Homogeneous rotation symmetric bent functions in twelve variables are quadratic

Filipe Martins Vono[1] André Oliveira Naufel de Toledo[1] Valéria Gonzaga Santos[2]
0009-0009-4994-8533 0000-0002-0619-6820 0009-0009-1333-2518
[1]Centro Universitário de Belo Horizonte (UniBH), Belo Horizonte, Brazil
[2]American Global Tech University (AGTU). Correspondence: contatofilipevono@gmail.com

IACR Generative AI Policy: Substantial AI contribution.
The authors used generative AI tools to assist with exposition, algebraic exploration, and verification code.

Abstract. Every homogeneous rotation symmetric bent Boolean function in twelve variables is quadratic. There are exactly sixteen such functions in labelled coordinates. The main step is to rule out degree four. The proof groups inputs according to which opposite coordinates agree. Walsh divisibility forces the restriction to each group to be quadratic. The squared Walsh sums of these restrictions must then fit a fixed total. This rules out one of the three possible restrictions on the diagonal and severely limits the other two. Explicit polynomial identities exclude the remaining possibilities. The supplement gives the identities, the case coverage and code to verify the calculations.

Keywords. Bent function; rotation symmetry; homogeneous Boolean function; Walsh transform; quadratic form; Pfaffian.

1 Introduction

A bent Boolean function has the largest possible distance from the set of affine Boolean functions. Rotation symmetry imposes a different kind of restriction: cycling the coordinates must leave the function unchanged. These two requirements are compatible, and rotation symmetric bent functions of degree greater than two are known. Requiring the algebraic normal form to be homogeneous makes the problem much more restrictive. The conjecture that every homogeneous rotation symmetric bent function is quadratic has motivated both searches and nonexistence results [1–4].

For twelve variables, the classification rests on ruling out degree four. A homogeneous quartic rotation symmetric function in twelve variables is specified by forty three orbit coefficients, so direct testing would involve 2^{43} functions. The proof uses the geometry of the six antipodal coordinate pairs to reduce the number of cases. The restrictions to the corresponding affine spaces become quadratic, allowing their Walsh sums to be controlled by ranks, radicals and a small number of symmetry types.

Theorem 1. Let $f : \mathbb{F}_2^{12} \to \mathbb{F}_2$ be homogeneous and invariant under cyclic rotation by one coordinate. If f is bent, then $\deg f = 2$.

The conclusion can be made explicit. With subscripts taken modulo twelve, define

$$C_d^{(12)}(x) = \sum_{i=0}^{11} x_i x_{i+d} \quad (1 \le d \le 5), \qquad C_6^{(12)}(x) = \sum_{i=0}^{5} x_i x_{i+6}.$$

Corollary 2. The functions in Theorem 1 are exactly

$$f = \sum_{d=1}^{6} c_d C_d^{(12)}, \qquad c_6 = 1, \qquad c_1 + c_2 + c_4 + c_5 = 0.$$

Consequently, there are sixteen functions in the fixed labelled coordinate system. This count concerns functions, rather than equivalence classes under changes of coordinates.

The list of quadratic functions follows from the circulant criterion in [7]. Ruling out quartic functions completes the classification. Degrees five and six are excluded by the bounds for homogeneous bent functions of Meng, Zhang, Yang and Cui [5]. A short argument using the same antipodal coordinates excludes degree three. Reference [8] gives a more general result for rotation symmetric functions of degree at most three. Section 7 gives a direct proof for twelve variables.

Earlier work provides several complementary approaches to the conjecture. Stănică and Maitra [1] formulated it following computations in small dimensions. Meng, Chen and Fu [2] obtained further nonexistence results, and Cusick and Sanger [3] studied the case of twice an odd prime. Sun, Shi, Liu and Fu [4] developed derivative and orbit arguments under arithmetic hypotheses on the number of variables. In particular, the prime size hypothesis in their Theorems 1 and 2 does not cover $12 = 4 \cdot 3$. The proof here uses the specific antipodal geometry of twelve variables. It establishes this dimension of the conjecture and supplies finite certificates that expose the remaining algebra after the structural reductions.

The quartic proof starts by fixing the pattern of agreements between opposite coordinates. Each pattern leaves six free bits. The pattern with all pairs equal is the diagonal, and the pattern with all pairs different is the complementary coset. These two restrictions already explain the simplest contradiction. A constant restriction on the diagonal uses the entire sum of squares allowed by bentness, but the complementary coset always contributes a positive amount.

Sections 2 and 3 establish this constraint and show why the quartic problem has only three diagonal types. In the other two types, a particular restriction must be balanced. Its balance guarantees a vector in its radical on which it takes value one. Once that vector is fixed, these two requirements give affine equations in the polar coefficients. Sections 4–6 cover the possible supports and exclude each case. The supplement records the exact identities and gives a verifier. Section 7 combines the quartic exclusion with the results for the other degrees.

2 Partial Walsh transforms in antipodal coordinates

For $a \in \mathbb{F}_2^{12}$, the Walsh transform is $W_f(a) = \sum_x (-1)^{f(x)+a\cdot x}$. The function is bent if $|W_f(a)| = 64$ for every a. In that case its nonlinearity is $2^{11} - 2^5 = 2016$, and its dual is defined by $W_f(a) = 64(-1)^{f^*(a)}$. We use the usual strict homogeneity convention: every nonzero ANF monomial has the same degree, with no additional lower degree terms.

Write an input as $x = (u, v)$, with $u, v \in \mathbb{F}_2^6$, and make the invertible change of coordinates

$$z = u + v, \qquad w = v, \qquad g_z(w) = f(z + w, w).$$

Fixing z gives a coset of the antipodal diagonal $U = \{(w, w) : w \in \mathbb{F}_2^6\}$. For $b \in \mathbb{F}_2^6$, let

$$r_b(z) = \sum_{w \in \mathbb{F}_2^6} (-1)^{g_z(w)+b\cdot w}.$$

The Walsh transform in the new coordinates is the transform in z of r_b. If f is bent, all these Walsh coefficients have modulus 64, and Parseval gives, for every b,

$$\sum_z r_b(z)^2 = 4096. \tag{1}$$

Think of the values $r_b(z)$ as a table with 64 rows indexed by z and 64 columns indexed by b. In column zero, $r_0(z)$ counts zeros minus ones of g_z. A balanced row contributes zero to (1). A constant row contributes $64^2 = 4096$, so every other row in that column must be balanced.

Let $R(w_0, \ldots, w_5) = (w_5, w_0, \ldots, w_4)$ denote the rotation on six coordinates. In the original twelve coordinates a rotation moves the last coordinate of each half to the first position of the other half. Consequently it sends (z, w) to $(Rz, Rw + z_5 e_0)$. In particular, $r_0(Rz) = r_0(z)$.

Let $\mathbf{1} = (1, 1, 1, 1, 1, 1)$. Half rotation exchanges u and v, so rotation symmetry implies

$$g_z(w + z) = g_z(w). \tag{2}$$

When g_z is quadratic, write $\mathcal{B}_z$ for its alternating polar matrix. Equation (2) gives $\mathcal{B}_z z = 0$. Hence, for $z \neq 0$, the rank is even and at most four. Its quadratic character sums are therefore either zero or have modulus 16, 32 or 64.

We use masks for a few particular vectors: m denotes the vector with coordinates given by the binary digits of m, with coordinate zero least significant. Thus $1 = e_0$, $9 = e_0 + e_3$, $27 = e_0 + e_1 + e_3 + e_4$, and $63 = \mathbf{1}$. In the supplement, five bit masks encode radical witnesses in coordinates $w_1, \ldots, w_5$; twelve bit masks encode subsets of the original coordinates.

2.1 A complementary coset cannot be balanced

For six variables, let C_1, C_2 be the sums of all unordered pairs at cyclic distances one and two, respectively, and put

$$C_3(w) = w_0 w_3 + w_1 w_4 + w_2 w_5.$$

Lemma 3. Suppose that f is rotation symmetric and that g_{63} is quadratic. Then

$$g_{63}(w) = c + \alpha C_1(w) + \beta C_2(w) + \alpha(w_1 + w_4) + (\alpha + \beta)(w_2 + w_3). \tag{3}$$

For $(\alpha, \beta) = (0,0), (1,0), (0,1), (1,1)$, the respective values of $|r_0(63)|$ are $64, 16, 16, 32$. In particular, this sum never vanishes.

Proof. Rotation on the complementary coset induces $T(w) = (w_5 + 1, w_0, w_1, w_2, w_3, w_4)$. Thus $g_{63} \circ T = g_{63}$. Its quadratic part must be a combination of C_1, C_2, C_3. The constant terms of this equality give $\ell_0 = 0$. Comparing the linear coefficients then gives the linear part in (3) and forces the coefficient of C_3 to vanish. For $(\alpha, \beta) = (1,0)$ or $(0,1)$, the polar has rank four and its radical is spanned by the indicators of the even and odd positions. The nonconstant part of (3) vanishes on

this radical, giving modulus sixteen. For $(1,1)$, the rank is two; a radical basis consists of the three antipodal pairs and $e_0 + e_1 + e_2$, and the same vanishing gives modulus thirty two. The constant case gives modulus sixty four. $\square$

This lemma yields a useful obstruction whenever $g_0 = 0$: the row $z = 0$ already contributes 64^2 to (1), while $z = 63$ contributes a positive amount.

