WHICH APN POWER FUNCTIONS ARE COMPONENTWISE WALSH UNIFORM? THE CLASSIFICATION AT $n = 12, 13, 14, 15$, AND HOW BADLY THE OTHERS FAIL

KOREA SUPERINTELLIGENCE LABS

Abstract. Let F be an APN function on $\mathbb{F}_{2^n}$, let $S_a(F) = \{F(x)+F(x+a)\}$ be a derivative image, and for distinct nonzero v_1, v_2 let $N_F(v_1, v_2) = \#\{(x, y, z) \in S_a(F)^3 : v_1x + v_2y + (v_1 + v_2)z = 0\}$. Carlet showed that for an APN power permutation the constancy $N_F \equiv 2^{2n-3}$ is componentwise Walsh uniformity, tabulated which of the classical APN power functions have it for $3 \le n \le 11$, and left the general classification open. We continue that table. For $n = 12, 13, 14, 15$ we decide the property for *every* exponent class that is APN — three classes at $n = 12$, twenty-seven at $n = 13$, five at $n = 14$, twenty-one at $n = 15$, the lists themselves computed rather than assumed. At $n = 13$ exactly twelve of the twenty-seven hold: the six Gold classes, the five Kasami classes and $127 = 2^{(n+1)/2} - 1$; at $n = 15$ exactly eight of twenty-one. All of the affirmative verdicts are instances of results of Carlet or of exhaustive verifications of the Kasami case, and are not claimed as new; neither is the inverse-function row, which has a paper of its own. What is new is that the affirmative verdicts are the only ones: at $n = 13$ and $n = 15$ the Welch, Niho and inverse-function classes fail, Dobbertin fails at $n = 15$, and so does every compositional inverse except $2^{(n+1)/2} - 1$. $n = 15$ is the first n at which Dobbertin, Welch, Niho and the inverse function are all present and all fail. We also attach numbers to the failures, which the literature we could find does not: for each of the thirty-nine classes that fail at $n = 7, 9, 10, 11, 13$, the exact number of $\rho = v_2/v_1$ at which equidistribution is violated, out of $2^n - 2$. These show that failure is far from uniform — Niho misses at two thirds of the ρ at $n = 7$ and at all of them at $n = 13$, and a class and its compositional inverse are not comparable. Finally we give a short, self-contained proof of the affine case of Carlet's sufficient condition. Every theorem is machine-checked in Lean 4; the one classical Fourier identity through which the $n \ge 12$ verdicts are read is not, and what that costs is stated.

1. Introduction

The object. Let $n \ge 3$ and let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. For $a \in \mathbb{F}_{2^n}^*$ the derivative $D_aF(x) = F(x) + F(x+a)$ satisfies $D_aF(x) = D_aF(x + a)$, so its image has at most 2^{n-1} elements, and F is *almost perfect nonlinear* (APN) exactly when

$$S_a(F) = \{ F(x) + F(x + a) : x \in \mathbb{F}_{2^n} \}$$

has exactly 2^{n-1} elements for every $a \neq 0$. For $v_1, v_2 \in \mathbb{F}_{2^n}$ put

$$N_{F,a}(v_1, v_2) = \#\bigl\{(x, y, z) \in S_a(F)^3 : v_1x + v_2y + (v_1 + v_2)z = 0\bigr\}, \tag{1}$$

and call the pair (v_1, v_2) *admissible* when $v_1 \neq v_2$ and $v_1v_2 \neq 0$. One $\mathbb{F}_2$-linear condition should cut the 2^{3n-3} triples of $S_a(F)^3$ by a factor 2^n, so 2^{2n-3} is the count that perfect equidistribution predicts; it is also, unconditionally, the mean of $N_{F,a}$ over the admissible pairs (Lemma 2.3). We write

(2) F has property (T) $\quad :\Longleftrightarrow \quad N_{F,a}(v_1, v_2) = 2^{2n-3}$ for every $a \neq 0$ and every admissible pair.

Property (T) says that $N_{F,a}$ is *constant*, pinned at its own mean: a statement of complete additive regularity for the derivative images of F.

Carlet's question. Property (T) is not an invention of this paper. Write

$$W_F(u, v) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(vF(x)+ux)}$$

for the Walsh transform. Carlet [2] calls F *componentwise Walsh uniform* (CWU) when

$$2^{-2n} \sum_{u_1,u_2\in\mathbb{F}_{2^n}} W_F(u_1,v_1)^2\, W_F(u_2,v_2)^2\, W_F(u_1+u_2,v_1+v_2)^2 \;=\; 2^{3n} \tag{3}$$

for every pair of distinct nonzero v_1, v_2. This is his Definition 4.2, stated there for (n,m)-functions with v_1, v_2 ranging over the nonzero distinct elements of $\mathbb{F}_2^m$, and in the unnormalised form in which the sum itself equals 2^{5n}; for $m = n$ that is (3), and the arithmetic-mean normalisation used above is the one his own abstract uses. He proves (his Proposition 4.11) that for an APN power *permutation* F this is equivalent to $\#\{(x,y,z) \in \Delta_F^3 : v_1x + v_2y + v_3z = 0\} = 2^{2n-3}$ for all distinct nonzero v_1, v_2, where $\Delta_F = \{F(x)+F(x+1)+1\}$ and $v_3 = v_1+v_2$; his Definition 4.12 names that condition on Δ_F by saying that Δ_F is a *cyclic-additive difference set with Singer-like parameters*. Since Δ_F is a translate of $S_1(F)$ and the count (1) is translation invariant (Proposition 2.2), that condition is property (T) at $a = 1$, and for a power function property (T) does not depend on a at all (Proposition 2.2 again). So for APN power permutations, (T) *is* componentwise Walsh uniformity. We keep the separate name (T) because the exponents swept below include ones that are not permutations, for which we make no claim about (3); and we use the phrase "the class d is CWU at n" only as an abbreviation for "x^d has property (T) on $\mathbb{F}_{2^n}$".

Carlet's paper contains three things that this one continues rather than repeats.

