sigma z - \operatorname{wt} \bar{z} \pmod 4$. First, $\Sigma z \equiv \operatorname{wt}(u+w) + \operatorname{wt} d - \operatorname{wt} c + 2\varepsilon + 2\,u \cdot d - 2\,u \cdot c$.

Second, by (F1) and $c \cdot d = 0$: $\operatorname{wt} \bar{z} \equiv \operatorname{wt}(u+w) + \operatorname{wt} c + \operatorname{wt} d + 2(u+w)\cdot c + 2(u+w)\cdot d$. Subtracting, and using $-2 \equiv 2$ and $4 \equiv 0$ modulo 4:

$$\Sigma z - \operatorname{wt} \bar{z} \equiv 2 \operatorname{wt} c + 2\varepsilon + 2\, w \cdot c + 2\, w \cdot d \equiv 2\varepsilon \pmod 4,$$

because $w \cdot c \equiv \operatorname{wt} c$ and $w \cdot d = 0$ ($w \in C$, $d \in C^\perp$). So $2 \operatorname{wt} z_1 \equiv 2\varepsilon$, i.e. $\operatorname{wt} z_1 \equiv \varepsilon \equiv n/2 + 1$, and $\nu^* = 2$ by Lemma 3.7.

(iii) *Counting.* By Parseval on H', $\sum_\chi |\hat{S}_H(\chi)|^2 = |H'||S|$, so $\sum_\chi \nu^*(\chi) = |T||H'|/|S| = |T|^2 = 2^{2r+2}$ (as $|H'| = |S||T|$). By Lemma 3.7 the even part sums to $2^{r+1} + 4(2^r - 1)2^{r-1} = 2^{2r+1}$; the odd part sums to 2^{2r+1}, and each odd value is 0 or 2. So exactly 2^{2r} odd characters have $\nu^* = 2$. By (i) and (ii) these are the $g(c,d)$.

(iv) $\nu^*(\bar{\chi}) = \nu^*(\chi)$, because $\hat{S}_H(\bar{\chi}) = \overline{\hat{S}_H(\chi)}$. So the set $G = \{g(c,d)\}$ satisfies $G = -G$, and by (i) $N(x) = [x \in G] = N(-x)$. Hence $\nu_T(x) = 2[x \in G] = \nu^*(x)$ for odd x. □

3.11 Proof of items 1 and 2

Item 1: L' is a lattice of periods and $|S| = 2^{r+1}$ (Lemma 3.1); $|H'| = 2^{2r+2}$ (Lemma 3.6(b)); T consists of 2^{r+1} distinct characters with the stated multiplicities and disjoint halves (Lemma 3.8). Item 2: every character of H' is χ_y with $y \in L'^\perp$, even or odd. By Lemmas 3.7, 3.9 and 3.10, $|T|\,|\hat{S}_H(\chi)|^2 = |S|^2 \nu^*(\chi) = |S|^2 \nu_T(\chi)$ for every $\chi \in \widehat{H'}$: this is the first identity.

Second identity. Let $g \in H'$. Multiply the first identity by $\overline{\chi(g)}$ and sum over $\chi \in \widehat{H'}$. On the left, $\sum_\chi |\hat{S}_H(\chi)|^2 \overline{\chi(g)} = |H'|\,\nu_S(g)$. On the right, $\sum_\chi \nu_T(\chi)\overline{\chi(g)} = \sum_{t,t' \in T} \overline{(t-t')(g)} = \big|\sum_{t\in T} t(g)\big|^2$. So $|T|\,|H'|\,\nu_S(g) = |S|^2\,|\hat{T}(g)|^2$ with $\hat{T}(g) = \sum_{t\in T} t(g)$; with $|H'| = |S||T|$ this is $|T|^2 \nu_S(g) = |S|\,|\hat{T}(g)|^2$. □

3.12 Proof of item 3

We use [CKRS, Cor. 2.7] (equivalently [CKRS, Thm. 2.8]): let $P = \bigcup_{j=1}^N (\Lambda + v_j)$ and $Q = \bigcup_{j=1}^M (\Gamma_Q + w_j)$ with lattices Λ, Γ_Q, $P - P \subseteq \Gamma_Q^*$ and $Q - Q \subseteq \Lambda^*$. Then P and Q are formally dual iff, for every $y \in \Lambda^*$,

$$\Big| N^{-1} \sum_j e^{2\pi i \langle v_j, y\rangle} \Big|^2 = M^{-1}\, \#\{(z,j,k) :\ z \in \Gamma_Q,\ y = z + w_j - w_k\}.$$

Take $\Lambda = L'$, v_j the elements of $\Gamma - x_0$ representing S ($N = |S|$), $\Gamma_Q = A^*$, $w_j = t_j/8$ for $t_j \in T$ ($M = |T|$). Translation by x_0 does not affect formal duality. The $t_j/8$ are distinct modulo A^* because the t_j are distinct characters (Lemma 3.8). The hypotheses hold: $P - P = \Gamma - \Gamma \subseteq A = (A^*)^*$; and $Q - Q \subseteq L'^*$ because $A^* \subseteq L'^*$ (as $L' \subseteq A$) and $T \subseteq L'^\perp$ gives $T/8 \subseteq L'^*$. Now let $y = m/8 \in L'^*$, with $m \bmod 8 \in L'^\perp$. The left side is $|\hat{S}_H(\chi_m)|^2/|S|^2$. On the right, for each pair $(t,t') \in T^2$ with $(m - t + t')/8 \in A^*$ the element z is determined, so the count is $\#\{(t,t') : t - t' = \chi_m \text{ in } L'^\perp/A^\perp\} = \nu_T(\chi_m)$ (Lemma 3.6(c)); the right side is $\nu_T(\chi_m)/|T|$. The equality is the first identity of item 2. Hence Γ and $Q = A^* + T/8$ are formally dual. □

3.13 Proof of item 4

By Lemmas 3.7, 3.9 and 3.10, ν_T equals 2^{r+1} at 0, 2^{r-1} on $4(2^r - 1)$ even characters, 2 on the 2^{2r} odd characters $g(c,d)$, and 0 elsewhere. These are three disjoint families of characters. For $r = 2$ the values 2^{r-1} and 2 coincide, and $\nu_T = 2$ on $4 \cdot 3 + 16 = 28$ characters. The statement on $\widehat{H'}$ is Lemma 3.6(e).

Remark (last line of Theorem A). If $\mathbf{1} \in R$ then $\mathbf{1} \in C^\perp$, so every $c \in C$ has even weight and $c \cdot c = 0$. The dot product is thus alternating on C. Its radical on C is $C \cap C^\perp = R$, so it is non-degenerate and alternating on C/R, and $r = \dim C/R$ is even. This remark was not reviewed.

3.14 Proof of item 5

Primitivity in the sense of [KS, Def. 3.1] means two conditions on each of S and T: not contained in a coset of a proper subgroup, and not a union of cosets of a non-trivial subgroup. For a formally dual pair, S lies in a coset of a subgroup K iff T is a union of cosets of the annihilator $K^\perp$, and symmetrically [KS, Thm. 3.2; CKRS, Lemma 4.2]. So it is enough to show that S and T lie in no coset of a proper subgroup, that is, that $S - S$ generates H' and $T - T$ generates $\widehat{H'}$.

