Des. Codes Cryptogr. (2014) 72:653–673
DOI 10.1007/s10623-013-9801-z

A systematic method of constructing Boolean functions with optimal algebraic immunity based on the generator matrix of the Reed–Muller code

Sihong Su · Xiaohu Tang · Xiangyong Zeng

Received: 25 March 2012 / Revised: 17 November 2012 / Accepted: 16 January 2013 /
Published online: 1 February 2013

Abstract Because of the recent algebraic attacks, optimal algebraic immunity is now an absolutely necessary (but not sufficient) property for Boolean functions used in stream ciphers. In this paper, we firstly determine the concrete coefficients in the linear expression of the column vectors with respect to a given basis of the generator matrix of Reed–Muller code, which is an important tool for constructing Boolean functions with optimal algebraic immunity. Secondly, as applications of the determined coefficients, we provide simpler and direct proofs for two known constructions. Further, we construct new Boolean functions on odd variables with optimal algebraic immunity based on the generator matrix of Reed–Muller code. Most notably, the new constructed functions possess the highest nonlinearity among all the constructions based on the generator matrix of Reed–Muller code, although which is not as good as the nonlinearity of Carlet–Feng function. Besides, the ability of the new constructed functions to resist fast algebraic attacks is also checked for the variable $n = 11$, 13 and 15.

Keywords Boolean functions · Algebraic immunity · Reed–Muller code · Generator matrix · Nonlinearity

---

Communicated by C. Carlet.

S. Su (✉) · X. Tang
Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, Chengdu 610031, China
e-mail: sush@henu.edu.cn

X. Tang
e-mail: xhutang@swjtu.edu.cn

S. Su
School of Mathematics and Information Sciences, Henan University, Kaifeng 475004, China

X. Zeng
Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China
e-mail: xiangyongzeng@yahoo.com.cn

Mathematics Subject Classification (2000) 94A60 · 05B10

1 Introduction

In recent years, there has been great interest in designing symmetric key algorithms for secure communication among devices with restrictions on memory, computing power, etc. Boolean functions play a critical role in cryptography, particularly as a main block of symmetric key algorithms. To resist the known attacks, many criteria have been developed for designing Boolean functions. Cryptographic Boolean functions usually should have balancedness, large algebraic degree, and high nonlinearity before 2003. In 2003, Courtois and Meier successfully proposed algebraic attacks on several stream ciphers [10]. As a result, a new criterion called algebraic immunity [22], the minimum algebraic degree of the nonzero annihilators of f or $f+1$, was imposed on cryptographic Boolean functions. It was shown in [10] that the optimal algebraic immunity of an n-variable Boolean function is $\lceil \frac{n}{2} \rceil$. The construction of Boolean functions with optimal algebraic immunity is obviously of great importance and therefore attracts a lot of attention [7,11–13,17]. Later, fast algebraic attack [9] was introduced by Courtois. The fast algebraic attack on a Boolean function f is feasible if there exists a function g of small degree such that the multiple gf has degree not too large. Another important characteristic for designing Boolean functions is good nonlinearity which measures the ability of the functions to resist fast correlation attacks [21].

Among the known Boolean functions with optimal algebraic immunity, the simplest one is the so-called majority function

$$F(x) = \begin{cases} 1, & \mathrm{wt}(x) \geq \lceil \frac{n}{2} \rceil \\ 0, & \text{otherwise} \end{cases}$$

which was firstly proposed by Ding et al. [15]. In 2006, Dalai et al. [14] showed that the majority function $F(x)$ achieves the optimal algebraic immunity. However, the nonlinearity of majority function is $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$, which is almost the worst possible value according to Lobanov's bound [20].

In 2005, Carlet et al. pointed out an interesting connection between the Boolean functions with optimal algebraic immunity and the Reed–Muller codes [6]. They presented a sufficient and necessary condition for constructing Boolean functions with optimal algebraic immunity based on the generator matrix of Reed–Muller code. Later, in 2007, Carlet [3] introduced a general method for constructing balanced Boolean functions on odd number of variables with optimal algebraic immunity, which can be viewed as a modification of the majority function. From then on, following this idea, many modifications of majority function have been proposed to improve its nonlinearity [4,8,16,19,24,25]. But, unfortunately the enhanced values are not too much.

In this paper, we explore the linear relationship of the column vectors in the generator matrix of Reed–Muller code. Mainly, we can give a systematic method of constructing Boolean functions with optimal algebraic immunity based on the generator matrix of Reed–Muller code. As an application, we are able to construct new Boolean functions with optimal algebraic immunity and highest nonlinearity among all the constructions based on the generator matrix of Reed–Muller code.

The paper is organized as follows. In Sect. 2, some preliminaries about the n-variable Boolean functions, the kth order Reed–Muller code $\mathrm{RM}(k, n)$ and its generator matrix $G(k, n)$ are reviewed. In Sect. 3, the linear expression of the column vectors in the generator matrix of RM(k, n) is established. In Sect. 4, a general method for constructing Boolean functions with optimal algebraic immunity is presented based on the determined linear expression. As applications, some known constructions are re-explained, and a new construction of Boolean functions with optimal algebraic immunity and high nonlinearity is presented as well. Finally, Sect. 5 concludes the paper.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the finite field $\mathbb{F}_2 = \{0, 1\}$. Given a vector $\alpha = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n$, we define its support supp(α) as the set $\{1 \le i \le n \,|\, a_i = 1\}$, and its Hamming weight wt(α) as the cardinality of its support, i.e., wt$(\alpha) = |\text{supp}(\alpha)|$.

For any two vectors $\alpha = (a_1, a_2, \ldots, a_n)$ and $\beta = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_2^n$, α is said to be covered by β if $a_i \le b_i$ for all $1 \le i \le n$. For short, written as $\alpha \preceq \beta$. In this paper, we define $\beta^\alpha = b_1^{a_1} b_2^{a_2} \cdots b_n^{a_n}$ with $0^0 = 1^1 = 1^0 = 1$ and $0^1 = 0$. Obviously,

$$\beta^\alpha = 1 \text{ if and only if } \alpha \preceq \beta. \tag{1}$$

A Boolean function on n variables is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. We denote by $\mathcal{B}_n$ the set of all n-variable Boolean functions. In cryptography, the most usual representation of a function $f \in \mathcal{B}_n$ is the algebraic normal form (ANF) as follows

$$f(x) = \bigoplus_{\alpha \in \mathbb{F}_2^n} c(\alpha) x^\alpha \tag{2}$$

where $c(\alpha) \in \mathbb{F}_2$.

For a function $f \in \mathcal{B}_n$, the support of f is supp$(f) = \{\alpha \in \mathbb{F}_2^n | f(\alpha) = 1\}$. By convenience, define zeros$(f) = \{\alpha \in \mathbb{F}_2^n | f(\alpha) = 0\}$ as well. The Hamming weight of f, wt(f), is the cardinality of its support. We say that a Boolean function f is balanced if wt$(f) = 2^{n-1}$. The Hamming distance between f and $g \in \mathcal{B}_n$ is $d_H(f, g) = \text{wt}(f \oplus g)$. The algebraic degree of a Boolean function f in (2) is defined as

$$\deg(f) = \max\{\text{wt}(\alpha) \,|\, c(\alpha) = 1\}.$$

If $\deg(f) \le 1$, then f is called an affine function.

Definition 1 ([22]) For an n-variable Boolean function f, define $AN(f) = \{g \in \mathcal{B}_n | fg = 0\}$. A Boolean function $g \in AN(f)$ is called an annihilator of f. The algebraic immunity (AI) of an n-variable Boolean function f, denoted by $AI(f)$, is defined as $AI(f) = \min\{\deg(g) | g \ne 0 \text{ such that } fg = 0 \text{ or } (f+1)g = 0\}$.

In this paper, an n-variable Boolean function f is said to have optimal AI if $AI(f) = \lceil \frac{n}{2} \rceil$ (see [10]). A high algebraic immunity is necessary but not sufficient condition for resistance against all kinds of algebraic attacks. If one can find g of low degree and $h \ne 0$ of reasonable degree such that $fg = h$, then a fast algebraic attack is feasible [1,9,18]. An n-variable Boolean function can be considered as optimal with respect to fast algebraic attacks if there do not exist two nonzero functions g and h such that $fg = h$ and $\deg(g) + \deg(h) < n$ with $\deg(g) < \frac{n}{2}$.

Walsh spectrum is an important tool for studying Boolean functions. The Walsh spectrum of an n-variable Boolean function f is a integer-valued function over $\mathbb{F}_2^n$ defined as

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus x \cdot \omega} \tag{3}$$

where $x \cdot \omega = x_1 a_1 \oplus x_2 a_2 \oplus \cdots \oplus x_n a_n$ for $x = (x_1, x_2, \ldots, x_n)$ and $\omega = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n$. The nonlinearity of f is the minimum Hamming distance between f and all affine functions, which can be expressed according to Walsh spectrum as

$$nl_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|. \tag{4}$$

Throughout this paper, assume that $\alpha_1, \alpha_2, \ldots, \alpha_{2^n}$ are all the 2^n vectors in $\mathbb{F}_2^n$, which are ordered according to the Hamming weight firstly and the lexicographic order secondly, i.e., $\alpha_1 = (0, 0, 0, \ldots, 0)$, $\alpha_2 = (1, 0, 0, \ldots, 0)$, $\alpha_3 = (0, 1, 0, \ldots, 0)$, $\ldots$, $\alpha_{n+1} = (0, 0, 0, \ldots, 0, 1)$, $\alpha_{n+2} = (1, 1, 0, \ldots, 0)$, $\alpha_{n+3} = (1, 0, 1, 0, \ldots, 0)$, $\alpha_{n+4} = (1, 0, 0, 1, \ldots, 0)$, $\ldots$, $\alpha_{\binom{n}{2}+n+1} = (0, \ldots, 0, 1, 1)$, $\ldots$, $\alpha_{2^n} = (1, 1, 1, \ldots, 1)$. Then, it is easy to see that $\mathrm{wt}(\alpha_i) \le k$ if and only if $1 \le i \le \sum_{j=0}^{k} \binom{n}{j}$. Hence, the ANF of a Boolean function f with $\deg(f) \le k$ can be expressed as

$$f(x) = \bigoplus_{i=1}^{s} c(\alpha_i) x^{\alpha_i} \tag{5}$$

where $s = \sum_{i=0}^{k} \binom{n}{i}$ and $c(\alpha_i) \in \mathbb{F}_2$, since $\deg(x^{\alpha_i}) \le k$ if and only if $\mathrm{wt}(\alpha_i) \le k$.

