When a Boolean Function can be Expressed as the Sum of two Bent Functions

Longjiang Qu[1], Shaojing Fu[2], Qingping Dai[1] and Chao Li[1]
1. College of Science, 2. College of Computer,
National University of Defense Technology, ChangSha, Hunan, P. R. China, 410073

Abstract

In this paper we study the problem that when a Boolean function can be represented as the sum of two bent functions. This problem was recently presented by N. Tokareva in studying the number of bent functions [20]. Firstly, many functions, such as quadratic Boolean functions, Maiorana-MacFarland bent functions, partial spread functions etc, are proved to be able to be represented as the sum of two bent functions. Methods to construct such functions from low dimension ones are also introduced. N. Tokareva's main hypothesis is proved for $n \leq 6$. Moreover, two hypotheses which are equivalent to N. Tokareva's main hypothesis are presented. These hypotheses may lead to new ideas or methods to solve this problem. At last, necessary and sufficient conditions on the problem when the sum of several bent functions is again a bent function are given.
Keywords : Bent functions, Sum of bent functions, Maiorana-MacFarland bent function, Partial spread function.

1 Introduction

Boolean functions constitute important building blocks for cryptographic systems, either as filter/combiner functions in stream ciphers or as S-boxes in block ciphers. The security of these systems is mainly attributed to the cryptographic properties of the underlying functions. In order to be resistant against cryptanalytic attacks, cryptographic Boolean functions need to satisfy specific criteria, such as balancedness, high nonlinearity, correlation immunity, etc. In recent years, the research of cryptographic Boolean functions are mainly on two problems. The first one is to study a new criteria called "Algebraic Immunity" which was introduced to measure the immunity of the underlying cryptographic systems to algebraic attacks [16]. Several constructions of Boolean functions with maximum algebraic immunity have been presented. These constructions include symmetric Boolean functions, rotation symmetric Boolean functions and general Boolean functions, see [8,11,12,17,18,22], etc. The second problem is to construct Boolean functions with high nonlinearity. Bent functions, as a particular class of such functions, are paid much attention these years, see for example surveys [3,21]. For many years, the focus was on the construction of binary bent functions. This paper will be focused on the second problem.

There are still many open problems on bent functions after many years of wide research. For example, Maiorana-McFarland bent functions and partial

spread bent functions are the two largest classes of bent functions that are now known to us. However, they occupy only a negligible part of all bent functions with $n \geq 8$ variables [15]. Further, the number of bent functions in n variables is still unknown if $n > 8$. Moreover, there is a large gap between existing lower $(2^{n/2})!2^{2^{n/2}}$ and upper $2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}$ bounds for this number. There are several improvements of these bounds, see [1] and [6], but not too significant. To find the asymptotic value for the number of all bent functions is a long-standing hard problem closely connected to the problem of enumeration of Hadamard matrices.

Recently, N. Tokareva presented a new way to study the number of bent functions [20]. The idea is to study lower bounds on the number of bent functions given by iterative constructions. Evaluation of this lower bound was then shown to be closely connected to the problem of decomposing a Boolean function into the sum of two bent functions. About this problem, N. Tokareva raised the following main hypothesis [20].

Hypothesis 1.1 *[20] Let n be an even positive integer. Then any Boolean function in n variables with degree $\leq \frac{n}{2}$ can be expressed as the sum of two bent functions.*

If the above hypothesis can be proved, then one can get a best asymptotic value of the number of all n-variable bent functions, $2^{2^{n-c}+d\binom{n}{n/2}}$ for some constants c, d with $1 \leq c \leq 2$ [20]. Hypothesis 1.1 was verified to be true via computer search for $n \leq 6$ in [20]. However, until now neither a proof nor an counterexample of this hypothesis is found yet.

In this paper it is studied the problem when a Boolean function can be expressed as the sum of two bent functions. Many functions, such as quadratic Boolean functions, Maiorana-MacFarland bent functions, partial spread functions etc, are proved to be such functions. We also provide a proof of Hypothesis 1.1 for $n \leq 6$. Moreover, two hypotheses which are equivalent to Hypothesesis 1.1 are presented. These hypotheses may lead to new methods to solve this problem. At last, necessary and sufficient conditions on the problem when the sum of several bent functions is again a bent function are given.

The rest of the paper is organized as follows. Some preliminaries of bent functions are introduced in Section 2. In section 3, several classes of functions are proved to be able to be expressed as the sum of two bent functions, and two hypotheses equivalent to Hypothesis 1.1 are also introduced. In Section 4, methods to construct such functions from low dimension ones are given. A proof of Hypothesis 1.1 for $n \leq 6$ is given in Section 5. In Section 6 some results on the problem when the sum of several bent functions is still a bent function are presented. Section 7 concludes the paper.