- **His Proposition 4.6**: "Every APN function whose component functions are all partially-bent … is CWU. In particular, every quadratic APN function is CWU." The parenthesis elided there is the definition: for every nonzero $a, v \in \mathbb{F}_2^n$ the function $v \cdot D_aF(x)$ is either constant or balanced. In particular every Gold function has (T).
- **His Table 2** (p. 28 of the ePrint), "Componentwise Walsh uniformity of known non-quadratic infinite classes of APN power functions": the classification for $3 \le n \le 11$ over the Kasami, inverse, Welch, Niho and Dobbertin classes and — since, in his words, "the notion of CWU is not CCZ-invariant" — over the compositional inverses of the Gold, Kasami, Welch, Niho and Dobbertin functions. Its entries are the labels Quad, PB, CWU, NotCWU, Na, annotated where needed with the values of i they apply to. It records no counts, and it stops at $n = 11$.
- **His Theorem 4.22**: "For every odd n, the compositional inverse F of Gold (n,n)-function $x^{2^{(n-1)/2}+1}$ is CWU and the associated set $\Delta_F = \{F(x) + F(x+1) + 1;\ x \in \mathbb{F}_{2^n}\}$ is a cyclic-additive difference set with Singer-like parameters." The exponent of that compositional inverse is $2^{(n+1)/2} - 1$ up to a cyclotomic shift.

The Kasami row of Table 2 is left open there — "for the Kasami functions, it seems impossible to adapt Dillon–Dobbertin's proof" — and became a prize problem of the Sixth International Olympiad in Cryptography [8]. Nagy and Vajda [9] prove it for $k \bmod n \in \{1, 2, n-2, n-1\}$ and verify it exhaustively for every admissible (n,k) with $n \le 13$; a companion paper [4] verifies it at $n = 14, 15, 16, 17$. The inverse function is the subject of a paper of Göloğlu [6] whose title is *Inverse function is not component-wise uniform*; that article is paywalled and we were unable to consult it, so we neither quote its theorem nor state the range of n it covers, and nothing below rests on it. Some restriction on n there must be, since Carlet's Table 2 records CWU for the inverse function at $n = 5$. The general problem is left open in the source, verbatim:

Question 1.1 ([2])**.** "Determining precisely what are those APN (n,n)-functions which are CWU is an interesting and probably very difficult question in general, that we leave open."

What is settled here. Nothing below crosses Question 1.1; what it does is map its boundary one to four values of n further out, exhaustively, and attach numbers to the negative side of the boundary.

Write a *class* at n for a cyclotomic class $\{d \cdot 2^i \bmod 2^n - 1\}$ of exponents with x^d APN, represented by its least element. Classes are the right unit: x^{2d} is x^d followed by the Frobenius, and property (T) is invariant under that (§2.3).

- **The rows $n = 12, 13$ (Theorem 4.1) and $n = 14, 15$ (Theorem 5.1), over every APN exponent class.** There are 3, 27, 5 and 21 classes respectively — computed, not quoted —

and each of them is decided. At $n = 13$ exactly twelve hold; at $n = 15$ exactly eight; at $n = 12$ and $n = 14$ all of them do. Carlet's table has none of these rows.

- **The pattern of $n = 9, 11$ continues.** From $n = 9$ up to $n = 15$ the classes with property (T) are exactly the Gold classes, the Kasami classes, and — for odd n — the single class $2^{(n+1)/2} - 1$. The sporadic extra holders that Carlet's table shows at $n = 5$ and $n = 7$ do not reappear.
- **$n = 15$ is the first n at which Dobbertin, Welch, Niho and the inverse function are simultaneously present and simultaneously fail**; Carlet's table has Dobbertin only at $n = 5$, where it holds, and $n = 10$, where it does not.
- **Thirty-nine failure counts (Theorem 6.1).** For every one of the thirty-nine classes that fails at $n = 7, 9, 10, 11, 13$, the exact number of $\rho \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ at which equidistribution is violated, out of $2^n - 2$. We have found no such number in the literature: Carlet's table records labels and no counts. The numbers say three things the labels cannot (§6): the Niho class misses at 84 of 126 values of ρ at $n = 7$ but at all 8190 at $n = 13$; there is no monotonicity between a class and its compositional inverse; and the compositional inverses of Gold and Kasami are the least bad failures at $n = 13$, at a little over half the ρ, which is the numerical shadow of the one Gold compositional inverse that reaches zero.
- **A short proof of the affine case (Proposition 3.1).** If $S_a(F)$ is a coset of a hyperplane — as it is whenever D_aF is affine — then $8N_{F,a}(v_1, v_2) = 2^{2n}$ for every admissible pair. This is the single-direction form of Carlet's Proposition 4.6, and the mathematics is his; the proof given here is elementary and self-contained, uses no subfield or dimension argument, and carries no computation. We also record which rows of the classification it does *not* explain.

What is not new here. The affirmative half of every row past $n = 11$ is already accounted for, and we claim none of it.

- Every **Gold** entry is an instance of Carlet's Proposition 4.6 (Gold functions are quadratic), reproved in the affine form as Proposition 3.1.
- Every **Kasami** entry at $n \leq 15$ is already known for the Kasami exponent alone: at $n \leq 11$ from Carlet's table, at $n = 12, 13$ from the exhaustive verification of Nagy and Vajda [9], and at $n = 14, 15$ from the companion verification [4], which reaches $n \leq 17$; the general case is the open olympiad conjecture. The Kasami classes are recomputed here only because the scan is exhaustive.
- The entry $2^{(n+1)/2} - 1$ at $n = 13$ and $n = 15$ is an instance of Carlet's Theorem 4.22, which is proved for every odd n. It is computed here as a check on the computation, not as a result.
- The **inverse function** is the class that [6] is about; we claim nothing about it beyond the computations reported here.
- The rows $3 \leq n \leq 11$ are Carlet's data. They were recomputed from the definitions used here before anything new was claimed, and every cell agrees (Proposition 7.6); that is a check on this paper, not a contribution.

What is left, and is new, is the negative half of the rows $n = 13$ and $n = 15$ outside the inverse function, the exhaustiveness of all four rows, and the failure counts.

Provenance of the computations. Every theorem and proposition below is machine-checked in Lean 4 and is stated exactly as far as the check goes: the ranges of n, of d and of ρ in each statement are the ranges actually searched. The three lemmas of §2 are elementary and are proved in the text. Two conventions are used throughout and are stated once here. First, the family names attached to exponent classes in the tables below — Gold $2^k + 1$, Kasami $4^k - 2^k + 1$, Welch $2^m + 3$, Niho, the inverse function $2^n - 2$, Dobbertin, and the compositional inverses of these, for which see [3] — are matched to classes by the elementary arithmetic $d\,d' \equiv 2^j \pmod{2^n - 1}$, a Gold or Kasami class being written with the smaller of the two values of k that produce it; that matching is a labelling, made outside the formal development, and no statement depends on it — the machine-checked statements quantify over exponent classes and name no family. Second, the verdicts at $n \geq 12$ are stated in the character form $Z \equiv 0$ and become statements about $N_{F,a}$ through the standard identity (4), which is not formalised here; §7 says exactly what that costs and what is done instead at $n \le 11$.

