Modular Walsh rigidity for Boolean functions of degree at most four

The uniform 1/2 bound

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

[1] Centro Universitário de Belo Horizonte (UniBH), Belo Horizonte, Brazil
[2] American Global Tech University (AGTU)

F. M. Vono: 0009-0009-4994-8533 A. O. Naufel de Toledo: 0000-0002-0619-6820
V. G. Santos: 0009-0009-1333-2518 Correspondence: contatofilipevono@gmail.com

Abstract

We establish the sufficient ratio $p/2^m \geq 1/2$ for Boolean functions of algebraic degree at most four in $4m$ variables for every $m \geq 4$. The modulus p is odd and may be composite. If every unnormalized Walsh coefficient is congruent to one of the two bent levels modulo p, the function is bent. This removes the dimension cutoff of the previous large-dimension result. The final argument finds an affine zero subspace of the quartic digit in a codimension excluded by the Walsh reductions. It also settles modulus 33 in 24 variables.

Theorem 1. *Let $m \geq 4$, $M = 2^m$, and let $p \geq M/2$ be an odd integer. Let $f : \mathbb{F}_2^{4m} \to \mathbb{F}_2$ have algebraic degree at most four and define*

$$W_f(b) = \sum_{x \in \mathbb{F}_2^{4m}} (-1)^{f(x)+b\cdot x}.$$

If $W_f(b) \equiv \pm M^2 \pmod{p}$ for every b, then $|W_f(b)| = M^2$ for every b.

1 Introduction

Bent functions have a flat Walsh spectrum. On $4m$ variables, its two possible values are $\pm 2^{2m}$. We ask whether these levels can be recognized from their residues modulo an odd integer. The signs in the residue condition may vary across frequencies. The degree bound limits the powers of two that can occur in the Walsh spectrum and makes the modular condition rigid.

The original version of this report established the sufficient ratio 9/16 [1]. An intermediate version improved it to 11/20, and the companion notes reached 8/15 [3]. The present revision proves the uniform sufficient ratio 1/2, including the smallest dimensions in its range. In particular, it applies at modulus 33 in 24 variables, a case below the earlier uniform thresholds.

Proof outline. We divide the Walsh spectrum by $M = 2^m$ and separate the possible residue patterns modulo four. The earlier reductions eliminate the odd spectrum and the case where the residue 2 occurs on exactly half the frequencies. If the residue is everywhere 0, Parseval gives the result directly. The remaining case has a quadratic phase and a quartic Boolean polynomial D that records the next residue bit after removing the phase. Energy estimates put its weight in a narrow interval and rule out low-codimension flats on which its degree drops. The new argument takes a cubic derivative of D, partitions its zeros into flats, and forces a zero flat of D in a forbidden codimension.

2 Walsh normalization and the remaining residue pattern

Put $X = W_f/M$. In any affine frequency coordinates, its integer multilinear coefficient of degree j is $(-2)^j/M$ times a sign sum on a coordinate flat of dimension $4m - j$ in the input space, with a possible affine twist. To see the divisibility of that sum, expand the sign into a product of factors $1 - 2x_I$ over the nonconstant monomials of the restricted Boolean polynomial. A term using k factors has valuation at least $k + \max(0, 4m - j - 4k)$, which is at least $\lceil (4m - j)/4 \rceil$. Thus X is integer valued, and its coefficient of degree j is divisible by $2^{\lceil 3j/4 \rceil}$. In particular the parity of X is constant, and if it is even, the residue 2 modulo four occurs on either the whole space, an affine hyperplane, or the empty set.

With normalized Fourier transform and averages over the frequency space,

$$\mathbb{E}X^2 = M^2, \qquad \widehat{X}(x) = (-1)^{f(x)}/M.$$

The residue assumption becomes $X(b) \equiv \pm M \pmod p$, since p is odd. At any point where $X \equiv 0 \pmod 4$, the possible values are $\pm M + 4p\mathbb{Z}$. Their magnitudes are at least M because $4p \geq 2M$. Thus Parseval proves the theorem if this residue occurs everywhere.

