ELSEVIER

Available at www.ElsevierComputerScience.com
POWERED BY SCIENCE @ DIRECT®

Journal of Complexity 20 (2004) 266–283

Journal of COMPLEXITY

http://www.elsevier.com/locate/jco

On the constructions and nonlinearity of binary vector-output correlation-immune functions ☆

Lusheng Chen,[a] Fang-Wei Fu,[b,*,1] and Victor K.-W. Wei[c]

[a] *Department of Mathematics, Nankai University, Tianjin 300071, P.R.China*

[b] *Temasek Laboratories, National University of Singapore, 10 Kent Ridge Crescent, Singapore 119260, Republic of Singapore*

[c] *Department of Information Engineering, The Chinese University of Hong Kong, Shatin, N.T., Hong Kong*

Received 29 October 2002; accepted 12 August 2003

Dedicated to Professor Harald Niederreiter on the occasion of his 60th birthday.

Abstract

The binary vector-output correlation-immune functions are studied in this paper. Some important properties of vector-output correlation-immune functions are obtained. A number of methods for constructing new vector-output correlation-immune functions from old ones are discussed. The nonlinearity of the newly constructed vector-output correlation-immune functions is studied. For some cases we give the exact formulas for the nonlinearity of constructed vector-output correlation-immune functions.

Keywords: Cryptography; Stream ciphers; Correlation-immune functions; Resilient functions; Nonlinearity; Unbiased functions

☆This research work is supported in part by the DSTA project (POD 0103223), and the National Natural Science Foundation of China under the Grant 60172060, the Trans-Century Training Program Foundation for the Talents by the Education Ministry of China, and the Foundation for University Key Teacher by the Education Ministry of China.

*Corresponding author.

E-mail addresses: lschen@nankai.edu.cn (L. Chen), tslfufw@nus.edu.sg (F.-W. Fu), kwwei@ie.cuhk.edu.hk (V.K.-W. Wei).

[1] On leave from the Department of Mathematics, Nankai University, Tianjin 300071, P. R. China

0885-064X/$ - see front matter
doi:10.1016/j.jco.2003.08.015

1. Introduction

Correlation-immune functions play an important role in cryptography. The concept of correlation-immune functions was first introduced and studied by Siegenthaler [10]. Correlation-immune functions are used in stream ciphers as combining functions for running-key generators that are resistant to a correlation attack [7]. Functions with high nonlinearity have important applications in cryptography. The nonlinearity of functions is very important in evaluating the security of some cryptosystems. In stream ciphers, the combining functions or the filter functions employed in the running key generator must be selected with care. Functions with low nonlinearity can be easily broken by the best approximation attack [5]. In order to increase the security of the cipher system, the combining functions selected should be correlation-immune functions with high nonlinearity. By using vector-output Boolean functions as the combining functions, it is possible to increase the speed of the cipher systems since we may get more than one bit at each clock pulse. Vector-output Boolean functions with certain cryptographic properties are also used to design S-boxes in block cipher systems.

In this paper, we study the binary vector-output correlation-immune functions. Some important properties of vector-output correlation-immune functions are obtained. A number of methods for constructing new vector-output correlation-immune functions from old ones are discussed. The nonlinearity of the newly constructed vector-output correlation-immune functions is studied. For some cases we give the exact formulas for the nonlinearity of constructed vector-output correlation-immune functions.

This paper is organized as follows. In Section 2 we introduce some basic definitions and notations. We also review some basic properties which will be used in this paper. In Section 3 we derive an important property of vector-output correlation-immune functions. In Section 4 we discuss a number of methods for constructing new correlation-immune functions from old ones. In Section 5 we study the nonlinearity of the newly constructed vector-output correlation-immune functions. For some cases we give the exact formulas for the nonlinearity of constructed vector-output correlation-immune functions. In Section 6 we summarize and conclude this paper.

2. Preliminaries

Let $V_n = GF(2)^n$ be the n-dimensional vector space over $GF(2)$. For a vector $u \in V_n$, the *Hamming weight* $w_H(u)$ is the number of 1's in u. Let $f(x)$ be a function from V_n to $GF(2)$ (or simply, a function on V_n). The *sequence* of $f(x)$ is defined as

$$((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})}),$$

where α_i, $0 \leqslant i \leqslant 2^n - 1$, denotes the vector in V_n whose integer representation is i, that is

$$i = \sum_{j=1}^{n} \alpha^i_j 2^{j-1}.$$

A function $f(x)$ on V_n is said to be an *affine function* if it takes the form of

$$f(x) = c_0 \oplus c_1 x_1 \oplus \cdots \oplus c_n x_n,$$

where $x = (x_1, x_2, \ldots, x_n)$ and $c_i \in GF(2)$, $0 \leqslant i \leqslant n$. The *Hamming distance* between two functions $f(x)$ and $g(x)$ on V_n is defined by

$$d(f,g) = |\{x \in V_n | f(x) \neq g(x)\}|.$$

The *nonlinearity* of $f(x)$, denoted by N_f, is defined as

$$N_f = \min_{\varphi \in AF_n} d(f, \varphi),$$

where AF_n is the set of all affine functions on V_n.

Let $\alpha = (a_1, a_2, \ldots, a_n)$ and $\beta = (b_1, b_2, \ldots, b_n)$. If $\alpha, \beta \in V_n$, the *scalar product* of α and β is defined as $\langle \alpha, \beta \rangle = a_1 b_1 \oplus \cdots \oplus a_n b_n$, where the addition and multiplication are over $GF(2)$. If $\alpha, \beta \in \{-1, +1\}^n$, the *scalar product* of α and β is defined as $\langle \alpha, \beta \rangle = a_1 b_1 + \cdots + a_n b_n$, where the addition and multiplication are over the reals. Let $\alpha = (a_1, a_2, \ldots, a_m)$ and $\beta = (b_1, b_2, \ldots, b_n)$. The *Kronecker product* of α and β is defined as $\alpha \otimes \beta = (a_1 \beta, a_2 \beta, \ldots, a_m \beta)$. Note that $\alpha \otimes \beta$ is a vector with length mn.

Let $f(x)$ and $g(x)$ be two functions on V_n, it is known that (see [9, Lemma 6])

$$d(f,g) = 2^{n-1} - \frac{1}{2} \langle \xi_f, \xi_g \rangle,$$

where ξ_f and ξ_g are the sequences of $f(x)$ and $g(x)$, respectively.

A function F from V_n to V_m can be expressed as

$$F = (f_1, f_2, \ldots, f_m),$$

where each component function f_i, $1 \leqslant i \leqslant m$, is a function on V_n. The *nonlinearity* of a function F from V_n to V_m is defined as

$$N_F = \min_{g \in NLC_F} N_g,$$

where NLC_F is the set of all nonzero linear combinations of the component functions of F. This definition regarding N_F was first introduced by Nyberg in [6].