2 Preliminaries

Let $\mathbb{F}_2$ be the binary finite field, and the vector space of dimension n over $\mathbb{F}_2$ is denoted by $\mathbb{F}_2^n$. By a little abuse of notation, we still use $+$ to denote the addition in $\mathbb{F}_2$ and $\mathbb{F}_2^n$. An n-variable Boolean function is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The set of all n-variable Boolean functions is denoted by $\mathbb{B}_n$. For any

$f \in \mathbb{B}_n$, f can be uniquely represented as

$$f(X) = f(x_1, \cdots, x_n) = \sum_{I \subseteq \{1,\cdots,n\}} a_I \prod_{i \in I} x_i, \quad a_I \in \mathbb{F}_2, \tag{1}$$

which is called the algebraic normal form(ANF) of f. The algebraic degree of $f \neq 0$, denoted by $\deg(f)$, is the maximum degree of the monomials in (1) whose coefficients are nonzero. All the Boolean functions with algebraic degree no more than 1 are called affine functions, and we use A_n to denote all the affine functions with n variables.

The set $\mathrm{supp}(f)$ is the subset of $\mathbb{F}_2^n$ where f takes the value 1. The Hamming weight of f is $\mathrm{wt}(f) = |\mathrm{supp}(f)|$. A Boolean function $f \in \mathbb{B}_n$ is called balanced if $\mathrm{wt}(f) = 2^{n-1}$. If $f \in \mathbb{B}_n$ is balanced, then $\deg(f) \leq n-1$. For $f, g \in \mathbb{B}_n$, the Hamming distance between f and g is given by $d(f,g) = \mathrm{wt}(f+g)$. The nonlinearity of f, denoted by nl_f, is the minimum Hamming distance between f and A_n. The Walsh transform of f is a real-valued function on $\mathbb{F}_2^n$, whose value at point $\omega \in \mathbb{F}_2^n$ is defined as: $W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\omega \cdot x}$. It is well-known that

$$nl_f = 2^{n-1} - \frac{1}{2} \max\{|W_f(\omega)| : \omega \in \mathbb{F}_2^n\} \leq 2^{n-1} - 2^{n/2-1}.$$

If the above equality holds, then f is called a bent function. Bent functions with n variables exist if and only if n is even. Denote by $\mathbb{BT}_n$ the set of all bent functions with n variables. It is known that if $f \in \mathbb{BT}_n$ and $n \geq 4$, then $\deg f \leq \frac{n}{2}$. If $f \in \mathbb{BT}_2$, then $\deg f = 2$.

Vectorial Boolean functions are the mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, and such a function is called an (n,m) function. For an (n,m) function $F = (f_1, \cdots, f_m)$, f_i is called its i-th coordinate function, the linear combinations, with non all-zero coefficients, of the coordinate functions of F are called its component functions. An (n,m) function F is called a vectorial bent function if all of its component functions are bent Boolean functions.

From now on, we always let $n = 2k$ be an even integer. Moreover, we assume that $n \geq 4$ such that any n-variable bent function have algebraic degree $\leq k$.

3 Several classes of functions in X_n

Let us first introduce some notations in [20]. Define the following set $X_n = \{f + g | f, g \in \mathbb{BT}_n\}$ and consider the system $\{C_f | f \in \mathbb{BT}_n\}$ of its subsets defined as $C_f = f + \mathbb{BT}_n$. So one can get $X_n = \cup_{f \in \mathbb{BT}_n} C_f$. Let ψ be an element of X_n. The number of subsets C_f that cover ψ we call multiplicity of ψ and denote it by $m(\psi)$. Then we have $\sum_{\psi \in X_n} m(\psi) = |\mathbb{BT}_n|^2$. It is clear that for any $l \in A_n$, we have $l \in X_n$ and $m(l) = |\mathbb{BT}_n|$. It is also clear that for any $\psi \in \mathbb{B}_n$, $l \in A_n$, $\psi \in X_n$ holds if and only if $\psi + l \in X_n$ holds. Further, if $\psi \in X_n$, then $m(\psi) \equiv 0 \mod 2^{n+1}$, and $m(\psi) = m(\psi + l)$ holds for any $l \in A_n$. More generally, we have

Lemma 3.1 *X_n and $m(\psi)$ are invariant under the action of general affine group and the addition of affine functions.*

If we assume that all the functions of both X_n and $\mathbb{BT}_n$ are free of affine terms, then we have

$$\left(\frac{|\mathbb{BT}_n|}{2^{n+1}}\right)^2 \geq \frac{|X_n|}{2^{n+1}}.$$

Thus we get the following result, which is a slight improvement of Proposition 3 of [20].

Proposition 3.2 *$|\mathbb{BT}_n|^2 \geq 2^{n+1}|X_n|$ for any even $n \geq 2$.*

Proposition 3.2 provides a new way to lower bound the number of all n-variable bent functions [20]. If Hypothesis 1.1 is true, then instantly one can get $|\mathbb{BT}_n| \geq 2^{2^{n-2}+\frac{1}{4}\binom{n}{n/2}+\frac{n+1}{2}}$, which will be the best lower bound of this number. It should be noted that even if Hypothesis 1.1 does not hold, it is also quite interesting to study the asymptotic value of X_n since it may lead to a bound better than all existing results. Moreover, the research of the properties of X_n may also be helpful to the research of the properties of bent functions.

Now we introduce the first several classes of functions in X_n.

