Minimum Distance between Bent and 1-resilient Boolean Functions

Soumen Maity
Management of Information Systems
Indian Institute of Management Calcutta
Diamond Harbour Road, Joka
Pin 700 104, INDIA
E-mail: soumenmaity@yahoo.co.in

Subhamoy Maitra
Applied Statistics Unit
Indian Statistical Institute
203 B. T. Road, Calcutta
Pin 700 108, INDIA
E-mail: subho@isical.ac.in

Abstract

In this paper we present a lower bound of the minimum distance between the set of bent functions and the set of 1-resilient Boolean functions. Further we present a strategy to modify bent functions in getting a large class of 1-resilient functions with very good nonlinearity and autocorrelation. In particular, the technique is applied upto 10-variable functions and we show that the construction provides a large class of 1-resilient functions achieving currently best known nonlinearity and autocorrelation.

Keywords: Boolean Function, Resiliency, Nonlinearity, Autocorrelation.

1 Introduction

Construction of resilient Boolean functions with very good parameters in terms of nonlinearity, algebraic degree and other cryptographic parameters has received lot of attention in literature [15, 16, 18, 19, 7, 21, 2, 3]. A recent construction method [11] of highly nonlinear 1-resilient functions presents modification of some output points of a bent function to construct highly nonlinear 1-resilient function. A natural question that arises in this context is "at least how many bits in the output of a bent function need to be changed to construct an 1-resilient Boolean function". The answer of this question gives the minimum distance between the set of bent functions and the set of 1-resilient functions. We here try to answer this question and show that the minimum distance for n-variable functions is

$$dBR_n(1) \geq 2^{\frac{n}{2}-1} + 2\left\lceil \frac{(r+1)(2^{\frac{n}{2}-1} - \sum_{i=0}^{r}\binom{n}{i}) + \sum_{i=1}^{r} i\binom{n}{i}}{n-r-1} \right\rceil$$

where r is the smallest integer such that both the conditions

$$\sum_{i=0}^{r}\binom{n}{i} \leq \frac{dBR_n(1)}{2} + 2^{\frac{n}{2}-2} < \sum_{i=0}^{r+1}\binom{n}{i} \text{ and } dBR_n(1) \geq 2^{\frac{n}{2}-1}$$

are satisfied. We also show that this result is tight for $n \leq 10$. The immediate corollary is the construction of 1-resilient Boolean functions with nonlinearity $\geq 2^{n-1} - 2^{\frac{n}{2}-1} - dBR_n(1)$ and maximum absolute value of autocorrelation spectra $\leq 4\, dBR_n(1)$. However, it is possible to get 1-resilient functions with better nonlinearity and autocorrelation than the bound. In particular, we concentrate on construction of 8 and 10-variable 1-resilient Boolean functions with best known nonlinearity and autocorrelation. *Note that throughout the paper we consider n is even.*

The bent functions chosen in [11, Section 3] use the concept of perfect nonlinear functions and one example function each for 8 and 10 variables were presented. However, it is not clear how a generalized construction of such bent functions can be achieved in that manner. We here identify a large subclass of Maiorana-McFarland type bent functions which can be modified to get 1-resilient functions with currently best known parameters. It should also be noted that the example functions presented in [11] are basically Maiorana-McFarland type, even though they are designed in a different manner by using perfect nonlinear functions.

1.1 Preliminaries

A Boolean function on n variables may be viewed as a mapping from $\{0,1\}^n$ into $\{0,1\}$. A Boolean function $f(x_1,\ldots,x_n)$ is also interpreted as the output column of its *truth table* f, i.e., a binary string of length 2^n, $f = [f(0,0,\cdots,0), f(1,0,\cdots,0), f(0,1,\cdots,0), \ldots, f(1,1,\cdots,1)]$.

The *Hamming distance* between two binary strings S_1, S_2 is denoted by $d(S_1,S_2)$, i.e., $d(S_1,S_2) = \#(S_1 \neq S_2)$. Also the *Hamming weight* or simply the weight of a binary string S is the number of ones in S. This is denoted by $wt(S)$. An n-variable function f is said to be *balanced* if its output column in the truth table contains equal number of 0's and 1's (i.e., $wt(f) = 2^{n-1}$).

Denote addition operator over $GF(2)$ by $\oplus$. An n-variable Boolean function $f(x_1,\ldots,x_n)$ can be considered to be a multivariate polynomial over $GF(2)$. This polynomial can be expressed as a sum of products representation of all distinct k-th order products ($0 \leq k \leq n$) of the variables. More precisely, $f(x_1,\ldots,x_n)$ can be written as

$$a_0 \oplus \bigoplus_{1\leq i\leq n} a_i x_i \oplus \bigoplus_{1\leq i<j\leq n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \{0,1\}$. This representation of f is called the *algebraic normal form* (ANF) of f. The number of variables in the highest order product term with nonzero coefficient is called the *algebraic degree*, or simply the degree of f and denoted by $deg(f)$.

Functions of degree at most one are called *affine* functions. An affine function with constant term equal to zero is called a *linear* function. The set of all n-variable affine (respectively linear) functions is denoted by $A(n)$ (respectively $L(n)$). The nonlinearity of an n-variable function f is

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

i.e., the distance from the set of all n-variable affine functions.

Let $x = (x_1,\ldots,x_n)$ and $\omega = (\omega_1,\ldots,\omega_n)$ both belong to $\{0,1\}^n$ and

$$x \cdot \omega = x_1\omega_1 \oplus \ldots \oplus x_n\omega_n.$$

Let $f(x)$ be a Boolean function on n variables. Then the *Walsh transform* of $f(x)$ is a real valued function over $\{0,1\}^n$ which is defined as

$$W_f(\omega) = \sum_{x\in\{0,1\}^n} (-1)^{f(x)\oplus x\cdot\omega}.$$

In terms of Walsh spectra, the nonlinearity of f is given by

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \{0,1\}^n} |W_f(\omega)|.$$

For n-even, the maximum nonlinearity of a Boolean function can be $2^{n-1} - 2^{\frac{n}{2}-1}$ and the functions possessing this nonlinearity are called bent functions [14]. Further, for a bent function f on n variables, $W_f(\omega) = \pm 2^{\frac{n}{2}}$ for all ω.

In [8], an important characterization of correlation immune and resilient functions has been presented, which we use as the definition here. A function $f(x_1, \ldots, x_n)$ is m-resilient (respectively m-th order correlation immune) iff its Walsh transform satisfies

$$W_f(\omega) = 0, \text{ for } 0 \leq wt(\omega) \leq m \text{ (respectively } W_f(\omega) = 0, \text{ for } 1 \leq wt(\omega) \leq m).$$

As the notation used in [15, 16], by an (n, m, d, σ) function we denote an n-variable, m-resilient function with degree d and nonlinearity σ.

We will now define *restricted Walsh transform* which will be frequently used in this text. The *restricted Walsh transform* of $f(x)$ on a subset S of $\{0,1\}^n$ is a real valued function over $\{0,1\}^n$ which is defined as

$$W_f(\omega)|_S = \sum_{x \in S} (-1)^{f(x) \oplus x \cdot \omega}.$$

Now we present the following technical result.

