Antipodal necessity for rotation symmetric bent functions of degree at most three

Filipe Martins Vono[1*]

[1*]Centro Universitário de Belo Horizonte (UniBH), Belo Horizonte, Brazil.

Corresponding author(s). E-mail(s): contatofilipevono@gmail.com;

Abstract

The conjecture that every homogeneous rotation symmetric bent Boolean function has degree two remains open in general. We prove a necessary condition that settles the degree-three case of this conjecture. Let $\boldsymbol{n} > \mathbf{0}$ be even. If a rotation symmetric Boolean function of degree at most three in $\boldsymbol{n}$ variables is bent, then its algebraic normal form contains the antipodal quadratic orbit $\sum_{\boldsymbol{i<n/2}} \boldsymbol{x_i x_{i+n/2}}$. A homogeneous cubic has no quadratic terms, so no homogeneous rotation symmetric cubic Boolean function is bent, in any even number of variables. The condition also applies to nonhomogeneous functions with arbitrary lower-degree terms compatible with rotation symmetry; it neither classifies these functions nor addresses degree four and higher. The proof uses only finite Fourier analysis and linear algebra over the binary field. Restriction to the fixed space of a rotation of odd order reduces the problem to a power-of-two number of variables. There, Parseval's identity and a rigidity property of rotation symmetric quadratic forms impose incompatible conditions on a single fiber of the function. A second proof replaces the final fiber argument by descent through a single unipotent Jordan block. Examples illustrate the hypotheses. A Lean formalization of the original proof is provided as supplementary material; the Jordan proof has not been formalized.

Keywords: Boolean functions, bent functions, rotation symmetry, algebraic normal form, quadratic forms, formal verification

Version 4 — 8 November 2026. Second proof added in Appendix B; the original formal supplement is unchanged.

1 Introduction

Bent functions have constant Walsh magnitude and attain the maximum possible distance from affine Boolean functions [1]; see [2–4] for their role in cryptography and coding theory. Rotation symmetric Boolean functions, which are invariant under cyclic shifts of the input coordinates, were introduced by Pieprzyk and Qu [5] in connection with fast hashing. Their orbit representation reduces the search space relative to unrestricted Boolean functions, making the class useful for computer searches [6, 7]. Rotation symmetric bent functions have accordingly received considerable attention [8–10]. Stănică and Maitra [6] conjectured that a homogeneous rotation symmetric bent function must have degree two. Theorem 1.1 settles the cubic case by identifying a quadratic term forced by bentness.

For $n = 2H > 0$, call $\{i, i + H\}$ an *antipodal pair* of coordinate indices. Cyclic rotation permutes these pairs. In a rotation symmetric function, all corresponding quadratic monomials have the same coefficient in the algebraic normal form (ANF). Denote that coefficient by $\alpha(f)$. Equivalently, $\alpha(f)$ is the coefficient of the orbit sum

$$P_n(\boldsymbol{x}) = \sum_{i=0}^{H-1} x_i x_{i+H}.$$

Theorem 1.1 *Let $n > 0$ be even. If $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is rotation symmetric, bent, and has algebraic degree at most three, then $\alpha(f) = 1$.*

Corollary 1.2 *No homogeneous rotation symmetric Boolean function of degree three is bent, in any positive even dimension.*

The corollary follows because a homogeneous cubic has no quadratic terms. The hypotheses of the theorem are attained: P_n is rotation symmetric and bent. Section 5 verifies this example and proves the theorem.

Related work

Meng, Chen and Fu [11], Zhang and Gao (preprint, arXiv:1303.2282), and Cusick and Sanger (preprint, arXiv:1708.09313) obtained partial results on the homogeneous conjecture. Antipodal necessity for quadratic rotation symmetric bent functions appears in Gao et al. [10], Remark 1, and Remark 3.8 of the Zhang–Gao preprint; the Cusick–Sanger preprint gives it as Corollary 2.8. Its Theorem 3.8 excludes homogeneous odd degrees when $n = 2p$, $p > 2$ prime. Sun, Shi, Liu and Fu [12] obtain nonexistence criteria involving orbit structure, index distances and derivatives. Their Theorem 5 treats cubic orbit sums with an even number of generators and $v_2(r_i), v_2(s_i) \geq v_2(n)$ for every generating pair (r_i, s_i), where v_2 is the exponent of two in an integer. For a fixed finite set of generating pairs, their Theorem 6 excludes bentness when 2^{e_0} divides n, with e_0 depending on that set. Their Corollary 2 excludes all homogeneous cubics when $n = 2\prod_{i=1}^{t} p_i^{a_i}$, with odd primes $p_1 < \cdots < p_t$ satisfying $p_i > 2^{2\prod_{j<i} p_j^{a_j}}$

for $i \geq 2$; this includes twice an odd prime power. These results do not state the unrestricted cubic conclusion of Corollary 1.2. Theorem 1.1 also supplies a coefficient condition for nonhomogeneous functions of degree at most three.

The rotational hypothesis is essential: Charnes, Rötteler and Beth [13] construct homogeneous cubic bent functions in 8, 10 and 12 variables without imposing cyclic invariance. Stănică, Maitra and Clark [8] studied single-orbit exclusions. The nonexistence result for degree at least three in the general single-orbit setting is given by Meng, Chen and Fu [11], Theorem 11, p. 1114; see also Section 3 of the Cusick–Sanger preprint. Remark 3.4 of the Zhang–Gao preprint explains a limitation of the earlier single-cycle argument. Earlier experiments reported no homogeneous rotation symmetric bent functions of degree greater than two through ten variables [6].

Nonhomogeneous cubic rotation symmetric bent functions are known, including the constructions of Gao et al. [10] and Wang et al. [14], and the ten-variable results of Polujan et al. [15]. These results concern algebraic degree three, which allows quadratic terms. Corollary 1.2 concerns homogeneity, which excludes them. The quadratic rigidity used below is consistent with the balancing theory of Chirvasitu and Cusick [16].

Contribution and outline

The contribution is a necessary quadratic coefficient condition for every rotation symmetric bent function of degree at most three, in every positive even dimension. The single-orbit results of Meng, Chen and Fu restrict the orbit structure of the function, and Theorem 3.8 of the Cusick–Sanger preprint restricts the dimension to $n = 2p$; Theorem 1.1 imposes neither restriction. The homogeneous cubic case follows because its quadratic coefficients vanish. The theorem permits lower-degree terms compatible with rotation symmetry; it neither classifies the nonhomogeneous cubic solutions nor settles higher degrees.

The proof proceeds in three steps. Write $n = Nm$ with $N = 2^s$, $s \geq 1$, and m odd.

