Maximum Nonlinearity of Symmetric Boolean Functions on Odd Number of Variables

Subhamoy Maitra and Palash Sarkar

***Abstract*—In this correspondence, we establish that for odd n, the maximum nonlinearity achievable by an n-variable symmetric Boolean function is $2^{n-1} - 2^{\frac{n-1}{2}}$ and characterize the set of functions which achieve this value of nonlinearity. In particular, we show that for each odd $n \geq 3$, there are exactly four possible symmetric Boolean functions achieving the nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$.**

***Index Terms*—Algebraic normal form, nonlinearity, symmetric Boolean function.**

I. Introduction

An interesting subclass of Boolean functions is the set of symmetric functions, where the output of the function depends only on the weight of the input vector. Another combinatorially important class of Boolean functions is the set of bent functions introduced by Rothaus [6]. An n-variable bent function achieves the maximum possible nonlinearity among all n-variable functions. Further, by its very definition [6], a bent function can exist only if n is even.

An n-variable symmetric Boolean function f can be represented by a bit array of length $n+1$, denoted by $re(f)[0, \ldots, n]$ and defined in the following manner:

$$re(f)[i] = f(X_1, \ldots, X_n) \tag{1}$$

where the weight of $X_1, \ldots, X_n$ is i for $0 \leq i \leq n$.

Let $n \geq 3$ be odd and f be an n-variable symmetric Boolean function. In this correspondence we show the following.

1) The maximum possible nonlinearity of f is $2^{n-1} - 2^{\frac{n-1}{2}}$.
2) The following are equivalent.
   a) The nonlinearity of f is equal to $2^{n-1} - 2^{\frac{n-1}{2}}$.
   b) $re(f)$ is a contiguous $(n+1)$ length substring of $(0011)^*$.
   c) The Walsh transform for f is three-valued and takes the values $0, \pm 2^{\frac{n+1}{2}}$.
   d) f is a quadratic function, i.e., the algebraic degree of f is 2.
3) A consequence of either 2b) or 2d) is that there are exactly four possible functions f which achieve the nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$.

For even n, the set of symmetric bent functions has been completely characterized in [7]. The characterization is very similar to the case for odd n. More precisely, the characterization for even n can be simply obtained on replacing $2^{\frac{n-1}{2}}$ by $2^{\frac{n-2}{2}}$ in the above, with the added restriction that for bent functions, the Walsh transform is two valued ($\pm 2^{\frac{n}{2}}$).

Manuscript received August 17, 2000; revised March 25, 2002.

S. Maitra is with the Computer and Statistical Service Center, Indian Statistical Institute, Calcutta, Pin 700 108, India (e-mail: subho@isical.ac.in).

P. Sarkar is with the Applied Statistics Unit, Indian Statistical Institute, Calcutta, Pin 700 108, India (e-mail: palash@isical.ac.in).

Communicated by A. M. Klapper, Associate Editor for Sequences.

Publisher Item Identifier 10.1109/TIT.2002.801482.

II. Preliminaries

The set of all n-variable Boolean functions will be denoted by Ω_n. An n-variable Boolean function f is a map $f: \{0,1\}^n \to \{0,1\}$. One representation of f is as a binary string of length 2^n.

For $n \geq 1$, let T_n be a $2^n \times n$ matrix defined as follows:

$$T_n = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \qquad \text{for } n = 1$$
$$T_n = \begin{bmatrix} 0 & \\ \vdots & T_{n-1} \\ 0 & \\ 1 & \\ \vdots & T_{n-1} \\ 1 & \end{bmatrix}, \qquad \text{for } n > 1. \tag{2}$$

For $0 \leq i \leq 2^n - 1$, let u_i denote the ith row of T_n. The truth table for an n-variable Boolean function f, denoted by $T_n(f)$ is defined to be the following matrix:

$$T_n(f) = \begin{bmatrix} & f(u_0) \\ & f(u_1) \\ T_n & \vdots \\ & f(u_{2^n-1}) \end{bmatrix}. \tag{3}$$

Thus, the function f can be uniquely represented by the following binary string of length 2^n:

$$f(u_0), f(u_1), \ldots, f(u_{2^n-1}).$$

By f^c (respectively, f^r) we denote the function obtained by bitwise complementing (respectively, reversing) the 2^n length binary string representing f. The truth table representation for Boolean function described earlier is conventionally used by electrical and electronics engineers (see, for example, [4]).

