On the Resistance of Prime-variable Rotation Symmetric Boolean Functions against Fast Algebraic Attacks

DU Yusong[1]*, WEI Baodian[2], ZHANG Fangguo[2] & ZHANG Huang[2]

[1]*School of Information Management, Sun Yat-sen University, Guangzhou* 510006*, China;*
[2]*School of Information Science and Technology, Sun Yat-sen University, Guangzhou* 510006*, China*

Abstract Boolean functions used in stream ciphers should have many cryptographic properties in order to help resist different kinds of cryptanalytic attacks. The resistance of Boolean functions against fast algebraic attacks is an important cryptographic property. Deciding the resistance of an n-variable Boolean function against fast algebraic attacks needs to determine the rank of a square matrix of order $\sum_{i=0}^{e}\binom{n}{i}$ over binary field $\mathbb{F}_2$, where $1 \leqslant e < \lceil \frac{n}{2} \rceil$. In this paper, for rotation symmetric Boolean functions in prime n variables, exploiting the properties of partitioned matrices and circulant matrices, we show that the rank of such a matrix can be obtained by determining the rank of a reduced square matrix of order $(\sum_{i=0}^{e}\binom{n}{i})/n$ over $\mathbb{F}_2$, so that the computational complexity decreases by a factor of n^{ω} for large n, where $\omega \approx 2.38$ is known as the exponent of the problem of computing the rank of matrices.

Keywords Boolean functions, cryptography, fast algebraic attacks, partitioned matrices, circulant matrices

1 Introduction

Boolean functions play a vital role in coding theory and in symmetric cryptography [1]. Various criteria related to cryptographically desirable Boolean functions have been proposed. Boolean functions used in stream ciphers, especially in the filer and combination generators of stream ciphers based on linear feedback shift registers, should have large algebraic immunity ($\mathcal{AI}$), in order to help resist algebraic attacks [2, 3, 4]. Moreover, Boolean functions should also have the resistance against fast algebraic attacks (FAA's) [5, 6, 7]. To a certain degree the algebraic immunity can be contained in the resistance of Boolean functions against FAA's [8, 9, 10], and the resistance against FAA's has been considered as an important cryptographic property.

Many problems on Boolean functions give rise to matrices. The study shows that an n-variable Boolean function f has the *optimal resistance against FAA's* if and only if there does not exist a nonzero n-variable Boolean function g of degree lower than $\frac{n}{2}$ such that $fg = h$ and $\deg(g) + \deg(h) < n$ [5, 11]. Usually, when considering the resistance of f against FAA's, we need to determine whether

$$\deg(fg) \geqslant n - e$$

holds for any nonzero n-variable Boolean function g with $\deg(g) \leqslant e$ [12, 8, 10]. Clearly, if it is ture for every $e = 1, 2, \cdots, \lceil \frac{n}{2} \rceil - 1$ then f has the optimal resistance. This problem can be converted into determining the rank of a $\sum_{i=0}^{e}\binom{n}{i} \times \sum_{i=0}^{e}\binom{n}{i}$ matrix over binary field $\mathbb{F}_2$.

As a matter of fact, there does not exist an n-variable Boolean function with optimal resistance against FAA's for most values of n. By investigating the determinant of such a $\sum_{i=0}^{e}\binom{n}{i} \times \sum_{i=0}^{e}\binom{n}{i}$ matrix, one can see that an n-variable Boolean function has the optimal resistance only if $n = 2^s$ or $n = 2^s + 1$ with positive integer s [13]. Therefore, an n-variable Boolean function f with *almost optimal resistance* against FAA's is also interesting, i.e., there does not exist a nonzero n-variable Boolean function g of degree lower than $\frac{n}{2}$ such that $fg = h$ and $\deg(g) + \deg(h) < n - 1$. This means that we need to determine whether $\deg(fg) \geqslant n - e - 1$ holds for any nonzero n-variable Boolean function g with $\deg(g) \leqslant e$ and this problem is then converted into determining the rank of a $\sum_{i=n-e-1}^{n}\binom{n}{i} \times \sum_{i=0}^{e}\binom{n}{i}$ matrix over $\mathbb{F}_2$. A class of n-variable balanced Boolean functions [11], called

[*] Corresponding author (email: duyusong@mail.sysu.edu.cn)

Carlet-Feng functions, was proved to have almost optimal resistance and even optimal resistance if $n = 2^s + 1$ exactly [13]. Another class of even n-variable balanced Boolean functions [14], called Tang-Carlet functions, was also proved to have almost optimal resistance [15]. But for Booelan functions that are neither Carlet-Feng nor Tang-Carlet we want to know if it is possible to decide their resistance against FAA's more efficiently.

The main contribution of this paper is to decide the resistance of a special class of Boolean functions, called rotation symmetric Boolean functions. We study the resistance of n-variable rotation symmetric Boolean functions against FAA's where n is prime. We show that (a small variant of) the $\sum_{i=0}^{e} \binom{n}{i} \times \sum_{i=0}^{e} \binom{n}{i}$ square matrix mentioned above for a prime n-variable rotation symmetric Boolean function can be represented as a partitioned matrix with circulant blocks, which is equivalent to a square matrix of order $(\sum_{i=0}^{e} \binom{n}{i})/n$ with circulant polynomial entries. Then, by the properties of partitioned matrices and circulant matrices, we prove that the determinant of the partitioned matrix over $\mathbb{F}_2$ can be obtained by computing the constant term of the determinant of such a polynomial matrix over $\mathbb{F}_2[x]/(x^n - 1)$. Finally, the problem on the polynomial matrix is converted into a reduced square matrix of order $(\sum_{i=0}^{e} \binom{n}{i})/n$ over integers.

2 Preliminaries

Let n be a positive integer. An n-variable Boolean function f is viewed as a mapping from vector space $\mathbb{F}_2^n$ to binary field $\mathbb{F}_2$ and has a unique n-variable polynomial representation over

$$\mathbb{F}_2[x_1, x_2, \cdots, x_n]/(x_1^2 - x_1, x_2^2 - x_2, \cdots, x_n^2 - x_n),$$

called the *algebraic normal form* (ANF) of f,

$$f(x_1, x_2, \cdots, x_n) = a_0 + \sum_{1 \leqslant i \leqslant n} a_i x_i + \sum_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j + \cdots + a_{12\cdots n} x_1 x_2 \cdots x_n,$$

where $a_0, a_i, a_{ij}, \ldots, a_{12\cdots n}$ belong to $\mathbb{F}_2$. For simplicity, an n-variable Boolean function $f(x)$ sometimes is written as $f(x) = \sum_{c \in \mathbb{F}_2^n} f_c x^c$, where $x^c = x_1^{c_1} x_2^{c_2} \cdots x_n^{c_n}$ and $f_c \in \mathbb{F}_2$. We denote by $\mathbb{B}_n$ the set of all the n-variable Boolean functions.

For $f \in \mathbb{B}_n$, the set of $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$ for which $f(x) = 1$ is called the support of the function, denoted by $\mathrm{supp}(f)$. The Hamming weight of f is the cardinality of $\mathrm{supp}(f)$, denoted by $\mathrm{wt}(f)$. Boolean function f is called balanced if $\mathrm{wt}(f) = 2^{n-1}$. The algebraic degree of Boolean function f, denoted by $\deg(f)$, is the degree of its ANF. It is well-known that the algebraic degree of a balanced n-variable Boolean function is less than n, i.e., the coefficient of term $x_1 x_2 \cdots x_2$ in its ANF must be zero.

An important class of Boolean functions are called rotation symmetric Boolean functions (RSBF's). For $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$, let

$$\rho(x_1, x_2, \cdots, x_n) = (x_2, x_3, \cdots, x_n, x_1),$$

and

$$\rho^k(x) = \rho(\rho^{k-1}(x)).$$

Definition 1. An n-variable Boolean function is called rotation symmetric if for any $x \in \mathbb{F}_2^n$, $f(\rho(x)) = f(x)$.

A rotation symmetric Boolean function is unchanged by any cyclic permutation ρ^k of the varaibles $x_1, x_2, \cdots, x_n$. The set of all n-variable rotation symmetric Boolean functions is denoted by $\mathbf{RS}\mathbb{B}_n$.

