Constructing Vectorial Boolean Functions with High Algebraic Immunity Based on Group Decomposition

Yu Lou[1], Huiting Han[1], Chunming Tang[1], and Maozhi Xu[1,2]

[1] LMAM, School of Mathematical Sciences, Peking University, Beijing, 100871, China.
[2] Key Laboratory of Network and Software Security Assurance, Beijing, 100871, China
windtker@pku.edu.cn
mzxu@math.pku.edu.cn

Abstract. In this paper, we construct a class of vectorial Boolean functions over $\mathbb{F}_{2^n}$ with high algebraic immunity based on the decomposition of the multiplicative group of $\mathbb{F}_{2^n}$. By viewing $\mathbb{F}_{2^n}$ as $G_1G_2\bigcup\{0\}$ (where G_1 and G_2 are subgroups of $\mathbb{F}_{2^n}^*$, $(\#G_1, \#G_2) = 1$ and $\#G_1 \times \#G_2 = 2^{2k} - 1$), we give a generalized description for constructing vectorial Boolean functions with high algebraic immunity. Moreover, when n is even, we provide two special classes of vectorial Boolean functions with high(sometimes optimal) algebraic immunity, one is hyper-bent, and the other is of balancedness and optimal algebraic degree .

Key words: vectorial Boolean function, polar decomposition, algebraic immunity, balancedness, algebraic degree, hyper-bent functions.

1 Introduction

Boolean functions play a very critical role in symmetric cryptographic systems. There are many criteria for a Boolean function to be a so-called "good" function, such as balancedness, high nonlinearity, high algebraic degree, and correlation immunity. In 2003, Courtois and Meier proposed a standard algebraic attack upon some well-known stream cryptographic systems(i.e. LILI128 and Toyocrypt)[12], which was then improved by Armknecht[2]. After that, algebraic attack has become an effective method to analyze stream ciphers, block ciphers. Besides LILI128 and Toyocrypt, many other cryptographic systems[1][11][13][4] were investigated by the means of algebraic attack. At the same time, algebraic immunity, which is used to measure a Boolean function's ability for resisting algebraic attack, has become a very important criterion to design Boolean functions. Because of the various algebraic properties and geometric constructions of Galois field, Boolean functions are most frequently studied over $\mathbb{F}_{2^n}$. When n is even, i.e., $n = 2k$, Boolean functions can also be viewed over $\mathbb{F}_{2^k}^2$. Based on those representations, several work has been done in constructing Boolean and vectorial Boolean functions with high(especially optimal) algebraic immunity[7][20][8][15].

As we know, for any commutative group G, if G has two subgroups G_1 and G_2, with $G_1 \bigcap G_2 = \{1\}$, $\#G = N_1 \times N_2$, $(N_1, N_2) = 1$, where $\#G_1 = N_1$ and $\#G_2 = N_2$, then G can be represented as $G = G_1 G_2$. Based on this fact, we offer a generalized description of constructing vectorial Boolean functions with high algebraic immunity over $\mathbb{F}_{2^n}$. When $n = 2k$, $\mathbb{F}_{2^n}^*$ has such two subgroups naturally: one is $\mathbb{F}_{2^k}^*$ and the other is the group of $2^k + 1$-th roots of unity in $\mathbb{F}_{2^n}$. Then, we construct two special classes of such kind of Boolean functions: one is hyper-bent and the other is balanced and with optimal algebraic degree.

The rest of this paper is organized as follows. We give some notations and recall some basic knowledge for this paper in Section 2. Then, we describe the main jobs in Section 3 and 4. Finally, in Section 5, we conclude our work.

2 Preliminary

2.1 Boolean and vectorial Boolean functions

Let n and m be two positive integers. A *Boolean function* of n variables is a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, and functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called $(n, m) - functions$. Such function F being given, the Boolean functions $f_1, \cdots, f_m$ defined, at every $x \in \mathbb{F}_2^n$, by $F(x) = (f_1(x), \cdots, f_m(x))$, are called the *coordinate function* of F. When the numbers m and n are not specified, $(n, m) - functions$ are called *multi-output Boolean functions or vectorial Boolean functions*[6].

2.2 Representations of Boolean functions

The basic representation of a n-varible Boolean function f is the truth-table, i.e., a binary string of length 2^n as

$$(f(0, \cdots, 0, 0), f(0, \cdots, 0, 1), f(0, \cdots, 1, 0), \cdots, f(1, \cdots, 1, 1)).$$

We say that a Boolean function f is *balanced* if its truth table contains an equal number of ones and zeros. The support of f is defined as

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

Let $\mathbb{B}_n$ be the set of n-variable(Boolean) functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Then, each $f \in \mathbb{B}_n$ has a unique representation as multivariate polynomial over $\mathbb{F}_2$, called the algebraic normal form(ANF), of the special form:

$$f(x_1, x_2, \cdots, x_n) = \sum_{I \subseteq \{1,2,\cdots,n\}} a_I (\prod_{i \in I} x_i) \qquad (a_I \in \mathbb{F}_2).$$

The algebraic degree of f or $\deg f$ is defined as the number of variables in the highest order term with nonzero coefficient. It should be noted that the maximal algebraic degree of a balanced Boolean functions of n variables is $n - 1$.