1. A missing antipodal term makes f constant on the fixed space of the coordinate half-turn. Distinct monomials cancel in pairs there (Lemma 3.1).
2. Restrict to inputs made of m repetitions of an N-bit block. The resulting function g remains bent and rotation symmetric. The key is that derivatives of a cubic are quadratic, and balance of invariant quadratics passes to odd-order fixed spaces (Lemma 3.2 and Corollary 3.3). The diagonal inputs $(\boldsymbol{u}, \boldsymbol{u})$ of the smaller space repeat to half-turn fixed inputs of the original space.
3. In dimension $N = 2^s$, a bent function constant on the diagonal must have balanced fibers $\boldsymbol{u} \mapsto g(\boldsymbol{u}, \boldsymbol{u} + \boldsymbol{z})$ for every nonzero $\boldsymbol{z}$. For $\boldsymbol{z}$ equal to the all-ones vector, quadratic rigidity and rotation symmetry force the same fiber to be constant (Proposition 4.4). This contradiction forces $\alpha(f) = 1$.

Section 2 fixes notation, Section 3 carries out the first two steps, Section 4 the third, and Section 5 assembles the proof. Section 6 discusses the role of the degree bound, and Section 7 describes the accompanying formalization. Appendix B gives a second proof by Jordan descent, sharing the reduction in Section 3 but replacing the complementary-fiber argument.

2 Definitions and elementary identities

Vectors are printed in bold and their scalar coordinates in italics. All vector spaces are finite-dimensional over $\mathbb{F}_2$. Put $V_d = \mathbb{F}_2^d$ and read coordinate indices modulo d. The cyclic shift is $(\rho\boldsymbol{x})_i = x_{i+1}$; its dimension will be clear from its argument. When $d = 2k$ is even and $\boldsymbol{u}, \boldsymbol{v} \in V_k$, we write $(\boldsymbol{u}, \boldsymbol{v}) \in V_d$ for the vector with coordinates $u_0, \ldots, u_{k-1}, v_0, \ldots, v_{k-1}$; thus $(\boldsymbol{u}, \boldsymbol{u})$ repeats the block $\boldsymbol{u}$ twice. A function is *rotation symmetric* if $f \circ \rho = f$. Its ANF is the unique squarefree polynomial

$$f(\boldsymbol{x}) = \sum_{A \subseteq \{0,\ldots,d-1\}} c_A(f) \prod_{i \in A} x_i.$$

The degree of a nonzero function is the largest size of a support with nonzero coefficient. The zero function is assigned degree minus infinity. A nonzero function is homogeneous of degree three if every such support has size three. We use *quadratic* to mean degree at most two. Sums of polynomial values are in $\mathbb{F}_2$; character sums and weights are integers.

For an input direction $\boldsymbol{a}$ and a frequency $\boldsymbol{\xi}$, define

$$\begin{aligned} D_{\boldsymbol{a}} f(\boldsymbol{x}) &= f(\boldsymbol{x} + \boldsymbol{a}) + f(\boldsymbol{x}), \\ W_f(\boldsymbol{\xi}) &= \sum_{\boldsymbol{x} \in V_d} (-1)^{f(\boldsymbol{x}) + \boldsymbol{\xi} \cdot \boldsymbol{x}}, \\ C_f(\boldsymbol{a}) &= \sum_{\boldsymbol{x} \in V_d} (-1)^{D_{\boldsymbol{a}} f(\boldsymbol{x})}. \end{aligned}$$

The function is *balanced* if $W_f(0) = 0$, equivalently if exactly half of its values are one. It is *bent* if d is even and $|W_f(\boldsymbol{\xi})| = 2^{d/2}$ for every $\boldsymbol{\xi}$. This condition is unchanged by an invertible linear change of coordinates or addition of an affine function.

Lemma 2.1 *A function on V_d is bent if and only if d is even and $D_{\boldsymbol{a}} f$ is balanced for every $\boldsymbol{a} \neq 0$.*

Proof Expanding $W_f(\boldsymbol{\xi})^2$ and substituting $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{a}$ gives

$$W_f(\boldsymbol{\xi})^2 = \sum_{\boldsymbol{a} \in V_d} C_f(\boldsymbol{a}) (-1)^{\boldsymbol{\xi} \cdot \boldsymbol{a}}. \tag{2.1}$$

Since $C_f(0) = 2^d$, balanced nonzero derivatives give $W_f(\boldsymbol{\xi})^2 = 2^d$. Conversely, Fourier inversion of (2.1) gives $C_f(\boldsymbol{a}) = 0$ for $\boldsymbol{a} \neq 0$ when the Walsh squares are constant. The same identity holds on any finite binary vector space after choosing coordinates. □

For any Boolean function q, put

$$q_0(\boldsymbol{x}) = q(\boldsymbol{x}) + q(0), \qquad B_q(\boldsymbol{a}, \boldsymbol{b}) = q(\boldsymbol{a} + \boldsymbol{b}) + q(\boldsymbol{a}) + q(\boldsymbol{b}) + q(0).$$

For quadratic q, B_q is an alternating bilinear form, called its *polar*. Its radical is $\operatorname{Rad} B_q = \{\boldsymbol{r} : B_q(\boldsymbol{r}, \boldsymbol{x}) = 0 \text{ for every } \boldsymbol{x}\}$.

Lemma 2.2 *If $\deg g \le 3$, the third difference $\Theta_g(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}) = D_{\boldsymbol{a}} D_{\boldsymbol{b}} D_{\boldsymbol{c}} g(0)$ is independent of the base point, symmetric and trilinear. Moreover,*

$$D_{\boldsymbol{a}} D_{\boldsymbol{b}} g(\boldsymbol{x}) = D_{\boldsymbol{a}} D_{\boldsymbol{b}} g(0) + \Theta_g(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{x}), \qquad B_{D_{\boldsymbol{c}} g}(\boldsymbol{a}, \boldsymbol{b}) = \Theta_g(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}). \tag{2.2}$$

Proof Each derivative lowers degree by at least one, so a third derivative is constant. Derivatives commute. The operator identity $D_{\boldsymbol{a}+\boldsymbol{a}'} = D_{\boldsymbol{a}} + D_{\boldsymbol{a}'} + D_{\boldsymbol{a}} D_{\boldsymbol{a}'}$ proves additivity in each argument, since a fourth derivative vanishes. Explicitly,

$$\Theta_g(\boldsymbol{a} + \boldsymbol{a}', \boldsymbol{b}, \boldsymbol{c}) = \Theta_g(\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}) + \Theta_g(\boldsymbol{a}', \boldsymbol{b}, \boldsymbol{c}) + D_{\boldsymbol{a}} D_{\boldsymbol{a}'} D_{\boldsymbol{b}} D_{\boldsymbol{c}} g(0).$$

The last term is zero because $\deg g \le 3$; symmetry gives additivity in the other arguments. The first identity in (2.2) is the definition of differentiation in direction $\boldsymbol{x}$ applied to $D_{\boldsymbol{a}} D_{\boldsymbol{b}} g$ at zero; the second expands the polar of $D_{\boldsymbol{c}} g$. □

3 Reduction from arbitrary even dimension

The first lemma explains why the antipodal coefficient controls diagonal values. Rotation of a support means adding one to each index modulo the dimension. Rotation invariance and uniqueness of ANF give $c_{\rho A}(f) = c_A(f)$, so $\alpha(f) = c_{\{0,H\}}(f)$ for $n = 2H$. It is one coefficient, rather than the sum of all antipodal coefficients.