Theorem 3.3 *Let $\psi \in \mathbb{B}_n$ with $\deg \psi \leq \frac{n}{2} = k$.*

1. *If $\deg \psi = 2$, then $\psi \in X_n$;*
2. *If $\psi = (x \cdot \pi_1(y) + g_1(y)) + (z \cdot \pi_2(w) + g_2(w))$, where $x, y, z, w \in \mathbb{F}_2^k$ such that every element of $\mathbb{F}_2^n$ can be uniquely expressed as (x, y) and also be uniquely expressed as (z, w), both π_1 and π_2 are permutations of $\mathbb{F}_2^k$, g_1, g_2 be any two Boolean functions with k variables. Then $\psi \in X_n$.*
3. *If $\psi(x, y) = x \cdot \pi(y) + g(y)$, where $x, y \in \mathbb{F}_2^k$, $\pi(y) = \pi_1(y) + \pi_2(y)$, both π_1 and π_2 are permutations of $\mathbb{F}_2^k$, g be any Boolean function with k variables. Then $\psi \in X_n$ and $m(\psi) \geq 2^{2^k}$.*
4. *If $\psi(x, y) = (x \cdot \pi_1(y) + y \cdot \pi_2(x)) + g_1(y) + g_2(x)$, where $x, y \in \mathbb{F}_2^k$, both π_1 and π_2 are permutations of $\mathbb{F}_2^k$, g_1, g_2 be any two Boolean functions with k variables. Then $\psi \in X_n$. In particular, if $\psi(x, y) = g_1(y) + g_2(x)$, then $\psi \in X_n$.*

Proof. 1. By Lemma 3.1, we only need to prove that for any $1 \leq r \leq k$, $f_r(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{r} x_{2i-1}x_{2i} \in X_n$. Note that $k \geq 2$ since $n \geq 4$. It is well known that a quadratic Boolean function with n variables is bent if and only if it is nonsingular.

For any $1 \leq r \leq k$, and any $1 \leq i \leq 2r$, let

$$y_i = \begin{cases} x_i, & \text{if } i \text{ is odd;} \\ \sum_{j=0}^{r-i/2} x_{i+2j}, & \text{if } i \text{ is even.} \end{cases}$$

Let $g_r(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{r-1} y_{2i-1}y_{2i} + x_{2r-1}(x_{2r} + x_2) + \sum_{i=r+1}^{k} x_{2i-1}x_{2i}$, and let $h_r(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{r-1} y_{2i-1}y_{2i+2} + x_{2r-1}x_2 + \sum_{i=r+1}^{k} x_{2i-1}x_{2i}$. It is easy to verify that $f_r = g_r + h_r$, and that both g_r and h_r are nonsingular quadratic Boolean functions. Hence f_r can be expressed as the sum of two quadratic bent functions. We proved the first part.

2. Let $f_1(x, y) = x \cdot \pi_1(y) + g_1(y)$, $f_2(z, w) = z \cdot \pi_2(w) + g_2(w)$ be two Maiorana-McFarland Bent functions. Then $\psi = f_1 + f_2$. Thus $\psi \in X_n$.

3. In the second part, let $z = x$, $w = y$ and $g(y) = g_1(y) + g_2(y)$, then we know $\psi \in X_n$. It is easy to see that $m(\psi) \geq 2^{2^k}$.

4. In the second part, let $z = y$ and $w = x$, then we know $\psi \in X_n$. Further, let $\pi_1 = \pi_2$, we have $\psi(x, y) = g_1(y) + g_2(x) \in X_n$. □

The first part of the above theorem tells us that any quadratic Boolean function with $n \geq 4$ variables can be expressed as the sum of two bent functions. The following corollary follows from the third part of the above theorem.

Corollary 3.4 *Let $\psi \in \mathbb{B}_n$. If ψ can be expressed as a Boolean function with at most $k = \frac{n}{2}$ variables, then $\psi \in X_n$ and $m(\psi) \geq (2^k)!2^{2^k}$. In particular, if $\psi = x_1 x_2 \cdots x_r$, where r is an integer such that $1 \leq r \leq k$, then $\psi \in X_n$.*

Proof. In the third part of Theorem 3.3, let $\pi_1 = \pi_2$ be any permutation on $\mathbb{F}_2^k$, the result of this corollary thus follows. □

It is clear that the set of all monomials with algebraic degree $\leq k$ is a basis of the vector space of the Boolean functions with algebraic degree $\leq k$. Thus it follows directly from Corollary 3.4 that the following hypothesis is equivalent to Hypothesis 1.1.

Hypothesis 3.5 *Let $n \geq 4$ be an even integer. Then X_n is closed with respect to addition, that is, if $f, g \in X_n$, then $f + g \in X_n$.*

Let $f, g \in X_n$, then there exist n-variable bent functions f_1, f_2, g_1, g_2 such that $f = f_1 + f_2$ and $g = g_1 + g_2$. To prove that $f + g \in X_n$, we need to find two n-variable bent functions h_1, h_2 such that $f + g = f_1 + f_2 + g_1 + g_2 = h_1 + h_2$. Thus it follows that Hypothesis 3.5 holds if and only if the sum of any four bent functions in n variables can be expressed as the sum of two bent functions with the same variables. Further, the number of bent functions involved can be reduced.

