Exact Five-Class Paley Offsets and Sharper Nonlinearity Bounds Exceeding the Patterson–Wiedemann Direct-Sum Threshold

Filipe Martins Vono [1] André Oliveira Naufel de Toledo [1]
Valéria Gonzaga Santos [2]

21 November 2026

[1] Centro Universitário de Belo Horizonte (UniBH), Belo Horizonte, Brazil
[2] American Global Tech University (AGTU)
0009-0009-4994-8533 0000-0002-0619-6820 0009-0009-1333-2518
Correspondence: contatofilipevono@gmail.com

Abstract

In a recent landmark preprint (IACR ePrint 2026/2680), Tang and Maitra established the first explicit fixed-dimension improvement over the Patterson–Wiedemann direct-sum nonlinearity bound $\mathcal{N}_{\mathrm{PW}}(n) = 2^{n-1} - 27 \cdot 2^{(n-11)/2} = \mathcal{N}_{\mathrm{BC}}(n) + 81920 \cdot 2^{(n-39)/2}$, proving the existence of (balanced) Boolean functions in $n = 375$ variables—and hence every odd $n \geq 375$—with nonlinearity exceeding $\mathcal{N}_{\mathrm{BC}}(n) + 81921 \cdot 2^{(n-39)/2}$. Their framework combines index-two Gauss-period offsets on multiplicative cosets of $\mathbb{F}_{2^n}^*$ with an unequal-threshold linear-feasibility criterion of Reis and Song and a sampling-without-replacement balancing lemma.

Building directly on Tang and Maitra's framework, we make four contributions. First, we prove an elementary closed-form theorem showing that, for every prime $q \equiv 3 \pmod 4$ with $n = \mathrm{ord}_q(2) = (q-1)/2$ odd and Gauss sum $G_1 = 2^{(n-h)/2-1}(a + b\mathrm{i}\sqrt{q})$ ($b > 0$, $\sigma = \mathrm{sgn}(a)$), the unmodified translated quadratic-residue template $S = c + \sigma\mathcal{R}$ (with Legendre symbol $e_c = \sigma$) produces an exact universal five-class offset magnitude distribution, eliminating case-by-case enumeration. Second, evaluating the Reis–Song potential directly on the unmodified template $S = 3 - \mathcal{R}$ at $n = 375$ ($q = 751$) sharpens the certified threshold from $C = 1.193239$ to $C = 1.192508$, yielding $\mathrm{NL}(f) > 2^{n-1} - 442096 \cdot 2^{(n-39)/2} = \mathcal{N}_{\mathrm{BC}}(n) + 82192 \cdot 2^{(n-39)/2}$ for every odd $n \geq 375$ (both unbalanced and balanced)—enlarging the strict margin above $\mathcal{N}_{\mathrm{PW}}(n)$ from $2^{(n-39)/2}$ to $272 \cdot 2^{(n-39)/2}$ while simplifying the construction to zero label exchanges. An exhaustive check over all 140,625 weight-preserving single exchanges confirms that $3-\mathcal{R}$ is locally optimal for the potential at $n = 375$; by contrast, at $n = 431$ ($q = 863$), where the isolated class carries 51.8% of the potential, two potential-guided exchanges strictly improve the threshold from $C = 1.184952$ to $C = 1.183620$. Third, a complete Hensel–Cornacchia screening of all 208 prime-order index-two candidates in $375 \leq n \leq 5000$ produces an explicit monotone hierarchy of certified bounds—reaching $\mathrm{NL}(f) > 2^{n-1} - 26 \cdot 2^{(n-11)/2}$ at $n \geq 743$ and $\mathrm{NL}(f) > 2^{n-1} - 24 \cdot 2^{(n-11)/2}$ at $n \geq 4935$, closing 69.38% of the normalized gap between the Patterson–Wiedemann constant and Schmidt's asymptotic limit. Fourth, we establish a structural lower bound $q \geq 713$ for single-coset Reis–Song feasibility and summarize a Stickelberger–LLL screening of higher-index primes below $n = 375$. All numerical inequalities are certified by exact integer and rational arithmetic.

Keywords. Boolean functions, nonlinearity, Patterson–Wiedemann bound, Gauss periods, quadratic residues, discrepancy, rational verification.

1 Introduction

Determining the maximum achievable nonlinearity $\mathrm{NL}(f)$ of an n-variable Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$—equivalently, the covering radius of the first-order Reed–Muller code $\mathrm{RM}(1, n)$—is a central problem in coding theory and symmetric cryptography [1]. For even n, bent functions [9] attain the Parseval upper bound $2^{n-1} - 2^{n/2-1}$. For odd n, integrality of the Walsh transform precludes equality, and concatenating two bent functions on $n-1$ variables gives the bent concatenation (BC) baseline

$$\mathcal{N}_{\mathrm{BC}}(n) = 2^{n-1} - 2^{(n-1)/2}.$$

For over four decades, the strongest explicit fixed-dimension bound for odd $n \geq 15$ was obtained by taking direct sums of bent functions with the 15-variable functions of nonlinearity $16276 = \mathcal{N}_{\mathrm{BC}}(15) + 20$ constructed by Patterson and Wiedemann [6, 7], yielding the Patterson–Wiedemann (PW) direct-sum bound

$$\mathcal{N}_{\mathrm{PW}}(n) = 2^{n-1} - 27 \cdot 2^{(n-11)/2} = \mathcal{N}_{\mathrm{BC}}(n) + 20 \cdot 2^{(n-15)/2} = \mathcal{N}_{\mathrm{BC}}(n) + 81920 \cdot 2^{(n-39)/2}. \tag{1}$$

On the asymptotic side, Schmidt [10] resolved the Patterson–Wiedemann conjecture by proving that $\max_f \mathrm{NL}(f) = 2^{n-1} - (1 + o(1))2^{n/2-1}$ as $n \to \infty$, including for balanced functions, though without yielding explicit finite values of n surpassing (1). On the small-dimension side, Kavut, Maitra, and Yücel [4, 5] achieved nonlinearity 242 in $n = 9$ variables—recently shown to be exact [2, 12]—and Kavut and Maitra [3] studied Patterson–Wiedemann type functions in $n = 21$ variables.

