The Maximum Possible Nonlinearity for a Balanced Boolean Function in 10 Variables is 492

Youle Xu* and Qichun Wang †‡

Abstract

Determining the maximum nonlinearity of 10-variable balanced Boolean functions has been a long-standing open problem. In this paper, we resolve it by proving that the maximum nonlinearity is exactly 492, thereby confirming Dobbertin's conjecture in dimension 10. To exclude nonlinearity 494, we derive a quadratic residue for the Walsh spectrum and refine a local energy table from four-block concatenation by retaining the signs of the Walsh coefficients. The resulting bounds exclude all but the largest polar rank; a product inequality and a parity argument eliminate the remaining case.

Keywords: Boolean functions, nonlinearity, Walsh transform, quadratic forms.

1 Introduction

Boolean functions are widely used in cryptography and coding theory [1, 8]. Balance and high nonlinearity are important design criteria for Boolean functions used in symmetric ciphers [4]. For $n \geq 2$, the classical upper bound for the nonlinearity of $2n$-variable balanced Boolean functions is $2^{2n-1} - 2^{n-1} - 2$, which is attained for $n = 2, 3$. Whether there exists a 10-variable balanced Boolean function with nonlinearity 494 has remained open [1, 2, 5, 9, 10].

*China Telecom Corporation Limited, Huaibei Branch, China. Email: youlexu@163.com.

†School of Computer and Electronic Information/School of Artificial Intelligence, Nanjing Normal University, Nanjing, China. Email: qcwang@fudan.edu.cn.

‡Corresponding author.

Let NB_n denote the maximum nonlinearity of n-variable balanced Boolean functions. Dobbertin conjectured that [6]

$$NB_{2n} = 2^{2n-1} - 2^n + NB_n.$$

In particular, since $NB_5 = 12$, the conjecture predicts $NB_{10} = 2^9 - 2^5 + NB_5 = 492$.

Kavut, Maitra and Yücel [7] obtained 10-variable Boolean functions with first-order resiliency and nonlinearity 492. In particular, these functions are balanced, so $NB_{10} \geq 492$. Thus it remains to exclude nonlinearity 494 in order to determine NB_{10}.

In this paper, we determine the maximum nonlinearity for 10-variable balanced Boolean functions, and prove the following theorem, establishing the 10-variable instance of Dobbertin's conjecture.

Theorem 1. *The maximum nonlinearity of 10-variable balanced Boolean functions is 492.*

The rest of the paper is organized as follows. Section 2 recalls the necessary background. Section 3 derives the local energy table and its signed refinement. Section 4 excludes all possible polar ranks, and Section 5 concludes the paper.

2 Preliminaries

Let $\mathbb{F}_2$ denote the binary finite field, and let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. A *Boolean function* of n variables is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. We denote by B_n the set of all n-variable Boolean functions.

Every Boolean function has a unique *algebraic normal form* (ANF), which is its multivariate polynomial representation over $\mathbb{F}_2$:

$$f(x_1, \ldots, x_n) = \bigoplus_{S \subseteq \{1,2,\ldots,n\}} a_S \prod_{i \in S} x_i.$$

The *algebraic degree* of f, denoted by $\deg(f)$, equals $\max\{|S| : a_S \neq 0\}$. The function f is *affine*, if $\deg(f) \leq 1$. We use A_n to denote the set of all n-variable affine functions.

Let $f \in B_n$ and

$$supp(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}.$$

The cardinality $|supp(f)|$ is called the *Hamming weight* of f, and will be denoted by $wt(f)$. The function f is *balanced* if $wt(f) = 2^{n-1}$.

Let $f, g \in B_n$. The *Hamming distance* between f and g is $d(f,g) = wt(f \oplus g)$. The *nonlinearity* of f, denoted by $nl(f)$, is the minimum distance between f and the set of affine functions. That is, $nl(f) = \min_{g \in A_n} d(f,g)$.

