Algorithmic techniques in algebraic cryptanalysis and their applications

Makarim, R.H.

8 Ideals of Vectorial Boolean Functions

Contents

The main object studied in this chapter is the multi-output Boolean functions, that is functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ for some positive integers n and m. Such functions are called *vectorial Boolean functions*. The vectorial Boolean functions arise in many aspect of symmetric-key primitives, from S-Boxes, round functions, block ciphers, hash functions, etc. Many criteria have been developed to evaluate their suitability for cryptographic purposes. For instance, to design a block cipher immune against linear cryptanalysis [Mat93] the S-Boxes used must have high nonlinearity [Nyb92]. Another criterion is related to immunity of a primitives against differential cryptanalysis [BS90], where the S-Boxes should have low differential uniformity [Nyb93]. In addition to the two previous criteria, the absence of linear structures [MS89b] is another criterion which was recently shown to be related with differential-linear cryptanalysis [CKL+19, BDKW19].

In this chapter we shall present the relation among cryptographic criteria of vectorial Boolean functions and their corresponding multivariate ideals. We focus on the (non)linearity, differential, and autocorrelation of vectorial Boolean functions. We also establish the relation between the Walsh transform as well as Fourier transform with properties of multivariate ideals. Moreover, we exhibit new algorithms to compute the bias of a linear approximation, the probability of a differential, and the autocorrelation of the component functions using a Gröbner bases algorithm.

Generous examples are provided to illustrate the important results. We provide an open-source SageMath [The18] module Gbsbox to facilitate the verification of examples and to stimulate the research on this area. The module is available for download in the following link

`https://github.com/rusydi/gbsbox`.

We begin this chapter by describing necessary terminologies, notations, and well-known results from computational commutative algebra and Boolean functions in Section 8.1. This will be followed by Section 8.2, which describes the relation between properties of a vectorial Boolean function relevant for linear cryptanalysis and its corresponding ideal. An algorithm to compute the bias of a linear approximation based on a Gröbner basis algorithm is described in the same section. Section 8.3 presents the relation between properties of a vectorial Boolean function relevant for differential cryptanalysis and its corresponding ideal. The same section also explains an algorithm to compute the probability of a differential using a Gröbner basis algorithm. The relation of the ideal of a vectorial Boolean function with the notions of autocorrelation is described in Section 8.4.

Related Work

To the best of our knowledge, the connection between computational commutative algebra and cryptographic properties of vectorial Boolean functions remains underexplored to this date. The closest related works that we found are due to Bellini, Simonetti, and Sala [BSS14] as well as the work of Bellini, Mora, and Sala [BMS16]. Both papers proposed new algorithms to compute the nonlinearity of Boolean functions using Gröbner bases algorithms, where the latter is an improvement of the former.

Our work differs from [BSS14, BMS16] in two respects. Firstly, their results as a mapping $\mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ are restricted for the case $m = 1$, while the results in this chapter holds for any positive integers n, m. Secondly, the applications of Gröbner bases in [BSS14, BMS16] are limited within the context of (non)linearity, while this work proposes new applications of Gröbner bases related to the notions of (non)linearity, differential and autocorrelation.

Another related work is by Samardjiska and Gligoroski [SG14]. In their work, the authors employ (non)linearity measures that are typically used to assess the security of symmetric-key primitives to redefine certain properties of MPKCs. Their framework enables a generalization of several known attacks on MPKC schemes and offers insights into the factors that determine their effectiveness.

The differences between the results in this chapter and those in [SG14] are twofold. First, while the work in [SG14] draws upon the notions from symmetric-key cryptography to analyze MPKC schemes, our work takes the opposite direction: we apply notions from computational commutative algebra, typically used in the analysis of MPKCs, to investigate the properties of functions used in symmetric-key cryptography. Second, whereas [SG14] mainly focuses on the notion of (non)linearity, this chapter extends the discussion to include not only (non)linearity, but also differential property and autocorrelation.