The truth table is another representation of a Boolean function. In this paper, for convenience, the truth table of a Boolean function f is of the following form

$$f = [f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_{2^n})].$$

Reed–Muller codes are amongst the oldest and most popular codes. They were discovered by Muller and Reed in 1954 [23,26]. The Reed–Muller code of order k, $1 \le k \le n$, is by definition the set of all n-variable Boolean functions with algebraic degrees at most k, denoted by $\mathrm{RM}(k, n)$. Clearly, it is a vector space of dimension $\sum_{i=0}^{k} \binom{n}{i}$ over $\mathbb{F}_2$, with monomials of degrees at most k, i.e., $\left\{ x^{\alpha_i} \,\middle|\, 1 \le i \le \sum_{j=0}^{k} \binom{n}{j} \right\}$, denoted by Γ_k, as its basis.

Define a mapping $\psi : \Gamma_k \to \mathbb{F}_2^{2^n}$

$$\psi(x^{\alpha_i}) = \left[{\alpha_1}^{\alpha_i}, {\alpha_2}^{\alpha_i}, \ldots, {\alpha_{2^n}}^{\alpha_i} \right]$$

which is the truth table of x^{α_i}, for $1 \le i \le \sum_{j=0}^{k} \binom{n}{j}$. Consider the following $\sum_{i=0}^{k} \binom{n}{i} \times 2^n$ matrix as

$$G(k, n) = \begin{pmatrix} \psi(x^{\alpha_1}) \\ \psi(x^{\alpha_2}) \\ \vdots \\ \psi(x^{\alpha_s}) \end{pmatrix} = \begin{pmatrix} {\alpha_1}^{\alpha_1} & {\alpha_2}^{\alpha_1} & \cdots & {\alpha_{2^n}}^{\alpha_1} \\ {\alpha_1}^{\alpha_2} & {\alpha_2}^{\alpha_2} & \cdots & {\alpha_{2^n}}^{\alpha_2} \\ \vdots & \vdots & & \vdots \\ {\alpha_1}^{\alpha_s} & {\alpha_2}^{\alpha_s} & \cdots & {\alpha_{2^n}}^{\alpha_s} \end{pmatrix} \tag{6}$$

where $s = \sum_{i=0}^{k} \binom{n}{i}$. Note that if $k = \lceil \frac{n}{2} \rceil - 1$ then $\sum_{i=0}^{k} \binom{n}{i}$ equals 2^{n-1} when n is odd, and $2^{n-1} - \binom{n-1}{\frac{n}{2}}$ otherwise. By means of the matrix $G(k, n)$, it is easy to check that any function $f \in \mathcal{B}_n$ with $\deg(f) \le k$, given by (5), can be expressed as follows

$$[f(\alpha_1), \ldots, f(\alpha_{2^n})] = [c(\alpha_1), \ldots, c(\alpha_s)] G(k, n).$$

That is, $G(k, n)$ is a generator matrix of the Reed–Muller code $\mathrm{RM}(k, n)$.

For instance, when $n = 3$, the vectors in $\mathbb{F}_2^3$ are $\alpha_1 = (0, 0, 0)$, $\alpha_2 = (1, 0, 0)$, $\alpha_3 = (0, 1, 0)$, $\alpha_4 = (0, 0, 1)$, $\alpha_5 = (1, 1, 0)$, $\alpha_6 = (1, 0, 1)$, $\alpha_7 = (0, 1, 1)$, $\alpha_8 = (1, 1, 1)$. By (1) and (6), the generator matrix of the Reed–Muller code RM(1, 3) is

$$G(1,3)=\begin{pmatrix}1&1&1&1&1&1&1&1\\0&1&0&0&1&1&0&1\\0&0&1&0&1&0&1&1\\0&0&0&1&0&1&1&1\end{pmatrix}.$$

Throughout this paper, given an n-variable Boolean function f and a positive integer $k \le n$, we denote by G the generator matrix $G(k,n)$ of the kth order Reed–Muller code $\mathrm{RM}(k,n)$, and denote by $R_f^{(1)}(k,n)$ (resp. $R_f^{(0)}(k,n)$) the submatrix of G consisting of all the ith column vectors in G, $1 \le i \le 2^n$, such that $\alpha_i \in \mathrm{supp}(f)$ (resp. $\alpha_i \in \mathrm{zeros}(f)$). It is easily seen that the matrix $R_f^{(1)}(k,n)$ (resp. $R_f^{(0)}(k,n)$) has $\sum_{i=0}^{k}\binom{n}{i}$ rows and $\mathrm{wt}(f)$ (resp. $2^n-\mathrm{wt}(f)$) columns.

Concerning a function $f \in \mathcal{B}_n$ with optimal AI, we have following sufficient and necessary conditions.

Proposition 1 ([2,6]) *Let $k=\lceil \frac{n}{2}\rceil-1$. A function $f \in \mathcal{B}_n$ with $\mathrm{wt}(f)=\sum_{i=0}^{k}\binom{n}{i}$ (resp. $\mathrm{wt}(f)=2^n-\sum_{i=0}^{k}\binom{n}{i}$) has optimal AI if and only if the $\sum_{i=0}^{k}\binom{n}{i}\times\sum_{i=0}^{k}\binom{n}{i}$ matrix $R_f^{(1)}(k,n)$ (resp. $R_f^{(0)}(k,n)$) is nonsingular.*

Finally, it should be noted that in this paper for simplicity we do not distinguish the vector $Y=(y_1,\ldots,y_n)\in\mathbb{F}_2^n$ and the integer $y=\sum_{i=1}^{n}y_i2^{i-1}$ if the context is clear, since they are one-to-one corresponding. Then, we can similarly define $x \preceq y$ for two integers $x, y \in \{0,1,\ldots,2^n-1\}$ and $X \le Y$ for two vectors $X, Y \in \mathbb{F}_2^n$.

3 The linear expression of the column vectors in G

From now on, we always assume $k=\lceil \frac{n}{2}\rceil-1$ and $s=\sum_{i=0}^{k}\binom{n}{i}$ in this paper.

By (6), we know that the jth column vector in the generator matrix G can be expressed as $({\alpha_j}^{\alpha_1},{\alpha_j}^{\alpha_2},\ldots,{\alpha_j}^{\alpha_s})^T$, $1\le j\le 2^n$. For simplicity, we will always use the notation c_{α_j} to denote the jth column vector in G, i.e.

$$c_{\alpha_j}=({\alpha_j}^{\alpha_1},{\alpha_j}^{\alpha_2},\ldots,{\alpha_j}^{\alpha_s})^T.$$

Thus, the generator matrix G in (6) can be written as

$$G=(c_{\alpha_1},c_{\alpha_2},\ldots,c_{\alpha_{2^n}}).$$

In order to find a function $f\in\mathcal{B}_n$ with $\mathrm{wt}(f)=s$ and optimal AI, by Proposition 1, it is necessary to get a submatrix $R_f^{(1)}(k,n)$ of G with rank s. In this section, we will explore the linear expression of the column vectors in G with respect to this basis $(c_{\alpha_1},c_{\alpha_2},\ldots,c_{\alpha_s})$, which is very useful to check whether the new submatrix of G is of rank s.

Theorem 1 *For any vector $u\in\mathbb{F}_2^n$, such that $\mathrm{wt}(u)=k+j$, $1\le j\le n-k$, we have*

$$c_u=\bigoplus_{i=0}^{k}a_i^{(j)}\left(\bigoplus_{\substack{\alpha\preceq u\\ wt(\alpha)=k-i}}c_\alpha\right) \tag{7}$$

where $a_i^{(j)}\in\mathbb{F}_2$, $0\le i\le k$, which satisfies

$$a_0^{(j)}=1 \text{ and } a_i^{(j)}=1\oplus\bigoplus_{l=0}^{i-1}a_l^{(j)}\binom{i+j}{i-l},\ 1\le i\le k. \tag{8}$$

Proof Partition the matrix G in (6) into block matrix as $G = (G_{il})_{(k+1)\times(n+1)}$, where G_{il} is a $\binom{n}{i} \times \binom{n}{l}$ matrix, $0 \le i \le k, 0 \le l \le n$. By (6), we know that each entry in G_{il} can be expressed as β^α for some $\alpha, \beta \in \mathbb{F}_2^n$ with $\mathrm{wt}(\alpha) = i$ and $\mathrm{wt}(\beta) = l$. If $i > l$, straightforwardly $\alpha \npreceq \beta$, which follows from (1) that $\beta^\alpha = 0$. Then, G_{il} is a zero matrix for $0 \le l < i \le k$. If $i = l$, it is easy to see that $\beta^\alpha = 1$ if and only if $\alpha = \beta$ by (1), which implies G_{ii} is an identity matrix for $0 \le i \le k$. Therefore, G has the following form

$$G = \begin{pmatrix} I_{d_0} & * & \cdots & * & * \cdots\cdots * \\ 0 & I_{d_1} & \ddots & \vdots & \vdots \qquad\quad \vdots \\ \vdots & \ddots & \ddots & * & \vdots \qquad\quad \vdots \\ 0 & \cdots & 0 & I_{d_k} & * \cdots\cdots * \end{pmatrix} \tag{9}$$

where I_{d_i} is an identity matrix of order $d_i = \binom{n}{i}$ for $0 \le i \le k$, which indicates that the first s column vectors $c_{\alpha_1}, c_{\alpha_2}, \ldots, c_{\alpha_s}$ are linearly independent and then form a basis of $\mathbb{F}_2^s$.