For $m = 4$, all admissible odd moduli satisfy $p \geq 9 = 9M/16$. For $m = 5$, modulus 17 is covered by the separate twenty-variable theorem [2], and every larger odd modulus satisfies $p \geq 19 > 9M/16$. For $m \geq 6$, the companion's 8/15 theorem covers $p/M \geq 8/15$. We henceforth work on the residual interval $1/2 \leq t = p/M \leq 8/15$. The specific earlier reductions used on this interval are listed in Appendix A.

In the remaining case $X \equiv 2 \pmod 4$ everywhere. Define the quadratic phase Q and the quartic residue bit D by

$$Y = (-1)^Q X \equiv 2p \pmod 8, \qquad Y \equiv 2p - 8pD \pmod{16}.$$

The degree bounds follow from the coefficient filtration. In detail, Q is obtained by dividing $X - 2p$ by four modulo two. The integer lift of a Boolean quadratic has degree at most four modulo four, by expanding its parity in its monomials. Then the identity $X \equiv 2p - 4pQ - 8pD \pmod{16}$ gives $\deg D \leq 4$. Write $2h$ for the polar rank of Q (so Q has semirank h) and $w = \mathbb{E}D$.

Put $A = 2p - M$ and $C = M - 6p$. On $D = 0$, the admissible values lie in $A + \{0, 2M\} + 16p\mathbb{Z}$, and on $D = 1$ they lie in $C + \{0, -2M\} + 16p\mathbb{Z}$. These follow by combining the odd-modulus residue with the specified residue modulo 16, using $16 \mid M$. The smallest magnitudes are $|A|$ and $|C|$, respectively. Subtracting their squares cell by cell gives the nonnegative excess

$$E = Y^2 - A^2 - (C^2 - A^2)D, \qquad \frac{\mathbb{E}E}{pM} = e_t(w) := 4(1 - t) - 8(4t - 1)w.$$

The remaining inputs are $h \geq 2m - 1$ and the following two restrictions. First, on any affine flat of codimension at most $h - 4$, the restriction of D still has degree four. Equivalently, the degree-four exterior symbol $[D]_4$ (defined in Appendix B.1) is nonzero on the direction of the flat. In particular, D has no zero flat of codimension at most $h - 4$, so the Klein–Storme theorem [5, Theorem 3] gives $w \geq (3 - 2^{5-h})/16$. Second, with $a = 8(8t - 1)$, the cost of the next residue bits gives

$$e_t(w) \geq \frac{a}{256}(3 - 2^{8-h}).$$

Appendix B gives the two arguments. These are restrictions on an assumed counterexample. The next two sections show that their permitted weight ranges force precisely the degree drop that the first restriction excludes.

3 Zero subspaces of cubics

Write $w(P)$ for the relative Hamming weight of a Boolean polynomial and $\Delta_a P(x) = P(x+a) + P(x)$. With $g = \Delta_a P$, translation by a pairs the points in $\{g = 1\}$ and exchanges the two values of P. Hence

$$w(P) = \tfrac{1}{2} w(g) + \Pr(P = 1, g = 0), \qquad \mathbb{E}_a w(\Delta_a P) = 2w(P)(1 - w(P)). \tag{1}$$

The zero set of the quadratic form $Q_{2r}(x, y) = x \cdot y$ on $\mathbb{F}_2^{2r}$ partitions into a flat of codimension r and $2^r - 1$ flats of codimension $r + 1$. Fix x. There is no condition on y if $x = 0$, and one linear equation otherwise. Free coordinates have no effect on the codimensions.

Lemma 1. *If a polynomial of degree at most three has no affine zero subspace of codimension at most j, its weight is at least b_j, where*

j	0	1	2	3	4	5
b_j	1/8	7/32	1/4	37/128	8/25	177/512.

Proof. Minimum distance gives b_0. Below weight $1/4$ the Kasami–Tokura forms [4] have an affine linear factor or are sums of two products of three independent affine coordinates on disjoint blocks. The latter form has weight $7/32$, and setting one factor of each product to zero gives a zero flat of codimension two. This proves the bounds for $j = 1, 2$.

Pass to the quotient by the period subspace of P, of dimension N after quotienting. Pullback preserves codimension and the quotient preserves the degree bound. If $w(P) < b_j$ and P has no zero flat of codimension at most j, then $N \geq j+1$. For $a \neq 0$, each derivative on the quotient is a nonzero quadratic and is constant on the cosets of $\langle a \rangle$. By the quadratic normal form, a positive quadratic weight at most $7/16$ is $1/4, 3/8$, or $7/16$. The corresponding functions are affinely equivalent to Q_2, Q_4, Q_6 with free coordinates.