In a very recent breakthrough, Tang and Maitra [11] provided the first explicit fixed-dimension improvement over (1). Working in $\mathbb{F}_{2^{375}}^*$ with the multiplicative subgroup $H = \langle \alpha^{751} \rangle$ of index $q = 751$, they combined the explicit index-two Gauss-sum evaluation [13, 10] with an unequal-threshold linear-feasibility theorem derived from Reis and Song [8] and a sampling-without-replacement balancing lemma. Starting from the translated quadratic-residue coset template $3 - \mathcal{R} \pmod{751}$ and performing the single label exchange $505 \mapsto 130$ to reduce the maximum fixed offset from $388 \cdot 2^{179}$ to $384 \cdot 2^{179}$, they proved the existence of both unbalanced and balanced Boolean functions on $n = 375$ variables—and hence every odd $n \geq 375$—satisfying

$$\mathrm{NL}(f) > 2^{n-1} - 442367 \cdot 2^{(n-39)/2} = \mathcal{N}_{\mathrm{BC}}(n) + 81921 \cdot 2^{(n-39)/2} > \mathcal{N}_{\mathrm{PW}}(n). \tag{2}$$

1.1 Contributions and overview

The present note builds directly on Tang and Maitra's construction and methodology [11], refining the analysis of the fixed offset spectrum and extending the explicit parameter search. Our main contributions are fourfold:

1. **Closed-form five-class offset theorem (Section 3).** We show that for *every* prime $q \equiv 3 \pmod 4$ with $n = \mathrm{ord}_q(2) = (q-1)/2$ odd and Gauss sum $G_1 = 2^{(n-h)/2-1}(a + b\mathrm{i}\sqrt{q})$ ($b > 0$, $\sigma = \mathrm{sgn}(a)$), the unmodified translated quadratic-residue set $S = c + \sigma\mathcal{R}$ with $e_c = \sigma$ produces an exact five-class distribution of $|\kappa_r|$ (Theorem 3.1):

$$\{2b : 1, \quad \big||a| - b\big| : \tfrac{q-3}{4}, \quad |a| + b : \tfrac{q-1}{2}, \quad |a| + 3b : \tfrac{q-3}{4}, \quad \big|b(q-2) - |a|\big| : 1\}.$$

   The proof takes ten lines using only quadratic character orthogonality, holds uniformly for both signs of a, and avoids any computer enumeration of the q offset classes.

2. **Sharper and simpler bound at $n = 375$, and the peak-versus-bulk trade-off (Section 4).** In [11], the exchange $505 \mapsto 130$ on $3-\mathcal{R} \pmod{751}$ was selected to reduce the peak $|\kappa_r|$ from 388 to 384. Evaluating the full Reis–Song potential directly reveals an instructive trade-off: lowering the single isolated peak by 4 disperses 140 bulk classes upward to 366 and 368, which increases the potential at $C = 1.193239$ from 0.938583 to 0.999855. Retaining the unmodified template $S = 3 - \mathcal{R}$ instead yields a strictly tighter certified constant $C = 1.192508$ and guarantees, for every odd $n \geq 375$ (both unbalanced and balanced),

$$\mathrm{NL}(f) > 2^{n-1} - 442096 \cdot 2^{(n-39)/2} = \mathcal{N}_{\mathrm{BC}}(n) + 82192 \cdot 2^{(n-39)/2},$$

increasing the margin above $\mathcal{N}_{\mathrm{PW}}(n)$ by a factor of 272 (from $2^{(n-39)/2}$ to $272 \cdot 2^{(n-39)/2}$) with a five-class proof requiring no label exchanges. An exhaustive evaluation of all $375^2 = 140{,}625$ weight-preserving single exchanges confirms that $3 - \mathcal{R}$ is locally optimal for the potential at $n = 375$. Conversely, at $n = 431$ ($q = 863$), the isolated spike accounts for 51.8% of the unmodified potential, and two potential-guided exchanges ($297 \mapsto 333$, $184 \mapsto 769$) genuinely tighten the certified constant from $C = 1.184952$ to $C = 1.183620$.

3. **Monotone hierarchy of fixed-dimension bounds up to $n = 5000$ (Section 5).** Combining Theorem 3.1 with Hensel-lifted Cornacchia reduction, we screen all 208 prime-order index-two candidates in $375 \leq n \leq 5000$ without omission. Six unmodified instances surpass (1), yielding a clean monotone ladder of certified bounds (Table 1). In particular, for all odd $n \geq 743$ ($q = 1487$) we obtain $\mathrm{NL}(f) > 2^{n-1} - 26 \cdot 2^{(n-11)/2}$ (one full integer step below the PW coefficient 27), and for all odd $n \geq 4935$ ($q = 9871$) we obtain $\mathrm{NL}(f) > 2^{n-1} - 24 \cdot 2^{(n-11)/2}$ (three full integer steps below PW, closing 69.38% of the normalized gap between $C_{\mathrm{PW}} = 27/(16\sqrt{2}) \approx 1.193243$ and Schmidt's asymptotic limit 1).

4. **Structural analysis below $n = 375$ (Section 6).** We prove that under the Reis–Song potential $\phi(t) = 5/\sinh(t^2/3)$ applied to a single coset $B \subseteq H$ of index q, even an ideally flat offset spectrum $|A_r| = 2^{n/2}$ ($r \neq 0$) requires $q \geq 713$. We also report exact Stickelberger–LLL evaluations for all seven index-six primes $q = 6n + 1 > 751$ and leading index-eight primes $q = 8n + 1 > 751$ with $n < 375$, clarifying why $n = 375$ remains the natural threshold under the current potential.

2 Preliminaries

We adopt the notation of [11] throughout so that all comparisons are direct. Identifying $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ via a basis and its trace-dual basis, the Walsh transform of $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ at $\omega \in \mathbb{F}_{2^n}$ is

$$W_f(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(\omega x)},$$

where $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. Its nonlinearity is $\mathrm{NL}(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_{2^n}} |W_f(\omega)|$, and f is balanced if $W_f(0) = 0$. If f on u variables is combined in direct sum with a bent function b on $2m$ disjoint variables, $F(x, z) = f(x) + b(z)$, then F is balanced whenever f is balanced and

$$\mathrm{NL}(F) = 2^{u+2m-1} - 2^m\big(2^{u-1} - \mathrm{NL}(f)\big). \tag{3}$$

Expressing a lower bound in the normalized form $\max_\omega |W_f(\omega)| < 2D \cdot 2^{(u-39)/2}$ for an odd integer $u \geq 39$ gives $\mathrm{NL}(f) > 2^{u-1} - D \cdot 2^{(u-39)/2} = \mathcal{N}_{\mathrm{BC}}(u) + (2^{19} - D) \cdot 2^{(u-39)/2}$, which propagates under

Table 1: Summary of lower bounds for odd-variable Boolean functions, written as $\mathrm{NL}(f) > \mathcal{N}_{\mathrm{BC}}(n) + G \cdot 2^{(n-39)/2} = 2^{n-1} - D \cdot 2^{(n-39)/2}$ with effective PW coefficient $k_{\mathrm{eff}} = D/2^{14}$ (so $2^{n-1} - k_{\mathrm{eff}} \cdot 2^{(n-11)/2}$). The first three rows list classical baselines (whose $u = 9, 15$ bent direct sums are unbalanced); the rows from [11] and the present work hold for both unbalanced and balanced Boolean functions. All entries from the present work are certified in exact rational arithmetic.