The *Walsh transform* of a given function $f \in B_n$ is the integer-valued function over $\mathbb{F}_2^n$ defined by

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\omega \cdot x},$$

where $\omega \in \mathbb{F}_2^n$, and $\omega \cdot x = \omega_1 x_1 + \cdots + \omega_n x_n$ is the usual inner product. It is easy to see that a Boolean function f is balanced if and only if $W_f(0) = 0$.

For a real-valued function v on $\mathbb{F}_2^m$, write

$$H_m v(a) = \sum_{x \in \mathbb{F}_2^m} v(x)(-1)^{a \cdot x}.$$

Thus $W_f = H_n((-1)^f)$ for $f \in B_n$. With the usual sum inner product, H_m is self-adjoint and $H_m^2 = 2^m I$. For such a function, $\mathrm{supp}(v) = \{x : v(x) \neq 0\}$.

The nonlinearity of f can be determined by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|.$$

By Parseval's identity, $\max_\omega |W_f(\omega)| \geq 2^{n/2}$. Therefore,

$$nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

If the upper bound is achieved, then f is a *bent* function [3, 11]. Since bent functions are not balanced and the nonlinearity of a balanced function in at least two variables is even, the nonlinearity of $2m$-variable balanced Boolean functions, for $m \geq 2$, is upper bounded by $2^{2m-1} - 2^{m-1} - 2$.

We use $||$ to denote the concatenation, that is,

$$(f_1||f_2)(x_1, \ldots, x_n, x_{n+1}) = (x_{n+1} \oplus 1) f_1(x_1, \ldots, x_n) \oplus x_{n+1} f_2(x_1, \ldots, x_n),$$

and $f_1||f_2||f_3||f_4 =$

$$(x_{n+1}+1)(x_{n+2}+1) f_1 + (x_{n+1}+1) x_{n+2} f_2 + x_{n+1}(x_{n+2}+1) f_3 + x_{n+1} x_{n+2} f_4,$$

where $f_1, f_2, f_3, f_4 \in B_n$.

Here quadratic means of algebraic degree at most two. For a quadratic Boolean function f with $f(0) = 0$, its polar form is $B_f(x,y) = f(x+y) + f(x) + f(y)$. Its radical is the set of y with $B_f(x,y) = 0$ for all x. The polar rank means the rank of B_f, and nondegenerate means that its radical is zero. It is known that the polar rank must be even [1].

Lemma 1 (Proposition 55 of [1])**.** *Let $f \in B_n$ be quadratic with $f(0) = 0$ and polar rank $2r$. Then W_f is supported on an affine subspace of size 2^{2r}, and all its nonzero values have magnitude 2^{n-r}. Therefore,*

$$wt(f) \in \{2^{n-1}, 2^{n-1} - 2^{n-r-1}, 2^{n-1} + 2^{n-r-1}\}.$$

3 The local energy table and its signed refinement

Lemma 2. *Let $f \in B_{10}$ be balanced with $nl(f) = 494$. There exist $L \in A_{10}$ and $R \in B_{10}$ of degree at most two such that, for every $\omega \in \mathbb{F}_2^{10}$,*

$$\frac{W_f(\omega)}{4} \equiv L(\omega) + 2R(\omega) \pmod 4,$$

Proof. Clearly,

$$W_f(a) = \sum_x (-1)^{f(x)+a\cdot x} = \sum_x (-1)^{f(x)} \prod_{i=1}^{10} (1 - 2a_i x_i).$$

Expanding $\prod_i (1 - 2a_i x_i)$ gives

$$W_f(a) = \sum_{I \subseteq [10]} (-2)^{|I|} a^I \sum_{x:\, x_i = 1 \ (i \in I)} (-1)^{f(x)}. \tag{1}$$

Here $[10] = \{1, \ldots, 10\}$ and $a^I = \prod_{i \in I} a_i$. The constant term vanishes by balance. For $1 \le |I| < 10$, the inner sum is even, while the term $|I| = 10$ already has a factor 2^{10}. After division by four, only linear terms and even quadratic terms remain modulo four. Their reduction modulo two is a linear Boolean function $L = \bigoplus_{i \in J} a_i$ for some $J \subseteq [10]$. Its integer representative satisfies

$$\bigoplus_{i \in J} a_i \equiv \sum_{i \in J} a_i - 2 \sum_{\substack{i<j \\ i,j \in J}} a_i a_j \pmod 4.$$