Lemma 3.1 (Half-turn cancellation) *For rotation symmetric $f : V_{2H} \to \mathbb{F}_2$ of degree at most three, every vector fixed by $\tau = \rho^H$ has the form $(\boldsymbol{u}, \boldsymbol{u})$, and*

$$f(\boldsymbol{u}, \boldsymbol{u}) = f(0) + \alpha(f) \sum_{i=0}^{H-1} u_i \qquad (\boldsymbol{u} \in V_H). \tag{3.1}$$

Proof The half-turn $\tau = \rho^H$ swaps the two coordinates of every antipodal pair. On $\boldsymbol{x} = (\boldsymbol{u}, \boldsymbol{u})$, the monomials with supports A and τA have equal values and equal coefficients. If these supports differ, their contributions cancel. A fixed support $A = \tau A$ is a union of antipodal pairs. With $|A| \le 3$, it is empty or consists of one pair. The empty support contributes $f(0)$; the pair $\{i, i+H\}$ contributes $\alpha(f) u_i^2 = \alpha(f) u_i$. This gives (3.1), including supports in short cyclic orbits. □

Next we transfer bentness to a smaller space. The quadratic character-sum identity used in the proof is

$$\left(\sum_{\boldsymbol{x} \in V} (-1)^{q(\boldsymbol{x})} \right)^2 = |V| \sum_{\boldsymbol{r} \in \operatorname{Rad} B_q} (-1)^{q_0(\boldsymbol{r})}. \tag{3.2}$$

Indeed, substitute $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{r}$ in the squared sum and use $q(\boldsymbol{x}+\boldsymbol{r}) + q(\boldsymbol{x}) = B_q(\boldsymbol{x}, \boldsymbol{r}) + q_0(\boldsymbol{r})$. Summing over $\boldsymbol{x}$ leaves only $\boldsymbol{r}$ in the radical. In particular, if q_0 vanishes on its radical, the character sum is nonzero.

Lemma 3.2 (Balance on an odd-order fixed space) *Let $T \in \mathrm{GL}(V)$ satisfy $T^m = I$ for an odd positive integer m, and put $U = \mathrm{Fix}(T)$. If q is quadratic and $q \circ T = q$, then q is balanced on V if and only if $q|_U$ is balanced.*

Proof Replace q by q_0, which preserves balance, and write $B = B_q$. Define the averaging projector $\Pi = I + T + \cdots + T^{m-1}$. We have $T\Pi = \Pi T = \Pi$, so $\Pi \boldsymbol{x} \in U$ for every $\boldsymbol{x}$, and $\Pi \boldsymbol{u} = m\boldsymbol{u} = \boldsymbol{u}$ on U. Thus $\Pi^2 = \Pi$ and $V = U \oplus K$, where $K = \ker \Pi$.

The two summands are orthogonal for B. For $\boldsymbol{u} \in U$ and $\boldsymbol{k} \in K$, invariance gives

$$B(\boldsymbol{u}, \boldsymbol{k}) = \sum_{j=0}^{m-1} B(\boldsymbol{u}, T^j \boldsymbol{k}) = B(\boldsymbol{u}, \Pi \boldsymbol{k}) = 0.$$

Here B is T-invariant because q is, so $B(\boldsymbol{u}, T^j \boldsymbol{k}) = B(T^{-j}\boldsymbol{u}, \boldsymbol{k}) = B(\boldsymbol{u}, \boldsymbol{k})$ for every j; the first equality holds because a sum of m equal terms equals one of them when m is odd. Consequently $q(\boldsymbol{u} + \boldsymbol{k}) = q(\boldsymbol{u}) + q(\boldsymbol{k})$ and, writing $S_E(q) = \sum_{\boldsymbol{x} \in E} (-1)^{q(\boldsymbol{x})}$,

$$S_V(q) = S_U(q|_U) S_K(q|_K). \tag{3.3}$$

It remains to show that the second factor is nonzero. Let R be the radical of $B|_{K \times K}$. Since K and B are T-invariant, R is T-invariant. Since B vanishes on $R \times R$, the normalized quadratic q is additive, hence linear, on R. Therefore for $\boldsymbol{r} \in R$,

$$q(\boldsymbol{r}) = \sum_{j=0}^{m-1} q(T^j \boldsymbol{r}) = q(\Pi \boldsymbol{r}) = q(0) = 0.$$

The first equality uses invariance and odd m; the second uses linearity on R. Applying (3.2) on K gives $S_K(q|_K)^2 = |K||R| > 0$. The factorization (3.3) proves the lemma. □

Corollary 3.3 *Under the same assumptions on T, if $f \circ T = f$, $\deg f \leq 3$, and f is bent, then $\dim U$ is even and $f|_U$ is bent.*

Proof Choose a basis of U to compute Walsh coefficients; bentness is independent of this choice by linear invariance. For nonzero $\boldsymbol{a} \in U$, $D_{\boldsymbol{a}} f$ is quadratic, balanced by Lemma 2.1, and T-invariant because $T\boldsymbol{a} = \boldsymbol{a}$. Lemma 3.2 makes $D_{\boldsymbol{a}}(f|_U)$ balanced. Equation (2.1) on U then gives $W_{f|_U}(\boldsymbol{\xi})^2 = 2^{\dim U}$ for every frequency. Since Walsh coefficients are integers, $\dim U$ is even, and the restriction is bent. The zero-dimensional case is included, with Walsh magnitude one. □

Coordinates of the smaller function. Write $n = Nm$, $N = 2^s$, $s \geq 1$, with m odd, and take $T = \rho^N$. Its fixed vectors are exactly the repetitions of an N-bit block. The linear isomorphism

$$\iota : V_N \longrightarrow \mathrm{Fix}(T), \qquad (\iota \boldsymbol{y})_i = y_{i \bmod N}$$

intertwines cyclic shifts. Thus $g = f \circ \iota$ is rotation symmetric, of degree at most three, and bent by Corollary 3.3. Put $N = 2h$. Every vector fixed by the original half-turn

is $(\boldsymbol{v}, \boldsymbol{v})$ for some $\boldsymbol{v} \in V_H$. The vector $\iota(\boldsymbol{u}, \boldsymbol{u})$ has period dividing h, so it is fixed by the original half-turn, since $n/2 = hm$. If $\alpha(f) = 0$, Lemma 3.1 therefore gives

$$g(\boldsymbol{u}, \boldsymbol{u}) = f(0) \qquad (\boldsymbol{u} \in V_h). \tag{3.4}$$

The remaining task is to exclude a bent g with this constant diagonal in power-of-two dimension.

