mathematics

MDPI

Article

On Resilient Boolean and Vectorial Boolean Functions with High Nonlinearity

Luyang Li [1,*], Linhui Wang [1], Qinglan Zhao [1] and Dong Zheng [1,2]

[1] School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[2] Westone Cryptologic Research Center (CRC), Chengdu 610095, China
[*] Correspondence: luyang_li@foxmail.com

Abstract: Boolean functions and vectorial Boolean functions are the most important nonlinear components of stream ciphers. They should satisfy several criteria such as high nonlinearity, proper resiliency and so on to guarantee the security of the whole system. However, there are some constraints among the criteria, and how to achieve a trade-off between them is an important issue. In this paper, some nonlinear Boolean functions possessing simple algebraic normal form with special Walsh spectrum are proposed. By using these functions, we provide two construction methods on balanced and resilient Boolean functions with high nonlinearity. In addition, based on the disjoint linear codes and vector matrices with special properties, some resilient vectorial Boolean functions with currently best-known nonlinearity have also been given.

Keywords: stream ciphers; boolean function; vectorial boolean functions; nonlinearity; resiliency

MSC: 06E30

check for updates

Citation: Li, L.; Wang, L.; Zhao, Q.; Zheng, D. On Resilient Boolean and Vectorial Boolean Functions with High Nonlinearity. *Mathematics* **2022**, *10*, 4822. https://doi.org/10.3390/math10244822

Academic Editors: Sergey Bezzateev and Patrick Solé

Received: 25 October 2022
Accepted: 15 December 2022
Published: 19 December 2022

1. Introduction

Stream ciphers play an important role in the confidential communication of government, military and other important departments and various mobile communication systems. Cryptographic functions, including Boolean functions and multi-output Boolean functions, are usually used as the most important nonlinear component in symmetric cryptosystems, especially in stream ciphers, and their properties directly affect the security of the whole encryption system. For the known linear cryptographic attack, related attack, Berlekamp–Massey attack, algebraic attack and other attack methods, it is necessary to use functions with high nonlinearity, certain resiliency, high algebraic degree and so on. However, there are some constraints among these criteria, and how to construct Boolean functions with a good trade-off among some of the criteria is an interesting research problem, for instance, the trade-off between the resiliency and nonlinearity, the optimization of algebraic immunity, the new class of Bent functions and the autocorrelation properties. In this paper, we mainly focus on the good trade-off between nonlinearity and resiliency of Boolean functions and vectorial Boolean functions.

In order to obtain Boolean functions satisfying certain criteria, modifications of the Maiorana–McFarland (M–M) construction [1] by concatenating small functions are often employed. The properties of the modified M-M functions absolutely depend on the small functions. Thus, properly selecting the small functions is crucial for the method. For an n-variable function ($n = 2k$), when the small functions are different k-variable linear functions with number 2^k, the constructed function is called Bent [2]. This kind of functions possess the maximal nonlinearity $2^{n-1} - 2^{n/2-1}$, but they are not balanced. In [3], balanced Boolean functions with known best nonlinearity have been given by iteratively replacing all zero linear functions in the M-M methods, and Dobbertin obtained the same result, respectively, in [4]. However, how to construct a resilient Boolean function with high nonlinearity is an interesting problem; many results have been provided by using modified M-M methods, see [5–16], and the nonlinearity of some resilient functions can be strictly larger than $2^{n-1} - 2^{n/2}$.

Vectorial Boolean functions are usually used to improve the production efficiency of the key that generated stream ciphers. They can be viewed as a collection of Boolean functions. An n-input and m-output vectorial Boolean function is referred to as an (n, m) function. Similarly to the Boolean function, vectorial Boolean functions also need to satisfy criteria such as nonlinearity, resiliency and so on. For (n, m) functions with n even, the upper bound of the nonlinearity is still $2^{n-1} - 2^{n/2-1}$. However, they are not balanced either. How to construct resilient (n, m) functions with nonlinearity lower than the upper bound but larger than $2^{n-1} - 2^{n/2}$ is also an important problem in recent years. By contrast, fewer results have been obtained than the Boolean ones [17–21].

In this paper, we provide some techniques to generate balanced Boolean and resilient Boolean and vectorial Boolean functions with high nonlinearity. For the Boolean case, several kinds of nonlinear small functions with special algebraic normal forms are given. These functions have simple spectral distributions and are suitable to use in the modified M-M method. For the vectorial Boolean case, a construction method based on the disjoint linear codes and vector matrices with special properties is given, and a class of resilient (n, m) functions with nonlinearity larger than $2^{n-1} - 2^{n/2}$ are obtained. It is shown that some of the functions even have currently best-known nonlinearity.

2. Preliminaries

An n-variable Boolean function $f(x)$ is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$; $x = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$ can be represented by the following algebraic normal form (ANF):

$$f(x_1, x_2, \cdots, x_n) = \sum_{u \in \mathbb{F}_2^n} \lambda_u \Big(\prod_{i=1}^{n} x_i^{u_i}\Big). \tag{1}$$

where $\lambda_u \in \mathbb{F}_2, u = (u_1, \cdots, u_n)$. The algebraic degree of $f(x)$, denoted by $deg(f)$, is the maximal value of $wt(u)$, where $wt(u)$ denotes the Hamming weight of u such that $\lambda_u \neq 0$. For any n-variable Boolean function $f(x)$, the Walsh transform of $f \in \mathcal{B}_n$ at point ω is denoted by $W_f(\omega)$ and calculated as follows:

$$W_f(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\omega \cdot x}, \tag{2}$$

where the scalar product of ω and x is defined as $\omega \cdot x = \omega_1 x_1 + \cdots + \omega_n x_n \pmod 2$.

Definition 1 ([22])**.** *The nonlinearity of a Boolean function $f \in \mathcal{B}_n$, denoted by N_f, is defined as the least distance to the set of all affine functions, and it can be obtained through the Walsh transform as follows:*

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|. \tag{3}$$

The function of the original Maiorana–McFarland class is defined as follows:

Definition 2 ([1])**.** *For any positive integers s and k such that $n = s + k$, the Maiorana–McFarland function is a function $f \in \mathcal{B}_n$ defined by*

$$f(y, x) = \phi(y) \cdot x + \pi(y), \qquad x \in \mathbb{F}_2^k, y \in \mathbb{F}_2^s,$$

where ϕ is any mapping from $\mathbb{F}_2^s$ to $\mathbb{F}_2^k$ and $\pi(y) \in \mathcal{B}_s$. When ϕ is a one-to-one mapping and $s = k$, the function is bent.

A spectral characterization of correlation-immune Boolean functions has been derived.

Theorem 1 ([23]). *A Boolean function $f(x) \in \mathcal{B}_n$ is t-resilient, where $0 \leq t \leq n-1$, if and only if its Walsh transform satisfies*

$$W_f(\omega) = 0, \text{ for } 0 \leq wt(\omega) \leq t, \tag{4}$$

where $wt(\omega)$ is the Hamming weight of the vector $\omega \in \mathbb{F}_2^n$, i.e., the number of ones in ω.

It is shown that [24] for a t-resilient Boolean function f, the algebraic degree $deg(f) \leq n-t-1$, and the maximum value is referred to as optimal algebraic degree.

The notion of algebraic immunity was introduced as a measure of resistance to algebraic attacks.