Construction (odd $n \geq u$)	Seed u	Index q	Certified C	Gain G	Margin $G - 81920$	k_{eff}
Bent concatenation	1	—	1.414214	0	—	32.0000
Kavut–Yücel [5]	9	—	1.237437	65536	—	28.0000
Patterson–Wiedemann [6]	15	—	1.193243	81920	0	27.0000
Tang–Maitra [11] (1 swap)	375	751	1.193239	> 81921	$+1$	26.9999
Unmodified $3 - \mathcal{R}$ (Thm. 4.1)	375	751	1.192508	> 82192	$+272$	26.9834
Unmodified $5 - \mathcal{R}$ (Thm. 4.3)	431	863	1.184952	> 84993	$+3073$	26.8124
2-swap $5 - \mathcal{R}$ (Thm. 4.3)	431	863	1.183620	> 85487	$+3567$	26.7823
Unmodified $1 + \mathcal{R}$ (Thm. 5.1)	575	1151	1.156612	> 95499	$+13579$	26.1712
Unmodified $5 - \mathcal{R}$ (Thm. 5.1)	743	1487	1.139356	> 101896	$+19976$	25.7808
Unmodified $3 - \mathcal{R}$ (Thm. 5.1)	4935	9871	1.059163	> 131626	$+49706$	23.9662

(3) to

$$\mathrm{NL}(F) > 2^{n-1} - D \cdot 2^{(n-39)/2} = \mathcal{N}_{\mathrm{BC}}(n) + (524288 - D) \cdot 2^{(n-39)/2} \tag{4}$$

for every odd $n \geq u$. In these units, $\mathcal{N}_{\mathrm{PW}}(n)$ corresponds to $D_{\mathrm{PW}} = 27 \cdot 2^{14} = 442368$ and gain $G_{\mathrm{PW}} = 524288 - 442368 = 81920$, with normalized Walsh ratio $C_{\mathrm{PW}} = 27/(16\sqrt{2}) \approx 1.193242693$.

Let $q > 3$ be an odd prime dividing $2^n - 1$, let α be a primitive element of $\mathbb{F}_{2^n}$, and set $H = \langle \alpha^q \rangle$, $N = |H| = (2^n - 1)/q$, and $C_r = \alpha^r H$ ($0 \leq r < q$, indices modulo q). The Gauss periods of order q and associated Gauss sums ($\zeta = e^{2\pi \mathrm{i}/q}$) are

$$\eta_r = \sum_{x \in C_r} (-1)^{\mathrm{Tr}_1^n(x)}, \qquad G_j = \sum_{k=0}^{2^n-2} \zeta^{jk} (-1)^{\mathrm{Tr}_1^n(\alpha^k)} = \sum_{r=0}^{q-1} \eta_r \zeta^{jr}.$$

We recall the index-two evaluation and the two existence lemmas established in [11].

Theorem 2.1 (Index-two Gauss sums [13, 10, 11])**.** *Let $q > 3$ be prime with $q \equiv 3 \pmod 4$ and $n = (q-1)/2 = \mathrm{ord}_q(2)$ odd, and let $h = h(-q)$ be the class number of $\mathbb{Q}(\sqrt{-q})$. There exist unique odd integers a, b with $b > 0$ such that*

$$a^2 + qb^2 = 2^{h+2}, \qquad a \cdot 2^{(n-h)/2} \equiv -2 \pmod q, \tag{5}$$

and a choice of primitive element $\alpha \in \mathbb{F}_{2^n}^*$ (replacing α by α^{-1} if needed) such that $G_1 = 2^{(n-h)/2-1}(a + b\mathrm{i}\sqrt{q})$. Writing $\mathcal{R} \subset \mathbb{Z}_q^*$ for the nonzero quadratic residues and $e_r = \left(\frac{r}{q}\right) \in \{0, 1, -1\}$ for the Legendre symbol, the Gauss periods satisfy

$$\eta_i = \frac{-1 - A_G}{q} + B_G e_i + A_G \delta_{i,0}, \qquad A_G = 2^{(n-h)/2-1} a, \quad B_G = 2^{(n-h)/2-1} b. \tag{6}$$

Note that $n = (q-1)/2$ odd forces $q \equiv 3 \pmod 4$, and $2^{(q-1)/2} \equiv 1 \pmod q$ forces $\left(\frac{2}{q}\right) = 1$, hence $q \equiv 7 \pmod 8$.

Given a subset $S \subseteq \{1, \ldots, q-1\}$ of cardinality $|S| = (q-1)/2$ with indicator $g_i = \mathbf{1}_S(i)$ ($g_0 = 0$) and a subset $B \subseteq H$, define $f_B : \mathbb{F}_{2^n} \to \mathbb{F}_2$ by

$$\operatorname{supp}(f_B) = B \cup \bigcup_{i \in S} \alpha^i H. \tag{7}$$

Since $\sum_{i=1}^{q-1}(1-2g_i) = 0$, the constant term in (6) cancels in the fixed signed sum $A_s = \sum_{i=1}^{q-1}(1-2g_i)\eta_{i+s}$. Setting

$$\kappa_s = a(1-\delta_{s,0})(1-2g_{-s}) + b\sum_{i=1}^{q-1}(1-2g_i)e_{i+s} \qquad (0 \le s < q), \tag{8}$$

we have $A_s = 2^{(n-h)/2-1}\kappa_s$ (note that our κ_s coincides with κ_{-s} in [11, eq. (3.4)]), and by (6) and $\sum_{r=0}^{q-1}\eta_r = -1$, the Walsh transform of f_B satisfies $W_{f_B}(0) = 1 + N - 2|B|$ and, for every $\omega \in \alpha^s H$,

$$W_{f_B}(\omega) = 1 + A_s + \eta_s - 2\sum_{x \in B}(-1)^{\mathrm{Tr}_1^n(\omega x)}. \tag{9}$$

The normalized offset magnitudes are therefore $|A_s|/2^{n/2} = |\kappa_s|/\sqrt{2^{h+2}}$.

Lemma 2.2 (Reis–Song unequal-threshold feasibility [11, Lemma 2.5], [8])**.** *Let $N > 4$ and $m \ge 1$ be integers, $a_1, \ldots, a_m \in [-1,1]^N$, and $\Delta_1, \ldots, \Delta_m > 0$. Set $\phi(t) = 5/\sinh(t^2/3)$ for $t > 0$. If $\sum_{j=1}^m \phi(\Delta_j/\sqrt{N}) \le N$, then there exists $x \in \{-1,1\}^N$ such that $\langle a_j, x\rangle \le \Delta_j + 4$ for all $1 \le j \le m$.*

Applying Lemma 2.2 to the $2 \cdot 2^n$ signed rows $\pm a_\omega$ ($a_{\omega,h} = (-1)^{\mathrm{Tr}_1^n(\omega h)}$ for $h \in H$) with offsets $d_0 = 0$ and $d_\omega = A_s$ for $\omega \in \alpha^s H$, and noting $2^n/N > q$ and monotonicity of ϕ, yields the following sufficient condition (cf. [11, Theorem 3.4]): if $C > \max_s |\kappa_s|/\sqrt{2^{h+2}}$ satisfies

$$\frac{2}{N} + \sum_{s=0}^{q-1}\left[\phi\!\left(\sqrt{q}\left(C - \frac{|\kappa_s|}{\sqrt{2^{h+2}}}\right)\right) + \phi\!\left(\sqrt{q}\left(C + \frac{|\kappa_s|}{\sqrt{2^{h+2}}}\right)\right)\right] < 1 \tag{10}$$

together with $\phi(C\sqrt{q}) < 1$, then there exists $B \subseteq H$ such that

$$\max_{\omega \in \mathbb{F}_{2^n}} |W_{f_B}(\omega)| \le C \cdot 2^{n/2} + 5. \tag{11}$$