8.1 Notations and Preliminaries

Let $F \subseteq \mathcal{R} = \mathbb{F}[x_1, \ldots, x_n]$ be a nonempty subset of $\mathcal{R}$. The main results in this chapter are relevant for $\mathbb{F} = \mathbb{F}_2$ but the propositions in this section are true for any field $\mathbb{F}$ or any finite field $\mathbb{F}_q$. We allow a mixed notation and write $\langle F, f\rangle$ for an ideal generated by $F \cup f$ where $f \in \mathcal{R}$. For any residue class ring $\mathcal{R}/I$ modulo an ideal $I \subseteq \mathcal{R}$, we denote by $\dim_{\mathbb{F}}(\mathcal{R}/I)$ the dimension of $\mathcal{R}/I$ as an $\mathbb{F}$-vector space. The set of zeros of $F \subseteq \mathcal{R}$ in an extension field $\mathbb{E}$ of $\mathbb{F}$ is denoted by $\mathbf{V}_{\mathbb{E}}(F) = \{\boldsymbol{v} \in \mathbb{E}^n : f(\boldsymbol{v}) = 0, \forall f \in F\}$.

Proposition 8.1. *For any ideal* $\{0\} \neq I \subset \mathcal{R}$*, we define* $\mathsf{RM}(I) = \mathsf{M}(\mathcal{R})\backslash\mathsf{LM}(I)$ *the set of* reduced monomials *w.r.t.* I*. Then*

$$\begin{aligned}\mathsf{RM}(I) &= \{\mathfrak{m} \in \mathsf{M}(\mathcal{R}) : s \nmid \mathfrak{m}, \forall s \in \mathsf{LM}(I)\}\\ &= \{\mathfrak{m} \in \mathsf{M}(\mathcal{R}) : s \nmid \mathfrak{m}, \forall s \in \mathsf{LM}(G)\}\end{aligned}$$

where G *is a Gröbner basis of* I*.*

Proof. See the proof of Lemma 6.51 in [BW93, pg. 272]. ■

Proposition 8.2. *The set* $\{\mathfrak{m} + I : \mathfrak{m} \in \mathsf{RM}(I)\}$ *is a basis of the* $\mathbb{F}$*-vector space* $\mathcal{R}/I$*.*

Proof. See the proof of Proposition 6.52 in [BW93, pg. 273]. ■

Proposition 8.3. *Let $\overline{\mathbb{F}}$ be an algebraic closure of the field $\mathbb{F}$ and assume that $I \subset \mathcal{R}$ is a zero-dimensional ideal. Then*

$$|\mathbf{V}_{\overline{\mathbb{F}}}(I)| \leq \dim_{\mathbb{F}}(\mathcal{R}/I).$$

*Moreover, if $\mathbb{F}$ has characteristic zero or is a finite field and I is a radical ideal, then the equality holds.**

Proof. See the proof of Theorem 8.32 in [BW93, pg. 348] ■

Definition 8.4. *For any polynomial ring $\mathcal{R} = \mathbb{F}_q[x_1, \ldots, x_n]$ defined over a finite field $\mathbb{F}_q$, we define the set of* field polynomials *of $\mathcal{R}$ as*

$$\mathsf{FP}(\mathcal{R}) = \{x_i^q - x_i : i = 1, \ldots, n\}.$$

Proposition 8.5. *If I is an ideal of $\mathcal{R} = \mathbb{F}_q[x_1, \ldots, x_n]$ where $\mathsf{FP}(\mathcal{R}) \subseteq I$, then the following holds*

1. *I is a zero-dimensional ideal,*
2. *I is a radical ideal,*
3. *$\mathbf{V}_{\mathbb{F}_q}(I) = \mathbf{V}_{\overline{\mathbb{F}_q}}(I)$.*

Proof. The proof of 1) follows from 5) in Proposition 3.46. The proof of 2) is immediate from Proposition 3.51. Finally, 3) is true since $\mathsf{FP}(\mathcal{R}) \subseteq I$ implies that $\mathbf{V}_{\overline{\mathbb{F}_q}}(I) \subseteq \mathbf{V}_{\mathbb{F}_q}(I)$. ■

In the pseudo-code of algorithms described in this chapter, the algorithm ReducedMonomials(G) takes a Gröbner basis G of a zero-dimensional ideal $I \subseteq \mathcal{R}$ and returns the set of reduced monomials of I. We provide the description of ReducedMonomials in Algorithm 8.1. The pseudo-code is adapted from the RedTerms algorithm in [BW93, pg. 424]. The algorithm maintain the set R of intermediate reduced monomials. In each iteration i, it multiplies all monomials in R by $x_i, x_i^2, \ldots, x_i^{k_i}$. The resulting non-reducible monomial product is then added to R.