3 Why the quartic restrictions become quadratic

For the remainder of Sections 3–6, suppose that f is homogeneous quartic and rotation symmetric. Let $O_0, \ldots, O_{42}$ be the sums of the distinct cyclic orbits of quartic monomials, ordered by their smallest twelve bit mask, and write $f = \sum_j t_j O_j$.

For an eight element subset S of the twelve coordinates, define

$$Q_S = \sum_{\{M, S\setminus M\}} t_{[M]} t_{[S\setminus M]}, \tag{4}$$

where the sum is over the thirty five unordered partitions into four element sets, and $[M]$ is the orbit index of M.

Lemma 4. If f is bent, then $Q_S = 0$ for every S in (4). Moreover, the two linear forms

$$L_1 = t_0 + t_4 + t_7 + t_9 + t_{22} + t_{27} + t_{29} + t_{37},$$

$$L_2 = t_1 + t_3 + t_5 + t_8 + t_{24} + t_{28} + t_{34} + t_{36}$$

vanish, and every g_z is quadratic in w.

Proof. Expand $(-1)^f$ as a product of the factors $1 - 2x^M$ belonging to its ANF. Its integer multilinear coefficient at x^S is $4Q_S$ modulo eight. Walsh inversion for a bent function expresses the same coefficient as four times a sum of sixteen signs. It is therefore divisible by eight.

The polynomial identities in Supplement S1 express L_1, L_2 as combinations of the Q_S, in the Boolean coefficient ring $t_j^2 = t_j$. Thus both forms vanish before any quadratic restriction is assumed.

On the diagonal, a monomial and its half rotation agree. They cancel unless the support is fixed by half rotation. A fixed quartic support is a union of two opposite pairs, so it becomes a quadratic monomial in w.

The only mixed terms with more than two w-variables have the form $z_i w_J$, where J has three elements. If $i \in J$, a contributing quartic monomial uses both members of the opposite pair at i and one member from each of the other two pairs. Half rotation toggles those two choices, so the contributions cancel in pairs.

If $i \notin J$, a contributing monomial picks one coordinate from each of the four opposite pairs indexed by $\{i\} \cup J$. The choice at pair i is fixed by the requirement to produce z_i. The eight choices thus select one representative from each pair of complementary supports. Up to rotation, the sets of pair indices are $0134, 0123, 0124$. For 0134, rotation by three steps preserves the set and swaps the complementary pairs in twos, so their orbit coefficients cancel. Indeed, its square is the half rotation, which swaps the two supports within each pair, so it cannot fix a pair. For 0123 and 0124,

the orbit coefficients sum to L_1 and L_2, as recorded in Supplement S1. All mixed terms of degree three in w therefore vanish. □

The same fixed point count simplifies the three equations (4) whose supports are unions of the four antipodal pairs just used. Put $(q, r, s) = (t_{42}, t_{30}, t_{40})$. After $L_1 = L_2 = 0$, they read

$$r + s + q = 0, \qquad r + s + rq = 0, \qquad sq = 0.$$

Their only solutions are

Case	(t_{42}, t_{30}, t_{40})	g_0
A	$(0, 0, 0)$	0
B	$(0, 1, 1)$	$C_1 + C_2$
C	$(1, 1, 0)$	$C_1 + C_3$

Indeed, $g_0 = t_{30}C_1 + t_{40}C_2 + t_{42}C_3$. Lemma 3 and (1) exclude A immediately. The corresponding zero frequency sums on the diagonal in B and C are 0 and 32.

4 Constraints that depend only on the polar matrices

The entries of $\mathcal{B}_z$ have degree at most two in z. They are determined by twenty one linear combinations of the orbit coefficients. We use the three diagonal parameters $(u_{30}, u_{40}, u_{42}) = (t_{30}, t_{40}, t_{42})$, followed by

$$(a, b, c, d, e, g, h, k, m, n, p, r, A_1, A_2, A_3, B_1, B_2, B_3). \tag{5}$$

Supplement S1 defines these combinations and gives three generating entries of $\mathcal{B}_z$; rotation gives all the others. Set

$$\alpha = p + A_2 + B_1 + B_2, \qquad \beta = r + A_1 + A_3 + B_2 + B_3, \qquad Y = a + d + h + m. \tag{6}$$

The pair α, β controls the complementary row through (3). We reserve the calligraphic letter $\mathcal{B}_z$ for polar matrices; the letters B_1, B_2, B_3 in (5) are scalar coordinates.

Lemma 5. The following conditions are necessary for bentness.

(i) For every $d_0 \neq 0$, the number $N_{d_0} = \#\{z : \mathcal{B}_z d_0 = 0\}$ is even.

(ii) For every two element set D and four element set I of six coordinate positions,

$$\Phi_{D,I} := \sum_{z \supseteq D} \mathrm{Pf}(\mathcal{B}_z|_I) = 0. \tag{7}$$

Here, for $I = \{i, j, k, l\}$ in increasing order, the Pfaffian is $b_{ij}b_{kl} + b_{ik}b_{jl} + b_{il}b_{jk}$, where $b_{ij} = (\mathcal{B}_z)_{ij}$.

Proof. A bent function has zero autocorrelation in every nonzero direction. Translate both halves of the original input by d_0. This keeps z fixed and sends w to $w + d_0$. The sum within a row is zero

unless $\mathcal{B}_z d_0 = 0$, in which case it is 64 or -64. The total can vanish only if the number of nonzero summands is even.

For (ii), fix $z_i = 1$ for $i \in D$ and $w_i = 0$ for $i \notin I$. This is an affine space of dimension eight. Walsh inversion makes its sign sum four times a sum of sixteen signs, hence a multiple of eight. On each row, a quadratic sum in four variables divided by four is odd exactly when its polar has rank four. That parity is the Pfaffian in (7). Summing the row parities proves the claim. □

Because each Pfaffian has degree at most four in z, $\Phi_{D,I}$ is also its coefficient at z^{D^c}. This makes the identities in (7) particularly small: only products of quadratic coefficients on complementary pairs of positions contribute.

For $d_0 = 63$, rotation leaves the set counted by N_{63} invariant. Only four six bit orbits have odd size, represented by $0, 9, 27, 63$. Evaluating $\mathcal{B}_z\mathbf{1}$ on these representatives gives

$$N_{63} \equiv u_{30} + u_{40} + u_{42} + \alpha + \beta + (1 + u_{42})Y \pmod 2. \tag{8}$$

The degree vectors and the four indicators are recorded in Supplement S1. This parity identity gives a direct entry to C.

4.1 From a balanced row to a radical witness

The restriction g_1 is a pure quadratic form: its values at $0, e_0, \ldots, e_5$ vanish because they evaluate f on inputs of weight at most three. Equation (2) also makes w_0 absent. Write $E = \mathcal{B}_1|_{\{1,\ldots,5\}}$ and $q_E(w) = \sum_{i<j} E_{ij} w_i w_j$.

A pure quadratic form has zero sign sum if and only if some radical vector y satisfies $q_E(y) = 1$. To see this, sum by cosets of the radical. A nonzero linear restriction to the radical cancels every coset; a zero restriction leaves a nondegenerate quadratic sum on the quotient, which is nonzero. Thus, whenever $r_0(1) = 0$,

$$Ey = 0, \qquad q_E(y) = 1 \tag{9}$$

has a solution. These are affine equations in the polar coefficients once y is fixed.

The possible supports are few. In C,

$$E_{24} = E_{12} + E_{15} + E_{45} = E_{13} + E_{25} + E_{34} = E_{14} + E_{23} + E_{35} = 0. \tag{10}$$

In B, the first two expressions in (10) equal one and the last two equal zero. In both cases the sum of all ten edges is zero. Witnesses of weights one or five therefore have quadratic value zero. At weight two, the value equals $E(y, e_i)$ for either position in the support; at weight four it equals $E(y, e_j)$ for the missing position. These values vanish on the radical.

For weight three, the remaining exclusions follow from the following identities in C; the identities for 134 and 235 also hold in B.

Support of y	124	134	135	234	235	245
$q_E(y) = E(y, \mathbf{1}_J)$, with $J =$	1	235	24	3	134	5

Reflection of the twelve indices, $i \mapsto -i$, preserves the problem. On the row $z = 1$, it reverses positions $1, \dots, 5$, so the witness supports 123 and 345, 124 and 245, and 125 and 145 are paired. Supports 234 and 135 are fixed. The diagonal type and the common value $\alpha = \beta$, when available, are preserved. These supports give a covering by witness branches; a function may have more than one witness.

5 Excluding case C

In C, (8) and Lemma 5 give $\alpha = \beta$. If both are zero, the rows 0 and 63 contribute $32^2 + 64^2 > 4096$ to (1). Hence $\alpha = \beta = 1$ and $|r_0(63)| = 32$.

We next show that $r_0(1) = 0$. Suppose otherwise. Its six rotations have equal sums. Their moduli must be sixteen, since modulus thirty two would already exceed (1) together with rows zero and sixty three. The remaining squared mass is 512. Every other nonconstant orbit has size at least three, except $\{21, 42\}$. Thus these two rows must each have modulus sixteen and all other rows must vanish.