Lemma 2.3 (Balanced modification [11, Lemma 4.1])**.** *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, $M = 2^n$, and $d = |W_f(0)|/2$. If $d = 0$, then f is already balanced. If $d > 0$, there exists a balanced Boolean function $\tilde{f}$ at Hamming distance d from f satisfying*

$$\max_{\omega \ne 0} |W_{\tilde{f}}(\omega)| < \max_{\omega \ne 0} |W_f(\omega)| + \sqrt{8d\log(4M)}.$$

3 Exact Five-Class Paley Offset Distribution

We now derive the exact multiset of offset magnitudes $|\kappa_s|$ for the unmodified translated quadratic-residue template, uniformly for every prime $q \equiv 3 \pmod 4$ and either sign of a.

Theorem 3.1 (Universal five-class Paley offset theorem)**.** *Let $q > 3$ be a prime with $q \equiv 3 \pmod 4$, let $a, b \in \mathbb{Z}$ with $a \ne 0$ and $b > 0$, and set $\sigma = \operatorname{sgn}(a) \in \{+1, -1\}$. Choose any $c \in \mathbb{Z}_q^*$ with Legendre symbol $e_c = \sigma$, and define the translated quadratic-residue set*

$$S = c + \sigma\mathcal{R} \subset \mathbb{Z}_q \setminus \{0\}.$$

Then $0 \notin S$, $|S| = (q-1)/2$, and the q integers κ_s defined in (8) for $g_i = \mathbf{1}_S(i)$ satisfy $\sum_{s=0}^{q-1}\kappa_s = 0$, $\sum_{s=0}^{q-1}\kappa_s^2 = (q-1)(a^2+qb^2)$, and take the exact magnitude distribution:

Magnitude $\lvert\kappa_s\rvert$	$2b$	$\big\lvert\lvert a\rvert - b\big\rvert$	$\lvert a\rvert + b$	$\lvert a\rvert + 3b$	$\big\lvert b(q-2) - \lvert a\rvert\big\rvert$
Multiplicity	1	$(q-3)/4$	$(q-1)/2$	$(q-3)/4$	1

(If two magnitudes coincide numerically, their multiplicities add.)

Proof. Since $q \equiv 3 \pmod 4$, we have $e_{-1} = -1$ and $e_\sigma = \sigma$. Thus $e_{-\sigma c} = (-1)\sigma e_c = -\sigma^2 = -1$, so $-\sigma c \notin \mathcal{R}$, which is equivalent to $0 \notin c + \sigma\mathcal{R} = S$. Clearly $|S| = |\mathcal{R}| = (q-1)/2$.

Put $v_0 = 0$ and $v_i = 1 - 2g_i$ for $1 \le i \le q-1$. At $i = c$ we have $g_c = 0$ and $v_c = 1$; for $i \notin \{0, c\}$, $g_i = 1 \iff \sigma e_{i-c} = 1$, hence $v_i = -\sigma e_{i-c}$. Therefore, for every $0 \le s < q$,

$$C_s := \sum_{i=1}^{q-1} v_i e_{i+s} = e_{c+s} - \sigma\left(\sum_{i=0}^{q-1} e_{i-c}e_{i+s} - e_{-c}e_s\right).$$

Because $e_{-c} = -e_c = -\sigma$, we have $\sigma e_{-c}e_s = -e_s$. By the standard quadratic-character autocorrelation identity over $\mathbb{F}_q$, $\sum_{i=0}^{q-1} e_{i-c}e_{i+s}$ equals $q-1$ when $s \equiv -c \pmod q$ and -1 otherwise. Consequently,

$$C_s = \begin{cases} 2\sigma, & s = 0, \\ -\sigma(q-2), & s \equiv -c \pmod q, \\ \sigma - e_s + e_{c+s}, & s \notin \{0, -c\}. \end{cases}$$

We now substitute $a = \sigma|a|$ into $\kappa_s = a(1 - \delta_{s,0})v_{-s} + bC_s$:

- At $s = 0$: $\kappa_0 = bC_0 = 2\sigma b$, so $|\kappa_0| = 2b$.
- At $s \equiv -c \pmod q$: $v_{-s} = v_c = 1$, so $\kappa_{-c} = \sigma|a| - \sigma b(q-2) = \sigma\big(|a| - b(q-2)\big)$ and $|\kappa_{-c}| = \big|b(q-2) - |a|\big|$.
- For $s \notin \{0, -c\}$: $-s \notin \{0, c\}$, so $v_{-s} = -\sigma e_{-s-c} = \sigma e_{c+s}$ and $av_{-s} = |a|e_{c+s}$. Thus

$$\kappa_s = (|a| + b)e_{c+s} + b(\sigma - e_s). \tag{12}$$

The $q-2$ indices $s \notin \{0, -c\}$ partition according to $e_s \in \{\sigma, -\sigma\}$:

1. If $e_s = \sigma$, then $\sigma - e_s = 0$ and (12) gives $|\kappa_s| = |a| + b$. Since $e_{-c} = -\sigma \ne \sigma$, all $(q-1)/2$ elements with $e_s = \sigma$ lie outside $\{0, -c\}$, giving multiplicity $(q-1)/2$.
2. If $e_s = -\sigma$ (and $s \ne -c$, leaving $(q-3)/2$ indices), then $\sigma - e_s = 2\sigma$, so (12) gives $\kappa_s = \sigma(|a| + 3b)$ when $e_{c+s} = \sigma$ and $\kappa_s = -\sigma(|a| - b)$ when $e_{c+s} = -\sigma$. To count each sign, observe that $\sum_{s\ne 0} e_{c+s} = -e_c = -\sigma$ and $\sum_{s\ne 0} e_s e_{c+s} = -1$, whence

$$\sum_{\substack{s\ne 0,-c \\ e_s = -\sigma}} e_{c+s} = \frac{1}{2}\sum_{s\ne 0}(1 - \sigma e_s)e_{c+s} = \frac{1}{2}\big(-\sigma - \sigma(-1)\big) = 0.$$

   Hence exactly half of the $(q-3)/2$ indices satisfy $e_{c+s} = \sigma$ and half satisfy $e_{c+s} = -\sigma$, yielding multiplicity $(q-3)/4$ for both $|a| + 3b$ and $\big||a| - b\big|$.