Assume that the linear expression of c_u with $\mathrm{wt}(u) = k + j$ is

$$c_u = \bigoplus_{0\le \mathrm{wt}(\alpha)\le k} a(\alpha)c_\alpha = \bigoplus_{i=1}^{s} a(\alpha_i)c_{\alpha_i} \tag{10}$$

where $a(\alpha_i) \in \mathbb{F}_2,\ 1 \le i \le s$. According to (6) and (9), we know (10) can be rewritten as

$$\begin{pmatrix} I_{d_0} & * & \cdots & * \\ 0 & I_{d_1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & I_{d_k} \end{pmatrix} \begin{pmatrix} a(\alpha_1) \\ a(\alpha_2) \\ \vdots \\ a(\alpha_s) \end{pmatrix} = \begin{pmatrix} u^{\alpha_1} \\ u^{\alpha_2} \\ \vdots \\ u^{\alpha_s} \end{pmatrix}. \tag{11}$$

In what follows, we make use of mathematical induction on i, $0 \le i \le k$, to prove that the coefficients $a(\alpha)$'s in (10) satisfy

I. $a(\alpha) = 0$ for all $\alpha \npreceq u$;
II. $a(\alpha) = a(\beta)$ for all $\alpha, \beta \preceq u$ with $\mathrm{wt}(\alpha) = \mathrm{wt}(\beta)$,

where $\mathrm{wt}(\alpha) = k - i$.

When $i = 0$, we get by (11)

$$I_{d_k} \begin{pmatrix} a(\alpha_t) \\ \vdots \\ a(\alpha_s) \end{pmatrix} = \begin{pmatrix} u^{\alpha_t} \\ \vdots \\ u^{\alpha_s} \end{pmatrix}$$

where $t = \sum_{l=0}^{k-1} \binom{n}{l} + 1$. Note that $\mathrm{wt}(\alpha_l) = k$ for $t \le l \le s$. Hence,

$$a(\alpha) = u^\alpha = \begin{cases} 1, & \alpha \preceq u \\ 0, & \alpha \npreceq u \end{cases}$$

for $\mathrm{wt}(\alpha) = k$, which gives $a_0^{(j)} = 1$. Hence, I and II hold for $i = 0$.

Suppose that the assertions I and II hold for all $k - i + 1 \le \mathrm{wt}(\alpha) \le k$ for some fixed $1 \le i \le k$. Denote the coefficients $a(\alpha)$ with $\alpha \preceq u$ and $\mathrm{wt}(\alpha) = k - l$ by $a_l^{(j)}$, $0 \le l \le i - 1$.

Substituting $a_l^{(j)}$ into (11), we have

$$\begin{pmatrix} I_{d_0} & & * \\ & \ddots & \\ 0 & & I_{d_{k-i}} \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} a(\alpha_1) \\ \vdots \\ \vdots \\ a(\alpha_m) \end{pmatrix} = c_u \oplus \bigoplus_{l=0}^{i-1} \left(\bigoplus_{\substack{v \preceq u \\ \mathrm{wt}(v)=k-l}} a_l^{(j)} c_v \right)$$

where $m = \sum_{l=0}^{k-i} \binom{n}{l}$. For any α with $\mathrm{wt}(\alpha) = k - i$, similarly to the case of $i = 0$, we can easily get

$$a(\alpha) = u^\alpha \oplus \bigoplus_{l=0}^{i-1} \left(\bigoplus_{\substack{v \preceq u \\ \mathrm{wt}(v)=k-l}} a_l^{(j)} v^\alpha \right).$$

If $\alpha \not\preceq u$, immediately $u^\alpha = 0$ and $\alpha \not\preceq v$ (i.e., $v^\alpha = 0$) for any $v \preceq u$, which implies that $a(\alpha) = 0$. If $\alpha \preceq u$, we know that $u^\alpha = 1$ and the number of the vectors $v \in \mathbb{F}_2^n$, satisfying $\alpha \preceq v \preceq u$ and $\mathrm{wt}(v) = k - l$ for $0 \le l \le i - 1$, is $\binom{i+j}{i-l}$, where $\mathrm{wt}(u) = k + j$. As a result,

$$a(\alpha) = 1 \oplus \bigoplus_{l=0}^{i-1} a_l^{(j)} \binom{i+j}{i-l}$$

for any $\alpha \preceq u$ with $\mathrm{wt}(\alpha) = k - i$. This finishes the proof. □

Further, we can determine the exact value of the coefficient $a_i^{(j)}$ in (7) based on the well-known combinatorial formula (Pascal's Formula) as

$$\binom{m}{p} + \binom{m}{p+1} = \binom{m+1}{p+1}.$$

Theorem 2 *For $1 \le j \le n - k$, let u be a vector in $\mathbb{F}_2^n$ with $\mathrm{wt}(u) = k + j$. In the linear expression of c_u in (7), the coefficients $a_i^{(j)}$ of c_α with $\alpha \preceq u$ and $\mathrm{wt}(\alpha) = k - i$ satisfy*

$$a_i^{(j)} = \binom{i+j-1}{i} \pmod 2 \tag{12}$$

for $0 \le i \le k$ and $1 \le j \le n - k$.

Proof We use mathematical induction on j and i to prove (12).

When $j = 1$, it is known that $a_0^{(1)} = 1$ by (8). Assume that $a_1^{(1)} = \cdots = a_{i-1}^{(1)} = 1$, then by (8) we have

$$a_i^{(1)} = 1 \oplus \bigoplus_{l=0}^{i-1} \binom{i+1}{i-l} = 2^{i+1} - 1 = 1 \pmod 2.$$

In other words, we have proved (12) holds for $j = 1$.

Suppose that $a_i^{(j-1)} = \binom{i+j-2}{i} \pmod 2$ for $0 \le i \le k$. As for j, we know $a_0^{(j)} = 1 = \binom{j-1}{0}$. Assuming that (12) holds up to $i-1$, then by (8) we know

$$\begin{aligned}
a_i^{(j)} &= 1 \oplus \bigoplus_{l=0}^{i-1} \binom{l+j-1}{l}\binom{i+j}{i-l} \\
&= 1 \oplus \bigoplus_{l=0}^{i-1} \binom{l+j-1}{l}\left[\binom{i+j-1}{i-l} \oplus \binom{i+j-1}{i-l-1}\right] \\
&= 1 \oplus \left[\binom{i+j-1}{i} \oplus \bigoplus_{l=1}^{i-1} \binom{l+j-1}{l}\binom{i+j-1}{i-l}\right] \oplus \left[\bigoplus_{l=0}^{i-2} \binom{l+j-1}{l}\binom{i+j-1}{i-l-1} \oplus \binom{i+j-2}{i-1}\right] \\
&= 1 \oplus \binom{i+j-1}{i} \oplus \bigoplus_{l=1}^{i-1} \left[\binom{l+j-1}{l} \oplus \binom{l+j-2}{l-1}\right]\binom{i+j-1}{i-l} \oplus \binom{i+j-2}{i-1} \\
&= 1 \oplus \binom{i+j-1}{i} \oplus \bigoplus_{l=1}^{i-1} \binom{l+j-2}{l}\binom{i+j-1}{i-l} \oplus \binom{i+j-2}{i-1} \\
&= 1 \oplus \bigoplus_{l=0}^{i-1} \binom{l+j-2}{l}\binom{i+j-1}{i-l} \oplus \binom{i+j-2}{i-1} \\
&= \binom{i+j-2}{i} + \binom{i+j-2}{i-1} \\
&= \binom{i+j-1}{i} \pmod 2
\end{aligned}$$

where we apply Pascal's Formula to the second identity, the fifth identity, and the eighth identity respectively, and in the seventh identity we use

$$a_i^{(j-1)} = 1 \oplus \bigoplus_{l=0}^{i-1} a_l^{(j-1)} \binom{i+j-1}{i-l}$$

from (8) and the assumption that (12) is valid for $j-1$.

This finishes the proof. □

4 The applications

In the remainder of this paper, for simplicity we denote $W^{\le i} = \{\alpha \in \mathbb{F}_2^n | \mathrm{wt}(\alpha) \le i\}$, $W^{\ge i} = \{\alpha \in \mathbb{F}_2^n | \mathrm{wt}(\alpha) \ge i\}$, and $W^i = \{\alpha \in \mathbb{F}_2^n | \mathrm{wt}(\alpha) = i\}$, for $0 \le i \le n$.

By Proposition 1, constructing an n-variable Boolean function f with $\mathrm{wt}(f) = s$ and optimal AI is equivalent to find out a nonsingular $s \times s$ submatrix of the generator matrix G given in (6). For example, $[c_{\alpha_1}, \dots, c_{\alpha_s}]$ is such a submatrix. Naturally, a general approach is to modify it and then get another nonsingular one. More precisely, for an integer $1 \le l \le s$, choose two vector subsets $U = \{u_1, \dots, u_l\} \subseteq W^{\ge k+1}$ and $T = \{\beta_1, \dots, \beta_l\} \subseteq W^{\le k}$. Set $W^{\le k} \setminus T = \{\gamma_1, \dots, \gamma_{s-l}\}$. Then, based on the basis $\{c_{\beta_1}, \dots, c_{\beta_l}, c_{\gamma_1}, \dots, c_{\gamma_{s-l}}\}$, the submatrix $[c_{u_1}, \dots, c_{u_l}, c_{\gamma_1}, \dots, c_{\gamma_{s-l}}]$ can be expressed as

$$[c_{u_1}, \dots, c_{u_l}, c_{\gamma_1}, \dots, c_{\gamma_{s-l}}] = [c_{\beta_1}, \dots, c_{\beta_l}, c_{\gamma_1}, \dots, c_{\gamma_{s-l}}] \begin{pmatrix} B & \mathbf{0} \\ C & I \end{pmatrix} \tag{13}$$

where $B = (b_{i,j})$ is an $l \times l$ matrix, $\mathbf{0}$ is a zero matrix, and I is an identity matrix of order $s-l$. Therefore, the key is to select the two vector subsets U and T such that B is nonsingular.