The Boolean functions over $\mathbb{F}_{2^n}$ can also be uniquely expressed by a *univariate polynomial*

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i,$$

where $a_0, a_{2^n-1} \in \mathbb{F}_2$, $a_i \in \mathbb{F}_{2^n}$ for $1 \leq i < 2^n - 1$ such that $a_i = a_{2i(\mod 2^n-1)}$, and the addition is modulo 2. In fact,

$$f(x) = \sum_{a \in \mathbb{F}_{2^n}} f(a)(1 + (x+a)^{2^n-1}).$$

For the 2-adic expansion $i = i_0 + i_1 2 + \cdots + i_{n-1}2^{n-1}$, the algebraic degree of f is defined as

$$\deg f = \max\{wt(i) : f_i \neq 0, 0 \leq i < 2^n\},$$

where $wt(i)$ is the number of ones in the 2-adic expansion of i or the Hamming weight of i. In this paper, we use $\bar{i}$ to denote the 2-adic expansion of i, i.e., $\bar{i} = (i_0, i_1, \cdots, i_{n-1})$.

For $\mathbb{F}_{2^n} = \mathbb{F}_{2^n}^* \bigcup \{0\}$, where $n = 2k$ and let α be a primitive element of $\mathbb{F}_{2^n}^*$, we consider the *polar decomposition* of $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^k}^* \times U$, where $\mathbb{F}_{2^k}^*$ is a subgroup of $\mathbb{F}_{2^n}^*$ with primitive element $\beta = \alpha^{2^k+1}$, U is the group of $2^k + 1$-th roots of unity in $\mathbb{F}_{2^n}$, that is, $U = \{z \in \mathbb{F}_{2^n}^* : z^{2^k+1} = 1\}$. Under the polar decomposition of $\mathbb{F}_{2^n}^*$, $\forall x \in \mathbb{F}_{2^n}^*$, x can be decomposed as $x = yz$, where $y \in \mathbb{F}_{2^k}^*$, $z \in U$. Especially, $\forall x \in \mathbb{F}_{2^n}^*$, $0 \leq r \leq 2^n - 1$, we have $x^r = (yz)^r = y^i z^j$, where $y \in \mathbb{F}_{2^k}^*$, $z \in U$ and $i \equiv r \mod 2^k - 1$, $j \equiv r \mod 2^k + 1$. According to the Chinese Remainder Theorem, $r = i(2^k+1)u + j(2^k-1)v \mod 2^n - 1$, where $u = 1 - 2^{k-1}$, $v = 2^{k-1}$. Hence, under the polar decomposition of $\mathbb{F}_{2^n}^*$, any Boolean function $f \in \mathbb{B}_n$ can be represented as

$$f(x) = \begin{cases} f^1(x) = f^1(y,z), & 0 \neq x = yz,\ y \in \mathbb{F}_{2^k}^* \text{ and } z \in U \\ f_0, & x = 0 \end{cases}$$

where $f^1(y,z) = \sum_{s=0}^{2^k-2} \sum_{t=0}^{2^k} f_{s,t} y^s z^t$, $f_{s,t} \in \mathbb{F}_{2^n}$, $f_0 \in \mathbb{F}_2$. The algebraic degree of f is

$$\deg(f) = \max\{wt(r) : r = s(2^k+1)u + t(2^k-1)v \mod 2^n - 1,\ f_{s,t} \neq 0\},$$

where $(2^k+1)u + (2^k-1)v = 1$.

The algebraic degree of vectorial Boolean functions is defined by

Definition 1. *[6] The algebraic degree of (n,m)-Boolean function F is*

$$\mathrm{Deg}(F) = \max\{\deg(f_i) : 0 \leq i \leq m-1\} = \max\{\deg(v \cdot F) :\ 0 \neq v \in \mathbb{F}_2^m\},$$

where $v \cdot F = \sum_{i=0}^{m-1} v_i f_i$. If F is balanced, then all f_i $(0 \leq i \leq m-1)$ are balanced, so that $Deg(F) \leq n-1$.

2.3 Algebraic immunity of Boolean and vectorial Boolean function

Definition 2. *[17]The algebraic immunity $AI(f)$ of an n-variable Boolean function $f \in \mathbb{B}_n$ is defined to be the lowest degree of nonzero functions g such that $f \cdot g = 0$ or $(f+1) \cdot g = 0$.*

In order to study the algebraic immunity property of vectorial Boolean functions, Armknecht introduced the idea of annihilating of set, and then generalized concept of annihilator from single-output Boolean functions to multi-output ones.

Definition 3. *[3]The basic algebraic immunity of a (n,m)-Boolean function F is*

$$AI(F) = \min\{\deg(g) : 0 \neq g \in \mathbb{B}_n, \text{ there exists } b \in \mathbb{F}_2^m \text{ such that } g\mid_{F^{-1}(b)} = 0\}$$

In 2003, Courois[12] gave the upper bound of Boolean functions, and in 2006, Armknecht[3] found the upper bound of the basic algebraic immunity of a (n,m)-Boolean function.