For $c \in \mathbb{F}_2^n$, we define

$$G_n(c) = \{\rho^k(c) \,|\, 0 \leqslant k \leqslant n - 1\}.$$

We denote $\nu(c)$ by the number of elements in $G_n(c)$, i.e., $\nu(c) = |G_n(c)|$, and select the representative element of $G_n(c)$ as the lexicographically first element. Let $\Gamma(n)$ be the set of all the representative element of $G_n(c)$. In particular, $\nu(c) = n$ if $c \in \mathbb{F}_2^n \setminus \{\mathbf{0}_n\}$ and n is prime.

With above notations, an n-variable rotation symmetric Boolean function f can be written as

$$f(x) = \sum_{c\in\Gamma(n)} f_c \sum_{u\in G_n(c)} x^u,$$

where $f_c \in \mathbb{F}_2$ and $x^u = x_1^{u_1}x_2^{u_2}\cdots x_n^{u_n}$. This also means that the existence of a representative term x^c implies the existence of all the term x^u $(u \in G_n(c))$ in the ANF of f.

3 Deciding the Resistance of Boolean Functions against Fast Algebraic Attacks

When studying the resistance against FAA's, the following two sets of vectors and a matrix over $\mathbb{F}_2$ are useful.

Denote $\mathcal{W}_e$ by the set $\{x \in \mathbb{F}_2^n \,|\, \mathrm{wt}_2(x) \leqslant e\}$ in lexicographic order and $\overline{\mathcal{W}}_d$ by the set $\{x \in \mathbb{F}_2^n \,|\, \mathrm{wt}_2(x) \geqslant d+1\}$ in reverse lexicographic order where $1 \leqslant e < \lceil \frac{n}{2} \rceil$ and $d < n$. For $x \in \mathbb{F}_2^n$, let $\bar{x} = (x_1 + 1, x_2 + 1, \cdots, x_n + 1)$. It is clear that if x is the j-th element in $\mathcal{W}_e$ and $\bar{x} \in \overline{\mathcal{W}}_d$ then $\bar{x}$ is the j the element in $\overline{\mathcal{W}}_d$. In particular, $\mathbf{1}_n = (1, 1, \cdots, 1)$ and $\mathbf{0}_n = (0, 0, \cdots, 0)$ are the first elements in $\overline{\mathcal{W}}_d$ and $\mathcal{W}_e$ respectively.

For $y, z \in \mathbb{F}_2^n$, let $z \subset y$ be an abbreviation for $\mathrm{supp}(z) \subset \mathrm{supp}(y)$, where $\mathrm{supp}(x) = \{i \,|\, x_i = 1\}$; and let $y \cap z = (y_1 \wedge z_1, y_2 \wedge z_2, \cdots, y_n \wedge z_n)$, where $\wedge$ is the AND operation. Recall the cyclic permutation ρ mentioned in Section 2, it is easy to see that $\rho(y \cap z) = \rho(y) \cap \rho(z)$. Denote $W(f; e, d)$ by a matrix over $\mathbb{F}_2$ related to function $f \in \mathbb{B}_n$, which is a $\sum_{i=d+1}^{n} \binom{n}{i} \times \sum_{i=0}^{e} \binom{n}{i}$ matrix with ij-th element equal to

$$w_{ij} = w_{yz} = f_{y\cap\bar{z}},$$

where y is the i-th element in $\overline{\mathcal{W}}_d$ and z is j-th element in $\mathcal{W}_e$.

It was proved in [13] that there exists no nonzero function g of degree at most e such that the product gh has degree at most d, which means that $\deg(fg) \geqslant d + 1$ holds for any nonzero n-variable Boolean function g with $\deg(g) \leqslant e$, if and only if the matrix $W(f; e, d)$ has full column rank. Therefore, if $W(f; e, n - e - 1)$ has full column rank then $\deg(fg) \geqslant n - e$ holds for any nonzero n-variable Boolean function g with $\deg(g) \leqslant e$, and if $W(f; e, n - e - 2)$ has full column rank then $\deg(fg) \geqslant n - e - 1$ holds for those g. That is to say, one can determine the optimal or almost optimal resistance by computing the rank of $W(f; e, n - e - 1)$ or $W(f; e, n - e - 2)$ for all the possible e.

It is easy to see that $W(f; e, n - e - 1)$ a symmetric $\sum_{i=0}^{e} \binom{n}{i} \times \sum_{i=0}^{e} \binom{n}{i}$, denoted by $W(f; e)$, and the resistance against FAA's is related to the problem whether matrix $W(f; e)$ has nonzero determinant over $\mathbb{F}_2$. It was also noted in [13] that $W(f; e)$ has an interesting property about its determinant.

Lemma 1. If $w_{\mathbf{11}} = \sum_{i=0}^{e} \binom{n}{i} + 1 \bmod 2$ then $\det(W(f; e)) = 0$, and if $w_{\mathbf{11}} = \sum_{i=0}^{e} \binom{n}{i} \bmod 2$ then $\det(W(f; e)) = \det(W(f; e)^{(1,1)})$, where $W(f; e)^{(1,1)}$ is the matrix that results from $W(f; e)$ by removing the first row and the first column. In particular, when $w_{\mathbf{11}} = 0$, $\det(W(f; e)) = 1$ only if $\sum_{i=0}^{e} \binom{n}{i}$ is even.

Generally and for simplicity, we define $V(f; e, d) = W(f; e, d)^{(1,1)}$, which is the matrix that results from $W(f; e, d)$ by removing the first row and the first column. In particular, we have $V(f; e) = W(f; e)^{(1,1)}$.

Usually, balanced Boolean functions are more interesting for cryptography. For balanced Boolean functions, entry $w_{\mathbf{11}}$ in Lemma 1 is always zero. When considering the resistance of balanced Boolean functions against FAA's, we have a definition of an n-variable balanced Boolean function having the (almost) optimal resistance against FAA's.

Definition 2. An n-variable balanced Boolean function has (almost) optimal resistance against FAA's if both of following two conditions hold for $1 \leqslant e < \lceil \frac{n}{2} \rceil$:

1. $\det(V(f;e)) = 1$ when $\sum_{i=0}^{e} \binom{n}{i}$ is even;
2. $W(f; e, n-e-2)$ has full column rank when $\sum_{i=0}^{e} \binom{n}{i}$ is odd. □

For balanced Boolean functions in odd number of variables, we give a simplified sufficient condition, compared with Definition 2, such that they have (almost) optimal resistance against FAA's. With this simplified condition, in Section 5, we can focus on the problem about the determinant of $V(f;e)$. This condition is mainly based on the following combinatoric property.

Lemma 2. Let n be odd and $e < n$. If $\sum_{i=0}^{e} \binom{n}{i}$ is odd, then both e and $\sum_{i=0}^{e+1} \binom{n}{i}$ are even.

Proof. Denote by $\mathrm{IntExp}_2(N)$ the exponent of the highest power of 2 that divides integer N. Let $\mathrm{IntExp}_2(n-1) = k$. We show that $\binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \cdots, \binom{n}{2^k-1}$ are all even, but $\binom{n}{2^k}$ is odd. Let $2 \leqslant t \leqslant 2^k$. When t is even the parity of $\binom{n}{t}$ is determined by

$$\mathrm{IntExp}_2 \left[\prod_{i=0}^{\frac{t-2}{2}} (n-1-2i) \right] - \mathrm{IntExp}_2 \left[\prod_{i=1}^{\frac{t}{2}} 2i \right].$$

Since $k = \mathrm{IntExp}_2(n-1)$ we have $n \equiv 1 \bmod 2^k$ and $\mathrm{IntExp}_2(n-1-2i) = \mathrm{IntExp}_2(2i)$ for every $i = 1, 2, \cdots, \frac{t-2}{2}$. Then when t is even, $\binom{n}{t}$ is also even if and only if

$$\mathrm{IntExp}_2(n-1) - \mathrm{IntExp}_2(t) > 0.$$

For $t = 2, 4, \cdots, 2^k - 2$ we have $\mathrm{IntExp}_2(n-1) - \mathrm{IntExp}_2(t) > 0$, and for $i = 2^k$ we have $\mathrm{IntExp}_2(n-1) - \mathrm{IntExp}_2(2i) = 0$ because $n \equiv 1 \bmod 2^k$ but $n \neq 1 \bmod 2^{k+1}$. Then $\binom{n}{2}, \binom{n}{4}, \binom{n}{6}, \cdots, \binom{n}{2^k-2}$ are all even, but $\binom{n}{2^k}$ is odd. Note that

$$\binom{n}{t+1} = \binom{n}{t} \cdot \frac{n-t}{t+1}.$$

This implies that the parity of $\binom{n}{t}$ is the same as that of $\binom{n}{t+1}$ when t is even. Therefore, $\binom{n}{3}, \binom{n}{5}, \binom{n}{7}, \cdots, \binom{n}{2^k-1}$ are all even, but $\binom{n}{2^k}$, $\binom{n}{2^k+1}$ are odd.