Example 3.4 (Reduction in six variables) Here $N = 2$ and $m = 3$. The fixed vectors are (a, b, a, b, a, b). The reduced function is symmetric in two variables, so it has the form $g(a, b) = \beta ab + \gamma(a + b) + \delta$. Bentness requires $\beta = 1$, since the other terms are affine. If $\alpha(f) = 0$, the diagonal identity forces $g(0, 0) = g(1, 1)$, whereas these values differ by β. This is the two-variable instance of the general contradiction.

4 Why a constant diagonal is impossible

4.1 The quadratic rigidity input

Lemma 4.1 *Let $N = 2^s$, $s \geq 0$. If $q : V_N \to \mathbb{F}_2$ is quadratic, rotation symmetric and balanced, then $B_q = 0$.*

Proof Suppose $B = B_q \neq 0$. Its radical R is a proper rotation-invariant subspace. Put $\nu = \rho + I$. Since N is a power of two, $\nu^N = \rho^N + I = 0$. Also

$$\operatorname{im} \nu = \{\boldsymbol{x} \in V_N : \textstyle\sum_i x_i = 0\}. \tag{4.1}$$

The inclusion from left to right follows by summing the coordinates of $\rho\boldsymbol{y} + \boldsymbol{y}$. Conversely, the equations $y_{i+1} + y_i = x_i$ can be solved successively around the cycle; their wraparound condition is exactly $\sum_i x_i = 0$.

We claim $R \subseteq \operatorname{im} \nu$. Otherwise R contains an odd-weight vector outside the hyperplane $\operatorname{im} \nu$, and (4.1) gives $V_N = R + \nu V_N$. Since $\nu R \subseteq R$, applying ν to $V_N = R + \nu^j V_N$ gives $\nu V_N \subseteq R + \nu^{j+1} V_N$. Substitution into $V_N = R + \nu V_N$ proves $V_N = R + \nu^{j+1} V_N$. Induction gives this equality for every j. At $j = N$, nilpotence gives $V_N = R$, a contradiction.

For $\boldsymbol{r} \in R$, choose $\boldsymbol{y}$ with $\boldsymbol{r} = \rho\boldsymbol{y} + \boldsymbol{y}$. Rotation invariance of q_0 gives

$$q_0(\boldsymbol{r}) = q_0(\rho\boldsymbol{y}) + q_0(\boldsymbol{y}) + B(\rho\boldsymbol{y}, \boldsymbol{y}) = B(\boldsymbol{r} + \boldsymbol{y}, \boldsymbol{y}) = 0.$$

The last equality uses $\boldsymbol{r} \in R$ and alternation. By (3.2), the character sum of q has square $2^N |R| > 0$, contradicting balance. □

The power-of-two assumption has a precise role: it makes $\rho + I$ nilpotent. For example, on six variables the quadratic $\sum_{i=0}^{5} x_i x_{i+2}$ is the sum of the edge forms of two disjoint triangles. It is balanced and has nonzero polar, so the same rigidity conclusion fails there. The broader balancing theory is developed in [16].

4.2 A fiber that must be balanced

For $N = 2h$, put $\Delta(\boldsymbol{u}) = (\boldsymbol{u}, \boldsymbol{u})$ and $e(\boldsymbol{z}) = (0, \boldsymbol{z})$, with $\boldsymbol{u}, \boldsymbol{z} \in V_h$. Define the fibers

$$F_{\boldsymbol{z}}(\boldsymbol{u}) = g(\boldsymbol{u}, \boldsymbol{u} + \boldsymbol{z}) = g(\Delta(\boldsymbol{u}) + e(\boldsymbol{z})).$$

The diagonal is the fiber $\boldsymbol{z} = 0$. The complementary fiber is $F_{\mathbf{1}_h}$, where $\mathbf{1}_h$ is the all-ones vector.

Lemma 4.2 *If $g : V_{2h} \to \mathbb{F}_2$ is bent and constant on the diagonal, then $F_{\boldsymbol{z}}$ is balanced for every $\boldsymbol{z} \neq 0$.*

Proof Let $A(\boldsymbol{z}) = \sum_{\boldsymbol{u}} (-1)^{F_{\boldsymbol{z}}(\boldsymbol{u})}$. For this integer-valued function, define the unnormalized Fourier transform by $\widehat{A}(\boldsymbol{\xi}) = \sum_{\boldsymbol{z}} A(\boldsymbol{z})(-1)^{\boldsymbol{\xi}\cdot\boldsymbol{z}}$. Substitution gives

$$\widehat{A}(\boldsymbol{\xi}) = \sum_{\boldsymbol{z},\boldsymbol{u}} (-1)^{g(\boldsymbol{u},\boldsymbol{u}+\boldsymbol{z})+\boldsymbol{\xi}\cdot\boldsymbol{z}} = W_g(\boldsymbol{\xi},\boldsymbol{\xi}).$$

Bentness gives $\widehat{A}(\boldsymbol{\xi})^2 = 2^{2h}$. Parseval for this convention states $\sum_{\boldsymbol{\xi}} \widehat{A}(\boldsymbol{\xi})^2 = 2^h \sum_{\boldsymbol{z}} A(\boldsymbol{z})^2$, and therefore

$$\sum_{\boldsymbol{z}} A(\boldsymbol{z})^2 = 2^{-h} \sum_{\boldsymbol{\xi}} \widehat{A}(\boldsymbol{\xi})^2 = 2^{2h}. \tag{4.2}$$

The constant diagonal already gives $A(0)^2 = 2^{2h}$. Every other nonnegative term in (4.2) must be zero, which is the required balance. □