Definition 1. Let F be a function from V_n to V_m and let $\{X_1, X_2, \ldots, X_n\}$ be the set of random input variables with independent equiprobable distributions over $GF(2)$. If for every subset $T = \{j_1, j_2, \ldots, j_t\} \subseteq \{1, 2, \ldots, n\}$ of cardinality t, random vector $Z = F(X_1, X_2, \ldots, X_n)$ is independent of random vector $(X_{j_1}, X_{j_2}, \ldots, X_{j_t})$, that is to say, for every $(b_1, b_2, \ldots, b_t) \in V_t$ and for every $\alpha \in V_m$,

$$Pr(Z = \alpha | X_{j_i} = b_i,\ 1 \leqslant i \leqslant t) = Pr(Z = \alpha),$$

then F is said to be an (n, m, t)-correlation-immune function, or (n, m, t)-CI function for short.

It is easy to see from Definition 1 that

Lemma 1. *F is an (n, m, t)-CI function if and only if it is an (n, m, s)-CI function for each s with $0 \leqslant s \leqslant t$.*

Definition 2. Let F be a function from V_n to V_m, where $n \geqslant m \geqslant 1$. F is said to be an unbiased function, if for every $\alpha \in V_m$,

$$|\{x \in V_n | F(x) = \alpha\}| = 2^{n-m}.$$

Particularly, the unbiased functions on V_n are usually called balanced functions.

Definition 3. Let F be a function from V_n to V_m, where $n \geqslant m \geqslant 1$. F is said to be an (n, m, t)-resilient function if it is an unbiased (n, m, t)-CI function.

The concept of resilient functions was first introduced by Chor et al. [4] and Bennett et al. [1]. Resilient functions have found applications in the fault-tolerant distributed computing, quantum cryptographic key distribution and random sequence generation for stream ciphers.

The following fact regarding unbiased functions can be found in [13].

Lemma 2. *$F = (f_1, f_2, \ldots, f_m)$ is an unbiased function from V_n to V_m if and only if every nonzero linear combination*

$$f(x) = \bigoplus_{i=1}^{m} c_i f_i(x)$$

of the component functions of F is a balanced function on V_n, where $x \in V_n$, $c_1, c_2, \ldots, c_m \in GF(2)$ and not all zeroes.

By the definition of balanced functions, it is easy to obtain

Lemma 3. *Let $f_i(y_i)$ be a function on V_{n_i}, where $y_i \in V_{n_i}$, $1 \leqslant i \leqslant r$. If at least one of $f_1(y_1), f_2(y_2), \ldots, f_r(y_r)$ is a balanced function, then*

$$f(y_1, y_2, \ldots, y_r) = f_1(y_1) \oplus f_2(y_2) \oplus \cdots \oplus f_r(y_r)$$

is also a balanecd function.

For a function $f(x)$ on V_n, the *Walsh transform* of $f(x)$ is the real valued function over V_n defined as

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus \langle x, u \rangle}, \quad u \in V_n.$$

Note that $f(x)$ is a balanced function if and only if $W_f(\mathbf{0}) = 0$. Xiao and Massey [11] gave a characterization of an $(n, 1, t)$-correlation-immune function as follows.

Lemma 4. *A function $f(x)$ on V_n is an $(n, 1, t)$-correlation-immune function if and only if its Walsh transform satisfies*

$$W_f(u) = 0, \text{ for all } u \in V_n \text{ with } 1 \leqslant w_{\mathrm{H}}(u) \leqslant t.$$

3. An important property of vector-output correlation-immune functions

The following lemma is a special case of the *linear combination lemma* given by Camion and Canteaut (see [2, Lemma 2]).

Lemma 5. *Let $\eta = (\eta_1, \eta_2, \dots, \eta_t)$ be a random vector in V_t and let $\xi = (\xi_1, \xi_2, \dots, \xi_m)$ be a random vector in V_m. Then η is independent of $\xi = (\xi_1, \xi_2, \dots, \xi_m)$ if and only if η is independent of every nonzero linear combination $\bigoplus_{i=1}^{m} c_i \xi_i$ of $\xi_1, \xi_2, \dots, \xi_m$, where $c_1, c_2, \dots, c_m \in GF(2)$ and not all zeroes.*

From Lemma 5, we have the following important property regarding vector-output correlation-immune functions.

Theorem 1. *$F = (f_1, f_2, \dots, f_m)$ is an (n, m, t)-CI function if and only if every nonzero linear combination*

$$f(x) = \bigoplus_{i=1}^{m} c_i f_i(x)$$

of the component functions of F is an $(n, 1, t)$-CI function, where $x \in V_n$, and $c_1, c_2, \dots, c_m \in GF(2)$ and not all zeroes.

Proof. Let $X_1, X_2, \dots, X_n$ be n random variables with independent equiprobable distributions over $GF(2)$, and let $Z_i = f_i(X_1, X_2, \dots, X_n)$, $i = 1, 2, \dots, m$. By Definition 1 and Lemma 5, $F = (f_1, f_2, \dots, f_m)$ is an (n, m, t)-CI function $\Leftrightarrow$ for every subset $\{j_1, j_2, \dots, j_t\} \subseteq \{1, 2, \dots, n\}$ of cardinality t, random vector

$$Z = F(X_1, X_2, \dots, X_n) = (Z_1, Z_2, \dots, Z_m)$$

is independent of $(X_{j_1}, X_{j_2}, \dots, X_{j_t}) \Leftrightarrow$ for every subset $\{j_1, j_2, \dots, j_t\} \subseteq \{1, 2, \dots, n\}$ of cardinality t, every nonzero linear combination

$$\bigoplus_{i=1}^{m} c_i Z_i = \bigoplus_{i=1}^{m} c_i f_i(X_1, X_2, \dots, X_n)$$

of $Z_1, Z_2, \dots, Z_m$ is independent of $(X_{j_1}, X_{j_2}, \dots, X_{j_t}) \Leftrightarrow$ every nonzero linear combination

$$f(x) = \bigoplus_{i=1}^{m} c_i f_i(x)$$

of the component functions of F is an $(n, 1, t)$-CI function, where $x \in V_n$. $\square$

It follows from Theorem 1 that if $F = (f_1, f_2, \dots, f_m)$ is an (n, m, t)-CI function, then $G = (f_{i_1}, f_{i_2}, \dots, f_{i_s})$ is an (n, s, t)-CI function for each subset $\{i_1, i_2, \dots, i_s\} \subseteq \{1, 2, \dots, m\}$ of cardinality s, $1 \leqslant s \leqslant m$.

4. Matrix-product construction of vector-output correlation-immune functions

In this section, we study the matrix-product construction of vector-output correlation-immune functions. We first introduce the following result which can be found in [12, Theorem 17.3.6]. For completeness, we present a new proof here by using the technique of Walsh transform.

