THE NSUCRYPTO 2019 CONJECTURE ON THE KASAMI APN FUNCTION: EXHAUSTIVE VERIFICATION FOR $n \le 18$, AN EQUIDISTRIBUTION OF CUBES AT EVEN n, AND THE WEIGHT DISTRIBUTIONS COMPUTED ALONG THE WAY

KOREA SUPERINTELLIGENCE LABS

Abstract. Let $\gcd(k,n)=1$, let $F(x)=x^{4^k-2^k+1}$ be the Kasami function on $\mathbb{F}_{2^n}$, and let $\Delta = \{F(b)+F(b+1)+1 : b \in \mathbb{F}_{2^n}\}$. A conjecture posed as an unsolved problem at NSUCRYPTO 2019, originating with Carlet, asserts that $\#\{(x,y,z)\in\Delta^3 : v_1x+v_2y+(v_1+v_2)z=0\} = 2^{2n-3}$ for every pair of distinct nonzero v_1, v_2. The conjecture is open; the largest published verified range is $n \le 13$. We verify it exhaustively at $n = 14, 15, 16, 17, 18$: for all 44 admissible pairs (n,k) in that range and for every one of the 2^n-2 values of $\rho = v_2/v_1$ — at $n=18$, all 262,142 of them for each of the six admissible k — covering $7.3\cdot 10^{11}$ ordered pairs (v_1,v_2) in total; together with the smaller cells this settles every admissible (n,k) with $n \le 18$ inside one machine-checked development. Part of the new range is confirmed a second time by counting the triples of Δ^3 directly, with no character sum anywhere. Three further findings come out of the same computation. First, in every even cell computed here the triples split evenly over the three cosets of the cubes: writing $s = v_1x+v_2y+(v_1+v_2)z$, each coset receives exactly $(2^{3n-3}-2^{2n-3})/3$ of the triples with $s\neq 0$, so the cubic multiplicative character sum over them vanishes. This is verified exhaustively at $n=4,6,8$ and at sampled ρ for $n=10,12$; it is the datum Carlet identifies as what the even case needs, and it is pinned at its mean in the same way the conjecture itself is. Second, the associated character spectrum is the weight distribution of a binary code of Ding, and it confirms Ding's own conjecture on that code at every odd cell computed, $m=15$ and $m=17$ included; at $m=18$, outside the conjecture's scope, the code is a fifteen-weight $[131072, 18, 64384]$ code. Third, writing $\max_{a\neq 0}|2S(a)| = 2^{(n+v)/2}$ for the character sum S of Δ, the value $v\in\{1,3\}$ holds at 46 of the 48 nondegenerate cells with n odd and $5\le n\le 17$ but fails at $(15,4)$ and $(15,11)$, where $v=7$; S is invariant under $a\mapsto a^2$, and that locates the exceptional value at $a=1$ in both places where this data is anomalous. What makes those cells exceptional is open. Every theorem is machine-checked in Lean 4; the computations that are not are labelled as such.

1. Introduction

Fix integers $n\ge 3$ and $k\ge 1$ with $\gcd(k,n)=1$, put

$$q=2^k, \qquad d=q^2-q+1=4^k-2^k+1, \qquad F(x)=x^d \ \text{ on } \ \mathbb{F}_{2^n},$$

so that F is the *Kasami function*, an almost perfect nonlinear (APN) function on $\mathbb{F}_{2^n}$ exactly when $\gcd(k,n)=1$. The exponent d goes back to Kasami [8], and the background [10] draws on — exceptional polynomials, permutation behaviour, cyclic difference sets — is that of Cohen and Matthews [4] and Dobbertin [6]. Set

$$\delta(b)=F(b)+F(b+1)+1, \qquad \Delta=\delta\big(\mathbb{F}_{2^n}\big)=\{\,\delta(b) : b\in\mathbb{F}_{2^n}\,\}. \tag{1}$$

The map δ is exactly 2-to-1 with fibres $\{b,b+1\}$, so $|\Delta|=2^{n-1}$ ([10, Lemma 3.3]). For $v_1,v_2\in\mathbb{F}_{2^n}$ write

$$N(v_1,v_2)=\#\big\{(x,y,z)\in\Delta^3 : v_1x+v_2y+(v_1+v_2)z=0\big\}. \tag{2}$$

Conjecture 1.1 (NSUCRYPTO 2019; Carlet)**.** $N(v_1,v_2)=2^{2n-3}$ for every pair of distinct nonzero $v_1,v_2\in\mathbb{F}_{2^n}$.

One $\mathbb{F}_2$-linear condition should cut the 2^{3n-3} triples of Δ^3 by a factor 2^n, so 2^{2n-3} is the count that perfect equidistribution predicts. It is also, unconditionally, the average of N over the admissible

pairs (Lemma 2.2). The conjecture therefore says that N is *constant*, pinned at its own mean. It is a statement of complete additive regularity for a set already known to be extremely regular multiplicatively: the set $\Delta \setminus \{0\}$ is a cyclic difference set with Singer parameters, a theorem of Dillon and Dobbertin quoted in [10, §14].

The conjecture originates in Carlet's study of componentwise Walsh uniformity [2], where the property is that of a *cyclic-additive difference set with Singer-like parameters* (Definition 4.12 in the ePrint version cited there); Carlet proves that componentwise Walsh uniformity of an APN power permutation is equivalent to such a property of Δ, records that Kasami functions are componentwise Walsh uniform for $n \leq 11$ and that "the cyclic-additive property is also true for $n \leq 10$ even", and leaves both as open problems. Both clauses are the *published* abstract's. The ePrint version's abstract states no range at all; the range its body records, after a Table 2 running $n = 3, \ldots, 11$ whose Kasami row is marked CWU at even $n = 8, 10$, is the first clause only — "all Kasami APN functions are CWU for $n \leq 11$, whatever is the parity of n". So the even-n figure $n \leq 10$ for the cyclic-additive property, used in §4 below, rests on the published abstract alone. The conjecture was then posed as a prize problem at the Sixth International Olympiad in Cryptography; the olympiad's report [11] states the conjecture in the form above, records that it was "presented in" [2] "for the first time and discussed in" [3], that "The conjecture was verified for small n (odd values $n \leq 11$, even values $n \leq 8$)", with no method given, and that two teams proved the case $k = 1$. The two accounts of the pre-2026 record therefore differ by one even value of n — Carlet's $n \leq 10$ against the olympiad's $n \leq 8$ — and neither states how the verification was carried out. The problem is still listed as unsolved on the olympiad's site [12].

The state of the art is the recent paper of Nagy and Vajda [10]. It proves the conjecture for $k \bmod n \in \{1, 2, n-2, n-1\}$, establishes a Frobenius transfer $k \leftrightarrow n-k$ and several exact character-sum reductions, and verifies the conjecture by computer for every admissible (n, k) with $n \leq 13$; its abstract and §13 both state that the general case remains open. Two features of that paper are relevant here and are stated as fact, not as comparison. Its numerics are, in its own words (§12), "implemented from first principles in pure Python (no external libraries)", and its coverage table stops at $n = 13$ with no reason given for the stopping point. Its abstract also states: "Every proof in this paper was obtained by the AI assistant Claude Fable 5 and has subsequently been formally verified in the Lean theorem prover by Aristotle (Harmonic)". The present paper takes the natural next step: it pushes the verified range five values of n further and machine-checks every claim.

What is settled here. Write a *cell* for a pair (n, k) with $1 \leq k \leq n-1$ and $\gcd(k, n) = 1$; there are $\varphi(n)$ of them at each n, since d depends only on $k \bmod n$ as an exponent on $\mathbb{F}_{2^n}^*$. Call a cell *degenerate* when $k \equiv \pm 1 \pmod{n}$, the cases already proved in [10].

(1) **The conjecture at** $n = 14, \ldots, 18$ (Theorems 3.1 and 4.1), for all $6 + 8 + 8 + 16 + 6 = 44$ admissible cells and, in each cell, for *every* one of the $2^n - 2$ values of $\rho = v_2/v_1$ — all 262,142 of them at $n = 18$. In total this covers 731,741,388,888 $\approx 7.3 \cdot 10^{11}$ ordered pairs (v_1, v_2). Each cell is an exhaustive search of size $\approx 2^{2n}$; nothing is sampled and no symmetry is used to skip a value of ρ or of k. Together with Propositions 3.2 and 3.4, every admissible cell with $n \leq 18$ is verified inside a single machine-checked development.

(2) **The same conclusion without characters** (Theorems 3.3 and 4.3), at sampled ρ throughout the new range, by counting the triples of Δ^3 from definition (2) directly. These statements do not pass through any published reduction. The corresponding cross-check in [10, §12] reached $n \leq 9$.

(3) **An equidistribution of cubes at even** n (§7). Carlet [2, §4.5] states that handling even n needs, beyond the count (2), the number of triples for which $v_1x + v_2y + (v_1 + v_2)z$ is a nonzero cube and the number for which it is not a cube. Those counts turn out to be constant in (v_1, v_2) as well, and equidistributed: each of the three cosets of the cubes receives exactly $(2^{3n-3} - 2^{2n-3})/3$ of the triples with $s \neq 0$ (Theorem 7.1), which is to say that the cubic multiplicative character sum over those triples vanishes — the multiplicative analogue of the

additive vanishing that *is* Conjecture 1.1. This is verified exhaustively at $n = 4, 6, 8$ and at sampled ρ for $n = 10, 12$, and fails, as it must, at odd n.

(4) **The weight distribution of a code of Ding** (§5). The set Δ is the defining set of a binary linear code $C_{D(f)}$ of [5], and the character spectrum of Δ is that code's weight distribution. Ding conjectured that $C_{D(f)}$ is a three- or five-weight code for odd m and $h \ge 2$, and stated no explicit verification range; the spectra computed here confirm it at every cell they cover, all sixteen cells at $m = 17$ included, and show that the even-m cells his conjecture does not cover are richer — nine weights at $(16, 7)$ and $(16, 9)$, and fifteen at $m = 18$, where $C_{D(f)}$ is a $[131072, 18, 64384]$ code (Proposition 4.4).