Proposition 1 *Let $S \subset \{0,1\}^n$ and $b(x), f(x)$ be two n-variable Boolean functions such that $f(x) = 1 \oplus b(x)$ when $x \in S$ and $f(x) = b(x)$ otherwise. Then $W_f(\omega) = W_b(\omega) - 2W_b(\omega)|_S$.*

Proof : Take $\omega \in \{0,1\}^n$. Now

$$\begin{array}{rcl}
W_f(\omega) & = & \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus \omega \cdot x} \\
& = & \sum_{x \in \{0,1\}^n - S} (-1)^{f(x) \oplus \omega \cdot x} + \sum_{x \in S} (-1)^{f(x) \oplus \omega \cdot x} \\
& = & \sum_{x \in \{0,1\}^n - S} (-1)^{b(x) \oplus \omega \cdot x} - \sum_{x \in S} (-1)^{b(x) \oplus \omega \cdot x} \\
& & \qquad \text{(since } f, b \text{ are same for the inputs } \notin S \\
& & \qquad \text{and complement when the inputs } \in S) \\
& = & \sum_{x \in \{0,1\}^n - S} (-1)^{b(x) \oplus \omega \cdot x} + \sum_{x \in S} (-1)^{b(x) \oplus \omega \cdot x} - 2 \sum_{x \in S} (-1)^{b(x) \oplus \omega \cdot x} \\
& = & \sum_{x \in \{0,1\}^n} (-1)^{b(x) \oplus \omega \cdot x} - 2 \sum_{x \in S} (-1)^{b(x) \oplus \omega \cdot x} \\
& = & W_b(\omega) - 2W_b(\omega)|_S.
\end{array}$$

■

Propagation Characteristics (PC) and Strict Avalanche Criteria (SAC) [13] are important properties of Boolean functions to be used in S-boxes. Further, Zhang and Zheng [22] identified related cryptographic measures called Global Avalanche Characteristics (GAC).

Let $\alpha \in \{0,1\}^n$ and f be an n-variable Boolean function. Define the autocorrelation value of f with respect to the vector α as

$$\Delta_f(\alpha) = \sum_{x \in \{0,1\}^n} (-1)^{f(x) \oplus f(x \oplus \alpha)}, \text{ and the absolute indicator } \Delta_f = \max_{\alpha \in \{0,1\}^n, \alpha \neq \bar{0}} |\Delta_f(\alpha)|.$$

A function is said to satisfy PC(k), if $\Delta_f(\alpha) = 0$ for $1 \leq wt(\alpha) \leq k$. Note that, for a bent function f on n variables, $\Delta_f(\alpha) = 0$ for all nonzero α, i.e., $\Delta_f = 0$.

Analysis of autocorrelation properties of correlation immune and resilient Boolean functions has gained substantial interest recently as evident from [20, 23, 10, 4]. In [10, 4], it has been identified that some well known construction of resilient Boolean functions are not good in terms of autocorrelation properties. Since the present construction is modification of bent functions which possess the best possible autocorrelation properties, we get very good autocorrelation properties of the 1-resilient functions. We present a bound on the Δ_f value of the 1-resilient functions and further achieve best known autocorrelation values for the cases $n = 8, 10$.

2 The Distance

Initially we start with a simple technical result.

Proposition 2 *$dBR_n(1) \geq 2^{\frac{n}{2}-1}$.*

Proof : For a bent function b on n variables, $W_b(\omega) = \pm 2^{\frac{n}{2}}$. Hence the distance between a balanced function and a bent function is exactly $2^{\frac{n}{2}-1}$. The 1-resilient functions are balanced by definition and hence the result. ■

Now we present a restricted result. Let $b(x)$ be an n-variable bent function with $W_b(\omega) = +2^{\frac{n}{2}}$ for $wt(\omega) \leq 1$. We denote by $M(n, 1)$ the minimum number of bits to be modified in the output column of $b(x)$ to construct an n variable 1-resilient function from $b(x)$.

Theorem 1 *Let $b(x)$ be an n-variable bent function with $W_b(\omega) = 2^{\frac{n}{2}}$ for $0 \leq wt(\omega) \leq 1$. Then*

$$M(n, 1) \geq 2^{\frac{n}{2}-1} + 2\left\lceil \frac{(r+1)(2^{\frac{n}{2}-1} - \sum_{i=0}^{r} \binom{n}{i}) + \sum_{i=1}^{r} i\binom{n}{i}}{n - r - 1} \right\rceil$$

where r is the smallest integer such that both the conditions

$$\sum_{i=0}^{r} \binom{n}{i} \leq \frac{M(n,1)}{2} + 2^{\frac{n}{2}-2} < \sum_{i=0}^{r+1} \binom{n}{i} \text{ and } M(n,1) \geq 2^{\frac{n}{2}-1}$$

are satisfied.

Proof : Let $S \subset \{0, 1\}^n$ and $f(x)$ be an n-variable Boolean function obtained by modifying the $b(x)$ values for $x \in S$ and keeping the other bits unchanged. Then from Proposition 1, $W_f(\omega) = W_b(\omega) - 2W_b(\omega)|_S \ \forall \omega$, and in particular, $W_f(\omega) = 2^{\frac{n}{2}} - 2W_b(\omega)|_S$ for $0 \leq wt(\omega) \leq 1$.

It is known that, f is 1-resilient iff $W_f(\omega) = 0$ for $0 \leq wt(\omega) \leq 1$, i.e., iff $W_b(\omega)|_S = 2^{\frac{n}{2}-1}$ for $0 \leq wt(\omega) \leq 1$. Thus, our problem is to minimize $|S| = k$ with the constraint $W_b(\omega)|_S = 2^{\frac{n}{2}-1}$ for $0 \leq wt(\omega) \leq 1$.

Given $S = \{x^{i_1}, x^{i_2}, \ldots, x^{i_k}\} \subset \{0, 1\}^n$, consider the matrices

$$\mathbf{S}^{k \times n} = (x^{i_1}, x^{i_2}, \ldots, x^{i_k})^T, \ b(\mathbf{S})^{k \times 1} = (b(x^{i_1}), b(x^{i_2}), \ldots, b(x^{i_k}))^T,$$

$$\text{and } (\mathbf{S} \oplus b(\mathbf{S}))^{k \times n} = (x^{i_1} \oplus b(x^{i_1}), x^{i_2} \oplus b(x^{i_2}), \ldots, x^{i_k} \oplus b(x^{i_k}))^T.$$

By A^T we mean transpose of a matrix A. Also by abuse of notation, $x^{i_j} \oplus b(x^{i_j})$ means the GF(2) addition (XOR) of the bit $b(x^{i_j})$ with each of the bits of x^{i_j}.