Definition 3 ([25]). *The function $g \in \mathcal{B}_n$ is said to be an annihilator of $f \in \mathcal{B}_n$ if it satisfies that $f(x)g(x) = 0$ for a nonzero $g \in \mathcal{B}_n$. The algebraic immunity of f, denoted by $AI(f)$, is the minimum degree of all nonzero annihilators of f and $1+f$.*

An (n,m) function can be regarded as a mapping from F_2^n to F_2^m , which is $F : F_2^n \rightarrow F_2^m$. In addition, it can be viewed as a collection of m Boolean functions, namely $F(X) = (f_1(X), f_2(X), \cdots, f_m(X))$, where $f_1, f_2, \cdots, f_m \in B_n$ are component Boolean functions.

Definition 4 ([26]). *The nonlinearity of an (n,m) function $F(X) = (f_1(X), f_2(X), \cdots, f_m(X))$ is denoted by N_F:*

$$N_F = \min_{c \in F_2^{m^*}} N_{f_c}, \tag{5}$$

where $f_c = \oplus_{i=1}^m c_i f_i$, $F_2^{m^*} = F_2^m \backslash \{0\}$.

Similarly, the nonlinearity of an (n,m) function can also be denoted by the Walsh transform:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega \in F_2^n, c \in F_2^{m^*}} W_{f_c}(\omega). \tag{6}$$

Definition 5 ([27]). *An (n,m) function $F(X) = (f_1(X), f_2(X), \cdots, f_m(X))$ is t-resilient if and only if for any $c = (c_1, c_2, \cdots, c_m) \in F_2^{m^*}$, $f_c(X_n) = \oplus_{i=1}^m c_i f_i(X_n)$ is t-resilient.*

3. Construction of Boolean Function

In this section, we give several nonlinear functions with special constructions and analyse their spectral distributions, respectively. These functions will be useful in the M-M construction methods, and two methods are given to obtain a balanced and resilient Boolean function with very high nonlinearity. First of all, we consider the case of a simple function with only a single nonlinear term.

3.1. Small Functions with Special ANF

Lemma 1 ([10]). *Let $f(x) = x_1 x_2 \cdots x_n$, then*

$$W_f(\alpha) = \begin{cases} 2^n - 2, & \text{if } \alpha = \mathbf{0} \\ (-1)^{\omega t(\alpha)+1} \cdot 2 & \text{if } \alpha \neq \mathbf{0} \end{cases}.$$

Remark 1. *Let $f = x_1 x_2 \cdots x_k + a \cdot X_n$, where $s + k = n$, $a = (a_k, a_s) \in \mathbb{F}_2^k \times \mathbb{F}_2^s$ and $X_n = (x_1, x_2, \cdots, x_n)$. Let $\alpha \in \mathbb{F}_2^k, \beta \in \mathbb{F}_2^s$, then*

$$W_f(\alpha, \beta) = \begin{cases} 0, & \beta \neq a_s \\ 2^s(2^k - 2), & \beta = a_s, \alpha = a_k \\ (-1)^{wt(\alpha_k + \alpha)+1} 2^{s+1}, & \beta = a_s, \alpha \neq a_k \end{cases}.$$

In Lemma 1 and Remark 1, both functions have only a single nonlinear term. Then, we consider the spectral distributions of some functions with two nonlinear terms.

Theorem 2. *Let $f = x_1x_2\cdots x_i + x_jx_{j+1}\cdots x_n, i < j < n$ be an n-variable Boolean function, and $(\alpha,\beta,\gamma) \in \mathbb{F}_2^i \times \mathbb{F}_2^{j-i-1} \times \mathbb{F}_2^{n-j+1}$, then*

$$W_f(\alpha,\beta,\gamma) = \begin{cases} 2^n - 2^{n-i+1} - 2^j + 2^{j-i+1}, & \alpha = 0, \beta = 0, \gamma = 0 \\ (-1)^{wt(\gamma)+1}(2^j - 2^{j-i+1}), & \alpha = 0, \beta = 0, \gamma \neq 0 \\ (-1)^{wt(\alpha)+1}(2^{n-i+1} - 2^{j-i+1}), & \alpha \neq 0, \beta = 0, \gamma = 0 \\ (-1)^{wt(\alpha)+wt(\gamma)}2^{j-i+1}, & \alpha \neq 0, \beta = 0, \gamma \neq 0 \\ 0, & \beta \neq 0 \end{cases}.$$

Proof of Theorem 2. Let $X = (X_i, X_{j-i-1}, X_{n-j+1}) \in \mathbb{F}_2^i \times \mathbb{F}_2^{j-i-1} \times \mathbb{F}_2^{n-j+1}$, then

$$\begin{aligned} W_f(\alpha,\beta,\gamma) &= \sum_{X\in F_2^n} (-1)^{f+\alpha\cdot X_i+\beta\cdot X_{j-i-1}+\gamma\cdot X_{n-j+1}} \\ &= \sum_{X_i}(-1)^{x_1x_2\cdots x_i+\alpha\cdot X_i} \cdot \sum_{X_{j-i-1}} (-1)^{\beta\cdot X_{j-i-1}} \cdot \sum_{X_{n-j+1}} (-1)^{x_jx_{j+1}\cdots x_n+\gamma\cdot X_{n-j+1}}. \end{aligned}$$

In order to obtain the value of the equation, the following cases are needed.

Case 1: When $\beta \neq 0$,

$$\sum_{X_{j-i-1}\in\mathbb{F}_2^{j-i-1}} (-1)^{\beta\cdot X_{j-i-1}} = 0.$$

Then,

$$W_f(\alpha,\beta,\gamma) = 0.$$

Case 2: When $\beta = 0$,

$$W_f(\alpha,\beta,\gamma) = 2^{j-i-1} \cdot \sum_{X_i}(-1)^{x_1x_2\cdots x_i+\alpha\cdot X_i} \cdot \sum_{X_{n-j+1}} (-1)^{x_jx_{j+1}\cdots x_n+\gamma\cdot X_{n-j+1}}.$$

Let $f_1(x) = x_1x_2\cdots x_i$ be an i-variable Boolean function and $f_2(x) = x_jx_j + 1\cdots x_n$ be an $(n-j+1)$-variable Boolean function, then

$$W_f(\alpha,\beta,\gamma) = 2^{j-i-1}W_{f_1}(\alpha)W_{f_2}(\gamma).$$

According to Lemma 1,

$$W_{f_1}(\alpha) = \begin{cases} 2^i - 2, & \alpha = 0 \\ (-1)^{wt(\alpha)+1}2, & \alpha \neq 0 \end{cases},$$

$$W_{f_2}(\gamma) = \begin{cases} 2^{n-j+1} - 2, & \gamma = 0 \\ (-1)^{wt(\gamma)+1}2, & \gamma \neq 0 \end{cases}.$$

So we have the next four cases:

Case 2.1: When $\alpha = 0, \gamma = 0$, then

$$W_f(\alpha,\beta,\gamma) = 2^{j-i-1}(2^i - 2)(2^{n-j+1} - 2) = 2^n - 2^{n-i+1} - 2^j + 2^{j-i+1}.$$

Case 2.2: When $\alpha = 0, \gamma \neq 0$, then

$$W_f(\alpha,\beta,\gamma) = 2^{j-i-1}(2^i - 2)(-1)^{wt(\gamma)+1}2 = (-1)^{wt(\gamma)+1}(2^j - 2^{j-i+1}).$$

Case 2.3: When $\alpha \neq 0, \gamma = 0$, then

$$W_f(\alpha,\beta,\gamma) = 2^{j-i-1}(-1)^{wt(\alpha)+1}2(2^{n-j+1}-2) = (-1)^{wt(\alpha)+1}(2^{n-i+1}-2^{j-i+1}).$$