For the rest of this chapter, we will work with the binary field $\mathbb{F}_2$. For any $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$, we sometimes write $\boldsymbol{v}$ as an integer $\sum_{i=1}^{n} v_i 2^{i-1}$ in hexadecimal format using teletype font family (e.g, $\boldsymbol{v} = (0, 1, 1, 1) \in \mathbb{F}_2^4$ can be written as `E`). The Hamming weight of $\boldsymbol{v}$ is denoted by $\mathsf{wt}(\boldsymbol{v})$ and the concatenation of $\boldsymbol{v}$ with $\boldsymbol{w} = (w_1, \ldots, w_m) \in \mathbb{F}_2^m$ is denoted by $(\boldsymbol{v} \parallel \boldsymbol{w}) = (v_1, \ldots, v_n, w_1, \ldots, w_m)$. For any Boolean function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$, we denote the $\mathbb{Z}$-valued function of f as $\widehat{f}$. We also define the Hamming weight of a Boolean function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ as $\mathsf{wt}(f) = |\{\boldsymbol{v} \in \mathbb{F}_2^n : f(\boldsymbol{v}) \neq 0\}|$. For any $\boldsymbol{b} \in \mathbb{F}_2^m$ and $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$, we define $S_{\boldsymbol{b}}(x) = \boldsymbol{b} \cdot S(x)$ as a component functions of S, where "$\cdot$" denotes the dot product vector. We call the function S_0 the trivial component function of S. For any $\boldsymbol{e}_j \in \mathbb{F}_2^m$, where $\boldsymbol{e}_j$ denotes a vector with a 1 in its j-th coordinate and 0 otherwise, we call $S_{\boldsymbol{e}_j}$ the j-th *coordinate function* of S.

* This proposition can be generalized to any perfect field $\mathbb{F}$ (see Definition 3.52 for the definition of perfect field).

Input: A Gröbner basis G of a zero-dimensional ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$
Output: The set $\mathsf{RM}(I)$ of reduced monomials of I

$R \leftarrow \{1\}$
for $i = 1$ **to** n **do**
  $M \leftarrow R$
  $k_i \leftarrow \max(\{e_i : x_1^{e_1} \cdots x_i^{e_i} \cdots x_n^{e_n} \in \mathsf{LM}(G)\})$
  while $M \neq \{\}$ **do**
    $\mathfrak{m} \leftarrow \textsc{Select}(M)$
    $M \leftarrow M \setminus \{\mathfrak{m}\}$
    for $l = 1$ **to** k_i **do**
      $\mathfrak{m} \leftarrow \mathfrak{m} \cdot x_i$
      if $\forall g \in G \ : \ \mathsf{LM}(g) \nmid \mathfrak{m}$ **then**
        $R \leftarrow R \cup \{\mathfrak{m}\}$
return R

Algorithm 8.1: Algorithm ReducedMonomials.

Definition 8.6. *Let f be an n-variable Boolean function. The Fourier transform $\mathcal{F}_f : \mathbb{F}_2^n \mapsto \mathbb{Z}$ and the Walsh transform $\mathcal{W}_f : \mathbb{F}_2^n \mapsto \mathbb{Z}$ of f are defined as*

$$\mathcal{F}_f(\boldsymbol{u}) = \sum_{\boldsymbol{v} \in \mathbb{F}_2^n} \widehat{f}(\boldsymbol{v}) \cdot (-1)^{\boldsymbol{u} \cdot \boldsymbol{v}}, \qquad \mathcal{W}_f(\boldsymbol{u}) = \sum_{\boldsymbol{v} \in \mathbb{F}_2^n} (-1)^{\widehat{f}(\boldsymbol{v})} \cdot (-1)^{\boldsymbol{u} \cdot \boldsymbol{v}}.$$

Proposition 8.7. *Let f be an n-variable Boolean function. We have the following relation*

$$\mathcal{F}_f(\boldsymbol{u}) = 2^{n-1}\delta(\boldsymbol{u}) - \frac{1}{2} \cdot \mathcal{W}_f(\boldsymbol{u})$$

where $\delta(\boldsymbol{u}) = 1$ if $\boldsymbol{u} = \boldsymbol{0}$ and 0 otherwise.