S. $A = \langle \Gamma - \Gamma \rangle$, so the differences of S generate $A/L' = H'$.

T. Since $h < k$, $C/R \neq 0$. Take $v \in C/R$, $v \neq 0$. As $v \notin R$ there is $c \in C$ with $c \cdot v = 1$. The differences $a(v) - a(0)$ and $a(c+v) - a(c)$ have ψ-images $(v, F_1(v))$ and $(v, F_1(v) + 2)$ (proof of Lemma 3.9). Their difference is $(0, 2)$. So $\langle X_1 - X_1 \rangle$ contains $(0, 2)$ and every (v, s) with $v \in C/R$ and $s \equiv \operatorname{wt} v \pmod 2$. The same holds for X_2 over $C^\perp/R$. As $R^\perp = C + C^\perp$, and $\operatorname{wt}(v_1 + v_2) \equiv \operatorname{wt} v_1 + \operatorname{wt} v_2 \pmod 2$, these differences generate the whole of $\mathcal{E}/A^\perp$, which has index 2 in $\widehat{H'}$ (Lemma 3.6(d)). Finally $y^* - a(0) = y^* \in T - T$ is odd. So $\langle T - T \rangle = \widehat{H'}$. □

4. Proof of Proposition I

Items 1 and 2 are identities between sets of residues mod 8 and use no external result. Item 3 uses Theorem A, item 3, and [CKRS, Lemma 2.4]. We use the conventions and facts (F1) to (F4) of § 3.0 and the description of A^* in (3). By (3), $8Q = 8A^* + T = 2M + T$ with

$$M = \{z \in \mathbb{Z}^n : \ \bar{z} \in R, \ \Sigma z \equiv 0 \pmod 4\}.$$

For $y \in (\mathbb{Z}/4)^n$, $\bar{y}$ and $\Sigma y \bmod 4$ are well defined. For the sign change σ_D we have $\sigma_D(y) \equiv y \pmod 2$, $\Sigma\, \sigma_D(y) \equiv \Sigma y + 2\, D \cdot \bar{y} \pmod 4$ (each flipped coordinate changes y_i to $y_i - 2y_i$), and $\sigma_D(\mathbf{1}) = \mathbf{1} - 2\tilde{D}$.

Step 1 (description of $8Q$ mod 8). *Even points.* An element of $2M + T$ of the first kind is $2z + 2\tilde{c} + 4(u \cdot c)e_1 = 2y$ with $z \in M$, $c \in C$, $y = z + \tilde{c} + 2(u \cdot c)e_1$. Put $h' = \bar{z} \in R$ and $b = \bar{y} = c + h' \in C$. Since $\Sigma z \equiv 0$: $\Sigma y \equiv \operatorname{wt} c + 2\, u \cdot c$. By (F1), (F2) and $b \cdot h' = 0$: $\operatorname{wt} c = \operatorname{wt}(b + h') \equiv \operatorname{wt} b + 2\lambda(h')$; and $2\, u \cdot c = 2\, u \cdot b + 2\lambda(h')$. Hence

$$\Sigma y \equiv \operatorname{wt} b + 2\, u \cdot b \pmod 4, \qquad b = \bar{y} \in C.$$

Odd points. An element of the second kind is $2z + y^* + a_2(d) = \mathbf{1} + 2y$ with $y = z + \widetilde{(u + w)} + \tilde{d} + 2(\varepsilon + u \cdot d)e_1$. Here $b = \bar{y} = h' + u + w + d$ with $h' = \bar{z} \in R$, $d \in C^\perp$, and

$$\Sigma y \equiv \operatorname{wt}(u + w) + \operatorname{wt} d + 2\varepsilon + 2\, u \cdot d \pmod 4.$$

Step 2 (even points go to E). Let $2y$ be as in Step 1. Then $g(2y) = 2\sigma_D(y) + 2(\tilde{\mathbf{1}} - \tilde{c}_0) + 4\tilde{v} = 2y'$ with $y' = \sigma_D(y) + \tilde{\mathbf{1}} - \tilde{c}_0 + 2\tilde{v}$. Its parity class is $\bar{y}' = b + \mathbf{1} + c_0 \in \mathbf{1} + C$. Its sum is

$$\Sigma y' \equiv \operatorname{wt} b + 2\, u \cdot b + 2\, D \cdot b + n - \operatorname{wt} c_0 + 2 \operatorname{wt} v \equiv \operatorname{wt} b + 2\, c_0 \cdot b + n - \operatorname{wt} c_0 + 2 \operatorname{wt} v,$$

because $2(u+D)\cdot b = 2(c_0+e)\cdot b = 2\,c_0\cdot b$ ($e \in C^\perp$, $b \in C$). By (F1), $-\mathrm{wt}\,\bar{y}' = -(n-\mathrm{wt}(b+c_0)) \equiv -n + \mathrm{wt}\,b + \mathrm{wt}\,c_0 + 2\,b\cdot c_0$. The difference between this value and $\Sigma y'$ is $2n + 2(\mathrm{wt}\,v - \mathrm{wt}\,c_0) \equiv 0 \pmod 4$, since n is even and $\mathrm{wt}\,v \equiv \mathrm{wt}\,c_0 \pmod 2$. By (F4), $g(2y) \in E$.

Step 3 (odd points go to O). Let $\mathbf{1}+2y$ be as in Step 1. Then $g(\mathbf{1}+2y) = \mathbf{1} - 2\tilde{D} + 2\sigma_D(y) + 2(\tilde{\mathbf{1}} - \tilde{c}_0) + 4\tilde{v} = \mathbf{1} + 2y'$ with $y' = \sigma_D(y) - \tilde{D} + \tilde{\mathbf{1}} - \tilde{c}_0 + 2\tilde{v}$. Its parity class is $\bar{y}' = \mathbf{1} + w + d + e + h'$, which lies in $C^\perp$: $\mathbf{1}+w \in C^\perp$ by (F3), and $d, e, h' \in C^\perp$. Next we compute $\Sigma y' \equiv \Sigma y + 2D\cdot b - \mathrm{wt}\,D + n - \mathrm{wt}\,c_0 + 2\,\mathrm{wt}\,v$ modulo 4. We use $D = u + c_0 + e$, $b = h' + u + w + d$ and these facts: $u\cdot h' = \lambda(h')$; $c_0\cdot h' = c_0\cdot d = e\cdot h' = e\cdot w = 0$; $c_0\cdot w = \mathrm{wt}\,c_0$. They give, modulo 2,

$$D\cdot b \equiv \lambda(h') + \mathrm{wt}\,u + u\cdot w + u\cdot d + c_0\cdot u + \mathrm{wt}\,c_0 + e\cdot u + e\cdot d.$$

By (F1), $\mathrm{wt}\,D \equiv \mathrm{wt}\,u + \mathrm{wt}\,c_0 + \mathrm{wt}\,e + 2\,u\cdot c_0 + 2\,u\cdot e$ and $\mathrm{wt}(u+w) \equiv \mathrm{wt}\,u + \mathrm{wt}\,w + 2\,u\cdot w$. Substituting, all cross terms cancel in pairs and

$$\Sigma y' \equiv \mathrm{wt}\,w + \mathrm{wt}\,d + 2\varepsilon + 2\lambda(h') + 2\,\mathrm{wt}\,u + 2\,e\cdot d + n - \mathrm{wt}\,e + 2\,\mathrm{wt}\,v.$$

On the other hand $\mathrm{wt}\,\bar{y}' = n - \mathrm{wt}(w+d+e+h')$, and by (F1) (using $w\cdot d = w\cdot e = w\cdot h' = d\cdot h' = e\cdot h' = 0$ and $\mathrm{wt}\,h' \equiv 2\lambda(h')$), $\mathrm{wt}(w+d+e+h') \equiv \mathrm{wt}\,w + \mathrm{wt}\,d + \mathrm{wt}\,e + 2\lambda(h') + 2\,d\cdot e$. So the value required by (F4) is

$$2 - \mathrm{wt}\,\bar{y}' \equiv 2 - n + \mathrm{wt}\,w + \mathrm{wt}\,d + \mathrm{wt}\,e + 2\lambda(h') + 2\,d\cdot e.$$

The difference between the required value and $\Sigma y'$ is $2(\varepsilon + 1 + \mathrm{wt}\,u + \mathrm{wt}\,e + \mathrm{wt}\,v) \equiv 2(\varepsilon + 1 + \mathrm{wt}\,D) \pmod 4$, using $\mathrm{wt}\,v \equiv \mathrm{wt}\,c_0$. It vanishes iff $\mathrm{wt}\,D \equiv \varepsilon + 1 \equiv n/2 \pmod 2$, which is the hypothesis on f. By (F4), $g(\mathbf{1}+2y) \in O$.