Given two n-variable functions f_0, f_1, by $F = f_0 f_1$ we will denote the $(n+1)$ variable function whose truth table is defined in the following manner:

$$T_{n+1}(F) = \begin{bmatrix} T_n(f_0) \\ T_n(f_1) \end{bmatrix}. \tag{4}$$

Thus, the string representation of F is simply formed by concatenating the string representations of f_0 and f_1.

Definitions (2), (3), and equation (4) suggest that the "new" variable X_{n+1} for the $(n+1)$-variable function F is "placed to the left" of the old variables $X_n, \ldots, X_1$. For this reason, we find it more intuitive to use the notation $F(X_{n+1}, X_n, \ldots, X_1)$ instead of the more common notation $F(X_1, \ldots, X_n, X_{n+1})$. However, this is really a minor point and the actual choice of notation depends on the way one feels comfortable in thinking about Boolean functions.

Another important representation of a Boolean function is by a unique multivariate polynomial over GF(2). More precisely, $f(X_n, \ldots, X_1)$ can be uniquely written as

$$f(X_n, \ldots, X_1) = a_0 \oplus \left(\bigoplus_{i=1}^{i=n} a_i X_i \right) \oplus \left(\bigoplus_{1 \leq i < j \leq n} a_{ij} X_i X_j \right) \oplus \cdots \oplus a_{12\cdots n} X_1 X_2 \ldots X_n$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\cdots n} \in \{0,1\}$. This representation of f is called the algebraic normal form (ANF) of f. The number

of variables in the highest degree monomial with a nonzero coefficient is called the algebraic degree, or simply degree of f. The ANF of the function F defined in (4) is as follows:

$$F(X_{n+1}, X_n, \ldots, X_1) = (1 \oplus X_{n+1}) f_0(X_n, \ldots, X_1) \oplus X_{n+1} f_1(X_n, \ldots, X_1).$$

Functions of degree at most one are called affine functions. The nonlinearity of an n-variable function f, denoted by $nl(f)$, is defined as

$$nl(f) = \min_{g \in L(n)} (d(f, g))$$

where $L(n)$ is the set of all n-variable affine functions and $d(f, g)$ is the Hamming distance between the two strings f, g of length 2^n. Also, by $\mathrm{wt}\,(s)$ we denote the weight (number of ones) of the binary string s.

Let $\overline{X} = (X_n, \ldots, X_1)$, $\overline{\omega} = (\omega_n, \ldots, \omega_1) \in \{0, 1\}^n$, and $\langle \overline{X}, \overline{\omega} \rangle = X_n \omega_n \oplus \cdots \oplus X_1 \omega_1$. Let $f(\overline{X})$ be a Boolean function on n variables. The Walsh transform of $f(\overline{X})$ is a real-valued function over $\{0, 1\}^n$ and is defined as (see [3], [1])

$$W_f(\overline{\omega}) = \sum_{\overline{X} \in \{0,1\}^n} (-1)^{f(\overline{X}) \oplus \langle \overline{X}, \overline{\omega} \rangle}.$$

Let f, g be two n-variable functions. By $wd(f, g)$ we denote the number of places f and g are equal minus the number of places they are unequal, i.e., $wd(f, g) = 2^n - 2d(f, g)$. The quantity $W_f(\overline{\omega})$ is related to $wd(\cdot)$ by the following relation: $W_f(\overline{\omega}) = wd(f, l_{\overline{\omega}})$, where $l_{\overline{\omega}}$ is the linear function defined as $l_{\overline{\omega}}(\overline{X}) = \langle \overline{X}, \overline{\omega} \rangle$.

The set of all n-variable symmetric Boolean functions will be denoted by A_n. Recall from (1) that an n-variable symmetric function can be represented by a binary string of length $(n+1)$ and is denoted by $re(f)$. Similarly, given a binary string g of length $(n+1)$, we define the extension of g, denoted by $ex(g)$, to be a symmetric function f of length 2^n as

$$f(X_n, \ldots, X_1) = g[wt(X_n, \ldots, X_1)].$$

The maps $re(f)$ and $ex(g)$ are one-to-one correspondences between n-variable symmetric Boolean functions and binary strings of length $(n+1)$.

The notation $(0011)^*$ denotes the one way infinite string

$$001100110011\cdots$$

formed by repeatedly concatenating the string 0011.

III. Maximum Nonlinearity for Odd n

One standard way to achieve highly nonlinear functions on odd number variables is to concatenate two bent functions. The nonlinearity obtained by this process is $2^{n-1} - 2^{\frac{n-1}{2}}$. We show that for symmetric functions on odd number of variables, this is the maximum nonlinearity achievable and further characterize the set of functions which achieve this nonlinearity. Our proof is in two parts. In the first part, we prove that the maximum nonlinearity is $\leq 2^{n-1} - 2^{\frac{n-1}{2}}$ and in the second part we characterize the functions achieving this nonlinearity. To prove the first part we require some preliminary results.