Proof. See the proof of Lemma 2.9 in [CS09, pg. 9]. ■

The primary theme of this chapter is the relation between cryptographic properties of S and ideals in multivariate polynomial ring. The variables of the input and output of S are denoted using x_i, y_j respectively. A system of equations that defines S is given by the set

$$F_S = \{y_j + h_j(x_1, \ldots, x_n) : 1 \leq j \leq m\} \subset \mathbb{F}_2[x_1, \ldots, x_n, y_1, \ldots, y_m]$$

where $h_j(x_1, \ldots, x_n)$ is the algebraic normal form of $S_{\boldsymbol{e}_j}$. We refer to the set F_S as the *algebraic normal form of S*.

Throughout this chapter, we also provide examples to illustrate the main results. All examples use the mapping defined in Table 20 and its algebraic normal form consists of the following polynomials

$$y_1 + x_1x_2x_3 + x_1x_3 + x_1 + x_2 + x_3x_4,$$
$$y_2 + x_1x_2x_4 + x_1x_2 + x_1x_3x_4 + x_1x_3 + x_1 + x_2x_3x_4 + x_2x_4 + x_3 + x_4,$$
$$y_3 + x_1x_2x_4 + x_1x_2 + x_1x_3 + x_2x_3x_4 + x_2x_3 + x_2 + x_3 + x_4,$$
$$y_4 + x_1x_2x_3 + x_1x_2 + x_1x_3x_4 + x_1x_3 + x_2x_3 + x_3x_4 + x_4.$$

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	0	3	5	8	6	A	F	4	E	D	9	2	1	7	C	B

Table 20: *An example of* $S : \mathbb{F}_2^4 \mapsto \mathbb{F}_2^4$.

8.2 Multivariate Ideals and Linear Property

In this section we shall prove the result stated in Theorem 1.3. The result establishes a relation between ideals in multivariate polynomial ring and properties of vectorial Boolean functions relevant for *linear cryptanalysis* [Mat93]. Linear cryptanalysis studies linear relations among parity bits of the plaintext, the ciphertext, and the secret key that holds with a certain probability. If there exists such relation with high probability, an attacker can estimate the parity bit of the key using the parity bits of known plaintexts and their corresponding ciphertexts. Formally, let $E : \mathbb{F}_2^n \times \mathbb{F}_2^k \mapsto \mathbb{F}_2^n$ where $\mathbb{F}_2^k$ is the key space and for any fix $\boldsymbol{k} \in \mathbb{F}_2^k$ we define $E_{\boldsymbol{k}}(x) = E(x, \boldsymbol{k})$. The goal of linear cryptanalysis is to find a linear expression of the following form

$$\boldsymbol{a} \cdot \boldsymbol{v} + \boldsymbol{b} \cdot E_{\boldsymbol{k}}(\boldsymbol{v}) = \boldsymbol{c} \cdot \boldsymbol{k} \qquad \boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^n, \boldsymbol{c} \in \mathbb{F}_2^k$$

that holds with probability $p \neq 1/2$ for randomly given plaintext $\boldsymbol{v}$ and its corresponding ciphertext $E_{\boldsymbol{k}}(\boldsymbol{v})$. Clearly, the effectiveness of linear cryptanalysis depends on the magnitude of $|p - 1/2|$. Once such approximation is found, it is possible to determine the value of $\boldsymbol{c} \cdot \boldsymbol{k}$ based on the maximum likelihood method (see Algorithm 1 of [Mat93]).

The probability of a linear approximation on $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ with input mask $\boldsymbol{a} \in \mathbb{F}_2^n$ and output mask $\boldsymbol{b} \in \mathbb{F}_2^m$ is equal to

$$\mathsf{Pr}[\boldsymbol{a} \cdot x = \boldsymbol{b} \cdot S(x)] = 2^{-n} \cdot |\{\boldsymbol{v} \in \mathbb{F}_2^n : \boldsymbol{a} \cdot \boldsymbol{v} = \boldsymbol{b} \cdot S(\boldsymbol{v})\}|.$$

and we refer to the value $\mathsf{Pr}[\boldsymbol{a} \cdot x = \boldsymbol{b} \cdot S(x)] - 1/2$ as the *bias* of the linear approximation. If n, m are relatively small, we can enumerate the bias of all possible linear approximations on S and store the corresponding numerator in a $2^n \times 2^m$ *linear approximation table* of S. The entry at row $\boldsymbol{a} \in \mathbb{F}_2^n$ and column $\boldsymbol{b} \in \mathbb{F}_2^m$ of the linear approximation table of S is defined as

$$\lambda_S(\boldsymbol{a}, \boldsymbol{b}) = |\{(\boldsymbol{v} \parallel S(\boldsymbol{v})) \in \mathbb{F}_2^{n+m} : \boldsymbol{a} \cdot \boldsymbol{v} = \boldsymbol{b} \cdot S(\boldsymbol{v})\}| - 2^{n-1}.$$

An example of a linear approximation table is provided in Table 21.