Lemma 6. *Let $f_1(y_1)$ be an $(n_1, 1, t_1)$-CI function and $f_2(y_2)$ be an $(n_2, 1, t_2)$-CI function, where $t_1 \leqslant t_2$, $y_1 \in V_{n_1}$, $y_2 \in V_{n_2}$. Let*

$$f(y_1, y_2) = f_1(y_1) \oplus f_2(y_2).$$

(a) *If both f_1 and f_2 are not balanced, then f is an $(n_1 + n_2, 1, t_1)$-CI function.*
(b) *If f_1 is not balanced but f_2 is balanced, then f is an $(n_1 + n_2, 1, t_2)$-CI function.*
(c) *If f_1 is balanced but f_2 is not balanced, then f is an $(n_1 + n_2, 1, t_1)$-CI function.*
(d) *If both f_1 and f_2 are balanced, then f is an $(n_1 + n_2, 1, t_1 + t_2 + 1)$-CI function.*

Proof. The Walsh transform of $f(y_1, y_2) = f_1(y_1) \oplus f_2(y_2)$ is given by

$$\begin{aligned} W_f(u_1, u_2) &= \sum_{y_1 \in V_{n_1},\ y_2 \in V_{n_2}} (-1)^{f_1(y_1) \oplus f_2(y_2) \oplus \langle (y_1, y_2), (u_1, u_2) \rangle} \\ &= \sum_{y_1 \in V_{n_1},\ y_2 \in V_{n_2}} (-1)^{f_1(y_1) \oplus f_2(y_2) \oplus \langle y_1, u_1 \rangle \oplus \langle y_2, u_2 \rangle} \\ &= \sum_{y_1 \in V_{n_1}} (-1)^{f_1(y_1) \oplus \langle y_1, u_1 \rangle} \sum_{y_2 \in V_{n_2}} (-1)^{f_2(y_2) \oplus \langle y_2, u_2 \rangle} \\ &= W_{f_1}(u_1) W_{f_2}(u_2). \end{aligned}$$

If $1 \leqslant w_H((u_1, u_2)) \leqslant t_1$, then either $1 \leqslant w_H(u_1) \leqslant t_1$ or $1 \leqslant w_H(u_2) \leqslant t_1$. By Lemma 4, for the case $1 \leqslant w_H(u_1) \leqslant t_1$, we have $W_{f_1}(u_1) = 0$ since $f_1(y_1)$ is an $(n_1, 1, t_1)$-CI function; for the case $1 \leqslant w_H(u_2) \leqslant t_1$, we have $W_{f_2}(u_2) = 0$ since $f_2(y_2)$ is an $(n_2, 1, t_2)$-CI function and $t_1 \leqslant t_2$. Hence, $W_f(u_1, u_2) = 0$ for all $(u_1, u_2) \in V_{n_1+n_2}$ with $1 \leqslant w_H((u_1, u_2)) \leqslant t_1$. The assertions (a) and (c) follow from Lemma 4.

If f_2 is a balanced $(n_2, 1, t_2)$-CI function, then by Lemma 4 and the definitions of balanced functions and Walsh transform, we have $W_{f_2}(u_2) = 0$ for all $u_2 \in V_{n_2}$ with $0 \leqslant w_H(u_2) \leqslant t_2$. Since $1 \leqslant w_H((u_1, u_2)) \leqslant t_2$ implies $0 \leqslant w_H(u_2) \leqslant t_2$, we have $W_f(u_1, u_2) = 0$ for all $(u_1, u_2) \in V_{n_1+n_2}$ with $1 \leqslant w_H((u_1, u_2)) \leqslant t_2$. Assertion (b) follows from Lemma 4.

If both f_1 and f_2 are balanced, then by Lemma 4 and the definitions of balanced functions and Walsh transform, we have $W_{f_1}(u_1) = 0$ for all $u_1 \in V_{n_1}$ with $0 \leqslant w_H(u_1) \leqslant t_1$, and $W_{f_2}(u_2) = 0$ for all $u_2 \in V_{n_2}$ with $0 \leqslant w_H(u_2) \leqslant t_2$. For $(u_1, u_2) \in V_{n_1+n_2}$ with $1 \leqslant w_H((u_1, u_2)) \leqslant t_1 + t_2 + 1$, if $0 \leqslant w_H(u_1) \leqslant t_1$, then $W_{f_1}(u_1) = 0$; if $w_H(u_1) \geqslant t_1 + 1$, then $0 \leqslant w_H(u_2) \leqslant t_2$, which implies $W_{f_2}(u_2) = 0$. Hence, $W_f(u_1, u_2) = 0$ for all $(u_1, u_2) \in V_{n_1+n_2}$ with $1 \leqslant w_H((u_1, u_2)) \leqslant t_1 + t_2 + 1$. Assertion (d) follows from Lemma 4. □

The following theorem is a generalization of Lemma 6.

Theorem 2. *Let $f_i(y_i)$ be an $(n_i, 1, t_i)$-CI function, where $y_i \in V_{n_i}$, $1 \leqslant i \leqslant r$. Then*

$$f(y_1, y_2, \ldots, y_r) = f_1(y_1) \oplus f_2(y_2) \oplus \cdots \oplus f_r(y_r)$$

is an $(\sum_{i=1}^{r} n_i, 1, t)$-CI function, where

$$t = \begin{cases} \min\{t_1, t_2, \ldots, t_r\} & \text{if } b_1 = b_2 = \cdots = b_r = 0, \\ \sum_{i=1}^{r} b_i t_i + w_{\mathrm{H}}(b_1, b_2, \ldots, b_r) - 1 & \text{if } (b_1, b_2, \ldots, b_r) \neq (0, 0, \ldots, 0), \end{cases} \quad (1)$$

$$b_i = \begin{cases} 1 & \text{if } f_i(y_i) \text{ is balanced}, \\ 0 & \text{if } f_i(y_i) \text{ is not balanced}, \end{cases} \quad i = 1, 2, \ldots, r,$$

and $w_{\mathrm{H}}(b_1, b_2, \ldots, b_r)$ represents the Hamming weight of the binary vector $(b_1, b_2, \ldots, b_r)$.

Proof. We show by mathematical induction that f is an $(\sum_{i=1}^{r} n_i, 1, t)$-CI function, where t is defined by (1). By Lemma 6, it is obvious that (1) is true for the case $r = 2$.

Suppose (1) holds for $r < k$. Consider $r = k$. Let

$$g(y_1, y_2, \ldots, y_{k-1}) = f_1(y_1) \oplus f_2(y_2) \oplus \cdots \oplus f_{k-1}(y_{k-1}).$$

Then

$$f(y_1, y_2, \ldots, y_k) = g(y_1, y_2, \ldots, y_{k-1}) \oplus f_k(y_k).$$

By Lemma 3, if $(b_1, b_2, \ldots, b_{k-1})$ is not a zero vector, then $g(y_1, y_2, \ldots, y_{k-1})$ is balanced. By the induction hypothesis, $g(y_1, y_2, \ldots, y_{k-1})$ is an $(\sum_{i=1}^{k-1} n_i, 1, s)$-CI function, where

$$s = \begin{cases} \min\{t_1, t_2, \ldots, t_{k-1}\} & \text{if } b_1 = b_2 = \cdots = b_{k-1} = 0, \\ \sum_{i=0}^{k-1} b_i t_i + w_{\mathrm{H}}(b_1, b_2, \ldots, b_{k-1}) - 1 & \text{if } (b_1, b_2, \ldots, b_{k-1}) \neq (0, 0, \ldots, 0). \end{cases}$$

Let

$$b = \begin{cases} 0 & \text{if } b_1 = b_2 = \cdots = b_{k-1} = 0, \\ 1 & \text{otherwise}. \end{cases}$$