Proposition 1: Let $f_1, f_2 \in \Omega_{n-1}$ and $F = f_1 f_2$. If $nl(F) = 2^{n-1} - \epsilon$ for some ϵ in $0 < \epsilon < 2^{n-2}$, then both $nl(f_1), nl(f_2) \geq 2^{n-2} - \epsilon$. Moreover, if $f_1 = f_2$, then $nl(f_1) = nl(f_2) = 2^{n-2} - \frac{\epsilon}{2}$.

Proof: Since $nl(F) = 2^{n-1} - \epsilon$, it follows that for any λ in $L(n)$, we have

$$2^{n-1} - \epsilon \leq d(F, \lambda) \leq 2^{n-1} + \epsilon. \tag{5}$$

We prove

$$2^{n-2} - \epsilon \leq d(f_1, l) \leq 2^{n-2} + \epsilon$$

for any $l \in L(n-1)$. The proof is by contradiction. There are two cases to consider.

Case 1: Let, if possible

$$d(f_1, l) = 2^{n-2} - \epsilon - t < 2^{n-2} - \epsilon$$

for some $t > 0$. Since $ll \in L(n)$, from (5)

$$2^{n-1} - \epsilon \leq d(f_1 f_2, ll) = d(f_1, l) + d(f_2, l) \leq 2^{n-1} + \epsilon. \tag{6}$$

Using $d(f_1, l) = 2^{n-2} - \epsilon - t$, we get $2^{n-2} + t \leq d(f_2, l)$. Now, $d(f_1, l^c) = 2^{n-2} + \epsilon + t$. Also $d(f_1 f_2, l^c l) = d(f_1, l^c) + d(f_2, l)$, and hence we get

$$2^{n-1} + \epsilon + 2t \leq d(f_1 f_2, l^c l) = d(F, l^c l).$$

Since $l^c l \in L(n)$, this contradicts (5). Thus, $d(f_1, l) \geq 2^{n-2} - \epsilon$.

Case 2: Again assume, if possible

$$d(f_1, l) = 2^{n-2} + \epsilon + t > 2^{n-2} + \epsilon$$

for some $t > 0$. The function $F^c = f_1^c f_2^c$ has nonlinearity $2^{n-1} - \epsilon$ and $d(f_1^c, l) = 2^{n-2} - \epsilon - t$. This is not possible by Case 1. Thus, $d(f_1, l) \leq 2^{n-2} + \epsilon$.

Hence we get $nl(f_1) \geq 2^{n-2} - \epsilon$. To see the last statement, note that if $f_1 = f_2$, then $nl(F) = 2nl(f_1)$. □

We state the following simple result which will prove to be useful later.

Lemma 1: Let $f \in A_n$ with $re(f) = a_0 a_1 \cdots a_{n-1} a_n$ and f be written as $f = f_0 f_1 f_2 f_3$ where each $f_i \in A_{n-2}$. Then

a) $re(f_0 f_1) = a_0 \cdots a_{n-1}$ b) $re(f_2 f_3) = a_1 \cdots a_n$
c) $re(f_0) = a_0 \cdots a_{n-2}$ d) $re(f_1) = re(f_2) = a_1 \cdots a_{n-1}$.
e) $re(f_3) = a_2 \cdots a_n$.

Proof: First note that it is enough to prove a) and b). Let $g_0 = f_0 f_1$ and $g_1 = f_2 f_3$. The functions g_0 and g_1 are obtained from f as follows:

$$g_0(X_{n-1}, \ldots, X_1) = f(X_n = 0, X_{n-1}, \ldots, X_1)$$
$$g_1(X_{n-1}, \ldots, X_1) = f(X_n = 1, X_{n-1}, \ldots, X_1).$$

From the definition of $re()$ it is clear that for $0 \leq i \leq n-1$, we have $re(f)[i] = 1$ iff $re(g_0)[i] = 1$ and for $1 \leq i \leq n$, we have $re(f)[i] = 1$ iff $re(g_1)[i-1] = 1$. From this we get a) and b), respectively. □

The following result establishes the maximum possible nonlinearity for symmetric functions.

Theorem 1: Let n be odd and $F \in A_n$. Then

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

Proof: The proof is by induction on odd n.