Theorem 1. *(1). Let f be a n-varible Boolean function, then*

$$AI(f) \leq \min\{\lceil \frac{n}{2} \rceil, \deg(f)\};$$

(2). If F is a (n,m)-Boolean function, $1 \leq m \leq n$, then $AI(F) \leq d(n,m)$, where $d = d(n,m)$ is the minimum positive integer such that

$$\sum_{i=0}^{d} \binom{n}{i} > 2^{n-m}.$$

Now, let's take a further look at the set and its algebraic immunity.

2.4 Algebraic immunity of set

Definition 4. *For any set $P \subseteq \mathbb{F}_2^n$, The algebraic degree of P is defined as*

$$AD(P) = \min\{deg(g) : g \neq 0, g|_P = 0\}.$$

Obviously, if $P_1 \subseteq P_2$, then $AD(P_1) \leq AD(P_2)$.

Here we give some more definitions about set:

Definition 5. *(1). $\mathcal{P} = \{P_0, \cdots, P_{M-1}\}$ is said to be a* M-division of set P, *if $P = \bigcup\limits_{0 \leq i < M} P_i,\ P_i \bigcap P_j = \emptyset,\ \forall i \neq j, 0 \leq i,j < M$.*
(2). Let $\mathcal{P} = \{P_0, \cdots, P_{M-1}\}$ be a M-division of set P, and $\mathcal{Q} = \{Q_0, \cdots, Q_{M-1}\}$. If $Q = \bigcup\limits_{0 \leq i < M} Q_i,\ Q_i \bigcap Q_j = \emptyset, Q \subseteq P,\ Q_i \subseteq P_k,\ \forall i \neq j,\ 0 \leq i,j,k < M$, $\mathcal{Q}$ is said to be a M-subdivision *of P (Sometimes we also call $\mathcal{Q}$ as a M-subdivision*

of $\mathcal{P}$, and denote as $\mathcal{Q} \preccurlyeq \mathcal{P}$).
(3). For any division $\mathcal{P} = \{P_0, \cdots, P_{M-1}\}$ of set P, the algebraic immunity of $\mathcal{P}$ is defined as

$$AI(\mathcal{P}) = \min\{AD(P_i) : 0 \le i < M\}.$$

(4).Let $\mathcal{P}_1$ be a M-subdivision of P, if $AI(\mathcal{P}_1) \ge d$, we call $\mathcal{P}_1$ as a d-base algebraic immunity *of P, and denote as $AD_{d,M}(P)$.*

From the above definitions, it follows that

Lemma 1. *Let both $\mathcal{P} = \{P_0, \ldots, P_{M-1}\}$ and $\mathcal{P}' = \{P'_0, \ldots, P'_M\}$ be the M-subdivisions of P. If $\mathcal{P} \preccurlyeq \mathcal{P}'$, then $AI(\mathcal{P}) \le AI(\mathcal{P}')$.*

Remark 1. By Lemma 1, if we can get a $AD_{d,M}(\mathbb{F}_{2^n})$ for the preimage set of some (n,m)-Boolean function F, where $AI(F) \ge d$ and $M = 2^m$, then any M-division of $\mathbb{F}_{2^n}$ $\mathcal{K}$ satisfying $AD_{d,M}(\mathbb{F}_{2^n}) \preccurlyeq \mathcal{K}$, has a algebraic immunity larger than d, hence the (n,m)-Boolean function FK whose preimage set is $\mathcal{K}$ satisfies $AI(FK) \ge d$. Specially, if $AI(AD_{d,M}(\mathbb{F}_{2^n}))$ reaches the maximum as Theorem 1 gives, then FK is a (n,m)-Boolean function with optimal algebraic immunity. Motivated by this strategy, we will construct high algebraic immunity (n,m)-Boolean functions from some known one.

2.5 Vectorial bent and hyper-bent functions

Bent function is a class of Boolean functions with even variables and with the maximal distance to linear and affine functions. In fact, the distance of a n-variable Bent function to any linear and affine function is $2^{n-1} - 2^{\frac{n}{2}-1}$. After introduced by Rothaus[18] in 1976, and thanks to their good algebraic and combinatorial properties, Bent functions have drawn more and more attention in designing cryptographic systems. In 2001, Youssef and Gong[21] found a subclass of Bent functions with even better cryptographic properties, which was named as hyper-bent function. The definition of Bent and hyper-bent functions can be referred to [18,21]. In this paper we will show some interest in vectorial hyper-bent function which is defined as follows.

Definition 6. *Let F be a (n,m)-Boolean function, if $F_v = v \cdot F = v_0 f_0 + \cdots + v_{m-1} f_{m-1} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is bent for every $0 \ne v = (v_0, v_1, \cdots, v_{m-1}) \in \mathbb{F}_2^m$, we call F a vectorial bent function. Moreover, if F_v is hyper-bent, we call* F *a vectorial hyper-bent function.*

3 A general way to constructing high algebraic immunity vectorial Boolean functions based on the decomposition of group

As mentioned before, for any commutative group G, if G has two subgroups G_1 and G_2, with $G_1 \bigcap G_2 = \{1\}$, $\#G = N_1 \times N_2$, $(N_1, N_2) = 1$, where $\#G_1 = N_1$

and $\#G_2 = N_2$, then G can be represented as $G = G_1G_2$. In this section, we assume $\mathbb{F}_{2^n}^*$ can be decomposed into G_1 and G_2 which satisfy the above requirements. Based on this representation, we will construct a class of vectorial Boolean functions with high algebraic immunity.