Put $s_z = r_0(z)/16$. Bentness implies $F(v) = \sum_z s_z(-1)^{z \cdot v} \in \{4, -4\}$. Expanding the character modulo eight, or taking its integer multilinear coefficients, gives

$$\sum_{z : z_i = z_j = 1} s_z \equiv 0 \pmod 2 \qquad (i \neq j). \tag{11}$$

For $(i, j) = (0, 2)$, the proposed support makes this sum $s_{21} + s_{63}$, which is odd. This contradiction proves that the unit row is balanced.

Equations (9)–(10) now give the four supports $123, 125, 145, 345$. Reflection leaves two representatives, 123 and 125, with five bit masks 7 and 19. In each branch, (9) and $\alpha = \beta = 1$ give seven affine substitutions in (5). There are twenty five distinct nonzero conditions (7). Their explicit sums in Supplement S3 give a contradiction after one additional binary split in each branch.

For clarity, the first branch begins as follows. Write $(v_0, \dots, v_{17})$ for (5), and let F_i be the conditions indexed in Supplement S3, after the initial substitutions. The common equation $F_{23} = 0$ gives $v_{11} = v_0 + v_8 + v_{10}$. In the branch $y = 7$, split $v_8 = v_0$ or $v_8 = 1 + v_0$. In the first subcase, successive expansion gives

$$F_2 + F_8 + F_{10} = 1 + v_{12} + v_{13} + v_{14},$$

$$F_6 + F_{12} + F_{19} = 1 + v_1 + v_4, \qquad F_7 + F_{21} = 1.$$

The last identity is read after substituting the two affine equalities supplied by the preceding sums. All the F_i must be zero, so it is impossible. The other value of the bit and the two subcases for $y = 19$ are recorded in the same format. This excludes C.

6 Excluding case B

In B we first need to prove that the unit row $z = 1$ is balanced. The route goes through two other rows. The spectrum forces row 27 to be balanced, and symmetry of that row then constrains the

complementary row 63. Once the latter is constrained, the same spectrum lemma settles row 1.

Lemma 6. In B, let $s_z = r_0(z)/16$. Then $s_{27} = 0$. If $|s_{63}| = 4$, all other entries vanish. If $|s_{63}| = 2$, the only other active orbit is represented by 9, with $s_9 = -s_{63}$.

Proof. Rotation makes s constant on six bit cyclic orbits. We have $s_0 = 0$, $\sum s_z^2 = 16$, and $|s_{63}| \in \{1, 2, 4\}$. Besides (11), the character expansion gives

$$\sum_z s_z \equiv 4 \pmod 8, \qquad \sum_{z:z_i=1} s_z \equiv 0 \pmod 4. \tag{12}$$

There are only fourteen orbits. The orbit sizes and the three pair incidences in Supplement S2 reduce (11)–(12) to the following list: the two patterns in the statement, or $s_9 = s_{63} = \pm 1$ together with two orbits of size six having opposite values ± 1. Their representative pairs are $(1, 11), (1, 13), (31, 11), (31, 13), (3, 23), (15, 5)$. None contains the orbit of 27. The supplement gives the elimination by orbit size and congruences, including the case $|s_{63}| = 1$. □

6.1 Period three symmetry forces two equal parameters

For $z = (\delta, \delta) \neq 0$, with $\delta \in \mathbb{F}_2^3$, write $w = (v + u', u')$ and define $\tilde{g}_z(v, u') = g_z(v + u', u')$. The rotation by three places fixes z and sends (v, u') to $(v + \delta, u' + v)$. Comparing coefficients under this change gives the following polar matrix and linear coefficients in the new coordinates:

$$\widetilde{\mathcal{B}}_z = \begin{pmatrix} A & D \\ D & 0 \end{pmatrix}, \quad D = D^{\mathsf{T}}, \quad D\delta = 0, \quad \ell_{u'} = A\delta + \operatorname{diag} D. \tag{13}$$

The tilde distinguishes the matrix in (v, u') from $\mathcal{B}_z$ in w. In particular, $A_{ik} = (\mathcal{B}_z)_{ik}$ and $D_{ik} = (\mathcal{B}_z)_{ik} + (\mathcal{B}_z)_{i,k+3}$ for $0 \leq i, k < 3$.

If D has rank two, then $\ker D = \langle \delta \rangle$. Since A is alternating, $A\delta$ is orthogonal to δ, so $Du_0 = A\delta$ has a solution. The radical of the full polar is spanned by $(0, \delta)$ and (δ, u_0). The nonconstant part of $\tilde{g}_z$ vanishes on these generators. At the first this follows from $\ell_{u'} \cdot \delta = 0$ in (13). At the second the mixed term vanishes since $D\delta = 0$, invariance gives $q_A(\delta) + \ell_v \cdot \delta = 0$, and $\ell_{u'} \cdot u_0 = u_0^{\mathsf{T}} D u_0 + \operatorname{diag}(D) \cdot u_0 = 0$. Thus the full polar has rank four and $|r_0(z)| = 16$.

Put $X = p + r$ and $J = A_1 + A_2 + A_3 + B_1 + B_3$. Equation (6) gives $X + J = \alpha + \beta$. The generating entries in Supplement S1.1 give

$$D_{27} = \begin{pmatrix} X & X & Y \\ X & X & Y \\ Y & Y & 0 \end{pmatrix}, \qquad D_9 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & X & J \\ 0 & J & X \end{pmatrix}. \tag{14}$$

If $Y = 1$, then D_{27} has rank two, so row 27 has a nonzero Walsh sum at frequency zero. Lemma 6 requires that sum to vanish. Hence $Y = 0$. To transfer this information to the complementary row, use the coefficient identity

$$[z_0 z_2 z_3 z_5] \operatorname{Pf}(\mathcal{B}_z|_{\{0,1,3,4\}}) = Y + \alpha + \beta + u_{42}(p + r). \tag{15}$$

The left hand side vanishes by (7). Since $Y = u_{42} = 0$, we get $\alpha = \beta = \varepsilon$. If $\varepsilon = 0$, Lemma 3 gives $|r_0(63)| = 64$, and the complementary row uses the entire sum of squares. If $\varepsilon = 1$, Lemma 3 gives

$|r_0(63)| = 32$, and Lemma 6 allows only the orbit of row 9 to contribute alongside it. In both cases $r_0(1) = 0$. In the second case $|r_0(9)| = 32$, so its polar has rank two and all its order four Pfaffians vanish.

6.2 A covering by ten radical branches

The witness argument in Section 4 leaves the eight triple supports 123, 124, 234, 125, 135, 145, 245, 345. Up to reflection, five remain, for each value of ε. For each such choice, impose

$$Y = 0, \quad \alpha = \beta = \varepsilon, \quad Ey = 0, \quad q_E(y) = 1. \tag{16}$$

One further quadratic form is impossible by (1). It is the form on five positions with every edge except 14 and 25. Setting $P = w_1 + w_4$, $Q = w_2 + w_5$, $H = w_3$, it equals $PQ + PH + QH$. On column nine, its six unit rows have moduli $0, 32, 32$, each twice, and row zero has modulus thirty two. Their squared mass is 5120. Supplement S4 gives the three variable character sum producing these values.

After the affine substitutions (16), use (7), this forbidden form, and the local Pfaffians at row nine when $\varepsilon = 1$. Successive sums of these equations yield the following complete reduction.

Five bit witness mask	Support	$\varepsilon = 0$	$\varepsilon = 1$
7	123	Contradiction	Contradiction
11	124	Contradiction	Contradiction
14	234	One parameter family	Four polars
19	125	Contradiction	Contradiction
21	135	Contradiction	Six polars

Supplement S4 gives the identities for all ten branches. Each step adds specified necessary equations, obtains an affine equality, and substitutes it. A sum equal to one closes a branch. Whenever an identity depends on the value of an undetermined bit, the tables give both paths.

A shared argument forces $a = d$ in the two branches with $\varepsilon = 1$. The initial equations give $h = a$ and $b+g+k+n = a+d$. On row 9, (13) gives $\ell_{u'} = (0, e+X, c+X)$, using $(\mathcal{B}_9)_{01} = e$ and $(\mathcal{B}_9)_{02} = c$ from Supplement S1.1. For fixed v, the sum of $(-1)^{\tilde{g}_9(v,u')}$ over u' vanishes unless $D_9 v = \ell_{u'}$. Since $J = X$, the image of D_9 lies in $\{0, (0,1,1)\}$. The required nonzero value of $r_0(9)$ therefore gives $c = e$, and gives $c = e = 0$ if $X = 0$.

Suppose $a + d = 1$. The first Pfaffian sum in Supplement S4.3 gives $X = 0$ using $c = e$. Row 9 then gives $c = e = 0$, which is needed for the remaining three sums. In order, these give

$$A_1 + A_2 + A_3 = 0, \quad p = 1, \quad bg + bk + gk = 1.$$

With these same coefficients, the quadratic sum on the unit row gives

$$r_0(1) = 16(bg + bk + gk).$$

The bit on the right is one, so the sum is 16. This contradicts $r_0(1) = 0$. Supplement S4.3 gives the evaluation by completing a quadratic pair.

The complete coordinate formulas are in Supplement S4.4. When $\varepsilon = 0$, the surviving family has one free bit, x. Its two choices give $N_1 = 11$ and $N_1 = 5$. Both violate the parity condition in Lemma 5(i).