Step 4 (counting; end of item 1). The set $8Q = 2M + T$ is invariant under $8\mathbb{Z}^n$, since $4e_i \in M$. The map g satisfies $g(x+8z) = g(x) + 8\sigma_D z$, so it induces a bijection of $(\mathbb{Z}/8)^n$. By Steps 2 and 3, g maps the residues of $8Q$ into Γ_8. We bound $|8Q \bmod 8|$ from below. *Even part:* for $b \in C$ take $z = 0$, $c = b$, $y_0 = \tilde{b} + 2(u\cdot b)e_1$. For every word s of even weight, $z = 2\tilde{s} \in M$ ($\bar{z} = 0$, $\Sigma z = 2\,\mathrm{wt}\,s \equiv 0$), so $y_0 + 2\tilde{s}$ also occurs. These are 2^{n-1} distinct residues mod 4 with $\bar{y} = b$. *Odd part:* for $b \in u + w + C^\perp$ take $h' = 0$ and $d = b + u + w$, and add $2\tilde{s}$ in the same way: 2^{n-1} distinct residues with $\bar{y} = b$. Distinct b give distinct $\bar{y}$. So $|8Q \bmod 8| \geq 2\cdot 2^k \cdot 2^{n-1} = 2^{n+k} = |\Gamma_8|$. As g is injective on residues and $g(8Q \bmod 8) \subseteq \Gamma_8$, we get $g(8Q \bmod 8) = \Gamma_8$, hence $g(8Q) = \Gamma$. The computation used only $c_0 \in C$, $e \in C^\perp$, $c_0 + e = f$ and $\mathrm{wt}\,v \equiv \mathrm{wt}\,c_0$, so any decomposition of f works. This proves item 1.

Step 5 (item 2). Since $\mathrm{wt}\,x \equiv x\cdot\mathbf{1} \pmod 2$, the condition is $(u+f)\cdot\mathbf{1} \equiv n/2$. If $\mathbf{1} \in R$: $u\cdot\mathbf{1} = \lambda(\mathbf{1}) = n/2 \pmod 2$ and $f\cdot\mathbf{1} = 0$ for every $f \in R^\perp$, so every f works. For $f = 0$ (so $c_0 = e = 0$, $v = 0$) we get $D = u$, $\tau = 2\cdot\mathbf{1}$ and $g(x) = \sigma_u x + 2\cdot\mathbf{1}$. If $\mathbf{1} \notin R$: the form $f \mapsto f\cdot\mathbf{1}$ is non-zero on $R^\perp$ (otherwise $\mathbf{1} \in (R^\perp)^\perp = R$), so $R^\perp$ contains an odd word f_1; of $f = 0$ and $f = f_1$ exactly one satisfies the condition.

Step 6 (item 3). By (F4), Γ is a union of 2^{3k} translates of $8\mathbb{Z}^n$, so its density is $\delta(\Gamma) = 2^{3k}/8^n = 2^{-3k}$. Scaling by $1/(2\sqrt{2})$ multiplies the density by $(2\sqrt{2})^n = 2^{3k}$, so $\delta(P) = 1$ for $P = \Gamma/(2\sqrt{2})$. Since $\sigma_D^{-1} = \sigma_D$, item 1 gives $8Q = g^{-1}(\Gamma) = \sigma_D(\Gamma - \tau)$, i.e. $Q = \sigma_D(\Gamma-\tau)/8$, which is the image of $\Gamma/8$ under an isometry of $\mathbb{R}^n$. By Theorem A, item 3, Γ and Q are formally dual. [CKRS, Lemma 2.4] says that if P_1, Q_1 are formally dual and $\varphi \in GL_n(\mathbb{R})$, then $\varphi(P_1)$ and $(\varphi^{\mathsf{T}})^{-1}(Q_1)$ are formally dual. With $\varphi = I/(2\sqrt{2})$: $\varphi(\Gamma) = P$ and $(\varphi^{\mathsf{T}})^{-1}(Q) = 2\sqrt{2}\,Q = \sigma_D(\Gamma-\tau)/(2\sqrt{2}) = \sigma_D(P - \tau/(2\sqrt{2}))$. This is an isometric copy of P, so P is formally isodual in the sense of [CKS], which does not require the isometry to be proper. The determinant of σ_D is $(-1)^{\mathrm{wt}\,D}$; the isometry is improper when $n/2$ is odd (for instance $n = 18$ and 30), which the definition in [CKS] allows. □

5. Proof of the remark on formal self-duality

Let C be a binary $[2k,k]$ code, $R = C \cap C^\perp$, $\Gamma = \Gamma(C, C^\perp)$, $P = \Gamma/(2\sqrt{2})$, $n = 2k$. We prove: P is formally self-dual if and only if k is even and R is doubly even. Both directions are proved directly, without Theorem A, and the proof does not use $C \neq C^\perp$. We use (F1) to (F4) of § 3.0, the description of E and O by X_E and X_O below, and the transform of § 3.2 and § 3.5.

5.1 The criterion

The pair sums Σ_f of P are unchanged by a translation of P and by $P \mapsto -P$. So formally self-dual (formally dual to P itself) is equivalent to formally dual to a translate of P or of $-P$ [CKS]. By [CKRS, Cor. 2.7] with $Q = P$ and $\Lambda = 2\sqrt{2}\,\mathbb{Z}^n$ (a lattice of periods of P; $P - P \subseteq \Lambda^* = \mathbb{Z}^n/(2\sqrt{2})$ since $\Gamma - \Gamma \subseteq \mathbb{Z}^n$), P is formally self-dual iff for every $\ell \in \mathbb{Z}^n$, with $y = \ell/(2\sqrt{2})$,

$$\Big|N^{-1} \sum_{\gamma \in \Gamma_8} \zeta^{\langle \gamma, \ell \rangle}\Big|^2 = N^{-1} \#\{(\gamma, \gamma') \in \Gamma_8^2 : \ \gamma - \gamma' \equiv \ell \pmod 8\}, \qquad N = |\Gamma_8| = 2^{3k}.$$

Write $F(z) = \hat{S}_8(z) = \sum_{\gamma \in \Gamma_8} \zeta^{\langle \gamma, z \rangle}$ and $\nu_8(z) = \#\{(\gamma, \gamma') \in \Gamma_8^2 : \gamma - \gamma' \equiv z \pmod 8\}$ for $z \in (\mathbb{Z}/8)^n$. The criterion is

$$|F(z)|^2 = 2^{3k}\, \nu_8(z) \qquad \text{for every } z \in (\mathbb{Z}/8)^n. \tag{T}$$

By (F4), $\Gamma_8 = 2X_E \cup (\mathbf{1} + 2X_O)$ with $X_E = \{x \in (\mathbb{Z}/4)^n : \bar{x} \in \mathbf{1} + C,\ \Sigma x \equiv -\mathrm{wt}\,\bar{x}\}$ and $X_O = \{x : \bar{x} \in C^\perp,\ \Sigma x \equiv 2 - \mathrm{wt}\,\bar{x}\}$; each class $\bar{x}$ has 2^{n-1} lifts in X_E (resp. X_O).

5.2 Residues z with $\bar{z} \notin \{0, \mathbf{1}\}$

Here $F(z) = 0$ (Lemma 3.2). Also $\nu_8(z) = 0$: a difference of two points of the same half is even, and a difference of points of different halves has all coordinates odd. So (T) holds.

5.3 Even residues $z = 2y$, $y \in (\mathbb{Z}/4)^n$

Transform. By (3.2.1), $F(2y) = 2^{n-1+k}\big((-1)^{\mathrm{wt}\,\bar{y}}[\bar{y} \in C^\perp] + i^{\Sigma y}[\bar{y} \in C]\big)$, hence $|F(2y)|^2/2^{3k}$ equals

- $2^{3k}\,[\Sigma y \equiv 0 \ (4)]$ if $\bar{y} \in R$ (the words of R are even, so the bracket is $|1 + i^{\Sigma y}|^2$, and Σy is even);
- 2^{3k-2} if $\bar{y} \in (C \cup C^\perp) \setminus R$ (one term only);
- 0 otherwise.

Pair count. A difference $\equiv 2y$ comes from two points of the same half. For two points $2x, 2x'$ of $2X_E$ with $x = x' + y$ we need $\bar{x}' \in \mathbf{1} + C$ and $\bar{x}' + \bar{y} \in \mathbf{1} + C$, so $\bar{y} \in C$; and the sum condition $\Sigma x \equiv -\mathrm{wt}\,\bar{x}$, given $\Sigma x' \equiv -\mathrm{wt}\,\bar{x}'$, reads (by (F1)) $\Sigma y + \mathrm{wt}\,\bar{y} \equiv 2\,\bar{x}' \cdot \bar{y} \pmod 4$. Write $\bar{x}' = \mathbf{1} + p$, $p \in C$, so $\bar{x}' \cdot \bar{y} = \mathrm{wt}\,\bar{y} + p \cdot \bar{y}$.