Case 2.4: When $\alpha \neq 0, \gamma \neq 0$, then

$$W_f(\alpha,\beta,\gamma) = 2^{j-i-1}(-1)^{wt(\alpha)+1}2(-1)^{wt(\gamma)+1}2 = (-1)^{wt(\alpha)+wt(\gamma)}2^{j-i+1}.$$

According to all cases above, the theorem is proved. □

Theorem 3. *Let $f = x_1x_2\cdots x_j + x_ix_{i+1}\cdots x_n, i < j < n$ be an n-variable Boolean function, and $(\alpha,\beta,\gamma) \in \mathbb{F}_2^{i-1} \times \mathbb{F}_2^{j-i+1} \times \mathbb{F}_2^{n-j}$, then*

$$W_f(\alpha,\beta,\gamma) = \begin{cases} 2^n - 2^i - (2^{n-j+1}-4), & \alpha = 0, \beta = 0, \gamma = 0 \\ (-1)^{wt(\beta)+1}((2^{n-j+1}-4)+2^i), & \alpha = 0, \beta \neq 0, \gamma = 0 \\ (-1)^{wt(\beta)+wt(\gamma)+1}(2^i-4), & \alpha = 0, \gamma \neq 0 \\ (-1)^{wt(\alpha)+wt(\beta)+1}(2^{n-j+1}-4), & \alpha \neq 0, \gamma = 0 \\ 4(-1)^{wt(\alpha)+wt(\beta)+wt(\gamma)}, & \alpha \neq 0, \gamma \neq 0 \end{cases}.$$

Proof of Theorem 3. Let $X = (X_{i-1}, X_{j-i+1}, X_{n-j}) \in \mathbb{F}_2^{i-1} \times \mathbb{F}_2^{j-i+1} \times \mathbb{F}_2^{n-j}$. We have that

$$W_f(\alpha,\beta,\gamma) = \sum_{X\in\mathbb{F}_2^n} (-1)^{f+\alpha\cdot X_{i-1}+\beta\cdot X_{j-i+1}+\gamma\cdot X_{n-j}}.$$

The mutual term between two polynomials $x_1x_2\cdots x_j$ and $x_ix_{i+1}\cdots x_n$ is $x_ix_{i+1}\cdots x_j$. The Walsh spectra will be discussed in the following situations:

Case 1: When $\alpha = 0, \gamma = 0$,

$$W_f(\alpha,\beta,\gamma) = \sum_{X\in\mathbb{F}_2^n} (-1)^{f+\beta\cdot X_{j-i+1}}.$$

In this case, it can be divided into the following two cases according to the value of β:

Case 1.1: When $\beta = 0$,

$$W_f(\alpha,\beta,\gamma) = \sum_{X\in\mathbb{F}_2^n} (-1)^{x_1x_2\cdots x_j+x_ix_{i+1}\cdots x_n}.$$

When X_n runs around $\mathbb{F}_2^n$, a total of $2^{n-j}-1+2^{i-1}-1 = 2^{n-j}+2^{i-1}-2$ ones of the value of $x_1x_2\cdots x_j + x_ix_{i+1}\cdots x_n$ are taken.

Therefore,

$$W_f(\alpha,\beta,\gamma) = 2^n - 2^{n-j+1} - 2^i + 4.$$

Case 1.2: When $\beta \neq 0$,

$$W_f(\alpha,\beta,\gamma) = \sum_{X\in\mathbb{F}_2^n} (-1)^{x_1x_2\cdots x_j+x_ix_{i+1}\cdots x_n+\beta\cdot X_{j-i+1}}.$$

It is known that $\beta \cdot X_{j-i+1}$ is a balanced function, and when X_n runs around $\mathbb{F}_2^n$, there are $2^{n-j}+2^{i-1}-2$ ones of the value of $x_1x_2\cdots x_j + x_ix_{i+1}\cdots x_n$. Note that when $x_1x_2\cdots x_j + x_ix_{i+1}\cdots x_n$ take the value 1, $x_i\cdots x_j$ should be 1.

Therefore,

$$W_f(\alpha,\beta,\gamma) = (-1)^{wt(\beta)+1}(2^{n-j+1}+2^i-4).$$

Case 2: When $\alpha = 0, \gamma \neq 0$, then we have

$$\begin{aligned}
W_f(\alpha,\beta,\gamma) &= \sum_{X\in\mathbb{F}_2^n} (-1)^{x_1x_2\cdots x_j + x_ix_{i+1}\cdots x_n + \beta\cdot X_{j-i+1} + \gamma\cdot X_{n-j}} \\
&= \sum_{X\in\mathbb{F}_2^n, X_{j-i+1}=1} (-1)^{x_1x_2\cdots x_j + x_ix_{i+1}\cdots x_n + \beta\cdot 1 + \gamma\cdot X_{n-j}} \\
&+ \sum_{X\in\mathbb{F}_2^n, X_{j-i+1}\neq 1} (-1)^{\beta\cdot X_{j-i+1} + \gamma\cdot X_{n-j}} \\
&= (-1)^{wt(\beta)} \sum_{X_{i-1}, X_{n-j}} (-1)^{x_1x_2\cdots x_{i-1} + x_{j+1}x_{j+2}\cdots x_n + \gamma\cdot X_{n-j}} \\
&= (-1)^{wt(\beta)} \sum_{X_{i-1}} (-1)^{x_1x_2\cdots x_{i-1}} \sum_{X_{n-j}} (-1)^{x_{j+1}x_{j+2}\cdots x_n + \gamma\cdot X_{n-j}} \\
&= (-1)^{wt(\beta)}(2^{i-1} - 2)(-1)^{wt(\gamma)+1}2 \\
&= (-1)^{wt(\beta)+wt(\gamma)+1}(2^i - 4).
\end{aligned}$$

Case 3: When $\alpha \neq 0, \gamma = 0$,

$$\begin{aligned}
W_f(\alpha,\beta,\gamma) &= \sum_{X\in\mathbb{F}_2^n} (-1)^{x_1x_2\cdots x_j + x_ix_{i+1}\cdots x_n + \alpha\cdot X_{i-1} + \beta\cdot X_{j-i+1}} \\
&= \sum_{X, X_{j-i+1}=1} (-1)^{x_1x_2\cdots x_j + x_ix_{i+1}\cdots x_n + \beta\cdot 1 + \alpha\cdot X_{i-1}} \\
&+ \sum_{X\in\mathbb{F}_2^n, X_{j-i+1}\neq 1} (-1)^{\beta\cdot X_{j-i+1} + \alpha\cdot X_{i-1}} \\
&= (-1)^{wt(\beta)} \sum_{X_{i-1}, X_{n-j}} (-1)^{x_1x_2\cdots x_{i-1} + x_{j+1}x_{j+2}\cdots x_n + \alpha\cdot X_{i-1}} \\
&= (-1)^{wt(\beta)} \sum_{X_{i-1}} (-1)^{x_1x_2\cdots x_{i-1} + \alpha\cdot X_{i-1}} \sum_{X_{n-j}} (-1)^{x_{j+1}x_{j+2}\cdots x_n} \\
&= (-1)^{wt(\beta)}(-1)^{wt(\alpha)+1}2(2^{n-j} - 2) \\
&= (-1)^{wt(\alpha)+wt(\beta)+1}(2^{n-j+1} - 4).
\end{aligned}$$