Subtracting this representative leaves twice a Boolean polynomial of degree at most two, as required. □

Throughout this section, assume f is balanced and $nl(f) = 494$. At the origin, the residue lemma gives $L(0) + 2R(0) \equiv 0 \pmod 4$, so $L(0) = 0$. If $L = 0$, then every Walsh coefficient is divisible by 8. The peak bound gives $|W_f(\omega)| \le 32$; since $W_f(0) = 0$, Parseval would give

$$\sum_\omega W_f(\omega)^2 \le 1023 \cdot 32^2 < 2^{20},$$

a contradiction. Thus L is a nonzero linear function. After an invertible linear change of variables, take $L(a,c)=c$, with $(a,c)\in\mathbb{F}_2^9\times\mathbb{F}_2$. Write the transformed function as h. Then

$$\frac{W_h(a,c)}{4}\equiv c+2R(a,c)\pmod 4,$$

where R is quadratic with $R(0)=0$. Decompose

$$W_h(a,c)\equiv 4c+8(Q(a)\oplus c(a\cdot t\oplus\alpha))\pmod{16},$$

where $t\in\mathbb{F}_2^9$, $\alpha\in\mathbb{F}_2$ and $Q\in B_9$. Let $\delta=(t,\alpha)$ and $g(x)=h(x\oplus\delta)$. Then g is balanced with $nl(g)=494$ and

$$W_g(a,c)=(-1)^{a\cdot t+c\alpha}W_h(a,c).$$

If $c=0$, then

$$W_g(a,c)=\pm W_h(a,c)\equiv 8Q(a)\pmod{16}.$$

If $c=1$, then

$$W_g(a,c)\equiv(-1)^{a\cdot t\oplus\alpha}(4+8(Q(a)\oplus a\cdot t\oplus\alpha))\equiv 4+8Q(a)\pmod{16}.$$

Therefore, we have

$$W_g(a,c)\equiv 4c+8Q(a)\pmod{16},\tag{2}$$

for any $(a,c)\in\mathbb{F}_2^9\times\mathbb{F}_2$, where $Q\in B_9$ is a quadratic function with $Q(0)=0$.

Write $g=g_0||g_1||g_2||g_3$, where $g_i\in B_8$ for $0\le i\le 3$; explicitly, $g_{2j+c}(x)=g(x,j,c)$ for $j,c\in\{0,1\}$. Let $A_i(u)=W_{g_i}(u)$ for $0\le i\le 3$ and $S_{ij}(u)=W_g(u,i,j)$ for $i,j\in\{0,1\}$. Then we have

$$\begin{aligned}
S_{00}&=A_0+A_1+A_2+A_3,\\
S_{01}&=A_0-A_1+A_2-A_3,\\
S_{10}&=A_0+A_1-A_2-A_3,\\
S_{11}&=A_0-A_1-A_2+A_3.
\end{aligned}\tag{3}$$

Let $q_0=Q(u,0)$ and $q_1=Q(u,1)$, where $u\in\mathbb{F}_2^8$. By (2), we have

$$\begin{aligned}
S_{00}&\equiv 8q_0\pmod{16},\ S_{01}\equiv 4+8q_0\pmod{16},\\
S_{10}&\equiv 8q_1\pmod{16},\ S_{11}\equiv 4+8q_1\pmod{16}.
\end{aligned}\tag{4}$$

The inverse Hadamard transform gives

$$\begin{aligned} 4A_0 &= S_{00} + S_{01} + S_{10} + S_{11}, \\ 4A_1 &= S_{00} - S_{01} + S_{10} - S_{11}, \\ 4A_2 &= S_{00} + S_{01} - S_{10} - S_{11}, \\ 4A_3 &= S_{00} - S_{01} - S_{10} + S_{11}. \end{aligned} \tag{5}$$