Now $W_b(\omega)|_S = 2^{\frac{n}{2}-1}$ for $0 \leq wt(\omega) \leq 1$ implies that there are exactly $\frac{k}{2} - 2^{\frac{n}{2}-2}$ many 1's in $b(\mathbf{S})$ and in each column of $\mathbf{S} \oplus b(\mathbf{S})$. Since all the rows of $\mathbf{S}$ are distinct and further $b(\mathbf{S})$ contains $\frac{k}{2} + 2^{\frac{n}{2}-2}$ many 0's, $\mathbf{S} \oplus b(\mathbf{S})$ should contain at least $\frac{k}{2} + 2^{\frac{n}{2}-2}$ distinct rows.

Thus, our problem is to find a $k \times n$ binary matrix $\mathbf{S} \oplus b(\mathbf{S})$ with minimum number of rows k such that each column contains $\frac{k}{2} - 2^{\frac{n}{2}-2}$ number of 1's and there are at least $\frac{k}{2} + 2^{\frac{n}{2}-2}$ distinct rows.

Note that, in each column, the difference between the number of 0's and 1's is $2^{\frac{n}{2}-1}$. This implies that the number of distinct rows $\frac{k}{2} + 2^{\frac{n}{2}-2}$ in the matrix $\mathbf{S} \oplus b(\mathbf{S})$ is $\geq 2^{\frac{n}{2}-1}$.

For a fixed n, if k is minimized then $\frac{k}{2} - 2^{\frac{n}{2}-2}$ (the number of 1's in each column) will also be minimized. For this, the $\frac{k}{2} + 2^{\frac{n}{2}-2}$ distinct rows in the matrix $\mathbf{S} \oplus b(\mathbf{S})$ should be of lowest possible weights. Getting the rows with lowest possible weights imply that the rows are in ascending order of weights $0, 1, 2, \ldots$.

(*It should be noted that this arguement is only to find out the minimum number of rows, which in turn will provide the calculation of* $dBR_n(1)$. *However, in case of actual construction it may not be possible to choose the rows in this manner due to the constraint that the number of 1's in each column has to be* $\frac{k}{2} - 2^{\frac{n}{2}-2}$ *and there are at least* $\frac{k}{2} + 2^{\frac{n}{2}-2}$ *distinct rows. See Remark 1 for more details.*)

Let r be the largest integer such that

$$\sum_{i=0}^{r} \binom{n}{i} \leq \frac{k}{2} + 2^{\frac{n}{2}-2} < \sum_{i=0}^{r+1} \binom{n}{i}.$$

This means that $\sum_{i=0}^{r} \binom{n}{i}$ rows are filled up by vectors of weight upto r and the rest $\frac{k}{2} + 2^{\frac{n}{2}-1} - \sum_{i=0}^{r} \binom{n}{i}$ rows are filled up with vectors of weight $r+1$. Also since there are n columns and each column contains exactly $\frac{k}{2} - 2^{\frac{n}{2}-2}$ many 1's, the total number of 1's in the matrix $\mathbf{S} \oplus f(\mathbf{S})$ is $n \times (\frac{k}{2} - 2^{\frac{n}{2}-2})$. The number of 1's in the $\frac{k}{2} + 2^{\frac{n}{2}-2}$ distinct rows is $\sum_{i=1}^{r} i\binom{n}{i} + (r+1)(\frac{k}{2} + 2^{\frac{n}{2}-2} - \sum_{i=0}^{r} \binom{n}{i})$ which must be less than or equal to the total number of 1's in the matrix $\mathbf{S} \oplus b(\mathbf{S})$. Hence,

$$\sum_{i=1}^{r} i\binom{n}{i} + (r+1)(\frac{k}{2} + 2^{\frac{n}{2}-2} - \sum_{i=0}^{r} \binom{n}{i}) \leq n \times (\frac{k}{2} - 2^{\frac{n}{2}-2}).$$

This gives,

$$k \geq 2\left\lceil \frac{(n+r+1)2^{\frac{n}{2}-2} + \sum_{i=1}^{r} i\binom{n}{i} - (r+1)\sum_{i=0}^{r} \binom{n}{i}}{n-r-1} \right\rceil.$$

■

Theorem 2 *Let $b(x)$ be any n variable bent function. Then*

$$dBR_n(1) \geq 2^{\frac{n}{2}-1} + 2\left\lceil \frac{(r+1)(2^{\frac{n}{2}-1} - \sum_{i=0}^{r} \binom{n}{i}) + \sum_{i=1}^{r} i\binom{n}{i}}{n-r-1} \right\rceil$$

where r is the smallest integer such that both the conditions

$$\sum_{i=0}^{r} \binom{n}{i} \leq \frac{dBR_n(1)}{2} + 2^{\frac{n}{2}-2} < \sum_{i=0}^{r+1} \binom{n}{i} \text{ and } dBR_n(1) \geq 2^{\frac{n}{2}-1}$$

are satisfied.

Proof : Without loss of generality, assume that $W_b(\omega) = +2^{\frac{n}{2}}$ for $wt(\omega) = 0$. Let $G_1 = \{\omega | wt(\omega) = 1, W_b(\omega) = +2^{\frac{n}{2}}\}$ and $G_2 = \{\omega | wt(\omega) = 1, W_b(\omega) = -2^{\frac{n}{2}}\}$. Let $S \subset \{0,1\}^n$ and $f(x)$ be an n-variable Boolean function obtained by modifying the $b(x)$ values for $x \in S$ and keeping the other bits unchanged. Then from Proposition 1, $W_f(\omega) = W_b(\omega) - 2W_b(\omega)|_S \, \forall \omega$, and in particular, $W_f(\omega) = 2^{\frac{n}{2}} - 2W_b(\omega)|_S$ for $wt(\omega) = 0, \omega \in G_1$ and $W_f(\omega) = -2^{\frac{n}{2}} - 2W_b(\omega)|_S$ for $\omega \in G_2$.

Given f is 1-resilient, we need to minimize $|S| = k$ with the constraints $W_b(\omega)|_S = 2^{\frac{n}{2}-1}$ for $wt(\omega) = 0$ and $\omega \in G_1$ and $W_b(\omega)|_S = -2^{\frac{n}{2}-1}$ for $\omega \in G_2$.

Let $|G_1| = \lambda$. Using the same argument as in the proof of Theorem 1, our problem is to find a $k \times n$ binary matrix $\mathbf{S} \oplus b(\mathbf{S})$ with minimum number of rows k such that there are λ columns with exactly $\frac{k}{2} - 2^{\frac{n}{2}-2}$ many 1's in each column and exactly $\frac{k}{2} + 2^{\frac{n}{2}-2}$ many 1's in each of the remaining $n - \lambda$ columns. Further, there are at least $\frac{k}{2} + 2^{\frac{n}{2}-2}$ distinct rows.