Case 4: When $\alpha \neq 0, \gamma \neq 0$,

$$\begin{aligned}
W_f(\alpha,\beta,\gamma) &= \sum_{X\in\mathbb{F}_2^n} (-1)^{x_1x_2\cdots x_j + x_ix_{i+1}\cdots x_n + \alpha\cdot X_{i-1} + \beta\cdot X_{j-i+1} + \gamma\cdot X_{n-j}} \\
&= \sum_{X_{j-i+1}=1} (-1)^{x_1x_2\cdots x_j + x_ix_{i+1}\cdots x_n + \beta\cdot 1 + \alpha\cdot X_{i-1} + \gamma\cdot X_{n-j}} \\
&+ \sum_{X_{j-i+1}\neq 1} (-1)^{\beta\cdot X_{j-i+1} + \alpha\cdot X_{i-1} + \gamma\cdot X_{n-j}} \\
&= (-1)^{wt(\beta)} \sum_{X\in\mathbb{F}_2^n, X_{j-i+1}=1} (-1)^{x_1x_2\cdots x_{i-1} + x_{j+1}x_{j+2}\cdots x_n + \alpha\cdot X_{i-1} + \gamma\cdot X_{n-j}} \\
&= (-1)^{wt(\beta)}(-1)^{wt(\alpha)+1}2(-1)^{wt(\gamma)+1}2 \\
&= 4(-1)^{wt(\alpha)+wt(\beta)+wt(\gamma)}.
\end{aligned}$$

Thus, the theorem is proved. □

The above theorems give some nonlinear functions with special spectral distributions. The following constructions shows that these nonlinear functions can be used as the small functions in the modified M-M construction method, and two classes of balanced and resilient Boolean functions with very high nonlinearity are obtained.

3.2. Balanced Boolean Function with High Nonlinearity

Construction 1. *Let $n \geq 8$ be even, and ϕ be a bijective mapping from $\mathbb{F}_2^{n/2}$ to $\mathbb{F}_2^{n/2}$. Let $\phi(\mathbf{0}) = \mathbf{0}$ and $\phi(\delta) = \theta$ with δ be a fixed vector satisfying that $wt(\theta) > k$ for $k \leq n/2$. Let $y = (y_1, \cdots, y_{n/2})$, $x = (x_1, \cdots, x_{n/2})$. For any $(y, x) \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2}$, a Boolean function $f \in B_n$ can be obtained as follows:*

$$f(y, x) = \sum_{b \in \mathbb{F}_2^{n/2}} y^b g_b(x),$$

where

$$y^b = \begin{cases} 1, & y = b \\ 0, & y \neq b \end{cases},$$

and for any $\{i_1, \cdots, i_k\} \subseteq \{1, \cdots, n/2\}, \{j_1, \cdots, j_k\} \subseteq \{1, \cdots, n/2\}$,

$$g_b(x) = \begin{cases} \phi(b) \cdot x, & b \notin \{\mathbf{0}, \delta\} \\ \phi(\delta) \cdot x \oplus x_{i_1} x_{i_2} \cdots x_{i_k}, & b = \mathbf{0} \\ \phi(\delta) \cdot x \oplus x_{j_1} x_{j_2} x_{j_k} \oplus 1, & b = \delta \end{cases}.$$

Theorem 4. *Let f be the function obtained by the above construction, and n is even, $n \geq 8$. Then, we have:*

1. *f is balanced;*
2. *$\deg(f) = n/2 + k$;*
3. *$N_f = 2^{n-1} - 2^{n/2} + 2^{n/2-2}$.*

Proof of Theorem 4. For any $(\beta, \alpha) \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2}$, we have

$$\begin{aligned} W_f(\beta, \alpha) &= \sum_{(y,x) \in \mathbb{F}_2^n} (-1)^{f(y,x) + (\beta,\alpha) \cdot (y,x)} \\ &= \sum_{b \in \mathbb{F}_2^{n/2}} (-1)^{\beta \cdot b} \sum_{x \in \mathbb{F}_2^{n/2}} (-1)^{g_b(x) + \alpha \cdot x} \\ &= \sum_{b \in \mathbb{F}_2^{n/2}} (-1)^{\beta \cdot b} \cdot W_{g_b}(\alpha). \end{aligned}$$

When $b \notin \{\mathbf{0}, \delta\}$,

$$W_{g_b}(\alpha) = \begin{cases} 2^{n/2}, & \alpha = \phi(b) \\ 0, & \alpha \neq \phi(b) \end{cases}.$$

Let $\alpha = (\alpha_1, \cdots, \alpha_{n/2}), \alpha_i{}' = (\alpha_{i_1}, \cdots, \alpha_{i_k}), \alpha_i{}'' = (\alpha_{i_{k+1}}, \cdots, \alpha_{i_{n/2}}), \{i_1, \cdots, i_k\} \cup \{i_{k+1}, \cdots, i_{n/2}\} \subseteq \{1, \cdots, n/2\}$. Let $\theta_i{}' = (\theta_{i_1}, \cdots, \theta_{i_k}), \theta_i{}'' = (\theta_{i_{k+1}}, \cdots, \theta_{i_{n/2}})$.

When $b = \mathbf{0}$,

$$W_{g_b}(\alpha) = \begin{cases} 2^{n/2} - 2^{n/2-2}, & \alpha = \phi(\delta) \\ \pm 2^{n/2-2}, & \alpha_j{}' \neq \theta_j{}', \alpha_i{}'' = \theta_i{}'' \\ 0, & \alpha_i{}'' \neq \theta_i{}'' \end{cases}.$$

Let $\alpha_j{}' = (\alpha_{j_1}, \cdots, \alpha_{j_k}), \alpha_j{}'' = (\alpha_{j_{k+1}}, \cdots, \alpha_{j_{n/2}}), \{j_1, \cdots, j_k\} \cup \{j_{k+1}, \cdots, j_{n/2}\} \subseteq \{1, \cdots, n/2\}$. Let $\theta_j{}' = (\theta_{j_1}, \cdots, \theta_{j_k}), \theta_j{}'' = (\theta_{j_{k+1}}, \cdots, \theta_{j_{n/2}})$.

When $b = \delta$,

$$W_{g_b}(\alpha) = \begin{cases} 2^{n/2} - 2^{n/2-2}, & \alpha = \phi(\delta) \\ \pm 2^{n/2-2}, & \alpha_j{}' \neq \theta_j{}', \alpha_j{}'' = \theta_j{}'' \\ 0, & \alpha_j{}'' \neq \theta_j{}'' \end{cases}.$$

Thus,

$$max|W_f(\alpha)| = 2^{n/2+1} - 2^{n/2-1}.$$

That means

$$N_f = 2^{n-1} - 2^{n/2} + 2^{n/2-2}.$$

When $b \notin \{0, \delta\}$, we have

$$W_{g_b}(0) = 0.$$

Since $wt(\theta) > k$, when $b = 0$ and $b = \delta$, we have

$$\alpha_i{}'' \neq \theta_i{}'', \alpha_j{}'' \neq \theta_j{}''.$$

This means $W_{g_0}(0) = 0$ and $W_{g_\delta}(0) = 0$. Thus, for any $b \in F_2^n$, $W_{g_b}(0) = 0$. So, we have $W_f(0) = \sum_{b \in F_2^{n/2}} W_{g_b}(0) = 0$, and f is balanced.