Then using (4),

$$4A_0 \equiv 8,\ 4A_1 \equiv 8,\ 4A_2 \equiv 0,\ 4A_3 \equiv 0 \pmod{16}.$$

Therefore,

$$A_0, A_1 \equiv 2 \pmod 4,\ A_2, A_3 \equiv 0 \pmod 4. \tag{6}$$

Furthermore, since $|W_g(\omega)| \leq 36$ for any $\omega \in \mathbb{F}_2^{10}$, we have

$$\max_{i,j \in \{0,1\}} |S_{ij}| \leq 36. \tag{7}$$

Let $E(u) = \sum_{i=0}^{3} A_i(u)^2$. By (3), (4) and (7),

$$4E(u) = \sum_{i,j} S_{ij}(u)^2 \leq 4640 - 448(q_0 + q_1),$$

since residues $0, 8, 4, 12$ modulo 16 allow magnitudes at most $32, 24, 36, 36$, respectively. This gives Table 1; each bound is attained under the stated local constraints by choosing these endpoints.

Table 1: Maximum local energy under the residue and peak constraints

q_0	q_1	$\max E(u)$
0	0	1160
0	1	1048
1	0	1048
1	1	936

Put $k = wt(Q)$. Summing Table 1 and applying Parseval gives only $262144 \leq 296960 - 112k$, or $k \leq 310$, which does not exclude the rank-eight weights $240, 256, 272$. We therefore retain the signs of S_{01} and S_{11}. Put

$t_j = (-1)^{q_j} S_{j1}$ and

$$C = \sum_{u,j} t_j(u),$$
$$D = \sum_{u,j} \big(1024 - 448 q_j(u) - S_{j0}(u)^2\big),$$
$$F = \sum_{u,j} (36 - t_j(u))(t_j(u) + 28).$$

The residue bounds give $D \geq 0$, and $t_j \in \{-28, -12, 4, 20, 36\}$ gives $F \geq 0$.

Lemma 3. *If Q has polar rank $2r$, then*

$$D \geq 1024, \qquad C = 1024 + 56k + \frac{D+F}{8} \leq 1024 \cdot 2^r. \tag{8}$$

Proof. Balance gives $S_{00}(0) = q_0(0) = 0$, hence $D \geq 1024$. Expanding $D+F$ and using $\sum_{u,i,j} S_{ij}(u)^2 = 1024^2$ gives the identity for C.

Write $\chi_i = (-1)^{g_i}$, $V_j = (\chi_{2j} - \chi_{2j+1})/2$, and $V(x,j) = V_j(x)$. Let $\sigma(u,j) = (-1)^{Q(u,j)}$ on $\mathbb{F}_2^9$. The block identity gives $S_{j1} = 2(H_9 V)(\cdot, j)$. By self-adjointness and $|V| \leq 1$,

$$C = 2\langle V, H_9\sigma\rangle \leq 2\|H_9\sigma\|_1 = 1024 \cdot 2^r,$$

where the last equality follows from Lemma 1. □

4 Proof of Theorem 1

It remains to prove that no balanced ten-variable function has nonlinearity 494. By the standard Walsh-distance formula, such a function would have Walsh peak 36. By Parseval, the four blocks satisfy

$$\sum_u E(u) = \sum_{i=0}^{3} \sum_u A_i(u)^2 = 4 \cdot 2^{16} = 262144. \tag{9}$$

We exclude every possible polar rank of Q.

4.1 Case I: $\mathrm{rank}(Q) \geq 4$

For ranks four and six, Lemmas 1 and 3 give $11904 \leq C \leq 4096$ and $13696 \leq C \leq 8192$, respectively, both impossible.