Then, by Lemma 6, $f(y_1, y_2, \ldots, y_k)$ is an $(\sum_{i=1}^{k} n_i, 1, t)$-CI function, where

$$t = \begin{cases} \min\{s, t_k\} & \text{if } b = b_k = 0, \\ bs + b_k t_k + w_{\mathrm{H}}(b, b_k) - 1 & \text{otherwise}. \end{cases}$$

If $b = b_k = 0$, it is obvious that

$$t = \min\{t_1, t_2, \ldots, t_k\}.$$

If $b = 0$ and $b_k = 1$, then

$$t = t_k = \sum_{i=1}^{k} b_i t_i + w_{\mathrm{H}}(b_1, b_2, \ldots, b_k) - 1.$$

If $b = 1$ and $b_k = 0$, then

$$\begin{aligned} t &= s \\ &= \sum_{i=0}^{k-1} b_i t_i + w_{\mathrm{H}}(b_1, b_2, \ldots, b_{k-1}) - 1 \\ &= \sum_{i=0}^{k} b_i t_i + w_{\mathrm{H}}(b_1, b_2, \ldots, b_k) - 1. \end{aligned}$$

If $b = 1$ and $b_k = 1$, then

$$\begin{aligned} t &= s + t_k + 1 \\ &= \sum_{i=0}^{k-1} b_i t_i + w_{\mathrm{H}}(b_1, b_2, \ldots, b_{k-1}) - 1 + t_k + 1 \\ &= \sum_{i=0}^{k} b_i t_i + w_{\mathrm{H}}(b_1, b_2, \ldots, b_k) - 1. \end{aligned}$$

By the above discussion, we know that (1) is true. This completes the proof. □

For convenience, let

$$\begin{aligned} &\psi((b_1, b_2, \ldots, b_r), (t_1, t_2, \ldots, t_r)) \\ &\quad = \begin{cases} \min\{t_1, t_2, \ldots, t_r\} & \text{if } b_1 = b_2 = \cdots = b_r = 0, \\ \sum_{i=1}^{r} b_i t_i + w_{\mathrm{H}}(b_1, b_2, \ldots, b_r) - 1 & \text{if } (b_1, b_2, \ldots, b_r) \neq (0, 0, \ldots, 0), \end{cases} \end{aligned}$$

where $r \geqslant 1$, $b_i = 0$ or 1, t_i is a nonnegative integer, $i = 1, 2, \ldots, r$.

Below we study the matrix-product construction of vector-output correlation-immune functions.

Theorem 3. *Let $F_j = (f_{j1}, f_{j2}, \ldots, f_{jm})$ be an (n_j, m, t_j)-CI function, $j = 1, 2, \ldots, r$. Let w be the number of unbiased functions in $F_1, F_2, \ldots, F_r$. Let $A = (a_{ij})_{r \times s}$ be an $r \times s$ matrix over $GF(2)$ such that $r \geqslant s$ and $\mathrm{Rank}(A) = s$. Let d be the minimum weight of the linear code generated by A^T, where A^T denotes the transpose of matrix A. Let*

$$F(y_1, y_2, \ldots, y_r) = (F_1(y_1), F_2(y_2), \ldots, F_r(y_r))A,$$

where $y_j \in V_{n_j}$, $j = 1, 2, \ldots, r$. If $w \leqslant r - d$, then F is an $(\sum_{j=1}^{r} n_j, sm, t)$-CI function, where

$$t = \min\{t_1, t_2, \ldots, t_r\}.$$

If $w > r - d$, then F is an $(\sum_{j=1}^{r} n_j, sm, t)$-resilient function, where

$$t = t_{i_1} + t_{i_2} + \cdots + t_{i_{w-r+d}} + w - r + d - 1,$$

and $\{i_1, i_2, \ldots, i_w\} \subseteq \{1, 2, \ldots, r\}$ such that $F_{i_1}, F_{i_2}, \ldots, F_{i_w}$ are unbiased and $t_{i_1} \leqslant t_{i_2} \leqslant \cdots \leqslant t_{i_w}$.

Proof. For each k with $1 \leqslant k \leqslant s$,

$$\begin{aligned}
&(F_1(y_1), F_2(y_2), \dots, F_r(y_r)) \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{rk} \end{pmatrix} \\
&\quad = a_{1k}F_1(y_1) \oplus a_{2k}F_2(y_2) \oplus \cdots \oplus a_{rk}F_r(y_r) \\
&\quad = \left(\bigoplus_{j=1}^{r} a_{jk} f_{j1}(y_j), \bigoplus_{j=1}^{r} a_{jk} f_{j2}(y_j), \dots, \bigoplus_{j=1}^{r} a_{jk} f_{jm}(y_j) \right).
\end{aligned}$$

Consider an arbitrary nonzero linear combination of the component functions of F,

$$\begin{aligned}
f(y_1, y_2, \dots, y_r) &= \bigoplus_{k=1}^{s} \bigoplus_{i=1}^{m} c_{ki} \bigoplus_{j=1}^{r} a_{jk} f_{ji}(y_j) \\
&= \bigoplus_{j=1}^{r} \bigoplus_{k=1}^{s} a_{jk} \bigoplus_{i=1}^{m} c_{ki} f_{ji}(y_j).
\end{aligned}$$

Let

$$C = \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1m} \\ c_{21} & c_{22} & \dots & c_{2m} \\ \dots & \dots & \dots & \dots \\ c_{s1} & c_{s2} & \dots & c_{sm} \end{pmatrix}_{s \times m}, \quad \beta_i = \begin{pmatrix} c_{1i} \\ c_{2i} \\ \vdots \\ c_{si} \end{pmatrix}, \quad i = 1, 2, \dots, m,$$

$$\alpha_j = (a_{j1}, a_{j2}, \dots, a_{js}), \quad j = 1, 2, \dots, r.$$

Then

$$f(y_1, y_2, \dots, y_r) = \bigoplus_{i=1}^{m} \alpha_1 \beta_i f_{1i}(y_1) \oplus \bigoplus_{i=1}^{m} \alpha_2 \beta_i f_{2i}(y_2) \oplus \cdots \oplus \bigoplus_{i=1}^{m} \alpha_r \beta_i f_{ri}(y_r).$$

Let $A_{r \times s} C_{s \times m} = B_{r \times m}$. Then each column vector of B is a linear combination of the column vectors of A. Thus when the jth column vector of C is not a zero vector, the number of ones in the jth column of B is at least d where d is the minimum weight of the linear code generated by A^T. Therefore, there are at least d rows of B which are not zero vectors. In fact, as C is an arbitrary nonzero $(0,1)$-matrix, there is at least one column of B in which there are at least d ones. Suppose for contradiction that there are only μ rows in B which are not zero vectors and $\mu < d$. Then the number of ones in each column of B is less than or equal to $\mu(< d)$, which leads to contradiction.