2. Preliminaries

2.1. **The field model.** All computations are carried out in the concrete model $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/(f_n)$ with f_n the lexicographically smallest irreducible binary polynomial of degree n and $\alpha = x \bmod f_n$. 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 2 denotes α and 3 denotes $\alpha+1$. Nothing depends on the choice of f_n: 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 $\mathbb{F}_{2^n}^*$ generates, and that the trace $\mathrm{Tr}(x) = \sum_{i<n} x^{2^i}$ is computed correctly are themselves machine-checked (Proposition 7.3).

2.2. **Derivative images, and the APN criterion.** For a power function the direction a is idle: $S_a(x^d) = \{a^d(y^d + (y+1)^d) : y \in \mathbb{F}_{2^n}\} = a^d\, S_1(x^d)$ after the substitution $x = ay$. The fibres of D_1F are unions of pairs $\{x, x+1\}$, so $|S_1(F)| \le 2^{n-1}$ with equality exactly when D_1F is 2-to-1. Hence:

Lemma 2.1. *x^d is APN on $\mathbb{F}_{2^n}$ if and only if $|S_1(x^d)| = 2^{n-1}$.*

This is the test the exhaustive scans use, so that nothing has to be assumed about which exponents are APN.

2.3. **Three invariances, and the reduction to one parameter.**

Proposition 2.2 (invariance of the count)**.** *Let K be a finite field of characteristic 2, $S \subseteq K$ finite, $v_1, v_2 \in K$ and $N_S(v_1,v_2) = \#\{(x,y,z) \in S^3 : v_1x + v_2y + (v_1+v_2)z = 0\}$. Then*

(a) *$N_{S+c}(v_1,v_2) = N_S(v_1,v_2)$ for every $c \in K$;*
(b) *$N_{tS}(v_1,v_2) = N_S(v_1,v_2)$ for every $t \ne 0$;*
(c) *$N_S(tv_1,tv_2) = N_S(v_1,v_2)$ for every $t \ne 0$.*

Part (a) holds because the three coefficients of the linear form sum to 0 in characteristic 2, so a constant shift of all three variables cancels; parts (b) and (c) are the substitutions $x \mapsto t^{-1}x$ and the homogeneity of the form. These are folklore — the translation half is stated in [2, §4.4] — and are recorded because they are what makes the computation finite and what identifies the object of this paper with the Δ_F of [2] and [4]: by (a), $N_{\Delta_F} = N_{S_1(F)}$. By (b) and $S_a(x^d) = a^dS_1(x^d)$, property (T) for a power function need only be checked at $a = 1$. By (c), $N_S(v_1,v_2) = N_S(1,\rho)$ with $\rho = v_2/v_1$, so all $(2^n-1)(2^n-2)$ admissible pairs collapse to the 2^n-2 values $\rho \in \mathbb{F}_{2^n} \setminus \{0,1\}$. Finally, $S_1(x^{2d}) = S_1(x^d)^2$, and squaring the equation $v_1x + v_2y + v_3z = 0$ carries a solution in S^3 to a solution in $(S^2)^3$ with the coefficients v_i^2, which again sum to zero; since $v \mapsto v^2$ permutes $\mathbb{F}_{2^n}$ and preserves admissibility, property (T) depends only on the cyclotomic class of d.

Throughout, then, $N(1,\rho)$ is the only quantity to compute, and a *cell* is a pair (n,d) with d least in its class.

Lemma 2.3 (the mean)**.** *If $|S| = 2^{n-1}$ then the average of $N_S(v_1,v_2)$ over the $(2^n-1)(2^n-2)$ admissible pairs is exactly 2^{2n-3}.*

Proof. Fix $(x,y,z) \in S^3$ and count the admissible pairs it contributes to, i.e. those with $v_1(x+z) + v_2(y+z) = 0$. If $x = z$ and $y = z$, every admissible pair qualifies. If exactly one of $x = z$, $y = z$ holds, the condition forces $v_2 = 0$ or $v_1 = 0$ and none qualifies. If $x \ne z$ and $y \ne z$, then $v_2 = v_1(x+z)/(y+z)$ is determined and nonzero, and $v_1 \ne v_2$ holds exactly when $x \ne y$; so 2^n-1 pairs qualify if x,y,z are pairwise distinct and none otherwise. With $s = |S|$ the total is $s(2^n-1)(2^n-2) + s(s-1)(s-2)(2^n-1)$, and dividing by $(2^n-1)(2^n-2) = (2^n-1)(2s-2)$ gives $s + s(s-2)/2 = 2^{n-1} + 2^{2n-3} - 2^{n-1} = 2^{2n-3}$. □

2.4. **The character route.** For finite $S \subseteq \mathbb{F}_{2^n}$ put $T(\lambda) = \sum_{s\in S}(-1)^{\mathrm{Tr}(\lambda s)}$. Expanding the indicator of $v_1x + v_2y + v_3z = 0$ as $2^{-n}\sum_\lambda(-1)^{\mathrm{Tr}(\lambda(v_1x+v_2y+v_3z))}$ gives, for every finite S and all v_1, v_2 with $v_3 = v_1 + v_2$,

$$2^n\, N_S(v_1, v_2) = |S|^3 + Z(v_1, v_2), \qquad Z(v_1, v_2) = \sum_{\lambda\neq 0} T(\lambda v_1)T(\lambda v_2)T(\lambda v_3). \tag{4}$$

By Proposition 2.2(c) we write $Z(\rho) = Z(1, \rho) = \sum_{\lambda\neq 0} T(\lambda)T(\lambda\rho)T(\lambda(1 + \rho))$. When $|S| = 2^{n-1}$, so that $|S|^3 = 2^{3n-3} = 2^n \cdot 2^{2n-3}$, identity (4) turns property (T) into

$$Z(\rho) = 0 \qquad \text{for every } \rho \in \mathbb{F}_{2^n} \setminus \{0, 1\}. \tag{5}$$

Criterion (5) costs 2^{2n} elementary steps for a whole sweep against the 2^{3n-3} of a direct triple count, which is the difference between $n \le 11$ and $n \le 15$. Identity (4) is classical Fourier inversion and is *not* proved in the formal development; §7 records what is done instead.