The induction base is $n = 1$. For $n = 1$, there are four Boolean functions and all of them are affine. Hence, the nonlinearity of any function on one variable is 0 and, thus, the statement of the result is satisfied for $n = 1$.

Assume the result holds for some odd $n-2$, i.e., the maximum possible nonlinearity of $(n-2)$-variable symmetric functions is $2^{n-3} - 2^{\frac{n-3}{2}}$. We claim that this forces the maximum possible nonlinearity for n-variable symmetric functions to be $2^{n-1} - 2^{\frac{n-1}{2}}$. This claim is proved by contradiction. Suppose the claim is false and there exists a function F in A_n such that $nl(F) > 2^{n-1} - 2^{\frac{n-1}{2}}$. We write $F = f_0 f_1 f_2 f_3$, where each f_i is in A_{n-2}. From Lemma 1 d), we have

$re(f_1) = re(f_2)$ and hence $f_1 = f_2$. Thus, F is of the form f_0fff_3, where

$$\begin{aligned} f_0(X_{n-2}, \ldots, X_1) &= F(0, 0, X_{n-2}, \ldots, X_1) \\ f(X_{n-2}, \ldots, X_1) &= F(0, 1, X_{n-2}, \ldots, X_1) \\ &= F(1, 0, X_{n-2}, \ldots, X_1) \\ f_3(X_{n-2}, \ldots, X_1) &= F(1, 1, X_{n-2}, \ldots, X_1). \end{aligned}$$

Define

$$\begin{aligned} &G(X_n, X_{n-1}, X_{n-2}, \ldots, X_1) \\ &\quad = F(X_n \oplus X_{n-1}, 1 \oplus X_{n-1}, X_{n-2}, \ldots, X_1). \end{aligned}$$

Clearly, G can be obtained from F by an affine transformation of the variables and hence F and G have the same nonlinearity. Write $G = g_0g_1$, where g_0, g_1 are $n-1$ variable functions. Then

$$\begin{aligned} g_0(X_{n-1}, \ldots, X_1) &= G(0, X_{n-1}, \ldots, X_1) \\ &= F(X_{n-1}, 1 \oplus X_{n-1}, X_{n-2}, \ldots, X_1), \\ g_1(X_{n-1}, \ldots, X_1) &= G(1, X_{n-1}, \ldots, X_1) \\ &= F(1 \oplus X_{n-1}, 1 \oplus X_{n-1}, X_{n-2}, \ldots, X_1). \end{aligned}$$

Further

$$\begin{aligned} g_0(0, X_{n-2}, \ldots, X_1) &= F(0, 1, X_{n-2}, \ldots, X_1) \\ &= f(X_{n-2}, \ldots, X_1) \\ &= F(1, 0, X_{n-2}, \ldots, X_1) \\ &= g_0(1, X_{n-2}, \ldots, X_1) \\ g_1(0, X_{n-2}, \ldots, X_1) &= F(1, 1, X_{n-2}, \ldots, X_1) \\ &= f_3(X_{n-2}, \ldots, X_1), \\ g_1(1, X_{n-2}, \ldots, X_1) &= F(0, 0, X_{n-2}, \ldots, X_1) \\ &= f_0(X_{n-2}, \ldots, X_1). \end{aligned}$$

Therefore, $g_0 = ff$ and $g_1 = f_3f_0$.

Using Proposition 1, we get

$$nl(ff) = nl(g_0) > 2^{n-2} - 2^{\frac{n-1}{2}}.$$

Since $nl(ff) = 2nl(f)$, we have $nl(f) > 2^{n-3} - 2^{\frac{n-3}{2}}$. This contradicts the induction hypothesis. □

For an odd number of variables, the first characterization of functions achieving maximum nonlinearity is described in the following result.

Theorem 2: Let $n \geq 3$ be odd and $F \in A_n$. Then the following are equivalent.

1) $nl(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$.
2) $re(F)$ is a contiguous $n+1$ length substring of $(1100)^*$.
3) The Walsh transform of F is three valued and takes the values $0, \pm 2^{\frac{n+1}{2}}$.

A consequence of 2) is that there are exactly four possible functions in A_n achieving the nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$.

Proof: The proof of 3) ⇒1) is obvious. The proof of 2) ⇒1) is also easy and can be seen by the following argument. Let $re(F) = a_0 \cdots a_n$. We write F as $F = f_1f_2$, where $f_1, f_2 \in A_{n-1}$ and by Lemma 1 a) and b), $re(f_1) = a_0 \cdots a_{n-1}$, $re(f_2) = a_1 \cdots a_n$. Then $re(f_1), re(f_2)$ are both contiguous length-n substrings of $(0011)^*$. Using the characterization in [7], it follows that both f_1 and f_2 are bent. Hence, both f_1 and f_2 have nonlinearity $2^{n-2} - 2^{\frac{n-3}{2}}$. Since F is formed by concatenating f_1 and f_2, the nonlinearity of F is $2^{n-1} - 2^{\frac{n-1}{2}}$.