Before constructing, we define some symbols. Let $t,\ A,\ D \in \mathbb{Z}$, $0 \le t,\ A \le 2^k - 1$. Define

$$\widetilde{S}_{N_1,t}(n, D) = \{i : wt(N_1 i + t) < D, 0 \le i \le N_2 - 1\},$$

and

$$\widetilde{N}_{N_1}(n, D) = \max\{\#\widetilde{S}_{N_1,t}(n, D) : 0 \le t < N_1\},$$

Obviously, $\widetilde{N}_{N_1}(n, D)$ is monotonic increasing about D. Let $\widetilde{D}_{N_1}(n, A)$ be the maximal integer satisfying $\widetilde{N}_{N_1}(n, D) \le A$, i.e.,

$$\widetilde{D}_{N_1}(n, A) = \max\{D : \widetilde{N}_{N_1}(n, D) \le A, 1 \le D \le \lceil \frac{n}{2} \rceil\}.$$

Now, we can construct set with high algebraic immunity as follows.

Theorem 2. *Let $\mathbb{F}_{2^n}^* = G_1G_2$, $\#G_1 = N_1$, $\#G_2 = N_2$, $(N_1, N_2) = 1$, α be a generator of G_2, $0 \le A < [\frac{N_2}{2}]$, $0 \le c < [\frac{N_2}{A}]$, where $[T]$ is the integer part of T. Define:*

$$\widetilde{P}_{c,A} = \{\beta \cdot \alpha^i : \beta \in G_1, cA \le i < (c+1)A\},$$

then $AD(\widetilde{P}_{c,A}) \ge \widetilde{D}_{N_1}(n, A)$.

Proof. Let $h(x)|_{\widetilde{P}_{c,A}} = 0,\ 1 \le \deg(h) < \widetilde{D}_{N_1}(n, A)$, then for any $\beta \in G_1,\ \gamma = \alpha^i(cA \le i < (c+1)A)$, we get $h(\beta\gamma) = 0$. Let $h(x) = \sum\limits_{wt(i)<\widetilde{D}_{N_1}(n,A)}^{2^n-2} h_i x^i$, then

$$\begin{aligned} h(\beta\gamma) &= \sum_{wt(i)<\widetilde{D}_{N_1}(n,A)}^{2^n-2} h_i(\beta\gamma)^i \\ &= \sum_{\substack{0\le i<2^n-1 \\ wt(i)<\widetilde{D}_{N_1}(n,A)}} \beta^{i \pmod{N_1}} h_i\gamma^i \\ &= \sum_{t=0}^{N_1-1} \beta^t \sum_{\substack{0\le i<2^n-1 \\ i\equiv t \pmod{N_1} \\ wt(i)<\widetilde{D}_{N_1}(n,A)}} h_i\gamma^i. \end{aligned}$$

Let $H_t(\gamma) = \sum\limits_{\substack{0\le i<2^n-1 \\ i\equiv t \pmod{N_1} \\ wt(i)<\widetilde{D}_{N_1}(n,A)}} h_i\gamma^i$, then $h(\beta\gamma) = \sum\limits_{t=0}^{N_1-1} \beta^t H_t(\gamma) = 0$ holds for any $\beta \in G_1$. Therefore, $H_t(\gamma) = 0$, where $0 \le t < N_1$, $\gamma = \alpha^i(cA \le i < (c+1)A)$.

Since

$$H_t(\gamma) = \sum_{\substack{0\le i<N_2 \\ wt(t+N_1 i)<\widetilde{D}_{N_1}(n,A)}} h_{t+N_1 i}\gamma^{t+N_1 i} = \gamma^t \sum_{\substack{0\le i<N_2 \\ wt(t+N_1 i)<\widetilde{D}_{N_1}(n,A)}} h_{t+N_1 i}(\gamma^{N_1})^i.$$

Let $\widetilde{H}_t(y) = \sum_{\substack{0\le i<N_2 \\ wt(t+N_1 i)<\widetilde{D}_{N_1}(n,A)}} h_{t+N_1 i}(y)^i$, $\widetilde{H}_t(y)$ takes A consecutive points i.e., $(\alpha^{N_1})^{cA}, \cdots, (\alpha^{N_1})^{(c+1)A-1}$ as its roots. Since $(N_1, N_2) = 1$, α^{N_1} is also a generator of G_2. Then $\hat{h}_t = (h_t, h_{t+N_1}, \cdots, h_{t+N_1(N_2-1)})$ is a codeword of some BCH code with designed distance $A+1$. If $\hat{h} \neq \bar{0}$, then the number of i satisfying $h_i \neq 0$, $t \le i \le N_1(N_2-1)$ is at least $A+1$. However, our hypothesis implies that there are at most A nonzero elements in $\{h_i\}$, which is a contradiction! Therefore, $\hat{h}_t = (0, \cdots, 0)$ holds for any t (i.e. $h \equiv 0$), thus $AD(\widetilde{P}_{c,A}) \ge \widetilde{D}_{N_1}(n, A)$.