4.3 The same fiber must be constant

Lemma 4.3 *Let $g : V_{2h} \to \mathbb{F}_2$ be rotation symmetric, of degree at most three, and constant on the diagonal. Put $\boldsymbol{J} = \mathbf{1}_{2h}$. If $B_{D_{\boldsymbol{J}}g} = 0$, then $F_{\mathbf{1}_h}$ is constant.*

Proof Write $F = F_{\mathbf{1}_h}$ and $\boldsymbol{w} = e(\mathbf{1}_h)$. We first show that $B_F = 0$, then use rotation to eliminate its linear part. Lemma 2.2 gives

$$B_F(\boldsymbol{u},\boldsymbol{v}) = D_{\Delta(\boldsymbol{u})}D_{\Delta(\boldsymbol{v})}g(\boldsymbol{w}) = D_{\Delta(\boldsymbol{u})}D_{\Delta(\boldsymbol{v})}g(0) + \Theta_g(\Delta(\boldsymbol{u}),\Delta(\boldsymbol{v}),\boldsymbol{w}).$$

The first term is zero: its four values of g lie on the constant diagonal. Let $\theta = \rho^h$ be the half-turn on V_N, analogous to τ on the original space. It swaps the blocks. Since $g \circ \theta = g$, we have $D_{\theta\boldsymbol{a}}g(\theta\boldsymbol{x}) = D_{\boldsymbol{a}}g(\boldsymbol{x})$; applying this three times proves invariance of Θ_g. Thus θ fixes $\Delta(\boldsymbol{u})$, preserves Θ_g, and satisfies $\boldsymbol{J} = \boldsymbol{w} + \theta\boldsymbol{w}$ and $\Delta(\boldsymbol{v}) = e(\boldsymbol{v}) + \theta e(\boldsymbol{v})$. Hence

$$\begin{aligned}\Theta_g(\Delta(\boldsymbol{u}),e(\boldsymbol{v}),\boldsymbol{J}) &= \Theta_g(\Delta(\boldsymbol{u}),e(\boldsymbol{v}),\boldsymbol{w}) + \Theta_g(\Delta(\boldsymbol{u}),e(\boldsymbol{v}),\theta\boldsymbol{w}) \\ &= \Theta_g(\Delta(\boldsymbol{u}),e(\boldsymbol{v}),\boldsymbol{w}) + \Theta_g(\Delta(\boldsymbol{u}),\theta e(\boldsymbol{v}),\boldsymbol{w}) \\ &= \Theta_g(\Delta(\boldsymbol{u}),\Delta(\boldsymbol{v}),\boldsymbol{w}).\end{aligned} \tag{4.3}$$

The middle equality applies θ to all arguments in the second term. By (2.2), the left side is $B_{D_{\boldsymbol{J}}g}(\Delta(\boldsymbol{u}),e(\boldsymbol{v})) = 0$. Thus $B_F = 0$. By the definition of the polar expression, $F + F(0)$ is additive, so $F(\boldsymbol{u}) = \boldsymbol{\lambda}\cdot\boldsymbol{u} + c$ for some $\boldsymbol{\lambda} \in V_h$.

For clarity in the following formula, write σ for the cyclic shift on the block space: $(\sigma\boldsymbol{u})_i = u_{i+1 \bmod h}$. Let $\boldsymbol{b}_{h-1}$ be its last standard basis vector. Directly from $(\rho\boldsymbol{x})_i = x_{i+1}$,

$$\rho(\boldsymbol{u},\boldsymbol{u}+\mathbf{1}_h) = (\sigma\boldsymbol{u}+\boldsymbol{b}_{h-1},\ \sigma\boldsymbol{u}+\boldsymbol{b}_{h-1}+\mathbf{1}_h).$$

Rotation invariance of g gives $F(\sigma\boldsymbol{u}+\boldsymbol{b}_{h-1}) = F(\boldsymbol{u})$. Comparing linear coefficients shows that all coordinates of $\boldsymbol{\lambda}$ are equal. Taking $\boldsymbol{u} = 0$ gives $\boldsymbol{\lambda}\cdot\boldsymbol{b}_{h-1} = 0$, so every coordinate is zero. Therefore F is constant. This calculation also covers $h = 1$. □

Proposition 4.4 *If $N = 2^s$, $s \geq 1$, a rotation symmetric function $g : V_N \to \mathbb{F}_2$ of degree at most three and constant on the diagonal cannot be bent.*

Proof Suppose g is bent and put $N = 2h$. Lemma 4.2 makes $F_{\mathbf{1}_h}$ balanced. The nonzero direction $\boldsymbol{J}$ is fixed by rotation, so $D_{\boldsymbol{J}}g$ is rotation symmetric, quadratic, and balanced by Lemma 2.1. Lemma 4.1 gives $B_{D_{\boldsymbol{J}}g} = 0$; Lemma 4.3 then makes $F_{\mathbf{1}_h}$ constant. Its character sum would be $\pm 2^h$, contradicting balance. □

5 Proof of the main theorem and examples

Proof of Theorem 1.1 Suppose $\alpha(f) = 0$. Section 3 constructs a rotation symmetric bent function g of degree at most three in dimension $N = 2^s$ and shows in (3.4) that it is constant on the diagonal. Proposition 4.4 gives a contradiction. Therefore $\alpha(f) = 1$. Corollary 1.2 follows by the absence of quadratic terms in a homogeneous cubic. □

Example 5.1 (A family satisfying the hypotheses) For every $H \geq 1$, P_{2H} is bent: its Walsh sum factors into H two-variable sums

$$\sum_{a,b \in \mathbb{F}_2} (-1)^{ab + \xi_i a + \xi_{i+H} b} = 2(-1)^{\xi_i \xi_{i+H}} \qquad (0 \leq i < H).$$

Thus every Walsh magnitude is 2^H. Adding either constant or the invariant linear form $\sum_i x_i$ preserves bentness and rotation symmetry. Antipodal necessity therefore applies to a nonempty family.

6 Concluding remarks

The proof establishes antipodal necessity in degree at most three. The argument in Example 3.4 illustrates the reduction, while Example 5.1 verifies that the hypotheses are attained. The homogeneous rotation symmetric conjecture in higher degree requires additional arguments.

The degree bound controls both monomial cancellation and the behavior of derivatives. In Lemma 3.1, a half-turn fixed support of size at most three is empty or one antipodal pair; degree four also allows two pairs. In Corollary 3.3, derivatives must be quadratic for the balance-transfer lemma to apply. The complementary-fiber argument also requires quadratic derivatives and a trilinear third difference (Lemma 2.2). These properties are not available for a general quartic, so the present proof does not settle that case.