Generally speaking, it is not easy to determine the rank of B. However, if B is an upper triangular matrix or a lower triangular matrix, it becomes much easier. Then, the crucial task is to properly choose two vector subsets $U = \{u_1, \dots, u_l\} \subseteq W^{\ge k+1}$ and $T = \{\beta_1, \dots, \beta_l\} \subseteq W^{\le k}$, satisfying the following two conditions C1 and C2.

C1. The coefficient of c_{β_i} in the linear expression of c_{u_i} is 1, i.e., $b_{i,i} = 1$ for $1 \le i \le l$;
C2. The coefficient of c_{β_i} in the linear expression of c_{u_j} is 0, i.e., $b_{i,j} = 0$ for all $1 \le j < i \le l$, (or for all $1 \le i < j \le l$).

In the sequel, we show that Theorem 2 is a powerful tool to check C1 and C2. It not only provides simpler and direct proofs for the known constructions, but also gives a new construction of Boolean functions with optimal AI and high nonlinearity.

4.1 Example 1: The construction given by Carlet in [3]

In [3], Carlet introduced a general way for constructing Boolean functions with optimal AI, which can be regarded as the application of C1 and C2.

Proposition 2 ([3]) *Let n be odd. For any integer $1 \le l \le \binom{n}{k}$, choose two sets $U = \{u_1, \ldots, u_l\} \subseteq W^{k+1}$ and $T = \{\beta_1, \ldots, \beta_l\} \subseteq W^{\le k}$ such that $\beta_i \preceq u_i$ for $1 \le i \le l$ and $\beta_i \not\preceq u_j$ for $1 \le j < i \le l$. Then, the function $f \in \mathcal{B}_n$ with $\mathrm{supp}(f) = \left(W^{\le k} \backslash T\right) \cup U$ has optimal AI.*

Proof For $1 \le i \le l$, assuming $\mathrm{wt}(\beta_i) = k - i'$ for some $i' \ge 0$. Since $\beta_i \preceq u_i$ and $\mathrm{wt}(u_i) = k + 1$, it follows from Theorem 2 that

$$b_{i,i} = a_{i'}^{(1)} = \binom{i' + 1 - 1}{i'} = 1.$$

When $1 \le j < i \le l$, $b_{i,j} = 0$ by Theorem 1 because of $\beta_i \not\preceq u_j$. This finishes the proof. □

4.2 Example 2: The construction given by Dong et al. in [16]

Later in [16], Dong et al. presented the following construction, which can be viewed as the application of C1 and C2 as well.

Proposition 3 ([16]) *Let n be odd. For any two vectors $Y_1, Y_2 \in \mathbb{F}_2^n$, define $[Y_1, Y_2) = \{Y \in \mathbb{F}_2^n | Y_1 \le Y < Y_2\}$. Let $Y_1, Y_2, \ldots, Y_s$ be all the s vectors in $W^{\le k}$ sorted by the order that $Y_i < Y_{i+1}$ for $1 \le i \le s-1$. Choose vector $X_i \in [Y_i, Y_{i+1})$ for $1 \le i \le s-1$ and X_s with $Y_s \preceq X_s$. Let f be the Boolean function defined by $\mathrm{supp}(f) = \bigcup_{i=1}^{s} \{X_i\}$. Then f has optimal AI.*

Proof For $1 \le i \le s-1$, it is easy to verify that

I. if $\mathrm{wt}(Y_i) < k$ then $Y_{i+1} = Y_i + 1$, which implies $X_i = Y_i$;
II. if $\mathrm{wt}(Y_i) = k$ then $Y_{i+1} = Y_i + 2^{j_1}$, where $Y_i = \sum_{l=1}^{k} 2^{j_l}$ with $0 \le j_1 < \cdots < j_k \le n-1$. Then, $X_i = Y_i$, or $Y_i < X_i < Y_{i+1}$ with $\mathrm{wt}(X_i) > k$, which both satisfy $Y_i \preceq X_i$.

Clearly, by the terminologies of U and T above, we have that $U = \{X_i | \mathrm{wt}(Y_i) = k, \mathrm{wt}(X_i) > k\}$ and $T = \{Y_i | \mathrm{wt}(Y_i) = k, \mathrm{wt}(X_i) > k\}$. From Case II, we see that $X_i < Y_{i+1} \le Y_j$ when $i < j$, which implies $Y_j \not\preceq X_i$ and then $b_{i,j} = 0$ by Theorem 1. When $i = j$, since $Y_i \preceq X_i$ indicated in Case II, applying Theorem 2 to $\beta = Y_i$ and $u = X_i$ with $\mathrm{wt}(Y_i) = k$ and $\mathrm{wt}(X_i) = k + i'$ for some $i' \ge 1$, we then get

$$b_{i,i} = a_0^{(i')} = \binom{0 + i' - 1}{0} = 1.$$

This completes the proof. □

4.3 A new construction of Boolean functions on odd variables with optimal AI and high nonlinearity

In this subsection, we give a new construction of Boolean function f with $\mathrm{supp}(f) = \left(W^{\geq k+1} \backslash U\right) \cup T$, where T and U are two properly chosen subsets of $W^{\leq k}$ and $W^{\geq k+1}$ respectively. We will prove that the new constructed Boolean function f has optimal AI and higher nonlinearity compared with the function defined in [8].

In this subsection, we always assume that $m = \lfloor \frac{n}{4} \rfloor$ with $n \geq 11$ being odd. That is, $n = 4m+1$ with $m \geq 3$ or $n = 4m+3$ with $m \geq 2$. Further, we always denote $t = \lceil \frac{m+1}{3} \rceil$ and $p = \lceil \log_2 t \rceil$ in this subsection.

Set $\mathbb{F}_2^p = \left\{ e_1^{(p)}, e_2^{(p)}, \ldots, e_{2^p}^{(p)} \right\}$, where the vectors are listed according to the Hamming weight firstly and the lexicographic order secondly. Denote $T_0 = \bigcup_{j=0}^{3} W^{k-j}$ and $U_0 = \bigcup_{j=0}^{3} W^{k+4-j}$. With these notations, we define $2m+2$ subsets T_i and U_i of $\mathbb{F}_2^n$, $1 \leq i \leq m+1$, as follows:

(1) $1 \leq i \leq t$,

$$T_i = \{\beta = (y_1, 0, y_2, 0, y_3, e_i^{(p)}, 0) \in \mathbb{F}_2^{4i-4} \times \mathbb{F}_2^4 \times \mathbb{F}_2^{4t-4i} \times \mathbb{F}_2 \times \mathbb{F}_2^{n-4t-p-2} \times \mathbb{F}_2^p \times \mathbb{F}_2 | \beta \in T_0\}$$

$$U_i = \{u = (y_1, 1, y_2, 0, y_3, e_i^{(p)}, 0) \in \mathbb{F}_2^{4i-4} \times \mathbb{F}_2^4 \times \mathbb{F}_2^{4t-4i} \times \mathbb{F}_2 \times \mathbb{F}_2^{n-4t-p-2} \times \mathbb{F}_2^p \times \mathbb{F}_2 | u \in U_0\}$$

(2) $t+1 \leq i \leq \min\{2t, m\}$,

$$T_i = \{\beta = (0, e_{i-t}^{(p)}, y_1, 0, y_2, 1) \in \mathbb{F}_2 \times \mathbb{F}_2^p \times \mathbb{F}_2^{4i-5-p} \times \mathbb{F}_2^4 \times \mathbb{F}_2^{n-4i-1} \times \mathbb{F}_2 | \beta \in T_0\}$$

$$U_i = \{u = (0, e_{i-t}^{(p)}, y_1, 1, y_2, 1) \in \mathbb{F}_2 \times \mathbb{F}_2^p \times \mathbb{F}_2^{4i-5-p} \times \mathbb{F}_2^4 \times \mathbb{F}_2^{n-4i-1} \times \mathbb{F}_2 | u \in U_0\}$$

(3) $\min\{2t, m\} + 1 \leq i \leq m$,

$$T_i = \{\beta = (1, e_{i-2t}^{(p)}, y_1, 1, y_2, 0, y_3) \in \mathbb{F}_2 \times \mathbb{F}_2^p \times \mathbb{F}_2^{4t-1-p} \times \mathbb{F}_2 \times \mathbb{F}_2^{4i-5-4t} \times \mathbb{F}_2^4 \times \mathbb{F}_2^{n-4i} | \beta \in T_0\}$$

$$U_i = \{u = (1, e_{i-2t}^{(p)}, y_1, 1, y_2, 1, y_3) \in \mathbb{F}_2 \times \mathbb{F}_2^p \times \mathbb{F}_2^{4t-1-p} \times \mathbb{F}_2 \times \mathbb{F}_2^{4i-5-4t} \times \mathbb{F}_2^4 \times \mathbb{F}_2^{n-4i} | u \in U_0\}$$

(4) $i = m+1$,

$$T_{m+1} = \{\beta = (1, e_\lambda^{(p)}, y_1, 1, y_2, 0) \in \mathbb{F}_2 \times \mathbb{F}_2^p \times \mathbb{F}_2^{4t-1-p} \times \mathbb{F}_2 \times \mathbb{F}_2^{4m-4t-1} \times \mathbb{F}_2^{n-4m} | \beta \in T'\}$$

$$U_{m+1} = \{u = (1, e_\lambda^{(p)}, y_1, 1, y_2, 1) \in \mathbb{F}_2 \times \mathbb{F}_2^p \times \mathbb{F}_2^{4t-1-p} \times \mathbb{F}_2 \times \mathbb{F}_2^{4m-4t-1} \times \mathbb{F}_2^{n-4m} | u \in U'\}$$

where $\lambda = m+1-\min\{2t, m\}$, and $T' = W^k$, $U' = W^{k+1}$ if $n = 4m+1$, or $T' = W^k \cup W^{k-2}$, $U' = W^{k+3} \cup W^{k+1}$ if $n = 4m+3$.