Let $M_1^{k \times \lambda}$ (respectively $M_2^{k \times n - \lambda}$) be a binary matrix with exactly $\frac{k}{2} - 2^{\frac{n}{2}-2}$ (respectively $\frac{k}{2} + 2^{\frac{n}{2}-2}$) many 1's in each column. Let J be the $k \times (n - \pi)$ matrix with all elements 1. Then the problem of finding a binary matrix $(M_1 : M_2)$ with minimum number of rows k such that there are at least $\frac{k}{2} + 2^{\frac{n}{2}-2}$ distinct rows is equivalent to find a binary matrix $(M_1 : J - M_2)$ with minimum number of rows k such that there are at least $\frac{k}{2} + 2^{\frac{n}{2}-2}$ distinct rows. Note that each column of $(M_1 : J - M_2)$ contains exactly $\frac{k}{2} - 2^{\frac{n}{2}-2}$ many 1's. Thus, the proof of the present theorem is similar to that of Theorem 1. ■

It is important to note that the expression of $dBR_1(n)$ contains the integer r, where the value of r is in turn restricted in some region depending on $dBR_1(n)$. Now we present an algorithm to find out the exact value of $dBR_1(n)$.

Algorithm calculateDistance

1. initialDistance $= 2^{\frac{n}{2}-1}$
2. Find smallest r such that $\sum_{i=0}^{r} \binom{n}{i} \leq \frac{\text{initialDistance}}{2} + 2^{\frac{n}{2}-2} < \sum_{i=0}^{r+1} \binom{n}{i}$ is satisfied.
3. newDistance $= 2 \left\lceil \frac{(n+r+1)2^{\frac{n}{2}-2} + \sum_{i=1}^{r} i\binom{n}{i} - (r+1)\sum_{i=0}^{r}\binom{n}{i}}{n-r-1} \right\rceil$
4. if $\sum_{i=0}^{r} \binom{n}{i} \leq \frac{\text{newDistance}}{2} + 2^{\frac{n}{2}-2} < \sum_{i=0}^{r+1} \binom{n}{i}$ is satisfied then output r, newDistance and terminate.
5. $r = r + 1$. Goto item 3.

End Algorithm

We discuss the algorithm for the cases $n = 8, 10$. For $n = 8$, initialDistance $= 8$. Thus r becomes 0. With $r = 0$, we get newDistance $= 10$ and the right hand side of the inequality in item 4 of the algorithm is not satisfied since $9 \not< 9$. Thus we update r to 1 and then also we find newDistance $= 10$ and the right hand side of the inequality in item 4 of the algorithm is then satisfied. For $n = 10$, the algorithm terminates in the first run and we get newDistance $= 22$.

With this algorithm, for $8 \leq n \leq 14$, it can be checked that $r = 1$. Thus we have the following result.

Corollary 1 *For even n, $8 \leq n \leq 14$, $dBR_n(1) = 2^{\frac{n}{2}-1} + 2\left\lceil \frac{2^{\frac{n}{2}} - n - 2}{n-2} \right\rceil$.*

Assume that one can construct a bent function b on n variables such that $dBR_n(1)$ bits at the output column of b are changed to get an n-variable 1-resilient function f. It is clear that toggling of a single bit can reduce the nonlinearity at most by 1 and increase the maximum absolute value of the autocorrelation spectra (absolute indicator) by at most 4. Thus we have the following result.

Theorem 3 $nl(f) \geq 2^{n-1} - 2^{\frac{n}{2}-1} - dBR_n(1)$ *and* $\Delta_f \leq 4\, dBR_n(1)$.

Proof : The proof follows from $nl(f) \geq nl(b) - dBR_n(1)$ and $\Delta_f \leq \Delta_b + 4\, dBR_n(1)$, where b is a bent function. ■

However, for the actual constructions of functions on 8, 10 variables, we will show that we get better nonlinearity and autocorrelation values than the bounds.

Remark 1 *We are not interested in the case $n = 2$, since there is no nonlinear 2-variable 1-resilient functions. We now consider the cases for $n = 4, 6$. Using the Algorithm* **calculateDistance** *we get that $r = 0$ for these two cases and then we arrive at $dBR_4(1) \geq 4$ and $dBR_6(1) \geq 6$. We have also checked that this bound is tight since we can construct 4-variable (respectively 6-variable) 1-resilient function by changing 4 (respectively 6) output points of 4-variable (respectively 6-variable) bent function. As we have commented in the proof of Theorem 1 (related to the actual construction instead of the lower bound), the rows chosen in the matrix $\mathbf{S} \oplus b(\mathbf{S})$ may not include the all zero row.*

For the 4-variable case, we have to take the rows of $\mathbf{S} \oplus b(\mathbf{S})$ as $\{0001, 0010, 0100, 1000\}$ due to the constraint that the number of 1's in each column has to be 1 and there are at least 3 distinct rows. Thus, take a bent function with truth table 0000011001010011 *and toggle the function at the inputs $\{(0,0,0,1), (0,0,1,0), (1,0,0,0), (1,0,1,1)\}$. Then we get a $(4, 1, 2, 4)$ function with the truth table* 0110011011000011.

For the 6-variable case, take a bent function with truth table 0000000001011010001111000110011001101001001100110101010100001111 *and toggle the outputs at the input points $\{(0,0,0,0,0,1), (0,0,0,0,1,0), (0,0,0,1,0,0), (0,0,1,0,0,0), (1,0,0,0,0,0), (1,0,1,1,1,1)\}$. Then we get a $(6, 1, 4, 24)$ function with the truth table* 0110100011011010001111000110011011101001001100100101010100001111.

In the following two sections we consider 8 and 10 varaible cases. In those cases we need to consider the all zero point for construction unlike the cases for 4 and 6 variables.

3 The 8-variable 1-resilient Functions

In the previous section we have presented a lower bound of the minimum distance between the bent and 1-resilient functions. However, it has not been discussed in Section 2 how exactly a construction is possible. Further to achieve the currently best known parameters (or even better than that, if possible) we may need to consider some other issues. In this section we consider the construction of an $(8, 1, 6, 116)$ function. Construction of this function was an important open question and the function has been first reported in [9] by interlinking combinatorial technique and computer search. Later this function has also been found by meta heuristic search (simulated annealing) in [5]. Further the function found in [5] has $\Delta_f = 24$, which is currently the best known value. We here follow the similar kind of technique used in [11]. In the course of discussion it will be clear that how our technique is an improvement over [11]. We present a generalized construction method of $(8, 1, 6, 116)$

functions by modifying Maiorana-McFarland type bent functions and in specific cases, these functions have the Δ_f value as low as 24, the best known one [5].

Construction 1 *Take a bent function $b(x)$ on 8 variables with the following properties :* **(1)** $b(x) = 0$ *for* $wt(x) \leq 1$ *and* $b(x) = 1$ *for* $wt(x) = 8$, **(2)** $W_b(\omega) = 16$ *for* $wt(\omega) \leq 1$ *and* $W_b(\omega) = -16$ *for* $wt(\omega) = 8$. *Define a set* $S = \{x \in \{0,1\}^8 | wt(x) = 0, 1, 8\}$. *Construct a function* $f(x)$ *as :*

$$\begin{array}{rcll} f(x) & = & 1 \oplus b(x), & \textit{if } x \in S \\ & = & b(x), & \textit{otherwise.} \end{array}$$

From Corollary 1, we get that $dBR_8(1) = 10$ and we here choose exactly 10 positions and modified them. It is important to point out that we here start with bent functions with some specific properties. The reason for choosing such bent functions is to get an actual construction of 1-resilient function with very high nonlinearity.