Now we can see that $\sum_{i=0}^{2^k} \binom{n}{i}$ is the first odd number in the sequence

$$\sum_{i=0}^{1} \binom{n}{i}, \sum_{i=0}^{2} \binom{n}{i}, \cdots, \sum_{i=0}^{2^k-1} \binom{n}{i}, \sum_{i=0}^{2^k} \binom{n}{i}, \cdots,$$

and $\sum_{i=0}^{2^k+1} \binom{n}{i} = \sum_{i=0}^{2^k} \binom{n}{i} + \binom{n}{2^k+1}$ must be even since $\binom{n}{2^k+1}$ is odd. The next possible odd number in the sequence must be in the form of $\sum_{i=0}^{2^k+2j} \binom{n}{i}$ where $1 \leqslant j \leqslant \frac{n-1-2^k}{2}$ and $\binom{n}{2^k+2j}$ is odd. Finally, if $\sum_{i=0}^{2^k+2j} \binom{n}{i}$ is odd then it must be followed by an even number $\sum_{i=0}^{2^k+2j+1} \binom{n}{i}$ in the sequence because $\binom{n}{2^k+2j}$ and $\binom{n}{2^k+2j+1}$ has the same parity. □

Theorem 1. Let n be odd, $1 \leqslant e \leqslant \lceil \frac{n}{2} \rceil$, and f be an n-variable balanced Boolean function. f has the (almost) optimal resistance against FAA's if $\det(V(f;e)) = 1$ holds for every e such that $\sum_{i=0}^{e} \binom{n}{i}$ is even.

Proof. Function f satisfies the first condition in Definition 2. When $\sum_{i=0}^{e} \binom{n}{i}$ is odd we need to check the rank of $W(f; e, n-e-2)$, which is a $\sum_{i=n-e-1}^{n} \binom{n}{i} \times \sum_{i=0}^{e} \binom{n}{i}$ matrix. By Lemma 2, if $\sum_{i=0}^{e} \binom{n}{i}$ is odd then $\sum_{i=0}^{e+1} \binom{n}{i}$ must be even. Note that matrix $W(f; e, n-e-2)$ consists of the first $\sum_{i=0}^{e} \binom{n}{i}$ columns of $W(f; e+1, n-e-2)$, which is a square matrix of order $\sum_{i=0}^{e+1} \binom{n}{i}$. We have $\det(W(f; e+1, n-e-2)) = \det(V(f; e+1)) = 1$ thus $W(f; e, n-e-2)$ has full column rank for $1 \leqslant e < \lceil \frac{n}{2} \rceil$ such that $\sum_{i=0}^{e} \binom{n}{i}$ is odd. This means that f also satisfies the second condition in Definition 2. Therefore, f has the (almost) optimal resistance against FAA's. □

4 Partitioned Property of $V(f;e,d)$ for RS-function f in Prime Variables

We concentrate on the resistance of rotation symmetric Boolean functions in prime number of variables and we always let $n > 2$ be a prime if not mentioned in the following content of this paper.

In this section, for $f \in \mathbf{RS}\mathbb{B}_n$, we show that matrix $V(f;e,d)$, the matrix that results from $W(f;e,d)$ by removing the first row and the first column, can be represented as a partitioned matrix with circulant blocks. In the next section, we consider computing the determinant of $V(f;e,n-e-1) = V(f;e)$ over $\mathbb{F}_2$.

Definition 3. An $n \times n$ circulant matrix C takes the form

$$\begin{pmatrix} c_0 & c_{n-1} & \cdots & c_2 & c_1 \\ c_1 & c_0 & c_{n-1} & & c_2 \\ \vdots & c_1 & c_0 & \ddots & \vdots \\ c_{n-2} & & \ddots & \ddots & c_{n-1} \\ c_{n-1} & c_{n-2} & \cdots & c_1 & c_0 \end{pmatrix}.$$

A circulant matrix is a special kind of matrix where each row vector is rotated one element to the right relative to the preceding row vector. It can be fully specified by the last row vector $(c_{n-1}, c_{n-2}, \cdots, c_0)$. The polynomial

$$\mathbf{a}(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

is called the *associated polynomial* of matrix C. □

Let P be a cyclic permutation matrix, given by

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

Substitute matrix P for x in the associated polynomial, we have $C = \mathbf{a}(P)$.

Moreover, for any two given circulant matrices A and B, and their associated polynomials $\mathbf{a}(x)$ and $\mathbf{b}(x)$ respectively, it is easy to see that the sum $A+B$ is a circulant matrix with associated polynomial $\mathbf{a}(x)+\mathbf{b}(x)$ and the product $AB = BA$ is a circulant matrix with associated polynomial $\mathbf{a}(x)\mathbf{b}(x) \bmod (x^n - 1)$. In other words, circulant matrices form a commutative algebra.

For rotation symmetric functions, recalling $\Gamma(n)$, the set of all the representative element of $G_n(c)$, we denote by $\Gamma_e(n)$ the set $\{y \in \Gamma(n) \,|\, \mathrm{wt}_2(y) \leqslant e\}$ ordered by increasing weight and by $\gamma_d(n)$ the set $\{y \in \Gamma(n) \,|\, \mathrm{wt}_2(y) \geqslant d+1\}$ in reverse order as $\Gamma_e(n)$. It is clear that applying the cyclic permutation to each element repeatedly in $\Gamma_e(n)$ and in $\gamma_d(n)$ results $\mathcal{W}_e$ and $\overline{\mathcal{W}}_d$ respectively.

Lemma 3. Let n be a prime and $f \in \mathbf{RS}\mathbb{B}_n$. For $\alpha \in \Gamma_e(n) \setminus \{\mathbf{0}_n\}$ and $\beta \in \gamma_d(n) \setminus \{\mathbf{1}_n\}$, matrix

$$V_{\beta\alpha} = \{w_{yz}\}_{y \in G_n(\beta), z \in G_n(\alpha)},$$

is circulant.

Proof. Note that $V_{\beta\alpha}$ is a $(\nu(\beta) \times \nu(\alpha))$ matrix, and prime n implies that $\nu(\beta) = \nu(\alpha) = n$, then $V_{\beta\alpha}$ is an

$n \times n$ square matrix, and can be written as follow,

$$\begin{pmatrix} w_{\beta\alpha} & w_{\beta\rho(\alpha)} & \cdots & w_{\beta\rho^{n-2}(\alpha)} & w_{\beta\rho^{n-1}(\alpha)} \\ w_{\rho(\beta)\alpha} & w_{\rho(\beta)\rho(\alpha)} & w_{\rho(\beta)\rho^{2}(\alpha)} & & w_{\rho(\beta)\rho^{n-1}(\alpha)} \\ \vdots & w_{\rho^{2}(\beta)\rho(\alpha)} & w_{\rho^{2}(\beta)\rho^{2}(\alpha)} & \ddots & \vdots \\ w_{\rho^{n-2}(\beta)\alpha} & & \ddots & \ddots & w_{\rho^{n-2}(\beta)\rho^{n-1}(\alpha)} \\ w_{\rho^{n-1}(\beta)\alpha} & w_{\rho^{n-1}(\beta)\rho(\alpha)} & \cdots & w_{\rho^{n-1}(\beta)\rho^{n-2}(\alpha)} & w_{\rho^{n-1}(\beta)\rho^{n-1}(\alpha)} \end{pmatrix}$$

Thanks to the rotation symmetry of f, we have

$$f_{y\cap\bar{z}} = f_{\rho(y\cap\bar{z})} = f_{\rho(y)\cap\rho(\bar{z})} = \cdots = f_{\rho^{n-1}(y\cap\bar{z})} = f_{\rho^{n-1}(y)\cap\rho^{n-1}(\bar{z})}.$$