(5) **An outlier at $n = 15$, and the shape of the even-n regime** (§6). Write $\max_{a\neq 0} |2S(a)| = 2^{(n+v)/2}$ for the character sum S of Δ. For $k = 2$ and odd n, [10, Theorem 11.8] forces $v \in \{1, 3\}$. Across all 48 nondegenerate cells with n odd and $5 \le n \le 17$ — all of them machine-checked here — the value $v \in \{1, 3\}$ holds *except* at $(15, 4)$ and its Frobenius twin $(15, 11)$, where $v = 7$; and $n = 17$ returns to $v \in \{1, 3\}$ at every k. At even n the quantity v is frequently not defined at all. Since $S(a^2) = S(a)$ (Proposition 4.6), every level set of S is a union of cyclotomic cosets, and a level set of size one can only be $\{1\}$: both places where this data is anomalous — the value $2^{(n+7)/2}$ at $(15, 4)$ and the value $\max_{a\neq 0} |2S(a)| = 5 \cdot 2^{10}$ at $(18, 5)$ — are therefore attained at $a = 1$ and nowhere else. What distinguishes those cells is open (Question 6.2).

Nothing here bears on a proof of Conjecture 1.1 in general. The contribution is evidence and data: a verified range, a second independent route through part of it, the cube-refined counts that the origin paper asks for at even n, a table of spectra that answers a different published conjecture, and one anomaly that a proof of the general case will have to accommodate.

Provenance of the computations. Every theorem and proposition below is machine-checked in Lean 4 and is stated exactly as far as the machine check goes — in particular, the ranges of n, of k and of ρ in each statement are the ranges actually searched. The three lemmas are elementary and are proved here in the text, and the one corollary is read off the machine-checked tables through one of them. Where a computation was run only outside the formal development (in an auxiliary C program), it is labelled as such and appears as a remark, never as a theorem. §8 says precisely what each search consisted of and what it rests on, and §10 describes the verification.

2. Setup

2.1. **The field model.** All computations are carried out in the concrete model

$$\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f_n), \qquad \alpha = x \bmod f_n,$$

with f_n the lexicographically smallest irreducible binary polynomial of degree n — the convention of [10], kept so that the spectrum data below is directly comparable with its Table 2. An element $\sum_{j<n} c_j \alpha^j$ is stored as the n-bit mask $\sum_{j<n} c_j 2^j$, so that addition is bitwise exclusive-or; we identify field elements with these integers whenever an explicit element is named, so that, for instance, 2 denotes α, 3 denotes $\alpha + 1$ and $2^n - 1$ denotes $1 + \alpha + \cdots + \alpha^{n-1}$. Nothing below depends on f_n being the smallest irreducible polynomial: all fields of order 2^n are isomorphic and every quantity computed here is invariant under an isomorphism. That the model is a field, that a tabulated generator of $\mathbb{F}_{2^n}^*$ really generates, and that the trace is computed correctly are themselves machine-checked; see Proposition 8.2.

$\mathrm{Tr}\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ denotes the absolute trace $\mathrm{Tr}(x) = \sum_{i<n} x^{2^i}$.

2.2. **Two reductions, and the mean.** The first is trivial but is what lets a statement about pairs be checked as a statement about a single parameter.

Lemma 2.1. *$N(tv_1, tv_2) = N(v_1, v_2)$ for every $t \in \mathbb{F}_{2^n}^*$. Consequently, for distinct nonzero v_1, v_2 we have $N(v_1, v_2) = N(1, \rho)$ with $\rho = v_2/v_1$, and Conjecture 1.1 at a cell (n, k) is equivalent to*

$$N(1, \rho) = 2^{2n-3} \qquad \text{for all } \rho \in \mathbb{F}_{2^n} \setminus \{0, 1\},$$

which is $2^n - 2$ conditions.

Proof. The defining condition of (2) is $\mathbb{F}_{2^n}$-homogeneous in (v_1, v_2): $t\big(v_1x + v_2y + (v_1 + v_2)z\big) = (tv_1)x + (tv_2)y + (tv_1 + tv_2)z$, and for $t \neq 0$ one side vanishes iff the other does. Take $t = v_1^{-1}$. The pairs excluded by the conjecture, $v_1 = v_2$ and $v_2 = 0$, are exactly $\rho = 1$ and $\rho = 0$. □

The next observation is elementary and presumably folklore, but it is what makes Conjecture 1.1 a statement about constancy rather than about size: the conjectured value is forced as soon as one asks for N to be constant at all.

Lemma 2.2. *Let $\Delta \subseteq \mathbb{F}_{2^n}$ with $|\Delta| = 2^{n-1}$ be arbitrary. Then*

$$\frac{1}{(2^n - 1)(2^n - 2)} \sum_{\substack{v_1, v_2 \neq 0 \\ v_1 \neq v_2}} N(v_1, v_2) \;=\; 2^{2n-3}.$$

Proof. Exchange the order of summation. For a triple $(x, y, z) \in \Delta^3$ the condition $v_1x + v_2y + (v_1 + v_2)z = 0$ reads $v_1u + v_2w = 0$ with $u = x + z$, $w = y + z$. If $u = w = 0$ every one of the $(2^n - 1)(2^n - 2)$ admissible pairs qualifies, and there are $|\Delta|$ such triples. If exactly one of u, w vanishes, the equation forces $v_1 = 0$ or $v_2 = 0$ and no pair qualifies. If $u, w \neq 0$ then $v_1 = v_2w/u$, so each of the $2^n - 1$ choices of v_2 gives exactly one v_1, and it is admissible precisely when $w \neq u$. Hence the triples contributing are those with x, y, z pairwise distinct, of which there are $|\Delta|(|\Delta| - 1)(|\Delta| - 2)$. The total is therefore $|\Delta|(2^n - 1)(2^n - 2) + (2^n - 1)|\Delta|(|\Delta| - 1)(|\Delta| - 2)$, and dividing by $(2^n - 1)(2^n - 2) = 2(2^n - 1)(2^{n-1} - 1)$ with $|\Delta| = 2^{n-1}$ gives $2^{n-1} + 2^{n-2}(2^{n-1} - 2) = 2^{2n-3}$. □

The second reduction is the character identity of [10], which is also the identity its own numerics use. For $a \in \mathbb{F}_{2^n}$ put

$$S(a) = \sum_{t \in \Delta} (-1)^{\mathrm{Tr}(at)}, \tag{3}$$

so $S(0) = |\Delta|$, and for $\rho \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ put

$$Z(\rho) = \sum_{\lambda \in \mathbb{F}_{2^n}^*} S(\lambda)\, S(\lambda\rho)\, S\big(\lambda(1 + \rho)\big). \tag{4}$$

Proposition 2.3 ([10, Proposition 4.1], in the general form its proof gives)**.** *For any subset $\Delta \subseteq \mathbb{F}_{2^n}$ and any $\rho \in \mathbb{F}_{2^n} \setminus \{0, 1\}$,*

$$2^n\, N(1, \rho) = |\Delta|^3 + Z(\rho). \tag{5}$$

In particular, when $|\Delta| = 2^{n-1}$ this reads $N(1, \rho) = 2^{2n-3} + 2^{-n} Z(\rho)$, so Conjecture 1.1 at the cell (n, k) is equivalent to $Z \equiv 0$ on $\mathbb{F}_{2^n} \setminus \{0, 1\}$.

In [10, Proposition 4.1] the identity is stated in the second form, for the Kasami set Δ, where $|\Delta| = 2^{n-1}$; the first form is what the same proof produces before that substitution, and it is the one used below. Identity (5) is the orthogonality of additive characters: expanding the product of three sums and summing over all $\lambda \in \mathbb{F}_{2^n}$ (including $\lambda = 0$, whose term is $|\Delta|^3$) leaves 2^n times the number of triples with $x + \rho y + (1 + \rho)z = 0$. We do not reprove it; it is used as a published result, and §8.3 records exactly what that dependence costs and how it was tested.

Two elementary identities are used repeatedly as global consistency checks on a computed spectrum. Summing (3) over all a and exchanging the order of summation gives $\sum_{a \in \mathbb{F}_{2^n}} S(a) = 2^n \cdot [\, 0 \in \Delta \,]$, and expanding $S(a)^2$ likewise gives $\sum_{a \in \mathbb{F}_{2^n}} S(a)^2 = 2^n |\Delta|$. Hence, when $0 \in \Delta$ and $|\Delta| = 2^{n-1}$,

$$\sum_{a \neq 0} S(a) = 2^{n-1}, \qquad \sum_{a \neq 0} S(a)^2 = 2^{2n-2}, \tag{6}$$

the two sanity sums that [10, §12.2] states as satisfied by every row of its Table 2. Both are reported alongside every spectrum computed below.

3. The conjecture at $n = 14, \dots, 17$

Theorem 3.1. *Let $n \in \{14, 15, 16, 17\}$ and let k satisfy $1 \le k \le n-1$ and $\gcd(k, n) = 1$. Then*

$$N(v_1, v_2) = 2^{2n-3}$$

for every pair of distinct nonzero $v_1, v_2 \in \mathbb{F}_{2^n}$. Explicitly, the admissible k are $\{1, 3, 5, 9, 11, 13\}$ at $n = 14$, $\{1, 2, 4, 7, 8, 11, 13, 14\}$ at $n = 15$, $\{1, 3, 5, 7, 9, 11, 13, 15\}$ at $n = 16$ and all of $1, \dots, 16$ at $n = 17$; and the constant is $2^{25}, 2^{27}, 2^{29}, 2^{31}$ respectively.

Proof, and the search it consisted of. By Lemma 2.1 the assertion at a cell (n, k) is the $2^n - 2$ statements $N(1, \rho) = 2^{2n-3}$, and by the second form of Proposition 2.3 — available because $|\Delta| = 2^{n-1}$, which is [10, Lemma 3.3] and is also part of the machine-checked data of Proposition 5.3 — each of them is the single equation $Z(\rho) = 0$ with Z as in (4). For each of the 38 cells the array $\big(S(a)\big)_{a \in \mathbb{F}_{2^n}}$ was computed from definition (3), and then $Z(\rho)$ was evaluated and compared with 0 for *every* $\rho \in \mathbb{F}_{2^n} \setminus \{0, 1\}$. This is an exhaustive computation of $\sum_{n,k}(2^n - 2)(2^n - 1)$ triple products, one cell at a time; no value of ρ was sampled or skipped, and no cell was derived from another by the Frobenius transfer of [10, Lemma 3.5] or by the settled cases $k \equiv \pm 1$. The whole of the theorem rests on exhaustive computation, together with Lemma 2.1 and Proposition 2.3. §8 describes how the sum was evaluated, why the evaluated sum is the sum (4) written above (Proposition 8.1), and what was done to make the dependence on Proposition 2.3 testable. □

Table 1. The new range. "Cells" is the number $\varphi(n)$ of admissible k at this n; "ρ per cell" is $2^n - 2$; "pairs per cell" is $(2^n - 1)(2^n - 2)$, the ordered pairs (v_1, v_2) a single cell (n, k) covers; the last column is the measured cost of the exhaustive check of one cell (user CPU seconds on one core; at $n = 17$ and $n = 18$, for a nondegenerate k). The $n = 18$ row is Theorem 4.1; its cells were run as two half-ranges each (§4.1), at about 650 seconds per half.

n	cells	ρ per cell	pairs per cell	cost per cell
14	6	16,382	268,386,306	4.0 s
15	8	32,766	1,073,643,522	20.9 s
16	8	65,534	4,294,770,690	53.9 s
17	16	131,070	17,179,475,970	370 s
18	6	262,142	68,718,690,306	2×650 s

The point of comparison one value of n below is the last row of [10, Table 1]. It is worth recording separately, because it is the calibration of the whole pipeline: the same code, the same statement, at an n where the answer is already published.