Based on Theorem 2, we can construct vectorial Boolean function with high algebraic immunity as follows.

Theorem 3. *Let* $A = [\frac{N_2}{2^m}]$, $\widetilde{P}_{c_i,A}(0 \le i \le 2^m - 1,\ c_i \in \mathbb{F}_{2^m})$ *be defined as in Theorem 2, and* $P_{c_i,A} \bigcap P_{c_j,A} = \emptyset (i \neq j)$. *If the vectorial Boolean function* $F : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^m}$ *satisfies* $F^{-1}(c_i) \supseteq \widetilde{P}_{c_i,A}$, *then* $AI(F) \ge D_{N_1}(n, A)$.

Proof. By Theorem 2 and Definition 3, the result stands.

4 Constructing high algebraic immunity vectorial Boolean functions over $\mathbb{F}_{2^{2k}}$

From section 2.2, we know, when $n = 2k$, the multiplicative group of $\mathbb{F}_{2^n}$, i.e., $\mathbb{F}_{2^n}^*$, always has two subgroups which satisfy the conditions listed in Theorem 2. Therefore, we can construct some classes of vectorial Boolean functions with high algebraic immunity based on Theorem 3.

From now on, we alwasy assume $n = 2k$, α is a primitive element in $\mathbb{F}_{2^n}^*$, U is the group of 2^k+1-th roots of unity in $\mathbb{F}_{2^n}$, that is, $U = \{z \in \mathbb{F}_{2^n}^* : z^{2^k+1} = 1\}$. $\xi = \alpha^{2^k-1}$ is a generator of U, and $\beta = \alpha^{2^k+1}$ is a primitive element in $\mathbb{F}_{2^k}^*$.

4.1 Constructing a class of hyper-bent functions with high algebraic immunity

In 2006, Carlet and Gaborit[9] found a class of hyper-bent functions which was named as $\mathcal{PS}_{ap}^{\#}$ class. After that, Charpin and Gong[10] derived a slightly different version of this kind of hyper-bent functions:

Proposition 1. *([10],Theorem 2)Let $n = 2k$, α be a primitive element in $\mathbb{F}_{2^n}$ and f be a Boolean function over $\mathbb{F}_{2^n}$ satisfying $f(\alpha^{2^{k+1}}x) = f(x)(\forall x \in \mathbb{F}_{2^n})$ and $f(0)=0$. Let ξ be a primitive 2^k+1-th root in $\mathbb{F}_{2^n}^*$. Then f is a hyper-bent function if and only if the cardinality of the set $\{i|f(\xi^i) = 1,\ 0 \le i \le 2^k\}$ is 2^{k-1}.*

Construction 1 *Let $1 \le m \le k, n = 2k, 0 \le i \le m-1$, $f_i : \mathbb{F}_{2^n} = \mathbb{F}_{2^k}^* \times U \bigcup \{0\} \longrightarrow \mathbb{F}_2$ defined as:*

$$f_i(x) = f_i(yz) = \begin{cases} 1, & y \in \mathbb{F}_{2^k}^*,\ z \in \bigcup\limits_{\substack{0 \le b \le 2^m-1 \\ b_i = 1}} A_b; \\ 0, & otherwise. \end{cases}$$

where $A_b = \{\xi^i \mid 2^{k-m}b \le i \le 2^{k-m}(b+1) - 1\}$. Then

$$F(x) = (f_0(x), f_1(x), \cdots, f_{m-1}(x)) : \mathbb{F}_{2^n} = \mathbb{F}_{2^k}^* \times U \bigcup \{0\} \longrightarrow \mathbb{F}_{2^m}.$$

Theorem 4. *The (n, m)-Boolean function defined in Construction 1 is a vectorial hyper-bent function, and $AI(F) \ge D_{N_1}(n, A)$, where $N_1 = 2^k - 1$, $A = [\frac{2^k+1}{2^m}] = 2^{k-m}$.*

Proof. 1. hyper-bentness

We will prove $F_v = \sum\limits_{i=0}^{m-1} v_i f_i$ is a hyper-bent function, $\forall v \in \mathbb{F}_{2^m}^*$. Following the definition of f_i, we get

$$F_v(x) = F_v(yz) = \begin{cases} 1, & y \in \mathbb{F}_{2^k}^*,\ z \in \bigcup\limits_{\substack{0 \le b \le 2^m-1 \\ \bar{v}\bar{b} = 1}} A_b; \\ 0, & \text{otherwise.} \end{cases}$$

then

$$\begin{aligned} F_v(\alpha^{2^k+1} \cdot x) &= F_v(\alpha^{2^k+1} \cdot yz) \\ &= F_v(y' \cdot z) \qquad where\ y' = \alpha^{2^k+1} \cdot y \in \mathbb{F}_{2^k}^* \end{aligned}$$

However, $F_v(y' \cdot z) = 1$ if and only if $y \in \mathbb{F}_{2^k}^*$ and $z \in \bigcup\limits_{\bar{v}\bar{b}=1} A_b$, so $F_v(\alpha^{2^k+1} \cdot x) = F_v(y' \cdot z) = F_v(y \cdot z) = F_v(x)$, $\forall v \in \mathbb{F}_{2^m}^*$. There are 2^{m-1} solutions(i.e., $\bar{b}$) for $\bar{v} \cdot \bar{b} = 1$, that is, the number of i such that $F_v(\xi^i) = 1$ is $2^{m-1} \cdot 2^{k-m} = 2^{k-1}$. By Proposition 1, we know F_v is hyper-bent, hence F is a vectorial hyper-bent function.