4.1.1 Rank eight: a common support bound

For rank eight, $k \in \{240, 256, 272\}$. Choose the radical as the ninth frequency direction, so that

$$Q(u, j) = p(u) \oplus \lambda j, \qquad p(0) = 0,$$

where p has polar rank eight. Apply the corresponding invertible linear change to the first nine input variables and form the four blocks in these coordinates. The Walsh frequencies are only reindexed, so k, C, D, F and the identities above are unchanged. Write $\chi_i = (-1)^{g_i}$ for these blocks and set

$$U(x, j) = \frac{\chi_{2j}(x) + \chi_{2j+1}(x)}{2}, \qquad V(x, j) = \frac{\chi_{2j}(x) - \chi_{2j+1}(x)}{2}.$$

Then U, V take values in $\{-1, 0, 1\}$, $U^2 + V^2 = 1$, and, by (3), $S_{\eta 0}(u) = 2H_9U(u, \eta)$, $S_{\eta 1}(u) = 2H_9V(u, \eta)$. Put

$$s = |\operatorname{supp}(U)|, \qquad z = |\operatorname{supp}(U(\cdot, 0))|.$$

Balance gives $\sum_{x,j} U(x, j) = 0$, so s is even. Parseval gives

$$\sum_{u,\eta} S_{\eta 0}(u)^2 = 4 \sum_{\xi \in \mathbb{F}_2^9} (H_9U(\xi))^2 = 4 \cdot 2^9 \sum_{\xi} U(\xi)^2 = 2048s.$$

By the definition of D and (8), using $k \geq 240$ and $D \geq 1024$, we obtain

$$s = 256 - \frac{7k}{32} - \frac{D}{2048} \leq 203, \qquad C = 256(260 - s) + \frac{F}{8} \geq 256(260 - s). \quad (10)$$

Since $q_1 = q_0 \oplus \lambda$, the signed terms satisfy

$$\begin{aligned} \sum_u t_0 t_1 &= (-1)^\lambda \sum_u S_{01} S_{11} \\ &= (-1)^\lambda 4 \sum_u \big((H_8V(\cdot, 0))^2 - (H_8V(\cdot, 1))^2 \big) \\ &= (-1)^\lambda 2^{10} \big((256 - z) - (256 - (s - z)) \big) \\ &= (-1)^\lambda 1024(s - 2z). \end{aligned}$$

Also $\sum_{u,j} t_j = C$ and $t_j \leq 36$, so

$$0 \leq \sum_u (36 - t_0)(36 - t_1) = 256 \cdot 36^2 - 36C + \sum_u t_0 t_1.$$

Since $0 \le z \le s$, it follows that

$$36C \le 256 \cdot 36^2 + (-1)^\lambda 1024(s - 2z) \le 256 \cdot 36^2 + 1024s. \tag{11}$$

Together with (10), this gives $36(260 - s) \le 1296 + 4s$, or $s \ge 1008/5$. Since s is even and $s \le 203$ by (10), we must have $s = 202$.

4.1.2 The cases $k = 256, 272$

For $k = 256, 272$, the first identity in (10) gives $s \le 199, 196$, respectively. Both contradict $s = 202$.

4.1.3 The case $k = 240$

Here $\lambda = 0$, since $\lambda = 1$ would make Q balanced. With $s = 202$, inequalities (10) and (11) read

$$2088 \le \frac{9C}{64} \le 2104 - 8z,$$

so $z \le 2$ and $232 \le C/64 < 234$.

Since $q_0 = q_1 = p$, equation (5) gives $4H_8U(\cdot, 0) = S_{00} + S_{10} \equiv 0 \pmod{16}$. Every Walsh coefficient of this slice is therefore divisible by four. Since $U(x, 0) \in \{-1, 0, 1\}$, each coefficient has absolute value at most $\sum_x |U(x, 0)| = z \le 2$, and hence vanishes. Walsh inversion gives $U(\cdot, 0) = 0$, so $z = 0$ and $V(\cdot, 0) = \chi_0$.