We now prove 1) ⇒2) and 3). Since $F \in A_n$, we can write F as $F = f_0fff_3$, where f_0, f, f_3 are symmetric functions of $n-2$ variables. We show by induction on odd $n \geq 3$, that F is a contiguous $n+1$ length substring of $(1100)^*$ and also the Walsh transform W_F of F takes only the three distinct values: $0, \pm 2^{\frac{n+1}{2}}$.

We first show that

$$nl(f) = 2^{n-3} - 2^{\frac{n-3}{2}}.$$

Since $nl(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$, using an argument similar to the proof of Theorem 1, we have

$$nl(ff) \geq 2^{n-2} - 2^{\frac{n-1}{2}}.$$

However, $nl(ff) = 2nl(f)$ and so $nl(f) \geq 2^{n-3} - 2^{\frac{n-3}{2}}$. Also, using Theorem 1, the maximum possible nonlinearity for a $(n-2)$-variable symmetric function is $2^{n-3} - 2^{\frac{n-3}{2}}$ and so $nl(f) = 2^{n-3} - 2^{\frac{n-3}{2}}$.

By the induction hypothesis we can assume that $re(f)$ is a contiguous $n-1$ length substring of $(1100)^*$ and the Walsh transform values of f are $0, \pm 2^{\frac{n-1}{2}}$. Thus, the possible forms of $re(f)$ are

1) $g_1 = 001100\cdots$,
2) $g_2 = 110011\cdots$,
3) $g_3 = 01100\cdots$,
4) $g_4 = 10011\cdots$.

Let $G = re(F) = xgy$, for some $x, y \in \{0, 1\}$. Using Lemma 1, we get that g must be one of g_1, g_2, g_3, g_4. We now show that the following must hold:

A) If $g = g_1$, then $x = 1$ and $y = b$,
B) If $g = g_2$, then $x = 0$ and $y = 1 - b$,
C) If $g = g_3$, then $x = 0$ and $y = b$,
D) If $g = g_4$, then $x = 1$ and $y = 1 - b$,

where $b = \frac{(n-1) \bmod 4}{2}$.

Note that it is sufficient to show A) and C). This is because $g_2 = g_1^c$ and $g_4 = g_3^c$ and $ex(xhy)$ and $ex(x^ch^cy^c)$ have the same nonlinearity for any $n-1$ length bit string h. Here, we prove only A), the proof of C) being similar. We have to prove that the other combinations of x and y result in lower nonlinearities. If x and y have the values given in the conditions then it is easy to check that G is an $n+1$-length contiguous substring of $(1100)^*$ and hence achieve the required nonlinearity.

Now we turn to the proof of A). We only prove for the condition $n-1 \equiv 0 \bmod 4$, the case $n-1 \equiv 2 \bmod 4$ being similar. Since $n-1 \equiv 0 \bmod 4$, we have

$$re(F) = x00110011\cdots0011y.$$

Let $s_0 = re(f_0)$, $s_3 = re(f_3)$ and $t = re(f)$. Therefore,

$$\begin{aligned} t &= 00110011\cdots0011 \\ s_0 &= x00110011\cdots001 \\ s_3 &= 0110011\cdots0011y. \end{aligned}$$

Let $s = 100110011\cdots11001$ (of length $n-1$) and l be a linear function such that $wd(ex(s), l) = a$. We now rule out the three possible options except the case $x = 1$, $y = 0$. In the rest of the proof, by $\#(\Phi)$ we denote the number of times a Boolean event Φ is true.

Case 1: $x = y = 0$: Let $\#(ex(s) = l) = a_1$ and $\#(ex(s) \neq l) = a_2$. Then $a = a_1 - a_2$.