Since

$$AC = B = \begin{pmatrix} \alpha_1\beta_1 & \alpha_1\beta_2 & \dots & \alpha_1\beta_m \\ \alpha_2\beta_1 & \alpha_2\beta_2 & \dots & \alpha_2\beta_m \\ \dots & \dots & \dots & \dots \\ \alpha_r\beta_1 & \alpha_r\beta_2 & \dots & \alpha_r\beta_m \end{pmatrix},$$

there are at least d vectors in $(\alpha_j\beta_1, \alpha_j\beta_2, \dots, \alpha_j\beta_m), j = 1, 2, \dots, r$, which are not zero vectors. Therefore, there are at least d functions in

$$\bigoplus_{i=1}^{m} \alpha_1\beta_i f_{1i}(y_1), \quad \bigoplus_{i=1}^{m} \alpha_2\beta_i f_{2i}(y_2), \quad \dots, \quad \bigoplus_{i=1}^{m} \alpha_r\beta_i f_{ri}(y_r)$$

which are not zero.

Since $F_j(y_j) = (f_{j1}(y_j), f_{j2}(y_j), \dots, f_{jm}(y_j))$ is an (n_j, m, t_j)-CI function, by Theorem 1, when $(\alpha_j\beta_1, \alpha_j\beta_2, \dots, \alpha_j\beta_m)$ is not a zero vector, $\bigoplus_{i=1}^{m} \alpha_j\beta_i f_{ji}(y_j)$ is an $(n_j, 1, t_j)$-CI function, $j = 1, 2, \dots, r$.

By Theorem 2 and Lemma 1, $f(y_1, y_2, \dots, y_r)$ is an $(\sum_{j=1}^{r} n_j, 1, t)$-CI function, where

$$t = \min_{1 \leqslant j_1 < j_2 < \dots < j_d \leqslant r} \psi((b_{j_1}, b_{j_2}, \dots, b_{j_d}), (t_{j_1}, t_{j_2}, \dots, t_{j_d})), \tag{2}$$

$$b_j = \begin{cases} 1 & \text{if } F_j \text{ is unbiased,} \\ 0 & \text{if } F_j \text{ is not unbiased,} \end{cases} \quad j = 1, 2, \dots, r.$$

Again by Theorem 1, $F(y_1, y_2, \dots, y_r)$ is an $(\sum_{j=1}^{r} n_j, sm, t)$-CI function.

If $w > r - d$, that is, at least $r - d + 1$ of $F_1, F_2, \dots, F_r$ are unbiased, then by Lemma 2 and the above discussion, there is at least one of

$$\bigoplus_{i=1}^{m} \alpha_1\beta_i f_{1i}(y_1), \quad \bigoplus_{i=1}^{m} \alpha_2\beta_i f_{2i}(y_2), \quad \dots, \quad \bigoplus_{i=1}^{m} \alpha_r\beta_i f_{ri}(y_r)$$

which is balanced. Therefore, by Lemma 3, $f(y_1, y_2, \dots, y_r)$ is balanced. Again by Lemma 2, $F(y_1, y_2, \dots, y_r)$ is an unbiased function from V_n to V_{sm}, where $n = \sum_{j=1}^{r} n_j$. So it follows from Definition 3 that $F(y_1, y_2, \dots, y_r)$ is an $(\sum_{j=1}^{r} n_j, sm, t)$-resilient function.

Now we calculate the t given in (2).

If $w \leqslant r - d$, then there are at least d of $F_1, F_2, \dots, F_r$ which are not unbiased. Let $F_{i_1}, F_{i_2}, \dots, F_{i_w}$ be unbiased and $F_{i_{w+1}}, F_{i_{w+2}}, \dots, F_{i_r}$ be not unbiased, where

$\{i_1, i_2, \ldots, i_r\}$ is a permutation of $\{1, 2, \ldots, r\}$. Then

$$\min_{\substack{1 \leqslant j_1 < j_2 < \cdots < j_d \leqslant r \\ b_{j_1} = b_{j_2} = \cdots = b_{j_d} = 0}} \psi((b_{j_1}, b_{j_2}, \ldots, b_{j_d}), (t_{j_1}, t_{j_2}, \ldots, t_{j_d}))$$
$$= \min_{\substack{1 \leqslant j_1 < j_2 < \cdots < j_d \leqslant r \\ b_{j_1} = b_{j_2} = \cdots = b_{j_d} = 0}} \min\{t_{j_1}, t_{j_2}, \ldots, t_{j_d}\}$$
$$= \min\{t_{i_{w+1}}, t_{i_{w+2}}, \ldots, t_{i_r}\},$$

$$\min_{\substack{1 \leqslant j_1 < j_2 < \cdots < j_d \leqslant r \\ b_{j_1}, b_{j_2}, \ldots, b_{j_d} \text{ are not all zeroes}}} \psi((b_{j_1}, b_{j_2}, \ldots, b_{j_d}), (t_{j_1}, t_{j_2}, \ldots, t_{j_d}))$$
$$= \min_{\substack{1 \leqslant j_1 < j_2 < \cdots < j_d \leqslant r \\ b_{j_1}, b_{j_2}, \ldots, b_{j_d} \text{ are not all zeroes}}} b_{j_1} t_{j_1} + b_{j_2} t_{j_2} + \cdots + b_{j_d} t_{j_d} + w_{\mathrm{H}}(b_{j_1}, b_{j_2}, \ldots, b_{j_d}) - 1$$
$$= \min\{t_{i_1}, t_{i_2}, \ldots, t_{i_w}\},$$

$$t = \min_{1 \leqslant j_1 < j_2 < \cdots < j_d \leqslant r} \psi((b_{j_1}, b_{j_2}, \ldots, b_{j_d}), (t_{j_1}, t_{j_2}, \ldots, t_{j_d}))$$
$$= \min\{\min\{t_{i_1}, t_{i_2}, \ldots, t_{i_w}\}, \min\{t_{i_{w+1}}, t_{i_{w+2}}, \ldots, t_{i_r}\}\}$$
$$= \min\{t_1, t_2, \ldots, t_r\}.$$

If $w > r - d$, then it is easy to show that

$$t = \min_{1 \leqslant j_1 < j_2 < \cdots < j_d \leqslant r} \psi((b_{j_1}, b_{j_2}, \ldots, b_{j_d}), (t_{j_1}, t_{j_2}, \ldots, t_{j_d}))$$
$$= \min_{1 \leqslant j_1 < j_2 < \cdots < j_d \leqslant r} b_{j_1} t_{j_1} + b_{j_2} t_{j_2} + \cdots + b_{j_d} t_{j_d} + w_{\mathrm{H}}(b_{j_1}, b_{j_2}, \ldots, b_{j_d}) - 1$$
$$= t_{i_1} + t_{i_2} + \cdots + t_{i_{w-r+d}} + w - r + d - 1,$$

where $\{i_1, i_2, \ldots, i_w\} \subseteq \{1, 2, \ldots, r\}$ such that $F_{i_1}, F_{i_2}, \ldots, F_{i_w}$ are unbiased and $t_{i_1} \leqslant t_{i_2} \leqslant \cdots \leqslant t_{i_w}$. □

5. Nonlinearity of matrix-product vector-output Boolean functions

Chen and Fu [3] presented a lower bound for the nonlinearity of matrix-product vector-output Boolean functions.