Then,

$$\begin{array}{ccccccc} w_{\beta\alpha} & = & w_{\rho(\beta)\rho(\alpha)} & = \cdots = & w_{\rho^{n-1}(\beta)\rho^{n-1}(\alpha)} & = & f_{\beta\cap\bar{\alpha}} \\ w_{\rho(\beta)\alpha} & = & w_{\rho^{2}(\beta)\rho(\alpha)} & = \cdots = & w_{\beta\rho^{n-1}(\alpha)} & = & f_{\rho(\beta)\cap\bar{\alpha}} \\ \vdots & & & & & & \\ w_{\rho^{n-2}(\beta)\alpha} & = & w_{\rho^{n-1}(\beta)\rho(\alpha)} & = \cdots = & w_{\rho^{n-3}(\beta)\rho^{n-1}(\alpha)} & = & f_{\rho^{n-2}(\beta)\cap\bar{\alpha}} \\ w_{\rho^{n-1}(\beta)\alpha} & = & w_{\beta\rho(\alpha)} & = \cdots = & w_{\rho^{n-2}(\beta)\rho^{n-1}(\alpha)} & = & f_{\rho^{n-1}(\beta)\cap\bar{\alpha}} \end{array}$$

which means that $V_{\beta\alpha}$ is circulant matrix with associated polynomial

$$\mathbf{a}_{V_{\beta\alpha}}(x) = f_{\beta\cap\bar{\alpha}} + f_{\rho(\beta)\cap\bar{\alpha}} \cdot x + \cdots + f_{\rho^{n-1}(\beta)\cap\bar{\alpha}} \cdot x^{n-1}. \qquad \square$$

The first row of $W(f;e,d)$ is $\{w_{\mathbf{1}_n,z}\}_{z\in\mathcal{W}_e}$ and the first column of $W(f;e,d)$ is $\{w_{y,\mathbf{0}_n}\}_{y\in\overline{\mathcal{W}}_d}$. From the definition of $V(f;e,d)$, it can seen that $V_{\beta\alpha}$ in Lemma 3 is a sub-matrix of $V(f;e,d)$ since $\alpha \neq \mathbf{0}_n$ and $\beta \neq \mathbf{1}_n$. Denote by $V_{ij}(1 \leqslant i \leqslant k_1, 1 \leqslant j \leqslant k_2)$ the matrix $V_{\beta\alpha}$ where β is the i-th element in $\gamma_d(n) \setminus \{\mathbf{1}_n\}$ and α is the j-th element in $\Gamma_e(n) \setminus \{\mathbf{0}_n\}$. Then matrix $V(f;e,d)$ can be represented as a partitioned matrix as follow,

$$\begin{pmatrix} V_{11} & V_{12} & \cdots & V_{1k_2} \\ V_{21} & V_{22} & \cdots & V_{2k_2} \\ \vdots & \vdots & & \vdots \\ V_{k_1 1} & V_{k_1 2} & \cdots & V_{k_1 k_2} \end{pmatrix}, \tag{1}$$

where $k_1 = |\gamma_d(n)| - 1$, $k_2 = |\Gamma_e(n)| - 1$ and each block V_{ij} is circulant. This means that we obtain a partitioned property of $V(f;e,d)$ for any RS-function f in prime variables.

Theorem 2. Let n be a prime and $f \in \mathbf{RS}\mathbb{B}_n$. Then matrix $V(f;e,d)$ can be partitioned into $(k_1 \times k_2)$ circulant blocks of order $n \times n$, where $k_1 = |\gamma_d(n)| - 1$ and $k_2 = |\Gamma_e(n)| - 1$.

Note that $|\gamma_{n-e-1}(n)| = |\Gamma_e(n)|$. Thus for prime n matrix $V(f;e)$ can be partitioned into $(k \times k)$ circulant blocks of order $n \times n$, where $k = |\Gamma_e(n)| - 1$. With the notations in Equation (1), denote by V_{ji} the symmetric block of $V_{ij}(1 \leqslant i,j \leqslant k, i \neq j)$ in matrix $V(f;e)$.

5 The Determinant of $V(f;e)$ for RS-function f in Prime Variables

The following property may be known as the generalized Schur's formula about the determinants of partitioned matrices or block matrices.

Lemma 4. [16] Let $\mathbb{R}$ be a commutative ring. Assume that M is a $(kn \times kn)$ matrix over $\mathbb{R}$ and can be partitioned into k^2 blocks of order $n \times n$. If all the blocks, denoted by $C_{ij}(1 \leqslant i, j \leqslant k)$, are commutative pairwise under the matrix multiplication over $\mathbb{R}$, then the determinant of M,

$$\det(M) = \det\left(\sum_{\pi \in \mathcal{P}[k]} \operatorname{sgn}(\pi) C_{1\pi(1)} C_{2\pi(2)} \cdots C_{k\pi(k)}\right),$$

where $\mathcal{P}[k]$ is set of all possible permutations of integer set $\{1, 2, \cdots, k\}$ and sgn is the sign of permutation π.

Corollary 1. Assume that M is a $(kn \times kn)$ non-zero matrix over $\mathbb{F}_2$ and can be partitioned into k^2 blocks of order $n \times n$. If all the blocks, denoted by $C_{ij}(1 \leqslant i, j \leqslant k)$, are pairwise commutative under the matrix multiplication, then the determinant of M,

$$\det(M) = \det\left(\sum_{\pi \in \mathcal{P}[k]} C_{1\pi(1)} C_{2\pi(2)} \cdots C_{k\pi(k)}\right),$$

where $\mathcal{P}[k]$ is set of all possible permutations of integer set $\{1, 2, \cdots, k\}$.

Circulant matrices are pairwise commutative under the matrix multiplication. Lemma 4 or Corollary 1 can be applied to $V(f; e)$ directly.

Theorem 3. Let n be a prime and $f \in \mathbf{RS}\mathbb{B}_n$. The determinant of matrix $V(f; e)$ is equal to

$$\det\left(\sum_{\pi \in \mathcal{P}[k]} V_{1\pi(1)} V_{2\pi(2)} \cdots V_{k\pi(k)}\right),$$

where $k = |\Gamma_e(n)| - 1$.

According to Theorem 3, the determinant of matrix $V(f; e)$ is equal to that of a circulant matrix of order $n \times n$. From the relationship between circulant matrices and their associated polynomials, we can see that its associated polynomial is the determinant of polynomial matrix

$$\begin{pmatrix} \mathbf{a}_{11}(x) & \mathbf{a}_{12}(x) & \cdots & \mathbf{a}_{1k}(x) \\ \mathbf{a}_{21}(x) & \mathbf{a}_{22}(x) & \cdots & \mathbf{a}_{2k}(x) \\ \vdots & \vdots & & \vdots \\ \mathbf{a}_{k1}(x) & \mathbf{a}_{k2}(x) & \cdots & \mathbf{a}_{kk}(x) \end{pmatrix}$$

over $\mathbb{F}_2[x]/(x^n - 1)$, which is equal to

$$\sum_{\pi \in \mathcal{P}[k]} \left(\prod_{i=1}^{k} \mathbf{a}_{i\pi(i)}\right) \bmod (x^n - 1),$$

where $\mathbf{a}_{i\pi(i)}$ is the associated polynomial of circulant matrix $V_{i\pi(i)}$ and $k = |\Gamma_e(n)| - 1$.

Corollary 2. Let n be a prime and $f \in \mathbf{RS}\mathbb{B}_n$. The determinant of matrix $V(f; e)$ is equal to that of a circulant matrix with associated polynomial $\sum_{\pi \in \mathcal{P}[k]} \left(\prod_{i=1}^{k} \mathbf{a}_{i\pi(i)} \bmod (x^n - 1)\right)$, where $\mathbf{a}_{i\pi(i)}$ is the associated polynomial of circulant matrix $V_{i\pi(i)}$ and $k = |\Gamma_e(n)| - 1$.

Lemma 5. Let n be a prime and $f \in \mathbf{RS}\mathbb{B}_n$. If the associated polynomials of V_{ij} and V_{ji} are $\mathbf{a}(x) = \sum_{t=0}^{n-1} a_t x^t$ and $\mathbf{b}(x) = \sum_{t=0}^{n-1} b_t x^t$ respectively, then $a_0 = b_0$, $a_t = b_{n-t}$ and $b_t = a_{n-t}$ hold for $1 \leqslant t \leqslant n - 1$.