Now $\#(ex(s_0) = l) = a_1 + 1$ and $\#(ex(s_0) \neq l) = a_2 - 1$ and so

$$wd(f_0, l) = wd(ex(s_0), l) = a + 2.$$

Also,

$$wd(f_2, l) = wd(ex(s_3), l) = -a$$

since $s_3 = s^c$ when $y = 0$. By the induction hypothesis, the Walsh transform values of f are $0, \pm 2^{\frac{n-1}{2}}$. Let l be such that $wd(f, l) = 2^{\frac{n-1}{2}}$. Then

$$wd(F, llll) = wd(f_0, l) + 2wd(f, l) + wd(f_3, l) = 2 + 2^{\frac{n+1}{2}}.$$

Hence

$$d(F, llll) = 2^{n-1} - 2^{\frac{n-1}{2}} - 1 < 2^{n-1} - 2^{\frac{n-1}{2}}$$

which contradicts $nl(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$.

Case 2: $x = 0, y = 1$: In this case $s_3 = (s_0)^{rc}$. Let l be a nondegenerate linear function on an odd number of variables and hence $l^r = l^c$. Then

$$wd(f_3, l) = wd(f_0^{rc}, l) = wd(f_0, l^{rc}) = wd(f_0, l) = b$$

(say). Since there are exactly 2^{n-3} linear functions such that $l^r = l^c$, it cannot be the case that $wd(f, l) = 0$ for all such functions as otherwise this would violate Parseval's theorem. So, we can choose l such that $wd(f, l) = \pm 2^{\frac{n-1}{2}}$. Now two cases arise

i) $wd(f, l) = 2^{\frac{n-1}{2}}$. If $b > 0$, then consider

$$wd(F, llll) = 2^{\frac{n+1}{2}} + 2b$$

and if $b < 0$, then consider

$$wd(F, l^c lll^c) = 2^{\frac{n+1}{2}} + 2b.$$

ii) $wd(f, l) = -2^{\frac{n-1}{2}}$. If $b > 0$, then consider

$$wd(F, l^c lll^c) = -2^{\frac{n+1}{2}} - 2b$$

and if $b < 0$, then consider

$$wd(F, llll) = -2^{\frac{n+1}{2}} - 2b.$$

Therefore either

$$d(F, llll) < 2^{n-1} - 2^{\frac{n-1}{2}}$$

or

$$d(F, l^c lll^c) < 2^{n-1} - 2^{\frac{n-1}{2}}$$

and so

$$nl(F) < 2^{n-1} - 2^{\frac{n-1}{2}}$$

which is a contradiction.

Case 3: $x = y = 1$: In this case $wd(f_0, l) = a$ and $wd(f_0^c, l) = -a$. Let l be such that the last bit of l is 0, i.e., nondegenerate on an even number of variables and hence $l^r = l$. Then $wd(f_3, l) = -a - 2$. Now combining the techniques of the above two cases we can show that $nl(F) < 2^{n-1} - 2^{\frac{n-1}{2}}$, which is a contradiction.

We now complete the induction step for the Walsh transform of F. We show that W_F is three valued and takes the values $0, \pm 2^{\frac{n+1}{2}}$. We have proved that $re(F)$ is a contiguous $(n+1)$ length substring of $(0011)^*$. Using Lemma 1, it is not difficult to see that this forces $re(f_0)$ and $re(f_3)$ to be bitwise complements of each other. Hence $f_0 = f_3^c$.

Let $l \in L_n$. Then l is one of the forms

$$l_1 l_1 l_1 l_1,\ l_1 l_1^c l_1 l_1^c,\ l_1 l_1 l_1^c l_1^c,\ l_1 l_1^c l_1^c l_1$$

for some $l_1 \in L_{n-2}$. Since $f_0 = f_3^c$ we have

$$wd(f_0, l_1) = -wd(f_3, l_1).$$

Since $F = f_0 f f f_3$, we have

$$wd(F, l) = 2wd(f_0, l_1) \quad \text{or} \quad 2wd(f, l_1). \tag{7}$$

Since $re(F)$ is a contiguous $(n+1)$-length substring of $(0011)^*$, both $re(f_0)$ and $re(f)$ are contiguous $(n-1)$-length substrings of $(0011)^*$. Hence by the induction hypothesis, the Walsh transforms of both f_0 and f are three-valued and take the values $0, \pm 2^{\frac{n-1}{2}}$. Now using (7) we complete the induction step for the Walsh transform of F. □

From Theorem 2, we get a characterization of the class of symmetric functions with maximum nonlinearity for odd number of input variables. It is well known [1] that in a symmetric Boolean function either all the kth-order terms are present or all are absent at the same time. Thus, the algebraic normal form of a symmetric Boolean function f can also be represented by an $n+1$-length bit vector $ra(f)$ (the reduced algebraic normal form of f), where $ra(f)[k] \in \{0, 1\}$ and $ra(f)[k] = 0$ (respectively, 1) means that all the kth-order terms are absent (respectively, present). For $f \in A_n$, the following result relates the vectors $re(f)$ and $ra(f)$.