Note that $|T_i| = |U_i|$ for $1 \leq i \leq m+1$, and $T_i \cap T_j = U_i \cap U_j = \emptyset$ for any $i \neq j$ by the first, the $(4t+1)th$ and the last entries of the vectors in T_i and U_i and by the $e_i^{(p)}$'s.

Table 1 Specific elements in T_i and U_i for $n = 21$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
T_1	0	0	0	0					0											0	0
U_1	1	1	1	1					0											0	0
T_2					0	0	0	0	0											1	0
U_2					1	1	1	1	0											1	0
T_3	0	0							0	0	0	0									1
U_3	0	0							1	1	1	1									1
T_4	0	1											0	0	0	0					1
U_4	0	1											1	1	1	1					1
T_5	1	0							1								0	0	0	0	
U_5	1	0							1								1	1	1	1	
T_6	1	1							1												0
U_6	1	1							1												1

Table 2 Specific elements in T_i and U_i for $n = 23$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
T_1	0	0	0	0					0													0	0
U_1	1	1	1	1					0													0	0
T_2					0	0	0	0	0													1	0
U_2					1	1	1	1	0													1	0
T_3	0	0							0	0	0	0											1
U_3	0	0							1	1	1	1											1
T_4	0	1											0	0	0	0							1
U_4	0	1											1	1	1	1							1
T_5	1	0							1								0	0	0	0			
U_5	1	0							1								1	1	1	1			
T_6	1	1							1												0	0	0
U_6	1	1							1												1	1	1

Example 1 For $n = 21$ and 23, some specific elements in T_i and U_i are illustrated in Tables 1 and 2.

Based on the subsets T_i and U_i, $1 \leq i \leq m + 1$, set

$$T = \bigcup_{i=1}^{m+1} T_i \text{ and } U = \bigcup_{i=1}^{m+1} U_i. \tag{14}$$

Now, we are able to give a new construction of Boolean functions as follows, which have optimal AI and high nonlinearity.

With T and U being subsets of $\mathbb{F}_2^n$ given by (14), define $f \in \mathcal{B}_n$ as

$$f(x) = \begin{cases} F(x) + 1, & x \in T \cup U \\ F(x), & \text{otherwise} \end{cases} \tag{15}$$

where $F(x)$ is the majority function on n variables.

In what follows, the algebraic immunity and nonlinearity of f in (15) are investigated respectively. Further, the ability of f to resist fast algebraic attacks is also checked for $n = 11, 13$ and 15.

For convenience, we respectively arrange all vectors in T_i and U_i, $1 \le i \le m+1$, according to the Hamming weight firstly and the lexicographic order secondly. Suppose

$$T_i = \{\beta_1^{(i)}, \beta_2^{(i)}, \ldots, \beta_{|T_i|}^{(i)}\},\ U_i = \{u_1^{(i)}, u_2^{(i)}, \ldots, u_{|T_i|}^{(i)}\} \tag{16}$$

for $1 \le i \le m+1$. By the definition of T_i and U_i, obviously $\beta_j^{(i)} \preceq u_j^{(i)}$, for $1 \le j \le |T_i|$ and $1 \le i \le m+1$. More precisely, if $\mathrm{wt}(\beta_j^{(i)}) = k - j'$ with $0 \le j' \le 3$, then $\mathrm{wt}(u_j^{(i)}) = k + 4 - j'$, for $1 \le j \le |T_i|$ and $1 \le i \le m$. Hence, from Theorem 2, we know that the corresponding coefficient $b_{j,j}$ in (13) is

$$b_{j,j} = a_{j'}^{(4-j')} = \binom{3}{j'} = 1 \pmod 2.$$

When $n = 4m+1$, it follows from the definition of T_{m+1} and U_{m+1} that $\mathrm{wt}(\beta_j^{(m+1)}) = k$ and $\mathrm{wt}(u_j^{(m+1)}) = k+1$, $1 \le j \le |T_{m+1}|$. By Theorem 2, we have $b_{j,j} = a_0^{(1)} = 1$. When $n = 4m+3$, similarly, $\mathrm{wt}(\beta_j^{(m+1)}) = k$ (resp. $k-2$) and $\mathrm{wt}(u_j^{(m+1)}) = k+3$ (resp. $k+1$), $1 \le j \le |T_{m+1}|$. Then from Theorem 2 we know that $b_{j,j} = a_0^{(3)} = 1$ or $b_{j,j} = a_2^{(1)} = 1$. That is, the vectors in T_i and U_i, $1 \le i \le m+1$, satisfy Condition C1.

Next we check that the vectors in T_i and U_i, $1 \le i \le m+1$, satisfy Condition C2. Define

$$\Lambda_i = \{4i-3, 4i-2, 4i-1, 4i\}, 1 \le i \le m,\ \text{and}\ \Lambda_{m+1} = \{4m+1, \ldots, n\}. \tag{17}$$

Note that the set Λ_i, $1 \le i \le m+1$, contains the positions where $\beta_j^{(i)} \in T_i$ and $u_j^{(i)} \in U_i$, $1 \le j \le |T_i|$, differ. We observe the following properties (e.g. Example 1) from the definition of the subsets T_i and U_i that

- $\beta_{j_2}^{(i)} \not\preceq \beta_{j_1}^{(i)}$, $1 \le j_1 < j_2 \le |T_i|$ and $1 \le i \le m+1$, follows from the order of the Hamming weight firstly and the lexicographic order secondly, which implies $\beta_{j_2}^{(i)} \not\preceq u_{j_1}^{(i)}$ since all the entries in $\beta_j^{(i)}$ and $u_j^{(i)}$, $1 \le j \le |T_i|$, are the same except for the ones at the fixed positions in Λ_i;
- Similarly $e_{i_2}^{(p)} \not\preceq e_{i_1}^{(p)}$, $1 \le i_1 < i_2 \le p$, which indicates $\beta_{j_2}^{(i_2)} \not\preceq u_{j_1}^{(i_1)}$ for $1 \le j_1 \le |T_{i_1}|$, $1 \le j_2 \le |T_{i_2}|$, and $1 \le i_1 < i_2 \le t$ or $t+1 \le i_1 < i_2 \le \min\{2t, m\}$ or $\min\{2t, m\} + 1 \le i_1 < i_2 \le m+1$;
- $\beta_{j_2}^{(i_2)} \not\preceq u_{j_1}^{(i_1)}$, $1 \le j_1 \le |T_{i_1}|$, $1 \le j_2 \le |T_{i_2}|$,
  - for $1 \le i_1 \le t < i_2 \le \min\{2t, m\}$ by the last entries of $\beta_{j_2}^{(i_2)}$ and $u_{j_1}^{(i_1)}$;
  - for $1 \le i_1 \le t$ and $\min\{2t, m\} + 1 \le i_2 \le m+1$ by the $(4t+1)$th entries of $\beta_{j_2}^{(i_2)}$ and $u_{j_1}^{(i_1)}$;
  - for $t+1 \le i_1 \le \min\{2t, m\} < i_2 \le m+1$ by the first entries of $\beta_{j_2}^{(i_2)}$ and $u_{j_1}^{(i_1)}$.

Thus, the following theorem holds.

Theorem 3 *For $n \ge 11$, the function $f \in \mathcal{B}_n$ constructed in (15) has optimal AI.*

Now, we study the nonlinearity of the Boolean function f constructed in (15). First of all, we need some useful lemmas.

Lemma 1 *For* $1 \le i \le 2^p$, *denote* $\mathrm{wt}(e_i^{(p)})$ *by* s_i. *Then,*

$$|T_i| = |U_i| = \begin{cases} \binom{2k-4-p}{k-s_i} + \binom{2k-4-p}{k-2-s_i}, & 1 \le i \le t, \\ \binom{2k-4-p}{k-1-s_{i-t}} + \binom{2k-4-p}{k-3-s_{i-t}}, & t+1 \le i \le \min\{2t, m\}, \\ \binom{2k-4-p}{k-2-s_{i-2t}} + \binom{2k-4-p}{k-4-s_{i-2t}}, & \min\{2t, m\}+1 \le i \le m, \\ \binom{2k-4-p}{k-2-s_\lambda} + \binom{2k-4-p}{k-4-s_\lambda}, & i = m+1, n = 4m+3, \\ \binom{2k-2-p}{k-2-s_\lambda}, & i = m+1, n = 4m+1, \end{cases} \tag{18}$$

where $\lambda = m + 1 - \min\{2t, m\}$.

Proof By the definition of T_i and U_i, it is easy to see that

$$|T_i| = |U_i| = \begin{cases} \sum_{j=0}^{3} \binom{2k-5-p}{k-j-s_i}, & 1 \le i \le t, \\ \sum_{j=0}^{3} \binom{2k-5-p}{k-j-1-s_{i-t}}, & t+1 \le i \le \min\{2t, m\}, \\ \sum_{j=0}^{3} \binom{2k-5-p}{k-j-2-s_{i-2t}}, & \min\{2t, m\}+1 \le i \le m, \\ \binom{2k-4-p}{k-2-s_\lambda} + \binom{2k-4-p}{k-4-s_\lambda}, & i = m+1, n = 4m+3, \\ \binom{2k-2-p}{k-2-s_\lambda}, & i = m+1, n = 4m+1. \end{cases}$$

Immediately, (18) follows from Pascal's Formula. □

Lemma 2 *The cardinality of* T_i, $1 \le i \le m+1$, *in* (18) *satisfies*

$$\min_{1 \le i \le m+1} |T_i| = |T_1| = \binom{2k-4-p}{k} + \binom{2k-4-p}{k-2}. \tag{19}$$

Proof Clearly, for $1 \le i \le 2^p$, we have $0 \le s_i = \mathrm{wt}(e_i^{(p)}) \le p$ with $s_1 = 0$ since $e_1^{(p)} = (0, 0, \ldots, 0)$. Subsisting it into (18), we can easily get

$$\min_{1 \le i \le m} |T_i| = |T_1| = \binom{2k-4-p}{k} + \binom{2k-4-p}{k-2}$$

by means of the facts that $\binom{a}{b} < \binom{a}{c}$ if $|b - a/2| > |c - a/2|$.