3. The affine case

The one structural theorem in this paper is the following, which needs no finiteness beyond $|K| < \infty$ and no computation at all.

Proposition 3.1 (the affine case)**.** *Let K be a finite field of characteristic 2, let $f : K \to \mathbb{F}_2$ be a nonzero additive map and $S = \ker f$. Then for every pair of distinct nonzero $v_1, v_2 \in K$,*

$$8\, N_S(v_1, v_2) = |K|^2.$$

Consequently, by Proposition 2.2(a), the same holds for every coset of $\ker f$*; so if F is APN on $\mathbb{F}_{2^n}$ and $S_a(F)$ is a coset of a hyperplane for every $a \neq 0$ — which is exactly the* crooked *property in the sense of* [5]*, and holds in particular whenever F is quadratic — then F has property (T).*

Proof sketch. Put $v_3 = v_1 + v_2 \neq 0$, $\sigma = v_1/v_3$, $\tau = v_2/v_3$, so $\sigma + \tau = 1$ and $\sigma, \tau \notin \{0, 1\}$. In the equation $v_1x + v_2y + v_3z = 0$ the variable z is determined by (x, y), and $z \in S$ reads $f(\sigma x + \tau y) = 0$, i.e. $f(\sigma x) = f(\tau y)$ because f is additive and takes values in $\mathbb{F}_2$. Hence

$$N_S(v_1, v_2) = |A|\,|B| + |A'|\,|B'|,$$

where A, A' are the sets of $x \in S$ with $f(\sigma x) = 0$, resp. $\neq 0$, and B, B' the same for y with τ. Write $u = f \circ \mu_\sigma$ and $w = f \circ \mu_\tau$ for the compositions with multiplication by σ and τ. Each of f, u, w is a nonzero additive map to $\mathbb{F}_2$ — nonzero because multiplication by a nonzero scalar is onto — and $f \neq u$, $f \neq w$: if $f \circ \mu_\sigma = f$ then $f \circ \mu_{1+\sigma} = 0$, and $1 + \sigma \neq 0$ forces $f = 0$. The content is then the following count, which needs no subfield and no dimension argument: two distinct nonzero additive maps $K \to \mathbb{F}_2$ have exactly $|K|/4$ common zeros. Indeed each of the four joint fibre sizes a, b, c, d of (u, w) satisfies $2(a + b) = 2(a + c) = 2(a + d) = a + b + c + d = |K|$, since a nonzero additive map to $\mathbb{F}_2$ is balanced and so is the sum of two distinct ones; whence $4a = |K|$. Applying this to the pairs (f, u) and (f, w) gives $|A| = |B| = |K|/4$ and $|A'| = |B'| = |K|/2 - |K|/4 = |K|/4$, so $N_S = 2(|K|/4)^2 = |K|^2/8$. □

Proposition 3.1 is the single-direction form of Carlet's Proposition 4.6 quoted in §1; the mathematics is his, and the proof above is offered only as an elementary route to it, one that formalises with no finite data. What matters for the classification is where it stops.

Proposition 3.2 (what the affine case does not cover)**.** *In the model of §2.1, S_1 is a coset of an $\mathbb{F}_2$-subspace for the Gold classes $d = 3, 5, 9$ at $n = 7$ and $d = 33$ at $n = 11$, and for the non-power Budaghyan–Carlet–Leander function $x^3 + \mathrm{Tr}(x^9)$ at $n = 7$ and $n = 9$; it is* not *a coset of a subspace for the Kasami classes $d = 13$ at $n = 7$ and $n = 11$, for the Gold compositional inverses $d = 15$ at $n = 7$ and $d = 63$ at $n = 11$, or for the inverse function at $n = 7$.*

Of the classes that fail the affine test here, the Kasami and Gold-inverse ones nevertheless have property (T) at those n (Proposition 7.6), while the inverse function does not. So Proposition 3.1 explains the Gold column of every row below and nothing else: the Kasami column is the open olympiad conjecture, and the $2^{(n+1)/2}-1$ column is Carlet's Theorem 4.22, proved by an argument of a different kind. This is what keeps the tables honest, and in particular it is why the Budaghyan–Carlet–Leander row below is not evidence of a new phenomenon: that function is quadratic, so Proposition 3.1 already covers it.

4. The classification at $n = 12$ and $n = 13$

Theorem 4.1 (the rows $n = 12, 13$)**.** *Let $n = 12$. There are exactly three exponents d with $1 \le d \le 2^n - 2$ that are least in their cyclotomic class and satisfy $|S_1(x^d)| = 2^{n-1}$, namely $d = 3, 33, 159$, and for each of them $Z(\rho) = 0$ at every one of the $2^{12} - 2 = 4094$ values of ρ.*

Let $n = 13$. There are exactly twenty-seven such exponents. For twelve of them, namely

$$3,\ 5,\ 9,\ 13,\ 17,\ 33,\ 57,\ 65,\ 127,\ 191,\ 241,\ 287,$$

$Z(\rho) = 0$ at every one of the $2^{13} - 2 = 8190$ values of ρ. For the remaining fifteen, namely

$$67,\ 71,\ 171,\ 347,\ 367,\ 635,\ 723,\ 911,\ 1243,\ 1245,\ 1453,\ 1639,\ 1691,\ 2731,\ 4095,$$

there is a ρ with $Z(\rho) \neq 0$.

Corollary 4.2. *Through* (4)*, the twelve classes listed have property* (T) *at $n = 13$ and the other fifteen do not; all three classes at $n = 12$ have it.*

In the labelling of §1 the twelve are: the six Gold classes $3, 5, 9, 17, 33, 65$; the five Kasami classes $13, 57, 191, 241, 287$ other than $k = 1$, which coincides with Gold; and $127 = 2^{(13+1)/2} - 1$, the compositional inverse of the Gold permutation x^{2^6+1}. The fifteen are the Welch class 67, the Niho class 71, the inverse function 4095, and the twelve compositional inverses of Gold, Kasami, Welch and Niho classes. At $n = 12$ the three classes are the Gold classes 3 and 33 and the Kasami class 159: at even n in this range the classical list has nothing else to offer, since the inverse function is APN only for n odd, Welch and Niho need n odd, and $5 \nmid 12$.