Proof. Let β be the i-th element in $\gamma_d(n) \setminus \{\mathbf{1}_n\}$ and α be the j-th element in $\Gamma_e(n) \setminus \{\mathbf{0}_n\}$. Since $\bar{\alpha}$ is the j-th element in $\gamma_d(n) \setminus \{\mathbf{1}_n\}$ and $\bar{\beta}$ is i-th element in $\Gamma_e(n) \setminus \{\mathbf{0}_n\}$, from the proof of Lemma 3, we have $a_t = f_{\rho^t(\beta)\cap\bar{\alpha}}$, and $b_t = f_{\rho^t(\bar{\alpha})\cap\beta}$. Then $b_{n-t} = f_{\rho^{n-t}(\bar{\alpha})\cap\beta}$ and $a_{n-t} = f_{\rho^{n-t}(\beta)\cap\bar{\alpha}}$ for $1 \leqslant t \leqslant n-1$, and it is clear that $a_0 = f_{\beta\cap\bar{\alpha}} = f_{\bar{\alpha}\cap\beta} = b_0$. Note that

$$\rho^t(\rho^{n-t}(\bar{\alpha}) \cap \beta) = \rho^t(\beta) \cap \bar{\alpha},$$

and

$$\rho^t(\rho^{n-t}(\beta) \cap \bar{\alpha}) = \rho^t(\bar{\alpha}) \cap \beta.$$

Thanks to the rotation symmetry of function f, we have $f_{\rho^t(\beta)\cap\bar{\alpha}} = f_{\rho^{n-t}(\bar{\alpha})\cap\beta}$ and $f_{\rho^t(\bar{\alpha})\cap\beta} = f_{\rho^{n-t}(\beta)\cap\bar{\alpha}}$, i.e., $a_t = b_{n-t}$ and $b_t = a_{n-t}$ for $1 \leqslant t \leqslant n-1$. □

Lemma 6. Let n be a prime and $f \in \mathbf{RS}\mathbb{B}_n$. The associated polynomial $\mathbf{a}(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ of a block on the diagonal of matrix $V(f;e)$ satisfies $c_i = c_{n-i}$ for $1 \leqslant i \leqslant n-1$.

Proof. Let $k = |\Gamma_e(n)| - 1$ and α be the k-th element in $\Gamma_e(n) \setminus \{\mathbf{0}_n\}$. Then $\beta = \bar{\alpha}$ is the k-th element in $\gamma_d(n) \setminus \{\mathbf{1}_n\}$. Hence, the k-th block on the diagonal of matrix $V(f;e)$, denoted by V_{kk}, can be fully determined by α. From the proof of Lemma 3, its associated polynomial can be given by

$$\mathbf{a}_{V_{kk}}(x) = \sum_{i=0}^{n-1} = f_{\rho^i(\beta)\cap\bar{\alpha}} \cdot x^i = \sum_{i=0}^{n-1} = f_{\rho^i(\bar{\alpha})\cap\bar{\alpha}} \cdot x^i,$$

i.e., $c_i = f_{\rho^i(\bar{\alpha})\cap\bar{\alpha}}$ and $c_{n-i} = f_{\rho^{n-i}(\bar{\alpha})\cap\bar{\alpha}}$ for $1 \leqslant i \leqslant n-1$.

Let $\bar{\alpha} = (a_1, a_2, \cdots, a_n)$. For $1 \leqslant i \leqslant \frac{n-1}{2}$ we have

$$\rho^i(\bar{\alpha}) \cap \bar{\alpha} = (a_{i+1}a_1, a_{i+2}a_2, \cdots, a_na_{n-i}, a_1a_{n-i+1}, a_2a_{n-i+2}, \cdots, a_ia_n),$$

and

$$\rho^{n-i}(\bar{\alpha}) \cap \bar{\alpha} = (a_{n-i+1}a_1, a_{n-i+2}a_2, \cdots, a_na_i, a_1a_{i+1}, a_2a_{i+2} \cdots, a_{n-i}a_n).$$

Therefore,

$$\rho^{n-i}(\bar{\alpha}) \cap \bar{\alpha} = \rho^{n-i}(\rho^i(\bar{\alpha}) \cap \bar{\alpha}),$$

which implies that $f_{\rho^i(\bar{\alpha})\cap\bar{\alpha}} = f_{\rho^{n-i}(\bar{\alpha})\cap\bar{\alpha}}$ and $c_i = c_{n-i}$ for $1 \leqslant i \leqslant n-1$ due to the rotation symmetry of function f. □

For simplicity, we say that a polynomial of degree less than n over $\mathbb{F}_2[x]$ is *coefficient symmetric* or a coefficient symmetric polynomial if its coefficients satisfy the conditions in Lemma 6. The following three lemmas are about the properties of coefficient symmetric polynomial.

Lemma 7. Let C be an $n \times n$ circulant matrix over $\mathbb{F}_2$. If the coefficients of associated polynomial $\mathbf{a}(x) = \sum_{i=0}^{n-1} c_ix^i$ satisfy $c_i = c_{n-i}$ for $1 \leqslant i \leqslant n-1$, then the determinant of matrix C, $\det(C) = c_0$.

Proof. View matrix C as a circulant matrix over the complex field $\mathbb{C}$. Let ω be the n-th roots of unity and $\sqrt{-1}$ is the imaginary unit, i.e., $\omega = \exp(\frac{2\pi\sqrt{-1}}{n}) = \cos\frac{2\pi}{n} + \sqrt{-1}\sin\frac{2\pi}{n}$. It can be verified that the eigenvalues of the transpose of matrix C are then given by $\lambda_j = c_0 + c_1\omega^j + c_2\omega^{2j} + c_{n-1}\omega^{(n-1)j}$ with $j = 0, 1, \cdots, n-1$. Then the determinant of matrix C over complex field $\mathbb{C}$ is equal to $\prod_{j=0}^{n-1}\lambda_j$, which must be an integer, and the determinant of matrix C in finite field $\mathbb{F}_2$ is

$$\det(C) = \prod_{j=0}^{n-1}(c_0 + c_1\omega^j + c_2\omega^{2j} + \cdots + c_{n-1}\omega^{(n-1)j}) \bmod 2.$$

Note that $\omega^{ij} + \omega^{(n-i)j} = 2 \cdot \cos\frac{2\pi ij}{n}$. From $c_i = c_{n-1}$ we have

$$\det(C) = \prod_{j=0}^{n-1} \left(c_0 + 2\sum_{i=1}^{\frac{n-1}{2}} c_i \cos(\frac{2\pi ij}{n}) \right) \bmod 2 \equiv c_0^n \bmod 2 = c_0.$$

Lemma 8. Let $\mathbf{a}(x) = \sum_{i=0}^{n-1} a_i x^i$ and $\mathbf{b}(x) = \sum_{j=0}^{n-1} b_j x^j$ be two polynomials of degree at most $n-1$ over $\mathbb{F}_2[x]$. Assume that $\mathbf{c}(x) = \mathbf{a}(x)\mathbf{b}(x) \bmod (x^n - 1) = \sum_{k=0}^{n-1} c_k x^k$. For $1 \leqslant i, j, k \leqslant n-1$, if $a_i = a_{n-i}$ and $b_j = b_{n-j}$, or if $a_i = b_{n-i}$, $b_j = a_{n-j}$ and $a_0 = b_0$, then $c_k = c_{n-k}$.

Proof. For $1 \leqslant k \leqslant n-1$ we have

$$c_k = a_0 b_k + a_k b_0 + \sum_{\substack{i+j=k \bmod n \\ 1\leqslant i,j\leqslant n-1}} a_i b_j, \quad c_{n-k} = a_0 b_{n-k} + a_{n-k} b_0 + \sum_{\substack{i+j=(n-k) \bmod n \\ 1\leqslant i,j\leqslant n-1}} a_i b_j.$$