Theorem 3: For $f \in A_n$, let us consider $g = re(f)$ and $q = ra(f)$. Then

$$g[i] = \left(\sum_{k=0}^{i} q[k] \binom{i}{k} \right) \pmod 2,$$

where $0 \le i \le n$ and $0 \le k \le i$.

Proof: Since all vectors of the same weight have the same output value it is sufficient to consider an arbitrary input vector of weight i, for $0 \le i \le n$. We now compute the output value corresponding to such a vector. All terms in the ANF having terms of length greater than i must necessarily evaluate to 0. Now consider terms of length k with $0 \le k \le i$, and $q[k] = 1$. Then, exactly $\binom{i}{k}$ number of k-length terms (out of the total $\binom{n}{k}$ number of k-length terms in the ANF) will evaluate to 1. From this the proof follows. □

This expression provides an algorithm to generate either g from q or q from g. If q is known, it is easy to get g from direct calculation. However, if g is known, then q needs to be generated recursively. That is, for calculating $q[k]$, all the values of $q[0], \ldots, q[k-1]$ need to be calculated. As example, if g is known, then $g[0] = q[0]$. For the next step

$$g[1] = \sum_{k=0}^{1} q[k] \binom{1}{k} \pmod 2 = q[0] + q[1] \bmod 2$$

and since $g[1], q[0]$ are known, $q[1]$ can be calculated. In this manner, all the bits of q can be calculated. Now we provide the algebraic normal form of the symmetric functions on odd number of variables with maximum nonlinearity. We show that the algebraic degree of the symmetric functions in Theorem 2 is 2 irrespective of the number of input variables.

Theorem 4: Let $F \in A_n$ for odd $n \ge 3$. Then the following are equivalent.

1) $re(F)$ is a contiguous $(n+1)$ length substring of $(0011)^*$.
2) The ANF of F is given by

$$F(X_1, \ldots, X_n) = \left(\bigoplus_{1 \le i < j \le n} X_i X_j \right) \oplus b \left(\bigoplus_{i=1}^{n} X_i \right) \oplus c$$

where, $b, c \in \{0, 1\}$.

Proof: Let $g = re(F)$ and $q = ra(F)$. We first note that it is sufficient to prove that $g = 0011 \cdots$ is a contiguous $(n+1)$ length substring of $(0011)^*$ iff $q[2] = 1$ and $q[i] = 0$ for $0 \le i \le n$ and $i \ne 2$. The reason for this is the following. The four possible contiguous $(n+1)$-length substrings of $(0011)^*$ are g, g^r, g^c, and g^{rc}. The functions corresponding to these strings are $F = ex(g)$, $F^r = ex(g^r)$, $F^c = ex(g^c)$, and $F^{rc} = ex(g^{rc})$. Since

$$F^r(X_n, \ldots, X_1) = F(1 \oplus X_n, \ldots, 1 \oplus X_1)$$

the functions F, F^r, F^c, and F^{rc} all have the same degree. This shows the claimed sufficiency. We now turn to proving that $g = 0011\cdots$ is a contiguous $(n+1)$-length substring of $(0011)^*$ iff $q[2] = 1$ and $q[i] = 0$ for $0 \le i \le n$ and $i \ne 2$.

First assume that $q[2] = 1$ and $q[i] = 0$ for $0 \le i \le n$ and $i \ne 2$. From Theorem 3, we have $g[0] = 0$, $g[1] = 0$, $g[2] = \binom{2}{2} \bmod 2 = 1$ and $g[3] = \binom{3}{2} \bmod 2 = 1$. Further, for $i \ge 4$, we have

$$\begin{aligned} g[i] &= \binom{i}{2} \bmod 2 \qquad = \frac{i(i-1)}{2} \bmod 2 \\ &= 0, \qquad \text{if } i \equiv 0, 1 \bmod 4 \\ &= 1, \qquad \text{if } i \equiv 2, 3 \bmod 4. \end{aligned}$$

For the converse, assume that $g = 0011\cdots$ is an $(n+1)$ length substring of $(0011)^*$. Using Theorem 3, it is easy to verify that $q[0] = q[1] = q[3] = 0$ and $q[2] = 1$. We now show by induction on k that for $k \ge 3$, $q[k] = 0$. The base for the induction is clearly $k = 3$ and is easy to see as mentioned before. The inductive step reduces to showing

$$q[4j] = q[4j+1] = q[4j+2] = q[4j+3] = 0, \qquad \text{for all } j \ge 1.$$

We have $g[4i] = g[4i+1] = 0$ and $g[4i+2] = g[4i+3] = 1$ for $i \ge 1$. Using Theorem 3 and the induction hypothesis, we have

$$\begin{aligned} g[4j] = 0 &= \left(\sum_{k=0}^{4j} q[k] \binom{4j}{k} \right) \bmod 2 \\ &= \left(\binom{4j}{2} q[2] + q[4j] \right) \bmod 2. \end{aligned}$$