2. algebraic immunity

F is a special case of the function defined in Theorem 2 with $G_1 = \mathbb{F}_{2^k}^*$ and $G_2 = U$, thus $AI(F) \ge D_{N_1}(n, A)$, where $N_1 = 2^k - 1$, $A = [\frac{2^k+1}{2^m}] = 2^{k-m}$. From the results of some small k we have checked(see Table 1), $D_{2^k-1}(n, 2^{k-m})$ is very close to $d(n, m)$ and some can even equal $d(n, m)$.

Table 1. The corresponding values of $d^* = D_{2^k-1}(n, 2^{k-m})$ and $d(n,m)$ for small k and m

(k,m)	(7,4)	(7,5)	(8,3)	(8,4)	(8,5)	(8,6)
d^*	4	3	5	4	4	3
$d(n,m)$	4	4	6	5	4	4
(k,m)	(9,3)	(9,4)	(9,5)	(9,7)	(9,8)	(10,3)
d^*	6	5	4	3	2	7
$d(n,m)$	7	6	5	4	4	7
(k,m)	(10,4)	(10,5)	(10,6)	(10,7)	(10,8)	(11,3)
d^*	6	5	4	4	3	8
$d(n,m)$	7	6	5	5	4	8
(k,m)	(11,4)	(11,5)	(11,6)	(11,7)	(11,8)	
d^*	7	6	5	4	4	
$d(n,m)$	7	7	6	5	5	

Although the (n,m)-Boolean function F defined in Construction 1 has high algebraic immunity, it's not balanced due to the hyper-bent property and the algebraic degree is too low (compared with $n-1$). We hope to find some functions which are balanced and with optimal algebraic degree. By the proof of Theorem 4, we know $\mathcal{P} = \{P_0, \cdots, P_{2^m-1}\}$ is a d-base algebraic immunity of $\mathbb{F}_{2^n}$, where $P_i = \{yz : y \in \mathbb{F}_{2^k}^*,\ z \in A_i\}$, $d = D_{2^k-1}(n, 2^{k-m})$. According to Lemma 1, if we can construct some functions whose 2^m-division of their preimage sets contain $\mathcal{P}$, then those functions have algebraic immunity greater than $AI(F)$. To achieve such goal, we only need to add the elements in $\mathbb{F}_{2^n} \backslash \mathcal{P}$ into A_i arbitrarily. And hence we obtain a large number of (n,m)-Boolean functions with high algebraic immunity from F.

Theorem 5. *We can derive* $(2^m!) \cdot 2^{m2^k}$ (n,m)*-Boolean functions from the one defined in Construction 1, whose algebraic immunities are greater than* $D_{2^k-1}(n, 2^{k-m})$*. Among them there are* $(2^m!) \cdot \frac{2^k!}{(2^{k-m}!)^{2^m}}$ *balanced functions.*

Proof. As $\mathcal{P} = \{P_0, \cdots, P_{2^m-1}\}$, $P_i = \{yz : y \in \mathbb{F}_{2^k}^*,\ z \in A_i\}$ is a d-base algebraic immunity of $\mathbb{F}_{2^n}$, we can get a new function by adding the elements in $Q = \mathbb{F}_{2^n} \backslash \mathcal{P} = \mathbb{F}_{2^k}^* \times \{1\} \bigcup \{0\}$ arbitrarily. There are $(2^m)^{\#Q} = (2^m)^{2^k} = 2^{m2^k}$ ways to do this. Moreover, there are $\frac{2^k!}{(2^{k-m}!)^{2^m}}$ ways to assign those $\#Q = 2^k$ numbers to P_i equally. Every assignment corresponds to a different balanced (n,m)-Boolean function.

For division $\mathcal{P} = \{P_0, \cdots, P_{2^m-1}\}$, if we re-permutate those P_i, we can get another division $\mathcal{P}' = \{P_{\tau(1)}, \cdots, P_{\tau(2^m-1)}\}$, where $\tau : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, τ is a bijection(or permutation). There are $2^m!$ such permutations in all, and obviously $\mathcal{P}'$ is a d-base algebraic immunity of $\mathbb{F}_{2^n}$.

Thus by Construction 1, we can get $(2^m!) \cdot 2^{m2^k}$ (n,m)-Boolean functions whose algebraic immunity are greater than $D_{2^k-1}(n, 2^{k-m})$. Among them $(2^m!) \cdot \frac{2^k!}{(2^{k-m}!)2^m}$ ones are balanced.

In the next subsection, we will find some balanced (n,m)-Boolean functions with optimal algebraic degree (i.e., $n-1$) among those vectorial Boolean functions mentioned in Theorem 5.