Proposition 3.2 (the published range, recomputed)**.** *Conjecture 1.1 holds at $n = 13$ for all twelve admissible k and every $\rho \in \mathbb{F}_{2^{13}} \setminus \{0, 1\}$, i.e. for all 8190 values of ρ in each cell.*

The mathematics of Proposition 3.2 is that of [10, Table 1] and is not new; only the verification is. It is slightly wider than the coverage stated there, which runs $k = 2, 3, 4, 5, 6$ exhaustively and obtains $k = 7, \dots, 11$ from the Frobenius transfer [10, Lemma 3.5] and $k = 1, 12$ from [10, Theorem 7.1]: here all twelve cells are swept, so the statement depends on neither result.

3.1. **The same conclusion without characters.** Theorem 3.1 passes through Proposition 2.3, a published identity that this work does not reprove. The following statements do not: they count the triples of Δ^3 from definition (2), with no character sum anywhere. A single ρ costs $|\Delta|^2 = 2^{2n-2}$ steps — z is determined by (x, y), since $v_1 + v_2 \neq 0$ — so individual values of ρ stay affordable well past the point where sweeping all of them does not.

Theorem 3.3. *Counting the triples of Δ^3 directly from (2), $N(1, \rho) = 2^{2n-3}$ in each of the following instances, where field elements are named by the bit-mask convention of §2.1:*

- *$n = 14$, every admissible k, and $\rho \in \{\alpha,\ \alpha+1,\ \alpha^2+1,\ \alpha^2+\alpha+1,\ \alpha^3+\alpha+1,\ \alpha^3+\alpha^2+1,\ \alpha^{13},\ \sum_{j<14}\alpha^j\}$;*
- *$n = 15$, every admissible k, and $\rho \in \{\alpha,\ \alpha+1,\ \alpha^2+1,\ \alpha^2+\alpha+1,\ \alpha^{14},\ \sum_{j<15}\alpha^j\}$;*
- *$n = 16$, every admissible k, and $\rho \in \{\alpha,\ \alpha+1,\ \alpha^{15},\ \sum_{j<16}\alpha^j\}$;*
- *$n = 17$, $k \in \{3, 5\}$, and $\rho \in \{\alpha,\ \alpha+1,\ \alpha^{16},\ \sum_{j<17}\alpha^j\}$.*

These are the only statements about $n = 14, \ldots, 17$ that are independent of Proposition 2.3; they are also independent of the arithmetic of characters altogether. The cross-check of the same kind reported in [10, §12] covers $n \leq 9$.

Exhausting ρ this way costs 2^{3n-3} and stops earlier. For completeness we record how far the character-free route reaches exhaustively; the conclusion there is inside the published range and is not new, but the route is stronger than any published one at those n.

Proposition 3.4. *Counting the triples of Δ^3 directly from (2), $N(1, \rho) = 2^{2n-3}$ for every $\rho \in \mathbb{F}_{2^n} \setminus \{0, 1\}$, every admissible k, and every n with $3 \leq n \leq 12$; and, for all twelve admissible k at $n = 13$, at the eight sampled ρ $\{\alpha,\ \alpha+1,\ \alpha^2+1,\ \alpha^2+\alpha+1,\ \alpha^3+\alpha+1,\ \alpha^3+\alpha^2+1,\ \alpha^{12},\ \sum_{j<13}\alpha^j\}$.*

At $n = 12$ this is exhaustive in all four admissible cells; [10, Table 1] records $n = 12$ as exhaustive for $k = 5$ only, with $k = 7$ obtained from [10, Lemma 3.5], $k = 1, 11$ from [10, Theorem 7.1] and 400 sampled ρ in addition.

4. The cell $n = 18$

At $n = 18$ there are $\varphi(18) = 6$ admissible k, and a single cell is a sweep over 262,142 values of ρ, each a sum of $2^{18} - 1$ triple products: about four times the work of a cell at $n = 17$. It is also the largest even n reached anywhere: even n is the case [10, §14(d)] sets apart — the closed form for S of its §10 is odd-n only, and it records that "the mechanisms available at even n differ" — and the even values recorded in the literature are $n \in \{4, 6, 8, 10, 12\}$ there, $n \leq 10$ in [2] and $n \leq 8$ in [11].

Theorem 4.1. *Let $k \in \{1, 5, 7, 11, 13, 17\}$, the admissible residues at $n = 18$. Then*

$$N(v_1, v_2) = 2^{33}$$

for every pair of distinct nonzero $v_1, v_2 \in \mathbb{F}_{2^{18}}$; equivalently, $Z(\rho) = 0$ for every one of the 262,142 values of $\rho \in \mathbb{F}_{2^{18}} \setminus \{0, 1\}$, in each of the six cells.

Proof, and the search it consisted of. As for Theorem 3.1: Lemma 2.1 reduces the pair statement to the ρ statement, Proposition 2.3 together with $|\Delta| = 2^{17}$ (Proposition 4.4) turns each instance into $Z(\rho) = 0$, and Z was evaluated and compared with 0 at every ρ, cell by cell, from the array $\big(S(a)\big)_a$ computed from definition (3). Nothing is sampled, and neither the Frobenius transfer $k \leftrightarrow 18 - k$ (which would collapse $\{5, 13\}$ and $\{7, 11\}$) nor [10, Theorem 7.1] (which settles $k = 1, 17$) is used to omit a cell. The only structural difference from Theorem 3.1 is bookkeeping: each of the four nondegenerate cells was run as two consecutive half-ranges of 131,071 values of ρ, and Proposition 4.2 is what turns the pair of half-range facts back into the statement about the whole range. □

4.1. **Splitting a sweep, proved rather than assumed.** The development caps the running time of any one source file at thirty minutes, and a nondegenerate cell at $n = 18$ is close enough to that bound that the sweeps were cut in two. A cut is only honest if the pieces provably reassemble. Write $W(l, c)$ for the assertion, as the program evaluates it, that $Z(\rho) = 0$ at the c consecutive values $\rho = l, l+1, \dots, l+c-1$ of the mask encoding of §2.1, so that the full sweep at a cell is $W(2,\, 2^n - 2)$.

Proposition 4.2. *For all c_1, c_2 with $c_1 + c_2 = 2^n - 2$,*

$$W(2,\, 2^n - 2) \;=\; W(2, c_1) \;\wedge\; W(2 + c_1,\, c_2),$$

at every n and k. More generally the evaluation loop is additive in its length: running $a + b$ steps from ρ is running a steps from ρ followed by b steps from $\rho + a$.

The general form is proved by induction on a, with no appeal to evaluation and no finite data; its axiom footprint is the two propositional axioms of the proof kernel, without the axiom of choice. The hypothesis $c_1 + c_2 = 2^n - 2$ is doing real work rather than decorating the statement, and the negative controls of Proposition 8.6(e) say so: a single chunk can hold where the whole sweep fails, and the misaligned pair $131071 + 131070$ does not satisfy the hypothesis at $n = 18$. At $n = 18$ the split used is $131071 + 131071 = 2^{18} - 2$.

4.2. **The same conclusion without characters, at $n = 18$.**

Theorem 4.3. *Counting the triples of Δ^3 directly from* (2)*, with no character sum anywhere, $N(1, \rho) = 2^{33}$ at $n = 18$ for*

$$k = 5,\ \rho \in \{\alpha,\ \textstyle\sum_{j<18} \alpha^j\}, \qquad k = 7,\ \rho \in \{\alpha + 1,\ \alpha^{17}\}.$$

Each of these four counts is a loop of $|\Delta|^2 = 2^{34}$ steps, about six minutes apiece here; that cost is why they are sampled. They are the part of the $n = 18$ evidence that rests on nothing unformalised, Proposition 2.3 included.

4.3. **The spectrum at $n = 18$, and a fifteen-weight code.**

Proposition 4.4. *At $n = 18$ and every admissible k one has $|\Delta| = 2^{17}$ and both sums* (6)*. The two degenerate cells $k = 1, 17$ have $|\operatorname{supp} S \setminus \{0\}| = 1$ and histogram $\{0 : 262142,\ 131072 : 1\}$. The four nondegenerate cells $k = 5, 7, 11, 13$ have* the same *spectrum, with $|\operatorname{supp} S \setminus \{0\}| = 68139$ and histogram*

S	-2560	-1536	-1280	-1024	-768	-512	-256	0
#	1	18	144	1206	5130	10539	17028	194004

S	256	512	768	1024	1280	1536	2304
#	16920	10611	5016	1341	108	39	38

Three features of this cell have no counterpart at smaller n. *(i)* Every value is a multiple of $256 = 2^{(n-2)/2}$, and as multiples of 256 the value set is $\{-10\} \cup \{-6, \dots, 6\} \cup \{9\}$: the extreme negative value is attained exactly once, the extreme positive value $9 \cdot 256$ thirty-eight times, and there are gaps at ± 7, ± 8, -9 and 10. *(ii)* All four nondegenerate cells agree. The Frobenius transfer [10, Lemma 3.5] forces $5 \leftrightarrow 13$ and $7 \leftrightarrow 11$ but says nothing about the two classes coinciding, and at $n = 16$ the analogous classes $\{3, 5, 11, 13\}$ and $\{7, 9\}$ do *not* coincide (Table 2). *(iii)* $\max_{a \neq 0} |2S(a)| = 5120 = 5 \cdot 2^{10}$ is not a power of two, so the exponent v of §6 is not defined here at all.