Finally, summing the signed values gives $\sum_{s=0}^{q-1} \kappa_s = 0$ directly from $\sum_{i=0}^{q-1} e_i = 0$ and $\sum_{i=1}^{q-1} v_i = 0$, while Parseval's identity on $\mathbb{Z}_q$ (or direct expansion of the five classes) gives $\sum_{s=0}^{q-1} \kappa_s^2 = (q-1)(a^2 + qb^2)$. □

Remark 3.2 (Two structural regimes)**.** Theorem 3.1 reveals two sharply distinct regimes for the unmodified Paley template, governed by the ratio $b(q-2)/|a|$:

- *Isolated-peak regime* ($b(q-2) > 2|a| + 3b$): the single class $|\kappa_{-c}| = b(q-2) - |a|$ exceeds the bulk ceiling $|a| + 3b$. This occurs at $n = 375$ ($q = 751$, where $388 > 364$) and $n = 431$ ($q = 863$, where $3138 > 2910$).
- *Bulk-dominated regime* ($b(q-2) < 2|a| - b$): the isolated class $\big|b(q-2) - |a|\big|$ falls *below* the bulk floor $|a| - b$, making its contribution to the Reis–Song potential negligible ($< 10^{-9}$). As shown in Section 5, this ideal regime occurs at $n = 575, 743$, and 4935, where the entire bulk lies within 0.05% to 0.21% of the Parseval level $\sqrt{2^{h+2}}$.

Note also that the distribution in Theorem 3.1 is independent of which c with $e_c = \sigma$ is chosen.

4 Refined Bound at $n = 375$ and Potential-Guided Optimization at $n = 431$

4.1 Why the unmodified template sharpens $n = 375$

For $n = 375$ and $q = 751$, Lemma 3.1 of [11] establishes $h(-751) = 15$, $a = -361$, and $b = 1$, with $361^2 + 751 \cdot 1^2 = 2^{17} = 131072$. Since $\sigma = \mathrm{sgn}(-361) = -1$ and $3 \in -\mathcal{R} \pmod{751}$, Theorem 3.1 immediately gives the five-class distribution of the unmodified template $S = 3 - \mathcal{R}$:

$$\{2 : 1, \quad 360 : 187, \quad 362 : 375, \quad 364 : 187, \quad 388 : 1\}.$$

In [11], the exchange $505 \mapsto 130$ was introduced to reduce the single peak from 388 to 384. However, changing one coset label modifies C_s by ± 2 or ± 4 across all 751 classes, spreading the bulk from $\{360, 362, 364\}$ into eight classes reaching 366 (multiplicity 106) and 368 (multiplicity 34). Because $\phi(\sqrt{q}(C - m/\sqrt{2^{h+2}}))$ is convex and sharply increasing in m, shifting 140 bulk classes upward outweighs lowering one isolated class from 388 to 384: at $C = 1.193239$, the potential of the unmodified template $3 - \mathcal{R}$ is 0.938583, compared with 0.999855 after the exchange $505 \mapsto 130$.

Theorem 4.1 (Sharpened bound for all odd $n \geq 375$)**.** *Let $q = 751$, $n = 375$, $H = \langle \alpha^{751} \rangle \subset \mathbb{F}_{2^{375}}^*$ with $\mathrm{Im}\, G_1 > 0$, and $S = 3 - \mathcal{R} \pmod{751}$. There exist both an unbalanced Boolean function f_B of the form (7) and a balanced modification $\tilde{f}_B$ on 375 variables satisfying*

$$\mathrm{NL}(f) > 2^{374} - 442096 \cdot 2^{168} = \mathcal{N}_{\mathrm{BC}}(375) + 82192 \cdot 2^{168}.$$

Consequently, for every odd $n \geq 375$, there exist both unbalanced and balanced Boolean functions F on n variables satisfying

$$\mathrm{NL}(F) > 2^{n-1} - 442096 \cdot 2^{(n-39)/2} = \mathcal{N}_{\mathrm{BC}}(n) + 82192 \cdot 2^{(n-39)/2} = \mathcal{N}_{\mathrm{PW}}(n) + 272 \cdot 2^{(n-39)/2}.$$

Proof. We certify (10) at $C = 1192508/10^6$ using exact rational arithmetic, following the protocol of [11, Section 3.2]. Set $a_{\mathrm{rat}} = 6678434726570384492722$, $L = a_{\mathrm{rat}}/2^{64}$, and $U = (a_{\mathrm{rat}} + 1)/2^{64}$, so that $L^2 < 131072 < U^2$. For each class m in Table 2, put

$$z_m^- = \min\left\{32, \ \frac{\lfloor 10^{12} \cdot \frac{751}{3}(C - m/L)^2 \rfloor}{10^{12}}\right\}, \qquad z_m^+ = \min\left\{32, \ \frac{\lfloor 10^{12} \cdot \frac{751}{3}(C + m/U)^2 \rfloor}{10^{12}}\right\}.$$

Every $z_m^{\pm}$ is a positive rational lower bound for $\frac{751}{3}(C \pm m/\sqrt{131072})^2$. Using the positive Taylor truncation $S_{48}(z) = \sum_{j=0}^{47} z^{2j+1}/(2j+1)! < \sinh z$, each class contribution $\nu_m\big(5/S_{48}(z_m^-) + 5/S_{48}(z_m^+)\big)$ is strictly bounded above by the entry in Table 2 (rounded up to multiples of 10^{-9}). The five classes sum to at most 0.999991201. At $\omega = 0$, $\frac{751}{3}C^2 > 32$ and $S_{48}(32) > 5$ give total zero-frequency contribution below $2/N < 10^{-6}$. Thus the full normalized potential is strictly below $0.999992201 < 1$.

Lemma 2.2 therefore yields $B \subseteq H$ such that $|W_{f_B}(\omega)| \le C \cdot 2^{375/2} + 5$ for all $\omega \in \mathbb{F}_{2^{375}}$. Applying Lemma 2.3 with $d = |W_{f_B}(0)|/2 < 2^{375/2}$ gives a balanced function $\tilde{f}_B$ with $\max_{\omega \neq 0} |W_{\tilde{f}_B}(\omega)| < C \cdot 2^{375/2} + 5 + u$, where $u = \sqrt{8d \log(4 \cdot 2^{375})}$. Since $\log(4 \cdot 2^{375}) = 377 \log 2 < 377$ and $8 \cdot 377 = 3016 < 2^{145}$, we have $u < 2^{375/2-21}$ and hence $5 + u < 2^{-20} \cdot 2^{375/2}$. Finally, the exact integer inequality

$$8 \cdot 442096^2 \cdot 10^{12} - \big(1192508 \cdot 2^{20} + 10^6\big)^2 = 123877701673742336 > 0$$

implies $442096/2^{37/2} > C + 2^{-20}$, whence $\max_\omega |W(\omega)| < 2 \cdot 442096 \cdot 2^{168}$ for both f_B and $\tilde{f}_B$. Direct sums with bent functions via (4) extend the bound to every odd $n \ge 375$. □

Table 2: Exact rational upper bounds for the five-class potential at $n = 375$ ($q = 751$, unmodified $S = 3 - \mathcal{R}$, $C = 1.192508$) and at $n = 431$ ($q = 863$, unmodified $S = 5 - \mathcal{R}$, $C = 1.184952$).