- If $\bar{y} \in R$: $p \cdot \bar{y} = 0$ and $\mathrm{wt}\,\bar{y}$ is even, so the condition is $\Sigma y \equiv \mathrm{wt}\,\bar{y} \pmod 4$, independent of p. Each of the 2^k classes $\bar{x}'$ has 2^{n-1} lifts: 2^{3k-1} pairs in $2X_E$ when the condition holds.
- If $\bar{y} \in C \setminus R$: $p \mapsto p \cdot \bar{y}$ is a non-zero form on C ($\bar{y} \notin C^\perp$), and for each p the condition fixes the value of $p \cdot \bar{y}$ (the left side is even): 2^{k-1} classes, 2^{3k-2} pairs.

For two points of $\mathbf{1}+2X_O$ the same computation, with $\bar{x}' = a \in C^\perp$, requires $\bar{y} \in C^\perp$ and gives the same congruence; $a \cdot \bar{y} = 0$ if $\bar{y} \in R$, and the form $a \mapsto a \cdot \bar{y}$ is non-zero on $C^\perp$ if $\bar{y} \in C^\perp \setminus R$. Adding the two halves:

$$\nu_8(2y) = \begin{cases} 2^{3k}\,[\Sigma y \equiv \operatorname{wt}\bar{y}\ (4)] & \bar{y} \in R, \\ 2^{3k-2} & \bar{y} \in (C \cup C^\perp) \setminus R, \\ 0 & \text{otherwise.} \end{cases}$$

Comparison. (T) holds at every $2y$ with $\bar{y} \notin R$. For $\bar{y} \in R$ it requires $[\Sigma y \equiv 0] = [\Sigma y \equiv \operatorname{wt}\bar{y}]$ for $\Sigma y \in \{0, 2\}$, i.e. $\operatorname{wt}\bar{y} \equiv 0 \pmod 4$; both lifts occur for every $\bar{y} \in R$. So:

$$\text{(T) holds at all even } z \iff R \text{ is doubly even} \qquad (\text{for every } k). \tag{5.3.1}$$

5.4 Odd residues $z = \mathbf{1} + 2y$, and conclusion

Put $t = (\Sigma y - \operatorname{wt}\bar{y})/2 \bmod 2$, which equals $\operatorname{wt} y_1$ in the notation of § 3.0.

Transform. Formula (3.5.1) holds for every y. It gives $|F(\mathbf{1}+2y)|^2 = 2^{2n}\,|G_{C^\perp}(\bar{y})|^2\,[\,t \not\equiv k \pmod 2\,]$. By the first form of Lemma 3.3 (with $K = C^\perp$), $|G_{C^\perp}(w)|^2 = 2^k \sum_{d\in R} i^{-\operatorname{wt} d}(-1)^{d\cdot w}$. If R is doubly even this is $2^{k+h}[w \in R^\perp]$, so

$$|F(\mathbf{1}+2y)|^2 = 2^{5k+h}\,[\bar{y} \in R^\perp]\,[\,t \not\equiv k\,] \qquad (R \text{ doubly even}).$$

Pair count (any R). Only pairs with one point in each half contribute.

- Pairs $(\mathbf{1}+2x,\ 2x')$, $x \in X_O$, $x' \in X_E$: the difference is $\equiv \mathbf{1}+2y$ iff $x = x' + y$ in $(\mathbb{Z}/4)^n$. Put $b = \bar{x}' \in (\mathbf{1}+C) \cap (\bar{y} + C^\perp)$. This set is non-empty iff $\bar{y} \in \mathbf{1} + C + C^\perp = R^\perp$, and then it is a coset $b_0 + R$ (2^h words). By (F1) the sum conditions reduce to $t + \operatorname{wt}\bar{y} \equiv 1 + b\cdot\bar{y} \pmod 2$. On the coset $b\cdot\bar{y} = b_0\cdot\bar{y}$ (as $\bar{y} \in R^\perp$). Write $b_0 = \mathbf{1} + p = \bar{y} + a$ with $p \in C$, $a \in C^\perp$; then $b_0\cdot\bar{y} = \operatorname{wt} b_0 + (\mathbf{1}+p)\cdot a = \operatorname{wt} b_0 + \operatorname{wt} a \equiv \operatorname{wt}\bar{y}$. So the condition is $t \equiv 1$, and the count is $2^{n-1+h}[\bar{y} \in R^\perp][t \equiv 1]$.
- Pairs $(2x,\ \mathbf{1}+2x')$, $x \in X_E$, $x' \in X_O$: the difference is $\equiv \mathbf{1}+2y$ iff $x = x' + y + \tilde{\mathbf{1}}$. Put $a = \bar{x}' \in (\bar{y} + C) \cap C^\perp$, non-empty iff $\bar{y} \in R^\perp$, a coset of R. The sum conditions reduce to $1 + t \equiv \operatorname{wt} a + a\cdot\bar{y}$, and $a\cdot\bar{y} = a\cdot(a+p) = \operatorname{wt} a$ with $p = \bar{y} + a \in C$. So again $t \equiv 1$, with count $2^{n-1+h}[\bar{y} \in R^\perp][t \equiv 1]$.

Hence $\nu_8(\mathbf{1}+2y) = 2^{n+h}[\bar{y} \in R^\perp][t \equiv 1]$ and $2^{3k}\nu_8 = 2^{5k+h}[\bar{y} \in R^\perp][t \equiv 1]$.

Comparison. Let R be doubly even. Both $t = 0$ ($y = 0$) and $t = 1$ ($y = 2e_1$) occur with $\bar{y} = 0 \in R^\perp$. So (T) holds at all odd z iff $[t \not\equiv k] = [t \equiv 1]$ for both values of t, iff k is even:

$$\text{given } R \text{ doubly even, (T) holds at all odd } z \iff k \text{ even.} \tag{5.4.1}$$

Conclusion. ($\Leftarrow$) If k is even and R is doubly even, (T) holds at every z by § 5.2, (5.3.1) and (5.4.1), so P is formally self-dual. ($\Rightarrow$) Suppose P is formally self-dual; then (T) holds everywhere. If R were not doubly even, (5.3.1) fails; explicitly, take $h' \in R$ with $\operatorname{wt} h' \equiv 2 \pmod 4$ and $z = 2\tilde{h}'$: then $\Sigma y = \operatorname{wt} h' \equiv 2$, so $F(z) = 0$ while $\nu_8(z) = 2^{3k}$. So R is doubly even. If k were odd, (5.4.1) fails; explicitly, at $z = \mathbf{1}$ ($y = 0$, $t = 0 \not\equiv k$): $|F(\mathbf{1})|^2 = 2^{5k+h}$ while $\nu_8(\mathbf{1}) = 0$. So k is even, that is $4 \mid n$. □

Remark. For $C = C^\perp$ one has $R = C$, $h = k$ and $(C \cup C^\perp) \setminus R = \emptyset$; the proof above is unchanged.

6. Remark: formally self-dual graphs over $\mathbb{F}_{2^m}$ for $m = 5, 7, 9$, and computed instances for $m = 11, 13$

Status: reviewed, with 3 hostile reviews for the description of S and its formal self-duality, 2 for the graphs for $m = 5, 7, 9$ and 3 for the construction that turns S into these graphs, which for $m = 3$ (field $\mathbb{F}_8$) gives Gold's x^3 graph up to translation and an orthogonal map. The instances for $m = 11, 13$ are exact computations, not reviewed.