Hypothesis 3.6 *Let $n \geq 4$ be even. Then the sum of any three bent functions in n variables can be expressed as the sum of two bent functions with the same variables.*

Proposition 3.7 *Hypothesis 1.1, Hypothesis 3.5 and Hypothesis 3.6 are all equivalent. Any one holds if and only if the other two hold.*

Proof. We have already known that Hypothesis 1.1 and Hypothesis 3.5 are equivalent. Now we prove that Hypothesis 3.6 is also equivalent to Hypothesis 1.1. First, Hypothesis 3.6 can be deduced from Hypothesis 1.1 since the sum of three bent functions has algebraic degree $\leq k$. Second, assume that Hypothesis 3.6 holds. Then it follows that the sum of any four bent functions in n variables can be expressed as the sum of two bent functions with the same variables. Thus Hypothesis 3.6 implies Hypothesis 3.5, and hence Hypothesis 1.1. The proof is now completed. □

Though both Hypothesis 3.5 and Hypothesis 3.6 are equivalent to Hypothesis 1.1, they provide us different sides of the same problem. We hope that these new hypotheses can lead to new ideas or methods to solve the problem.

Let $f = g_1 + g_2 + g_3$, where $f \in \mathbb{B}_n$ and $g_1, g_2, g_3 \in \mathbb{BT}_n$. Assume there exists $h_1, h_2 \in \mathbb{BT}_n$ such that $f = g_1 + g_2 + g_3 = h_1 + h_2$. Then we have $h_2 = g_1 + g_2 + g_3 + h_1$. Thus it is equivalent to find $h_1 \in \mathbb{B}_n$ such that both h_1

and $g_1+g_2+g_3+h_1$ are bent. Hence Hypothesis 3.6 is related to the following questions: When the sum of four bent functions is a bent function again? When the sum of two bent functions is a bent function again? Some results on these two questions will be presented in Section 6.

Let k be a positive integer, and let

$$S_k = \{f : \mathbb{F}_2^k \longrightarrow \mathbb{F}_2^k | f = \pi_1 + \pi_2, \text{ both } \pi_1 \text{ and } \pi_2 \text{ are permutations on } \mathbb{F}_2^k\}. \tag{2}$$

According to Theorem 3.3(3), we want to investigate the set S_k for any positive integer k. First, we recall a result by M. Hall, Jr. in 1952.

Theorem 3.8 *[13] Let $G = \{a_1, \cdots, a_n\}$ be an abelian additive group with order n, and let $b_1, \cdots, b_n \in G$. Then there exists a permutation π of $\{1, \cdots, n\}$ such that $\{a_1 + b_{\pi(1)}, \cdots, a_n + b_{\pi(n)}\} = G$ if and only if $\sum_{i=1}^{n} b_i = 0$.*

Let $f : \mathbb{F}_2^k \longrightarrow \mathbb{F}_2^k$. Then $f \in S_k$ if and only if there exist two permutations π_1 and π_2 on $\mathbb{F}_2^k$ such that $\pi_2 = \pi_1 + f$. Hence the following result follows from Theorem 3.8.

Theorem 3.9 *Let k be a positive integer, and let $f : \mathbb{F}_2^k \longrightarrow \mathbb{F}_2^k$. Then $f \in S_k$ if and only if $\sum_{x \in \mathbb{F}_2^k} f(x) = 0$, where S_k is defined in (2).*

Now all the elements of S_k are determined by the above theorem. Particularly, we know that all permutations of $\mathbb{F}_2^k$ are in S_k, which implies the following result.

Theorem 3.10 *Let ψ be a Maiorana-McFarland bent function with $n \geq 4$ variables. Then $\psi \in X_n$.*

We have seen that all Maiorana-McFarland bent functions are in X_n. Now we turn to the other widely known bent class–partial spread bent function. Recall that a partial spread of order m(an m-spread) in $\mathbb{F}_2^n$ is a set of k-dimensional subspaces $H_1, \cdots, H_m$ of $\mathbb{F}_2^n$ such that $H_i \cap H_j = \{0\}$ holds for all $1 \leq i < j \leq m$. Clearly, the order of a partial spread is less than or equal to $2^k + 1$, and such a maximal partial spread is called a spread. Let $\{H_1, \cdots, H_m\}$ be an m-spread. Let $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ be the indicator function of H_i, i.e. $f_i^{-1}(1) = H_i$. The Boolean function $f = \sum_{i=1}^{m} f_i$ is called a partial spread function of order m or an m-spread function. The partial spread functions of order 2^{k-1} or $2^{k-1}+1$ consists of the class of partial spread bent functions [10].