When $\varepsilon = 1$, support 234 gives four polar candidates, indexed by the bits x, t. Support 135 gives six, indexed by x, t, u with $(1 + x + t)(1 + u) = 0$. We now use the Walsh sums to reduce these ten candidates to two.

6.3 Two spectral checks leave two polars

The test on row 9**.** This row must have zero frequency Walsh modulus 32. If $p = r = 1$, then $X = J = 0$, so $D_9 = 0$. Equations (13)–(14) give the linear part $(0, e, c) \cdot u'$. Therefore $c = e = 1$ would make row nine balanced, a contradiction. This removes $y = 14, t = 1$ and $y = 21, u = 1, t = 0$, four polars altogether.

The test on column 63**.** For the other four choices with $p = r = 1$, consider column sixty three. The diagonal gives $r_{63}(0) = -32$. If f^* is the bent dual, the function $G(v) = f^*(v, v + \mathbf{1})$ has Walsh transform r_{63}. Rotation makes G invariant under $v \mapsto Rv + e_0$, whose orbits have sizes $12, 12, 12, 12, 12, 4$. Since G has weight forty eight, its zeros are the short orbit and one long orbit. The five possibilities, tabulated in Supplement S2, require either modulus sixteen on at least one of rows $3, 5, 15, 23$, or modulus thirty two on row 27.

For the four choices in question, the polars of rows $3, 5, 15, 23$ have rank at most two by the factorizations in Supplement S5. Their quadratic sums cannot have modulus 16. On row 27, $D_{27} = 0$ and $\delta = e_0 + e_1$. Equation (13) gives $(\ell_{u'})_0 = (\mathcal{B}_{27})_{01} = p = 1$. The character $\mathbf{1} \cdot (v + u', u')$ depends only on v. Summing over u' therefore gives $r_{63}(27) = 0$. This excludes the last of the five column patterns.

The final two candidates. Only $y = 21, u = 0, x \neq t$ remains. In the order consisting of the three diagonal parameters followed by (5), these two polars are

$$P = 11001000010000010100 00, \qquad P' = 11010111010111101010 00 00.$$

Fixing the polar still leaves twenty free bits among the original orbit coefficients. We rule out every choice of those bits by adding equations from Lemma 4. On the fibre of P,

$$Q_{255} + Q_{831} = 1 + T, \qquad Q_{639} + Q_{1215} = T,$$

where $T = t_{22} + t_{23} + t_{27} + t_{29} + t_{32} + t_{37}$. On the fibre of P',

$$Q_{255} + Q_{831} = 1 + T_1, \quad Q_{703} + Q_{1343} = T_2,$$

$$Q_{639} + Q_{1215} + Q_{1375} = T_3,$$

with

$$T_1 = t_{21} + t_{22} + t_{27} + t_{29} + t_{33} + t_{37} + t_{38} + t_{41},$$

$$T_2 = t_{21} + t_{26} + t_{31} + t_{33} + t_{38} + t_{41}, \qquad T_3 = t_{22} + t_{26} + t_{27} + t_{29} + t_{31} + t_{37}.$$

Since $T_1 + T_2 + T_3 = 0$, summing the two identities for P, or the three for P', gives $1 = 0$. Each Q must vanish by Lemma 4. These are identities on the full twenty dimensional affine fibres defined by the polar and $L_1 = L_2 = 0$; no choice of phase coefficients is omitted. They are checked by substituting those affine equations into (4). This excludes B and completes the quartic nonexistence proof.

7 Completing the classification

Proof of Theorem 1. The degree of a bent function in twelve variables is at most six [6]. The bounds of Meng, Zhang, Yang and Cui [5] exclude homogeneous degrees six and five: in $2m$ variables, degree m is impossible for $m > 3$, and degree $m - 1$ for $m > 4$.

For a homogeneous cubic rotation symmetric function, half rotation pairs every cubic support with a distinct support. Thus $f(w, w) = 0$. After the antipodal coordinate change, a term of degree three in w could have no z factor, since the total degree is at most three. Its coefficient is therefore already visible on the diagonal, where it vanishes. Hence every g_z is quadratic. Lemma 3 and (1) now contradict $g_0 = 0$. The quartic case was excluded in Sections 3–6, and affine functions are not bent. Only degree two remains. □

Proof of Corollary 2. Every homogeneous rotation symmetric quadratic has the stated expansion in the six pair orbits. Such a quadratic is bent exactly when its alternating polar is nonsingular. That polar is circulant, with polynomial

$$P(X) = c_6 X^6 + \sum_{d=1}^{5} c_d (X^d + X^{12-d}).$$

It is invertible precisely when $\gcd(P, X^{12} + 1) = 1$. Over $\mathbb{F}_2$,

$$X^{12} + 1 = (X + 1)^4 (X^2 + X + 1)^4.$$

At a primitive cube root ω, $P(1) = c_6$ and $P(\omega) = c_6 + c_1 + c_2 + c_4 + c_5$. Both must be nonzero. This is equivalent to the two conditions in the corollary, which leave four free bits. □

8 Verification and scope

Theorem 1 and the coefficient characterization in Corollary 2 were formally verified in Lean 4.36.0. Both proofs use only Lean's standard axioms of propositional extensionality, classical choice, and quotient soundness. The accompanying Lean source archive contains the two theorem statements and their proofs.

The finite certificates form part of the proof. The supplement supplies the affine substitutions, source equation conventions and successive sums used in every witness branch. The accompanying code reconstructs the orbit coefficients and polar matrices and checks the identities with exact

arithmetic. Independent enumeration of the polar parameters is retained as a consistency check; it is not the coverage argument used in Sections 5–6.

The result classifies homogeneous rotation symmetric bent functions in twelve variables. The contribution to the general degree conjecture is this complete dimension and a concrete method for combining antipodal restrictions, partial Walsh mass and Pfaffian identities. Extending the method to other dimensions requires new control of the diagonal types and of the relevant restriction spectra. The present proof makes no nonexistence claim for unrestricted homogeneous quartics or for all numbers of variables.

Supplementary material. The supplement and verification sources accompany this manuscript. Its English guide distinguishes the certificate checks from the optional enumeration checks and gives a single command for reproduction.

References

[1] P. Stănică and S. Maitra. Rotation symmetric Boolean functions–Count and cryptographic properties. *Discrete Applied Mathematics* **156** (2008), 1567–1580. https://doi.org/10.1016/j.dam.2007.04.029

[2] Q. Meng, L. Chen and F.-W. Fu. On homogeneous rotation symmetric bent functions. *Discrete Applied Mathematics* **158** (2010), 1111–1117. https://doi.org/10.1016/j.dam.2010.02.009

[3] T. W. Cusick and E. M. Sanger. Rotation symmetric bent Boolean functions for $n = 2p$. arXiv:1708.09313 (2017). https://arxiv.org/abs/1708.09313

[4] L. Sun, Z. Shi, J. Liu and F.-W. Fu. On the conjecture about the nonexistence of homogeneous rotation symmetric bent functions. *Designs, Codes and Cryptography* **94** (2026), article 93. https://doi.org/10.1007/s10623-026-01848-4

[5] Q. Meng, H. Zhang, M. Yang and J. Cui. On the degree of homogeneous bent functions. *Discrete Applied Mathematics* **155** (2007), 665–669. https://doi.org/10.1016/j.dam.2006.10.008. Preliminary version: Cryptology ePrint Archive, Report 2004/284. https://eprint.iacr.org/2004/284

[6] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A* **20** (1976), 300–305. https://doi.org/10.1016/0097-3165(76)90024-8

[7] X. Zhang and G. Gao. Note on the conjecture about the nonexistence of rotation symmetric bent functions. arXiv:1303.2282 (2013), Theorem 3.7. https://arxiv.org/abs/1303.2282

[8] F. M. Vono. Antipodal necessity for rotation symmetric bent functions of degree at most three. Cryptology ePrint Archive, Report 2026/2844 (2026). https://eprint.iacr.org/2026/2844

Supplement to Homogeneous rotation symmetric bent functions in twelve variables are quadratic

Filipe Martins Vono André Naufel de Toledo ORCID 0000-0002-0619-6820 Valeria Gonzaga Santos ORCID 0009-0009-1333-2518

This supplement contains the exact algebraic data used in the quartic proof. Sections S1 and S2 define the model and the spectral classifications. Sections S3 and S4 give the witness certificates. Section S5 records the final rank factorizations. All coefficient arithmetic is in a Boolean polynomial ring over $\mathbb{F}_2$, so $v_i^2 = v_i$ and $t_j^2 = t_j$.

The witness branches cover the possible functions and may overlap. The two representatives in C and the ten branches in B are obtained by reflection. Binary splits within a branch are separate steps of the certificate. No assertion that witnesses partition the function space is needed.

S1 Orbit coefficients and the antipodal model

Coordinates start at zero. An integer mask m denotes the subset of positions where its binary digits are one. A twelve bit mask labels a subset of the original coordinates. A six bit mask labels z or a frequency. A five bit witness mask uses bit zero for w_1, and bit four for w_5.

To generate the orbit order, scan the twelve bit masks of weight four in increasing numerical order. If the mask has not appeared before, form its orbit under cyclic left shift and assign the next index. This gives exactly forty three orbits. The monomial orbit sum includes every distinct support once, including for short orbits.