Corollary 4.5. *Through the dictionary of Lemma 5.1, the code $C_{D(f)}$ of* [5] *at $m = 18$ and $h \in \{5, 7, 11, 13\}$ is a fifteen-weight* $[131072, 18, 64384]$ *binary code: its nonzero weights are the fifteen numbers $(2^{17} - s)/2$ for s running over the values listed in Proposition 4.4, with the same multiplicities, so they run from* 64384 *(of multiplicity* 38*) up to* 66816 *(of multiplicity* 1*). At $h \in \{1, 17\}$ it is the one-weight* $[131072, 17, 65536]$ *code.*

Proof. Apply Lemma 5.1 with $|\Delta| = 2^{17}$: the weight at x is $(2^{17} - S(x))/2$. No $a \neq 0$ has $S(a) = 2^{17}$ in the nondegenerate cells, so the kernel is trivial and the dimension is 18; the minimum distance is $(131072 - 2304)/2 = 64384$. In the degenerate cells the kernel has order 2 and the single nonzero weight is 2^{16}. □

Ding's Conjecture 5.2 covers odd m only, so $m = 18$ lies outside its scope; what Corollary 4.5 supplies is the weight distribution in the case the conjecture does not reach, and the fifteen values are a measure of how far the even case departs from the three or five it predicts for odd m.

4.4. **Frobenius invariance, and where the extreme values sit.** The multiplicity column of every spectrum table in this paper is constrained by one identity.

Proposition 4.6. *For every admissible cell with $5 \le n \le 16$, and additionally for all six cells at $n = 18$: the set Δ is closed under $t \mapsto t^2$. For every admissible cell with $5 \le n \le 16$, and additionally at $(18, 5)$: $S(a^2) = S(a)$ for every $a \in \mathbb{F}_{2^n}$. Moreover $S(1) = 1024$ at $(15, 4)$ and $S(1) = -2560$ at $(18, 5)$, and in each case no other $a \neq 0$ attains that value.*

Both halves are elementary: $x \mapsto x^2$ is additive and fixes 1, so $\delta(b^2) = \delta(b)^2$ and Δ is closed under squaring; reindexing $t \mapsto t^2$ in (3) and using $\mathrm{Tr}(a^2t^2) = \mathrm{Tr}\big((at)^2\big) = \mathrm{Tr}(at)$ gives $S(a^2) = S(a)$. They are nevertheless checked from the concrete model at every affordable cell rather than argued, since everything else in this paper is. The consequence is what makes the proposition worth stating: *every level set of S is a union of cyclotomic cosets $\{a, a^2, a^4, \dots\}$, whose sizes divide n*, so multiplicities are constrained — $30 = 2 \cdot 15$ at $(15, 4)$, and $38 = 2 + 18 + 18$ and $39 = 3 + 9 + 9 + 18$ at $(18, 5)$, these three decompositions into coset sizes being computed outside the formal development — and, in the sharp case, a level set of size 1 can only be $\{1\}$, because a coset of size 1 forces $a^2 = a$. The last sentence of the proposition is the instance that matters: both places where the data of this paper is anomalous have their exceptional value at $a = 1$. Two controls are recorded: the invariance is specific to squaring ($S(a^3) \neq S(a)$ at $(9, 2)$, $(11, 3)$, $(13, 2)$), and the lone-extreme test rejects a value of multiplicity greater than one (512, of multiplicity 30 at $(15, 4)$) and a value $S(1)$ does not take.

Remark 4.7. Two honest limits. Deleting $a = 1$ does not dissolve either anomaly: at $(15, 4)$ it leaves $\max_{a \neq 0,1} |S(a)| = 512$, hence $v = 5$, still outside $\{1, 3\}$; at $(18, 5)$ it leaves 2304, still not a power of two. And a lone extreme at $a = 1$ is not by itself a sign of anomaly — at $(9, 2)$ the value -32 is attained only at $a = 1$, yet that cell has $v = 3$ and is entirely ordinary.

5. The spectra, and a conjecture of Ding

5.1. **Δ as a defining set.** Ding [5] constructs binary linear codes from a defining set $D = \{d_1, \dots, d_N\}$ inside $\mathbb{F}_{2^m}$ by the rule

$$C_D = \big\{c(x) : x \in \mathbb{F}_{2^m}\big\}, \qquad c(x) = \big(\mathrm{Tr}(xd_1), \dots, \mathrm{Tr}(xd_N)\big),$$

and studies in particular $D(f) = \{f(x) : x \in \mathbb{F}_{2^m}\}$ for $f(x) = F(x) + F(x + 1) + 1$. For the Kasami monomial that defining set *is* the set Δ of (1), with $m = n$ and $h = k$. The dictionary between the two objects is immediate.

Lemma 5.1. *Let $\Delta \subseteq \mathbb{F}_{2^m}$ and let C_D be as above with $D = \Delta$. For every x the Hamming weight of $c(x)$ is $\big(|\Delta| - S(x)\big)/2$, and $x \mapsto c(x)$ is $\mathbb{F}_2$-linear with kernel $K = \{x : S(x) = |\Delta|\}$. Hence C_D has length $|\Delta|$ and dimension $m - \dim_{\mathbb{F}_2} K$, and its nonzero weights are exactly the numbers $(|\Delta| - s)/2$ for s a value taken by S on $\mathbb{F}_{2^m} \setminus K$. In particular, if $K = \{0\}$ then the number of nonzero weights of C_D is the number of distinct values taken by S on $a \neq 0$.*

Proof. $S(x) = \#\{t : \mathrm{Tr}(xt) = 0\} - \#\{t : \mathrm{Tr}(xt) = 1\} = |\Delta| - 2\,\mathrm{wt}(c(x))$, which is the weight formula, and $c(x) = 0$ iff $\mathrm{Tr}(xt) = 0$ for all $t \in \Delta$ iff $S(x) = |\Delta|$. Linearity of $x \mapsto c(x)$ is linearity of the trace. □

So the value histogram of S on $a \neq 0$ *is* the weight distribution of $C_{D(f)}$, and a table of spectra answers questions about that code directly. [5] states the following.

Conjecture 5.2 ([5, Conjecture 34], verbatim)**.** Let $F(x) = x^{2^{2h}-2^h+1}$, and let $\gcd(h, m) = 1$. It is known that F is both APN and AB. When $h = 1$, $C_{D(f)}$ is a $[2^{m-1}, m - 1, 2^{m-2}]$ one-weight code. When $h \ge 2$ and m is odd, $C_{D(f)}$ is a three-weight or five-weight code with length 2^{m-1} and

dimension m. In particular, when $h = 3$ and m is odd, $C_{D(f)}$ is a three-weight code with length 2^{m-1} and dimension m for every odd $m \ge 5$ and $m \not\equiv 0 \pmod 3$. …

No verification range is stated for it in [5]: its concluding remarks record only that "All the conjectures on difference sets, o-polynomials and the corresponding binary codes were confirmed for sufficiently many integers m by Magma." Nor does the conjecture appear to have been settled since. Göloğlu and Krasnayová [7] prove, in their abstract's words, "four of these conjectures (Conjectures 38–41)" — not this one; Ahmadi and Shafaeiabr [1] prove another (Ding's Conjecture 36) and resolve his Conjecture 37 for nine of the eleven trinomials it concerns, closing with the remark that "in order to prove the claim of Conjecture 37 … it suffices to prove Conjecture 34 of" [5] — that is, they use Conjecture 5.2 as an unproved hypothesis for the two trinomials they do not settle. That sentence, and their use of the numbers 36 and 37, are read from arXiv:2108.10042v1, whose published version differs from it at least in title and reference list and was not accessible here; the numbers are in any case explicitly attributed there to the published [5]. Finally, [10] does not cite [5]: the two conjectures appear to have been posed independently about the same set.

5.2. **The spectra past the published table.**

Proposition 5.3. *For $n = 14, 15, 16, 17$ and* every *admissible k, one has $|\Delta| = 2^{n-1}$, both sums* (6) *hold, and the support size $|\operatorname{supp} S \setminus \{0\}|$ and the complete value histogram of S on $a \neq 0$ are as listed in Table 2. The same computation fills in every admissible cell with n odd and $5 \le n \le 13$ that* [10, Table 2] *does not print.*

TABLE 2. The spectrum of S past the last row of [10, Table 2]. Cells sharing a row have identical spectra. Every row satisfies $|\Delta| = 2^{n-1}$, $\sum_{a\neq 0} S(a) = 2^{n-1}$ and $\sum_{a\neq 0} S(a)^2 = 2^{2n-2}$. The $n = 18$ row is Proposition 4.4.

n	k	$\lvert\operatorname{supp} S \setminus \{0\}\rvert$	histogram of S on $a \neq 0$
14	$1, 13$	1	{0:16382, 8192:1}
14	$3, 5, 9, 11$	3088	{−256:168, −128:1344, 0:13295, 128:1408, 256:168}
15	$1, 14$	1	{0:32766, 16384:1}
15	$2, 7, 8, 13$	14296	{−256:316, −128:6800, 0:18471, 128:6800, 256:380}
15	$4, 11$	15871	{−128:7920, 0:16896, 128:7920, 512:30, 1024:1}
16	$1, 15$	1	{0:65534, 32768:1}
16	$3, 5, 11, 13$	12352	{−512:640, −256:5504, 0:53183, 256:5504, 512:704}
16	$7, 9$	17928	{−384:800, −256:3568, −128:5536, 0:47607, 128:3584, 256:2768, 384:640, 512:952, 768:80}
17	$1, 16$	1	{0:131070, 65536:1}
17	$2, 5, 7, 8, 9, 10, 12, 15$	57274	{−512:1377, −256:27132, 0:73797, 256:27388, 512:1377}
17	$3, 6, 11, 14$	65536	{−256:32640, 0:65535, 256:32896}
17	$4, 13$	56662	{−512:1479, −256:26724, 0:74409, 256:26980, 512:1479}

Three shapes in Table 2 are worth naming. The rows $(17, k)$ for $k = 3, 6, 11, 14$ continue the "plateaued" class of [10, Table 2]: values $\{0, \pm 2^{(n-1)/2}\}$ and support of size exactly 2^{n-1}, as at $(11, 3)$ and $(13, 3)$. The row $(17, 4)$, $(17, 13)$ is a fourth $n = 17$ shape, five-valued like $(17, 2)$ but with different multiplicities. The row $(16, 7)$, $(16, 9)$ is nine-valued, the richest shape at any $n \le 17$; the only comparable rows are $(12, 5)$, $(12, 7)$ of [10, Table 2], also nine-valued and also at even n — and

both are surpassed by the fifteen values at $n = 18$. Grouping is by equality of spectra: at $n = 14$ the four cells $k = 3, 5, 9, 11$ agree although only $3 \leftrightarrow 11$ and $5 \leftrightarrow 9$ are related by the Frobenius transfer, and the same happens at $k = 2, 7, 8, 13$ for $n = 15$, at $k = 3, 5, 11, 13$ for $n = 16$ and at $k = 2, 5, 7, 8, 9, 10, 12, 15$ for $n = 17$.