Three readings of the row $n = 13$ are worth stating.

It is sharp on both sides. The Welch class shows that not every APN power function has property (T), and the Kasami class 13 together with the Gold-inverse class 127 shows that the functions with affine derivatives are not the only ones that do — the Kasami class 13 and the class $2^{(n+1)/2} - 1$ both fail the affine hypothesis at $n = 7$ and at $n = 11$ (Proposition 3.2). The affine test was run at $n = 7, 9, 11$ only, so its verdict at $n = 13$ is not part of the formal development.

It confirms the pattern of $n = 9$ and $n = 11$ one row past the published table. From $n = 9$ upward, the classes with property (T) are exactly the Gold classes, the Kasami classes and the single class $2^{(n+1)/2} - 1$ for odd n; the sporadic extra holders in Carlet's table — the inverse function and Dobbertin at $n = 5$, the Welch class 11 and the Gold-inverse class 27 at $n = 7$ — do not recur at $n = 9, 11, 13, 15$.

It is a table of the failure of CCZ-invariance. The class 241 (Kasami, $k = 4$) has property (T) and its compositional inverse 171 does not; 65 (Gold, $k = 6$) has it and so does its inverse 127; 3 (Gold, $k = 1$) has it and its inverse 2731 does not. Carlet's reason for including compositional inverses in Table 2 was exactly this, and the row makes it visible on a scale his table could not.

5. The rows $n = 14$ and $n = 15$

Theorem 5.1 (the rows $n = 14, 15$)**.** *The exponents d with $1 \le d \le 2^n - 2$ that are least in their cyclotomic class and satisfy $|S_1(x^d)| = 2^{n-1}$ are exactly the following. For $n = 13$ there are twenty-seven of them:*

$$3,\ 5,\ 9,\ 13,\ 17,\ 33,\ 57,\ 65,\ 67,\ 71,\ 127,\ 171,\ 191,\ 241,\ 287,$$
$$347,\ 367,\ 635,\ 723,\ 911,\ 1243,\ 1245,\ 1453,\ 1639,\ 1691,\ 2731,\ 4095.$$

For $n = 14$ there are five, namely 3*,* 9*,* 33*,* 57 *and* 543*. For $n = 15$ there are twenty-one:*

$$3,\ 5,\ 13,\ 17,\ 129,\ 131,\ 241,\ 255,\ 383,\ 1371,\ 1935,$$
$$2033,\ 2523,\ 3657,\ 3671,\ 4791,\ 4815,\ 5851,\ 6555,\ 10923,\ 16383.$$

For each of the five exponents at $n = 14$, $Z(\rho) = 0$ at every one of the $2^{14} - 2 = 16382$ values of ρ. At $n = 15$ the same holds for exactly eight of the twenty-one exponents, namely 3*,* 5*,* 13*,* 17*,* 129*,* 241*,* 255 *and* 383*, each swept over all $2^{15} - 2 = 32766$ values of ρ; for each of the other thirteen, namely*

$$131,\ 1371,\ 1935,\ 2033,\ 2523,\ 3657,\ 3671,$$
$$4791,\ 4815,\ 5851,\ 6555,\ 10923,\ 16383,$$

there is a ρ with $Z(\rho) \neq 0$.

Again by (4): all five classes at $n = 14$ have property (T), and at $n = 15$ exactly eight of the twenty-one do. The eight are the Gold classes $3, 5, 17, 129$, the Kasami classes $13, 241, 383$, and $255 = 2^{(15+1)/2} - 1$. The thirteen that fail are the Welch class 131, the Niho class 2033, the Dobbertin class 3657 (which exists because $5 \mid 15$), the inverse function 16383, and nine compositional inverses — of Welch (4815), of Niho (1371), of Dobbertin (5851), of Gold $(1935, 6555, 10923)$ and of Kasami $(2523, 3671, 4791)$.

Remark 5.2. $n = 15$ is the first n at which Dobbertin, Welch, Niho and the inverse function are all present and all fail. Carlet's Table 2 carries Dobbertin at $n = 5$, where it holds, and at $n = 10$, where it does not; $n = 15$ is the next n divisible by 5 and is odd, so it is the first at which the Dobbertin class meets the three odd-n classes.

Remark 5.3. Every one of the thirteen affirmative verdicts in Theorem 5.1 — five at $n = 14$, eight at $n = 15$ — is an instance of a known result: Gold by Carlet's Proposition 4.6, Kasami by the verification of [4], and 255 by Carlet's Theorem 4.22. The same is true of all fifteen affirmative verdicts of Theorem 4.1 — three at $n = 12$ and twelve at $n = 13$ — with [9] in place of [4] as the source for the Kasami classes there. The new content of the two theorems is the negative half and the exhaustiveness: that the lists of classes are complete, and that everything not in the three known columns fails.

Remark 5.4. The computed class lists contain nothing outside the classical families: at every n with $5 \leq n \leq 15$, each class in the list is a Gold, Kasami, Welch, Niho, Dobbertin or inverse-function class, or the compositional inverse of one. That match is the labelling of §1, arithmetic carried out outside the formal development, so what is machine-checked is the lists themselves and not their naming. Whether the classical list of APN exponents is complete for every n is a long-standing open question [3]; nothing here bears on it past $n = 15$.

6. How badly the failures fail

Carlet's Table 2 records CWU or NotCWU and prints no count. Define

$$\mathrm{off}(n, d) = \#\{\rho \in \mathbb{F}_{2^n} \setminus \{0, 1\} : Z(\rho) \neq 0\} \ \in\ \{0, 1, \ldots, 2^n - 2\},$$

so that $\mathrm{off}(n, d) = 0$ is property (T) and $\mathrm{off}(n, d) = 2^n - 2$ says that equidistribution fails at every ρ. When $|S_1| = 2^{n-1}$, identity (4) makes $Z(\rho) \neq 0$ the same condition as $N(1, \rho) \neq 2^{2n-3}$, so off counts the ρ at which the triple count misses its target; Proposition 7.2 recomputes some of these counts from the triples themselves.