For a code with $\mathbf{1} \in R$, as for 18.1, 28.1 and 30.1, the group H' is $\mathbb{F}_2^{2r+2}$. For $r = 4, 6, 8$ ($m = r + 1 = 5, 7, 9$; $r = 8$ is the case of 18.1), S is, up to a group isomorphism and a translation, the graph of the quadratic map $(x, \alpha) \mapsto ((1 + \alpha)x,\, q(x))$ on $\mathbb{F}_2^r \times \mathbb{F}_2$, with q a non-degenerate quadratic form of Arf invariant 0, and it is primitive and formally self-dual in the finite-group sense of [KS]. For these three values, an $\mathbb{F}_2$-linear identification (a written construction) turns S into a set $\{(x, F(x)) : x \in \mathbb{F}_{2^m}\}$ with F a permutation, formally self-dual under the trace pairing $\langle (x, y), (a, b)\rangle = (-1)^{\mathrm{Tr}(ax+by)}$ of [KS, § 6]. The step from S to the tables of F (§ 6.1) rests on that construction and on the program that built them; the formal self-duality of these tables was checked by exact integer computation on every character by two programs. The same construction, run at $r = 10$ and $r = 12$ ($m = 11, 13$) on the graph of the quadratic map above, gives permutations of $\mathbb{F}_2^{11}$ and $\mathbb{F}_2^{13}$ whose graphs are formally self-dual, checked by exact integer computation on every character (2^{22} and 2^{26}): under the dot product by two programs written independently, each on the permutation it built, and, after transport to $\mathbb{F}_{2^{11}}$ and $\mathbb{F}_{2^{13}}$ through an orthonormal basis of the trace form, under the trace pairing by one of them. These permutations have algebraic degree 3 and are CCZ-equivalent to the quadratic map above (by construction: the identification is linear on the graph of the quadratic map). For $r = 2$, S is affinely equivalent to the example $\{(x, x^3) : x \in \mathbb{F}_8\}$ of [KS]. The sets for $m = 5, 7, 9$ are primitive and are not equivalent (in the sense of [LPS, Def. 2.17]) to the graph of a power map, to an affine graph, or to a non-trivial direct product. We point them out in connection with open question 3 of [KS], which asks for other formally self-dual sets of the form $\{(x, F(x))\}$.

6.1 Explicit tables for the remark of § 6

Explicit instance, $m = 5$, field $\mathbb{F}_{32} = \mathbb{F}_2[x]/(x^5 + x^2 + 1)$, elements written as integers $0, \ldots, 31$ in the polynomial basis:

$$F = [\,0, 13, 14, 3, 4, 26, 18, 7, 23, 24, 16, 31, 22, 1, 2, 30,\\ 17, 28, 6, 9, 21, 15, 27, 8, 25, 20, 5, 10, 29, 12, 19, 11\,].$$

For $m = 7$ and $m = 9$ the tables are available in coordinates where the trace pairing becomes the dot product, together with self-dual bases:

- $\mathbb{F}_{128} = \mathbb{F}_2[x]/(x^7 + x + 1)$ with basis $[3, 65, 71, 99, 111, 119, 127]$;
- $\mathbb{F}_{512} = \mathbb{F}_2[x]/(x^9 + x^4 + 1)$ with basis $[3, 17, 23, 27, 60, 263, 354, 424, 494]$

($\mathrm{Tr}(b_i b_j) = \delta_{ij}$ checked on all pairs). For $m = 9$ one review derived the trace-pairing statement from the dot-product check and the self-dual basis; another review computed the [KS] criterion after transport through a self-dual basis, for $m = 5, 7, 9$. For $m = 11$ and $m = 13$ the tables (not reviewed, see § 6) can be regenerated by the program in the fields $\mathbb{F}_2[x]/(x^{11} + x^2 + 1)$ and $\mathbb{F}_2[x]/(x^{13} + x^4 + x^3 + x + 1)$, with a self-dual basis for the trace form ($\mathrm{Tr}(b_i b_j) = \delta_{ij}$ checked); the program proves the irreducibility of both moduli.

7. Status

Labels: *paper-proof* (complete written proof), *reviewed* (paper proof plus hostile reviews by model instances that did not write it, see § 9; number given), *certified* (exact arithmetic, scope given), *numerical* (exact computation on a sample of cases, no general proof). The proofs, scripts and outputs behind each row are available on request.

The table gives one line per result. The list after it gives the sixteen claims behind it, each with what it does not establish; the row numbers in the table below refer to it.

Result	**Proof and reviews**	**Exact computer check (scope)**
Theorem A, items 1, 2, 4: finite pair, sizes, ν_T (row 1)	Paper proof (§ 3). Two hostile reviews, one re-deriving it from the statement alone; two GPT-6 Astra reviews.	$n = 18$: all 2^{18} characters; $n = 28, 30$: all 2^{26}; two independent programs. Small codes: exhaustive $n \leq 6$, 483 codes $n = 10$ to 16.
Theorem A, item 3: formal duality in $\mathbb{R}^n$, $Q = A^* + T/8$ (row 2)	Paper step via [CKRS, Cor. 2.7]. Two hostile reviews: one of the two above, and one on item 3 alone; the other review above took this step from them. Also the GPT-6 Astra reviews.	Not machine-checked.
Theorem A, item 5: primitivity (row 3)	One hostile review.	None claimed.
Proposition I (rows 7, 8)	Items 1, 2: three hostile reviews, then the repaired text re-read, found correct. Item 3: three reviews, conditional on Theorem A, item 3.	Items 1, 2: all codes $n \leq 4$, 21 permutation classes at $n = 6$, 4 507 instances $n = 2$ to 16.
Remark on formal self-duality (row 9)	Three hostile reviews; the third redid both directions without Theorem A.	Every $[n, n/2]$ code for $n \leq 8$; random and forced codes up to $n = 16$.
Entries 18.1, 28.1, 30.1 are $\Gamma(C, C^\perp)/\sqrt{8}$ up to signs and a translation; $d^2_{\min}(\Gamma) = 24, 32, 32$ (rows 10, 12)	Identification: computation only. $d^2_{\min}$: paper lemma for $\mathbf{1} \in R$ (§ 8.4). No review listed.	Two independent programs, all translates; d, d' enumerated. Coordinates of [RP]: 512 base points ($n = 18$), 4 ($n = 28$), 1 ($n = 30$).
Duals of the earlier note [EN] are isometric, at unit density, to the packings; stealth radius $\sqrt{3}, 2, 2$ (rows 11, 13)	Stealth radius: paper proof for formula (2), conditional on Theorem A, item 3, with [CCV, § 5.1]; for the duals of [EN], through row 11 (§ 8.3), or from its certificates (stated there, not proved here) and [CCV, § 5.1].	Two independent exact programs: signs and translation; point-set isometry on all 512 / 8192 / 8192 translates. Both read the T files of the earlier note the same way.
Graphs over $\mathbb{F}_{2^m}$ (§ 6; rows 14, 15)	Description of S: 3 hostile reviews; graphs for $m = 5, 7, 9$: 2; construction from S: 3. $m = 11, 13$: not reviewed.	Every character: $m = 5, 7, 9$ by two programs; $m = 11, 13$ (2^{22}, 2^{26}): dot product by two programs, trace pairing by one.

- **Row 1.** *Statement:* Theorem A, items 1, 2, 4 (finite pair, sizes, ν_T values). *Label and exact scope:* reviewed (2 hostile reviews, one of which re-derived the result from the statement alone; also the two GPT-6 Astra reviews, see § 9). Certified for $n = 18$ on all 2^{18} characters and $n = 28, 30$ on all 2^{26} by two independent programs on the codes of our earlier computations (first: Walsh transform and pair counting, direct sums on all characters at $n = 18$, on 4096 random characters at $n = 28, 30$; second: exact transform in $\mathbb{Z}[\zeta_8]$ on all characters), the

second also on the codes extracted from the entries of [RP]; exhaustive $n \le 6$ (1380 codes at $n = 6$); 483 codes $n = 10$–16; 78 random codes $k = 2..8$. *Not established:* no check of the proof by a person; among the two hostile reviews, § 3.6 (b), (c) and § 3.10 (ii) were redone by one only (and by the Astra review); pairs $C_2' \subsetneq C_2^\perp$; odd n; a necessary condition.