The two model forms are

$$L_1 = t_0 + t_4 + t_7 + t_9 + t_{22} + t_{27} + t_{29} + t_{37}, \qquad L_2 = t_1 + t_3 + t_5 + t_8 + t_{24} + t_{28} + t_{34} + t_{36}.$$

For the necessary equations Q_S, use the thirty five unordered divisions of an eight element set into two four element sets. Write Q_m for the equation with twelve bit support mask m. Define

$$\begin{aligned} R = {} & t_1Q_{1151} + t_3Q_{383} + t_5Q_{1343} + t_8Q_{703} + t_{10}Q_{1823} + t_{12}Q_{1631} + t_{13}Q_{1439} \\ & + t_{15}Q_{1247} + t_{17}Q_{863} + t_{19}Q_{479} + t_{21}Q_{1871} + t_{24}Q_{1711} + t_{26}Q_{1487} + t_{28}Q_{1391} \\ & + t_{31}Q_{943} + t_{33}Q_{751} + t_{34}Q_{1655} + t_{36}Q_{887} + t_{38}Q_{1751} + t_{40}Q_{1495} + t_{41}Q_{1463}. \end{aligned}$$

The identities used before passing to quadratic restrictions are

$$L_2 = Q_{1495} + R, \qquad L_1 = Q_{975} + (t_{30} + t_{40})Q_{1755} + R.$$

These hold in the full forty three variable Boolean coefficient ring, without imposing the model. Expanding each complementary partition and using $t_j^2 = t_j$ verifies them.

For completeness, the transversal count in Lemma 4 and the three diagonal equations use the same three residue sets. With $(q, r, s) = (t_{42}, t_{30}, t_{40})$, the table is

Four residues	Transversal sum	Equation after the model
0134	0	$r + s + q = 0$
0123	L_1	$r + s + rq = 0$
0124	L_2	$sq = 0$

For an eight element support invariant under half rotation, the nonfixed unordered divisions cancel in pairs. The fixed divisions either separate the four antipodal pairs into two groups, or select complementary transversals. In the first row, rotation by three pairs the eight transversal classes without fixed points. In the other two rows the eight orbit indices are the ones in L_1 and L_2. This explains both the quadratic model and its three diagonal types.

S1.1 The twenty one polar coordinates

The diagonal coordinates are $(u_{30}, u_{40}, u_{42}) = (t_{30}, t_{40}, t_{42})$. The other eighteen are

Coordinate	Orbit coefficient expression
a	$t_{10} + t_{31}$
b	$t_{11} + t_{32}$
c	$t_{13} + t_{33}$
d	$t_{16} + t_{20}$
e	$t_{17} + t_{21}$
g	$t_{18} + t_{23}$
h	$t_{19} + t_{26}$
k	$t_{12} + t_{41}$
m	$t_{14} + t_{35}$
n	$t_{15} + t_{38}$
p	$t_6 + t_{25}$
r	$t_2 + t_{39}$
A_1	$t_0 + t_7 + t_9 + t_{29}$
A_2	$t_0 + t_4 + t_9 + t_{37}$
A_3	$t_0 + t_4 + t_7 + t_{22}$
B_1	$t_1 + t_3 + t_8 + t_{34}$
B_2	$t_1 + t_3 + t_5 + t_{36}$
B_3	$t_3 + t_5 + t_8 + t_{28}$

The map consisting of L_1, L_2 and these twenty one coordinates has rank twenty three. Thus fixing the model and a polar leaves an affine fibre of dimension twenty in the original coefficient space. Only the last phase exclusions require equations on this fibre.

Let R send e_i to e_{i+1} on six positions. Rotation symmetry gives

$$(\mathcal{B}_z)_{i,i+d} = (\mathcal{B}_{R^{-i}z})_{0,d}.$$

Together with symmetry of the matrix, the following three generating entries determine it. Each row gives the coefficient of the indicated monomial in z.

Monomial in z	$(\mathcal{B}_z)_{01}$	$(\mathcal{B}_z)_{02}$	$(\mathcal{B}_z)_{03}$
1	u_{30}	u_{40}	u_{42}
z_0	u_{30}	u_{40}	u_{42}
z_1	u_{30}	$a+h$	$b+n$
z_0z_1	u_{30}	a	b
z_2	$a+d$	u_{40}	$g+k$
z_0z_2	a	u_{40}	k
z_1z_2	d	h	A_2
z_3	$b+e$	$c+k$	u_{42}
z_0z_3	b	k	u_{42}
z_1z_3	e	A_2+A_3	n
z_2z_3	A_3	c	g
z_4	$c+g$	0	$b+n$
z_0z_4	c	m	n
z_1z_4	g	B_1+B_3	$p+r$
z_2z_4	$B_1+B_2+B_3$	m	B_1+B_2
z_3z_4	p	B_2	b
z_5	$d+h$	$e+n$	$g+k$
z_0z_5	d	e	g
z_1z_5	h	A_1+A_2	B_1+B_2
z_2z_5	$A_1+A_2+A_3$	n	$p+r$
z_3z_5	B_3	r	k
z_4z_5	A_1	B_1	A_2

The entries can also be reconstructed without this table. Evaluate the orbit polynomial at $x = (z+w, w)$, and take its second difference at $w = 0, e_i, e_j, e_i+e_j$. Integer masks specify the inputs completely. A coefficient of degree at most two in z is then recovered by its Boolean finite difference, using at most four evaluations.

S1.2 The parity identity

Write $s = u_{30}+u_{40}+u_{42}+\alpha+\beta$ for this paragraph only. The vectors $\mathcal{B}_z\mathbf{1}$ on the four odd orbits are

Row	Degree vector
0	$(u_{42}, u_{42}, u_{42}, u_{42}, u_{42}, u_{42})$
9	$(0, s, s, 0, s, s)$

Row	Degree vector
27	$(Y, Y, u_{42}, Y, Y, u_{42})$
63	$(0, 0, 0, 0, 0, 0)$

The respective indicators of the zero vector are $1 + u_{42}$, $1 + s$, $(1 + Y)(1 + u_{42})$, and 1. Adding them gives equation (8) in the article. All other cyclic orbits have even size.

S1.3 Reflection

Let R_0 be reflection on six positions and let $Dz = z + z_0 e_0$. Reflection of the twelve original indices induces

$$(z, w) \longmapsto (R_0 z, R_0(w + Dz)).$$

It preserves each diagonal form and the sum on the complementary row. On $z = 1$, the translation vanishes; hence a radical witness is reflected by reversing positions one through five. In C the support pairs are $123 \leftrightarrow 345$ and $125 \leftrightarrow 145$. In B there is also $124 \leftrightarrow 245$, and the supports $234, 135$ are fixed. The values of α, β, and therefore ε, are preserved. This proves that the chosen branches cover the problem up to a symmetry preserving bentness.

S2 Small column spectra

Put $s_z = r_0(z)/16$. In B, $s_0 = 0$; in C, $s_0 = 2$. Bentness requires $\sum_z s_z^2 = 16$ and $F(v) = \sum_z s_z(-1)^{z \cdot v} = \pm 4$. The latter gives

$$\sum_z s_z \equiv 4 \pmod 8, \qquad \sum_{z : z_i = 1} s_z \equiv 0 \pmod 4, \qquad \sum_{z : z_i = z_j = 1} s_z \equiv 0 \pmod 2.$$

The three pair congruences need only be checked at distances one, two and three. The following table lists every six bit cyclic orbit. The column k counts members containing position zero. The triple P gives, modulo two, the numbers containing $01, 02, 03$, in that order.

Representative	Size	k	P
0	1	0	000
1	6	1	000
3	6	2	100
5	6	2	010
7	6	3	010
9	3	1	001
11	6	3	110
13	6	3	110
15	6	4	100
21	2	1	010

Representative	Size	k	P
23	6	4	010
27	3	2	110
31	6	5	000
63	1	1	111

An active orbit of size six has modulus one, since modulus two would exceed the squared mass. An entry of modulus four occupies the entire column. For $|s_{63}| = 1$ or 2, reduction of the squared mass modulo three gives $s_{21} = 0$ in B. The third pair incidence then gives $s_9 \equiv s_{63} \pmod 2$.

If $|s_{63}| = 2$, either $|s_9| = 2$, which saturates the squared mass and forces $s_9 = -s_{63}$, or $s_9 = 0$. In the latter case the remaining twelve units would be an entry of modulus two at orbit 27 or two size six orbits. The first violates the single position congruence; the second violates the total congruence modulo eight. Thus only the first pattern occurs.

If $|s_{63}| = 1$, then $|s_9| = 1$, leaving twelve units. An entry of modulus two at 27 fails the pair congruences. Two size six orbits must have pair signatures whose XOR is 110. The total congruence forces equal signs at 9 and 63 and opposite signs on the two long orbits. The single position congruence becomes $k_x - k_y \equiv 2 \pmod 4$. The only possible pairs are $(1, 11), (1, 13), (31, 11), (31, 13), (3, 23), (15, 5)$. In particular, orbit 27 is absent in every B pattern, before $\alpha = \beta$ is deduced.

This proves exactly the portion of the zero column classification used in the article. Case C instead uses the direct parity and moment argument of Section 5.