4.2 Construction of balanced high algebraic immunity (n,m)-Boolean function with optimal algebraic degree

Construction 2 *Let $1 \leq m \leq k$, $n = 2k \geq 4$, β be a primitive element of $\mathbb{F}_{2^k}^*$, $F'(x) = F(x) + G(x) : \mathbb{F}_{2^n} = \mathbb{F}_{2^k}^* \times U \bigcup \{0\} \longrightarrow \mathbb{F}_{2^m}$, where F is the (n,m)-Boolean function defined in Construction 1, and $G(x) = G(yz) = (g_0(yz), \ldots, g_{m-1}(yz)) : \mathbb{F}_{2^n} = \mathbb{F}_{2^k}^* \times U \bigcup \{0\} \longrightarrow \mathbb{F}_{2^m}$, $y \in \mathbb{F}_{2^k}^*$, $z \in U$, defined by*

$$g_i(x) = g_i(yz) = \begin{cases} 1, y \in \bigcup\limits_{\substack{0 \leq b \leq 2^m-1 \\ b_i=1}} C_b, \ z = 1; \\ 0, otherwise. \end{cases}$$

where $C_b = \{\beta^i \mid 2^{k-m}b \leq i \leq 2^{k-m}(b+1) - 1\}$, $0 \leq i \leq m-1$.

Theorem 6. *F' defined in Construction 2 is a balanced (n,m)-function with optimal algebraic degree satisfying $AI(F') \geq D_{2^k-1}(n, 2^{k-m})$.*

Proof. First, we show that F' is balanced. For all $b \in \mathbb{F}_{2^k}$,

$$\begin{aligned} x \in F^{-1}(b) &\Leftrightarrow y \in \mathbb{F}_{2^k}^*, \ z \in A_b \\ x \in G^{-1}(b) &\Leftrightarrow g_i(x) = g_i(yz) = b_i \qquad (0 \leq i < m) \\ &\Leftrightarrow y \in \bigcap \{C_c \mid 0 \leq c \leq 2^m - 1, \ c_i = b_i\}, \ z = 1 \\ &\Leftrightarrow y \in C_b, \ z = 1. \end{aligned}$$

Since $F^{-1}(b) \bigcap G^{-1}(b) = \emptyset$, thus $\left|F'^{-1}(b)\right| = \left|F^{-1}(b)\right| + \left|G^{-1}(b)\right| = (2^k - 1) \times 2^{k-m} \times 2^{m-1} + 2^{k-m} \times 2^{m-1} = 2^{2k-1} = 2^{n-1}$.

Second, we compute the algebraic immunity of F' as follows. By the proof for Theorem 4, we know $\mathcal{P} = \{A_0, \cdots, A_{2^m-1}\}$ is a M-subdivision of $\mathbb{F}_{2^n}$, where $M = 2^m$. Let $\mathcal{R} = \{D_0, \cdots, D_{2^m-1}\}$ be a M-division of $\mathbb{F}_{2^n}$, where $D_i = A_i \bigcup C_i$, $0 \leq i \leq 2^m - 1$. $\mathcal{R}$ is the preimage set of F' that makes up a division of $\mathbb{F}_{2^n}$. It's easy to check $\mathcal{P} \preccurlyeq \mathcal{R}$, then $AI(\mathcal{P}) \leq AI(\mathcal{R})$. Thus $AI(F') \geq AI(F) \geq D_{2^k-1}(n, 2^{k-m})$.

At last, we prove that F' has optimal algebraic degree. Let $F'(x) = F(x) + G(x)$, $F(x)$ be a hyper-bent vectorial function, then $Deg(F(x)) = \frac{n}{2} = k$. We only need to compute the algebraic degree of $G(x)$. Consider the coefficient of

item $x^r = y^i z^j$ in $G(x)$, where $r = 2^n - 2,\ i = r \mod 2^k - 1 = 2^k - 2,\ j = r \mod 2^k + 1 = 2^k$.

$$\begin{aligned} g_i(x) = g(yz) = &\sum_{\gamma \in C_i,\ \delta = 1} (1 + (y+\gamma)^{2^k-1})((1 + (z+\delta)^{2^k+1})) \\ =&(1 + (z+1)^{2^k+1}) \sum_{\gamma \in C_i} (1 + (y+\gamma)^{2^k-1}) \\ =&(1 + (z+1)^{2^k+1}) \sum_{\gamma \in C_i} \sum_{\lambda=0}^{2^k-2} \gamma^\lambda y^{2^k-1-\lambda} \\ =&(1 + (z+1)^{2^k+1}) \sum_{\lambda=1}^{2^k-2} y^{2^k-1-\lambda} \sum_{\gamma \in C_i} \gamma^\lambda \end{aligned}$$

where $C_i = \bigcup_{\substack{0 \le b \le 2^m-1 \\ b_i = 1}} C_b$, $\sum_{\lambda \in C_i} 1 = \mid C_i \mid = 2^{k-1} = 0 \in \mathbb{F}_2$. The coefficient of item $y^{2^k-2} z^{2^k}$ is $\sum_{\lambda \in C_i} \lambda$. By Eq. (8) in [8],

$$\sum_{\lambda \in C_i} \lambda = \beta^{-1}(1+\beta)^{2^k-1} (\frac{\beta}{1+\beta})^{(2^{k-m+i})} \neq 0$$

Then, for any i, $0 \le i \le m-1$, $\deg(g_i(x)) \ge wt(2^n - 2) = n - 1$, which means $\deg(G(x)) \ge n - 1$. By the balancedness of $F'(x) = F(x) + G(x)$ and $Deg(F(x)) = k = \frac{n}{2}$, $Deg(F'(x)) \le n - 1$, we obtain $Deg(F'(x)) = n - 1$.