Lemma 7. *Let $F_j = (f_{j1}, f_{j2}, \ldots, f_{jm})$ be a function from V_{n_j} to V_m, $j = 1, 2, \ldots, r$. Let $A = (a_{ij})_{r \times s}$ be an $r \times s$ matrix over $GF(2)$ such that $r \geqslant s$ and* $\mathrm{Rank}(A) = s$. *Let d be the minimum weight of the linear code generated by A^T, where A^T denotes the transpose of matrix A. Let*

$$F(y_1, y_2, \ldots, y_r) = (F_1(y_1), F_2(y_2), \ldots, F_r(y_r))A,$$

where $y_j \in V_{n_j}$, $j = 1, 2, \ldots, r$. *Assume*

$$N_{F_{j_1}} \leqslant N_{F_{j_2}} \leqslant \cdots \leqslant N_{F_{j_r}},$$

where $\{j_1, j_2, \ldots, j_r\}$ *is a permutation of* $\{1, 2, \ldots, r\}$. *Then*

$$N_F \geqslant 2^{n-1} - 2^{(\sum_{k=d+1}^{r} n_{j_k})-1} \prod_{k=1}^{d} (2^{n_{j_k}} - 2N_{F_{j_k}}), \tag{3}$$

where $n = \sum_{j=1}^{r} n_j$.

In this section, we further study the nonlinearity of matrix-product vector-output Boolean functions. For some cases we give the exact formulas for the nonlinearity of matrix-product vector-output Boolean functions.

The following lemma slightly generalizes a result of Sarkar and Maitra [8]. For completeness, we present a new proof here by using the technique of sequences of Boolean functions.

Lemma 8. *Let* $f_i(y_i)$ *be a function on* V_{n_i}, *where* $y_i \in V_{n_i}$, $1 \leqslant i \leqslant r$. *Let*

$$f(y_1, y_2, \ldots, y_r) = f_1(y_1) \oplus f_2(y_2) \oplus \cdots \oplus f_r(y_r).$$

Then the nonlinearity of f *is given by*

$$N_f = 2^{n-1} - \frac{1}{2} \prod_{i=1}^{r} (2^{n_i} - 2N_{f_i}), \tag{4}$$

where $n = \sum_{i=1}^{r} n_i$.

Proof. Let ξ_f be the sequence of f and ξ_{f_i} be the sequence of f_i, $i = 1, 2, \ldots, r$. Then

$$\xi_f = \xi_{f_1} \otimes \xi_{f_2} \otimes \cdots \otimes \xi_{f_r}.$$

Let $\theta_i(y_i)$ be an arbitrary affine function on V_{n_i} and its sequence be ξ_{θ_i}, $i = 1, 2, \ldots, r$. Let

$$\theta(y_1, y_2, \ldots, y_r) = \theta_1(y_1) \oplus \theta_2(y_2) \oplus \cdots \oplus \theta_r(y_r).$$

Then θ is an arbitrary affine function on V_n. Let ξ_θ be the sequence of θ. Then

$$\xi_\theta = \xi_{\theta_1} \otimes \xi_{\theta_2} \otimes \cdots \otimes \xi_{\theta_r}.$$

Since

$$\begin{aligned} \langle \xi_f, \xi_\theta \rangle &= \langle \xi_{f_1} \otimes \xi_{f_2} \otimes \cdots \otimes \xi_{f_r}, \xi_{\theta_1} \otimes \xi_{\theta_2} \otimes \cdots \otimes \xi_{\theta_r} \rangle \\ &= \langle \xi_{f_1}, \xi_{\theta_1} \rangle \langle \xi_{f_2}, \xi_{\theta_2} \rangle \cdots \langle \xi_{f_r}, \xi_{\theta_r} \rangle \\ &= \prod_{i=1}^{r} (2^{n_i} - 2d(f_i, \theta_i)), \end{aligned}$$

we have

$$\begin{aligned} N_f &= \min_{\theta \in AF_n} d(f,\theta) \\ &= \min_{\theta \in AF_n} (2^{n-1} - \frac{1}{2}\langle \xi_f, \xi_\theta \rangle) \\ &= 2^{n-1} - \frac{1}{2} \max_{\theta \in AF_n} \langle \xi_f, \xi_\theta \rangle \\ &= 2^{n-1} - \frac{1}{2} \prod_{i=1}^{r} \max_{\theta_i \in AF_{n_i}} (2^{n_i} - 2d(f_i,\theta_i)) \\ &= 2^{n-1} - \frac{1}{2} \prod_{i=1}^{r} (2^{n_i} - 2N_{f_i}). \qquad \square \end{aligned}$$

Let $r = 2$ and $f_2(y_2) = 0$ in Lemma 8, one can obtain

Lemma 9. *Let h be a function on V_{n_1}. Set $f(y_1, y_2) = h(y_1)$, where $y_1 \in V_{n_1}$, $y_2 \in V_{n_2}$. Then f is a function on $V_{n_1+n_2}$ whose nonlinearity is given by $N_f = 2^{n_2} N_h$.*

By Lemmas 8 and 9, it immediately follows

Lemma 10. *Let f_i be a function on V_{n_i}, $i = 1, 2, \ldots, r$. Let $\alpha = (a_1, a_2, \ldots, a_r) \in V_r$. Let*

$$f(y_1, y_2, \ldots, y_r) = a_1 f_1(y_1) \oplus a_2 f_2(y_2) \oplus \cdots \oplus a_r f_r(y_r),$$

where $y_i \in V_{n_i}$, $i = 1, 2, \ldots, r$. Then

$$N_f = 2^{n_1+n_2+\cdots+n_r-1} - \frac{1}{2} \prod_{i=1}^{r} (2^{n_i} - 2a_i N_{f_i}).$$

Theorem 4. *Let f_j be a function on V_{n_j}, $j = 1, 2, \ldots, r$. Let $A = (a_{ij})_{r\times s}$ be an $r \times s$ matrix over $GF(2)$ such that $r \geqslant s$ and $\mathrm{Rank}(A) = s$. Let L be the linear code generated by A^T and its minimum weight be d. Let*

$$F(y_1, y_2, \ldots, y_r) = (f_1(y_1), f_2(y_2), \ldots, f_r(y_r))A,$$

where $y_j \in V_{n_j}$, $j = 1, 2, \ldots, r$. Then

$$N_F = 2^{n_1+n_2+\cdots+n_r-1} - \frac{1}{2} \max_{\alpha \in L^*} \left(\prod_{j=1}^{r} (2^{n_j} - 2a_j N_{f_j}) \right), \tag{5}$$

where L^* is the set of nonzero codewords of L and $\alpha = (a_1, a_2, \ldots, a_r) \in L^*$. Particularly, if $n_1 = n_2 = \cdots = n_r = n$ and $N_{f_1} = N_{f_2} = \cdots = N_{f_r} = N$, then

$$N_F = 2^{rn-1} - 2^{(r-d)n-1}(2^n - 2N)^d.$$

Proof. For any nonzero vector $c \in V_s$,

$$\begin{aligned} f(y_1, y_2, \ldots, y_r) &= F(y_1, y_2, \ldots, y_r)c^T \\ &= (f_1(y_1), f_2(y_2), \ldots, f_r(y_r))Ac^T \end{aligned}$$

is a nonzero linear combination of the component functions of F. Note that $cA^T \in L^*$. Therefore, an arbitrary nonzero linear combination $f(y_1, y_2, \ldots, y_r)$ of the component functions of F can be expressed as

$$\begin{aligned} f(y_1, y_2, \ldots, y_r) &= (f_1(y_1), f_2(y_2), \ldots, f_r(y_r))\alpha^T \\ &= a_1 f_1(y_1) \oplus a_2 f_2(y_2) \oplus \cdots \oplus a_r f_r(y_r), \end{aligned}$$

where $\alpha = (a_1, a_2, \ldots, a_r) \in L^*$. By the definition of nonlinearity, we have

$$N_F = \min_{\alpha \in L^*} N_f .$$

Therefore, Eq. (5) follows immediately from Lemma 10.