Theorem 3.11 *Let $\psi \in \mathbb{B}_n$ be a partial spread function of order t, $1 \leq t \leq 2^k + 1$. Then $\psi \in X_n$. In particular, all partial spread bent functions are in X_n.*

Proof. Without loss of generality, we can assume that $E_1, E_2, \cdots, E_{2^k+1}$ is a spread of $\mathbb{F}_2^n$ and ψ equals the sums (modulo 2) of the indicators of subspaces $E_1, E_2, \cdots, E_t$. Let $a_0, b_0 \in \{0, 1\}$ and satisfying $a_0 + b_0 \equiv t \mod 2$, and let $a = \frac{t+a_0-b_0}{2}$ and $s = \frac{2^k+a_0+b_0-t}{2}$. Then $a + s = 2^{k-1} + a_0$ and $t - a + s = 2^{k-1} + b_0$. Let f be an n-variable Boolean function such that f equals the sums (modulo 2) of the indicators of a subspaces of $E_1, E_2, \cdots, E_t$ and s subspaces of $E_{t+1}, E_{t+2}, \cdots, E_{2^k+1}$, and let $h = f + \psi$. Then it is easy to verify that both f and h are partial spread bent functions. We are done. □

Two classes of bent functions have been derived in [4] from Maiorana-McFarland class, by adding to some functions of this class the indicators of some vector spaces. The first class, denoted by Class $\mathbb{D}$, is the set of the functions of the form $f(x,y) = x \cdot \pi(y) + 1_{E_1}(x)1_{E_2}(y)$, where π is any permutation on $\mathbb{F}_2^{n/2}$ and where E_1, E_2 are two linear subspaces of $\mathbb{F}_2^{n/2}$ such that $\pi(E_2) = E_1^{\perp}$(1_{E_1} and 1_{E_2} denote their indicators). The second class, denoted by Class $\mathbb{C}$, is the set of the functions of the form $f(x,y) = x \cdot \pi(y) + 1_L(x)$, where π is any permutation on $\mathbb{F}_2^{n/2}$ and L is any linear subspace such that for any element a of $\mathbb{F}_2^{n/2}$, the set $\pi^{-1}(a + L^{\perp})$ is a flat. Thus we have the following proposition:

Proposition 3.12 *Let $\psi \in \mathbb{B}_n$. If ψ can be expressed as the sum of two functions from the union of the sets Class $\mathbb{D}$ and Class $\mathbb{C}$ bent functions, then $\psi \in X_n$.*

The functions in the above proposition do not have an explicit form or an explicit structure as those in the former theorems or propositions do. The reason is the restrictions needed in constructing Class $\mathbb{D}$ and Class $\mathbb{C}$ bent functions. Indeed, more restrictions on constructing bent functions will lead to more complicated structure of the corresponding sum set. There are several quite general constructions, such as Generalized Partial Spread Class in [5] or a general class of Maiorana-McFarland's construction in [7], etc. However, if we use such bent functions to construct elements of X_n, we can only get some results similar with Proposition 3.12, which provide functions with no explicit forms. We do not introduce these results here since it may be more interesting to construct the functions of X_n with explicit forms.

4 Constructing new functions from those with lower dimension

In last section several classes of functions of X_n are presented. Those are mainly coming from existing constructions of bent functions, more precisely, from the primary constructions of bent functions. There are also some secondary constructions of bent functions, which means recursive constructions. From direct sum and indirect sum constructions of bent functions([9, Proposition 3.2]), we can have the following result.

Theorem 4.1 *Let n and m be two positive even integers, and let $f(x)$ and $g(y)$ be any functions of X_n and X_m respectively. Then $f(x) + g(y) \in X_{n+m}$ and $f(x)g(y) \in X_{n+m}$.*

Proof. Let $f(x) = f_1(x)+f_2(x), g(y) = g_1(y)+g_2(y)$, where $f_1(x), f_2(x) \in \mathbb{BT}_n$, $g_1(y), g_2(y) \in \mathbb{BT}_m$. Then by the well-known direct sum construction of bent functions, both $h_1(x,y) = f_1(x) + g_1(y)$ and $h_2(x,y) = f_2(x) + g_2(y)$ are bent functions with $n+m$ variables. Thus $f(x) + g(y) = f_1(x) + g_1(y) + f_2(x) + g_2(y) \in X_{n+m}$. Moreover, by the so-called indirect sum construction of bent functions([9, Proposition 3.2]), we have

$$\begin{aligned} h(x,y) &= f_1(x) + g_1(y) + (f_1(x) + f_2(x))(g_1(y) + g_2(y)) \\ &= h_1(x,y) + f(x)g(y) \in \mathbb{BT}_{n+m}. \end{aligned}$$

Hence $f(x)g(y) = h_1(x,y) + h(x,y) \in X_{n+m}$. □

Theorem 4.1 can help us to build many functions of X_n from those with lower dimensions. With this result, we can get more functions that can not be obtained before.

Example 4.2 *Let n and m be two positive even integers.*

(1) Let $f(x_1, \cdots, x_n) = f_1(x_1, \cdots, x_{\frac{n}{2}})$, and for integer $1 \le r \le \frac{m}{2}$, let $g_r(x_{n+1}, \cdots, x_{n+m}) = \sum_{i=1}^{r} x_{n+2i-1}x_{n+2i}$. Then both $f_1(x_1, \cdots, x_{\frac{n}{2}}) + \sum_{i=1}^{r} x_{n+2i-1}x_{n+2i}$ and $f_1(x_1, \cdots, x_{\frac{n}{2}}) \cdot (\sum_{i=1}^{r} x_{n+2i-1}x_{n+2i})$ are in X_{n+m}.