Since $\binom{4j}{2} \bmod 2 = 0$ and $g[4j] = 0$, we have $q[4j] = 0$. Similarly, it can be shown that $q[4j+1] = 0$. The proofs that $q[4j+2]$, $q[4j+3]$ are zero are similar and we only show $q[4j+2] = 0$. Again, using Theorem 3 and the induction hypothesis we have

$$\begin{aligned} g[4j+2] = 0 &= \left(\sum_{k=0}^{4j+2} q[k] \binom{4j+2}{k} \right) \bmod 2 \\ &= \left(\binom{4j+2}{2} q[2] + q[4j+2] \right) \bmod 2. \end{aligned}$$

Since $\binom{4j+2}{2} \bmod 2 = 1$ and $q[2] = g[4j+2] = 1$, we have $q[4j+2] = 0$. Thus, we get that $q[i] = 0$ for $0 \le i \le n$, $i \ne 2$ and $q[2] = 1$. Thus, F is of the form $(\bigoplus_{1 \le i < j \le n} X_i X_j)$. □

Combining Theorems 2 and 4 we obtain the following characterization of symmetric functions on odd number of variables attaining the maximum possible nonlinearity.

Theorem 5: Let $n \ge 3$ be odd and f be an n-variable symmetric Boolean function. The following are equivalent.

1) The nonlinearity of f is equal to $2^{n-1} - 2^{\frac{n-1}{2}}$.
2) $re(f)$ is a contiguous $(n+1)$ length substring of $(0011)^*$.
3) The Walsh transform for f is three valued and takes the values $0, \pm 2 \times 2^{\frac{n-1}{2}}$.
4) f is a quadratic function, i.e., the algebraic degree of f is 2.

An important property of Boolean functions is its propagation characteristics defined as follows. An n-variable Boolean function f is said to satisfy $PC(k)$ if $f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})$ is balanced for all $1 \le \mathrm{wt}(\overline{\alpha}) \le k$.

Theorem 6: For n odd, there exists balanced $F \in A_n$ with nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$ satisfying $PC(n-1)$.

Proof: For $n = 4m+1$ consider the $4m+2$-length string $g = 0(1100)^m 1$ and let $F = ex(g)$. Then F is of the form ff^{rc} where f is a symmetric bent function on $4m$ variables. Thus, F is balanced. Similarly, for $n = 4m+3$ consider the $4m+4$ length string $g = 00(1100)^m 11$ and let $F = ex(g)$. Then also F is of the form ff^{rc} where f is a symmetric bent function on $4m+2$ variables. Thus, F is balanced. The nonlinearity is equal to the nonlinearity achieved by the concatenation of two bent functions.

The function f is a symmetric bent function. It is well known [3] that bent functions of $(n-1)$ variables satisfy $PC(n-1)$. Since F is of the form ff^{rc}, it satisfies propagation characteristics with respect to all the n-bit vectors except the all one vector. □

ACKNOWLEDGMENT

The authors are grateful to Prof. Cunsheng Ding for providing several comments on an initial draft of this correspondence. An anonymous referee pointed out reference [7]. Also detailed comments from the anonymous referees significantly improved the technical quality and presentation of the correspondence.

REFERENCES

[1] C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, vol. 561.
[2] X. Hou, "On the norm and covering radius of the first-order Reed–Muller codes," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1025–1027, May 1997.
[3] F. J. MacWillams and N. J. A. Sloane, *The Theory of Error Correcting Codes* Amsterdam, The Netherlands, 1977.
[4] M. M. Mano, *Logic and Computer Design Fundamentals*, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 1999.
[5] N. J. Patterson and D. H. Wiedemann, "Correction to—the covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276," *IEEE Trans. Inform. Theory*, vol. 36, p. 443, Mar. 1990.
[6] O. S. Rothaus, "On bent functions," *J. Comb. Theory*, ser. A, vol. 20, pp. 300–305, 1976.
[7] P. Savicky, "On the bent Boolean functions that are symmetric," *Europ. J. Comb.*, vol. 15, pp. 407–410, 1994.