Before presenting the theorem regarding the properties of f, let us enumerate the issues we improve here over the work presented in [11].

1. There is a gap in the proof of [11, Theorem 3]. Note the conditions imposed on the bent function b above. In the statement of [11, Theorem 3], only the conditions of item 1 has been considered and the conditions of the item 2 has not been considered as given in Construction 1. The conditions of item 2 has been implicitly assumed in the proof of [11, Theorem 3]. Fortunately, the bent function considered in [11, Section 3] satisfies the conditions of item 2. However, it should be noted that there exist bent functions which satisfy the conditions of item 1 and not all the conditions of item 2 and in that case the proof of [11, Theorem 3] does not go through.

2. The bent function chosen in [11, Section 3] uses the concept of perfect nonlinear functions and they presented one example function which satisfies the conditions of item 1 (and also conditions of item 2). However, it is not clear how a generalized construction of such bent functions can be achieved in that manner. We here identify a subclass of Maiorana-McFarland type bent functions which satisfy the conditions of both item 1 and 2. This gives a large class of $(8, 1, 6, 116)$ functions. In fact we show that there are more than $2^{46.297}$ many distinct (upto complementation) $(8, 1, 6, 116)$ functions f with $\Delta_f \leq 40$.

3. The proof of Theorem 4 below is much simpler than the proof of [11, Theorem 3] and it presents a clear picture of the Walsh spectra of the function f with respect to the spectra of the function b.

Theorem 4 *The function $f(x)$ as described in Construction 1 is an* $(8, 1, 6, 116)$ *function.*

Proof : Take $\omega \in \{0,1\}^8$ with $wt(\omega) = i$. Now

$$\begin{array}{rcl} W_f(\omega) & = & \sum_{x \in \{0,1\}^8} (-1)^{b(x) \oplus \omega \cdot x} - 2 \sum_{x \in S} (-1)^{b(x) \oplus \omega \cdot x} \text{ (from Proposition 1)} \\ & = & W_b(\omega) - 2 \ (\ 8 - 2wt(\omega) + 2(wt(\omega) \bmod 2) \ ). \end{array}$$

Now we explain how the last step is deduced. Note that $b(x) = 0$ when $wt(x) = 0$ and $b(x) = 1$, when $wt(x) = 8$. Thus,

$$\sum_{x\in\{0,1\}^8|wt(x)=0,8}(-1)^{b(x)\oplus\omega\cdot x} = 0, \text{ when } wt(\omega) \text{ is even,}$$
$$= 2, \text{ when } wt(\omega) \text{ is odd.}$$

Moreover, $\sum_{x\in\{0,1\}^8|wt(x)=1}(-1)^{b(x)\oplus\omega\cdot x} = 8 - 2wt(\omega)$, as

(i) $b(x) = 0$ when $wt(x) = 1$ and

(ii) $\omega \cdot x = 1$ at $wt(w)$ input points when $wt(x) = 1$.

Since $\sum_{x\in S}(-1)^{b(x)\oplus\omega\cdot x} = \sum_{x\in\{0,1\}^8|wt(x)=0,8}(-1)^{b(x)\oplus\omega\cdot x} + \sum_{x\in\{0,1\}^8|wt(x)=1}(-1)^{b(x)\oplus\omega\cdot x}$, we get,

$$W_f(\omega) = W_b(\omega) - 2\ (\ 8 - 2wt(\omega) + 2(wt(\omega) \bmod 2)\ ).$$

When $wt(\omega) \leq 1$, $W_f(\omega) = W_b(\omega) - 16 = 16 - 16 = 0$. Thus the function is 1-resilient.

Further, if $wt(\omega) = 8$, $W_f(\omega) = W_b(\omega) + 16 = -16 + 16 = 0$. For any other choice, i.e., for $2 \leq wt(\omega) \leq 7$, $|W_f(\omega)| \leq |W_b(\omega)| + 8 = 16 + 8 = 24$. Hence, $nl(f) = 2^{8-1} - \frac{24}{2} = 116$.

Since the function attains the maximum possible nonlinearity, the algebraic degree [1, 3] of the function must be $8 - 2 = 6$. ■

$wt(\omega)$	0	1	2	3	4	5	6	7	8
$W_f(\omega) = W_b(\omega)+$	-16	-16	-8	-8	0	0	8	8	16

Table 1: Relationship between Walsh spectra of f, g as described in Construction 1.

3.1 A Subclass of Maiorana-McFarland Bent Functions

The original Maiorana-McFarland class of bent function is as follows [6]. Consider n-variable Boolean functions on (X, Y), where $X, Y \in \{0,1\}^{\frac{n}{2}}$ of the form $f(X,Y) = X \cdot \pi(Y) + g(Y)$ where π is a permutation on $\{0,1\}^{\frac{n}{2}}$ and g is any Boolean function on $\frac{n}{2}$ variables. Note that f can be seen as concatenation of $2^{\frac{n}{2}}$ distinct (upto complementation) affine function on $\frac{n}{2}$ variables.

Once again we write what kind of bent function $b(x)$ on 8 variables we require.

1. $b(x) = 0$ for $wt(x) \leq 1$ and $b(x) = 1$ for $wt(x) = 8$,
2. $W_b(\omega) = 16$ for $wt(\omega) \leq 1$ and $W_b(\omega) = -16$ for $wt(\omega) = 8$.

Note that in this case, $n = 8$, i.e., $\frac{n}{2} = 4$. We have to decide what permutations π on $\{0,1\}^4$ and what kind of functions g on $\{0,1\}^4$ we can take such that the conditions on b are satisfied. We present a set of conditions below, which taken all together, provides sufficient condition for construction of such functions. Before going into the conditions, let us fix the notation and ordering of input variables as $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8)$, $X = (X_1, X_2, X_3, X_4)$, and $Y = (Y_1, Y_2, Y_3, Y_4)$. Further we identify $X_1 = x_1, X_2 = x_2, X_3 = x_3, X_4 = x_4, Y_1 = x_5, Y_2 = x_6, Y_3 = x_7, Y_4 = x_8$.

1. First of all note that the function b has the value 0 at the points $(0,0,0,0,0,0,0,0)$, $(1,0,0,0,0,0,0,0)$, $(0,1,0,0,0,0,0,0)$, $(0,0,1,0,0,0,0,0)$, $(0,0,0,1,0,0,0,0)$ and this condition is satisfied if we choose $\pi(0,0,0,0) = (0,0,0,0)$ and $g(0,0,0,0) = 0$.

2. Next we need that the function b should have value 0 at the points $(0,0,0,0,1,0,0,0)$, $(0,0,0,0,0,1,0,0)$, $(0,0,0,0,0,0,1,0)$, $(0,0,0,0,0,0,0,1)$, and this condition is satisfied if we choose $g(0,0,0,0)=0$ and any permutation π which maps any input of nonzero weight to another input of nonzero weight.

3. We need b to be 1 when the input is $(1,1,1,1,1,1,1,1)$. Thus if $\pi(1,1,1,1)$ is a vector of odd weight then $g(1,1,1,1)$ need to be 0. otherwise if $\pi(1,1,1,1)$ is a vector of even weight then $g(1,1,1,1)$ has to be 1.