(2) Let $f(x,y) = x \cdot \pi(y) + g(y)$, where $x, y \in \mathbb{F}_2^{\frac{n}{2}}$, π is a permutation of $\mathbb{F}_2^{\frac{n}{2}}$, $g \in \mathbb{B}_{\frac{n}{2}}$, and let $h(z_1, \cdots, z_m) = h_1(z_1, \cdots, z_{\frac{m}{2}})$. Then both $f(x,y) + h(z)$ and $f(x,y)h(z)$ are in X_{n+m}.

The following result is a link with vectorial bent functions.

Proposition 4.3 *Let $r \le \frac{n}{2}$ be a positive integer, and let $F = (f_1, \cdots, f_r)$ be an (n,r)-bent function. Then all the component functions of F are in X_n.*

Proof. Let $\psi = \sum_{i=1}^{r} c_i f_i = c \cdot F$ be a component function of F, where $0 \ne c = (c_1, \cdots, c_r) \in \mathbb{F}_2^r$. Then there exists $d \ne 0, c$ such that $\psi = d \cdot F + (c+d) \cdot F$. Hence $\psi \in X_n$. □

From Proposition 4.3, we know that any construction of vectorial bent functions can provide a set of elements of X_n. All the known primary and secondary constructions of vectorial bent functions were surveyed and studied by Carlet in 2010 [9]. The component functions of all these primary constructions belongs, up to affine equivalence, to the Maiorana-MacFarland class of Boolean bent functions or Partial Spread constructions or power functions. All the existing secondary constructions of vectorial bent functions are either direct sum constructions or indirect sum constructions. Thus we can hardly get new elements of X_n from existing constructions of vectorial bent functions.

5 Proof of Hypothesis 1.1 for $n \le 6$

Hypothesis 1.1 have been verified via exhaust research in [20] for $n \le 6$. In this section we present a proof of Hypothesis 1.1 for all $n \le 6$. The case for $n = 2$ is quite trivial. If $n = 4$, then it follows from Theorem 3.3(1) that X_4 consists of all Boolean functions of degree not more than 2. Now we assume $n = 6$. It is known that there are 34 affine equivalent classes of $RM(3,6)/RM(1,6)$ [14]. By Lemma 3.1, to verify Hypothesis 1.1, we only need to prove that all these representatives are in X_6. We give these results in Table 1. The follows are the comments of the table.

1. The representatives of all the equivalent classes of $RM(3,6)/RM(2,6)$ and those of $RM(3,6)/RM(1,6)$ have been listed in Table B.1 and Table D.1 of [2].

2. To simplify notation, as in [2], we use 123 to denote $x_1x_2x_3$ and 1· (23+3) to denote $x_1 \cdot (x_2x_3 + x_3)$, and so on.

Table 1: Proof of Hypothesis 1.1 for $n = 6$

Class	Representative of $RM(3,6)/RM(2,6)$	Representative of $RM(3,6)/RM(1,6)$	Proofs
f_1	0	0 12 14+23 16+25+34	Theorem 3.3 (1)
f_2	123	0	Corollary 3.4
		14	1·(23+4)
		24+15	1·(23+5)+4 ·2
		16+25+34	Proposition 3.10
		45	1·(23)+4 ·5
		16+45	2·(13)+5·4+6·1
f_3	123+245	0	1·(23)+5 ·(24)
		13	1·(23+3)+5 ·(24)
		14	1·(23+4)+5 ·(24)
		16	3·(12)+5 ·(24)+6 ·(1)
		26	1·(23)+5 ·(24)+6 ·(2)
		26+13	1·(23+3)+5 ·(24)+6 ·(2)
		26+14	1·(23+4)+5 ·(24)+6 ·(2)
		13+15+26+34	Proposition 3.10
		34+13+15	1·(23+3+5)+4 ·(25 + 3)
		34+16	3·(12+4)+5 ·(24)+6 ·(1)
f_4	123+456	0	Theorem 3.3(4)
		14	2·(13+4)+5 ·(1)+6 ·(3)+(14); 4·(56+2)+1 ·(5)+3 ·(6)
		15+24	1·(23+4)+5 ·(2)+6 ·(3)+(24); 1·(4+5)+2 ·(5)+6 ·(45 + 3)
		34+25+16	2·(13+4)+5 ·(1)+6 ·(3)+(34); 4·(56+2)+1 ·(5 + 6)+3 ·(6)+(25)
f_5	123+245+346	0	1·(23)+5 ·(24)+6 ·(34)
		12+13	1·(23+2+3)+5 ·(24)+6 ·(34)
		15	2·(45+6)+3 ·(46 + 5 + 6)+1 ·(4); 2·(13+6)+4 ·(1)+5 ·(3 + 1) + (36)
		12+13+25	1·(23+2+3)+5 ·(24 + 2)+6 ·(34)
		14+25	1·(23+4)+5 ·(24 + 2)+6 ·(34)
		35+26+25+12 +13+14	Proposition 3.10
		25+15+16	2·(45+5+6)+3 ·(46 + 5)+1 ·(4); 2·(13+6)+4 ·(1)+5 ·(3 + 1) + (16)
f_6	123+145+246 +356+456	0	1·(23+3+4)+6 ·(24 + 3)+5 ·(2); 1·(45+3+4)+6 ·(35 + 45 + 3)+2 ·(5)
		12+13	1·(23+2+3+6)+5 ·(36 + 2)+4 ·(3) + (26); 1·(45+6)+2 ·(46 + 5 + 6)+3 ·(4) + (456)
		23+15+14	1·(23+6)+5 ·(36 + 2 + 6)+4·(3) + (23); 1·(45+4+5+6)+2·(46 + 5)+3·(4) + (456 + 56)

3. The proofs for the representative functions to be in X_6 are listed in the last column of the table. All of them are the results in the former sections, such as Theorems 3.3, Proposition 3.10 etc. Proposition 3.10 is shown as a proof for some functions since those are bent functions and the widely known fact that any bent function with 6 variables is affine equivalent to a Maiorana-MacFarland bent function.