- **Row 2.** *Statement:* Theorem A, item 3 (formal duality in $\mathbb{R}^n$, $Q = A^* + T/8$). *Label and exact scope:* reviewed (2 hostile reviews: one of the two of row 1, and one on item 3 alone with items 1, 2, 4 admitted; the other review of row 1 took this step from them; also the GPT-6 Astra reviews, § 9); paper step via CKRS Cor. 2.7, not machine-checked. *Not established:* nothing identified.
- **Row 3.** *Statement:* Theorem A, item 5 (primitivity). *Label and exact scope:* reviewed (1 hostile review). *Not established:* nothing identified.
- **Row 4.** *Statement:* For $\mathbf{1} \in R$, r even ≥ 4: pair is no LPS / KS example and no direct product. *Label and exact scope:* reviewed (1 hostile review), in this restricted form. *Not established:* the list of [LPS] pairs in 2-groups that the argument uses (including their sporadic pair in $\mathbb{Z}_2 \times \mathbb{Z}_4^2$ and their computer lists for $|G| \le 63$) has not been reviewed since it was completed; the one review counted in the label found that list incomplete before it was completed; the infinite families that LPS attribute to other work (extending their sporadic example) were not read for this row; $\mathbf{1} \notin R$, $r \ge 2$ not compared with LPS.
- **Row 5.** *Statement:* $r = 1$: equivalent to TITO $\times$ TITO; $r = 2$, $\mathbf{1} \in R$: S, T each affinely equivalent to Gold in $\mathbb{F}_8^2$. *Label and exact scope:* $r = 1$: numerical, 20/20 codes, plus an explicit automorphism; $r = 2$: certified per instance, 12/12 and 18/18 codes. *Not established:* a common isomorphism for the pair at $r = 2$.
- **Row 6.** *Statement:* No Theorem A pair with $r \ge 2$ comes from a Li–Pott construction. *Label and exact scope:* paper-proof plus exact checks. *Not established:* product route for $\mathbf{1} \notin R$, $r \ge 4$ and $\mathbf{1} \in R$, r even ≥ 6.
- **Row 7.** *Statement:* Proposition I, items 1, 2. *Label and exact scope:* reviewed (3 hostile reviews; the text repaired after them was reviewed again). Certified for $n \le 6$ (all codes $n \le 4$, 21 permutation classes at $n = 6$); 4 507 instances $n = 2..16$. *Not established:* nothing identified.
- **Row 8.** *Statement:* Proposition I, item 3: $\Gamma/(2\sqrt{2})$ formally isodual. *Label and exact scope:* reviewed (3 hostile reviews, as row 7), conditional on Theorem A item 3. *Not established:* nothing identified (formal self-duality for 18, 28, 30: row 9).
- **Row 9.** *Statement:* Remark of § 2.4: P formally self-dual if and only if $4 \mid n$ and R doubly even; hence 18.1, 28.1, 30.1 not formally self-dual. *Label and exact scope:* reviewed (3 hostile reviews; *only if* without Theorem A; *if* through Theorem A item 3 and Proposition I in all three reviews, by a direct proof in the second and third; the third redid both directions without Theorem A, by an argument that does not use $C \ne C^\perp$). Certified by exact computation on every $[n, n/2]$ code for $n \le 8$ and on random and forced codes up to $n = 16$. *Not established:* for 18.1, 28.1, 30.1: the identification of the codes of row 10 (two programs, which give the same hull weights; set equality in the second rests on an L'-periodicity argument (item 1 of Theorem A states this) plus a sample).
- **Row 10.** *Statement:* Entries 18.1, 28.1, 30.1 equal $\Gamma(C, C^\perp)/\sqrt{8}$ after sign changes and a translation; hulls 1, 2, 3; $\mathbf{1} \in R$; $d = 6, 8, 8$. *Label and exact scope:* certified by two independent programs, all translates (first: lattice equality; second: membership of every translate and a density identity). *Not established:* in the second program, set equality rests on a short paper argument that Γ is L'-periodic (item 1 of Theorem A states this), tested on a sample of points; equivalence of the codes with Bierbrauer–Edel's printed codes (only equal weight enumerators).

- **Row 11.** *Statement:* The duals of the earlier note [EN] are, at unit density, isometric to the packings 18.1, 28.1, 30.1. *Label and exact scope:* certified by two independent exact programs (signs + translation in the code frame; point-set isometry in the coordinates of [RP], all 512 / 8192 / 8192 translates); the T files and the certificates of formal duality of [EN] are not part of this deposit. *Not established:* both read the T files of the earlier note the same way; that reading is validated by the identities (all characters in the first program; all at $n = 18$, 400 samples at $n = 28, 30$ in the second), not against the producing code; whether the T of the earlier note equals the formula T up to isometry.
- **Row 12.** *Statement:* $d^2_{\min}(\Gamma) = 24, 32, 32$; on the coordinates of [RP] at unit density $3, 4, 4$. *Label and exact scope:* paper-proof lemma (for $\mathbf{1} \in R$) plus exact enumeration of d, d' (one program, agrees with a second); on the coordinates of [RP]: all 512 base points at $n = 18$, four base points at $n = 28$, one at $n = 30$. *Not established:* exhaustive pair search at $n \geq 18$.
- **Row 13.** *Statement:* Stealth radius at unit density of the duals of the earlier note [EN] $= d_{\min}(\Gamma)/(2\sqrt{2}) = \sqrt{3}, 2, 2$. *Label and exact scope:* paper-proof: for the dual given by formula (2), conditional on Theorem A item 3, with CCV § 5.1; for the duals of the earlier note [EN], through the computer-certified isometry of Row 11 (§ 8.3), or from the certificates of formal duality in that note (stated there, not proved here) and CCV § 5.1. *Not established:* any optimality; comparison with non-lattice configurations other than those of Cohn's table of stealth radius records [ST].
- **Row 14.** *Statement:* Remark of § 6: graphs for $m = 5, 7, 9$ formally self-dual under the trace pairing; same for the computed instances $m = 11, 13$. *Label and exact scope:* certified on every character (1024, 16384, 262144) by two programs; reviewed (2 hostile reviews); the construction from S to the tables: reviewed (3 hostile reviews); tables built by one program. $m = 11, 13$: certified on every character (2^{22}, 2^{26}), dot product by two programs written independently (each on its own permutation), trace pairing by one program; not reviewed. *Not established:* the step from S to the tables beyond that construction and that program; for $m = 3$ the construction gives Gold's x^3 graph up to translation and an orthogonal map, hence no example beyond [KS] there; the general family is not claimed here (trace-pairing graphs for $r \geq 14$ not computed); for $m = 11, 13$, a second program for the trace pairing, and the comparisons of row 15; prior work: see § 10.2.
- **Row 15.** *Statement:* Remark of § 6: S for $r = 2$ affinely equivalent to KS's x^3 on $\mathbb{F}_8$; $m = 5, 7, 9$ sets not equivalent to power maps, affine graphs or products. *Label and exact scope:* certified (spectra, explicit equivalences) plus paper-proof (product exclusion); reviewed (2 hostile reviews). *Not established:* prior work: not found in the sources of § 10.2, which also lists the sources not reached.
- **Row 16.** *Statement:* Prior art for Theorem A and Proposition I: not found in the sources of § 10.2. *Label and exact scope:* search, not proof. *Not established:* absence in the literature; sources not read or not queried: § 10.2.

8. Computations, comparison with known pairs, and the configurations of the earlier note

8.1 What is computed

For $n = 18, 28, 30$ both identities of item 2 were checked on every character (2^{18}, 2^{26}, 2^{26}) by two independent programs on the codes of our earlier computations. The first uses a Walsh transform and pair counting, with direct character sums on every character at $n = 18$ and on 4096 random characters at $n = 28, 30$. The second uses an exact transform in $\mathbb{Z}[\zeta_8]$ on every character and

counts differences directly; it was also run on the codes extracted from the coordinates of [RP] (entries 18.1, 28.1, 30.1; hull dimensions 1, 2, 3; $d(C) = d(C^\perp) = 6, 8, 8$). Here $H' \cong \mathbb{F}_2^{18}, \mathbb{F}_2^{26}, \mathbb{F}_2^{26}$ and $|S| = |T| = 512, 8192, 8192$. The ν_T histograms are $\{0\colon 195587,\ 2\colon 65536,\ 128\colon 1020,\ 512\colon 1\}$ in dimension 18 and $\{0\colon 50315267,\ 2\colon 16777216,\ 2048\colon 16380,\ 8192\colon 1\}$ in dimensions 28 and 30, as item 4 predicts for $r = 8, 12, 12$. Negative controls fail as they should: with ε flipped, the first identity fails on half of the characters; with one element of T moved, the second identity fails at every non-zero group element. On small codes: an exhaustive exact search for $n = 2, 4, 6$ (all 1380 codes at $n = 6$), 483 codes for $n = 10$ to 16, and 78 random codes with $k = 2, \ldots, 8$, all passing. Item 3 is a paper step (CKRS Cor. 2.7) and was not machine-checked.