7 Formal verification

A Lean 4 formalization of Theorem 1.1 and Corollary 1.2 accompanies this article; the proof given above does not depend on it. The formal sources and historical build records are unchanged from version 3. They certify the original proof route, including the odd-order reduction, not the Jordan descent introduced in Appendix B. No new

Lean execution is claimed for this revision. Appendix A states the formal hypotheses and conclusion and relates the main formal declarations to the statements above. Online Resource 1 contains the formal sources at a fixed revision, reproduction instructions, build and axiom-check records, and finite computational controls, which are separate from the universal proof. The predecessor manuscript and the unchanged formal archive are available in version 3 at https://doi.org/10.6084/m9.figshare.34165260.v3. The earlier supporting source archive is also identified in [17].

Statements and Declarations

Funding. This research received no specific funding.

Competing interests. The author declares no competing interests.

Ethics approval. Not applicable.

Author contribution. F.M.V. formulated the research question, planned the formalization and computational checks, and directed the development and presentation of the manuscript. The V4 review package records the new AI-assisted proof review and finite controls separately from the unchanged Lean archive.

Use of AI-assisted tools. Generative AI systems (OpenAI ChatGPT and Codex, Google Gemini, and Anthropic Claude) were used extensively to explore proof strategies and intermediate lemmas, search for errors in preliminary arguments, write and debug Lean and Python verification code, search the literature, and revise the text. The proof strategy was developed through iterative exchanges between the author and these tools. The main theorem and its corollary were checked by the Lean 4 kernel; Appendix A specifies the formal statements and their correspondence with the article. The author checked the cited results against the original publications. The Jordan-descent strategy in Appendix B was proposed by the OpenAI model used under the session name Astra, and the argument received additional AI-assisted mathematical review. These reviews and the new finite controls do not constitute formal verification of that proof or external peer review. AI systems are not authors; the author takes full responsibility for the content.

Data and code availability. The proof is contained in this article. Supporting formal sources at the pinned revision, finite verification scripts and reproduction instructions are provided in Online Resource 1. The public preprint archive and verification repository are identified in Section 7 and Appendix A.

Supplementary information. Online Resource 1 (ESM_1.zip): formal proof sources at the pinned revision, project configuration, finite controls, provenance manifest and reproduction instructions.

A Formal statement and correspondence

The formal sources are those of commit

`6dd183685ef8a5b033c1bcf8733496d57b853cc7`

of the GitHub repository

`contatofilipevono-rgb/hrsbf-bent-verification`,

checked with Lean 4.15.0 and the Mathlib revision recorded in Online Resource 1. The source files cited below are in `formalization/Antipodal/`, and all declarations lie in the namespace `HRSBF.Antipodal`.

Formal statement. The hypotheses of the main formal theorem are positive half-dimension H, canonical ANF degree at most three, cyclic invariance, and integer Walsh magnitude 2^H on $2H$ variables. Its conclusion is that the canonical ANF coefficient of $x_0 x_H$ equals one, which is precisely $\alpha(f) = 1$. In `CanonicalANF.lean`, `anfCoefficient` is defined by the Boolean Möbius transform, with reconstruction and uniqueness; the degree predicate requires all coefficients on supports larger than three to vanish, and the homogeneous-cubic predicate requires all coefficients outside size three to vanish and at least one size-three coefficient to equal one. Rotation symmetry means $f(\mathrm{rotate}\,\boldsymbol{x}) = f(\boldsymbol{x})$, where $\mathrm{rotate}\,\boldsymbol{x}$ has coordinate $x_{i+1 \bmod n}$. In `Autocorrelation.lean`, `walsh` is the integer character sum of Section 2, and `IsBent` requires its square to equal 2^n at every frequency; for $n = 2H$ this is equivalent to magnitude 2^H.

The declarations for the theorem and the corollary, respectively, are

`universal_antipodal_walsh_absolute`

`no_homogeneous_cubic_rotation_symmetric_bent_absolute`

The archived axiom-check records list only the standard axioms `propext`, `Classical.choice` and `Quot.sound`; the build and axiom-check records are included in Online Resource 1.

Correspondence. Table 1 records interfaces and dependencies, rather than asserting identical theorem statements in every case. The formal result `complementary_fiber_balance` supplies the complementary-fiber instance of Lemma 4.2, which is the only instance needed for the contradiction. The finite-difference identities of Lemma 2.2 are distributed across the listed interfaces and their dependencies. The formal rigidity theorem uses block coordinates and a cubic representation; the surrounding modules derive these hypotheses from canonical ANF degree at most three.

Table 1: Correspondence between the mathematical argument and the main Lean interfaces at the pinned revision.

Mathematical step	Source and interface
Lemma 2.1	`Autocorrelation.lean`: `bent_iff_derivative_balanced`
Lemma 2.2	`LocalRigidity.lean`: `third_add_right`, `third_swap`, `polar_derivative` (finite-difference interfaces)
Lemma 3.1	`PowerTwoCubic.lean`: `constant_on_halfTurn_fixed_of_antipodal_zero` (zero-coefficient implication)

Mathematical step	Source and interface
Lemma 3.2	`OddRestriction.lean`: `odd_order_quadratic_balance_iff`
Corollary 3.3	`OddRestriction.lean`: `odd_order_bent_restriction`
Repeated-block coordinates	`CyclicOddCoordinates.lean`: `cyclicFixedEquiv`, `bent_repeatInto`
Lemma 4.1	`CyclicQuadraticRigidity.lean`: `balanced_rotation_invariant_quadratic_polar_zero`
Lemma 4.2	`Fourier.lean`: `complementary_fiber_balance` (the complementary-fiber instance used in the contradiction)
Lemma 4.3	`Cyclic.lean`: `local_complementary_fiber_rigidity`
Proposition 4.4	`PowerTwoCubic.lean`: `not_bent_constant_diagonal_power_two_of_cubic`
Theorem 1.1	`GlobalAntipodal.lean`: `universal_antipodal`; conventional Walsh interface in `WalshNormalization.lean`
Corollary 1.2	`GlobalAntipodal.lean`: `no_homogeneous_cubic_rotation_symmetric_bent`

B A second proof by Jordan descent

This appendix gives a second proof of Theorem 1.1. It shares the half-turn cancellation and odd-order restriction of Section 3 with the first proof. It replaces the Parseval and complementary-fiber argument of Section 4 by descent through a single unipotent Jordan block. No new nonexistence theorem is claimed. The formal sources described in Appendix A certify the original route; the Jordan argument below has not been formalized in Lean.