$n = 375,\ q = 751,\ C = 1.192508$			$n = 431,\ q = 863,\ C = 1.184952$		
m	ν_m	Rational upper bound	m	ν_m	Rational upper bound
2	1	0.000000001	14	1	0.000000001
360	187	0.100845333	2882	215	0.067218842
362	375	0.347158911	2896	431	0.226964926
364	187	0.292675164	2910	215	0.188152839
388	1	0.259311792	3138	1	0.517572114
Sum	751	0.999991201	Sum	863	0.999908722

Proposition 4.2 (Local optimality of $3 - \mathcal{R}$ at $n = 375$)**.** *Among all* $375^2 = 140{,}625$ *sets* $S' = (S \setminus \{p\}) \cup \{v\}$ *obtained from* $S = 3 - \mathcal{R} \pmod{751}$ *by a single weight-preserving label exchange* ($p \in S$, $v \in \{1, \dots, 750\} \setminus S$)*, every* S' *has Reis–Song potential strictly exceeding* 1.066908 *at* $C = 1.192508$*, whereas the unmodified set* S *has potential strictly below* $0.999992 < 1$.

Proof. Using exact rational lower bounds for $\phi(\sqrt{751}(C - k/\sqrt{131072}))$ (via $U = (a_{\text{rat}} + 1)/2^{64}$ and an upper Taylor remainder bound for sinh), scaled by 10^9 into exact integer table entries, an exhaustive evaluation over all 140,625 integer offset vectors $\kappa(S')$ in `verify_all_theorems.py` certifies that the minimum potential across all single exchanges is at least $1.0669082 > 1$ (attained at the exchange $659 \mapsto 408$). □

4.2 When potential-guided exchanges help: $n = 431$ ($q = 863$)

Notice from Table 2 that at $n = 375$ the isolated class $m = 388$ accounts for 25.9% of the potential, whereas at $n = 431$ ($q = 863$, $h(-863) = 21$, $a = -2889$, $b = 7$, $a^2 + 863b^2 = 2^{23}$) the isolated class $m = 3138$ accounts for 51.8% of the unmodified potential. In this regime, selecting exchanges to minimize the potential directly—rather than only the peak—yields a strict further improvement.

Theorem 4.3 (Bounds for all odd $n \geq 431$)**.** *Let $q = 863$, $n = 431$, and $H = \langle \alpha^{863} \rangle \subset \mathbb{F}_{2^{431}}^*$ with $\operatorname{Im} G_1 > 0$.*

(a) Using the unmodified template $S = 5 - \mathcal{R} \pmod{863}$, there exist unbalanced and balanced Boolean functions on every odd $n \geq 431$ variables satisfying

$$\mathrm{NL}(F) > 2^{n-1} - 439295 \cdot 2^{(n-39)/2} = \mathcal{N}_{\mathrm{BC}}(n) + 84993 \cdot 2^{(n-39)/2}.$$

(b) Using the two-exchange template $S' = \big((5 - \mathcal{R}) \setminus \{184, 297\}\big) \cup \{333, 769\} \pmod{863}$, there exist unbalanced and balanced Boolean functions on every odd $n \geq 431$ variables satisfying

$$\mathrm{NL}(F) > 2^{n-1} - 438801 \cdot 2^{(n-39)/2} = \mathcal{N}_{\mathrm{BC}}(n) + 85487 \cdot 2^{(n-39)/2}.$$

Proof. Direct arithmetic verifies that 863 is prime, $\mathrm{ord}_{863}(2) = 431$, $h(-863) = 21$, $(-2889)^2 + 863 \cdot 7^2 = 2^{23} = 8388608$, and $(-2889) \cdot 2^{205} \equiv -2 \pmod{863}$. We bracket $\sqrt{2^{23}}$ by $L = a_{\mathrm{rat}}/2^{64}$ and $U = (a_{\mathrm{rat}} + 1)/2^{64}$ with $a_{\mathrm{rat}} = 53427477812563075941783$. For part (a), $5 \in -\mathcal{R} \pmod{863}$, so Theorem 3.1 gives the five classes in Table 2, whose exact rational potential sum at $C = 1184952/10^6$ is at most 0.999908722; adding $2/N < 10^{-6}$ stays below 1. For part (b), $184, 297 \in 5 - \mathcal{R}$ and $333, 769 \notin 5 - \mathcal{R}$ (with $0 \notin S'$), and exact integer evaluation of (8) yields the 13-class distribution in Table 3, whose exact rational potential sum at $C = 1183620/10^6$ is at most 0.999935978, giving full potential $< 0.999936978 < 1$. In both cases, $8 \cdot 433 = 3464 < 2^{173}$ ensures $5 + u < 2^{-20} \cdot 2^{431/2}$ in Lemma 2.3, and the exact integer checks

$$8 \cdot 439295^2 \cdot 10^{12} - (1184952 \cdot 2^{20} + 10^6)^2 = 1653570290703364096 > 0,$$
$$8 \cdot 438801^2 \cdot 10^{12} - (1183620 \cdot 2^{20} + 10^6)^2 = 311882056408985600 > 0$$

complete the proof via (4). □

Table 3: Exact 13-class magnitude distribution and rational upper bounds for the two-exchange template $S' = ((5 - \mathcal{R}) \setminus \{184, 297\}) \cup \{333, 769\} \pmod{863}$ at $n = 431$, $C = 1.183620$.

m	ν_m	Rational upper bound	m	ν_m	Rational upper bound
70	1	0.000000001	2910	163	0.163689413
2826	26	0.001035960	2924	116	0.190298330
2840	26	0.001834490	2938	62	0.163936105
2854	59	0.007273245	2952	30	0.126145587
2868	96	0.020400638	2966	3	0.019792559
2882	117	0.042287948	3082	1	0.164377626
2896	163	0.098864076	**Sum**	**863**	**0.999935978**

5 An Explicit Monotone Hierarchy up to $n = 5000$

Because Theorem 3.1 determines the complete offset distribution from (q, h, a, b) alone, screening higher dimensions reduces to solving (5). Since $q \equiv 7 \pmod 8$, $-q \equiv 1 \pmod 8$ has a square root modulo 2^{h+2} obtainable in h steps by Hensel lifting, and $\gcd(a, b) = 1$ allows Cornacchia's Euclidean algorithm to recover (a, b) in $O(h)$ arithmetic operations—even when $h \approx 50$.

Applying this procedure across all odd $n \in [375, 5000]$ identifies exactly 208 primes $q = 2n+1 \equiv 7 \pmod 8$ with $\mathrm{ord}_q(2) = n$, with zero unresolved instances. Exactly six unmodified five-class templates surpass $\mathcal{N}_{\mathrm{PW}}(n)$: $n \in \{375, 431, 575, 743, 3975, 4935\}$. Omitting $n = 3975$ (which is dominated by $n = 743$), the remaining five dimensions form a strictly improving monotone ladder. Notably, $n = 575, 743$, and 4935 all lie in the bulk-dominated regime of Remark 3.2, and $n = 575$ realizes the positive-a branch ($S = 1 + \mathcal{R}$) of Theorem 3.1.