Consider

$$\{(i,j) \,|\, i+j = k \bmod n, 1 \leqslant i,j \leqslant n-1\}$$

and

$$\{(i,j) \,|\, i+j = n-k \bmod n, 1 \leqslant i,j \leqslant n-1\}.$$

There exist two one-to-one correspondences,

$$(i,j) \mapsto (n-i, n-j) \quad \text{and} \quad (i,j) \mapsto (n-j, n-i),$$

between the above two sets. Then, for $1 \leqslant k \leqslant n-1$ we have

$$c_{n-k} = a_0 b_{n-k} + a_{n-k} b_0 + \sum_{\substack{i+j=k \bmod n \\ 1\leqslant i,j\leqslant n-1}} a_{n-i} b_{n-j} = a_0 b_k + a_k b_0 + \sum_{\substack{i+j=k \bmod n \\ 1\leqslant i,j\leqslant n-1}} a_i b_j = c_k$$

if $a_i = a_{n-i}$ and $b_j = b_{n-j}$, and have

$$c_{n-k} = a_0 b_{n-k} + a_{n-k} b_0 + \sum_{\substack{i+j=k \bmod n \\ 1\leqslant i,j\leqslant n-1}} a_{n-j} b_{n-i} = a_0 a_k + b_k b_0 + \sum_{\substack{i+j=k \bmod n \\ 1\leqslant i,j\leqslant n-1}} b_j a_i = b_0 a_k + b_k a_0 + \sum_{\substack{i+j=k \bmod n \\ 1\leqslant i,j\leqslant n-1}} b_j a_i = c_k$$

if $a_0 = b_0$, $a_i = b_{n-i}$ and $b_j = a_{n-j}$. This completes the proof. □

Lemma 9. Let $\{\mathbf{a}_1(x), \mathbf{a}_2(x), \cdots, \mathbf{a}_k(x), \mathbf{b}_1(x), \mathbf{b}_2(x), \cdots, \mathbf{b}_k(x)\}$ be $2k$ polynomials of degree at most $n-1$ over $\mathbb{F}_2[x]$. Assume that $\mathbf{a}_i(x) = \sum_{j=0}^{n-1} a_{ij} x^i$, $\mathbf{b}_i(x) = \sum_{j=0}^{n-1} b_{ij} x^i$,

$$\mathbf{h}_1(x) = \prod_{i=0}^{k} \mathbf{a}_i(x) \bmod (x^n - 1) = \sum_{j=0}^{n-1} h_{1j} x^j,$$

and

$$\mathbf{h}_2(x) = \prod_{i=0}^{k} \mathbf{b}_i(x) \bmod (x^n - 1) = \sum_{j=0}^{n-1} h_{2j} x^j.$$

For $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant n-1$, if $a_{i0} = b_{i0}$, $a_{ij} = b_{i(n-j)}$ and $b_{ij} = a_{i(n-j)}$, then $h_{1j} + h_{2j} = h_{1(n-j)} + h_{2(n-j)}$.

Proof. Let $\Lambda = \{1, 2, 3, \cdots, n-1, n\}$. For $1 \leqslant j \leqslant n-1$ we have $h_{1j} + h_{2j}$ eqauls

$$\sum_{u=1}^{n} \sum_{\substack{\{s_1, s_2, \cdots, s_u\} \subseteq \Lambda \\ \{s_{u+1}, s_{u+2}, \cdots, s_k\} \\ \subseteq \Lambda \setminus \{s_1, s_2, \cdots, s_u\}}} \sum_{\substack{j_{s_1} + \cdots + j_{s_u} = j \bmod n \\ 1 \leqslant j_{s_1}, \cdots, j_{s_u} \leqslant n-1}} \left(a_{s_1 j_{s_1}} \cdots a_{s_u j_{s_u}} a_{s_{u+1} 0} \cdots a_{s_k 0} + b_{s_1 j_{s_1}} \cdots b_{s_u j_{s_u}} b_{s_{u+1} 0} \cdots b_{s_k 0} \right).$$

The proof is similar to Lemma 8. There exists one-to-one correspondence

$$(j_{s_1}, j_{s_2}, \cdots, j_{s_u}) \mapsto (n - j_{s_1}, n - j_{s_2}, \cdots, n - j_{s_u})$$

between

$$\{(j_{s_1}, \cdots, j_{s_u}) \,|\, j_{s_1} + \cdots + j_{s_u} = j \bmod n, 1 \leqslant j_{s_1}, \cdots, j_{s_u} \leqslant n-1\}$$

and

$$\{(j_{s_1}, \cdots, j_{s_u}) \,|\, j_{s_1} + \cdots + j_{s_u} = (n-j) \bmod n, 1 \leqslant j_{s_1}, \cdots, j_{s_u} \leqslant n-1\}.$$

Since $a_{i0} = b_{i0}$, $a_{ij} = b_{i(n-j)}$ and $b_{ij} = a_{i(n-j)}$ for $1 \leqslant j \leqslant n-1$, it follows that $h_{1(n-j)} + h_{2(n-j)}$ equals

$$\begin{aligned}
&\sum_{u=1}^{n} \sum_{\substack{\{s_1,s_2,\cdots,s_u\}\subseteq\Lambda \\ \{s_{u+1},s_{u+2},\cdots,s_k\} \\ \subseteq\Lambda\setminus\{s_1,s_2,\cdots,s_u\}}} \sum_{\substack{j_{s_1}+\cdots+j_{s_u}=(n-j) \bmod n \\ 1\leqslant j_{s_1},\cdots,j_{s_u}\leqslant n-1}} \big(a_{s_1 j_{s_1}} \cdots a_{s_u j_{s_u}} a_{s_{u+1}0} \cdots a_{s_k 0} + b_{s_1 j_{s_1}} \cdots b_{s_u j_{s_u}} b_{s_{u+1}0} \cdots b_{s_k 0}\big) \\
&= \sum_{u=1}^{n} \sum_{\substack{\{s_1,s_2,\cdots,s_u\}\subseteq\Lambda \\ \{s_{u+1},s_{u+2},\cdots,s_k\} \\ \subseteq\Lambda\setminus\{s_1,s_2,\cdots,s_u\}}} \sum_{\substack{j_{s_1}+\cdots+j_{s_u}=j \bmod n \\ 1\leqslant j_{s_1},\cdots,j_{s_u}\leqslant n-1}} \Big(a_{s_1(n-j_{s_1})} \cdots a_{s_u(n-j_{s_u})} a_{s_{u+1}0} \cdots a_{s_k 0} + b_{s_1(n-j_{s_1})} \cdots b_{s_u(n-j_{s_u})} b_{s_{u+1}0} \cdots b_{s_k 0}\Big) \\
&= \sum_{u=1}^{n} \sum_{\substack{\{s_1,s_2,\cdots,s_u\}\subseteq\Lambda \\ \{s_{u+1},s_{u+2},\cdots,s_k\} \\ \subseteq\Lambda\setminus\{s_1,s_2,\cdots,s_u\}}} \sum_{\substack{j_{s_1}+\cdots+j_{s_u}=j \bmod n \\ 1\leqslant j_{s_1},\cdots,j_{s_u}\leqslant n-1}} \big(b_{s_1 j_{s_1}} \cdots b_{s_u j_{s_u}} b_{s_{u+1}0} \cdots b_{s_k 0} + a_{s_1 j_{s_1}} \cdots a_{s_u j_{s_u}} a_{s_{u+1}0} \cdots a_{s_k 0}\big) \\
&= h_{1j} + h_{2j}.
\end{aligned}$$

This completes the proof. □

Now we prove that the determinant of $V(f;e)$ over $\mathbb{F}_2$ can be obtained by computing the constant term of the determinant of polynomial matrix

$$\begin{pmatrix}
\mathbf{a}_{11}(x) & \mathbf{a}_{12}(x) & \cdots & \mathbf{a}_{1k}(x) \\
\mathbf{a}_{21}(x) & \mathbf{a}_{22}(x) & \cdots & \mathbf{a}_{2k}(x) \\
\vdots & \vdots & & \vdots \\
\mathbf{a}_{k}(x) & \mathbf{a}_{k2}(x) & \cdots & \mathbf{a}_{kk}(x)
\end{pmatrix},$$

over $\mathbb{F}_2[x]/(x^n - 1)$.

Theorem 4. Let n be a prime and $f \in \mathbf{RS}\mathbb{B}_n$. The determinant of matrix $V(f;e)$ is equal to the coefficient of constant term of polynomial

$$\mathbf{p}(x) = \sum_{i=0}^{n-1} p_i x^i = \sum_{\pi\in\mathcal{P}[k]} \left(\prod_{i=1}^{k} \mathbf{a}_{i\pi(i)}\right) \bmod (x^n - 1),$$

i.e., $\det(V(f;e)) = p_0$, where $\mathbf{a}_{i\pi(i)}$ is the associated polynomial of circulant matrix $V_{i\pi(i)}$ and $k = |\Gamma_e(n)| - 1$.