S2.1 The complementary frequency column

For B, the diagonal has $r_{63}(0) = -32$. The restriction $G(v) = f^*(v, v + \mathbf{1})$ therefore has weight forty eight and is invariant under $T(v) = Rv + e_0$. Its orbit representatives are $0, 2, 4, 6, 10$, of size twelve, and 12, of size four. Its zeros consist of the short orbit and exactly one long orbit.

For $z \neq 0$, the normalized transform is one eighth of the character sum on these sixteen zeros. The five possibilities are as follows. An omitted representative has value zero; other members of an orbit follow $r_{63}(Rz) = (-1)^{z_5} r_{63}(z)$.

Long zero orbit representative	Nonzero entries besides $s_0 = -2$
0	$s_3 = 1,\ s_{15} = 1$
2	$s_{27} = -2$
4	$s_5 = -1,\ s_{23} = -1$
6	$s_5 = -1,\ s_{23} = 1$
10	$s_3 = -1,\ s_{15} = 1$

Each entry can be checked by iterating T on its two zero orbits and summing the character. Thus this table uses five explicit sixteen term sums.

S3 Certificates for case C

Write $(v_0, \ldots, v_{17}) = (a, b, c, d, e, g, h, k, m, n, p, r, A_1, A_2, A_3, B_1, B_2, B_3)$. Let F_i denote the following conditions $\Phi_{D,I}$, first in the case C coordinates and then with the witness substitutions applied. The indexing is fixed before any witness substitution. Thus two expressions that become equal in a particular branch retain their listed indices.

Index	Positions in D	Positions in I
0	01	0123
1	01	0124
2	01	0125
3	01	0134
4	01	0135
5	01	0145
6	01	0234
7	01	0235
8	01	0245
9	01	0345
10	01	1235
11	01	1245
12	01	1345
13	02	0123
14	02	0124
15	02	0125
16	02	0134
17	02	0135
18	02	0234
19	02	0235
20	02	0245
21	02	1245
22	03	0123
23	03	0134
24	03	0135

The generating polar table in S1 and the coefficient rule $\Phi_{D,I} = [z^{D^c}] \operatorname{Pf}(\mathcal{B}_z|_I)$ completely specify every equation in this list. Only the three products of complementary quadratic coefficients are needed, so expanded lists of all monomials are unnecessary.

The affine witness substitutions below follow from $Ey = 0, q_E(y) = 1, \alpha = \beta = 1$. Unlisted variables remain free. The equations in each right hand side involve only unlisted variables.

Variable	Witness mask 7	Witness mask 19
v_3	v_0	$1 + v_0$
v_4	Free	v_1
v_5	v_2	Free

Variable	Witness mask 7	Witness mask 19
v_6	v_0	$1 + v_0$
v_7	$v_1 + v_2 + v_4$	$1 + v_5$
v_9	$1 + v_4$	v_1
v_{16}	$1 + v_{10} + v_{13} + v_{15}$	$1 + v_{10} + v_{13} + v_{15}$
v_{17}	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$

For a sum table, the first column lists indices of the equations to add. The second is the result after all earlier substitutions on the same path, and the last gives the next variable to eliminate. Since each equation must vanish, an affine result is an equality to zero. A final result 1 is a contradiction. Every split below covers both values of its selected bit.

S3 witness mask 7

Initial common step

Source indices	Expanded sum	Consequence
23	$v_0 + v_8 + v_{10} + v_{11}$	Solve for v_{11}

Subcase $v_8 = v_0$.

Source indices	Expanded sum	Consequence
2, 8, 10	$1 + v_{12} + v_{13} + v_{14}$	Solve for v_{14}
6, 12, 19	$1 + v_1 + v_4$	Solve for v_4
7, 21	1	Contradiction

Subcase $v_8 = 1 + v_0$.

Source indices	Expanded sum	Consequence
2, 8, 10	$1 + v_2 + v_4 + v_{10}$	Solve for v_{10}
4, 9, 12, 20	$v_{14} + v_{15}$	Solve for v_{15}
7, 21	$1 + v_1 + v_2 + v_{12} + v_{13} + v_{14}$	Solve for v_{14}
5, 6, 9, 11, 13, 16	1	Contradiction

S3 witness mask 19

Initial common step

Source indices	Expanded sum	Consequence
23	$v_0 + v_8 + v_{10} + v_{11}$	Solve for v_{11}

Subcase $v_{10} = 0$.

Source indices	Expanded sum	Consequence
3, 6, 7, 9, 11, 12, 16, 17, 19, 21	$1 + v_{14} + v_{15}$	Solve for v_{15}
3, 11, 16, 19	$1 + v_0 + v_8$	Solve for v_8
7	$v_0 + v_2 + v_{12}$	Solve for v_{12}
8	$1 + v_2 + v_5$	Solve for v_5
21	$v_0 + v_1 + v_{13} + v_{14}$	Solve for v_{14}
6, 13, 17, 18	1	Contradiction

Subcase $v_{10} = 1$.

Source indices	Expanded sum	Consequence
3, 6, 7, 9, 11, 12, 16, 17, 19, 21	$v_0 + v_8 + v_{14} + v_{15}$	Solve for v_{15}
3, 7, 19, 21	$1 + v_0 + v_8$	Solve for v_8
22, 24	1	Contradiction

S4 Certificates for case B

The coordinate order is the same as in S3. There are three equation conventions in this supplement. The conditions $\Phi_{D,I}$ always have their literal subset labels. The F_i in S3 use the fixed C list. The G_i below are renumbered separately after the initial affine substitution in each B branch. Every table states which convention it uses.

To reconstruct the B input list, first run through two element sets D and four element sets I in lexicographic order. Form $\Phi_{D,I}$ in case B and discard zeros and exact duplicates, retaining the first occurrence. This gives twenty five equations. For $\varepsilon = 1$, append the order four Pfaffians of the matrix $\mathcal{B}_9$, with I again in lexicographic order.

For each witness, solve $Y = 0, \alpha = \beta = \varepsilon, Ey = 0, q_E(y) = 1$ by affine elimination. Choose the largest variable index as pivot and reduce earlier pivots. Substitute the resulting expressions into the input list, and again remove zeros and exact duplicates in their existing order. Finally append, if nonzero, the forbidden form indicator

$$H_E = \prod_{1 \le i < j \le 5} (1 + E_{ij} + E^{\mathrm{bad}}_{ij}),$$

where E^{bad} has every edge except 14 and 25. The resulting list, indexed from zero, is $G_0, G_1, \ldots$. The indicator is a necessary zero equation because that form violates the column nine squared mass. After the initial affine substitutions it has degree at most two in every branch where it is used.

To check the veto directly, put $P = w_1 + w_4, Q = w_2 + w_5, H = w_3$. The quadratic is $PQ + PH + QH$. The six unit rows correspond to the characters $w_0 + w_3, P, Q$, each twice. The first cancels on w_0. For the character P, summation in P keeps $Q + H = 1$, and the remaining two terms both contribute positively. The eight preimages of (P, Q, H) give modulus thirty two. The same holds for Q. The

diagonal $C_1 + C_2$ has the same three parity expression and contributes another modulus thirty two. Thus the squared mass is $5 \cdot 32^2 = 5120$.

S4.1 Initial affine substitutions

The following tables specify the initial elimination completely. They also make reconstruction independent of any choice of implementation. Unlisted coordinates are free.

Witness mask 7.

Variable	$\varepsilon = 0$	$\varepsilon = 1$
v_3	v_0	v_0
v_5	v_2	v_2
v_6	v_0	v_0
v_7	$v_1 + v_2 + v_4$	$v_1 + v_2 + v_4$
v_8	v_0	v_0
v_9	v_4	v_4
v_{16}	$v_{10} + v_{13} + v_{15}$	$1 + v_{10} + v_{13} + v_{15}$
v_{17}	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$

Witness mask 11.

Variable	$\varepsilon = 0$	$\varepsilon = 1$
v_5	$1 + v_2$	$1 + v_2$
v_6	v_3	v_3
v_7	v_2	v_2
v_8	v_0	v_0
v_9	v_1	v_1
v_{16}	$v_{10} + v_{13} + v_{15}$	$1 + v_{10} + v_{13} + v_{15}$
v_{17}	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$

Witness mask 14.

Variable	$\varepsilon = 0$	$\varepsilon = 1$
v_4	v_1	v_1
v_5	v_2	v_2
v_6	v_0	v_0
v_8	v_3	v_3
v_9	$v_0 + v_1 + v_2 + v_3 + v_7$	$v_0 + v_1 + v_2 + v_3 + v_7$
v_{16}	$v_{10} + v_{13} + v_{15}$	$1 + v_{10} + v_{13} + v_{15}$
v_{17}	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$

Witness mask 19.

Variable	$\varepsilon = 0$	$\varepsilon = 1$
v_3	v_0	v_0
v_4	v_1	v_1
v_6	v_0	v_0
v_7	v_5	v_5
v_8	v_0	v_0
v_9	$1 + v_1$	$1 + v_1$
v_{16}	$v_{10} + v_{13} + v_{15}$	$1 + v_{10} + v_{13} + v_{15}$
v_{17}	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$

Witness mask 21.