5 Conclusion

Based on the decomposition of $\mathbb{F}_{2^n}^*$, we give a generalize way to construct a class of vectorial Boolean functions with high algebraic immunity. Then, under the polar decomposition of $\mathbb{F}_{2^{2k}}^*$, we construct two class of vectorial Boolean functions with high algebraic immunity over $\mathbb{F}_{2^{2k}}$: one is hyper-bent and the other is of balancedness and optimal algebraic degree .

References

1. M. Albrecht, Algebraic Attacks on the Courtois Toy Cipher, Journal Cryptologia archive, Volume 32 Issue 3, July 2008, pp. 220-276.
2. F. Armknecht, Improving fast algebraic attacks, in 11th International Workshop on Fast Software Encryption, FSE 2004. Lecture Notes in Computer Science, vol. 3017, pp.65-82 (2004).
3. F. Armknecht and M. Krause, Constructing Single- and Multi-output Boolean Functions with Maximal Algebraic Immunity, In ICALP 2006, Lecture Notes in Computer Science, 2006, Volume 4052/2006.

4. T.P. Berger and M. Minier, Two Algebraic Attacks Against the F-FCSRs Using the IV Mode, In INDOCRYPT(2005)143-154.
5. 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 (Peter Hammer and Yves Crama editors), pp. 257-397, 2010.
6. C. Carlet, Vectorial Boolean Functions for Cryptography, In Carma, Y.Hammer, P.(eds.) Boolean Methods and Models. Cambridge Univ. Press, Cambridge.
7. C. Carlet and K. Feng, An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity, in Advances in Cryptology-ASIACRYPT 2008 (Lecture Notes in Computer Science), Springer-Verlag, vol. 5350, pp. 425-440, 2008.
8. C. Carlet and K. Feng, An Infinite Class of Balanced Vectorial Boolean Functions with optimal Algebraic Immunity and Good Nonlinearity,CODING AND CRYPTOLOGY, Lecture Notes in Computer Science, 2009, Volume 5557/2009, 1-11, DOI: 10.1007/978-3-642-01877-0_1.
9. C. Carlet and P. Gabority, Hyperbent funcitons and cyclic codes, Journal of Combinatorial Theory, Series A, Volume 113, Issue 3, April 2006, pp. 466-482.
10. P. Charpin and G. Gong, Hyperbent functions, Kloosterman sums, and Dickson polynomials, IEEE Transactions on Information Theory, 54(9):4230-4238, 2008.
11. J. Y. Cho and J. Pieprzyk, Algebraic attacks on SOBER-t32 and SOBER-t16 without stuttering, Lecture Notes in Computer Science : Fast Software Encryption (2004), pp. 49-64.
12. N. Courois and W. Meier, Algebraic attack on stream ciphers with linear feedback, in Advances in Cryptology - EUROCRYPTO 2003 (Lecture Notes in Computer Science), Springer-Verlag, vol. 2656, pp. 345-359, 2003.
13. N. Courtois, G. Bard and D. Wagner, Algebraic and Slide Attacks on KeeLoq, in Fast Software Encryption (2008), pp. 97-115, DOI:10.1007/978-3-540-71039-4_6.
14. X. Duan, Proof of a Combinatoric Conjecture, Procedia Engineering 29(2012), pp.2793-2797.
15. K. Feng and J. Yang, Vectorial Boolean Functions with Good Cryptographic Properties, International Journal of Foundations of Computer Science,Vol.22, No 6(2011) 1271-1282, DOI:10.1142/S0129054111008702.
16. F.J. MacWilliams and N.J. Sloane, The theory of error-correcting codes, North-Holland, Amsterdam (1977).
17. W. Meier , E. Pasalic and C. Carlet, Algebraic attacks and decomposition of boolean functions, in Advances in Cryptology, Eurocrypt 2004. Lecture Notes in Computer Science, vol. 3027, pp. 474-491 (2004).
18. O. S. Rothaus, On bent functions, J. Combin. Theory, ser. A, vol. 20, pp. 300-305, 1976.
19. D. Tang, C.Carlet and X. Tang, Highly Nonlinear Boolean Functions with Optimal Algebraic Immunity and Good Behavior Against Fast Algebraic Attacks, IACR Cryptology ePrint Archive 2011: 366 (2011).
20. Z. Tu and Y. Deng, A conjecture about binary strings and its applications on construciong Boolean functions with optimal algebraic mmunity, DESIGNS, CODES AND CRYPTOGRAPHY,Volume 60, Number 1, 1-14, DOI: 10.1007/s10623-010-9413-9.
21. A. M. Youssef and G. Gong, Hyper-bent functions, in Advances in Crypology C Eurocrypt01, 2001, LNCS, pp. 406-419