Proof. By Corollary 2 and Lemma 7, if $\mathbf{p}(x)$ is coefficient symmetric then $\det(V(f;e)) = p_0$. Therefore, it suffices to prove that $\mathbf{p}(x)$ is coefficient symmetric, i.e., $p_i = p_{n-i}$ holds for $1 \leqslant i \leqslant n-1$. □

For a given permutation $\pi \in \mathcal{P}[k]$, we consider the following two sets,

$$\Delta_1 = \{r \,|\, \pi(r) = r, 1 \leqslant r \leqslant k\}$$

and

$$\Delta_2 = \{(s,t) \,|\, \pi(s) = t, \pi(t) = s, 1 \leqslant s, t \leqslant k, s \neq t\}.$$

Let $\{r_1, r_2, \cdots, r_u\} = \Delta_1$, $\{(s_1, t_1), (s_2, t_2), \cdots, (s_v, t_v)\} = \Delta_2$, where $0 \leqslant u \leqslant k$ and $0 \leqslant v \leqslant \frac{k}{2}$. Then every product in the sum

$$\sum_{\pi \in \mathcal{P}[k]} \left(\prod_{i=1}^{k} \mathbf{a}_{i\pi(i)} \right) \bmod (x^n - 1) \tag{2}$$

can be written as

$$\mathbf{a}_{r_1 r_1} \cdots \mathbf{a}_{r_u r_u} \mathbf{a}_{s_1 t_1} \mathbf{a}_{t_1 s_1} \cdots \mathbf{a}_{s_v t_v} \mathbf{a}_{t_v s_v} \mathbf{a}_{i_1 j_1} \mathbf{a}_{i_2 j_2} \cdots \mathbf{a}_{i_{k-u-2v} j_{k-u-2v}} \bmod (x^n - 1),$$

where $(i_1, j_1), \cdots, (i_{k-u-2v}, j_{k-u-2v}) \notin \Delta_2$ and $i_1 \neq j_1, \cdots, i_{k-u-2v} \neq j_{k-u-2v}$. Note that

$$\mathbf{a}_{r_1 r_1} \cdots \mathbf{a}_{r_u r_u} \mathbf{a}_{s_1 t_1} \mathbf{a}_{t_1 s_1} \cdots \mathbf{a}_{s_v t_v} \mathbf{a}_{t_v s_v} \mathbf{a}_{j_1 i_1} \mathbf{a}_{j_2 i_2} \cdots \mathbf{a}_{j_{k-u-2v} i_{k-u-2v}} \bmod (x^n - 1)$$

is also a product in Sum (2). We add above two products and obtain

$$\mathbf{a}_{r_1 r_1} \cdots \mathbf{a}_{r_u r_u} \mathbf{a}_{s_1 t_1} \mathbf{a}_{t_1 s_1} \cdots \mathbf{a}_{s_v t_v} \mathbf{a}_{t_v s_v} \left(\prod_{\lambda=1}^{k-u-2v} \mathbf{a}_{i_\lambda j_\lambda} + \prod_{\lambda=1}^{k-u-2v} \mathbf{a}_{j_\lambda i_\lambda} \right) \bmod (x^n - 1).$$

This means that some products in Sum (2) can be combined in pairs. In particular, for a given permutation π such that $k = u + 2v$,

$$\mathbf{a}_{r_1 r_1} \cdots \mathbf{a}_{r_u r_u} \mathbf{a}_{s_1 t_1} \mathbf{a}_{t_1 s_1} \cdots \mathbf{a}_{s_v t_v} \mathbf{a}_{t_v s_v}$$

is a single product in Sum (2).

Recall that $\mathbf{a}_{r_1 r_1}, \cdots, \mathbf{a}_{r_u r_u}$ are the associated polynomial of blocks on the diagonal of matrix $V(f; e)$. Thus, they are coefficient symmetric and by Lemma 8 the product

$$\mathbf{a}_{r_1 r_1} \cdots \mathbf{a}_{r_u r_u} \bmod (x^n - 1)$$

is also coefficient symmetric. Similarly, By Lemma 5 $\mathbf{a}_{s_1 t_1} \mathbf{a}_{t_1 s_1} \bmod (x^n - 1), \cdots, \mathbf{a}_{s_v t_v} \mathbf{a}_{t_v s_v} \bmod (x^n - 1)$ are coefficient symmetric and by Lemma 8 again the product

$$\mathbf{a}_{s_1 t_1} \mathbf{a}_{t_1 s_1} \cdots \mathbf{a}_{s_v t_v} \mathbf{a}_{t_v s_v} \bmod (x^n - 1)$$

is also coefficient symmetric. Moreover, by Lemma 5

$$\mathbf{a}_{i_1 j_1} \bmod (x^n - 1), \mathbf{a}_{i_2 j_2} \bmod (x^n - 1), \cdots, \mathbf{a}_{i_{k-u-2v} j_{k-u-2v}} \bmod (x^n - 1)$$

and

$$\mathbf{a}_{j_1 i_1} \bmod (x^n - 1), \mathbf{a}_{j_2 i_2} \bmod (x^n - 1), \cdots, \mathbf{a}_{j_{k-u-2v} i_{k-u-2v}} \bmod (x^n - 1)$$

are two lists of polynomials satisfying the conditions in Lemma 9. Then it follows from Lemma 9 that

$$\left(\prod_{\lambda=1}^{k-u-2v} \mathbf{a}_{i_\lambda j_\lambda} + \prod_{\lambda=1}^{k-u-2v} \mathbf{a}_{j_\lambda i_\lambda} \right) \bmod (x^n - 1)$$

is a coefficient symmetric associated polynomial. Finally, we come to the conclusion that

$$\mathbf{a}_{r_1 r_1} \cdots \mathbf{a}_{r_u r_u} \mathbf{a}_{s_1 t_1} \mathbf{a}_{t_1 s_1} \cdots \mathbf{a}_{s_v t_v} \mathbf{a}_{t_v s_v} \left(\prod_{\lambda=1}^{k-u-2v} \mathbf{a}_{i_\lambda j_\lambda} + \prod_{\lambda=1}^{k-u-2v} \mathbf{a}_{j_\lambda i_\lambda} \right)$$

modulo $(x^n - 1)$ must be a coefficient symmetric polynomial and then $\mathbf{p}(x)$ is a sum of some coefficient symmetric polynomials. This completes the proof. □

Finally, in fact, we need not to compute the whole $\mathbf{p}(x)$. Due to its coefficient symmetry, the coefficient of its constant term can be obtained by computing an integer matrix of order $k \times k$.

Theorem 5. Let n be a prime and $f \in \mathbf{RS}\mathbb{B}_n$. The determinant of matrix $V(f;e)$ is equal to the determinant of $k \times k$ integer matrix

$$\begin{pmatrix} \mathbf{a}_{11}(1) & \mathbf{a}_{12}(1) & \cdots & \mathbf{a}_{1k}(1) \\ \mathbf{a}_{21}(1) & \mathbf{a}_{22}(1) & \cdots & \mathbf{a}_{2k}(1) \\ \vdots & \vdots & & \vdots \\ \mathbf{a}_{k}(1) & \mathbf{a}_{k2}(1) & \cdots & \mathbf{a}_{kk}(1) \end{pmatrix}$$

modulo 2, where $\mathbf{a}_{ij}(x)$ is the associated polynomial of circulant matrix V_{ij} and $k = |\Gamma_e(n)| - 1$.

Proof. The determinant of matrix $V(f;e)$ is equal to the coefficient of constant term of polynomial $\mathbf{p}(x) = \sum_{i=0}^{n-1} p_i x^i$ in $\mathbb{F}_2[x]/(x^n - 1)$ and

$$\mathbf{p}(x) = \det(\{\mathbf{a}_{ij}(x)\}_{1 \leqslant i,j \leqslant k}) = \det \begin{pmatrix} \mathbf{a}_{11}(x) & \mathbf{a}_{12}(x) & \cdots & \mathbf{a}_{1k}(x) \\ \mathbf{a}_{21}(x) & \mathbf{a}_{22}(x) & \cdots & \mathbf{a}_{2k}(x) \\ \vdots & \vdots & & \vdots \\ \mathbf{a}_{k}(x) & \mathbf{a}_{k2}(x) & \cdots & \mathbf{a}_{kk}(x) \end{pmatrix},$$

where the determinant of polynomial matrix $\{\mathbf{a}_{ij}(x)\}_{1 \leqslant i,j \leqslant k}$ is defined in $\mathbb{F}_2[x]/(x^n - 1)$. This determinant can also be defined in $\mathbb{Z}[x]$, and viewed as a polynomial with integer coefficients of degree at most $(n-1)k$, denoted by $\mathbf{q}(x) = \sum_{i=0}^{(n-1)k} q_i x^i$ with $q_i \in \mathbb{Z}$. Then we can denote by $\mathbf{q}(1)$ the determinant of integer matrix

$$\begin{pmatrix} \mathbf{a}_{11}(1) & \mathbf{a}_{12}(1) & \cdots & \mathbf{a}_{1k}(1) \\ \mathbf{a}_{21}(1) & \mathbf{a}_{22}(1) & \cdots & \mathbf{a}_{2k}(1) \\ \vdots & \vdots & & \vdots \\ \mathbf{a}_{k}(1) & \mathbf{a}_{k2}(1) & \cdots & \mathbf{a}_{kk}(1) \end{pmatrix} = \sum_{i=0}^{(n-1)k} q_i.$$