Obviously, the terms $y_1 y_2 \cdots y_{n/2} x_{i_1} x_{i_2} \cdots x_{i_k}$ and $y_1 y_2 \cdots y_{n/2} x_{j_1} x_{j_2} \cdots x_{j_k}$ are all in the ANF of the function and cannot cancel each other out. Thus, $\deg(f) = n/2 + k$. □

Remark 2. *In this subsection, we provide some small nonlinear functions with special Walsh spectrum which can be applied to construction method of M-M functions, and Construction 1 shows a method to obtain a balanced Boolean function using the small functions. It is known that the best nonlinearity for a balanced function is given by Seberry et al. in [3] and Dobbertin in [4]. When $n < 10$, the nonlinearity in Construction 1 can equal the best result, but when $n > 12$, the nonlinearity will be smaller. Further research on the applications of the small function in Theorems 2 and 3, such as using the high-meets-low technology [15], will be an interesting challenge.*

3.3. The Algebraic Immunity

Next, we discuss the algebraic immunity of the functions in Construction 1. Let $y = (y_1, y_2, \cdots, y_{n/2})$, $\tau = (\tau_1, \tau_2, \cdots, \tau_{n/2})$, then $f(y, x)$ can be represented as

$$f(y, x) = f_1(y, x) + f_2(y, x),$$

where

$$f_1(y, x) = \sum_{\tau \in \mathbb{F}_2^{n/2} \setminus \Delta} (\prod_{i=1}^{n/2} (y_i + \tau_i + 1)) g_{c_\tau}(x),$$

where $g_{c_\tau}(X) = c_\tau \cdot X$, $wt(c_\tau) \neq 0$, and $\Delta = \{0, \delta\}$. We define $f_1'(y, x) = \phi(y) \cdot x + \pi(y)$ as an M-M bent function containing $f_1(y, x)$ as a part of its ANF. Then, $f(y, x)$ can be rewritten as the following form:

$$f(y, x) = f_1'(y, x) + f_2'(y, x).$$

Let f and g be two n-variable functions. Noticing

$$AI(f) - deg(g) \leq AI(f + g) \leq AI(f) + deg(g),$$

we have

$$AI(f_1'(y, x)) - deg(f_2'(y, x)) \leq AI(f(y, x)) \leq AI(f_1'(y, x)) + deg(f_2'(y, x)). \tag{7}$$

As it is known that

$$AI(f_1'(y, x)) \leq deg(\phi) + AI(\pi(y)) + 1. \tag{8}$$

By Inequations (7) and (8), it can be seen that the degree of the permutation ϕ and the algebraic immunity of function $\pi(y)$ will have a great effect on the $AI(f(y,x))$, and the functions $g_0(x)$ and $g_\delta(x)$ chosen in the constructions may also influence the algebraic immunity of $f(y,x)$. Simulations show that the usage of different ϕ, $g_0(x)$, $g_\delta(x)$ and $\pi(y)$ will result in different algebraic immunity. Since the mapping ϕ, the functions $\pi(y)$, $g_0(x)$ and $g_\delta(x)$ used in the construction do not need to be unique, so in our constructions, for a fixed n, we can easily obtain a large number of balanced functions with the same high nonlinearity but different algebraic immunity. The following examples list balanced functions that possess good algebraic immunity and high nonlinearity.

Example 1. *When $n = 8, k = 3$, and $(y,x) \in \mathbb{F}_2^4 \times \mathbb{F}_2^4$, $f(y,x) = \sum_{b \in \mathbb{F}_2^4} y^b g_b(x)$. According to Theorem 4, it is a balanced Boolean function, and $\deg(f) = n/2 + k = 4 + 3 = 7$ is the known optimal algebraic degree, $N_f = 2^{n-1} - 2^{n/2} + 2^{n/2-2} = 116$ is equal to the best nonlinearity in [3,4]. The truth table of $f(y,x)$ is as follows:*

$$\begin{aligned}&0110100010010111||0101010101010101||0011001100110011||0110011001100110||\\&0000111100001111||0101101001011010||0011110000111100||0110100101101001||\\&0000000011111111||0101010110101010||0011001111001100||0110011010011001||\\&0000111111110000||0101101010100101||0011110011000011||1001011001101010.\end{aligned}$$

3.4. Resilient Boolean Function with High Nonlinearity

Definition 6 ([11])**.** *A set of Boolean functions $\{g_1, g_2, \cdots, g_c\} \in \mathcal{B}_n$ such that for any $\alpha \in \mathbb{F}_2^n$,*

$$W_{g_i}(\alpha) W_{g_j}(\alpha) = 0,\ 1 \le i < j \le c, \tag{9}$$

is called a set of disjoint spectra functions.

Obviously, the following set of all $n/2$-variable t-resilient affine functions

$$T_1 = \{g_c(x) = c \cdot x \mid c \in \mathbb{F}_2^{n/2}, wt(c) > t\},$$

is a set of disjoint spectra functions.

Let $x = (x', x'')$, where $x' \in \mathbb{F}_2^{n/2-2k}$, $x'' \in \mathbb{F}_2^{2k}$ and $h(x'')$ be a fixed $2k$-variable function. Then,

$$T_2 = \{g_{c'}(x) = c' \cdot x' + h(x'') \mid c' \in \mathbb{F}_2^{n/2-2k}, wt(c') > p\}$$

is also a set of disjoint spectra functions. If $h_{c'}(x'')$ is q-resilient, then $g_{c'}(X)$ is $(p+q+1)$-resilient.

Construction 2. *Let $n \ge 12, 1 \le t \le n/2 - 2, 1 \le k < n/4$ and $p + q + 1 = t$ satisfying that $\sum_{i=0}^{t} \binom{n/2}{i} \le \sum_{i=p+1}^{n/2-2k} \binom{n/2-2k}{i} = |T_2|$. Let $T_2' \subseteq T_2$ with $|T_2'| = \sum_{i=0}^{t} \binom{n/2}{i}$, and $T = T_1 \cup T_2'$. Let $x \in \mathbb{F}_2^{n/2}, y \in \mathbb{F}_2^{n/2}$ and ϕ be a bijective mapping from $\mathbb{F}_2^{n/2}$ to T. Then, we construct the function $f \in \mathcal{B}_n$ as follows:*

$$f(y,x) = \bigoplus_{b \in \mathbb{F}_2^{n/2}} y^b \phi(b), y \in \mathbb{F}_2^{n/2}, \tag{10}$$

where y^b is defined as in Construction 1.

Theorem 5. *Let $f(y,x)$ be as in Construction 2. Then,*

1. *f is t-resilient;*
2. *$N_f = 2^{n-1} - 2^{n/2} + 2^{n/2-2k} N_h$;*
3. *$deg(f) = n/2 + deg(h)$.*

Proof of Theorem 5. Let $(\beta, \alpha) = \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2}$, Then,

$$\begin{aligned} W_f(\beta, \alpha) = \sum_{y \in \mathbb{F}_2^{n/2}} \sum_{x \in \mathbb{F}_2^{n/2}} (-1)^{f(y,x)+\alpha \cdot x + \beta \cdot y} \\ = \sum_{b \in \mathbb{F}_2^{n/2}} (-1)^{\beta \cdot b} \sum_{x \in \mathbb{F}_2^{n/2}} (-1)^{\phi(b)+\alpha \cdot x} \\ = \sum_{b \in \mathbb{F}_2^{n/2}} (-1)^{\beta \cdot b} W_{\phi(b)}(\alpha). \end{aligned}$$

Note that the functions $\phi(b)$ are t-resilient. When $0 \le wt(\beta, \alpha) \le t$, we have $0 \le wt(\alpha) \le t$, so $W_{\phi(b)}(\alpha) = 0$. Thus, $W_f(\beta, \alpha) = 0$, which means $f(y, x)$ is t-resilient.