8.2 Position with respect to known finite pairs

For $\mathbf{1} \in R$ and r even ≥ 4, which covers 18.1, 28.1, 30.1 ($r = 8, 12, 12$), the finite pair is neither one of the examples of Li–Pott–Schüler [LPS] or Kölsch–Schüler [KS] nor a direct product of formally dual pairs: ν_T takes the value 2, while a product of non-trivial factors in elementary 2-groups only takes values ≥ 4 off 0. For $r = 1$ the finite pair is equivalent to a product of two TITO pairs [CKRS] (20 of 20 codes checked); for $r = 2$ with $\mathbf{1} \in R$, S and T are each affinely equivalent to the Gold graph $\{(x, x^3)\} \subset \mathbb{F}_8^2$ of [KS] (checked on samples). No pair with $r \geq 2$ comes from the Li–Pott constructions [LP1, LP2], whose groups have order 2^{4m+1} and whose pairs have $|T| = 2|S|$.

8.3 What it means for the configurations of the earlier note

The entries 18.1, 28.1 and 30.1 of [RP] are, after sign changes of coordinates and a translation, exactly $\Gamma(C, C^\perp)/\sqrt{8}$ for binary $[n, n/2]$ codes C with hull dimensions 1, 2, 3 and $\mathbf{1} \in R$ (exact check on all translates by two independent programs; in the second, equality of the sets, beyond the membership of every translate, rests on a short argument that Γ is periodic under the lattice L' of Theorem A (item 1 of Theorem A states this), tested on a sample of points). Proposition I therefore applies to them. Independently of that chain, we compared the dual configurations Q rebuilt from the files of T of the earlier note [EN], not part of this deposit and given there for the packings of [RP], by two independent exact programs: one finds a map of sign changes and a translation from the $8Q$ of the earlier note onto $\Gamma(C, C^\perp)$; the other, working on point sets in the Gram coordinates of [RP], finds an explicit isometry at scale factor 1 between the packing at unit density and the dual of the earlier note, and recovers the contact numbers 3264, 71400 and 59340 of [RP]. So, at unit density, the dual configurations of the earlier note are isometric copies of the record packings themselves, which are Bierbrauer–Edel packings $\Gamma(C, C^\perp)$. Both programs read the files of T of the earlier note the same way, and that reading is validated by the duality identities, not by comparison with the code that produced the files.

8.4 Minimal distances

For the three codes, $d^2_{\min}(\Gamma) = 24, 32, 32$: for $\mathbf{1} \in R$, $\min(4d, 4d', 32, n + 8) \leq d^2_{\min}(\Gamma) \leq \min(4d, 4d', 32)$, with $d = d' = 6, 8, 8$ and explicit pairs of points at these distances. On the coordinates of [RP] at unit density the minimal squared distances are $3, 4, 4$ (enumerated from all 512 base points in dimension 18, from four base points in dimension 28 and from one base point in dimension 30). The radii $\sqrt{3}$, 2, 2 of the earlier note [EN] are therefore the minimal distances of the packings at unit density, restated; the comparison with duals of lattices made there is a comparison of center densities. For the dual given by formula (2), this step depends on Theorem A, item 3, with [CCV, § 5.1]; for the duals of the earlier note [EN], it follows from the isometry

above, or from the certificates of formal duality in that note (stated there, not proved here) and [CCV, § 5.1].

Proof of the bounds. Here $d = d(C)$ and $d' = d(C^\perp)$ are the minimum weights, and $\mathbf{1} \in R$, so C and $C^\perp$ are even. Let $x \neq x'$ be points of Γ.

- *Both in E* ($x = -2\tilde{b} + 4\tilde{c} + 8\mathbb{Z}^n$, $x' = -2\tilde{b}' + 4\tilde{c}' + 8\mathbb{Z}^n$). If $b \neq b'$, then $b + b'$ is a non-zero word of C, so at least d coordinates of $x - x'$ are $\equiv 2 \pmod 4$, and $|x - x'|^2 \geq 4d$. If $b = b'$ and $c \neq c'$, then $c + c'$ is a non-zero word of even weight, so at least two coordinates are $\equiv 4 \pmod 8$, and $|x - x'|^2 \geq 2 \cdot 16 = 32$. If $b = b'$ and $c = c'$, then $x - x' \in 8\mathbb{Z}^n$ and $|x - x'|^2 \geq 64$.
- *Both in O:* the same argument with $C^\perp$ gives $|x - x'|^2 \geq \min(4d', 32)$.
- *One in each half:* all coordinates of $x - x'$ are odd, so $|x - x'|^2 \geq n$ and $|x - x'|^2 \equiv n \pmod 8$. Equality $|x - x'|^2 = n$ would need every coordinate $\equiv \pm 1 \pmod 8$. Write $x = \mathbf{1} - 2\tilde{a} + 4\tilde{c}$ ($a \in C^\perp$, $\operatorname{wt} c$ odd) and $x' = -2\tilde{b} + 4\tilde{c}'$ ($b \in \mathbf{1} + C$, $\operatorname{wt} c'$ even). Coordinate i of $x - x'$ is $\equiv 1 + 2(b_i - a_i) + 4(c_i - c'_i)$, and it is ± 1 iff $c_i + c'_i \equiv b_i(1 - a_i) \pmod 2$. Summing over i gives $\operatorname{wt}(c + c') \equiv \operatorname{wt} b - |a \cap b| \pmod 2$. The left side is odd. The right side is even: $\operatorname{wt} b = n - \operatorname{wt}(b + \mathbf{1})$ is even because $b + \mathbf{1} \in C$ is even, and $|a \cap b| \equiv a \cdot b = a \cdot \mathbf{1} + a \cdot (b + \mathbf{1}) = 0$. This is a contradiction, so $|x - x'|^2 \geq n + 8$.

Upper bounds: the points $-2 \cdot \mathbf{1}$ and $-2\widetilde{(\mathbf{1} + c_{\min})}$ of E ($c_{\min} \in C$ of weight d) differ by a vector of squared norm $4d$. The points $\mathbf{1} + 4e_1$ and $\mathbf{1} - 2\tilde{d}_{\min} + 4e_1$ of O ($d_{\min} \in C^\perp$ of weight d') differ by a vector of squared norm $4d'$. The points $-2 \cdot \mathbf{1}$ and $-2 \cdot \mathbf{1} + 4(e_1 + e_2)$ of E differ by a vector of squared norm 32. For $n = 18, 28, 30$: $\min(4d, 4d', 32, n + 8) = \min(4d, 4d', 32) = 24, 32, 32$.

8.5 Formal self-duality, as opposed to isoduality

If $4 \mid n$ and R is doubly even, $D = 0$ is admissible and P is formally self-dual. For the three record packings the condition fails: $n/2$ is odd for $n = 18$ and 30, and for $n = 28$ the hull is not doubly even (basis weights 14, 14). Since formal duals are not unique, this failure alone would not exclude formal self-duality; the *only if* direction of the remark of § 2.4 does.

8.6 Context: the densest packings and formal duality

Cohen, Cohn and Viazovska write: "We see no reason why the densest sphere packing should even have a formal dual" [CCV, § 1, line 96 of the source of arXiv:2609.03121v1].

The packings 18.1, 28.1 and 30.1 are the densest known in their dimensions; none is proved to be the densest. In Cohn's table of sphere packing density bounds, read on 17 November 2026 at `https://cohn.mit.edu/sphere-packing`, the best upper bound in dimensions 18, 28 and 30 exceeds their density by the factors 2.121, 4.507 and 10.91 printed there. Their formal isoduality therefore says nothing about the densest packing in these dimensions, which is unknown.

9. Tool and computational resource disclosure

The work for Theorem A, Proposition I and the remarks was done between 16 and 18 November 2026. Agents run in Claude Code did it. The Astra reviews were run through Codex. The codes and certificates of the earlier note predate this work.

Antoine Olivier read the statements of this note and redid the example of § 2.5 by hand; he did not check the proofs. The decision to pursue this family and the decision to submit it for deposit are Antoine Olivier's.

Search, computation, proofs, the reviews other than Astra's and Gemini's, and this draft were produced by AI agents (Anthropic Claude models, Opus-, Sonnet- and Fable-class). They asked him multiple-choice questions along the way.