As for $|T_{m+1}|$, if $n = 4m+3$, then $|T_{m+1}| \ge \binom{2k-4-p}{k} + \binom{2k-4-p}{k-2}$; if $n = 4m+1$, then $|T_{m+1}| = \binom{2k-2-p}{k-2-s_{m+1-\min\{2t,m\}}} \ge \binom{2k-2-p}{k-2-p}$. Further, applying Pascal's Formula, we have $\binom{2k-2-p}{k-2-p} = \binom{2k-2-p}{k} = \binom{2k-3-p}{k} + \binom{2k-3-p}{k-1} = \binom{2k-4-p}{k} + \binom{2k-4-p}{k-1} + \binom{2k-4-p}{k-1} + \binom{2k-4-p}{k-2} > \binom{2k-4-p}{k} + \binom{2k-4-p}{k-2}$, which gives the desired (19). □

Lemma 3 ([14,27]) *Let* $F(x)$ *be the* n*-variable majority function with* n *odd. Then the Walsh spectrum of* $F(x)$ *satisfies*

1. $W_F(\omega) = 2\binom{2k}{k}$ *if* $\mathrm{wt}(\omega) = 1$;
2. $W_F(\omega) = 2(-1)^k\binom{2k}{k}$ *if* $\mathrm{wt}(\omega) = n$;
3. $|W_F(\omega)| \le 2\left[\binom{2k-2}{k-1} - \binom{2k-2}{k}\right]$ *if* $2 \le \mathrm{wt}(\omega) \le 2k$ *and* $n \ge 7$.

Now, we are ready to compute the nonlinearity of the function f given in (15).

Theorem 4 *For $n \geq 11$ being odd, the nonlinearity of $f \in \mathcal{B}_n$ constructed in (15) is*

$$nl_f = 2^{2k} - \binom{2k}{k} + 2\left[\binom{2k-4-p}{k} + \binom{2k-4-p}{k-2}\right]$$

where $p = \lceil \log_2 \lceil \frac{m+1}{3} \rceil \rceil$, $m = \lfloor \frac{n}{4} \rfloor$ and $k = \frac{n-1}{2}$.

Proof Firstly, it is clear that $W_f(0) = 0$ since f is balanced.

Next, if $\omega = (\omega_1, \omega_2, \ldots, \omega_n) \neq 0$, by (3), we have

$$\begin{aligned} W_f(\omega) &= \sum_{x \notin T \cup U} (-1)^{f(x) \oplus \omega \cdot x} + \sum_{x \in T} (-1)^{1 \oplus \omega \cdot x} + \sum_{x \in U} (-1)^{\omega \cdot x} \\ &= W_F(\omega) - 2\left[\sum_{x \in T} (-1)^{\omega \cdot x} - \sum_{x \in U} (-1)^{\omega \cdot x}\right] \\ &= W_F(\omega) - 2\sum_{i=1}^{m+1} \left[\sum_{x \in T_i} (-1)^{\omega \cdot x} - \sum_{x \in U_i} (-1)^{\omega \cdot x}\right] \end{aligned} \tag{20}$$

Note that the corresponding vectors $\beta_j^{(i)} \in T_i$ and $u_j^{(i)} \in U_i$ in (16) are almost the same except for the entries at the positions in Λ_i defined in (17). Hence,

$$\sum_{x \in T_i} (-1)^{\omega \cdot x} - \sum_{x \in U_i} (-1)^{\omega \cdot x} = \left[1 - (-1)^{\sum_{l \in \Lambda_i} \omega_l}\right] \sum_{x \in T_i} (-1)^{\omega \cdot x}$$

which will be discussed in the following three cases.

Case 1. If $\mathrm{wt}(\omega) = 1$, assuming $\mathrm{supp}(\omega) = \{j\}$ for some $1 \leq j \leq n$, then $\sum_{x \in T_i} (-1)^{\omega \cdot x} - \sum_{x \in U_i} (-1)^{\omega \cdot x} = 0$ if $i \neq \lceil \frac{j}{4} \rceil$ due to $\omega_l = 0$ for all $l \in \Lambda_i$. Otherwise, if $i = \lceil \frac{j}{4} \rceil$, then

$$\sum_{x \in T_i} (-1)^{\omega \cdot x} - \sum_{x \in U_i} (-1)^{\omega \cdot x} = 2|T_i|$$

because of $\omega \cdot x = 0$ for all $x \in T_i$. Thus, applying (19) and Lemma 3 to (20), it results in

$$\begin{aligned} |W_f(\omega)| &\leq \left|W_F(\omega) - 4 \min_{1 \leq i \leq m+1} |T_i|\right| \\ &= 2\binom{2k}{k} - 4\left[\binom{2k-4-p}{k} + \binom{2k-4-p}{k-2}\right] \end{aligned}$$

since $2\binom{2k}{k} = 4\binom{2k-1}{k} > 4|T_i|$ holds for all $1 \leq i \leq m+1$.

Case 2. If $\mathrm{wt}(\omega) = n$, i.e., $\omega = (1, 1, \ldots, 1)$, then $\sum_{x \in T_i} (-1)^{\omega \cdot x} - \sum_{x \in U_i} (-1)^{\omega \cdot x} = 0$ for $1 \leq i \leq m$, since $\sum_{l \in \Lambda_i} \omega_l = 4$. While,

$$\sum_{x \in T_{m+1}} (-1)^{\omega \cdot x} - \sum_{x \in U_{m+1}} (-1)^{\omega \cdot x} = 2(-1)^k |T_{m+1}|$$

because of $\sum_{l \in \Lambda_{m+1}} \omega_l = 1$ and $T_{m+1} \subseteq W^k$ if $n = 4m+1$, or $\sum_{l \in \Lambda_{m+1}} \omega_l = 3$ and $T_{m+1} \subseteq W^k \cup W^{k-2}$ if $n = 4m+3$. Associated with Lemma 3 and (19), it leads to

Table 3 The value of Δ for $n = 4m + 1$

m	3	4	5	6
Δ	476	3498	23452	2387684
m	7	8	9	10
Δ	31077768	391434010	4721199420	54682807740
m	11	12	13	
Δ	645670754040	34504882753380	498844567560528	

Table 4 The value of Δ for $n = 4m + 3$

m	2	3	4	5
Δ	44	2784	26884	236912
m	6	7	8	9
Δ	10661584	139902928	1815787440	22877032800
m	10	11	12	13
Δ	281752245720	3413238837840	143645921427528	2087086960013776

$$\begin{aligned}|W_f(\omega)| &= \left|2(-1)^k\binom{2k}{k} - 4(-1)^k|T_{m+1}|\right| \\ &\le 2\binom{2k}{k} - 4\left[\binom{2k-4-p}{k} + \binom{2k-4-p}{k-2}\right]\end{aligned}$$

Case 3. If $2 \le \mathrm{wt}(\omega) \le 2k$, then by Lemma 3 we have

$$\begin{aligned}|W_f(\omega)| &\le 2\binom{2k-2}{k-1} - 2\binom{2k-2}{k} + 4\sum_{i=1}^{m+1}|T_i| \\ &= \frac{1}{2k-1}\binom{2k}{k} + 4|T|\end{aligned}$$

Denote

$$\Delta = 2\binom{2k}{k} - 4\min_{1\le i\le m+1}|T_i| - \frac{1}{2k-1}\binom{2k}{k} - 4|T|.$$

Next we will prove that $\Delta > 0$ for $n \ge 11$.
If $m \le 13$, we know that

$$\begin{aligned}\Delta &= 2\binom{2k}{k} - 4|T_1| - \frac{1}{2k-1}\binom{2k}{k} - 4|T| \\ &= \frac{4k-3}{2k-1}\binom{2k}{k} - 8|T_1| - 4\sum_{i=2}^{m+1}|T_i| \\ &> 0\end{aligned}$$

by a direct calculation listed in the following Tables 3 and 4.
If $m \ge 14$, we investigate it in two subcases according to p is even or odd.

When p is even, by (18) we have

$$|T_i| \leq 2\binom{2k-4-p}{k-2-\frac{p}{2}},\ 1 \leq i \leq m$$

and

$$|T_{m+1}| \leq \binom{2k-2-p}{k-1-\frac{p}{2}} \leq 4\binom{2k-4-p}{k-2-\frac{p}{2}}.$$

Then,

$$\begin{aligned}
\Delta &= \frac{4k-3}{2k-1}\binom{2k}{k} - 4|T_1| - 4\sum_{i=1}^{m}|T_i| - 4|T_{m+1}| \\
&\geq \frac{4k-3}{2k-1}\binom{2k}{k} - 8(m+3)\binom{2k-4-p}{k-2-\frac{p}{2}} \\
&\geq \frac{4k-3}{2k-1}\binom{2k}{k} - \frac{8(m+3)k}{2^{3+\log_2\frac{m+1}{3}}(2k-3-p)}\binom{2k}{k} \\
&\geq \Big[\frac{8m-3}{4m-1} - \frac{3(m+3)(2m+1)}{(m+1)(3m+8)}\Big]\binom{2k}{k} \\
&= \frac{m^2+16m-15}{(4m-1)(m+1)(3m+8)}\binom{2k}{k} \\
&> 0
\end{aligned}$$

where in the second inequality we use

$$\frac{\binom{2r}{r}}{\binom{2k}{k}} = \frac{(2r)!(k!)^2}{(2k)!(r!)^2} = \frac{k^2(k-1)^2\cdots(r+1)^2}{(2k)(2k-1)(2k-2)\cdots(2r+1)} < (\frac{1}{2})^{2k-2r-1}\frac{k}{2r+1} \quad (21)$$

for $r = k-2-\frac{p}{2}$, and $p \geq \log_2\frac{m+1}{3}$; in the third inequality we use

$$\frac{4k-3}{2k-1} \geq \frac{8m-3}{4m-1}$$

and

$$\frac{k}{2k-3-p} \leq \frac{2m+1}{4m-3-p} \leq \frac{2m+1}{3m+8}$$

since $m-p \geq 11$ for $m \geq 14$, and $k = \lceil n/2 \rceil - 1$ is $2m$ if $n = 4m+1$ or $2m+1$ if $n = 4m+3$.