Theorem 6.1 (the failure counts)**.** *The values of* $\mathrm{off}(n, d)$ *are as follows, for every one of the thirty-nine classes d that fails at $n = 7, 9, 10, 11, 13$.*

$n = 7$

29	*Niho*	84 / 126
43	*inverse of Gold* $k = 1$	126 / 126
63	*inverse function*	126 / 126

$n = 9$

19	*Welch* = *Niho*	342 / 510
27	*its compositional inverse*	510 / 510
59	*inverse of Kasami* $k = 2$	504 / 510
87	*inverse of Kasami* $k = 4$	402 / 510
103	*inverse of Gold* $k = 2$	432 / 510
171	*inverse of Gold* $k = 1$	270 / 510
255	*inverse function*	510 / 510

$n = 10$

213	*Dobbertin*	962 / 1022

$n = 11$

35	*Welch*	1848 / 2046
43	*inverse of Kasami* $k = 4$	1188 / 2046
107	*inverse of Niho*	1980 / 2046
117	*inverse of Welch*	2046 / 2046
151	*inverse of Kasami* $k = 5$	2046 / 2046
231	*inverse of Gold* $k = 3$	1122 / 2046
249	*Niho*	1980 / 2046
315	*inverse of Kasami* $k = 2$	2046 / 2046
365	*inverse of Gold* $k = 4$	1254 / 2046
411	*inverse of Gold* $k = 2$	1716 / 2046
413	*inverse of Kasami* $k = 3$	2046 / 2046
683	*inverse of Gold* $k = 1$	1518 / 2046
1023	*inverse function*	1848 / 2046

$n = 13$

67	*Welch*	7566 / 8190	1243	*inverse of Gold* $k = 5$	5070 / 8190
71	*Niho*	8190 / 8190	1245	*inverse of Kasami* $k = 6$	8034 / 8190
171	*inverse of Kasami* $k = 4$	4992 / 8190	1453	*inverse of Gold* $k = 4$	5538 / 8190
347	*inverse of Niho*	8112 / 8190	1639	*inverse of Gold* $k = 2$	5538 / 8190
367	*inverse of Welch*	8112 / 8190	1691	*inverse of Kasami* $k = 5$	8190 / 8190
635	*inverse of Kasami* $k = 2$	8190 / 8190	2731	*inverse of Gold* $k = 1$	4836 / 8190
723	*inverse of Kasami* $k = 3$	8112 / 8190	4095	*inverse function*	8112 / 8190
911	*inverse of Gold* $k = 3$	5070 / 8190			/

Moreover $\mathrm{off}(n, d) = 0$ *for* $(n, d) = (11, 63), (11, 143), (13, 13), (13, 127), (13, 241)$.

The last line is a control rather than an addition: for five classes that do have property (T) the same counter is run and returns 0, so a bug that made off count nothing would show up.

Three things these numbers say that the labels cannot.

Failure is not uniform across the zoo, and it deepens with n. The Niho class misses at 84 of 126 values of ρ at $n = 7$ — exactly two thirds — at 1980 of 2046 at $n = 11$, and at all 8190 at $n = 13$. A label reading NotCWU covers all three.

There is no monotonicity between a class and its compositional inverse. At $n = 13$ the Welch class fails at 7566 values and its compositional inverse at 8112; the Niho class fails at all 8190 and its inverse at 8112. At $n = 9$ the Welch–Niho class fails at 342 and its inverse at all 510. Neither direction of comparison holds in general.

The compositional inverses of Gold and Kasami are the least bad failures. At $n = 13$ the two smallest counts are 4836 (inverse of Gold, $k = 1$) and 4992 (inverse of Kasami, $k = 4$), at a little over half the ρ; the six smallest are all inverses of Gold or Kasami classes. Exactly one Gold compositional inverse at $n = 13$ reaches 0, namely $127 = 2^{(n+1)/2} - 1$, and the numbers show the others crowding closer to it than any other family does. Whether that is evidence of anything is exactly Question 1.1.

7. What the computations rest on

7.1. The searches. Every verdict above is one of three finite searches, all run in the model of §2.1.

- *The class list.* For each d with $1 \le d \le 2^n - 2$ that is least in its cyclotomic class, build the value table of x^d (2^n entries, read off a discrete logarithm table), form S_1, and keep d when $|S_1| = 2^{n-1}$. Cost 2^n per representative; at $n = 15$ there are 2185 representatives.
- *The character sweep.* For a kept d, tabulate $T(\lambda)$ for all λ and evaluate $Z(\rho)$ for every $\rho \in \mathbb{F}_{2^n} \setminus \{0, 1\}$, each $Z(\rho)$ being a sum of $2^n - 1$ products; total $\approx 2^{2n}$ steps. A sweep that returns true has examined all $2^n - 2$ values of ρ; a sweep that returns false stops at the first bad ρ. Theorem 4.1 runs $3+27$ such sweeps and Theorem 5.1 runs $5+21$; the eight affirmative sweeps at $n = 15$ examine 32766 values of ρ each, about $8.6 \cdot 10^9$ term evaluations in total.

- *The direct count.* $N(1, \rho)$ counted over S_1^3 by enumerating (x, y) and testing membership of the determined z: $|S|^2 = 2^{2n-2}$ steps per ρ, 2^{3n-3} for a full sweep. That is affordable exhaustively to $n = 11$ and at single values of ρ to $n = 15$.

7.2. **The identity (4), and the character-free route.** Theorems 4.1, 5.1 and 6.1 are statements about Z; they become statements about N through (4), which is classical but is not proved in the formal development. Two things are done about that.

Proposition 7.1 (the identity, tested where it can fail)**.** *Identity* (4)*, as an equality of integers, holds at the sampled cells* $(n, d, \rho) = (9, 9, 252)$, $(9, 57, 2)$ *and* $(10, 33, 5)$*, where* x^d *is* not *APN, and at* $(7, 63, 2)$*,* $(11, 1023, 2)$*,* $(13, 4095, 2)$*,* $(13, 13, 2)$ *and* $(13, 127, 2)$*, where it is. Moreover* $|S_1(x^9)| = 64$ *at* $n = 9$ *and there* $N(1, 252) = 4096$ *and* $Z(252) = 1835008$.