It is known that for any $\phi(b) \in T_1$, $W_{\phi(b)}(\alpha) = 2^{n/2}$, and for any $\phi(b) \in T_2$, $W_{\phi(b)}(\alpha) = 2^{n/2-2k}(2^{2k} - 2N_h)$. Since T_1 and T_2 are two sets of disjoint spectra functions

$$\max_{(\beta,\alpha)} |W_f(\beta, \alpha)| = 2^{n/2} + 2^{n/2} - 2^{n/2-2k+1} N_h,$$

which means

$$N_f = 2^{n-1} - 2^{n/2} + 2^{n/2-2k} N_h.$$

Similar to the proof of Theorem 1, the algebraic degree is $n/2 + deg(h)$. □

Example 2. *For $n = 44, t = 2$, let $k = 7$, $p = 0$ and $q = 1$. We have $\sum_{i=0}^{2} \binom{44/2}{i} \le \sum_{i=1}^{8} \binom{8}{i}$. Let $T_2' \subseteq T_2$ with $|T_2'| = 254$. Let h be a 14-variable, 1-resilient function with nonlinearity 8100 and ϕ be a bijective mapping from $\mathbb{F}_2^{22}$ to $T = T_1 \cup T_2'$. By Construction 2, we can construct a 2-resilient function $f \in \mathcal{B}_{20}$ with nonlinearity $2^{43} - 2^{21} - 2^{14} - 2^{12} - 2^{11} - 2^{10}$, which agrees with Theorem 2 and has nonlinearity larger than [11].*

In this subsection, a construction method to obtain a resilient Boolean function with high nonlinearity is given. Since this method is also a modified M-M class, the algebraic properties are similar to the balanced case.

4. Construction of Vectorial Boolean Function

In this section, by using disjoint linear codes and vector matrices with special properties, a class of resilient (n, m) function with very high nonlinearity is given.

4.1. Disjoint Linear Codes and Vector Matrices

Definition 7 ([19])**.** *Disjoint linear codes are a set of $[u, m, t]$ linear codes $C = \{C_1, C_2, \cdots, C_N\}$ satisfying that:*

$$C_i \cap C_j = \{\mathbf{0}\}, 1 \le i < j \le N.$$

*where **0** is the all-zero vector.*

We denote $N(u, m, t)$ the number of $[u, m, t]$ disjoint linear codes, where t is the minimum weight of the $[u, m]$ code.

Lemma 2 ([18])**.** *Let $\theta_0, \cdots, \theta_{m-1}$ be a basis of a $[u, m, t+1]$ linear code C. Let β be a primitive elememt of $\mathbb{F}_{2^m}$, and let $(1, \beta, \cdots, \beta^{m-1})$ be a polynomial basis in $\mathbb{F}_{2^m}$. Define a bijection $\phi : \mathbb{F}_{2^m} \to C$,*

$$\phi(b_0 + b_1\beta + \cdots + b_{m-1}\beta^{m-1}) = b_0\theta_0 + \cdots + b_{m-1}\theta_{m-1}.$$

Define the matrix A that contains all the code words by

$$A = \begin{pmatrix} \phi(1) & \phi(\beta) & \cdots & \phi(\beta^{m-1}) \\ \phi(\beta) & \phi(\beta^2) & \cdots & \phi(\beta^m) \\ \vdots & \vdots & \ddots & \vdots \\ \phi\left(\beta^{2^m-2}\right) & \phi(1) & \cdots & \phi(\beta^{m-2}) \end{pmatrix}.$$

Then, for any nonzero linear combination of all columns in matrix A, each nonzero code word of C appears only once.

Lemma 3 ([20])**.** *Let u, m, d be integers with $2 \leq m \leq u$. Let α be a root of the primitive polynomial $p(x) = 1 + p_1 x + \cdots + p_{k-1}x^{k-1} + x^u \in \mathbb{F}_2[x]$, and $\left(1, \alpha, \alpha^2, \cdots \alpha^{u-1}\right)$ be a polynomial basis of $\mathbb{F}_{2^u}$. Define a bijection $\pi : \mathbb{F}_{2^u} \to \mathbb{F}_2^u$,*

$$\pi(b_0 + b_1\alpha + \cdots + b_{u-1}\alpha^{u-1}) = (b_0, b_1, \cdots, b_{u-1}).$$

Define matrix B of size $(2^u - 1) \times m$ by

$$B = \begin{pmatrix} \pi(1) & \pi(\alpha) & \cdots & \pi(\alpha^{m-1}) \\ \pi(\alpha) & \pi(\alpha^2) & \cdots & \pi(\alpha^m) \\ \vdots & \vdots & \ddots & \vdots \\ \pi\left(\alpha^{2^u-2}\right) & \pi(1) & \cdots & \pi(\alpha^{m-2}) \end{pmatrix} = \begin{pmatrix} B_0 \\ B_1 \\ \vdots \\ B_{2^u-2} \end{pmatrix}.$$

It is known that for any nonzero linear combination of columns in matrix B, the nonzero vector in $\mathbb{F}_2^u$ appears only once. If for any vector $c \in \mathbb{F}_2^{m*}$ such that $wt(c \cdot B_i) \leq t$, where $i = 0, 1, \cdots, 2^u - 2$. Then, this row will be deleted from matrix B. Thus, we will obtain a new matrix $\widetilde{B}$. The number of rows of matrix $\widetilde{B}$ is denoted by $M(u, m, t+1)$.

4.2. Resilient Vectorial Function with High Nonlinearity

Construction 3. *Let $n = 2u \geq 12$ be even. Let m, t, k be positive integers with $m, t < \lfloor n/4 \rfloor$ and $m < k < u$. Let $X_n = \left(X'_u, X''_u\right) = \left(X'_{n-k}, X''_k\right) \in \mathbb{F}_2^n$ with $X'_u, X''_u \in \mathbb{F}_2^u$, $X'_{n-k} \in \mathbb{F}_2^{n-k}$, and $X''_k \in \mathbb{F}_2^k$. Then, an (n, m) function can be constructed as*

$$\mathbb{F}(X_n) = [f_1(X_n), f_2(X_n), \cdots, f_m(X_n)], \tag{11}$$

where for any $i = 1, 2, \cdots, m$,

$$f_i(X_n) = \begin{cases} \varphi_i\left(X'_u\right) \cdot X''_u, X'_u \in E_0 \\ \psi_i\left(X'_{n-k}\right) \cdot X''_k, X'_{n-k} \in E_1 \end{cases} \tag{12}$$

and ψ_i, φ_i, E_0, E_1 are defined as follows.

Let $C_1, C_2, \cdots, C_s$ be a set of $[u, m, t+1]$ disjoint linear codes satisfying that $s = N(u, m, t+1)$. Let $A_1, \cdots, A_s$ be the matrices associated with $C_1, C_2, \cdots, C_s$ as defined in Lemma 2. For $1 \leq j \leq s$ and $1 \leq i \leq m$, we denote A_j^i the i column of matrix A_j and

$$\widetilde{A} = \begin{pmatrix} A_1^1 & A_1^2 & \cdots & A_1^m \\ A_2^1 & A_2^2 & \cdots & A_2^m \\ \vdots & \vdots & \ddots & \vdots \\ A_s^1 & A_s^2 & \cdots & A_s^m \end{pmatrix}.$$

It is easy to know that the size of the matrix $\widetilde{A}$ is $s \cdot (2^m - 1) \times m$. Let $E_0 = \{e_1, \cdots, e_\delta\} \subset \mathbb{F}_2^u$ and $\delta = s \cdot (2^m - 1)$. For any $1 \le i \le m$, φ_i will be a bijective from E_0 to $\widetilde{A}$:

$$\begin{pmatrix} \varphi_1(e_1) & \varphi_2(e_1) & \cdots & \varphi_m(e_1) \\ \varphi_1(e_2) & \varphi_2(e_2) & \cdots & \varphi_m(e_2) \\ \vdots & \vdots & \ddots & \vdots \\ \varphi_1(e_\delta) & \varphi_2(e_\delta) & \cdots & \varphi_m(e_\delta) \end{pmatrix} = \widetilde{A}.$$