These are new data — [10, Table 2] stops at $n = 13$ and is the only published table of these spectra — but a cheap computation: S costs 2^{2n-1} steps, seconds rather than the 2^{2n} of a ρ-sweep. Two external consistency checks pass, both using results of [10] *proved* for n it never computed. Its Lemma 3.5, the Frobenius transfer $k \leftrightarrow n - k$, forces the spectra of k and $n - k$ to coincide, and every such pair at $n = 14, \ldots, 18$ does. Its Theorem 11.8(iii), proved for every odd n, puts the spectrum of $2S$ for $k = 2$ inside $\{0, \pm 2^{(n+1)/2}, \pm 2^{(n+3)/2}\}$; at $n = 15$ that predicts $S \in \{0, \pm 128, \pm 256\}$ and at $n = 17$ it predicts $S \in \{0, \pm 256, \pm 512\}$, and those are exactly the value sets found. (One value of n lower, [10, §12] states that at $(13, 2)$ the extreme values are attained at exactly 182 elements, and the histogram computed here has $-128{:}91$ and $128{:}91$.)

Corollary 5.4. *Conjecture 5.2 is confirmed, cell by cell, at every cell of Propositions 8.7, 4.4 and 5.3 to which it applies. Concretely:*

(a) *at every computed cell with $k = 1$, that is at $m \in \{3, 4, 5, 7, 9, 11, 13, 14, 15, 16, 17, 18\}$, the code $C_{D(f)}$ is a $[2^{m-1}, m - 1, 2^{m-2}]$ one-weight code, exactly as the conjecture asserts for $h = 1$: S takes the value $|\Delta| = 2^{m-1}$ at one $a \neq 0$ and the value 0 at all others. The same holds at the computed cells with $k = m - 1$, which the conjecture does not mention; and its preamble calls F both APN and AB, which restricts it to odd m, so the even m in the list above lie outside its scope too and are recorded here as data;*

(b) *at all 48 cells with m odd, $5 \leq m \leq 17$ and $k \not\equiv \pm 1 \pmod m$, the code has length 2^{m-1} and dimension m, and has exactly three nonzero weights at 18 of them and exactly five at the other 30. The three-weight cells are exactly those where S takes only the values $0, \pm 2^{(m-1)/2}$, namely $(5, 2)$, $(5, 3)$, $(7, k)$ for $k = 2, 3, 4, 5$, $(11, k)$ for $k = 3, 4, 7, 8$, $(13, k)$ for $k = 3, 4, 9, 10$, and $(17, k)$ for $k = 3, 6, 11, 14$;*

(c) *the sub-claim for $h = 3$ is confirmed at $m = 5, 7, 11, 13, 17$ — the odd $m \leq 17$ with $m \not\equiv 0 \pmod 3$, which are exactly those for which $k = 3$ is admissible: three weights in each case.*

For even m, which Conjecture 5.2 does not cover, the codes are richer: fifteen nonzero weights at $m = 18$ and $h = 5, 7, 11, 13$ (Corollary 4.5), nine at $(16, 7)$, $(16, 9)$ and at $(12, 5)$, $(12, 7)$, five at $(14, 3)$.

Proof. Apply Lemma 5.1 to the tables of Propositions 8.7, 4.4 and 5.3, in which $|\Delta| = 2^{m-1}$ throughout. In case (a) the kernel of $x \mapsto c(x)$ has order 2, so the dimension is $m - 1$, and the single nonzero weight is $(2^{m-1} - 0)/2 = 2^{m-2}$, which is then also the minimum distance. In cases (b) and (c) no $a \neq 0$ has $S(a) = 2^{m-1}$ — in those cells $\max_{a \neq 0} |S(a)| \leq 2^{m-1}/4$, for instance 1024 against $|\Delta| = 16384$ at $(15, 4)$ — so the kernel is trivial, the dimension is m, and by Lemma 5.1 the number of nonzero weights is the number of distinct values taken by S on $a \neq 0$. □

Corollary 5.4 is a computational confirmation, cell by cell, not a proof of Conjecture 5.2; what it adds is that the conjecture now has an explicitly recorded verified range, that the range reaches $m = 17$ and covers every cell there, and that the uncovered even case is now populated as far as $m = 18$.

6. An outlier at $n = 15$, and the even-n regime

For odd n write

$$\max_{a \in \mathbb{F}_{2^n}^*} |2S(a)| = 2^{(n+v)/2},$$

which defines an odd integer $v = v(n, k)$. At a degenerate cell $k \equiv \pm 1$ one has $v = n$ trivially, since S takes only the values 0 and 2^{n-1}; the interesting range is $k \not\equiv \pm 1$. For $k = 2$ and every odd n, [10, Theorem 11.8(iii)] gives $v \in \{1, 3\}$ — that is its radical-dimension dichotomy — and the same $v \in \{1, 3\}$ is visible in every nondegenerate odd row of [10, Table 2], at every k, not only $k = 2$.

Proposition 6.1. *Let E be the set of all 48 cells with n odd, $5 \le n \le 17$, $\gcd(k,n) = 1$ and $k \not\equiv \pm 1 \pmod n$. Then $v(n,k) \in \{1,3\}$ at 46 of the cells of E — with $v = 1$ at 18 of them and $v = 3$ at 28 — and the two exceptions are $(15,4)$ and its Frobenius twin $(15,11)$, where*

$$S \text{ takes the values } \{-128, 0, 128, 512, 1024\} \text{ with multiplicities } \{7920, 16896, 7920, 30, 1\},$$

so $2S$ reaches $2^{11} = 2^{(n+7)/2}$ once and $2^{10} = 2^{(n+5)/2}$ thirty times, and $v(15,4) = v(15,11) = 7$. In particular $v \in \{1,3\}$ at all fourteen nondegenerate cells with $n = 17$.

The two large values occur *only* with positive sign, while the ± 128 level is exactly symmetric; both sums (6) hold, as $512 \cdot 30 + 1024 = 2^{14} = 2^{n-1}$ and $2 \cdot 7920 \cdot 128^2 + 30 \cdot 512^2 + 1024^2 = 2^{28} = 2^{2n-2}$. The number of distinct values is still five, so Conjecture 5.2 survives the outlier (Corollary 5.4(b)); what fails at $(15,4)$ is only the amplitude dichotomy. By Proposition 4.6 the value 1024, of multiplicity one, is $S(1)$.

At even n the picture is different in kind, and it is worth setting beside the odd one, because it says why v is an odd-n quantity rather than a quantity with different values at even n. Table 3 collects every nondegenerate even cell whose spectrum is computed here.

TABLE 3. The nondegenerate even cells, from Propositions 8.7, 4.4 and 5.3. "Values" is the number of distinct values of S on $a \neq 0$.

cells	values	$\max_{a \neq 0} \lvert 2S(a) \rvert$
$(8,3), (8,5)$	4	2^6
$(10,3), (10,7)$	5	2^7
$(12,5), (12,7)$	9	$3 \cdot 2^7$
$(14,3), (14,5), (14,9), (14,11)$	5	2^9
$(16,3), (16,5), (16,11), (16,13)$	5	2^{10}
$(16,7), (16,9)$	9	$3 \cdot 2^9$
$(18,5), (18,7), (18,11), (18,13)$	15	$5 \cdot 2^{10}$

Over the 48 odd and 20 even nondegenerate cells verified here — and $8 \le n \le 18$ covers every even n that has a nondegenerate cell at all — the pattern is: every nondegenerate odd cell has $\max_{a \neq 0} \lvert 2S(a) \rvert$ a power of two, while a nondegenerate even cell has one exactly when its spectrum has at most five values, and does not when it has nine or more. This is an observation over the computed cells, not a theorem. It does say, though, that the failure at even n is not new at $n = 18$: it is already there at $(12,5)$, inside [10, Table 2] itself. At $n = 18$ the failure is extreme — $5 \cdot 2^{10}$ is not even of the form $3 \cdot 2^j$ — and at $(18,5)$, by Proposition 4.6, the responsible value -2560 is again $S(1)$, attained there and nowhere else.

Question 6.2. What distinguishes $(15,4)$? Is it the first member of an infinite class of cells with $v \ge 5$, and if so, which? Equivalently, in the language of [5]: for which odd m and admissible h does the five-weight code $C_{D(f)}$ have minimum weight $2^{m-2} - 2^{(m+5)/2-1}$ rather than $2^{m-2} - 2^{(m+1)/2-1}$?

The question is sharpened, rather than answered, by the shape of the data. The exception is not isolated in k alone — it appears at $k = 4$ and at $k = n - k = 11$, as the Frobenius transfer requires — but it is isolated in n: neither $n = 13$ nor $n = 17$ has any cell with $v \ge 5$, so whatever mechanism produces $v = 7$ at $n = 15$ is not monotone in n. Note also that $15 = 3 \cdot 5$ is the only odd composite n in $\{13, 15, 17\}$, and that $\gcd(4, 15) = 1$ while 4 divides neither 15 ± 1; a proof of Conjecture 1.1 that argues uniformly in k through an amplitude bound on S will have to accommodate this cell. What Proposition 4.6 adds is a place to look: the exceptional values sit on the smallest cyclotomic cosets — on $\mathbb{F}_2$ in both anomalous cells, and at $(18,5)$ the next two extremes sit on $\mathbb{F}_4 \setminus \mathbb{F}_2$ and inside $\mathbb{F}_8$, again by a coset decomposition computed outside the formal development. Since $S(1) = \sum_{t \in \Delta} (-1)^{\mathrm{Tr}(t)}$ costs only 2^{n-1} steps to evaluate, "is the extreme of S attained at $a = 1$?" is a question that can be pushed far past $n = 18$ by anyone who wants to.