B.1 Balanced invariant quadratics on a single block

Throughout this appendix let $d \geq 1$, let $V = \mathbb{F}_2^d$, and choose a basis $\boldsymbol{e}_0, \dots, \boldsymbol{e}_{d-1}$. Define the nilpotent map L by $L\boldsymbol{e}_0 = 0$ and $L\boldsymbol{e}_i = \boldsymbol{e}_{i-1}$ for $i > 0$, and put $J = I + L$. Write

$$E_k = \langle \boldsymbol{e}_0, \dots, \boldsymbol{e}_{k-1} \rangle \quad (0 \leq k \leq d), \qquad t\left(\sum_{i=0}^{d-1} x_i \boldsymbol{e}_i\right) = x_{d-1},$$

where $E_0 = \{0\}$. These coordinates are Jordan coordinates, not the original cyclic coordinates of the main theorem.

Lemma B.1 *If $q : V \to \mathbb{F}_2$ is quadratic, $q \circ J = q$, and q is balanced, then $q = t + c$ for some $c \in \mathbb{F}_2$.*

Proof Replace q by $q + q(0)$, so that $q(0) = 0$, and let $K = \operatorname{Rad} B_q$. Since J is invertible and preserves B_q, it preserves K; hence K is also stable under $L = J + I$.

Every L-stable subspace is one of the prefixes E_k. To see this without a classification theorem, take the largest index $k - 1$ that occurs with a nonzero coefficient in any vector of a nonzero stable subspace. A vector with that last index, together with its images under $L, L^2, \dots, L^{k-1}$, gives k independent vectors in E_k: their last nonzero indices are $k-1, k-2, \dots, 0$. Thus the subspace equals E_k. The zero subspace is E_0.

On K, the normalized quadratic q is linear. If $K = E_k$ with $0 < k < d$, its invariance implies $q(L\boldsymbol{r}) = 0$ for every $\boldsymbol{r} \in K$, so it vanishes on $LK = E_{k-1}$. Invariance at $\boldsymbol{e}_k$ also gives

$$0 = q(J\boldsymbol{e}_k) + q(\boldsymbol{e}_k) = q(\boldsymbol{e}_{k-1}) + B_q(\boldsymbol{e}_k, \boldsymbol{e}_{k-1}) = q(\boldsymbol{e}_{k-1}),$$

because $\boldsymbol{e}_{k-1} \in K$. Therefore q vanishes on K. It also vanishes on K when $K = E_0$. In both proper-radical cases, the quadratic character-sum identity (3.2) gives

$$\left(\sum_{\boldsymbol{x} \in V} (-1)^{q(\boldsymbol{x})}\right)^2 = |V|\,|K| > 0,$$

contradicting balance.

Consequently $K = V$, and q is linear on all of V. The equality $q \circ J = q$ is then equivalent to $q \circ L = 0$. Since $LV = E_{d-1}$, the only invariant linear forms are 0 and t. Balance excludes zero. Restoring the constant proves the lemma, including $d = 1$. □

B.2 Descent by two dimensions

Proposition B.2 *Let $d = 2m > 0$. No J-invariant function $g : V \to \mathbb{F}_2$ of degree at most three, constant on E_m, is bent.*

Proof Suppose such a g is bent. Since $J\boldsymbol{e}_0 = \boldsymbol{e}_0$, the derivative $q = D_{\boldsymbol{e}_0} g$ is J-invariant. It is quadratic and balanced, by the degree bound and Lemma 2.1. Moreover $q(0) = g(\boldsymbol{e}_0) + g(0) = 0$, since both points belong to E_m. Lemma B.1 therefore gives

$$D_{\boldsymbol{e}_0} g = t. \tag{B.1}$$

If $d = 2$, evaluate this identity at $\boldsymbol{e}_1$. Its right side is one, whereas

$$D_{\boldsymbol{e}_0} g(\boldsymbol{e}_1) = g(\boldsymbol{e}_1 + \boldsymbol{e}_0) + g(\boldsymbol{e}_1) = g(J\boldsymbol{e}_1) + g(\boldsymbol{e}_1) = 0.$$

This settles the base case without invoking a zero-dimensional descent.

Now assume $d \geq 4$ and write $\boldsymbol{z} = (x_1, \ldots, x_{d-2})$. Identity (B.1) gives the Boolean polynomial decomposition

$$g(x_0, \boldsymbol{z}, t) = x_0 t + h(\boldsymbol{z}, t), \qquad h(\boldsymbol{z}, t) = g(0, \boldsymbol{z}, t). \tag{B.2}$$

In particular $\deg h \leq 3$. For a frequency $(u_0, \boldsymbol{u}_z, u_t)$, summing first over x_0 gives

$$\begin{aligned} W_g(u_0, \boldsymbol{u}_z, u_t) &= \sum_{\boldsymbol{z}, t} (-1)^{h(\boldsymbol{z}, t) + \boldsymbol{u}_z \cdot \boldsymbol{z} + u_t t} \sum_{x_0 \in \mathbb{F}_2} (-1)^{x_0 (t + u_0)} \\ &= 2(-1)^{u_0 u_t} W_{h(\,\cdot\,, u_0)}(\boldsymbol{u}_z). \end{aligned} \tag{B.3}$$

Thus bentness of g implies that both functions $h(\,\cdot\,, 0)$ and $h(\,\cdot\,, 1)$ are bent in $d-2$ variables, with Walsh magnitude 2^{m-1}.

It remains to check the symmetry and the constant-prefix hypothesis for the zero slice. Set $H = \ker t = E_{d-1}$. This subspace is J-stable, and (B.1) shows that $g|_H$ is constant on each coset of $\langle \boldsymbol{e}_0 \rangle$. It therefore defines a function $\bar{g}$ on $H / \langle \boldsymbol{e}_0 \rangle$. In the basis $\bar{\boldsymbol{e}}_1, \ldots, \bar{\boldsymbol{e}}_{d-2}$, this function is exactly $h(\boldsymbol{z}, 0)$, so it is bent and has degree at most three. The degree assertion follows by the linear section $x_0 = t = 0$; restriction and a linear coordinate change do not increase Boolean algebraic degree.