The inadmissible cells are the ones with content. There $|S| \neq 2^{n-1}$, so the right-hand side of (4) is not 2^{3n-3}, both sides are large numbers depending on ρ, and an incorrect identity would not survive: at $(9, 9, 252)$ one has $2^9 \cdot 4096 = 64^3 + 1835008$ exactly, while the constant $2^{2n-3} = 32768$ is wrong and the naive reading "N misses 2^{2n-3} by $Z/2^n$" gives 36352, wrong by a factor of nine. So the constant 2^{2n-3} in every statement above carries the hypothesis $|S| = 2^{n-1}$, and that hypothesis is checked — it is the APN test of Lemma 2.1, run as part of every class list — rather than assumed.

Proposition 7.2 (the same verdicts with no characters)**.** *Counted directly over* S_1^3*, with no use of* (4)*: at* $\rho = 2$*,* $N(1, \rho)$ *equals* 2042 *for* $(n, d) = (7, 63)$ *and* $(7, 126)$*,* 32576 *for* $(9, 19)$*,* 524278 *for* $(11, 1023)$*,* 8388992 *for* $(13, 67)$*,* 8388760 *for* $(13, 71)$*,* 8388630 *for* $(13, 4095)$*,* 134220288 *for* $(15, 131)$ *and* 134217646 *for* $(15, 16383)$*; the targets* 2^{2n-3} *are* 2048*,* 32768*,* 524288*,* 8388608 *and* 134217728*, and none of the nine values equals its target. Sweeping every* ρ *directly,* $\#\{\rho : N(1, \rho) \neq 2^{2n-3}\}$ *equals* 84 *and* 126 *and* 126 *for* $(7, 29), (7, 63), (7, 43)$ *and* $342, 510, 510$ *for* $(9, 19), (9, 27), (9, 255)$*; and* $N(1, \rho) = 2^{2n-3}$ *at every* ρ *for* $(7, 11), (7, 13), (7, 15), (7, 23), (7, 27)$*,* $(9, 13), (9, 31), (9, 47)$*,* $(11, 63)$ *and* $(11, 143)$*.*

A single line of the first list refutes property (T) for that class at that n with no Fourier analysis and no appeal to any published reduction: the count is over a set of 2^{n-1} field elements and it is not the number it would have to be. In particular the negative verdicts at $n = 13$ for the Welch, Niho and inverse classes and at $n = 15$ for the Welch and inverse classes — cells that lie past Carlet's table — do not depend on (4) at all. The second and third lists reproduce, with no characters, the failure counts of Theorem 6.1 at $n = 7, 9$ and the affirmative verdicts of Carlet's table at $n \leq 11$ including the Kasami and Gold-inverse rows. Formalising (4) over the concrete model — that is, proving $\sum_\lambda (-1)^{\mathrm{Tr}(\lambda w)} = 2^n [w = 0]$ there — would make the $n \geq 12$ statements unconditional; it has not been done.

7.3. **The model, the executed sum, and the controls.**

Proposition 7.3 (the field model)**.** *For every* n *with* $5 \leq n \leq 15$*,* $\mathbb{F}_2[x]/(f_n)$ *is a field with* 2^n *elements. For* $n \in \{5, 7, 9, 10, 11, 12, 13, 14, 15\}$ *the tabulated element* g *generates* $\mathbb{F}_{2^n}^*$*, and* Tr *takes values in* $\{0, 1\}$ *and equals the parity-mask formula at every point. For* $n \in \{5, 6, 7\}$ *the shift-and-xor product is commutative and associative and distributes over addition on all* 2^{3n} *triples. The discrete-logarithm power table agrees entry by entry with square-and-multiply at twelve sampled pairs* (n, d) *with* $7 \leq n \leq 15$*, and the two evaluations of* T *agree at every* λ *at six sampled cells with* $7 \leq n \leq 11$.

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. Both 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 $x^6 + x^3 + 1$.

Proposition 7.4 (the executed sum is the stated sum)**.** *The skipping accumulator — in which a term of* $Z(\rho)$ *whose first or second factor vanishes is dropped — computes the plain sum, for all* *values of its arguments, and the ρ-loop built from it returns the same Boolean as the ρ-loop built from the plain sum, again for all values of its arguments. In particular the sweep that is executed for a single exponent agrees with the plain-sum sweep for every n, every function, every exponent and every direction.*

This is proved by induction, with no computation; it is the one place where the code that runs differs from the sum that is written, and skipping is worth about a factor of three because T vanishes on roughly half of $\mathbb{F}_{2^n}^*$ in the nondegenerate cases.

Proposition 7.5 (negative controls)**.** (a) *The constant is pinned from both sides and off by one: the direct sweep at $(n,d)=(8,3)$ succeeds against $2^{2n-3}=8192$ and fails against 16384, 4096, 8193 and 8191; at $(9,13)$ it succeeds against 32768 and fails against 65536 and 16384. The character sweep rejects $Z\equiv 1$ at $(7,13)$ and $(11,63)$ and $Z\equiv -1$ at $(7,13)$.*

(b) *The hypothesis "v_1, v_2 distinct and nonzero" is not idle: at $(8,3)$ the count is $16384=2^{2n-2}$ at the excluded pairs $v_1=v_2$ and $v_2=0$, twice the value 8192 it takes at an admissible pair.*

(c) *The APN size is not idle: $|S_1|=64$ at $(9,9)$ and $(9,57)$, 32 at $(10,33)$ and 256 at $(12,17)$ — against $2^{n-1}=256,256,512,2048$ — and at all four cells the sweep returns* false.

(d) *The field test rejects reducible moduli of the right degree and accepts an irreducible one that is not lexicographically smallest.*

(e) *The classification is refuted in both directions at $n=13$: the Welch class 67 fails, so not every APN power function has property (T); the Kasami class 13 and the Gold-inverse class 127 hold, so the functions with affine derivatives are not the only ones that do.*

7.4. **Carlet's table, reproduced.** Finally, before anything new was claimed, the published data was recomputed from the definitions used here.