7. Cube-refined counts at even n

For even n the Kasami exponent satisfies $\gcd(d, 2^n - 1) = 3$, and Carlet [2, §4.5] identifies precisely what that costs. In his words:

> If n is even then, as proved by Dobbertin … we have $\gcd(d, 2^n - 1) = 3$ and we cannot then use Proposition 4.11. … To be able to handle the case n even, we would then need to have information not only on the size of the set $\{(x, y, z) \in \Delta_F^3 \,;\, v_1x + v_2y + (v_1 + v_2)z = 0\}$ as in the case of n odd, but also on the sets $\{(x, y, z) \in \Delta_F^3 \,;\, v_1x+v_2y+(v_1+v_2)z$ is a nonzero cube$\}$ and $\{(x, y, z) \in \Delta_F^3 \,;\, v_1x + v_2y + (v_1 + v_2)z$ is not a cube$\}$.

He also records, in §4.4 of the same paper, that the object one would want in order to compute such things — the Fourier transform of the indicator of Δ — is unknown. Immediately after the passage above he proposes a route around the two counts, through the unbalancedness of the component functions at even n, and then records that it does not settle the matter: "the CWUness of a plateaued APN power function over $\mathbb{F}_{2^n}$, n even, does not seem to depend only on the distribution of its values". This section computes the two counts he names, and finds that they behave exactly as Conjecture 1.1 does: constant in (v_1, v_2), and pinned at the value equidistribution predicts.

Let n be even, so that $3 \mid 2^n - 1$ and the cubes $C = (\mathbb{F}_{2^n}^*)^3$ form a subgroup of index 3 with cosets C, ωC, $\omega^2 C$, where ω is a primitive cube root of unity. For $\rho \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ and $(x, y, z) \in \Delta^3$ write $s = x + \rho y + (1 + \rho)z$, and set

$$N_C(\rho) = \#\{(x, y, z) \in \Delta^3 : s \in C\},$$

and likewise $N_{\omega C}(\rho)$ and $N_{\omega^2 C}(\rho)$. Scaling a pair (v_1, v_2) multiplies s by the scalar and hence permutes the three cosets, so by Lemma 2.1 the three counts for a general admissible pair (v_1, v_2) are the three counts above at $\rho = v_2/v_1$, read in some order; once the three are known to be equal, the value is a statement about every admissible pair and not only about $(1, \rho)$.

Theorem 7.1. *Put $T(n) = \big(2^{3n-3} - 2^{2n-3}\big)/3$, and name ρ by the bit-mask convention of §2.1.*

(i) *$N_C(\rho) = T(n)$ for* every $\rho \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ *at each of the eight cells $(4, 1)$, $(4, 3)$, $(6, 1)$, $(6, 5)$, $(8, 1)$, $(8, 3)$, $(8, 5)$, $(8, 7)$ — that is, at every admissible cell with $n \in \{4, 6, 8\}$ — and at the following further instances: $n = 10$, $k \in \{3, 7\}$, $\rho \in \{\alpha,\ \alpha+1,\ \alpha^2+1,\ \alpha^9,\ \sum_{j<10} \alpha^j\}$; $(12, 5)$, $\rho \in \{\alpha,\ \sum_{j<12} \alpha^j\}$; and $(12, 7)$, $\rho = \alpha + 1$.*

(ii) *$N_{\omega C}(\rho) = T(n)$ for every $\rho \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ at the same eight cells with $n \in \{4, 6, 8\}$; at $(10, 3)$ for $\rho \in \{\alpha,\ \sum_{j<10} \alpha^j\}$; at $(10, 7)$ for $\rho = \alpha$; and at $(12, 5)$ for $\rho = \alpha$.*

(iii) *Consequently, wherever (i) and (ii) both apply, $N_{\omega^2 C}(\rho) = T(n)$ as well: each of the three cosets of the cubes receives exactly $T(n)$ of the triples, the number of triples with $s \notin C \cup \{0\}$ — Carlet's "not a cube" — is $2T(n)$, and $\sum \chi_3(s) = 0$, the sum being over the triples of Δ^3 with $s \neq 0$ and χ_3 either nontrivial cubic character of $\mathbb{F}_{2^n}^*$.*

Proof, and the search it consisted of. The counts N_C and $N_{\omega C}$ were evaluated directly: for each of the $|\Delta|^2$ pairs (x, y), the elements $t \in (1+\rho)\Delta$ with $x+\rho y+t$ in the class were counted, so a single ρ costs 2^{3n-3} steps and an exhaustive sweep 2^{4n-3}. That cost is why the exhaustive statements stop at $n = 8$ and the rest are at listed ρ. The class membership test is $a \mapsto a^{(2^n-1)/3}$, whose fibres on $\mathbb{F}_{2^n}^*$ are exactly the three cosets, and ω is taken to be $g^{(2^n-1)/3}$ for the generator g of Proposition 8.2; that $\omega^3 = 1$ and $\omega \neq 1$ is checked at $n = 8$ and $n = 10$. Part (iii) is then arithmetic: $|\Delta^3| = 2^{3n-3}$, the triples with $s = 0$ number $N(1, \rho) = 2^{2n-3}$ by Proposition 3.4 at every $n \leq 12$, and $3T(n) = 2^{3n-3} - 2^{2n-3}$, so the third coset count is forced by the other two. Everything in (i) and (ii) rests on exhaustive computation over the stated ranges. □

Conjecture 7.2. For every even n, every k with $\gcd(k, n) = 1$, and every pair of distinct nonzero $v_1, v_2 \in \mathbb{F}_{2^n}$, each of the three cosets of the cubes receives exactly $\big(2^{3n-3} - 2^{2n-3}\big)/3$ of the triples $(x, y, z) \in \Delta^3$ with $s = v_1x + v_2y + (v_1 + v_2)z \neq 0$.

Conjecture 7.2 is the multiplicative counterpart of Conjecture 1.1: the latter says an additive character sum over Δ^3 vanishes, the former that the first nontrivial multiplicative one does. Note

that it has content only at even n. For odd n cubing is a bijection of $\mathbb{F}_{2^n}$, every nonzero element is a cube, $N_C = 2^{3n-3} - 2^{2n-3}$ and the other two counts are 0; that is verified exhaustively at $(9, 2)$ and is one of the controls of Proposition 8.6(g). So the statement fails at odd n, as it must, and it is exactly at even n — where Carlet says the difficulty lies — that it says something.

Remark 7.3 (wider evidence, outside the formal development). The auxiliary C program carries the same computation further, and none of the following is machine-checked. $N_C = T(n)$ holds at every ρ for every admissible cell at $n = 4, 6, 8, 10$ and at $(12, 1)$, $(12, 5)$; and at sampled ρ at $(12, 7)$, at $(14, 3)$, $(14, 5)$, at $(16, 3)$, $(16, 7)$, $(16, 9)$ and at $(18, 5)$, $(18, 7)$, $(18, 13)$, with $N_C = 750{,}597{,}074{,}583{,}552 = (2^{51} - 2^{33})/3$ at $n = 18$. The number of triples with s a non-cube was $2N_C$ in every case. The three-coset refinement was checked at every ρ at $n = 4, 6, 8$ and at sampled ρ at $(10, 3)$, $(10, 7)$, $(12, 5)$, $(14, 3)$, $(16, 7)$ and $(18, 5)$.

Neither source computes this quantity. [10, §14(d)] is aware of the 3-structure at even n — it notes that $x \mapsto x^{q+1}$ is 3-to-1 on $\mathbb{F}_{2^n}^*$ — but does not evaluate the refined counts, and Conjecture 5.2 is a statement about the spectrum of S for odd m, a different object. What is new here is not a range but a quantity: the value of the counts Carlet names, on the evidence of the cells above.

8. The computation: what was run, and what it rests on

8.1. **The search.** For a cell (n, k) the character sweep is the following finite computation, and nothing else.

(1) Build Δ from (1) by evaluating F at all 2^n points and marking $\delta(b)$ for each b (2^n field exponentiations).
(2) Build $\big(S(a)\big)_{a \in \mathbb{F}_{2^n}}$ from definition (3): $|\Delta|$ terms for each of 2^n values of a, i.e. 2^{2n-1} steps. There is no fast Walsh–Hadamard transform in the formal development, deliberately, so that no butterfly identity has to be justified. The only shortcut used is $\mathbb{F}_2$-linearity of $t \mapsto \mathrm{Tr}(at)$ in the form $\mathrm{Tr}(at) = \mathrm{parity}\big(\varphi(a) \wedge t\big)$, where $\varphi(a)$ is the n-bit mask with j-th bit $\mathrm{Tr}(a\alpha^j)$; this identification is itself checked against multiply-and-trace (Proposition 8.3).
(3) For each of the $2^n - 2$ values of ρ, evaluate $Z(\rho)$ as in (4) — a sum of $2^n - 1$ triple products — and compare it with 0. The cell passes only if every comparison succeeds.

Step (3) dominates, at $\approx 2^{2n}$ multiplications per cell. The definition-level count behind Theorems 3.3 and 4.3 and Proposition 3.4 is step (1) followed by a double loop over $\Delta \times \Delta$ with a membership test, 2^{2n-2} steps per value of ρ.

8.2. **Making 2^{2n} affordable.** Three implementation decisions separate a range that stops around $n = 15$ from one that reaches $n = 18$. Each of them changes what can be stated at all, so each is recorded here.

Compiled evaluation. The evaluation core of the development imports nothing at all — no library, not even the standard mathematical one — so that it can be compiled to a shared object and loaded by the proof checker, which then runs native code instead of interpreting an intermediate representation. The difference is not a constant-factor nicety: the sweep at $(13, 2)$ takes 2.4 seconds with the compiled library loaded and had not finished after 120 seconds without it, so the speed-up on this code shape is at least $50\times$ (a lower bound: the interpreted run was killed, not allowed to finish). Every check in this development was run with the library loaded; without it the results at $n \ge 15$ would not be reachable at all.

Discrete-logarithm re-indexing. Written as (4), each ρ appears to need the maps $\lambda \mapsto \lambda\rho$ and $\lambda \mapsto \lambda(1 + \rho)$, i.e. a multiplication table rebuilt $2^n - 2$ times. Writing $\lambda = g^i$ for a generator g of $\mathbb{F}_{2^n}^*$ turns both into index shifts:

$$Z(\rho) = \sum_{i < 2^n - 1} T[i]\, T[i + \ell_\rho]\, T[i + \ell_\sigma], \qquad T[i] = S(g^i), \quad \sigma = 1 + \rho,$$

with ℓ the discrete logarithm and indices read modulo 2^n-1 (implemented by doubling the array T so that no reduction is needed in the inner loop). That the tabulated g is a generator is machine-checked (Proposition 8.2). Worth on its own: about a factor of 2.