For $j = 3$, there is a nonzero derivative of weight at most $3/8$. Otherwise, in dimension $N \geq 5$ the mean derivative weight would be at least $(31/32)(7/16) > 2b_3(1 - b_3)$. For $N = 4$ the derivative has at most three effective coordinates, so under the same supposition its weight is at least $1/2$; the resulting mean bound also contradicts (1).

For $j = 4$, there is again a nonzero derivative of weight at most $3/8$. The lower bound on the mean in the opposite case is $(255/256)(7/16) > 2b_4(1 - b_4)$ for $N \geq 8$. For $N = 5, 6$, the next possible quadratic weight after $3/8$ is at least $1/2$ because at most five coordinates remain. For $N = 7$, a cubic has weight divisible by four in absolute counts. Indeed, expand its sign as a product of factors $1 - 2x_I$. A term with k factors and union of size $u \leq \min(3k, 7)$ contributes a multiple of 2^{k+7-u}, whose exponent is at least three (since $k + 7 - u \geq 7 - 2k \geq 3$ for $k \leq 2$, and $k + 7 - u \geq k \geq 3$ for $k \geq 3$). The sign sum is therefore divisible by eight. Thus $w(P) < b_4$ gives $w(P) \leq 5/16$, and $(127/128)(7/16) > 2(5/16)(11/16)$.

For $j = 5$, a nonzero derivative of weight at most $7/16$ exists because the opposite case gives a mean at least $(63/64)(15/32) > 2b_5(1 - b_5)$. In each case use (1) and the partition of the quadratic zero set. A derivative of type Q_{2r} gives

$$w(P) \;\geq\; \frac{1/2 - 2^{-r-1}}{2} + 2^{-r} b_{j-r} + (2^r - 1) 2^{-r-1} b_{j-r-1}.$$

For $j = 3$ these bounds are $39/128, 37/128$ for $r = 1, 2$; for $j = 4$ they are $85/256, 85/256$. For $j = 5$ they are $4573/12800, 181/512, 177/512$. All are at least b_j, a contradiction. □

4 Zero subspaces of quartics

Lemma 2. *A Boolean polynomial of degree at most four and weight in* $[191/1024, 3393/17408]$ *has a zero flat of codimension at most seven. A Boolean polynomial of degree at most four and weight in* $[191/1024, 55/256]$ *has a zero flat of codimension at most eight.*

Proof. Suppose there is no zero flat of codimension at most d, with $d = 7$ or $d = 8$, and write w for the weight of D. The weight on any flat of absolute codimension j is bounded below by

$$F_d(j) = \begin{cases} 0 & j > d, \\ 1/16 & j = d, \\ 15/128 & j = d-1, \\ (3 - 2^{1-(d-j)})/16 & j \le d-2. \end{cases}$$

These bounds follow respectively from nonnegativity, minimum distance, Kasami–Tokura below weight $1/8$, and Klein–Storme [5, Theorem 3] applied in order four. In the third case the only form below twice minimum distance without a zero hyperplane is a sum of two disjoint four-fold products of independent affine coordinates, of weight $15/128$.

Put $\alpha(a) = 8w(\Delta_a D)$ and $s = 95/512 = F_7(1)$; since $F_8(1) = 191/1024 > s$, the bound s lower-bounds the weight of D on every hyperplane for both $d = 7$ and $d = 8$. The normalized Fourier transform of $\phi = (-1)^D$ gives

$$\mu = \mathbb{E}\alpha = 16w(1-w), \qquad \mathrm{Var}(\alpha) = 16 \sum_{\xi \neq 0} \widehat{\phi}(\xi)^4 \le 256(w-s)^2 w(1-w).$$

Indeed $\alpha(a) = 4\big(1 - \sum_\xi \widehat{\phi}(\xi)^2 (-1)^{\xi \cdot a}\big)$, and each nonconstant $\widehat{\phi}(\xi)$ has modulus at most $2(w-s)$, by comparing the two parallel hyperplanes. The sum of their squares is $4w(1-w)$.