Theorem 5.1 (Explicit fixed-dimension hierarchy beyond integer PW thresholds)**.** *For each seed (u, q, S, D, G) listed below, there exist both unbalanced and balanced Boolean functions F on every odd $n \geq u$ variables satisfying* $\mathrm{NL}(F) > 2^{n-1} - D \cdot 2^{(n-39)/2} = \mathcal{N}_{\mathrm{BC}}(n) + G \cdot 2^{(n-39)/2}$*:*

1. $u = 575$, $q = 1151$, $S = 1 + \mathcal{R}$: $D = 428789$, $G = 95499$ *($C = 1.156612$).*
2. $u = 743$, $q = 1487$, $S = 5 - \mathcal{R}$: $D = 422392$, $G = 101896$ *($C = 1.139356$). In particular,*
$$\mathrm{NL}(F) > 2^{n-1} - 26 \cdot 2^{(n-11)/2} \qquad (\textit{for every odd } n \geq 743).$$
3. $u = 4935$, $q = 9871$, $S = 3 - \mathcal{R}$: $D = 392662$, $G = 131626$ *($C = 1.059163$). In particular,*
$$\mathrm{NL}(F) > 2^{n-1} - 24 \cdot 2^{(n-11)/2} \qquad (\textit{for every odd } n \geq 4935).$$

Proof. Each parameter tuple is certified by the exact same rational-arithmetic pipeline as Theorem 4.1, summarized in Table 4. In every case, direct computation confirms primality of q, $\mathrm{ord}_q(2) = u$, the class number $h = h(-q)$ by enumerating reduced primitive positive definite binary quadratic forms of discriminant $-q$, the norm and congruence equations (5), and the choice of c with $e_c = \mathrm{sgn}(a)$. Theorem 3.1 supplies the exact five-class distribution; the exact rational potential upper bound (using $L = a_{\mathrm{rat}}/2^{64}$, $U = (a_{\mathrm{rat}} + 1)/2^{64}$ with $L^2 < 2^{h+2} < U^2$ and $S_{48}(z)$) plus $2/N < 10^{-6}$ is strictly less than 1. For balancing via Lemma 2.3, $8(u+2) < 2^{(u-85)/2}$ holds with huge margin for all three seeds ($4616 < 2^{245}$, $5960 < 2^{329}$, $39496 < 2^{2425}$), ensuring $5 + u_{\mathrm{bal}} < 2^{-20} \cdot 2^{u/2}$. The exact integer deficit inequalities $8D^2 \cdot 10^{12} - (C_{\mathrm{num}} 2^{20} + 10^6)^2 > 0$ are strictly positive in all three cases (Table 4). Finally, $422392 < 26 \cdot 2^{14} = 425984$ and $392662 < 24 \cdot 2^{14} = 393216$ yield the clean integer-coefficient statements, and (4) extends them to every odd $n \geq u$. □

Table 4: Exact arithmetic parameters and rational verification certificates for Theorem 5.1. In every row, $a^2 + qb^2 = 2^{h+2}$, $L = a_{\mathrm{rat}}/2^{64} < \sqrt{2^{h+2}} < (a_{\mathrm{rat}} + 1)/2^{64}$, and $\Delta_{\mathrm{int}} = 8D^2 \cdot 10^{12} - (C_{\mathrm{num}} 2^{20} + 10^6)^2 > 0$.

Parameter	$u = 575$ ($q = 1151$)	$u = 743$ ($q = 1487$)	$u = 4935$ ($q = 9871$)
Class number $h(-q)$	41	37	49
$(a,\ b)$	(2964687, 2417)	(−741441, 119)	(−47447177, 7567)
Template S	$1 + \mathcal{R}$ ($e_1 = +1$)	$5 - \mathcal{R}$ ($e_5 = -1$)	$3 - \mathcal{R}$ ($e_3 = -1$)
Isolated $\lvert b(q-2) - \lvert a\rvert\rvert$	187554	564726	27231546
Bulk $\lvert a\rvert - b$	2962270	741322	47439610
Bulk $\lvert a\rvert + b$	2967104	741560	47454744
Bulk $\lvert a\rvert + 3b$	2971938	741798	47469878
$a_{\mathrm{rat}} = \lfloor 2^{64}\sqrt{2^{h+2}} \rfloor$	54709737280064589764386658	13677434320016147441096664	87535579648103343623018653 4
Certified $C = C_{\mathrm{num}}/10^6$	1.156612	1.139356	1.059163
Nonzero potential UB	0.999841850	0.999842689	0.999609433
Deficit D / Gain G	428789 / 95499	422392 / 101896	392662 / 131626
Exact margin Δ_{int}	4496764027241721856	6291356837887012864	4330885111910035456

Recall that $C_{\mathrm{PW}} - 1 \approx 0.193242693$ measures the normalized distance between the Patterson–Wiedemann bound and Schmidt's asymptotic limit 1 [10]. At $n = 4935$, the certified threshold $C = 1.059163$ reduces this gap to 0.059163, closing $(0.193243 - 0.059163)/0.193243 \approx 69.38\%$ of the entire gap by an explicit fixed-dimension certificate.

6 Structural Analysis Below $n = 375$

A natural open question highlighted in [11] is whether the dimension $n = 375$ can be lowered. Our analysis clarifies why $n = 375$ sits immediately above a sharp structural threshold for the single-coset Reis–Song criterion.

Proposition 6.1 (Flat-spectrum index threshold for Lemma 2.2)**.** *Let $q > 1$ be an odd divisor of $2^n - 1$, and consider an ideally flat fixed offset spectrum satisfying $A_0 = 0$ and $|A_s| = 2^{n/2}$ for every $1 \le s < q$ (which attains the Parseval identity $\sum_{s=0}^{q-1} A_s^2 = (q-1) \cdot 2^n$ with minimum possible peak). At $C = C_{\mathrm{PW}} = 27/(16\sqrt{2})$, the nonzero potential sum*

$$P_{\mathrm{flat}}(q) := (q-1)\left[\phi(\sqrt{q}(C_{\mathrm{PW}} - 1)) + \phi(\sqrt{q}(C_{\mathrm{PW}} + 1))\right]$$

satisfies $P_{\mathrm{flat}}(q) > 1$ for every $q \le 712$ (with $P_{\mathrm{flat}}(712) \approx 1.006603$) and $P_{\mathrm{flat}}(q) < 1$ for every $q \ge 713$ (with $P_{\mathrm{flat}}(713) \approx 0.995549$).