It is clear that $\mathbf{p}(x) = (\mathbf{q}(x) \bmod (x^n - 1)) \bmod 2$. We have $p_i = \left(\sum_{j=0}^{k-1} q_{i+jn}\right) \bmod 2$ for $0 \leqslant i \leqslant n-1$. Recall that $\mathbf{p}(x)$ is coefficient symmetric, i.e., $p_i = p_{n-i}$ for $1 \leqslant i \leqslant n-1$, then

$$\left(\sum_{j=0}^{k-1} q_{i+jn}\right) \equiv \left(\sum_{j=0}^{k-1} q_{n-i+jn}\right) \bmod 2,$$

which implies that

$$\begin{aligned} \left(\sum_{i=0}^{(n-1)k} q_i\right) \bmod 2 &= \left(\sum_{j=0}^{k-1} q_{0+jn}\right) \bmod 2 + \sum_{i=0}^{\frac{n-1}{2}} \left(\sum_{j=0}^{k-1} q_{i+jn} + \sum_{j=0}^{k-1} q_{n-i+jn}\right) \bmod 2 \\ &= \left(\sum_{j=0}^{k-1} q_{0+jn}\right) \bmod 2. \end{aligned}$$

This means that $\det(V(f;e)) = p_0 = \left(\sum_{j=0}^{k-1} q_{0+jn}\right) \bmod 2 = \mathbf{q}(1) \bmod 2$. □

Thanks to Theorem 5, we obtain an algorithm for computing the determinant of $V(f;e)$ over $\mathbb{F}_2$ more efficiently compared with the straightforward computation of the determinant of $V(f;e)$ over $\mathbb{F}_2$.

```
Computing the Determinant of $V(f;e)$ over $\mathbb{F}_2$
**Input**: balanced rotation symmetric function $f$ in $n$ variables (including all the coefficients of $f$), integer $e$ with $1 \leqslant e \leqslant \lceil \frac{n}{2} \rceil$
**Output**: $\det(V(f;e))$
**Initialize**: $d = n - e - 1$, $E = \sum_{i=0}^{e} \binom{n}{i}$, $\Gamma_e(n)$, $\gamma_d(n)$, $k = ((E-1)/n)$ and $(k \times k)$ matrix $A$
if $E$ is odd then output 0
for $i$ from 1 to $k$ do
    $\beta \leftarrow$ the $i$-th element in $\gamma_d(n) \setminus \{\mathbf{1}_n\}$
    for $j$ from 1 to $k$ do
        $\alpha \leftarrow$ the $j$-th element in $\Gamma_e(n) \setminus \{\mathbf{0}_n\}$
        $a_{ij} \leftarrow f_{\beta \cap \bar{\alpha}} + f_{\rho(\beta) \cap \bar{\alpha}} + \cdots + f_{\rho^{n-1}(\beta) \cap \bar{\alpha}}$
    end for
end for
$A \leftarrow \{a_{ij}\}_{1 \leqslant i,j \leqslant k}$
Compute and output $\det(A)$ mod 2
```

For prime n, we have that $k = (\sum_{i=0}^{e} \binom{n}{i} - 1)/n \approx (\sum_{i=0}^{e} \binom{n}{i})/n$. The complexity of computing $\det(V(f;e))$ in the way of Theorem 5 is about

$$\mathcal{O}\left(\left(\sum_{i=0}^{e} \binom{n}{i}\right)^{\omega} \cdot \left(\frac{1}{n}\right)^{\omega}\right),$$

where ω is known as the exponent of the problems of computing the determinant, the matrix inverse, the rank, the characteristic polynomial etc. As far as we know, the algorithm of Coppersmith-Winograd (for matrices that can be operated over fields) has the lowest aymptotical estimate that $\omega \approx 2.38$ [17].

Note that obtaining the integer matrix in the Theorem 5 needs $\mathcal{O}\left(\left(\sum_{i=0}^{e} \binom{n}{i}\right)^2 \cdot (1/n)\right)$ extra field operations. Thus the total complexity is about

$$\mathcal{O}\left(\left(\sum_{i=0}^{e} \binom{n}{i}\right)^{2} \cdot \frac{1}{n} + \left(\sum_{i=0}^{e} \binom{n}{i}\right)^{\omega} \cdot \left(\frac{1}{n}\right)^{\omega}\right),$$

which decreases by a factor of n^{ω} for large n, compared with the complexity of computing $\det(V(f;e))$ directly, that is about $\mathcal{O}\left(\left(\sum_{i=0}^{e} \binom{n}{i}\right)^{\omega}\right)$.

References

[1] Crama Y., Hammer P. L.: Boolean Models and Methods in Mathematics, Computer Science, and Engineering (Encyclopedia of Mathematics and its Applications). Cambridge University Press, Cambridge (2010)

[2] Courtois, N., Meier, W.: Algebraic attacks on stream ciphers with linear feedback. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 345-359. Springer, Heidelberg (2003)

[3] Meier, W., Pasalic, E., Carlet, C.: Algebraic attacks and decomposition of Boolean functions. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 474-491. Springer, Heidelberg (2004)

[4] Carlet, C., Dalai, D.K., Gupta, K.C., Maitra, S.: Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. IEEE Trans. Inform. Theory 52(7), 3105-3121 (2006)

[5] Courtois, N.: Fast algebraic attacks on stream ciphers with linear feedback. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 176-194. Springer, Heidelberg (2003)

[6] Armknecht F.: Improving fast algebraic attacks. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 65-82. Springer, Heidelberg (2004)

[7] Courtois, N.: Cryptanalysis of SFINKS. In: Won, D.H., Kim., S. (eds.) ICISC 2005, LNCS, vol. 3935, pp. 261-269. Springer, Heidelberg (2006)

[8] Pasalic, E.: Almost Fully Optimized Infinite Classes of Boolean Functions Resistant to (Fast) Algebraic Cryptanalysis. In: Lee, P.J., Cheon, J.H. (eds.) ICISC 2008. LNCS, vol. 5461, pp. 399-414. Springer, Heidelberg (2009)

[9] Rizomiliotis, P.: On the Resistance of Boolean Functions Against Algebraic Attacks Using Univariate Polynomial Representation. IEEE Transactions on Information Theory, 56(8), 4014-4024 (2010)

[10] Du Y., Zhang F., Liu M.: On the Resistance of Boolean Functions against Fast Algebraic Attacks. In: Kim, H. (ed.) ICISC 2011, LNCS, vol. 7259, 261-274. Springer, Heidelberg (2012)

[11] Carlet, C., Feng, K.: An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 425-440. Springer, Heidelberg (2008)

[12] Armknecht, F., Carlet, C., Gaborit, P., Künzli, S., Meier, W., Ruatta, O.: Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 147-164. Springer, Heidelberg (2006)

[13] Liu M., Zhang Y., Lin D.: Perfect Algebraic Immune Functions. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, 172-189. Springer, Heidelberg (2012)

[14] Tang D., Carlet C., Tang X.: Highly Nonlinear Boolean Functions With Optimal Algebraic Immunity and Good Behavior Against Fast Algebraic Attacks. IEEE Transactions on Information Theory, 59(1), 653-664 (2013)

[15] Liu M., Lin D.: Almost perfect algebraic immune functions with good nonlinearity. In: International Symposium on Information Theory, ISIT 2014. New York: IEEE, 2014, 1837-1841.

[16] Kovacs I., Silver D. S., Williams S. G.: Determinants of Commuting-Block Matrices. The American Mathematical Monthly. 106(10):950-952 (1999).

[17] Brgisser P., Clausen M., Shokrollahi A.: Algebraic Complexity Theory (Grundlehren der mathematischen Wissenschaften), Springer, Heidelberg (1997)