Proposition 7.6 ([2, Table 2] reproduced, exhaustively)**.** *For $n=5,6,7,8,9,10,11$ the full list of exponent classes with $|S_1|=2^{n-1}$, each with the verdict of the complete sweep over all 2^n-2 values of ρ, is computed; the lists have $5,1,11,3,13,4,23$ entries. The classes with $Z\equiv 0$ are: all five at $n=5$; 3 at $n=6$; $3,5,9,11,13,15,23,27$ at $n=7$; $3,9,39$ at $n=8$; $3,5,13,17,31,47$ at $n=9$; $3,9,57$ at $n=10$; and $3,5,9,13,17,33,57,63,95,143$ at $n=11$. In addition, the non-power Budaghyan–Carlet–Leander function $x^3+\mathrm{Tr}(x^9)$ [1] has $Z\equiv 0$ at $n=7$ for the directions $a=1,2,3,5$, at $n=8$ and $n=11$ for $a=1$, and at $n=9$ for $a=1,7$.*

Every cell agrees with Carlet's Table 2, including his per-i annotation that among the Gold compositional inverses exactly $i=(n-1)/2$ is CWU at $n=9$ and $n=11$ (and $i\in\{2,3\}$ at $n=7$). This is his data, recomputed and certified, not new mathematics; its role here is that of a compute-first-values gate, passed before the rows past $n=11$ were claimed. Note that the form is stronger than the table it reproduces: the scan runs over every APN exponent class rather than over the named families, so the agreement includes the statement that in this range the named families are all there is — a statement that rests on the labelling of §1 as well as on the scan.

8. Verification

Every theorem and proposition in this paper is formally verified in Lean 4 [7]; the development contains no `sorry` and no hand-written axiom, and it builds against *Mathlib*, although the evaluation core is written against Lean's built-in prelude alone so that it can be compiled to a shared object and executed as native code by the proof checker. Propositions 2.2 and 3.1 are proved abstractly, over an arbitrary finite field of characteristic 2, and carry no finite data at all: their axiom footprint is the three standard axioms of *Mathlib* developments, with no evaluation axiom. Proposition 7.4, which identifies the sum that is executed with the sum that is stated, is proved by induction and needs only the two propositional axioms, without the axiom of choice. Everything else — Theorems 4.1, 5.1, 6.1 and Propositions 3.2, 7.1, 7.2, 7.3, 7.5, 7.6 — is a finite search delegated to compiled evaluation, and the axiom footprint of each such statement is one propositional axiom together with the single evaluation axiom generated for it. The searches are the ones described in §7. Lemmas 2.1 and 2.3, and the elementary reductions of §2.3 that leave ρ and the cyclotomic class of d as the only parameters, are proved in the text rather than in the formal development; Corollary 4.2, which is the only corollary here, and the corresponding reading of Theorem 5.1 in terms of N, pass through identity (4), which is not formalised. Every table quoted here was produced first by an independent implementation of the same definitions in C and only then stated and checked formally, so that the formal run re-checks a known answer rather than searching for one. Repository reference to be added at submission.

9. What is open

Question 1.1 is untouched. Three smaller things are now visible.

The next rows. $n = 16$ has only Gold and Kasami classes and is cheap; $n = 17$ has roughly thirty-five classes, of which about half are expected to hold, and is the first row where the cost of the affirmative sweeps becomes the binding constraint. Neither is done here.

The symmetry of the sweep. $N(1, \rho)$ is invariant under $\rho \mapsto 1/\rho$ and $\rho \mapsto 1 + \rho$, so the ρ-sweep carries a sixfold redundancy that the computation does not exploit. Exploiting it is worth a factor of six and would put $n = 17$ and $n = 18$ within reach.

The shape of the boundary. From $n = 9$ to $n = 15$ the answer is: Gold, Kasami, and $2^{(n+1)/2} - 1$. Two of the three columns are theorems — Carlet's Proposition 4.6 and his Theorem 4.22 — and the third is the olympiad conjecture, verified in [9] and [4]. What is missing is any reason why nothing else should appear, and the failure counts of §6 are the only quantitative data we have found bearing on it. The cheapest experiment that Carlet's table cannot supply would be a non-quadratic, non-power APN function; the only non-power function carried here, $x^3 + \mathrm{Tr}(x^9)$, is quadratic and is therefore already covered by Proposition 3.1.

References

[1] L. Budaghyan, C. Carlet and G. Leander, *Constructing new APN functions from known ones*, Finite Fields Appl. **15** (2009), no. 2, 150–159, doi:10.1016/j.ffa.2008.10.001; preprint, from which the numbering here is taken: IACR Cryptology ePrint Archive 2007/063, version 20070523:155707. The function used here is $x^3 + \mathrm{Tr}(x^9)$; it is quadratic, it is APN on $\mathbb{F}_{2^n}$ for every n (their Corollary 1), it is EA-inequivalent to every power function for $n \geq 7$ with $n > 2p$, where p is the smallest integer larger than 1, different from 3 and coprime to n (their Theorem 2 and Corollary 2), and at $n = 7$ it is CCZ-inequivalent to every power function (their Corollary 3). CCZ-inequivalence to every power function in general is their Conjecture 1, not a theorem.

[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, from which all numbering and all quotations above are taken: IACR Cryptology ePrint Archive 2017/528, version 20170918:184412. In that version, Definition 4.2 is the definition of CWU, Propositions 4.6 and 4.11 and Definition 4.12 and Theorem 4.22 are as quoted, and Table 2 is on p. 28. The published version was not accessible to us and its numbering may differ.

[3] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, Cambridge, 2020, xiv+562 pp., ISBN 978-1-108-47380-4, doi:10.1017/9781108606806. Standard reference for the classical APN exponents — Gold $2^k + 1$, Kasami $4^k - 2^k + 1$, Welch $2^m + 3$, Niho, the inverse function $2^n - 2$ and Dobbertin — used above only for their names and for the status of the question whether that list is complete.

[4] Korea Superintelligence Labs, *The NSUCRYPTO 2019 conjecture on the Kasami APN function: exhaustive verification for $n \leq 17$, the weight distributions it computes, and an outlier at $n = 15$*, companion paper (2026). Its archival identifier will be supplied at submission, together with that of the present paper.

[5] C. Carlet and D. Thornburgh, *Resolving a conjecture on quadratic APN functions and a new quadratic (n, n)-function associated to crooked functions*, arXiv:2608.23888v1 (2026). Source of the term *crooked* as used above: "An (n, n)-function F is *crooked* if the image of $D_a F$ is an affine hyperplane … for all nonzero $a \in \mathbb{F}_2^n$." All known crooked functions are quadratic; whether a non-quadratic one exists is open.

[6] F. Göloğlu, *Inverse function is not component-wise uniform*, Cryptogr. Commun. **12** (2020), no. 6, 1179–1194, doi:10.1007/s12095-020-00441-3. Cited by title only; it was not accessible to us.

[7] 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.

[8] 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; arXiv:2005.09563.

[9] 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).