When p is odd, by (18) we then get

$$|T_i| \leq \binom{2k-4-p}{k-2-\frac{p+1}{2}} + \binom{2k-4-p}{k-2-\frac{p-1}{2}} = \binom{2k-3-p}{k-2-\frac{p-1}{2}}$$

for $1 \leq i \leq m$, and

$$|T_{m+1}| \leq \binom{2k-2-p}{k-1-\frac{p-1}{2}} < 2\binom{2k-3-p}{k-2-\frac{p-1}{2}}.$$

Similarly, we can derive that

$$\Delta = 2\binom{2k}{k} - 4\min_{1\leq i\leq m+1}|T_i| - \frac{1}{2k-1}\binom{2k}{k} - 4|T| > 0.$$

Therefore, for all $\omega \in \mathbb{F}_2^n$, we always have

$$|W_f(\omega)| \le 2\binom{2k}{k} - 4\left[\binom{2k-4-p}{k} + \binom{2k-4-p}{k-2}\right].$$

Note that this bound is tight, since the bound can be attained in case 1 with equality $\min_{1\le i\le m+1} |T_i| = |T_1|$.

We complete the proof for $n \ge 11$ by applying (4) to the above inequality. □

Recall that in our construction p is defined as $p = \lceil \log_2 \lceil \frac{m+1}{3} \rceil \rceil$. If $p = \log_2 \frac{m+1}{3}$, then each vector $e_i^{(p)}$, $1 \le i \le 2^p$, is used three times for constructing $T_1, T_2, \ldots, T_{m+1}$. However, if $n = 4m+1$ with $3 \cdot 2^p - 1 \ge m+1$, i.e., $m = 3, 4, 6, 7, 8, 9, 10, 12, 13, \ldots$, then some subsets of $e_2^{(p)}, \ldots, e_{2^p}^{(p)}, e_1^{(p)}, \ldots, e_{2^p}^{(p)}, e_1^{(p)}, \ldots, e_{2^p}^{(p)}$ are enough to construct $T_1, T_2, \ldots, T_{m+1}$; if $n = 4m+3$ with $3 \cdot 2^p - 2 \ge m+1$, i.e., $m = 3, 6, 7, 8, 9, 12, 13, \ldots$, then some subsets of $e_2^{(p)}, \ldots, e_{2^p}^{(p)}, e_1^{(p)}, \ldots, e_{2^p}^{(p)}, e_1^{(p)}, \ldots, e_{2^p-1}^{(p)}$ are enough to construct $T_1, T_2, \ldots, T_{m+1}$. In this way, by the same method as we did in Lemmas 1 and 2, we have

$$\min_{1\le i\le m+1} |T_i| = |T_1| = \binom{2k-4-p}{k-1} + \binom{2k-4-p}{k-3}.$$

Then, by the same method as we did in Theorem 4, the nonlinearity of $f \in \mathcal{B}_n$ constructed in (15) can be improved as

$$nl'_f = 2^{2k} - \binom{2k}{k} + 2\left[\binom{2k-4-p}{k-1} + \binom{2k-4-p}{k-3}\right].$$

To the best of our knowledge, among all the Boolean functions constructed from the generator matrix of Reed–Muller code, the ones proposed in [8] have the highest nonlinearity. When n is odd, the functions in [8] have nonlinearity

$$nl_g = 2^{n-1} - \binom{2k}{k} + 2\left\lfloor \sum_{i=0}^{m-1} \binom{3m-2}{m+i-1} \frac{m-i}{m} \right\rfloor$$

for $n = 4m+1$, $m \ge 4$, and

$$nl_g = 2^{n-1} - \binom{2k}{k} + 2\left\lfloor \sum_{i=0}^{m+1} \binom{3m-1}{m+i} \frac{m+2-i}{m+2} \right\rfloor$$

for $n = 4m+3$, $m \ge 5$.

Let us consider the enhanced nonlinearity of our functions and the ones in [8] over that of the majority function. For simplicity, denote

$$\varDelta_1 = \begin{cases} 2\left\lfloor \sum_{i=0}^{m-1} \binom{3m-2}{m+i-1} \frac{m-i}{m} \right\rfloor, & n = 4m+1, m \ge 4 \\ 2\left\lfloor \sum_{i=0}^{m+1} \binom{3m-1}{m+i} \frac{m+2-i}{m+2} \right\rfloor, & n = 4m+3, m \ge 5 \end{cases}$$

$$\varDelta_2 = 2\left[\binom{2k-4-p}{k} + \binom{2k-4-p}{k-2}\right]$$

$$\varDelta_3 = 2\left[\binom{2k-4-p}{k-1} + \binom{2k-4-p}{k-3}\right]$$

Table 5 Comparison of the enhanced nonlinearity for $n = 4m + 1$

m	Δ_1	Δ_2	Δ_3	$\lfloor \frac{\Delta_2}{\Delta_1} \rfloor$	$\lfloor \frac{\Delta_3}{\Delta_1} \rfloor$
4	912	1254	1584	1	1
5	7436	18876	18876	2	2
6	60502	124644	160888	2	2
7	490960	1932832	2405704	3	4
8	3974192	29938870	36253520	7	9
9	32102020	463831800	549754740	14	17
10	258852810	7191874140	8379147480	27	32
11	2084241600	111635950080	111635950080	53	53

where we assume Δ_3 be equal to Δ_2 for $n = 4m + 1$ with $3 \cdot 2^p - 1 \geq m + 1$ or $n = 4m + 3$ with $3 \cdot 2^p - 2 \geq m + 1$

By a direct calculation, we know that

$$\Delta_1 = \sum_{i=0}^{m} \binom{3m-2}{m+i-1} < (m+1)\binom{3m-2}{\lfloor \frac{3m}{2} \rfloor - 1} \leq 3 \cdot 2^p \binom{3m-2}{\lfloor \frac{3m}{2} \rfloor - 1}$$

for $n = 4m + 1$, and

$$\Delta_1 < 2(m+1)\binom{3m-1}{\lfloor \frac{3m-1}{2} \rfloor} \leq 6 \cdot 2^p \binom{3m-1}{\lfloor \frac{3m-1}{2} \rfloor}$$

for $n = 4m + 3$. On the other hand,

$$\Delta_2 > 2\binom{2k-4-p}{k-2} = 2\binom{2k-4-p}{k-2-p} > 2\binom{2k-4-2p}{k-2-p}.$$

If $n = 4m + 1$, then

$$\frac{\Delta_2}{\Delta_1} > \frac{2\binom{4m-4-2p}{2m-2-p}}{3 \cdot 2^p \binom{3m-2}{\lfloor \frac{3m}{2} \rfloor - 1}} > \frac{2}{3 \cdot 2^p} 2^{m-3-2p} \frac{3m-1}{2m-2-p} > 2^{m-3-3p}$$

where the second inequality holds by the same method as we did in (21). If $n = 4m + 3$, similarly

$$\frac{\Delta_2}{\Delta_1} > \frac{2\binom{4m-2-2p}{2m-1-p}}{6 \cdot 2^p \binom{3m-1}{\lfloor \frac{3m-1}{2} \rfloor}} > \frac{2}{6 \cdot 2^p} 2^{m-2-2p} \frac{3m}{2m-1-p} > 2^{m-3-3p}.$$

When $m \leq 11$, some concrete values of the enhanced nonlinearities Δ_1, Δ_2, and Δ_3 are given in Tables 5 and 6.

In 2008, Carlet and Feng [5] proposed an infinite class of balanced functions(Carlet–Feng functions) with optimal algebraic immunity, the nonlinearity of which satisfies

$$nl_g \geq 2^{n-1} + \frac{2^{\frac{n}{2}+1}}{\pi} \ln\left(\frac{\pi}{4(2^n - 1)}\right) - 1.$$

Table 6 Comparison of the enhanced nonlinearity for $n = 4m + 3$

m	Δ_1	Δ_2	Δ_3	$\lfloor \frac{\Delta_2}{\Delta_1} \rfloor$	$\lfloor \frac{\Delta_3}{\Delta_1} \rfloor$
5	19878	73372	73372	3	3
6	158056	490960	621452	3	3
7	1257546	7607296	9330824	6	7
8	10007736	117832680	141076710	11	14
9	79648832	1826192640	2145031980	22	26
10	633918466	28330798320	28330798320	44	44
11	5045431420	440029574400	440029574400	87	87

Table 7 Comparison of the nonlinearity for $11 \le n \le 21$ with n odd

n	11	13	15	17	19	21
Nonlinearity of majority function	772	3172	12952	52666	213524	863820
Nonlinearity of functions in this paper	824	3256	13276	53920	218386	882696
$2^{n-1} + \frac{2^{\frac{n}{2}+1}}{\pi} \ln\left(\frac{\pi}{4(2^n-1)}\right) - 1$	796	3561	15156	62763	255960	1034932
$2^{n-1} - \left(\frac{\ln 2}{3}(n-1) + \frac{5}{6} + \frac{1}{3\sqrt{3}} + \frac{1}{6\sqrt{2}}\right)2^{\frac{n}{2}} - 1$	866	3740	15590	63782	258303	1040226
$2^{n-1} - \left(\frac{n \ln 2}{\pi} + 0.74\right)2^{\frac{n}{2}} - 1$	879	3768	15649	63909	258571	1040793
The upper bound $\lceil 2^{n-1} - 2^{\frac{n-1}{2}} \rceil$	992	4032	16256	65280	261632	1047552

In 2011, Zeng et al. [29] improved the lower bound of the nonlinearity of Carlet–Feng function to be

$$nl_g > 2^{n-1} - \left(\frac{\ln 2}{3}(n-1) + \frac{5}{6} + \frac{1}{3\sqrt{3}} + \frac{1}{6\sqrt{2}}\right)2^{\frac{n}{2}} - 1.$$

In 2012, Tang et al. [28] presented a much better lower bound of the nonlinearity of Carlet–Feng function as

$$nl_g > 2^{n-1} - \left(\frac{n \ln 2}{\pi} + 0.74\right)2^{\frac{n}{2}} - 1.$$

For $11 \le n \le 21$ with n odd, the comparison of nonlinearity of our function with nonlinearity of the majority function, the above three lower bounds on nonlinearity of the Carlet–Feng function, and the upper bound $\lceil 2^{n-1} - 2^{\frac{n-1}{2}} \rceil$ is given in Table 7.