4. Since we have already decided that $\pi(0,0,0,0)=(0,0,0,0)$ and $g(0,0,0,0)=0$, the $W_f(\omega)$ values for $\omega \in \{(0,0,0,0,1,0,0,0),\ (0,0,0,0,0,1,0,0),\ (0,0,0,0,0,0,1,0),\ (0,0,0,0,0,0,0,1)\}$ becomes $+2^{\frac{n}{2}}=16$.

5. Further if $\pi(Y) \in \{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\}$, then we take $g(Y)=0$. This guarantees that the $W_f(\omega)$ values for $\omega \in \{(1,0,0,0,0,0,0,0),\ (0,1,0,0,0,0,0,0),\ (0,0,1,0,0,0,0,0),\ (0,0,0,1,0,0,0,0)\}$ becomes $+2^{\frac{n}{2}}=16$.

6. Lastly, if $\pi(Y)=(1,1,1,1)$, then we have to fix $g(Y)=1$. This guarantees that $W_f(1,1,1,1,1,1,1,1)=-2^{\frac{n}{2}}=-16$.

Theorem 5 *Let $n=8$, $x \in \{0,1\}^n$ and $X,Y \in \{0,1\}^{\frac{n}{2}}$. Let $b(x)$ be a Maiorana-McFarland type bent function $b(x)=b(X,Y)=X\cdot\pi(Y)+g(Y)$ where π is a permutation on $\{0,1\}^{\frac{n}{2}}$ and g is a Boolean function on $\frac{n}{2}$ variables with the following conditions.*

(1) *if $Y=(0,0,0,0)$, $\pi(Y)=Y$;* **(2)** *if $wt(\pi(Y))\leq 1$, or $wt(Y)\leq 1$, then $g(Y)=0$;*

(3) *if $Y=(1,1,1,1)$, $g(Y)=(wt(\pi(Y))+1) \bmod 2$;* **(4)** *if $wt(\pi(Y))=4$, $g(Y)=1$.*

Then **(1)** *$b(x)=0$ for $wt(x)\leq 1$ and $b(x)=1$ for $wt(x)=8$,* **(2)** *$W_b(\omega)=16$ for $wt(\omega)\leq 1$ and $W_b(\omega)=-16$ for $wt(\omega)=8$.*

Further there are $\geq 2^{46.297}$ many distinct b's (upto complementation) satisfying these conditions and in turn there are $\geq 2^{46.297}$ many distinct (upto complementation) $(8,1,6,116)$ functions.

Proof : The proof of the properties of b is discussed above in detail. The count of such functions is arrived as follows. Note that there are $2^{\frac{n}{2}}=16$ places for the permutation π.

Let there are i many Y's, $0\leq i\leq 4$ such that $wt(\pi(Y))=1$ for $wt(Y)=1$. There are 4 elements of weight 1 and 10 elements of weight 2 or 3. Thus the $\pi(Y)$'s for $wt(Y)=1$ may be chosen in $\binom{4}{i}\binom{10}{4-i}$ ways. Note that $\pi(Y)$ can not be $(1,1,1,1)$ for $wt(Y)=1$. Now there are two cases.

1. Consider that $\pi(1,1,1,1)=(1,1,1,1)$. Then the number of options is $\binom{4}{i}\cdot\binom{10}{4-i}\cdot 4!\cdot 10!\cdot 2^{6+i}$. This is because the 4 elements where $wt(Y)=1$ can be permuted in 4! ways. The 4 elements where $wt(Y)=2,3$ can be permuted in 10! ways. The function $g(Y)$ is fixed when Y is $(0,0,0,0)$ (1 place, $g(Y)=0$) or $wt(Y)=1$ (4 places, $g(Y)=0$) or $wt(\pi(Y))=1$ ($4-i$ places, $g(Y)=0$) or $wt(Y)=wt(\pi(Y))=4$ (1 place, $g(Y)=1$). Thus $g(Y)$ is fixed in $10-i$ places and we can put any choice from $\{0,1\}$ for $16-(10-i)=6+i$ places.

2. Consider that $\pi(1,1,1,1) \neq (1,1,1,1)$. Then the number of options is $\binom{4}{i} \cdot \binom{10}{4-i} \cdot 10 \cdot 4! \cdot 10! \cdot 2^{5+i}$. Choose one element of $wt(Y) \neq 4$ as $\pi(1,1,1,1)$. This can be done in 10 ways. The 4 elements where $wt(Y) = 1$ can be permuted in 4! ways. The 4 elements where $wt(Y) = 2, 3$ can be permuted in 10! ways. The function $g(Y)$ is fixed when Y is $(0,0,0,0)$ (1 place, $g(Y) = 0$) or $wt(Y) = 1$ (4 places, $g(Y) = 0$) or $wt(\pi(Y)) = 1$ ($4-i$ places, $g(Y) = 0$) or $wt(Y) = 4$ (1 place, $g(Y) = 1$ if $wt(\pi(Y)) = 0$, else $g(Y) = 1$) or $wt(\pi(Y)) = 4$ (1 place, $g(Y) = 1$). Thus $g(Y)$ is fixed in $11-i$ places and we can put any choice from $\{0,1\}$ for $16-(11-i) = 5+i$ places.

So the total number of options is $6\sum_{i=0}^{4}\binom{4}{i} \cdot \binom{10}{4-i} \cdot 4! \cdot 10! \cdot 2^{6+i} = 6 \cdot 4! \cdot 10! \cdot 2^6 \sum_{i=0}^{4}\binom{4}{i} \cdot \binom{10}{4-i} \cdot 2^i =\approx 2^{46.297492}$. ∎

Remark 2 *Following Theorem 3, it is clear that for the function f as discussed in Theorem 4, $\Delta_f \leq 40$. Now we present the following specific case.*

Consider $\pi(Y) = Y$ for all $Y \in \{0,1\}^4$, $g(Y) = 0$ for all $Y \in \{0,1\}^4 \setminus \{(1,1,1,1)\}$ and $g(Y) = 1$ for $Y = (1,1,1,1)$. Let $b(x) = b(X,Y) = X \cdot \pi(Y) + g(Y)$ and $f(x)$ is as given in Construction 1. Then f is an $(8,1,6,116)$ function with $\Delta_f = 24$.

Note that we get an $(8,1,6,116)$ function f with $\Delta_f = 24$ in this method which has earlier been found by simulated annealing and linear transformation in [5].

4 The 10-variable 1-resilient Functions

We here start with 10-variable bent functions. Note that Theorem 1 and Theorem 2 do not directly provide the idea how the exact construction of an 1-resilient function from a bent function is possible. Let us now describe a method where we will be able to identify a subclass of 10-variable Maiorana-McFarland type bent functions for this purpose.