Let $U = 177/64$. For $2 < \mu < U$, the two one-sided Cantelli bounds guarantee a direction a with $2 < \alpha(a) < U$ whenever $\mathrm{Var}(\alpha) < (\mu - 2)(U - \mu)$. The conclusion follows by adding the two tail bounds and clearing their positive denominators. On each interval $[l, r]$ in the following table, $(\mu(l) - 2)(U - \mu(r))$ lower-bounds the product, and the variance bound is largest at r.

$[l, r]$	$(\mu(l) - 2)(U - \mu(r)) - 256(r-s)^2 r(1-r)$
$[191/1024, 13/64]$	$1046583/16777216$
$[13/64, 55/256]$	$150897/67108864$

Both margins are positive and $2 < \mu(l) \le \mu(r) < U$. The selected nonzero derivative g has weight less than $177/512$ and therefore has a zero flat of minimum codimension $1 \le c \le 5$, by Lemma 1.

Take affine coordinates in which the zero flat of g fixes the first c coordinates to zero. Every monomial of g contains one of them. Each other coset therefore carries a nonzero quadratic q_i. A parallel zero coset would combine with the first to give a zero flat of codimension $c - 1$. Define $x_i = 4w(q_i)$ with relative weight in the coset, so $\sum_i x_i = 2^{c-1}\alpha$.

Using the quadratic partitions, the local contribution to $\Pr(D = 1, g = 0)$ in a coset is bounded below by

x_i	$Z_c(x_i)$
1	$F_d(c+1)/2 + F_d(c+2)/4$
$3/2$	$F_d(c+2)/4 + 3F_d(c+3)/8$
$7/4$	$F_d(c+3)/8 + 7F_d(c+4)/16$
$\ge 15/8$	0.

The quadratic weight formula exhausts the cases. For each row of Table 1, $u + vx_i \le Z_c(x_i)$, by comparison at $1, 3/2, 7/4, 15/8$ and the fact that $v \le 0$. The initial coset contributes at least $F_d(c)$ in its own measure. From (1) we obtain

$$w \ge \frac{\alpha}{16} + 2^{-c}\big(F_d(c) + (2^c - 1)u + v\,2^{c-1}\alpha\big).$$

The last column of Table 1 gives the minimum of this affine expression at the two endpoints of $[2, U]$.

Table 1: Affine lower-bound coefficients $u + vx_i \le Z_c(x_i)$ and minima on $[2, U]$ for $d \in \{7, 8\}$.

d	c	u	v	Minimum
7	1	0	0	223/1024
7	2	255/896	−17/112	3187/14336
7	3	15/56	−1/7	13/56
7	4	123/512	−17/128	3689/16384
7	5	49/256	−15/128	1623/8192
8	1	0	0	447/2048
8	2	75/256	−5/32	913/4096
8	3	255/896	−17/112	421/1792
8	4	15/56	−1/7	3407/14336
8	5	123/512	−17/128	931/4096

For $d = 7$ the smallest bound exceeds 3393/17408 by 447/139264. For $d = 8$ the smallest exceeds 55/256 by 7/2048. □

5 Finishing the proof

For $m = 6$, only $p = 33$ lies in the residual interval, and $h \in \{11, 12\}$ (since $2m - 1 \le h \le 2m$). The inequalities in Section 2, evaluated at $t = 33/64$, give

h	lower bound on w	upper bound on w
11	191/1024	3393/17408
12	383/2048	6761/34816

Both intervals are contained in $[191/1024, 3393/17408]$. Lemma 2 yields a zero flat of codimension at most seven, contradicting the degree obstruction since $h - 4 \ge 7$.

For $m \ge 7$, we have $h \ge 13$, so $w \ge 191/1024$ and any zero flat of codimension at most eight is forbidden. Write $s_t = t - 1/2$. If $w \ge 55/256$, then

$$e_t(w) \le e_t(55/256) = \frac{9}{32} - \frac{87}{8}s_t.$$

The lower bound from Section 2 is at least $3a/256 - 2a/M^2$, since $h \ge 2m-1$. Here $24 \le a \le 392/15$ (so $3a/256 \ge 9/32$) and $s_t \ge 1/M$, since p is odd and $M/2$ is even. Comparing the two bounds on $e_t(w)$ cancels 9/32 and gives $(87/8)s_t \le 2a/M^2$, hence $87M/8 \le 2a \le 784/15$, impossible for $M \ge 128$. Therefore $w < 55/256$, and the second conclusion of Lemma 2 supplies the forbidden zero flat. This proves Theorem 1.