Variable	$\varepsilon = 0$	$\varepsilon = 1$
v_5	$v_0 + v_1 + v_2 + v_3 + v_4$	$v_0 + v_1 + v_2 + v_3 + v_4$
v_6	v_0	v_0
v_7	v_2	v_2
v_8	v_3	v_3
v_9	v_4	v_4
v_{16}	$v_{10} + v_{13} + v_{15}$	$1 + v_{10} + v_{13} + v_{15}$
v_{17}	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14} + v_{15}$

S4.2 Seven contradictory branches

Apply all preceding affine substitutions before reading a table row. Where a bit is split, the paths are exhaustive. A source index always refers to the original G_i of that branch, with the current substitutions applied; it is not renumbered after a step.

Witness mask 7 and $\varepsilon = 0$.

Source indices	Expanded sum	Consequence
23	$1 + v_1 + v_4$	Solve for v_4
0, 4, 5, 7, 8, 10, 11, 13, 15, 20	v_{11}	Solve for v_{11}
0, 2, 4, 5, 13	$v_{10} + v_{12} + v_{13} + v_{14}$	Solve for v_{14}
2, 8, 10	v_{10}	Solve for v_{10}
8	v_{13}	Solve for v_{13}
1, 4	$v_1 + v_2$	Solve for v_2
1, 3, 6	1	Contradiction

Witness mask 7 and $\varepsilon = 1$.

Source indices	Expanded sum	Consequence
24	$1 + v_1 + v_4$	Solve for v_4
0, 2, 4, 5, 13	$1 + v_{10} + v_{12} + v_{13} + v_{14}$	Solve for v_{14}

Source indices	Expanded sum	Consequence
2, 8, 10	$v_{10} + v_{11}$	Solve for v_{11}
0, 1, 2, 3, 4, 5	$v_{10} + v_{12} + v_{13} + v_{15}$	Solve for v_{15}
0, 2, 4, 6, 9	$v_1 + v_2 + v_{10}$	Solve for v_{10}
1, 4, 7	$v_0 + v_2 + v_{12}$	Solve for v_{12}
3, 4, 6	$v_1 + v_2$	Solve for v_2
0, 4	$1 + v_1$	Solve for v_1
0	1	Contradiction

Witness mask 11 and $\varepsilon = 0$.

Source indices	Expanded sum	Consequence
2, 7, 8, 10, 11, 15, 20	$1 + v_{10} + v_{11} + v_{14} + v_{15}$	Solve for v_{15}

Path $v_{10} = 0$.

Source indices	Expanded sum	Consequence
5, 6, 8, 9, 10, 13	$v_0 + v_3 + v_{13}$	Solve for v_{13}
1, 3, 5, 6, 9	$1 + v_{12} + v_{14}$	Solve for v_{14}
1, 3, 4, 8, 10	$v_2 + v_4$	Solve for v_4
2, 4, 6, 7, 8, 11	$v_0 + v_1 + v_2 + v_3$	Solve for v_3
1, 3, 4	$1 + v_{11}$	Solve for v_{11}
0, 3, 6, 7	1	Contradiction

Path $v_{10} = 1$.

Source indices	Expanded sum	Consequence
1, 3, 8, 10, 13	$v_1 + v_2 + v_{13}$	Solve for v_{13}
2	$1 + v_0 + v_1 + v_2 + v_3 + v_{11} + v_{12} + v_{14}$	Solve for v_{14}
0, 3, 4, 6, 16	$v_2 + v_4$	Solve for v_4
1, 3, 4	1	Contradiction

Witness mask 11 and $\varepsilon = 1$.

Source indices	Expanded sum	Consequence
1, 3, 6, 9, 12, 13, 16, 23	$v_{10} + v_{11}$	Solve for v_{11}
7, 20	1	Contradiction

Witness mask 19 and $\varepsilon = 0$.

Source indices	Expanded sum	Consequence
2, 7, 8, 10, 11, 15, 20	$1 + v_{11} + v_{12} + v_{13} + v_{15}$	Solve for v_{15}

Path $v_{10} = 0$.

Source indices	Expanded sum	Consequence
0, 1, 4, 8, 9, 10, 12, 13	$v_{11} + v_{13}$	Solve for v_{13}
2, 4, 5, 8, 10, 12, 16	1	Contradiction

Path $v_{10} = 1$.

Source indices	Expanded sum	Consequence
1, 3, 8, 10, 13	$1 + v_1 + v_5 + v_{13}$	Solve for v_{13}
0, 2, 3, 4, 9, 12	$1 + v_{11}$	Solve for v_{11}
8, 10	1	Contradiction

Witness mask 19 and $\varepsilon = 1$.

Source indices	Expanded sum	Consequence
1, 3, 6, 9, 12, 13, 16, 23	$v_{10} + v_{11}$	Solve for v_{11}
11, 15	1	Contradiction

Witness mask 21 and $\varepsilon = 0$.

Path $v_{11} = 0$.

Path $v_{11} = 0$, $v_{13} = 0$.

Source indices	Expanded sum	Consequence
0, 3, 5, 8, 9, 10, 16	$v_{12} + v_{14}$	Solve for v_{14}
2	v_{10}	Solve for v_{10}
1, 3, 4, 23	$1 + v_{12} + v_{15}$	Solve for v_{15}
0, 1, 3, 6, 7, 9, 20	$v_1 + v_2$	Solve for v_2
0, 1, 3, 6, 9, 11, 15	$v_0 + v_3$	Solve for v_3
3	1	Contradiction

Path $v_{11} = 0$, $v_{13} = 1$.

Source indices	Expanded sum	Consequence
0, 3, 5, 8, 9, 10, 16	$1 + v_0 + v_2 + v_3 + v_4$	Solve for v_4
0, 1, 2, 4, 5, 6, 8, 10, 12	$1 + v_{10} + v_{12} + v_{14}$	Solve for v_{14}

Source indices	Expanded sum	Consequence
0, 1, 2, 3, 4, 7, 8, 9, 11, 23	1	Contradiction

Path $v_{11} = 1$.

Path $v_{11} = 1$, $v_{10} = 0$.

Source indices	Expanded sum	Consequence
1, 3, 6, 9, 12, 13, 16	$1 + v_0 + v_2 + v_3 + v_4$	Solve for v_4
0, 4, 5, 13	$1 + v_0 + v_3 + v_{13}$	Solve for v_{13}
0, 2, 8, 9, 15, 20	$1 + v_0 + v_3 + v_{12} + v_{14}$	Solve for v_{14}
4, 6, 7, 8, 11	$v_0 + v_3$	Solve for v_3
0, 4, 6	$1 + v_0$	Solve for v_0
23	$v_1 + v_2$	Solve for v_2
0, 1, 4	$v_1 + v_{12}$	Solve for v_{12}
0	$v_1 + v_{15}$	Solve for v_{15}
1	1	Contradiction

Path $v_{11} = 1$, $v_{10} = 1$.

Source indices	Expanded sum	Consequence
0, 4, 5, 13	$1 + v_2 + v_4 + v_{12} + v_{13} + v_{14}$	Solve for v_{14}
0, 5	$1 + v_2 + v_4 + v_{13}$	Solve for v_{13}
0, 2, 3	$1 + v_0 + v_3$	Solve for v_3
1, 2, 6, 15, 20	1	Contradiction

S4.3 A shared lemma forces $a = d$

Assume case B, $\alpha = \beta = 1, Y = 0, h = a, b + g + k + n = a + d$, the equations $\Phi_{D,I} = 0$, and $r_0(1) = 0, r_0(9) \neq 0$. We prove $a = d$.

Suppose instead that $a + d = 1$. Then $m = d = 1 + a$ and $n = 1 + b + g + k$. In the period three coordinates on row nine, D_9 has image contained in $\{0, (0, 1, 1)\}$, and the linear part in the lower three variables is $(0, e + X, c + X)$. Summation in these variables forces $D_9 v = (0, e + X, c + X)$. Activity therefore gives $c = e$, and, when $X = 0$, gives $c = e = 0$.

For the four identities below, the indices refer to the following literal subset pairs, rather than to the branch equations G_i.

Index	D	I
0	01	0123
2	01	0125
3	01	0134
6	01	0234

Index	D	I
7	01	0235
8	01	0245
9	01	0345
10	01	1235
11	01	1245
12	01	1345
16	02	0134
17	02	0135
19	02	0235
21	02	1245

Put $S = A_1 + A_2 + A_3$ and $\gamma = bg + bk + gk$. Each row uses the hypotheses and the conclusions of earlier rows.

Additional available equations	Source indices of Φ	Expanded result
$c = e$	3, 6, 9, 12, 17, 19	X
$X = 0, c = e = 0$	3, 9, 17	S
Previous and $S = 0$	2, 8, 10	$1 + p$
Previous and $p = 1$	0, 7, 11, 16, 17, 21	$1 + \gamma$

Thus $\gamma = 1$. For comparison with the balanced row, its ten edges are

ij	12	13	14	15	23	24	25	34	35	45
E_{ij}	0	$1+n$	$g+k$	1	$1+g$	1	$b+n$	$1+b$	$1+k$	0.