Thanks to the existing affine equivalent classes of $RM(3,6)/RM(1,6)$, we can give a proof of Hypothesis 1.1 for $n = 6$. This reverified N. Tokareva's computer search result, which lasted 14 days by using processor Intel Core i7 3.0 Ghz 256 Gb, and running with full loading of RAM [20]. However, our proofs can be easily checked and save much time.

6 When the sum of several bent functions is again a bent function?

As pointed out in Section 3, Hypothesis 3.6 is related to the following questions: When the sum of four bent functions is again a bent function? When the sum of two bent functions is again a bent function? Here we present some necessary and sufficient conditions on these questions. The following lemma is quite well known, see for example [3].

Lemma 6.1 *Let $f \in \mathbb{B}_n$, then f is a bent function if and only if $W_f(\alpha) \equiv 2^{\frac{n}{2}} \mod 2^{\frac{n}{2}+1}$ holds for any $\alpha \in \mathbb{F}_2^n$.*

Let $f_1, f_2, f_3, f_4 \in \mathbb{B}_n$, and let $s_1^4 = \sum_{i=1}^4 f_i$, $s_2^4 = \sum_{1\le i<j\le 4} f_i f_j$, $s_3^4 = \sum_{i=1}^4 \prod_{j\neq i} f_j$, $s_4^4 = \prod_{j=1}^4 f_j$. Then it is easy to check the following equality(Note that the sums being computed in $\mathbb{Z}$ and not modulo 2):

$$f_1 + f_2 + f_3 + f_4 = s_1^4 + 2s_2^4 + 4s_4^4.$$

Proposition 6.2 *Let $f_1, f_2, f_3, f_4 \in \mathbb{BT}_n$, and let $s_1^4, s_2^4, s_3^4, s_4^4$ be defined as above. Then $s_1^4 \in \mathbb{BT}_n$ if and only if $W_{s_2^4}(\alpha) + 2W_{s_4^4}(\alpha) \equiv 2^{\frac{n}{2}-1} \mod 2^{\frac{n}{2}}$ holds for any $\alpha \in \mathbb{F}_2^n$. In particular, if $s_4^4 \equiv 0$, then $s_1^4 \in \mathbb{BT}_n$ if and only if $W_{s_2^4}(\alpha) \equiv 2^{\frac{n}{2}-1} \mod 2^{\frac{n}{2}}$ holds for any $\alpha \in \mathbb{F}_2^n$.*

Proof. Let $\alpha \in \mathbb{F}_2^n$. Then

$$\begin{aligned}
& W_{f_1}(\alpha) + W_{f_2}(\alpha) + W_{f_3}(\alpha) + W_{f_4}(\alpha) \\
= & \sum_{x\in\mathbb{F}_2^n} (-1)^{\alpha\cdot x}[(1-2f_1(x)) + \cdots + (1-2f_4(x))] \\
= & \sum_{x\in\mathbb{F}_2^n} (-1)^{\alpha\cdot x}[4 - 2(s_1^4(x) + 2s_2^4(x) + 4s_4^4(x))] \\
= & W_{s_1^4}(\alpha) + 2W_{s_2^4}(\alpha) + 4W_{s_4^4}(\alpha) - 3\sum_{x\in\mathbb{F}_2^n} (-1)^{\alpha\cdot x} \\
= & W_{s_1^4}(\alpha) + 2W_{s_2^4}(\alpha) + 4W_{s_4^4}(\alpha) - 3\cdot 2^n\delta_0(\alpha),
\end{aligned}$$

where δ_0 denotes the Dirac symbol, that is, defined by $\delta_0(\alpha) = 1$ if $\alpha = 0$ and $\delta_0(\alpha) = 0$ otherwise. Since $f_1, f_2, f_3, f_4 \in \mathbb{BT}_n$, we have $W_{f_1}(\alpha) + W_{f_2}(\alpha) +$

$W_{f_3}(\alpha) + W_{f_4}(\alpha) \equiv 0 \mod 2^{\frac{n}{2}+1}$ for any $\alpha \in \mathbb{F}_2^n$. Thus $W_{s_1^4}(\alpha) + 2W_{s_2^4}(\alpha) + 4W_{s_4^4}(\alpha) \equiv 0 \mod 2^{\frac{n}{2}+1}$ holds for any $\alpha \in \mathbb{F}_2^n$. Therefore, s_1^4 is bent if and only if $W_{s_1^4}(\alpha) \equiv 2^{\frac{n}{2}} \mod 2^{\frac{n}{2}+1}$ holds for any $\alpha \in \mathbb{F}_2^n$, if and only if $W_{s_2^4}(\alpha) + 2W_{s_4^4}(\alpha) \equiv 2^{\frac{n}{2}-1} \mod 2^{\frac{n}{2}}$ holds for any $\alpha \in \mathbb{F}_2^n$. The second argument follows similarly. □

Similarly, we can get the following result on the problem when the sum of two bent functions is again a bent function.