As described in Section 2, we need to modify at least $k = 22$ points (see Corollary 1). Now following Theorem 1 and Theorem 2, it is clear that we first need to select $\frac{k}{2} + 2^{\frac{n}{2}-2} = 19$ distinct points. Note that we can have 1 point of weight 0 and 10 points of weight 1. Thus we need to find out 8 more points from weight 2. Once these 19 points are selected, further there are 3 more points to be chosen.

$$
\mathbf{S} \oplus b(\mathbf{S}) = \left(\begin{array}{cccccccccc}
x_{10} & x_9 & x_8 & x_7 & x_6 & x_5 & x_4 & x_3 & x_2 & x_1 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0
\end{array}\right)
$$

Now we refer to the $\mathbf{S} \oplus b(\mathbf{S})$ matrix given here. We present the first 19 points and after the horizontal line we show the next 3 points. Note that the choice of the all zero point and the points of weight 1 are clear from the discussion in Theorem 1. However, it is still to be sorted out how exactly the 8 points of weight 2 are chosen. We here do that by observation and choose the 8 points of weight 2 out of total $\binom{10}{2} = 45$ weight 2 points. The rest 3 points (one of weight 0 and other two of weight 2) are chosen properly to satisfy that weight of each column should be $\frac{k}{2} - 2^{\frac{n}{2}-2} = 3$. Now we need a bent function b on 10 variables with the property that $b(x) = 0$ when x is any of the first 19 points and $b(x) = 1$ when x is complement of any of the last 3 points. This means that the last three rows need to be complemented when they will be considered as input points in the function. Thus, we construct two sets S_1, S_2 as follows and then denote $S = S_1 \cup S_2$.

$S_1 = \{(0,0,0,0,0,0,0,0,0,0), (0,0,0,0,0,0,0,0,0,1), (0,0,0,0,0,0,0,0,1,0),$
$(0,0,0,0,0,0,0,1,0,0), (0,0,0,0,0,0,1,0,0,0), (0,0,0,0,0,1,0,0,0,0),$
$(0,0,0,0,1,0,0,0,0,0), (0,0,0,1,0,0,0,0,0,0), (0,0,1,0,0,0,0,0,0,0),$
$(0,1,0,0,0,0,0,0,0,0), (1,0,0,0,0,0,0,0,0,0), (0,0,0,0,0,0,0,1,1,0),$
$(0,0,0,0,0,1,1,0,0,0), (0,0,0,0,0,1,0,0,0,1), (0,0,0,1,1,0,0,0,0,0),$
$(0,0,1,1,0,0,0,0,0,0), (0,1,1,0,0,0,0,0,0,0), (1,1,0,0,0,0,0,0,0,0),$
$(1,0,0,0,1,0,0,0,0,0)\}$ and

$S_2 = \{(1,1,1,1,1,1,1,1,1,1), (1,1,1,1,1,1,1,1,0,0), (1,1,1,1,1,1,0,0,1,1)\}$.

Also consider

$S_1' = \{(0,0,0,0,0,0,0,0,0,0), (0,0,0,0,0,0,0,0,0,1), (0,0,0,0,0,0,0,0,1,0), (0,0,0,0,0,0,0,1,0,0), (0,0,0,0,0,0,1,0,0,0), (0,0,0,0,0,1,0,0,0,0), (0,0,0,0,1,0,0,0,0,0), (0,0,0,1,0,0,0,0,0,0), (0,0,1,0,0,0,0,0,0,0), (0,1,0,0,0,0,0,0,0,0), (1,0,0,0,0,0,0,0,0,0), (0,0,0,0,0,0,0,1,1,0), (0,0,0,0,0,1,1,0,0,0), (0,0,0,0,0,1,0,0,0,1)\}$,

$S_3 = \{(0,0,0,0,0,0,0,1,0,1), (0,0,0,0,0,0,0,1,1,1), (0,0,0,0,0,0,1,0,0,1), (0,0,0,0,0,0,1,0,1,0), (0,0,0,0,0,0,1,1,1,0), (0,0,0,0,0,1,0,0,1,1), (0,0,0,0,1,1,1,0,0,1), (0,0,0,0,0,1,1,1,0,0), (0,0,0,0,0,1,1,1,1,1)\}$ and

$S_4 = \{(0,0,1,1,1,0,0,0,0,0), (0,1,1,1,0,0,0,0,0,0), (1,0,0,1,1,0,0,0,0,0), (0,0,0,0,0,1,1,0,0,0), (1,1,0,0,1,0,0,0,0,0), (1,1,1,0,0,0,0,0,0,0), (1,1,1,1,1,0,0,0,0,0)\}$. We will talk about these sets S_1', S_3 and S_4 little later.

We now write the exact construction.

Construction 2 *We need a 10-variable bent function $b(x)$ with the following properties:*

1. *$b(x) = 0$ when $x \in S_1$ and $b(x) = 1$ when $x \in S_2$,*
2. *$W_b(\omega) = +32$ when $\omega \in S_1' \cup S_3 \cup S_4$.*

The function $f(x)$ is as follows.

$$\begin{aligned} f(x) &= 1 \oplus b(x), && \textit{if } x \in S \\ &= b(x), && \textit{otherwise.} \end{aligned}$$

From Theorem 1, it is clear that the function $f(x)$ is 1-resilient. Now we need to calculate the nonlinearity of f. In fact, we will prove that $nl(f) = 488$, the currently best known nonlinearity for 10-variable 1-resilient functions. By Proposition 1, $W_f(\omega) = W_b(\omega) - 2W_b(\omega)|_S$. Thus, it is important to analyse the values of $W_b(\omega)|_S$ for all $\omega \in \{0,1\}^{10}$. However, this can not be done in a nice way as it has been done in the 8-variable case in Theorem 4. So we use a computer program to calculate $W_b(\omega)|_S$ for all $\omega \in \{0,1\}^{10}$. Note that when $|W_b(\omega)|_S| \leq 8$, then at those points $|W_f(\omega)| \leq 48$. Thus, we have no restriction on the Walsh spectra of the bent function b at these points to get the nonlinearity 488 for f. However, we need to concentrate on the cases when $|W_b(\omega)|_S| \geq 12$. We have checked that this happens when $\omega \in S_1' \cup S_3 \cup S_4$ and all these values are either $+12$ or $+16$. Thus as given in Construction 2, the Walsh spectra of the function b should be $+32$ at these points. Hence Constrution 2 provides 10-variable 1-resilient functions having nonlinearity 488. Using similar technique as in Theorem 5, it is possible to get the count of such functions. Due to space constraint we do not include that in this version.

Note that we have not yet discussed the algebraic degree and autocorrelation properties of the functions. We now consider a specific case and check the algebraic degree and autocorrelation property.

Take $x = (x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10})$, $X = (X_1, X_2, X_3, X_4, X_5)$, and $Y = (Y_1, Y_2, Y_3, Y_4, Y_5)$. Further we identify $X_1 = x_1, X_2 = x_2, X_3 = x_3, X_4 = x_4, X_5 = x_5, Y_1 = x_6, Y_2 = x_7, Y_3 = x_8, Y_4 = x_9, Y_5 = x_{10}$.