Set $P = w_1, \sigma = w_2, \tau = w_3, \upsilon = w_4, Q = w_5$. Write $q_E = PQ + PL + QM + N$, where

$$\begin{aligned} L &= (b + g + k)\tau + (g + k)\upsilon, \\ M &= (1 + g + k)\sigma + (1 + k)\tau, \\ N &= (1 + g)\sigma\tau + \sigma\upsilon + (1 + b)\tau\upsilon. \end{aligned}$$

Summing in P, Q and the absent variable w_0 gives

$$r_0(1) = 4 \sum_{\sigma,\tau,\upsilon} (-1)^{N+LM}.$$

Expansion yields $N + LM = \sigma\upsilon + A\sigma\tau + C\tau\upsilon + T\tau$, with

$$A = 1 + g + b + bg + bk, \quad C = 1 + b + g + gk, \quad T = b + bk + g + gk.$$

Use $\sigma' = \sigma + C\tau$, $\upsilon' = \upsilon + A\tau$. The exponent becomes $\sigma'\upsilon' + (T + AC)\tau$, and Boolean multiplication gives $T + AC = 1 + \gamma$. Therefore

$$r_0(1) = 4\left(\sum_{\sigma',\upsilon'}(-1)^{\sigma'\upsilon'}\right)\left(\sum_{\tau}(-1)^{(1+\gamma)\tau}\right) = 16\gamma.$$

Balancedness forces $\gamma = 0$, a contradiction. This proves the lemma. The initial tables for witnesses 14 and 21 imply $h = a$, $m = d$ and $b+g+k+n = a+d$, so it applies to both branches with $\varepsilon = 1$.

S4.4 The three remaining parametrizations

For witness 14 with $\varepsilon = 0$, split $v_{12} + v_{14}$, and, on its zero branch, split $v_{10} + v_{13}$. The first two paths below contradict the equations, and the last gives the one parameter family. For the two branches with $\varepsilon = 1$, first apply the shared lemma, $v_0 = v_3$. The following thirty two sums then give exactly the displayed families in the article. The final product equation for witness 21 is recorded separately.

Witness mask 14 and $\varepsilon = 0$.

Path $v_{12} + v_{14} = 1$.

Source indices	Expanded sum	Consequence
4, 13	$v_1 + v_2 + v_{10} + v_{13}$	Solve for v_{13}
0, 5	v_{10}	Solve for v_{10}
2, 6, 12, 18	$1 + v_0 + v_1 + v_2 + v_3$	Solve for v_3
2, 8, 10	$1 + v_1 + v_2$	Solve for v_2
23	$v_1 + v_7$	Solve for v_7
0, 7, 8, 9, 15	1	Contradiction

Witness mask 14 and $\varepsilon = 0$.

Path $v_{12} + v_{14} = 0$, $v_{10} + v_{13} = 1$.

Source indices	Expanded sum	Consequence
6, 9, 12, 16, 23	$v_0 + v_3$	Solve for v_3
0, 2, 5	1	Contradiction

Witness mask 14 and $\varepsilon = 0$.

Path $v_{12} + v_{14} = 0$, $v_{10} + v_{13} = 0$.

Source indices	Expanded sum	Consequence
6, 9, 12, 16, 23	$1 + v_{10} + v_{11} + v_{12} + v_{15}$	Solve for v_{15}
2, 7, 8, 10, 11, 15, 20	$v_0 + v_3$	Solve for v_3
23	$1 + v_2 + v_7$	Solve for v_7
7, 11	$v_1 + v_2$	Solve for v_2
3	$v_{10} + v_{11}$	Solve for v_{11}
7	$v_0 + v_1 + v_{10} + v_{12}$	Solve for v_{12}

Source indices	Expanded sum	Consequence
0, 6	v_1	Solve for v_1
0, 1	$1 + v_{10}$	Solve for v_{10}

Free coordinates: v_0.

Witness mask 14 and $\varepsilon = 1$.

Path $v_0 + v_3 = 0$.

Source indices	Expanded sum	Consequence
24	$1 + v_2 + v_7$	Solve for v_7
0, 2, 4, 5, 13	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14}$	Solve for v_{14}
2, 7, 8, 10, 11, 15, 20	$1 + v_{11}$	Solve for v_{11}
9, 16, 18	$1 + v_{12} + v_{13} + v_{15}$	Solve for v_{15}
11, 15	$1 + v_{10}$	Solve for v_{10}
8	v_{13}	Solve for v_{13}
3	$v_1 + v_2$	Solve for v_2
0	$v_0 + v_1 + v_{12}$	Solve for v_{12}

Free coordinates: v_0, v_1.

Witness mask 21 and $\varepsilon = 1$.

Path $v_0 + v_3 = 0$.

Source indices	Expanded sum	Consequence
24	$1 + v_1 + v_4$	Solve for v_4
0, 2, 4, 5, 13	$v_{10} + v_{11} + v_{12} + v_{13} + v_{14}$	Solve for v_{14}
2, 7, 8, 10, 11, 15, 20	$1 + v_{11}$	Solve for v_{11}
9, 16, 18	$1 + v_{12} + v_{13} + v_{15}$	Solve for v_{15}
1, 17	$v_0 + v_1 + v_{12} + v_{13}$	Solve for v_{13}
6, 9	$1 + v_1 + v_2$	Solve for v_2
3	$1 + v_0 + v_1 + v_{10} + v_{12}$	Solve for v_{12}

Free coordinates: v_0, v_1, v_{10}.

The additional necessary sum with source indices 0 is $1 + v_0 + v_1 + v_{10} + v_0v_{10} + v_1v_{10} = (1 + v_0 + v_1)(1 + v_{10}) = 0$.

The complete parametrizations are below. The bits x, t, u are free where they occur, subject to the additional product condition just given. A single entry in a grouped row is shared by all listed coordinates.

Polar coordinates	$y = 14, \varepsilon = 0$	$y = 14, \varepsilon = 1$	$y = 21, \varepsilon = 1$
a, d, h, m	x	x	x

Polar coordinates	$y=14,\varepsilon=0$	$y=14,\varepsilon=1$	$y=21,\varepsilon=1$
b,g	0	t	t
c,e	0	t	$1+t$
k,n	1	$1+t$	$1+t$
p,r	$(1,1)$	$(1,1)$	$(u,1)$
A_1,A_3	$1+x$	$x+t$	$1+x+t+u$
A_2	1	0	$1+u$
B_1,B_2,B_3	$(x,x,1+x)$	$1+x+t$	$1+x+t$

These substitutions give all eighteen coordinates, not merely the free ones. In the last branch the product condition removes the two choices $u=0, x=t$. The initial affine equations and every subsequent step are consequences of necessary zero equations, so all possible polars of the branch occur in the resulting families.

In the one parameter family $(y,\varepsilon)=(14,0)$, the rows with $\mathcal{B}_z e_0=0$ are

Parameter	Row masks
$x=0$	1, 5, 9, 10, 17, 18, 20, 34, 36, 40, 63
$x=1$	1, 9, 18, 36, 63

Thus N_1 is odd in both choices. These lists follow by substituting the family into the generating entries in S1.

S5 Final rank and phase checks

Four of the ten remaining B polars are ruled out by the inactive row nine argument in the article. The other four with $p=r=1$ are listed below. A pair (m,n) denotes the alternating matrix $m\wedge n$, with entries $m_i n_j+m_j n_i$. The masks here have six bits. Every such matrix has rank at most two.

Witness and parameters	$\mathcal{B}_3$	$\mathcal{B}_5$	$\mathcal{B}_{15}$	$\mathcal{B}_{23}$
$14,(x,t)=(0,0)$	(24,39)	0	0	(58,5)
$14,(x,t)=(1,0)$	(60,3)	(18,45)	(54,9)	(40,23)
$21,(x,t,u)=(0,1,1)$	(24,36)	(40,5)	(54,57)	(40,18)
$21,(x,t,u)=(1,1,1)$	(36,3)	(58,45)	(48,6)	(18,5)

These entries are verified by substituting the family into S1 and rotating its three generators. Also $X=Y=0, p=1$, so $D_{27}=0$ and the lower linear part in the period three coordinates is nonzero. The character at frequency sixty three depends only on the upper coordinates. Thus that row is zero in the complementary frequency column. The five possibilities of S2.1 are all excluded.

The final two polars and their five phase identities are given in Section 6.3 of the article. They can be reconstructed by ordinary affine elimination on the two model forms and the twenty one fixed polar coordinates. One choice of free orbit indices is

$$20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 41.$$

Substitute the resulting affine forms for the forty three t_j into each thirty five term equation Q_S. The quadratic terms cancel in the five specified sums. Their affine remainders are exactly the ones displayed in the article, and adding the appropriate two or three sums leaves 1. This checks the full affine fibres of dimension twenty.

S6 Reproduction

The verification package accompanies the paper. From its verification directory, run `python run_verification.py`. Python 3.10 or later and NumPy are required for the full suite. The English README maps the individual checks to the sections above. Polynomial identities are represented as sets of squarefree monomials: addition is symmetric difference and multiplication replaces the two supports by their union. This representation uses exact arithmetic and has no numerical tolerance.

The certificate checks reconstruct the input equations, expand the stated sums and substitutions, check binary branch coverage, and compare all resulting coordinates with the three families. Separate checks verify reflection, the parity and Pfaffian identities, the column spectra, the common lemma and the full phase fibre identities. The package also retains larger historical certificates and independent enumerations for comparison. Those computations are supplementary checks, not additional hypotheses of this proof.