Proposition 6.3 *Let $f_1, f_2 \in \mathbb{BT}_n$. Then $f_1+f_2 \in \mathbb{BT}_n$ if and only if $W_{f_1 f_2}(\alpha) \equiv 2^{\frac{n}{2}-1} \mod 2^{\frac{n}{2}}$ holds for any $\alpha \in \mathbb{F}_2^n$.*

7 Conclusion

This paper studies on the problem when a Boolean function can be expressed as the sum of two bent functions. Many functions are proved to be able to be represented as the sum of two bent functions. Two hypotheses which are equivalent to Hypotheses 1.1 are presented. We hope that these hypotheses can lead to new ideas or methods to study this problem. At last, to find new constructions of large classes of bent functions with "simple" forms other than Maiorana-MacFarland class and partial spread class are quite important to the research of bent functions and this problem.

Acknowledgments

The authors would like to thank Prof. Qing Xiang for bringing Theorem 3.8 to their attention, which leads directly to Theorem 3.9. This work is supported by the National Natural Science Foundation of China (No: 61103191, 61272484).

References

[1] S. Agievich, On the representation of bent functions by bent rectangles, In Proc. of probabilistic methods in discrete mathematics, 121-135, 2000.

[2] A. Braeken, Cryptographic properties of Boolean functions and S-boxes. PhD thesis. Available at http://homes.esat.kuleuven.be/∼abraeken/thesisAn.pdf. Katholieke University. 2006.

[3] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Cambridge University Press, Y. Crama and P. Hammer (eds.), pp. 257-397, 2010.

[4] C. Carlet. Two new classes of bent functions. EUROCRYPT' 93, LNCS 765(1994), 77-101.

[5] C. Carlet and P. Guillot. A characterization of binary bent functions, Journal of Combinatorial Theory, Series A, 76(1996), 328-335.

[6] C. Carlet and A. Klapper, Upper bounds on the numbers of resilient functions and of bent functions, ISIT 2002, 307-314, 2002.

[7] C. Carlet. On the confusion and diffusion properties of Maiorana- McFarland's and extended Maiorana-McFarland's functions. Journal of Complexity, 20(2004), 182-204.

[8] C. Carlet and K.Q. Feng, An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity, ASIACRYPT 2008, LNCS 5350(2008), 425-440.

[9] C. Carlet, S. Mesnager, On the construction of bent vectorial functions, Int. J. Inform. and Coding Theory, 1(2010), 133-148.

[10] J. F. Dillon, Elementary Hadamard Difference sets, Ph. D. Thesis. Univ. of Maryland, 1974.

[11] S.J. Fu, L.J Qu, C.Li, etc. Balanced Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity. IET Information Security, 5(2011), 93-99.

[12] S.J. Fu, C. Li, K. Matsuura, etc, Construction of Even-variable Rotation Symmetric Boolean Functions with Maximum Algebraic Immunity, SCIENCE CHINA Information Sciences, DOI: 10.1007/s11432-011-4350,2012.

[13] M. Hall, Jr., A combinatorial problem on abelian groups, Proceedings of the American Mathematical Society 3 (1952), 584C587.

[14] X.D. Hou, $AGL(m;2)$ acting on $R(r;m)/R(s;m)$, Journal of Algebra 171 (1995), 921-938.

[15] P. Langevin, G. Leander, Counting all bent functions in dimension eight, Design, codes, crypt. 59(2011), 193-205.

[16] W. Meier, E. Pasalic, and C. Carlet, Algebraic attacks and decomposition of Boolean functions, EUROCRYPT 2004, LNCS 3027, 474-491.

[17] L.J. Qu, C. Li, On the 2^m-variable symmetric Boolean functions with maximum algebraic immunity. SCIENCE CHINA Information Sciences, 51(2008), 120-127.

[18] L.J. Qu, K.Q. Feng, F. Liu, etc, Constructing Symmetric Boolean Functions With Maximum Algebraic Immunity, IEEE Transactions on Information Theory, 55(2009), 2406-2412.

[19] O. Rothaus, On bent functions, J. Combin. Theory. Ser. A. 20 (1976), 300-305.

[20] N. N. Tokareva, On the number of bent functions: lower bounds and hypotheses, Advances in Mathematics of Communications, 5(2011), 609-621.

[21] N. N. Tokareva, Nonlinear Boolean functions: bent functions and their generalizations, LAP Lambert Academic Publishing (Saarbrucken, Germany), 2011. ISBN: 978-3-8433-0904-2.

[22] X.Y. Zeng, C. Carlet, J.Y. Shan and L. Hu, More Balanced Boolean Functions with optimum Algebraic Immunity and good Nonlinearity and Resistance to Fast Algebraic Attacks, IEEE Transactions on Information Theory, 57(2011), 6310-6320.