The induced operator satisfies

$$\bar{J}\bar{\boldsymbol{e}}_1 = \bar{\boldsymbol{e}}_1, \qquad \bar{J}\bar{\boldsymbol{e}}_i = \bar{\boldsymbol{e}}_i + \bar{\boldsymbol{e}}_{i-1} \quad (2 \leq i \leq d-2).$$

It is a single block of size $d-2$, and $\bar{g} \circ \bar{J} = \bar{g}$ follows from $g \circ J = g$. The image of E_m is the middle prefix $\langle \bar{\boldsymbol{e}}_1, \ldots, \bar{\boldsymbol{e}}_{m-1} \rangle$, on which $\bar{g}$ is constant. Hence every hypothesis is preserved when d is replaced by $d-2$. Induction reaches the impossible base case $d = 2$. □

B.3 Return to cyclic coordinates

Second proof of Theorem 1.1 Assume $\alpha(f) = 0$ and write $n = d\ell$ with $d = 2^s$, $s \geq 1$, and ℓ odd. The half-turn lemma and odd-order restriction in Section 3 give a bent rotation symmetric function g on $\mathbb{F}_2^d$, of degree at most three and constant on the fixed space of the half-turn. Indeed, on the repeated-block subspace the original half-turn induces $\rho^{d\ell/2} = \rho^{d/2}$, since ℓ is odd and $\rho^d = I$ on the smaller block.

The cyclic shift ρ in dimension d has a cyclic vector: successive shifts of any coordinate basis vector form a basis. Consequently its minimal polynomial has degree d. Since $\rho^d = I$ and $X^d - 1 = (X+1)^d$ over $\mathbb{F}_2$, its minimal polynomial is $(X+1)^d$. Thus ρ is similar to a single block $J = I + L$ as above. In these coordinates,

$$\rho^{d/2} = I + L^{d/2}, \qquad \mathrm{Fix}(\rho^{d/2}) = \ker L^{d/2} = E_{d/2}.$$

The first equality uses that $d/2$ is a power of two, including $d = 2$. Invertible linear coordinate changes preserve degree and bentness. Proposition B.2 now contradicts the existence of g. Hence $\alpha(f) = 1$, and Corollary 1.2 follows as before. □

B.4 Scope of the second proof and finite controls

The descent proposition treats every positive even block size; the intermediate sizes need not be powers of two. Only its return to a cyclic shift uses $d = 2^s$. The shared odd-order reduction still requires quadratic derivatives, so this second proof does not establish a general quartic nonexistence result.

The accompanying V4 checking package constructs the invariant ANF spaces by binary linear algebra and tests the full Walsh spectrum of every function in the indicated finite spaces. The checks do not assume the Jordan derivative conclusion as a filter. They are numerical controls for the written proof, not a Lean verification or a proof in arbitrary dimension.

Block size d	Invariant cubics constant on $E_{d/2}$	Bent
2	4	0
4	16	0
6	64	0
8	4096	0

Here "cubics" includes all functions of degree at most three, including constants. A separate exhaustive check of invariant quadratics in dimensions $1 \le d \le 8$ finds precisely the two balanced functions t and $t + 1$ in each dimension. These checks include odd block sizes for the quadratic lemma and the non-power-of-two size $d = 6$ for descent.

References

[1] Rothaus, O.S.: On "bent" functions. J. Comb. Theory Ser. A **20**(3), 300–305 (1976) https://doi.org/10.1016/0097-3165(76)90024-8

[2] Carlet, C., Mesnager, S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5–50 (2016) https://doi.org/10.1007/s10623-015-0145-8

[3] Carlet, C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2021). https://doi.org/10.1017/9781108606806

[4] Cusick, T.W., Stănică, P.: Cryptographic Boolean Functions and Applications, 2nd edn. Academic Press, London (2017). https://doi.org/10.1016/C2016-0-00852-5

[5] Pieprzyk, J., Qu, C.X.: Rotation-symmetric functions and fast hashing. In: Boyd, C., Dawson, E. (eds.) Information Security and Privacy (ACISP 1998). Lecture Notes in Computer Science, vol. 1438, pp. 169–180. Springer, Berlin, Heidelberg (1998). https://doi.org/10.1007/BFb0053731

[6] Stănică, P., Maitra, S.: Rotation symmetric Boolean functions—Count and cryptographic properties. Discrete Appl. Math. **156**(10), 1567–1580 (2008) https://doi.org/10.1016/j.dam.2007.04.029

[7] Kavut, S., Maitra, S., Yücel, M.D.: Search for Boolean functions with excellent profiles in the rotation symmetric class. IEEE Trans. Inf. Theory **53**(5), 1743–1751 (2007) https://doi.org/10.1109/TIT.2007.894696

[8] Stănică, P., Maitra, S., Clark, J.A.: Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions. In: Roy, B., Meier, W. (eds.) Fast Software Encryption 2004. Lecture Notes in Computer Science, vol. 3017, pp. 161–177. Springer, Berlin, Heidelberg (2004). https://doi.org/10.1007/978-3-540-25937-4_11

[9] Dalai, D.K., Maitra, S., Sarkar, S.: Results on rotation symmetric bent functions. Discrete Math. **309**(8), 2398–2409 (2009) https://doi.org/10.1016/j.disc.2008.05.017

[10] Gao, G., Zhang, X., Liu, W., Carlet, C.: Constructions of Quadratic and Cubic Rotation Symmetric Bent Functions. IEEE Trans. Inf. Theory **58**(7), 4908–4913 (2012) https://doi.org/10.1109/TIT.2012.2193377

[11] Meng, Q., Chen, L., Fu, F.-W.: On homogeneous rotation symmetric bent functions. Discrete Appl. Math. **158**(10), 1111–1117 (2010) https://doi.org/10.1016/j.dam.2010.02.009

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

[13] Charnes, C., Rötteler, M., Beth, T.: Homogeneous Bent Functions, Invariants, and Designs. Des. Codes Cryptogr. **26**(1-3), 139–154 (2002) https://doi.org/10.1023/A:1016509410000

[14] Wang, T., Liu, M., Zhao, S., Lin, D.: Construction of cubic rotation symmetric bent functions in power-of-two variables. In: 2015 IEEE International Symposium on Information Theory (ISIT), pp. 486–490 (2015). https://doi.org/10.1109/ISIT.2015.7282502

[15] Polujan, A., Kudin, S., Pasalic, E.: Rotation-Symmetric Bent Functions Outside the Completed Maiorana-McFarland Class. IEEE Trans. Inf. Theory **72**(6), 4341–4351 (2026) https://doi.org/10.1109/TIT.2026.3685133

[16] Chirvasitu, A., Cusick, T.W.: Quadratic rotation symmetric Boolean functions. Discrete Appl. Math. **343**, 91–105 (2024) https://doi.org/10.1016/j.dam.2023.10.010

[17] Vono, F.: Antipodal Necessity and the Cubic Case of the Homogeneous Rotation-Symmetric Bent Function Conjecture. Figshare. Version 2. Supporting formal source archive (2026). https://doi.org/10.6084/m9.figshare.34165260.v2