In Lemma 3, let π be a bijective from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2^k$, then a matrix $\widetilde{B}$ of the size $M(k, m, t+1) \times m$ can be obtained. We define $E_1 = (\mathbb{F}_2^u \backslash E_0) \times \mathbb{F}_2^{u-k} = \{\epsilon_1, \cdots, \epsilon_\gamma\} \subset \mathbb{F}_2^{n-k}$, then $\gamma = |E_1| = 2^{u-k} \cdot (2^u - s \cdot (2^m - 1)) = 2^{u-k} \cdot (2^u - N(u, m, t+1) \cdot (2^m - 1))$. For any $1 \le i \le m$, ψ_i will be a bijective from E_1 to $\widetilde{B}_\gamma$:

$$\begin{pmatrix} \psi_1(\epsilon_1) & \psi_2(\epsilon_1) & \cdots & \psi_m(\epsilon_1) \\ \psi_1(\epsilon_2) & \psi_2(\epsilon_2) & \cdots & \psi_m(\epsilon_2) \\ \vdots & \vdots & \ddots & \vdots \\ \psi_1(\epsilon_\gamma) & \psi_2(\epsilon_\gamma) & \cdots & \psi_m(\epsilon_\gamma) \end{pmatrix} = \widetilde{B}_\gamma$$

where $\widetilde{B}_\gamma$ consists of any γ rows of $\widetilde{B}$.

Theorem 6. *Let $\mathbb{F}(X_n) = [f_1(X_n), f_2(X_n), \cdots, f_m(X_n)]$ be the vectorial functions constructed above. Then, we have*

1. *$\mathbb{F}$ is t-resilient;*
2. *$N_f = 2^{n-1} - 2^{n/2-1} - 2^{k-1}$.*

Proof of Theorem 6. From the definitions of φ_i and ψ_i, it is known that both of them are bijective. Let $\alpha = \left(\beta', \beta''\right) = \left(\gamma', \gamma''\right) \in \mathbb{F}_2^n$ with $\beta', \beta'' \in \mathbb{F}_2^u$, $\gamma' \in \mathbb{F}_2^{n-k}$ and $\gamma'' \in \mathbb{F}_2^k$. For any $c \in \mathbb{F}_2^m$, let $f_c(X_n) = c \cdot \mathbb{F}(X_n)$. Then, we have

$$W_{f_c}(\alpha) = \sum_{X_n \in \mathbb{F}_2^n} (-1)^{f_c(X_n) \oplus \alpha \cdot X_n} = H_1 + H_2.$$

where

$$\begin{aligned} H_1 &= \sum_{X'_u \in E_0} \sum_{X''_u \in \mathbb{F}_2^u} (-1)^{\varphi_c\left(X'_u\right) \cdot X''_u \oplus \left(\beta', \beta''\right) \cdot \left(X'_u, X''_u\right)} \\ &= \sum_{X'_u \in E_0} (-1)^{\beta' \cdot X'_u} \sum_{X''_u \in \mathbb{F}_2^u} (-1)^{\left(\varphi_c\left(X'_u\right) + \beta''\right) \cdot X''_u}, \end{aligned}$$

and

$$H_2 = \sum_{X'_{n-k} \in E_1} (-1)^{\gamma' \cdot X'_{n-k}} \sum_{X''_k \in \mathbb{F}_2^k} (-1)^{\left(\psi_c\left(X'_{n-k}\right) + \gamma''\right) \cdot X''_k}.$$

When $\varphi_c^{-1}\left(\beta''\right) = \emptyset$, we have $H_1 = 0$, otherwise $H_1 = 2^{n/2} \cdot (-1)^{\beta' \cdot \varphi_c^{-1}\left(\beta''\right)} = \pm 2^{n/2}$. So $H_1 \in \left\{0, \pm 2^{n/2}\right\}$, in the same way, $H_2 \in \left\{0, \pm 2^k\right\}$. Thus, the maximum value of $|W_{f_c}|$ is $2^{n/2} - 2^k$.

According to (3),

$$N_{f_c} = 2^{n-1} - 2^{n/2-1} - 2^{k-1}.$$

Combined with (5), we can obtain that the nonlinearity of the constructed function $\mathbb{F}$ is

$$N_{\mathbb{F}} = 2^{n-1} - 2^{n/2-1} - 2^{k-1}.$$

When $0 \le wt(\alpha) \le t$, we have $wt\left(\beta''\right) \le t$ and $wt\left(\gamma''\right) \le t$. Therefore, for $X_u' \in E_0$ and $X_{n-k}' \in E_1$, by the definitions of ψ_i and φ_i, we can obtain $wt\left(\psi_c\left(X_u'\right)\right) \ge t+1$ and $wt\left(\varphi_c\left(X_{n-k}'\right)\right) \ge t+1$. Obviously, $\psi_c\left(X_u'\right) + \beta'' \ne 0$ and $\varphi_c\left(X_{n-k}'\right) + \gamma'' \ne 0$. Thus, $H_1 = H_2 = 0$, which means for any $0 \le wt(\alpha) \le t$, $W_{f_c}(\alpha) = 0$. By Theorem 1, f_c is a t-resilient function and so is $\mathbb{F}$. □

Remark 3. *In Construction 3, the numbers of rows of the matrixs $\widetilde{A}$ and $\widetilde{B}$ should be enough to ensure that both φ_i and ψ_i are bijective mappings. Hence, the following inequation must hold $N(u,m,t+1) \cdot (2^m - 1) \cdot 2^u + M(k,m,t+1) \cdot 2^k \ge 2^n$, where the value of $N(u,m,t+1)$ and $M(k,m,t+1)$ can be found in [19,20].*

Example 3. *Let $n = 32$, $m = 4$, $t = 1$ and $k = 11$. Note that $N(16,4,2) = 4365$, $M(11,4,2) = 1957$ and $4365 \times (2^4 - 1) \times 2^{16} + 1957 \times 2^{11} \ge 2^{32}$ holds. By Construction 2, a 1-resilient $(32,4)$ functions with nonlinearity $\left(32,4,1,2^{31} - 2^{15} - 2^{11}\right)$ can be obtained. The nonlinearity of this function is better than the results in [19,20].*

Based on Construction 3, we list some results in Table 1:

Table 1. $(n,m,t,N_{\mathbb{F}})$ S-boxes with higher nonlinearity than [19].

Ours	[19]
$(22,4,1,2^{21} - 2^{10} - 2^{8})$	$(22,4,1,2^{21} - 2^{10} - 2^{9})$
$(30,4,1,2^{29} - 2^{14} - 2^{10})$	$(30,4,1,2^{29} - 2^{14} - 2^{11})$
$(32,4,1,2^{31} - 2^{15} - 2^{10})$	$(32,4,1,2^{31} - 2^{15} - 2^{11})$
$(28,5,1,2^{27} - 2^{13} - 2^{10})$	$(28,5,1,2^{27} - 2^{13} - 2^{11})$
$(38,5,1,2^{37} - 2^{18} - 2^{13})$	$(38,5,1,2^{37} - 2^{18} - 2^{14})$
$(42,5,1,2^{41} - 2^{20} - 2^{13})$	$(42,5,1,2^{41} - 2^{20} - 2^{14})$
$(32,6,1,2^{31} - 2^{15} - 2^{12})$	$(32,6,1,2^{31} - 2^{15} - 2^{13})$
$(58,7,1,2^{57} - 2^{28} - 2^{18})$	$(58,7,1,2^{57} - 2^{28} - 2^{19})$

The table shows that our constructions can sometimes obtain functions with higher nonlinearity than the known result. In other cases, our methods can at least provide the same nonlinearity as the known result, and how to improve the nonlinearity in the equal cases will be the future work.