6 Restriction of rotation-symmetric bent functions

Corollary 1. *Let $m \geq 4$ and let $p \geq 2^{m-1}$ be an odd prime. If $f : \mathbb{F}_2^{4mp} \to \mathbb{F}_2$ is a rotation-symmetric bent function of degree at most four, then $g(x) = f(x, \ldots, x)$, where $x \in \mathbb{F}_2^{4m}$ is repeated p times, is bent.*

Proof. At frequency $(b, \ldots, b)$, rotate the input by one block. The summand in the Walsh transform is constant on each orbit. The orbits have size one or p, so reduction modulo p retains only repeated-block inputs. The repeated-block dot product equals the single-block dot product because p is odd. Therefore

$$W_g(b) \equiv W_f(b, \ldots, b) \equiv \pm 2^{2mp} \equiv \pm 2^{2m} \pmod{p}.$$

The last congruence follows from Fermat's little theorem. The repetition map is linear, so $\deg g \leq 4$, and Theorem 1 applies. □

For example, $m = 7$ and $p = 71$ recover the restriction from 1988 variables to 28. The uniform bound also allows $p = 67$ at $m = 7$, giving a restriction from 1876 variables to 28. The main theorem itself permits composite moduli, including 33 at $m = 6$.

A Earlier reductions used in the proof

The companion archive [3] preserves the earlier proof notes for the Walsh reductions under their original Portuguese filenames, indexed in English by `PROOF-INDEX.md`. We identify their exact roles here using those English titles and filenames. The final zero-flat argument, including the arithmetic of its tables, is given in full in this manuscript.

Range $t \geq 8/15$. The *uniform* 8/15 *bound* note (`proofs/rigidez_walsh_limite_8_15.md`, Sections 1–2) covers this range. The even proof uses costs of successive residue bits, and the odd proof uses the quadratic phase after affine-sign normalization.

Odd spectra below that threshold. The *nonconstant phases* note (`proofs/rigidez_walsh_1_2_fases_nao_constantes.md`, Sections 1–3) eliminates nonconstant phases. The *residual cuts* note (`proofs/rigidez_walsh_1_2_cortes_residuais.md`, Section 1) gives the obstruction to a degree drop in the constant phase. The *codimension-one reduction* note (`proofs/rigidez_walsh_1_2_fecha_codim_um.md`, Section 3) supplies the residue-bit estimates used in the *odd branch closure* note (`proofs/rigidez_walsh_ramo_impar_completo_e_limite_59_112.md`, Sections 1–4), which excludes the remaining odd case, including $m = 6$.

Even spectra. The *even low weights* note (`proofs/rigidez_walsh_1_2_ramo_par_pesos_baixos.md`, Sections 2–6) and the *residual cuts* note (`proofs/rigidez_walsh_1_2_cortes_residuais.md`, Section 2) give the low-weight and rank reductions. The *codimension-one reduction* note (`proofs/rigidez_walsh_1_2_fecha_codim_um.md`, Sections 1–2) then excludes the hyperplane case, including its exceptional range at $m = 6$. With $X \equiv 2 \pmod 4$ everywhere, these results leave $h \geq 2m - 1$ and $w \geq 23/128$.

Restrictions in the global even case. The *global even branch* note (`proofs/rigidez_walsh_constante_179_344_ramo_par_global.md`, Section 1) gives the obstruction to a degree drop. Its proof supposes that a direction of codimension $k \le h-4$ makes D cubic on every coset. On each coset, the restricted phase has semirank at least four. The cubic weight classification and the degree-six symbol of the next residue bit give a local excess cost strictly larger than e_t of the local weight. Averaging contradicts the affine formula for e_t. The *odd branch closure* note (`proofs/rigidez_walsh_ramo_impar_completo_e_limite_59_112.md`, Section 5.2) proves the second-bit energy bound used in Section 2. There the first excess bit has degree at most eight. On its zero flats, a degree-ten bit must be nonzero when the restricted phase has semirank at least seven. This is the exterior obstruction of [2, Sections 4–5]. The cost of that bit, together with the minimum and second weights of the appropriate Reed–Muller codes, gives the stated lower bound.