Set $\epsilon = H_8((-1)^p)/16$. Lemma 1 and Walsh inversion give $\epsilon \in \{\pm 1\}^{256}$ and $H_8\epsilon = 16(-1)^p$. Since $p(0) = 0$, the last identity yields $\sum_x \epsilon(x) = H_8\epsilon(0) = 16$; hence ϵ has exactly 120 negative entries. From (4)–(5), $A_0(0) \equiv 2 \pmod 4$. As $A_0(0) = \sum_x \chi_0(x) = 256 - 2\,\mathrm{wt}(g_0)$, g_0 has odd weight, whereas ϵ has 120 negative entries. Thus χ_0 and ϵ disagree at an odd number of points. Transformation in the radical coordinate gives

$$H_9((-1)^Q)(x, j) = \begin{cases} 32\epsilon(x), & j = \lambda, \\ 0, & j \ne \lambda. \end{cases}$$

By self-adjointness and $S_{j1} = 2H_9V(\cdot, j)$,

$$C = 2\sum_{x,j} V(x, j)H_9((-1)^Q)(x, j) = 64\sum_x V(x, \lambda)\epsilon(x).$$

Since $\lambda = 0$ and $z = 0$, $C/64 = \sum_x \chi_0(x)\epsilon(x) \equiv 2 \pmod 4$. But the energy inequalities give $232 \le C/64 < 234$, an interval containing no integer congruent to 2 modulo 4. This contradiction completes Case I.

4.2 Case II: $\mathrm{rank}(Q) = 2$

Lemma 1 gives $k \in \{128, 256, 384\}$. By Lemma 3,

$$8320 = 1152 + 56 \cdot 128 \leq C \leq 2048,$$

a contradiction in all three weight cases.

4.3 Case III: $\mathrm{rank}(Q) = 0$

If $\mathrm{rank}(Q) = 0$, then Q is linear and $k \in \{0, 256\}$. By Lemma 3,

$$1152 \leq C = 1024 + 56k + \frac{D+F}{8} \leq 1024,$$

a contradiction.

Every possible rank of Q has been excluded, so nonlinearity 494 is impossible. Since the nonlinearity of a balanced ten-variable function is even and at most 494, it is at most 492. Together with the known examples in [7], this proves Theorem 1.

5 Conclusions

In this paper, we proved that the maximum nonlinearity of balanced Boolean functions in 10 variables is 492. A similar analysis for more than 10 variables may deduce more interesting results. We leave this for future work.

References

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

[2] C. Carlet, M. Djurasevic, D. Jakobovic, L. Mariot and S. Picek, "Evolving constructions for balanced, highly nonlinear boolean functions," *GECCO*, 2022, pp. 1147–1155.

[3] C. Carlet and S. Mesnager, "Four decades of research on bent functions," *Designs, Codes and Cryptography*, 78:1 (2016), 5–50.

[4] T. W. Cusick and P. Stanica, "Cryptographic Boolean Functions and Applications," Academic Press, 2017.

[5] M. Djurasevic, D. Jakobovic, L. Mariot and S. Picek, "A survey of metaheuristic algorithms for the design of cryptographic Boolean functions," *Cryptography and Communications*, 15 (2023), 1171–1197.

[6] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Fast Software Encryption*, Lecture Notes in Computer Science, vol. 1008, pp. 61–74, Springer, 1995. doi: 10.1007/3-540-60590-8_5.

[7] S. Kavut, S. Maitra, and M. D. Yücel, "Search for Boolean Functions With Excellent Profiles in the Rotation Symmetric Class," *IEEE Transactions on Information Theory*, vol. 53, no. 5, pp. 1743–1751, 2007. doi: 10.1109/TIT.2007.894696.

[8] O. A. Logachev, A. A. Salnikov and V. V. Yashchenko, "Boolean Functions in Coding Theory and Cryptography," American Mathematical Society, 2012.

[9] S. Maitra, B. Mandal and M. Roy, "Modifying Bent Functions to Obtain the Balanced Ones with High Nonlinearity," in *Progress in Cryptology – INDOCRYPT 2022*, Lecture Notes in Computer Science, vol. 13774, pp. 449–470, Springer, 2022. doi: 10.1007/978-3-031-22912-1_20.

[10] S. Picek, R. Santana and D. Jakobovic, "Maximal nonlinearity in balanced boolean functions with even number of inputs, revisited," *2016 IEEE Congress on Evolutionary Computation*, 2016, pp. 3222–3229.

[11] O. S. Rothaus, "On bent functions," *Journal of Combinatorial Theory, Series A*, 20:3 (1976), 300–305.