If $n_1 = n_2 = \cdots = n_r = n$ and $N_{f_1} = N_{f_2} = \cdots = N_{f_r} = N$, then by (5), we have

$$\begin{aligned} N_F &= 2^{rn-1} - \frac{1}{2} \max_{\alpha \in L^*} \left(\prod_{j=1}^{r} (2^n - 2a_j N) \right) \\ &= 2^{rn-1} - \frac{1}{2} \max_{\substack{\alpha \in L^* \\ w_H(\alpha) = d}} \left(\prod_{j=1}^{r} (2^n - 2a_j N) \right) \\ &= 2^{rn-1} - 2^{(r-d)n-1}(2^n - 2N)^d. \qquad \square \end{aligned}$$

Example 1. Let $A = (a_{ij})_{r \times (r-1)}$ be an $r \times (r-1)$ matrix over $GF(2)$, where

$$a_{ij} = \begin{cases} 1 & \text{if } i = j \text{ or } i = r, \\ 0 & \text{otherwise,} \end{cases} \qquad 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant r-1.$$

It is obvious that the minimum weight of the linear code generated by A^T is 2. It is also easy to observe that every vector of V_r with even weight is a codeword of the linear code generated by A^T. Let f_j be a function on V_n, $j = 1, 2, \ldots, r$. Let

$$\begin{aligned} F(y_1, y_2, \ldots, y_r) &= (f_1(y_1), f_2(y_2), \ldots, f_r(y_r))A \\ &= (f_1(y_1) \oplus f_r(y_r), f_2(y_2) \oplus f_r(y_r), \ldots, f_{r-1}(y_{r-1}) \oplus f_r(y_r)), \end{aligned}$$

where $y_j \in V_n$, $j = 1, 2, \ldots, r$. Then, by Theorem 4, we have

$$N_F = 2^{rn-1} - 2^{(r-2)n-1}(2^n - 2N_{f_{j_1}})(2^n - 2N_{f_{j_2}}),$$

where $\{j_1, j_2, \ldots, j_r\}$ is a permutation of $\{1, 2, \ldots, r\}$ such that $N_{f_{j_1}} \leqslant N_{f_{j_2}} \leqslant \cdots \leqslant N_{f_{j_r}}$.

The following lemma is a generalization of Lemma 9 from single-output Boolean functions to vector-output Boolean functions.

Lemma 11. *Let H be a function from V_{n_1} to V_m. Set $F(y_1, y_2) = H(y_1)$, where $y_1 \in V_{n_1}$, $y_2 \in V_{n_2}$. Then F is a function from $V_{n_1+n_2}$ to V_m whose nonlinearity is given by $N_F = 2^{n_2} N_H$.*

Proof. Let $F = (f_1, f_2, \ldots, f_m)$, $H = (h_1, h_2, \ldots, h_m)$. For any $c_1, c_2, \ldots, c_m \in GF(2)$ and not all zeroes, let

$$f(y_1, y_2) = c_1 f_1(y_1, y_2) \oplus c_2 f_2(y_1, y_2) \oplus \cdots \oplus c_m f_m(y_1, y_2),$$

$$h(y_1) = c_1 h_1(y_1) \oplus c_2 h_2(y_1) \oplus \cdots \oplus c_m h_m(y_1).$$

Since $F(y_1, y_2) = H(y_1)$, we have $f(y_1, y_2) = h(y_1)$. Therefore, by Lemma 9, $N_f = 2^{n_2} N_h$. By the definition of nonlinearity, it follows that

$$N_F = \min_{\substack{c_1, \ldots, c_m \in GF(2) \\ \text{and not all zeroes}}} N_f = 2^{n_2} \min_{\substack{c_1, \ldots, c_m \in GF(2) \\ \text{and not all zeroes}}} N_h = 2^{n_2} N_H. \qquad \square$$

For the special case of all functions are equal, the following lemma is a generalization of Lemma 8 from single-output Boolean functions to vector-output Boolean functions.

Lemma 12. *Let $F = (f_1, f_2, \ldots, f_m)$ be a function from V_n to V_m. Let*

$$G(y_1, y_2, \ldots, y_r) = F(y_1) \oplus F(y_2) \oplus \cdots \oplus F(y_r),$$

where $y_j \in V_n$, $j = 1, 2, \ldots, r$. Then

$$N_G = 2^{rn-1} - \frac{1}{2}(2^n - 2N_F)^r.$$

Proof. For any $c_1, c_2, \ldots, c_m \in GF(2)$ and not all zeroes, let

$$f(x) = c_1 f_1(x) \oplus c_2 f_2(x) \oplus \cdots \oplus c_m f_m(x),$$

where $x \in V_n$. Then

$$\begin{aligned} g(y_1, y_2, \ldots, y_r) &= c_1 \bigoplus_{j=1}^{r} f_1(y_j) \oplus c_2 \bigoplus_{j=1}^{r} f_2(y_j) \oplus \cdots \oplus c_m \bigoplus_{j=1}^{r} f_m(y_j) \\ &= \bigoplus_{i=1}^{m} c_i f_i(y_1) \oplus \bigoplus_{i=1}^{m} c_i f_i(y_2) \oplus \cdots \oplus \bigoplus_{i=1}^{m} c_i f_i(y_r) \\ &= f(y_1) \oplus f(y_2) \oplus \cdots \oplus f(y_r) \end{aligned}$$

is an arbitrary nonzero linear combination of the component functions of G. Therefore, by Lemma 8,

$$N_g = 2^{rn-1} - \frac{1}{2}(2^n - 2N_f)^r.$$

By the definition of nonlinearity, it follows that

$$N_G = \min_{\substack{c_1, \ldots, c_m \in GF(2) \\ \text{and not all zeroes}}} N_g$$

$$= 2^{rn-1} - \frac{1}{2}\left(2^n - 2 \min_{\substack{c_1, \ldots, c_m \in GF(2) \\ \text{and not all zeroes}}} N_f\right)^r$$

$$= 2^{rn-1} - \frac{1}{2}(2^n - 2N_F)^r. \qquad \square$$

By Lemmas 11 and 12, we generalize Lemma 10 from single-output Boolean functions to vector-output Boolean functions for the case of all functions are equal.

Lemma 13. *Let F be a function from V_n to V_m. Let $c = (c_1, c_2, \ldots, c_r) \in V_r$. Let*

$$G(y_1, y_2, \ldots, y_r) = c_1 F(y_1) \oplus c_2 F(y_2) \oplus \cdots \oplus c_r F(y_r),$$

where $y_j \in V_n$, $j = 1, 2, \ldots, r$. Then

$$N_G = 2^{rn-1} - \frac{1}{2} \prod_{j=1}^{r} (2^n - 2c_j N_F).$$

Below we generalize Theorem 4 from single-output Boolean functions to vector-output Boolean functions for the case of all functions are equal.