Skipping killed terms. S vanishes on about half of $\mathbb{F}_{2^n}^*$ in every nondegenerate cell and on all but one point in the degenerate ones, so testing the first two factors before multiplying is worth a further factor of about 1.5 to 3. This is the one place where the code executed differs from the sum (4) as written, and the gap is closed by proof rather than by inspection.

Proposition 8.1. *The term-skipping evaluation of* (4) *equals the plain term-by-term sum, for all arguments; consequently the sweep that is executed and the sweep stated as the plain sum decide the same thing, at every n and k.*

Proposition 8.1 is proved by induction, with no appeal to evaluation and no finite data; its axiom footprint is the two propositional axioms of the proof kernel, without even the axiom of choice. Proposition 4.2 is the second and last statement of that kind: together they close both gaps between the code that is executed and the sum that is stated.

The two figures just quoted are estimates of what each of the last two optimisations is worth, and they are not independent — what the skip saves depends on the loop the re-indexing leaves. What was measured is the pair together: they took the check at $(13,2)$ from 2.40 to 1.50 seconds in total, and its sweep proper from 2.0 to 1.05 seconds, a factor of 1.9; that factor is the reason the whole $n=17$ row costs about an hour and a half rather than three.

8.3. **What the conclusions rest on.** Theorems 3.1 and 4.1 rest on exhaustive computation and on Proposition 2.3, which is not reproved here. Six groups of checks pin down everything else.

Proposition 8.2 (the field model)**.** *For every n with $3 \le n \le 20$: $\mathbb{F}_2[x]/(f_n)$ is a field with 2^n elements; the tabulated element g generates its multiplicative group; and* $\mathrm{Tr}(x) = \sum_{i<n} x^{2^i}$ *takes values in $\{0,1\}$ and equals* $\mathrm{parity}(x \wedge \mu_n)$ *for every x, where μ_n is the mask with j-th bit* $\mathrm{Tr}(\alpha^j)$*. Moreover, for $n \le 7$ the shift-and-xor product is commutative and associative and distributes over addition on all 2^{3n} triples of elements.*

The field test is complete, not a sample: every nonzero a is checked to satisfy $a^{2^n-1}=1$, hence to be a unit with inverse a^{2^n-2}, and a finite commutative ring whose nonzero elements are all units is a field. The generator test is complete for the same reason: 2^n-1 powers of g occupying all 2^n-1 nonzero slots force $i \mapsto g^i$ to be a bijection. Both tests are non-vacuous: the field test rejects the reducible moduli x^4+1, x^4+x^3+x+1 and x^8+1 and accepts the irreducible but not lexicographically smallest x^6+x^3+1. Isomorphism invariance was checked as well: three spectra recomputed over a different irreducible modulus of the same degree give the same table. The range $n \le 20$ exceeds anything computed here; $n = 19, 20$ were checked because the tables of moduli and generators carry entries there, and an unchecked table entry is a place for an error to hide.

Proposition 8.3 (S computed two ways)**.** *For each of the eight cells* $(5,2)$, $(7,3)$, $(8,3)$, $(9,2)$, $(10,3)$, $(11,2)$, $(11,3)$, $(12,5)$ *and every $a \in \mathbb{F}_{2^n}$, the value of $S(a)$ obtained from* $\mathrm{Tr}(at) = \mathrm{parity}(\varphi(a) \wedge t)$ *agrees with the value obtained by multiplying a by t in the field and taking the full trace of the product.*

The honest evaluation costs a field multiplication and a full trace per term, which is what limits this comparison to $n=12$. Beyond that, the two identities (6) take over as global checks: they hold exactly when $a \mapsto \varphi(a)$ is a bijection of $\mathbb{F}_2^n$ and the parity formula computes the trace, and a wrong φ would not satisfy them. Both are reported as part of every spectrum in §4.3 and §5, at $n=18$ included.

Proposition 8.4 (the reduction, tested where it has content)**.** *Identity* (5) *holds, as an equality of integers, at every sampled ρ in ten cells with* $\gcd(k,n) > 1$ — $(6,2)$, $(6,3)$, $(6,4)$, $(9,3)$, $(9,6)$, $(10,2)$, $(10,5)$, $(12,4)$, $(12,8)$, $(12,9)$ — *and in seven admissible cells, namely* $(8,3)$, $(9,2)$, $(11,2)$, $(11,3)$, $(12,5)$, $(13,2)$, $(13,3)$.

The point of the inadmissible cells is that there identity (5) has content. At an admissible cell both sides are the same constant, and the test is nearly vacuous. At $\gcd(k,n) > 1$ the set Δ does not even have size 2^{n-1} — $|\Delta| = 16$ and 29 at $(6,2)$ and $(6,3)$, 64 at $(9,3)$, 256 at $(10,2)$, 497 at $(10,5)$, 256 at $(12,4)$ — so $|\Delta|^3$ is not 2^{3n-3}, and $Z(\rho)$ is a large number varying with ρ (for instance $Z = 24576$ and 16384 at two values of ρ in $(9,3)$, $Z = -69$ in $(6,3)$, $Z = 851968$ in $(12,4)$). The left side of (5) is then a triple count made by set membership and the right side a character sum over a discrete-logarithm re-indexing, and they agree exactly. The test is also sharp in the term that matters: replacing $|\Delta|^3$ by the conjectured 2^{3n-3} makes (5) false at the inadmissible cells $(9,3)$ and $(10,5)$ while leaving it true at the admissible $(9,2)$.

Formalising (5) itself — that is, proving orthogonality of additive characters, $\sum_\lambda (-1)^{\mathrm{Tr}(\lambda w)} = 2^n[w=0]$, over the concrete model of §2.1 — would make Theorems 3.1 and 4.1 independent of [10]. It has not been done here; Theorems 3.3 and 4.3 are the substitute actually built, since they pin $N(1,\rho)$ itself with no character sum at all.

The next check is the only published invariant of Δ itself that this development tests: the Frobenius transfer, [10, Theorem 11.8(iii)] and the two sums (6) are all checks on S. So it is what validates the construction of Δ at the new n independently of everything the character sum does.

Proposition 8.5 (the Dillon–Dobbertin invariant)**.** $|\Delta \cap \mu\Delta| = 2^{n-2}$, *equivalently* $|(\Delta\setminus\{0\}) \cap \mu(\Delta\setminus\{0\})| = 2^{n-2}-1$, *for every* $\mu \in \mathbb{F}_{2^n}^*$ *with* $\mu \ne 1$, *at every admissible cell with* $5 \le n \le 15$ *and at* $(16,3)$, $(16,7)$.

This is the combinatorial form of the Dillon–Dobbertin theorem that $\Delta\setminus\{0\}$ is a cyclic difference set with Singer parameters, recorded in [10, §14(c)]; the mathematics is theirs and only the verification is new. The check costs 2^{2n+1} steps, so $n = 16$ is its ceiling. It is non-vacuous: it fails at every inadmissible cell tested — $(9,3)$, $(9,6)$, $(10,2)$, $(10,5)$, $(12,4)$, $(12,8)$ — and against the targets $2^{n-2} \pm 1$ at $(9,2)$, so the constant is pinned exactly.

Proposition 8.6 (negative controls)**.**

(a) *The constant is pinned from both sides and off by one: run against* 2^{2n-2} *(twice too large),* 2^{2n-4} *(twice too small),* $2^{2n-3}+1$ *and* $2^{2n-3}-1$, *the definition-level sweep at* $(8,3)$ *fails in each case and succeeds only at* 2^{2n-3}, *and the same at* $(9,2)$ *against* 2^{2n-2} *and* 2^{2n-4}; *likewise the character sweep rejects* $Z \equiv 1$ *at* $(8,3)$ *and at* $(11,2)$, *and* $Z \equiv -1$ *at* $(8,3)$; *and at* $(18,5)$ *already the first half-range rejects* $Z \equiv 1$ *and* $Z \equiv -1$.

(b) *The hypothesis* $\gcd(k,n) = 1$ *is not idle: the conclusion fails at* $(6,2)$, $(6,3)$, $(9,3)$, $(9,6)$, $(10,2)$, $(10,5)$, $(12,4)$, $(12,8)$, *and at six of those cells — the same six — it is checked in addition that* $|\Delta| \ne 2^{n-1}$, *so* [10, Lemma 3.3] *fails there too.*

(c) *The hypothesis "*v_1, v_2 *distinct and nonzero" is not idle: at* $v_1 = v_2$ *and at* $v_2 = 0$ *the count is* 2^{2n-2}, *twice the conjectured value.*

(d) *The field test rejects reducible moduli of the right degree and accepts non-lexicographically-smallest irreducible ones.*

(e) *A partial sweep is strictly weaker than a whole one, so the splitting of §4.1 is not doing the work: at the inadmissible* $(9,3)$ *the one-value range* $\rho = \alpha$ *satisfies* $Z \equiv 24576$ *while the range* $\rho = \alpha^2 + \alpha + 1$ *does not and the whole sweep does not. The arithmetic hypothesis of Proposition 4.2 is a real constraint:* $131071 + 131070 \ne 2^{18} - 2$. *And the split lemma agrees with computation at* $(10,3)$, *where the two halves and the undivided sweep are each checked independently.*

(f) *The Frobenius invariance of Proposition 4.6 is specific to squaring, and its lone-extreme test rejects values of multiplicity greater than one.*

(g) *Theorem 7.1 fails where it should: at odd* n *the count* N_C *is* $2^{3n-3} - 2^{2n-3}$, *three times the target — proved exhaustively at* $(9,2)$ *and rejected at* $(9,2)$, $(11,2)$ *against the even-*n *target — and it also fails at* $(10,2)$, $(12,4)$, *where* $\gcd(k,n) > 1$, *and against the targets* $T(8) \pm 1$ *at* $(8,3)$.

Finally, before anything new was claimed, the published data was recomputed from the definitions used here.

Proposition 8.7 ([10, Table 2] reproduced)**.** *For all thirty-two cells (n, k) making up the thirteen classes listed in* [10, Table 2]*, the value $|\operatorname{supp} S \setminus \{0\}|$ and the full value histogram of S on $a \neq 0$ agree with the table, and both sums* (6) *hold.*

All thirty-two cells reproduce exactly, with no mismatch; the comparison against the typeset table was itself made programmatically. This is the data of [10], recomputed and certified, not new mathematics.