5. Conclusions

This paper introduces three construction methods to obtain Boolean functions and vectorial Boolean functions with good properties. Firstly, several types of nonlinear functions with special Walsh spectra are given. They can be used in the modified M-M construction methods. For instance, the functions with only a nonlinear term are usually used to optimize the algebraic degree, and in this paper we use them to obtain balanced and resilient functions with high nonlinearity. How to use the other special functions provided is a very interesting research problem. Secondly, a construction of resilient vectorial Boolean function with very high nonlinearity is proposed. The construction combines the disjoint linear codes and the vector matrices with special properties together and provides some functions with currently best-known nonlinearity. Further improvements towards increasing the output dimension as much as possible under the premise of ensuring the nonlinearity appear to be an interesting research task.

Author Contributions: L.L. worked on conceptualization, methodology, writing—original draft preparation, research, and formal analysis of the work; L.W. conducted the formal analysis, writing—original draft preparation and supervision; Q.Z. was dedicated to visualization, software, validation, and writing—review and editing; D.Z. dedicated himself to project administration, writing—review and editing, and supervision. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (No. 61902314), the Natural Science Basic Research Plan in Shaanxi Province of China (No. 2019JQ867), the Equipment Pre-research Key Laboratory Foundation of China (No. 6142103190101) and the Natural Science Foundation of Shaanxi Provincial Department of Education (No. 20JK0911).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Camion, P.; Carlet, C.; Charpin, P.; Sendrier, N. On Correlation-Immune Functions. In *International Cryptology Conference on Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1991; pp. 86–100.
2. Rothaus, O.S. On bent function. *J. Comb. Theory Ser. A* **1976**, *20*, 300–305. [CrossRef]
3. Seberry, J.; Zhang, X.M.; Zheng, Y.L. Nonlinearly balanced Boolean functions and their propagation characteristics. In *Advances in Cryptology—CRYPTO*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1993; Volume 773, pp. 49–60.
4. Dobbertin, H. Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity. In *Fast Software Encryption*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 1994; pp. 61–74.
5. Sarkar, P.; Maitra, S. Construction of nonlinear Boolean functions with important crypto -graphic properties. In *Advances in Cryptology—EUROCRYPT 2000*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2000 ; pp. 485–506.
6. Tarannikov, Y. New Constructions of Resilient Boolean Functions with Maximal Nonlinearity. In Proceedings of the International Workshop on Fast Software Encryption, Yokohama, Japan, 2–4 April 2000; Springer: Berlin/Heidelberg, Germany, 2001; pp. 66–77.
7. Fedorova, M.; Tarannikov, Y. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices. In Proceedings of the International Conference on Cryptology in India, Chennai, India, 16–20 December 2022; Springer: Berlin/Heidelberg, Germany, 2001; pp. 254–266.
8. Carlet, C. A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction. In *Advances in Cryptology— Eurocrypt 2002*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2002; pp. 549–564.
9. Maitra, S.; Pasalic, E. A Maiorana-McFarland type construction for resilient Boolean functions on variables (even) with nonlinearity. *Discret. Appl. Math.* **2006**, *154*, 357–369. [CrossRef]
10. Pasalic, E. Maiorana-McFarland class: Degree optimization and algebraic properties. *IEEE Trans. Inf. Theory* **2006**, *52*, 4581–4594. [CrossRef]
11. Zhang, W.G.; Pasalic, E. Construction of almost optimal resilent Boolean functions on large even number of variables. *IEEE Trans. Inf. Theory* **2009**, *55*, 5822–5831. [CrossRef]
12. Tarannikov, Y. Generalized proper matrices and constructing of *m*-resilient Boolean functions with maximal nonlinearity for expanded range of parameters. *Cryptol. ePrint Arch.* **2014**, *11*, 229–245.
13. Zhang, W.G.; Pasalic, E. Generalized Maiorana-McFarland construction of resilient Boolean functions with high nonlinearity and good algebraic properties. *IEEE Trans. Inf. Theory* **2014**, 60, 6681–6695. [CrossRef]
14. Zhang, F.R.; Wei, Y.Z.; Pasalic, E. Large sets of disjoint spectra plateaued functions inequivalent to partially linear functions. *IEEE Trans. Inf. Theory* **2018**, 64, 2987–2999. [CrossRef]
15. Zhang, W.G. High-Meets-Low: Construction of Strictly Almost Optimal Resilient Boolean Functions via Fragmentary Walsh Spectra. *IEEE Trans. Inf. Theory* **2019**, *65*, 5856–5864. [CrossRef]
16. Sosa-Gómez, G.; Paez-Osuna, O.; Rojas, O.; Rodrigues, P.L.d.A.; Kanarek, H.; Madarro-Capo, E.J. Construction of Boolean Functions from Hermitian Codes. *Mathematics* **2022**, *10*, 899. [CrossRef]
17. Cheon, J.H. Nonlinear Vector Resilient Functions. In *Advances in Cryptology—CRYPTO*; Lecture Notes in Computer Science; Kilian, J., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2139, pp. 458–469.
18. Johansson, T.; Pasalic, E. A construction of resilient functions with high nonlinearity. *IEEE Trans. Inf. Theory* **2003**, *49*, 494–501. [CrossRef]
19. Zhang, W.G.; Pasalic, E. Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes. *IEEE Trans. Inf. Theory* **2014**, *60*, 1638–1651. [CrossRef]
20. Zhang, W.G.; Li, L.Y.; Pasalic, E. Construction of resilient S-boxes with higher-dimensional vectorial outputs and strictly almost optimal non-linearity. *IET Inf. Secur.* **2017**, *11*, 199–203. [CrossRef]

21. Zhao, H.; Wei, Y. New construction of highly nonlinear resilient S-boxes via linear codes. *Front. Comput. Sci.* **2022**, *16*, 1–7. [CrossRef]
22. Meier, W.; Staffelbach, O. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology-Eurocrypt 1990*; Lecture Notes in Computer Sceince; Springer: Berlin/Heidelberg, Germany, 1990; Volume 434, pp. 549–562.
23. Xiao, G.; Massey, J.L. A spectral characterization of correlation-immune combining functions. *IEEE Trans. Inf. Theory* **1988**, *34*, 569–571. [CrossRef]
24. Siegenthaler, T. Correalation immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Inf. Theory* **1984**, *30*, 776–780. [CrossRef]
25. Meier, W.; Pasalic, E.; Carlet, C. Algebraic attacks and decomposition of Boolean functions. In *Advances in Cryptology—EUROCRYPTO 2004*; Lecture Notes in Computer Sceince; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3027, pp. 474–491.
26. Nyberg, K. On the Construction of Highly Nonlinear Permutations. In *Advances in Cryptology—EUROCRYPT' 92. EUROCRYPT 1992*; Lecture Notes in Computer Science; Rueppel, R.A., Ed.; Springer: Berlin/Heidelberg, Germany, 1993; Volume 658, pp. 92–98.
27. Zhang, X.M.; Zheng, Y. Cryptographically resilient functions. *IEEE Trans. Inf. Theory* **1997**, *43*, 1740–1747. [CrossRef]