Theorem 5. *Let F be a function from V_n to V_m. Let $A = (a_{ij})_{r \times s}$ be an $r \times s$ matrix over $GF(2)$ such that $r \geqslant s$ and $\mathrm{Rank}(A) = s$. Let L be the linear code generated by A^T and its minimum weight be d. Let*

$$G(y_1, y_2, \ldots, y_r) = (F(y_1), F(y_2), \ldots, F(y_r))A,$$

where $y_j \in V_n$, $j = 1, 2, \ldots, r$. Then

$$N_G = 2^{rn-1} - 2^{(r-d)n-1}(2^n - 2N_F)^d. \tag{6}$$

Proof. Let $\alpha_j = (a_{1j}, a_{2j}, \ldots, a_{rj})^T$, $j = 1, 2, \ldots, s$. Let

$$H(y_1, y_2, \ldots, y_r) = (F(y_1), F(y_2), \ldots, F(y_r)).$$

Then

$$G(y_1, y_2, \ldots, y_r) = (F(y_1), F(y_2), \ldots, F(y_r))A$$
$$= (H(y_1, y_2, \ldots, y_r)\alpha_1, H(y_1, y_2, \ldots, y_r)\alpha_2, \ldots, H(y_1, y_2, \ldots, y_r)\alpha_s),$$

where

$$H(y_1, y_2, \ldots, y_r)\alpha_j = a_{1j} F(y_1) \oplus a_{2j} F(y_2) \oplus \cdots \oplus a_{rj} F(y_r), \quad j = 1, 2, \ldots, s.$$

For any $\lambda_1, \lambda_2, \ldots, \lambda_s \in GF(2)$ and not all zeroes, let

$$\begin{aligned} E(y_1, y_2, \ldots, y_r) &= \lambda_1 H\alpha_1 \oplus \lambda_2 H\alpha_2 \oplus \cdots \oplus \lambda_s H\alpha_s \\ &= H[\lambda_1\alpha_1 \oplus \lambda_2\alpha_2 \oplus \cdots \oplus \lambda_s\alpha_s]. \end{aligned}$$

Note that

$$c = (c_1, c_2, \cdots, c_r) = (\lambda_1\alpha_1 \oplus \lambda_2\alpha_2 \oplus \cdots \oplus \lambda_s\alpha_s)^T$$

is a nonzero codeword of the linear code L generated by A^T. Therefore, E can be expressed as

$$\begin{aligned} E(y_1, y_2, \ldots, y_r) &= H(y_1, y_2, \ldots, y_r)c^T \\ &= c_1F(y_1) + c_2F(y_2) + \cdots + c_rF(y_r), \end{aligned}$$

where $c \in L^*$. Note that E is a function from V_{nr} to V_m, and any nonzero linear combination of the component functions of E is a nonzero linear combination of the component functions of G. Hence, by the definition of nonlinearity, for any $c \in L^*$,

$$N_{Hc^T} \geqslant N_G.$$

Therefore,

$$N_G \leqslant \min_{c \in L^*} N_{Hc^T}.$$

By Lemma 13, we have

$$\begin{aligned} N_G &\leqslant \min_{c \in L^*}\left(2^{rn-1} - \frac{1}{2}\prod_{j=1}^{r}(2^n - 2c_jN_F)\right) \\ &= 2^{rn-1} - \frac{1}{2}\max_{c \in L^*}\prod_{j=1}^{r}(2^n - 2c_jN_F) \\ &= 2^{rn-1} - 2^{(r-d)n-1}(2^n - 2N_F)^d, \end{aligned} \tag{7}$$

where $c = (c_1, c_2, \ldots, c_r)$. On the other hand, by Lemma 7, we have

$$N_G \geqslant 2^{rn-1} - 2^{(r-d)n-1}(2^n - 2N_F)^d. \tag{8}$$

Combining (7) with (8) yields (6). This completes the proof. □

6. Conclusion

In this paper, we study the constructions and nonlinearity of binary vector-output correlation-immune functions. It is shown that a vector-output Boolean function F is an (n, m, t) vector-output correlation-immune function if and only if every nonzero linear combination of the component functions of F is an $(n, 1, t)$ correlation-immune function. The matrix-product construction of vector-output correlation-immune functions is studied. A number of methods for constructing new vector-output correlation-immune functions from old ones are discussed. Furthermore, we study the nonlinearity of matrix-product vector-output Boolean functions. For some cases we give the exact formulas for the nonlinearity of matrix-product vector-output Boolean functions.

Acknowledgments

The authors would like to thank the anonymous reviewers and the Guest Editor Chaoping Xing for their valuable suggestions and comments that helped to improve the paper.

References

[1] C.H. Bennett, G. Brassard, J.M. Robert, Privacy amplification by public discussion, SIAM J. Comput. 17 (2) (1988) 210–229.

[2] P. Camion, A. Canteaut, Correlation-immune and resilient functions over a finite alphabet and their applications in cryptography, Designs Codes Cryptography 16 (1999) 121–149.

[3] L. Chen, F.-W. Fu, On the constructions of new resilient functions from old ones, IEEE Trans. Inform. Theory 45 (6) (1999) 2077–2082.

[4] B. Chor, O. Goldreich, J. Håstad, J. Friedman, S. Rudich, R. Smolensky, The bit extraction problem or t-resilient functions, Proceedings of the 26th IEEE Symposium on Foundations of Computer Science, IEEE Computer Society, 1985, pp. 396–407.

[5] C. Ding, G.Z. Xiao, W. Shan, The Stability Theory of Stream Ciphers, in: Lecture Notes in Computer Science, Vol. 561, Springer, Berlin, 1991.

[6] K. Nyberg, On the construction of highly nonlinear permutations, in: Advances in Cryptology—EUROCRYPT'92, Lecture Notes in Computer Science, Vol. 658, Springer, Berlin, 1993, pp. 92–98.

[7] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer, Berlin, 1986.

[8] P. Sarkar, S. Maitra, Construction of nonlinear Boolean functions with important cryptographic properties, in: Advances in Cryptology—EUROCRYPT'2000, Lecture Notes in Computer Science, Vol. 1807, Springer, Berlin, 2000, pp. 485–506.

[9] J. Seberry, X.M. Zhang, Y. Zheng, Nonlinearity and propagation characteristics of balanced Boolean functions, Inform. Comput. 119 (1) (1995) 1–13.

[10] T. Siegenthaler, Correlation immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. Inform. Theory 30 (5) (1984) 776–780.

[11] G.Z. Xiao, J.L. Massey, A spectral characterization of correlation-immune combining functions, IEEE Trans. Inform. Theory 34 (3) (1988) 569–571.

[12] Y. Yang, X. Lin, Codes and Cryptography, Posts and Telecommunications Press, Beijing, China, 1992 (in Chinese).

[13] X.M. Zhang, Y. Zheng, Cryptographically resilient functions, IEEE Trans. Inform. Theory 43 (5) (1997) 1740–1747.