On 18 November, Theorem A was also reviewed by GPT-6 Astra (OpenAI). The first review was an attack from the statement, without the proof. The statement given to it cited two earlier reviews; a second attack, from a copy of the statement without them, reached the same conclusions. The second review was line by line and had read the first. Both found the five items true. Item 4 was read as counting disjoint families, and item 1 half by half; the wording of items 1 and 4 above follows its corrections. Its other two reservations concerned the report of the second computer check of § 8.1. That report has since been repaired; the repair was re-read once by a Claude reviewer, not by Astra. The two reservations did not concern the proof.

On 18 November, before the last corrections of wording, Gemini 4 Carbon (Google), run through OpenRouter, read the whole note once from the PDF as a hostile referee. It judged Theorem A, Proposition I, the remark on formal self-duality and every lemma of §§ 3 and 8.4 correct, and found nothing fatal or serious. A Claude model checked its minor findings; the one that needed a change, a congruence mod 2 in § 8.4, is applied. Its report stops partway through its hand check of the tables of § 6.1.

The hostile reviews cited in the table were made by fresh model instances that did not write the proofs. They were not human referees. No human has checked the proofs yet.

The proofs in §§ 3 to 5 and the proof of the lemma in § 8.4 were rewritten from the proofs that these reviews read. This rewritten text has not itself been reviewed by a hostile reviewer; one model reviewer compared it with the reviewed proofs and redid the computations without a program. The remark at the end of § 3.13 (last line of Theorem A: r is even when $\mathbf{1} \in R$) was not reviewed.

All computations ran on a local PC in exact integer or rational arithmetic. The scripts and outputs are kept and available on request.

10. Limits

10.1 Two readings of Bierbrauer–Edel 2000

The definition of the packing on p. 97 of [BE] puts the cosets $\mathbf{1} + C_2$ in the even type and C_2' in the odd type; the table in the proof of Theorem 1, p. 98, uses the opposite assignment. The minimal-distance formula printed in Theorem 1 agrees with the p. 98 reading on every orthogonal pair we enumerated (all pairs of linear codes at $n = 5$ (5769) and $n = 6$ (95706), and 1920 sampled pairs for $n = 7$ to 10). For the p. 97 reading (all 102 069 orthogonal pairs with $n \leq 6$, and 1920 sampled pairs for $n = 7$ to 10), the term $\sqrt{n+8}$ is attained exactly when n is even and both codes are even, and is $\sqrt{n}$ otherwise; for $\Gamma(C, C^\perp)$ this condition is $\mathbf{1} \in R$. For the p. 97 reading this is also derived on paper. Non-linear codes, which [BE] allow, were not tested. Theorem A and Proposition I are stated for the p. 97 reading, formula (1). For $\mathbf{1} \in R$, which covers 18.1, 28.1 and 30.1, the two readings give the same packing up to translation and exchange of the codes (27 of 27 cases tested), and the entries of [RP] were matched directly to formula (1). For $\mathbf{1} \notin R$, Theorem A concerns the configuration (1), which may differ from the packing of the p. 98 reading.

10.2 Prior art

For Theorem A, three rounds of search (16 November 2026) in zbMATH Open, Crossref, OpenAlex and the arXiv API, plus web searches, found no source giving a formal dual of $\Gamma(C, C^\perp)$ or implying

one; Semantic Scholar was rate-limited. For Proposition I, three rounds (17 November 2026) in OpenAlex and Semantic Scholar (works citing [CKS], [CKRS], [BE] and [V99]), the arXiv API, zbMATH Open, web search and MathOverflow titles found no statement that the Bierbrauer–Edel or Vardy configurations built on $(C, C^\perp)$ are formally isodual or formally self-dual. The closest work in both searches is [CCV, § 5], which constructs a formal dual of Vardy's 20-dimensional packing, a different configuration with 16 translates against the packing's 4. Not read: the full text of [BE] beyond pp. 97–98, [V95] and [V99], [SPLAG], [CS94] in full; Google Scholar, MathSciNet and Crossref were not queried for Proposition I; the November 2026 preprint on dimensions 10–12 listed in Cohn's table of stealth radius records [ST] was not read. These are statements of the form not found in the sources listed, not of absence.

For the remark of § 6: full texts of the theses of Schüler and Kölsch extracted and searched by regular expressions (formulas not re-read on the page images; Kölsch's thesis only partly extracted, read by grep), and the works citing [KS] in OpenAlex, Semantic Scholar and OpenCitations (two; the second, a bibliography list, not read): not found in these sources; not reached: Google Scholar, the Springer page of [KS], the text of the 36 references of [KS], the WCC/SETA/BFA proceedings, the personal pages of Schüler, Li and Pott, possible Master's or habilitation theses (not searched). Literature after [KS] beyond these searches is not covered.

10.3 What this note does not claim

- That the packings in dimensions 18, 28, 30 are the densest in their dimensions: they are the densest known (§ 8.6).
- A change of the values in dimensions 18, 28 and 30 of Cohn's table of stealth radius records [ST]: for the dual given by the formula of Theorem A, by [CCV, § 5.1] and Theorem A, item 3; for the duals of the earlier note [EN], through § 8.3, or by its certificates of formal duality (stated there, not proved here) and [CCV, § 5.1]; in both cases the radii are the packings' minimal distances at unit density, and only their description changes.
- Optimality of any configuration, or a comparison with configurations that are not in Cohn's table of stealth radius records [ST].
- Anything for pairs $C_2' \subsetneq C_2^\perp$ or for odd n, beyond this: entries 27.1 and 29.1 have no formal dual (certified by exact computation: $|\hat{S}|^2$ is irrational on 2^{26} of the 2^{27} characters).
- For $\mathbf{1} \notin R$, that the configuration (1) is the packing of the p. 98 reading of [BE] (see § 10.1).

References

BE J. Bierbrauer, Y. Edel, Dense sphere packings from new codes, J. Algebraic Combin. 11 (2000) 95–100, doi:10.1023/A:1008733715001 (pp. 97–98 read).

CCV A. Cohen, H. Cohn, M. Viazovska, The stealthiest particle configurations in 8 and 24 dimensions, arXiv:2609.03121v1.

CKRS H. Cohn, A. Kumar, C. Reiher, A. Schürmann, Formal duality and generalizations of the Poisson summation formula, arXiv:1306.6796v2.

CKS H. Cohn, A. Kumar, A. Schürmann, Ground states and formal duality relations in the Gaussian core model, arXiv:0911.2169v2.

CS94 J. H. Conway, N. J. A. Sloane, On lattices equivalent to their duals, J. Number Theory 48 (1994) 373–382, doi:10.1006/jnth.1994.1073 (abstract only).

KS L. Kölsch, R. Schüler, Formal self duality, arXiv:2011.08486v3.

LPS S. Li, A. Pott, R. Schüler, Formal duality in finite abelian groups, arXiv:1804.06328v3.

LP1 S. Li, A. Pott, Constructions of primitive formally dual pairs having subsets with unequal sizes, arXiv:1810.05433v3.

LP2 S. Li, A. Pott, A direct construction of primitive formally dual pairs having subsets with unequal sizes, arXiv:1907.04208v2.

SPLAG J. H. Conway, N. J. A. Sloane, Sphere Packings, Lattices and Groups, 3rd ed., Springer, 1999, doi:10.1007/978-1-4757-6568-7 (not read).

V95 A. Vardy, A new sphere packing in 20 dimensions, Invent. Math. 121 (1995) 119–133, doi:10.1007/BF01884292 (not read).

V99 A. Vardy, Density doubling, double-circulants, and new sphere packings, Trans. Amer. Math. Soc. 351 (1999) 271–283, doi:10.1090/S0002-9947-99-02169-8 (not read).

RP H. Cohn, record packings data, `recordpackings.toml` (MIT DSpace hdl 1721.1/153311; MD5 a14f397db4b45ca65a5384ae3a462b31), entries 18.1, 28.1, 30.1, 27.1, 29.1.

ST H. Cohn, Stealth, MIT DSpace, `https://dspace.mit.edu/handle/1721.1/178306` (hdl 1721.1/178306). Table of lower and upper bounds for the largest stealth radius in dimensions 1 to 48 at unit density.

EN A. Olivier, Formal duals of the Bierbrauer–Edel and Vardy record packings in dimensions 18, 28 and 30, personal communication, 2026 (note dated 9 November 2026, not deposited; cited in this form in [ST]).