The exact-rational script in the companion checks the numerical comparisons used in the zero-flat argument. The geometric steps are proved separately in the text.

B Two estimates in the global even case

We give the local argument for the degree obstruction and the counting argument for the energy bound. These are the two inputs that directly connect the Walsh reduction to Lemma 2. Throughout this appendix we work on the residual interval ($m \ge 6$, $1/2 < t \le 8/15$), so $64 \mid M$, $h \ge 2m-1 \ge 11$, and $a = 8(8t-1) > 24$.

Define B_4, B_5 by

$$\frac{Y - A - (C-A)D}{16} \equiv B_4 + 2B_5 \pmod 4.$$

The progressions in Section 2 show that this quotient is integral. Since $64 \mid M$, the two bits record the parity and the next bit of the multiple of $16p$ in those progressions, up to replacing B_5 by $B_5 + B_4$ when dividing by p modulo 64. In particular this replacement has no effect on the set $B_4 = 0$. Comparing the nearest admissible value in each cell yields

$$\frac{E}{pM} \ge \begin{cases} 3a & D = 0,\ B_4 = 1, \\ a & D = 1,\ B_4 = 1, \\ b = 40(16t-1) & B_4 = 0,\ B_5 = 1. \end{cases}$$

The minimizing magnitudes in the first two rows are $14p - M$ and $10p - M$, respectively. In the last row, the two candidates are $30p - M$ and $26p - M$, of which the latter gives the smaller excess after subtracting the appropriate baseline square.

B.1 Degree obstruction on affine flats

Write $[P]_j$ for the degree-j symbol in the exterior algebra of the coordinate linear forms, and γ_i for its divided powers. We use the residue-bit identities from the *global even branch* note (`proofs/rigidez_walsh_constante_179_344_ramo_par_global.md`, Section 1 of [3]). On a flat where D has degree at most three, B_4 has degree at most six, and

$$[B_4]_6 = \gamma_2([D]_3) + \gamma_3([Q]_2),$$

with all polynomials restricted to that flat. The identities follow by expanding the phase and comparing coefficients modulo 32. When the first summand vanishes, the relative weight of B_4 is at least $1/64$ if the restricted phase has semirank three, and $1/32$ if it has semirank at least

four. For the stronger bound, restrict to each translate of a symplectic eight-space. The degree-six symbol is dual to a rank-eight alternating form there. In eight variables, a degree-six word has weight at least four, and the words of weights four and six have dual symbols of ranks two and four by Kasami–Tokura [4]. Thus each restriction has absolute weight at least eight.

Suppose the quartic symbol of D vanishes on a direction of codimension $k \le h - 4$. On every coset J of that direction, D is at most cubic and the semirank of the restricted phase is at least $h - k \ge 4$. Write $v = \mathbb{E}_J D$. Since $a > 24$, each point with $B_4 = 1$ contributes at least $a > 24$ to $E/(pM)$, and at least $3a = a + 2a > 24 + 48 = 72$ when $D = 0$. Compare the local cost $\mathbb{E}_J E/(pM)$ with $e_t(v)$. For $v \ge 1/4$, the latter is negative since $t > 1/2$. For $v = 0$, the cost is at least $72/32 > 2 \ge e_t(0)$. The other possibilities are classified by the cubic weights below twice the minimum distance.

- If $v = 1/8$, the support is a codimension-three flat and the cubic symbol is decomposable. Its second divided power vanishes, so B_4 has weight at least $1/32$. Hyperplanes avoiding the support cover its complement with uniform multiplicity and retain semirank at least three. On each of them the weight of B_4 is at least $1/64$. The total cost is at least $24/32 + 48(7/8)/64 = 45/32 > e_t(1/8)$.

- If $1/8 < v < 1/4$ and there is a common affine factor, then $v \ge 3/16$. On the zero hyperplane of that factor, the phase has semirank at least three and $D = 0$. The cost is at least $72/(2 \cdot 64) = 9/16 > e_t(v)$.

- The remaining form is a sum of two disjoint triple products and $v = 7/32$. Its second divided power is a decomposable degree-six form. On a symplectic eight-space its dual has rank at most two and thus cannot cancel the dual of the phase term, which has rank eight. The symbol of B_4 is therefore nonzero. The local cost is at least $24/64 = 3/8 > e_t(7/32)$.