Proof. Set $\delta = C_{\mathrm{PW}} - 1 > 0$. For $x = q\delta^2/3 > 1$, the derivative of $\log\big((q-1)/\sinh(q\delta^2/3)\big)$ with respect to q is $\frac{1}{q-1} - \frac{\delta^2}{3}\coth(q\delta^2/3) < \frac{1}{q-1} - \frac{\delta^2}{3}$, which is strictly negative for all $q > 1 + 3/\delta^2 \approx 81.3$; the same holds for the smaller term $\phi(\sqrt{q}(C_{\mathrm{PW}} + 1))$. Exact rational arithmetic (bracketing $\sqrt{2}$ to 64 binary bits and bounding sinh from above and below via Taylor polynomials with remainder in `verify_all_theorems.py`) certifies $P_{\mathrm{flat}}(q) \ge 1.0066026 > 1$ for every $3 \le q \le 712$ and $P_{\mathrm{flat}}(713) \le 0.9955488 < 1$. □

Proposition 6.1 explains the situation in the prime-order index-two family ($q = 2n + 1$) below $n = 375$:

- Every prime-order index-two candidate with $n \le 323$ has $q \le 647 < 713$, placing it strictly below the flat-spectrum threshold of Proposition 6.1.
- Only two candidates lie in $713 \le q < 751$: $q = 719$ ($n = 359$, where $|a|/\sqrt{2^{33}} \approx 0.5835$ is far from 1) and $q = 743$ ($n = 371$, where $b = 17$ gives an isolated peak of 3.362 for $c - \mathcal{R}$, and greedy swap optimization stalls at $\max_s |A_s|/2^{n/2} \approx 1.249 > C_{\mathrm{PW}}$).
- Interestingly, at $n = 299$ ($q = 599$, $h = 25$, $a = -11523$, $b = 49$) and $n = 323$ ($q = 647$, $h = 23$, $a = -5763$, $b = 23$), cancelling the isolated spike of $c - \mathcal{R}$ via 24 and 28 label exchanges reduces $\max_s |A_s|/2^{n/2}$ from 1.5304 and 1.5661 down to 1.1244 and 1.1214, respectively—comfortably below C_{PW}. Thus, any future sharpening of the constant 1/3 in the Reis–Song potential $\phi(t) = 5/\sinh(t^2/3)$ would immediately open the range $n \in \{299, 323\}$.

To test whether larger indices $q > 751$ with smaller dimensions $n < 375$ could bypass $q = 2n+1$, we also evaluated all seven index-six primes $q = 6n + 1 > 751$ with $n < 375$ odd ($\mathrm{ord}_q(2) = n$: $n \in \{153, 221, 233, 237, 245, 305, 333\}$) and the five lowest-weight-spread index-eight primes $q = 8n + 1 > 751$ ($n \in \{117, 161, 179, 201, 215\}$). Using the integral period basis of $\mathbb{Q}(\zeta_q)^{\langle 2 \rangle}$, Stickelberger's prime-ideal factorization above 2, and LLL lattice reduction in the Minkowski embedding, we recovered the exact Gauss periods η_r (verified to integer error 0 and exact Parseval sum). In all

twelve cases, the $e/2$ conjugate pairs of Gauss sums do not align tightly enough to produce a near-identity circulant matrix: the largest achieved ratio $|\eta_0|/2^{n/2}$ is 0.7093 at $n = 221$ ($q = 1327$), compared with 0.9971 at $n = 375$ ($q = 751$). Consequently, the best cyclotomic templates yield $\max_s |A_s|/2^{n/2} \geq 1.404$.

7 Concluding Remarks and Reproducibility

Starting from the index-two Gauss-period and linear-feasibility framework of Tang and Maitra [11], we have shown that an elementary closed-form analysis of the unmodified Paley template $S = c + \mathrm{sgn}(a)\mathcal{R}$ simplifies the offset calculation to five exact classes, sharpens the guaranteed nonlinearity margin at $n = 375$ by a factor of 272, explains when potential-guided exchanges improve the bound (as at $n = 431$), and yields an explicit hierarchy of certified fixed-dimension bounds passing $2^{n-1} - 26 \cdot 2^{(n-11)/2}$ at $n \geq 743$ and $2^{n-1} - 24 \cdot 2^{(n-11)/2}$ at $n \geq 4935$. As in [11], all existence results are non-constructive on the single coset $B \subseteq H$ and the balancing set D. Finding explicit descriptions of B, tightening the discrepancy constant in Lemma 2.2 to reach dimensions such as $n = 299$ or $n = 323$, and pushing the fixed-dimension hierarchy still closer to Schmidt's asymptotic limit remain attractive directions for further work.

Reproducibility. Every arithmetic identity, class-number count, five-class distribution (cross-checked directly against Theorem 3.1), rational Reis–Song potential upper bound, exact integer deficit inequality, and exact rational check of Propositions 4.2 and 6.1 is independently verified without floating-point arithmetic by the accompanying Python script `verify_all_theorems.py`. The complete screening of Sections 5 and 6 is reproduced by `scan_records_fast.py`, `solve_index6_gauss.py`, and `solve_index8.py`. The verification package is archived at doi:10.6084/m9.figshare.35082409.

Use of AI-assisted tools. Generative AI systems were used to assist in exploring parameter ranges, drafting and debugging exact verification and screening scripts, and refining the exposition. All mathematical proofs, exact rational certificates, and numerical claims were independently verified by deterministic computation and checked by the authors, who take full responsibility for the content.

References

[1] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, Cambridge, 2021.

[2] X.-d. Hou, E. Sabo, and F. Slaughter, "The covering radius of RM(1, 9) is precisely 242," Cryptology ePrint Archive, Paper 2026/2529, 2026.

[3] S. Kavut and S. Maitra, "Patterson–Wiedemann type functions on 21 variables with nonlinearity greater than bent concatenation bound," *IEEE Trans. Inform. Theory*, vol. 62, no. 4, pp. 2277–2282, 2016.

[4] S. Kavut, S. Maitra, and M. D. Yücel, "Search for Boolean functions with excellent profiles in the rotation symmetric class," *IEEE Trans. Inform. Theory*, vol. 53, no. 5, pp. 1743–1751, 2007.

[5] S. Kavut and M. D. Yücel, "9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class," *Inform. Comput.*, vol. 208, no. 4, pp. 341–350, 2010.

[6] N. J. Patterson and D. H. Wiedemann, "The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276," *IEEE Trans. Inform. Theory*, vol. 29, no. 3, pp. 354–356, 1983.

[7] N. J. Patterson and D. H. Wiedemann, "Correction to—The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276," *IEEE Trans. Inform. Theory*, vol. 36, no. 2, p. 443, 1990.

[8] V. Reis and Z. Song, "Three standard deviations suffice while one does not," arXiv:2609.34471v1, 2026.

[9] O. S. Rothaus, "On 'bent' functions," *J. Combin. Theory Ser. A*, vol. 20, no. 3, pp. 300–305, 1976.

[10] K.-U. Schmidt, "Asymptotically optimal Boolean functions," *J. Combin. Theory Ser. A*, vol. 164, pp. 50–59, 2019.

[11] D. Tang and S. Maitra, "(Balanced) Boolean functions on 375 variables with nonlinearity exceeding the Patterson–Wiedemann direct-sum bound," Cryptology ePrint Archive, Paper 2026/2680, 2026.

[12] Q. Wang, Y. Lou, and Z. Wang, "The covering radius of the Reed–Muller code $\mathrm{RM}(1, 9)$ is 242," arXiv:2610.17871v1, 2026.

[13] J. Yang and L. Xia, "Complete solving of explicit evaluation of Gauss sums in the index 2 case," *Sci. China Math.*, vol. 53, no. 9, pp. 2525–2542, 2010.