9. Range, cost, and what is next

The formal development is about 6.8 CPU-hours on one core of a shared machine, with peak resident memory 1.64 GB, of which 1.49 GB is the proof checker itself, so the marginal memory cost of the largest sweep is under 0.15 GB: the computation is bound by processor time, not by memory. The cost per cell of the exhaustive character sweep is given in Table 1; the $n = 18$ row is about 1.8 CPU-hours for all six cells, of which about 0.33 went on recomputing S a second time inside each half-range. An auxiliary C implementation of the same algorithm, used to price the formal runs and to cross-check their numbers, ran the whole $n = 18$ row in 345–425 seconds per cell.

The Lean-to-C ratio is not a single number, and the reason matters for what comes next. For the sweep proper it is about 2 at $n = 18$; for the evaluation of S it is about 10. And the cost of a cell is not a function of n alone. The inner loop's real cost is governed by how often the first two factors of a term are both nonzero, i.e. by p^2 where $p = |\operatorname{supp} S|/2^n$ — and p is exactly what Table 2 and Proposition 4.4 measure. It falls from $57274/2^{17} = 43.7\%$ at $(17, 2)$ to $68139/2^{18} = 26.0\%$ at $(18, 5)$, so p^2 falls by a factor 2.8 and largely cancels the factor 4 growth in 2^{2n}: measured, a nondegenerate cell grew only 2.7× from $n = 17$ to $n = 18$, against the 4–8× that extrapolating from $n = 16 \to 17$ would have predicted.

Remark 9.1 ($n = 19$, and why it is blocked rather than merely expensive)*.* The following is a measurement, not a theorem. The auxiliary C program completed the cell $(19, 2)$ in 1772 seconds (122 s for S, 1650 s for the sweep) with no mismatch over all 524,286 values of ρ, and returned the spectrum $\{-1024 : 5434,\ -512 : 109080,\ 0 : 294747,\ 512 : 109592,\ 1024 : 5434\}$, both sums (6) exact. Note $\max|2S| = 2^{11} = 2^{(n+3)/2}$: the cell is back inside the dichotomy of §6, leaving $(15, 4)$ and $(15, 11)$ still the only exceptions known. That spectrum also prices the formal check. Its support density is 43.8%, back at the $n = 17$ value, so the term-skipping does not help as it did at $n = 18$ and one cell is about 2.5 CPU-hours — past the thirty-minute-per-file limit of §4.1. Splitting does not rescue it, because every piece pays for S again, and S alone is about twenty minutes at $n = 19$: bringing each piece under thirty minutes needs at least fourteen of them, which costs about 6.8 CPU-hours for that one cell, and $\varphi(19) = 18$. The binding constraint is therefore the repeated evaluation of S, not the sweep, and the highest-leverage improvement available is a faster S — the part running at 10× the C prototype rather than 2.

Two published symmetries would cut the work by an order of magnitude and were deliberately not used: the S_3-action $\rho \mapsto 1/\rho$, $\rho \mapsto 1 + \rho$ leaving $N(1, \rho)$ invariant ([10, Proposition 4.1]), worth about 6×, and the Frobenius transfer $k \leftrightarrow n - k$ ([10, Lemma 3.5]), worth 2×. Using them would make the statements above conditional on [10] beyond the single dependence on Proposition 2.3 that is already recorded. Establishing the S_3 invariance directly over the model of §2.1 would cut a cell to roughly a third of its cost, but it would not move the S floor that blocks $n = 19$.

The open mathematics is, of course, the general case, and [10, §13, §14] says what a proof would need: genuine cancellation — its §8 refutes the termwise mechanism for $2 \le k \le n - 2$ — or an exact fibration argument of the kind that settles the Gold and inverse analogues. Carlet had already identified the obstruction in the preprint of [2]: adapting the Dillon–Dobbertin proof would need the Fourier transform of the indicator of Δ itself, and that transform is unknown; a route to it could come from the image set of the Dickson polynomial $D_3(x) = x^3 + x$, which is also unknown. That

Fourier transform is precisely the array S tabulated here, cell by cell — and §7 adds that the first multiplicative statistic he asks for, at even n, appears to be the trivial one.

10. Verification

Every theorem, proposition and corollary in this paper except Proposition 2.3, which is quoted from [10] and not reproved, is formally verified in Lean 4 [9] (toolchain `v4.32.0`); the development contains no `sorry` and no hand-written axiom, and the repository it lives in builds against *Mathlib*, although the evaluation core used here imports no library beyond Lean's built-in prelude, so that it can be compiled to a shared object and executed as native code by the proof checker. Propositions 8.1 and 4.2, which identify the sum that is executed with the sum (4) that is stated and a pair of consecutive sub-ranges with the whole range, are proved by induction and depend on no axioms beyond the two propositional ones, without the axiom of choice. Everything else — Theorems 3.1, 3.3, 4.1, 4.3, 7.1 and Propositions 3.2, 3.4, 4.4, 4.6, 5.3, 6.1, 8.2, 8.3, 8.4, 8.5, 8.6 and 8.7 — is a finite search delegated to compiled evaluation, and the axiom footprint of each such statement is exactly the propositional axiom together with the evaluation axioms generated for it, one per search (ten, for Theorem 4.1: two whole-range cells and eight half-ranges). The searches are the ones described in §8: for Theorems 3.1 and 4.1, one Boolean per cell (or per half-cell) asserting $Z(\rho) = 0$ at all the values of ρ in its range; for Theorems 3.3 and 4.3 and Proposition 3.4, one Boolean per cell asserting a listed set of direct triple counts, or all of them; for Theorem 7.1, one Boolean per cell and class; for Propositions 4.4, 5.3, 8.7 and 6.1, one equality of tuples per cell. Lemmas 2.1, 2.2 and 5.1 are elementary and are proved in the text above rather than in the formal development, and Corollaries 4.5 and 5.4 are read off the machine-checked tables through Lemma 5.1. Every numerical table quoted here was produced first by an independent C implementation of the same definitions and only then stated and checked formally, so that the formal run re-checks a known answer rather than searching for one; the published range of Proposition 3.2 was reproduced in both, and the $n = 18$ spectrum of Proposition 4.4 was reproduced digit for digit by a third implementation using a different algorithm (logarithm tables and a fast Walsh–Hadamard transform), itself cross-validated at smaller n against a naive $O(4^n)$ computation and against a different irreducible modulus. Repository reference to be added at submission.

References

[1] O. Ahmadi and M. Shafaeiabr, *Difference sets and three-weight linear codes from trinomials*, Finite Fields Appl. **89** (2023), Paper No. 102195, doi:10.1016/j.ffa.2023.102195, Zbl 1519.94231; preprint, titled *Difference sets and tri-weight linear codes from trinomials over binary fields*, arXiv:2108.10042v1, from which the passage quoted in §5 is taken.

[2] C. Carlet, *Componentwise APNness, Walsh uniformity of APN functions, and cyclic-additive difference sets*, Finite Fields Appl. **53** (2018) 226–253, doi:10.1016/j.ffa.2018.06.007; preprint: IACR Cryptology ePrint Archive 2017/528, version `20170918:184412` (the later of the two posted). Definition 4.12, §4.2, §4.4, §4.5 and the displayed passages quoted above are that version's; the two clauses about verified ranges quoted in §1 are the published abstract's, whose body we could not obtain.

[3] C. Carlet, *On APN exponents, characterizations of differentially uniform functions by the Walsh transform, and related cyclic-difference-set-like structures*, Des. Codes Cryptogr. **87** (2019), no. 2–3, 203–224, doi:10.1007/s10623-018-0512-3.

[4] S. D. Cohen and R. W. Matthews, *A class of exceptional polynomials*, Trans. Amer. Math. Soc. **345** (1994), no. 2, 897–909, doi:10.1090/S0002-9947-1994-1272675-0.

[5] C. Ding, *A construction of binary linear codes from Boolean functions*, Discrete Math. **339** (2016), no. 9, 2288–2303, doi:10.1016/j.disc.2016.03.029; arXiv:1511.00321v1, whose numbering of the conjectures is the one used above (resolved by compiling its source; [7] and [1] cite the published article and use the same numbers).

[6] H. Dobbertin, *Kasami power functions, permutation polynomials and cyclic difference sets*, in: A. Pott et al. (eds.), Difference Sets, Sequences and their Correlation Properties (Proc. NATO Advanced Study Institute, Bad Windsheim, 1998), NATO ASI Series C **542**, Kluwer, Dordrecht, 1999, 133–158, doi:10.1007/978-94-011-4459-9_6.

[7] F. Göloğlu and D. Krasnayová, *Proofs of several conjectures on linear codes from Boolean functions*, Discrete Math. **342** (2019), no. 2, 572–583, doi:10.1016/j.disc.2018.10.022.

[8] T. Kasami, *The weight enumerators for several classes of subcodes of the 2nd order binary Reed–Muller codes*, Inform. and Control **18** (1971), no. 4, 369–394, doi:10.1016/S0019-9958(71)90473-6.

[9] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, 625–635, doi:10.1007/978-3-030-79876-5_37.

[10] G. P. Nagy and A. Vajda, *On a conjecture on the Kasami APN function: reductions, structure theorems, a proof for $k \bmod n \in \{1, 2, n-2, n-1\}$, and exhaustive verification for $n \leq 13$*, arXiv:2608.18584v1 (2026). Every result, table and section of it cited above is numbered as in that version, the only one posted.

[11] A. Gorodilova, N. Tokareva, S. Agievich, C. Carlet, E. Gorkunov, V. Idrisova, N. Kolomeec, A. Kutsenko, R. Lebedev, S. Nikova, A. Oblaukhov, I. Pankratova, M. Pudovkina, V. Rijmen and A. Udovenko, *On the Sixth International Olympiad in Cryptography NSUCRYPTO*, J. Appl. Ind. Math. **14** (2020), no. 4, 623–647, doi:10.1134/S1990478920040031; Russian original in Diskretn. Anal. Issled. Oper. **27** (2020), no. 4, 21–57; arXiv:2005.09563.

[12] NSUCRYPTO, *Unsolved problems*, `https://nsucrypto.nsu.ru/unsolved-problems/`, accessed 28 August 2026 (the 2019 problem “Conjecture” is listed as unsolved).