Consider a 10-variable Maiorana-McFarland type bent function $b(x) = b(X, Y) = X \cdot \pi(Y) + g(Y)$ where π is a permutation on $\{0,1\}^5$ with $\pi(Y) = Y$ and g is any Boolean function on 5 variables which is a constant 0 function. It can be checked that this bent function satisfies the conditions required in Construction 2. Then we prepare f as given in Construction 2. We checked that nonlinearity of f is 488, algebraic degree is 8 and $\Delta_f = 48$. Now it is important to note the following two points.

1. The construction in [11, Theorem 4] required 26 points to be modified to get 1-resilient function from a bent function. We here need only 22 points to modify. Further, we have checked that the Δ_f value of the function constructed in [11] is 64. The function we construct here has $\Delta_f = 48$ and this is the best known value which is achieved for the first time here.

2. The $(10, 1, 8, 488)$ function was first constructed in [9] and we have checked that Δ_f value is 320 for that function. Thus our construction provides better parameter.

5 Conclusion

In this paper we present a lower bound on the minimum distance $dBR_n(1)$ between bent and 1-resilient functions on n variables, where n is even. We have also shown that it is possible to get 1-resilient functions by modifying exactly $dBR_n(1)$ many bits for $n = 4, 6, 8, 10$ which shows that the minimum distance is tight in these cases. Further the functions provide currently best known parameters.

A lot of open questions are still to be solved. First of all, a relatively hard question is to find out the minimum distance between bent and m-resilient functions on n variables, which we may denote as $dBR_n(m)$. It seems natural that $dBR_n(n-2) > dBR_n(n-3) > \ldots > dBR_n(1)$, though it needs a proof. Note that $(n-2)$-resilient functions on n variables are basically the affine functions, which are known to be at maximum distance from the bent function [14].

Showing that the lower bound is tight requires construction of n-variable 1-resilient functions from bent functions by modifying $2^{\frac{n}{2}-1} + 2\left\lceil \frac{(r+1)(2^{\frac{n}{2}-1} - \sum_{i=0}^{r} \binom{n}{i}) + \sum_{i=1}^{r} i\binom{n}{i}}{n-r-1} \right\rceil$ many bits for any n. However, for the cases $n \geq 12$, the bound seems not tight and we may need more points than the lower bound. The case for $n = 8$ could be nicely handled, but it starts to become complicated from $n = 10$ and requires some computer simulation. We are currently working in this direction.

Note that the upper bound of nonlinearity on 1-resilient function is $2^{n-1} - 2^{\frac{n}{2}-1} - 4$ for n even as described in [16]. The tightness of this bound has been shown upto $n = 8$. For $n \geq 10$, there is no evidence of an 1-resilient function attaining that bound. Note that the construction, we propose, modifies $dBR_n(1) > 2^{\frac{n}{2}-1}$ many bits and it seems unlikely that modifying all these bits will result in a fall of nonlinearity only 4 for $n \geq 10$.

References

[1] C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation immune functions. In *Sequences and Their Applications - SETA 2001*, Discrete Mathematics and Theoretical Computer Science, pages 131–144. Springer Verlag, 2001.

[2] C. Carlet. A larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Constructions. In *Advances in Cryptology - CRYPTO 2002*, number 2442 in Lecture Notes in Computer Science, pages 549–564. Springer Verlag, 2002.

[3] C. Carlet and P. Sarkar. Spectral domain analysis of correlation immune and resilient Boolean functions. *Finite Fields and Its Applications*, 8(1):120–130, January 2002.

[4] P. Charpin and E. Pasalic. On Propagation Characteristics of Resilient Functions. In *SAC 2002*, number 2595 in Lecture Notes in Computer Science, pages 175–195. Springer-Verlag, 2003.

[5] J. Clark, J. Jacob, S. Stepney, S. Maitra and W. Millan. Evolving Boolean Functions Satisfying Multiple Criteria. In *INDOCRYPT 2002*, Volume 2551 in Lecture Notes in Computer Science, pages 246–259, Springer Verlag, 2002.

[6] J. F. Dillon. Elementary Hadamard Difference sets. PhD Thesis, University of Maryland, 1974.

[7] M. Fedorova and Y. V. Tarannikov. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices. In *Progress in Cryptology - INDOCRYPT 2001*, number 2247 in Lecture Notes in Computer Science, pages 254–266. Springer Verlag, 2001.

[8] X. Guo-Zhen and J. Massey. A spectral characterization of correlation immune combining functions. *IEEE Transactions on Information Theory*, 34(3):569–571, May 1988.

[9] S. Maitra and E. Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity. *IEEE Transactions on Information Theory*, 48(7):1825–1834, July 2002.

[10] S. Maitra. Autocorrelation Properties of correlation immune Boolean functions. INDOCRYPT 2001, number 2247 Lecture Notes in Computer Science. Pages 242–253. Springer Verlag, December 2001.

[11] S. Maity and T. Johansson. Construction of Cryptographically Important Boolean Functions. In *INDOCRYPT 2002*, Volume 2551 in Lecture Notes in Computer Science, pages 234–245, Springer Verlag, 2002.

[12] E. Pasalic, S. Maitra, T. Johansson and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity. In *Workshop on Coding and Cryptography - WCC 2001*, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001.

[13] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, Lecture Notes in Computer Science, pages 161–173. Springer-Verlag, 1991.

[14] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20:300–305, 1976.

[15] P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology - EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 485–506. Springer Verlag, 2000.

[16] P. Sarkar and S. Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. In *Advances in Cryptology - CRYPTO 2000*, number 1880 in Lecture Notes in Computer Science, pages 515–532. Springer Verlag, 2000.

[17] J. Seberry, X. M. Zhang, and Y. Zheng. On constructions and nonlinearity of correlation immune Boolean functions. In *Advances in Cryptology - EUROCRYPT'93*, number 765 in Lecture Notes in Computer Science, pages 181–199. Springer-Verlag, 1994.

[18] Y. V. Tarannikov. On resilient Boolean functions with maximum possible nonlinearity. In *Progress in Cryptology - INDOCRYPT 2000*, number 1977 in Lecture Notes in Computer Science, pages 19–30. Springer Verlag, 2000.

[19] Y. V. Tarannikov. New constructions of resilient Boolean functions with maximal nonlinearity. In *Fast Software Encryption - FSE 2001*, to be published in Lecture Notes in Computer Science, pages 70–81 (in preproceedings). Springer Verlag, 2001.

[20] Y. V. Tarannikov, P. Korolev and A. Botev. Autocorrelation coefficients and correlation immunity of Boolean functions. In *ASIACRYPT 2001*, Lecture Notes in Computer Science. Springer Verlag, 2001.

[21] Y. Zheng and X. M. Zhang. Improved upper bound on the nonlinearity of high order correlation immune functions. In *Selected Areas in Cryptography - SAC 2000*, number 2012 in Lecture Notes in Computer Science, pages 264–274. Springer Verlag, 2000.

[22] X. M. Zhang and Y. Zheng. GAC - the criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science*, 1(5):316–333, 1995.

[23] Y. Zheng and X. M. Zhang. On relationships among propagation degree, nonlinearity and correlation immunity. In *Advances in Cryptology - ASIACRYPT'00*, Lecture Notes in Computer Science. Springer Verlag, 2000.