Every coset gives a strict inequality. Since e_t is affine in the weight, averaging contradicts $\mathbb{E}E/(pM) = e_t(w)$.

B.2 Lower bound from the excess bits

Set $\delta = 2^{-8}$, $k_0 = h - 7$, and $\omega = \mathbb{E}B_4$. The residue-bit expansion gives $\deg B_4 \le 8$. On a zero flat of B_4, the next bit B_5 has degree at most ten. The exterior obstruction of [2, Section 4] forces it to be nonzero if the restricted semirank is at least seven. If the semirank is at least eight, its weight is at least $(3/2)2^{-10}$. Indeed, a minimum-weight word would have flat support. A hyperplane avoiding that support would make both bits zero while retaining semirank at least seven.

Suppose that the energy budget is smaller than $a(3 - 2^{1-k_0})\delta$. Then $\omega < (3 - 2^{1-k_0})\delta$. If $B_4 = 0$, the improved lower bound on B_5 alone costs more than $3a\delta$. For $0 < \omega < 2\delta$, Kasami–Tokura [4] gives three cases. When at least two factors are common, the complement of the common support flat has density at least $3/4$ and is uniformly covered by zero hyperplanes. For two disjoint eight-fold products, the points outside both support flats are uniformly covered by zero flats of codimension two. Their density is $(255/256)^2 > 3/4$: in the two independent blocks, impose one nonzero linear form equal to one in each block. These cuts retain semirank at least eight (since $h \ge 11$ and imposing two linear equations drops the semirank by at most two). In both cases the cost of B_5 alone is at least $(3/4)(3/2)b2^{-10} > 3a\delta$. With just one common factor and two disjoint seven-fold products, $\omega \ge (7/4)\delta$ and there is a zero hyperplane. The combined cost is at least $(7/4)a\delta + (3/2)b2^{-11} > 3a\delta$.

Finally suppose $2\delta \le \omega < (3 - 2^{1-k_0})\delta$, and take the smallest $k \ge 2$ with $\omega < (3 - 2^{1-k})\delta$. The Klein–Storme theorem [5] provides a zero flat of codimension $k \le k_0$. Minimality gives $\omega \ge$

$(3 - 2^{2-k})\delta$. If $k < k_0$, the flat retains semirank at least eight, and the total cost is at least

$$a(3 - 2^{2-k})\delta + \frac{3}{2}b2^{-10-k} > 3a\delta.$$

If $k = k_0$, the semirank is at least seven. The minimum-distance bound gives a total cost at least

$$a(3 - 2^{2-k_0})\delta + b2^{-10-k_0} > a(3 - 2^{1-k_0})\delta.$$

The comparisons use $(3/2)b > 16a$ and $b > 8a$ on the residual interval. In all cases the cost exceeds the assumed budget, proving the lower bound in Section 2.

Use of generative AI

Generative AI tools assisted with algebraic exploration, arithmetic checks, and preparation of the manuscript.

References

[1] F. M. Vono, A. O. Naufel de Toledo, and V. G. Santos. Modular Walsh rigidity for Boolean functions of degree at most four. IACR ePrint 2026/2900 (original version); doi:10.6084/m9.figshare.34963642.

[2] F. M. Vono, A. O. Naufel de Toledo, and V. G. Santos. Walsh rigidity modulo 17 for Boolean functions of degree at most four in twenty variables. Figshare preprint, doi:10.6084/m9.figshare.35059441.

[3] F. M. Vono, A. O. Naufel de Toledo, and V. G. Santos. Proof companion for the uniform half-threshold theorem. Archive accompanying doi:10.6084/m9.figshare.34963642. See `PROOF-INDEX.md` for the proof notes and exact-arithmetic verifier.

[4] T. Kasami and N. Tokura. On the weight structure of Reed–Muller codes. *IEEE Trans. Inform. Theory* 16 (1970), 752–759. doi:10.1109/TIT.1970.1054545.

[5] A. Klein and L. Storme. On the non-minimality of the largest weight codewords in the binary Reed–Muller codes. *Adv. Math. Commun.* 5 (2011), 333–337. doi:10.3934/amc.2011.5.333.