It should be noted that the actual value of the nonlinearity of Carlet–Feng function is significantly larger than the lower bounds above. Then, the nonlinearity of our function is not as good as that of Carlet–Feng function. Nevertheless, the most useful properties of Boolean function based on the generator matrix of Reed–Muller code are the efficient computation and easy implementation. In order to construct Boolean function with optimal algebraic immunity and higher nonlinearity in this way, according to the computation of Walsh spectrum, we should construct two larger sets $T \subseteq W^{\le k}$ and $U \subseteq W^{\ge k+1}$ such that the nonsingular matrix B in (13) is a more generalized one instead of an upper triangular matrix or a lower triangular matrix.

At last, we analyze the resistance to fast algebraic attacks of the function $f \in \mathcal{B}_n$ constructed in (15) for $n = 11, 13, 15$. It is known that an n-variable Boolean function f can be considered as optimal with respect to fast algebraic attacks if there do not exist two nonzero functions g and h such that $fg = h$ and $\deg(g)+\deg(h) < n$ with $\deg(g) < \frac{n}{2}$. Nevertheless, the resistance to fast algebraic attacks turns out to be hard to estimate, and we must rely on computer simulations feasible only for relatively small value of n. Denote

$$\Omega_f = \min\{\deg(g) + \deg(h) | 0 \neq g, h \in \mathcal{B}_n, fg = h\}$$

We have checked the resistance of our functions to the fast algebraic attacks for $n = 11, 13$ and 15. The results are that if $n = 11$ then $\Omega_f = 8$; if $n = 13$ then $\Omega_f = 10$; if $n = 15$ then $\Omega_f = 12$. We conjecture that $\Omega_f = n - 3$. If this conjecture is true, we can say that the behavior of our functions against fast algebraic attacks is not too bad although these functions are not optimal with respect to fast algebraic attacks.

5 Conclusion

In this paper, an important property about the kth order Reed–Muller code $\mathrm{RM}(k, n)$ is proved by studying the linear relationship of the column vectors in its generator matrix G. This property can be used to provide simple and efficient proofs for AI properties of the Boolean functions in some known constructions. The study also leads to a new class of Boolean functions with optimal AI and high nonlinearity. Although it is still a small subset of all such functions with optimal AI, in terms of practical applications our constructions provide a large source of such functions. In addition, there are still some problems needing to be studied further such as how to improve the nonlinearity and how to give a rigorous proof of our conjecture on the behavior against fast algebraic immunity.

Acknowledgments The authors would like to thank the three anonymous referees and the Editor for their helpful suggestions and comments that improved the quality of this paper and they are indebted to Simon Fischer for the evaluation of the resistance of the functions to fast algebraic attacks. The work was supported in part by the National Science Foundation of China (NSFC) under Grant 61171095, in part by the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry.

References

1. Armknecht F.: Improving fast algebraic attacks. In: Fast Software Encryption 2004. Lecture Notes in Computer Science, vol. 3017. Springer, Berlin, pp. 65–82 (2004).
2. Canteaut A.: Open problems related to algebraic attacks on stream ciphers. In: Workshop on Coding and Cryptography 2005. Lecture Notes in Computer Science, vol. 3969. Springer, Berlin, pp. 120–134 (2006).
3. Carlet C.: A method of construction of balanced functions with optimum algebraic immunity. In: International Workshop on Coding and Cryptology, pp. 25–43, 2007.
4. Carlet C.: Constructing balanced functions with optimum algebraic immunity. In: IEEE International Symposium on Information Theory 2007, pp. 451–455.
5. Carlet C., Feng K.: 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, vol. 5350. Springer, Berlin, pp. 425–440 (2008).
6. Carlet C., Gaborit P.: On the construction of balanced Boolean functions with a good algebraic immunity. In: Proceeding of IEEE International Symposium on Information Theory (ISIT) 2005, pp. 1101–1105, 2005.
7. Carlet C., Dalai D., Gupta K., Maitra S.: Algebraic immunity for cryptographically significant Boolean functions: analysis and construction. IEEE Trans. Inf. Theory, **52**, 3105–3121 (2006).
8. Carlet C., Zeng X., Li C., Hu L.: Further properties of several classes of Boolean functions with optimum algebraic immunity. Des. Codes Cryptogr. **52**, 303–338 (2009).

9. Courtois N.: Fast algebraic attacks on stream ciphers with linear feedback. In: Advances in Cryptology-CRYPTO 2003. Lecture Notes in Computer Science, vol. 2729. Springer, Berlin, pp. 176–194 (2003).
10. Courtois N., Meier W.: Algebraic attacks on stream ciphers with linear feedback. In: EUROCRYPT 2003. Lecture Notes in Computer Science, vol. 2656. Springer, Berlin, pp. 345–359 (2003).
11. Dalai D., Maitra S.: Reducing the number of homogeneous linear equations in finding annihilators. In: Sequences and Their Applications 2006. Lecture Notes in Computer Science, vol. 4086. Springer, Berlin, pp. 376–390 (2006).
12. Dalai D., Gupta K., Maitra S.: Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity. In: Workshop on Fast Software Encryption, FSE 2005. Lecture Notes in Computer Science, vol. 3557. Springer, Berlin, pp. 98–111 (2005).
13. Dalai D., Gupta K., Maitra S.: Notion of algebraic immunity and its evaluation related to fast algebraic attacks. In: Second International Workshop on Boolean Functions: Cryptography and Applications, BFCA 2006, Cryptology ePrint Archive, Report 2006/018. http://eprint.iacr.org/2006/018.pdf.
14. Dalai D., Maitra S., Sarkar S.: Basic theory in construction of Boolean functions with maximum possible annihilator immunity. Des. Codes Cryptogr. **40**, 41–58 (2006).
15. Ding C., Xiao G., Shan W.: The Stability Theory of Stream Ciphers. Springer, Berlin (1991).
16. Dong D., Fu S., Qu L., Li C.: A new construction of Boolean functions with maximum algebraic immunity. In: ISC 2009. Lecture Notes in Computer Science, vol. 5735. Springer, Berlin, pp. 177–185 (2009).
17. Feng K., Liao Q., Yang J.: Maximal values of generalized algebraic immunity. Des. Codes Cryptogr. **50**, 243–252 (2009).
18. Hawkes P., Rose G.: Rewriting variables: The complexity of fast algebraic attacks on stream ciphers. In: Advances in Cryptology-CRYPTO 2004. Lecture Notes in Computer Science, vol. 3152. Springer, Berlin, pp. 390–406 (2004).
19. Limniotis K., Kolokotronis N., Kalouptsidis N.: Constructing Boolean functions in odd number of variables with maximum algebraic immunity. In: Proceeding of IEEE International Symposium on Information Theory (ISIT) 2011, pp. 2662–2666, 2011.
20. Lobanov M.: Tight bound between nonlinearity and algebraic immunity. In: Cryptology ePrint Archive, Report 2005/441. http://eprint.iacr.org/2005/441.pdf.
21. Meier W., Staffelbach O.: Fast correlation attacks on stream ciphers. In: Advances in Cryptology-EUROCRYPT 1988. Lecture Notes in Computer Science, vol. 330. Springer, Berlin, pp. 301–314 (1988).
22. Meier W., Pasalic E., Carlet C.: Algebraic attacks and decomposition of Boolean functions. In: Advances in Cryptology-EUROCRYPT 2004. Lecture Notes in Computer Science, vol. 3027. Springer, Berlin, pp. 474–491 (2004).
23. Muller D.: Application of Boolean algebra to switching circuit design and to error detection. IEEE Trans. Comput. **3**, 6–12 (1954).
24. Peng J., Wu Q., Kan H.: On symmetric Boolean functions with high algebraic immunity on even number of variables. IEEE Trans. Inf. Theory, **57**, 7205–7220 (2011).
25. Qu L., Feng K., Liu F., Wang L.: Constructing symmetric Boolean functions with maximum algebraic immunity. IEEE Trans. Inf. Theory **55**, 2406–2412 (2009).
26. Reed S.: A class of multiple-error-correcting codes and the decoding scheme. IEEE Trans. Inf. Theory **4**, 38–49 (1954).
27. Sarkar S., Maitra S.: Construction of rotation symmetric Boolean functions with maximun algebraic immunity on odd number of variables. In: AAECC 2007. Lecture Notes in Computer Science, vol. 4851. Springer, Berlin, pp. 271–280 (2007).
28. Tang D., Carlet C., Tang X.: Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks. IEEE Trans. Inf. Theory, to be published (2012).
29. Zeng X., Carlet C., Shan J., Hu L.: More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks. IEEE Trans. Inf. Theory **57**, 6310–6320 (2011).