Definition 8.8 (Linear ideal)**.** *Let* $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ *and let* $\mathcal{R}$ *be the polynomial ring* $\mathbb{F}_2[x_1, \ldots, x_n, y_1, \ldots, y_m]$. *For any* $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{F}_2^n, \boldsymbol{b} = (b_1, \ldots, b_m) \in \mathbb{F}_2^m$ *we define the linear ideal* $\lambda I_S(\boldsymbol{a}, \boldsymbol{b}) \subseteq \mathcal{R}$ *of* S *with input mask* $\boldsymbol{a}$ *and output mask* $\boldsymbol{b}$ *as*

$$\lambda I_S(\boldsymbol{a}, \boldsymbol{b}) = \left\langle F_S, \sum_{i=1}^{n} a_i x_i + \sum_{j=1}^{m} b_j y_j, \mathsf{FP}(\mathcal{R}) \right\rangle$$

where $F_S \subset \mathcal{R}$ *is the algebraic normal form of* S.

Theorem 8.9. *Let* $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ *and* $\mathcal{R} = \mathbb{F}_2[x_1, \ldots, x_n, y_1, \ldots, y_m]$. *The bias of a linear approximation on* S *with input mask* $\boldsymbol{a} \in \mathbb{F}_2^n$ *and output mask* $\boldsymbol{b} \in \mathbb{F}_2^m$ *is equal to*

$$2^{-n} \cdot (\dim_{\mathbb{F}_2}(\mathcal{R}/\lambda I_S(\boldsymbol{a}, \boldsymbol{b})) - 2^{n-1}).$$

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	2	-2	-2	-2	4	-	-	-	2	-2	2	2	-	4
2	-	-	-2	-2	-	-	2	2	2	-2	-	4	2	-2	4	-
3	-	4	-	-	2	-2	2	2	2	2	2	-2	-	-	-	-4
4	-	-	2	-2	2	2	-	4	-	-	-2	2	2	2	-4	-
5	-	-	-	-	-	-	-	-	-	-	4	4	-4	4	-	-
6	-	-	-	4	-2	-2	-2	2	-2	2	2	2	4	-	-	-
7	-	4	-2	2	-	4	2	-2	-2	-2	-	-	2	2	-	-
8	-	2	-	2	-	2	-	2	2	-	2	-	-2	-4	-2	4
9	-	-2	-2	-	-2	4	-	2	2	4	-	-2	-	2	2	-
A	-	2	-2	-	4	-2	-2	-	-	2	-2	-	-	2	2	4
B	-	2	4	2	-2	-	2	-	-	2	-4	2	-2	-	2	-
C	-	-2	2	4	2	-	-	2	2	-4	-	-2	-	2	2	-
D	-	2	4	-2	-	2	-4	-2	2	-	2	-	2	-	2	-
E	-	-2	-	2	2	-	2	-4	4	2	-	2	2	-	-2	-
F	-	-2	2	-	4	2	2	-	-4	2	2	-	-	-2	2	-

Table 21: *Linear approximation table of S defined in Table 20. The entries denoted by '-' are equal to zero.*

Proof. Let $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ and $\boldsymbol{b} = (b_1, \ldots, b_m) \in \mathbb{F}_2^m$. Suppose that the system of equations $F = F_S \cup \{\sum_{i=1}^n a_i x_i + \sum_{j=1}^m b_j y_j\} \cup \mathsf{FP}(\mathcal{R})$ has a solution in $\mathbb{F}_2^{n+m}$. We claim that

$$\mathbf{V}_{\mathbb{F}_2}(\lambda I_S(\boldsymbol{a}, \boldsymbol{b})) = \{(\boldsymbol{v} \parallel \boldsymbol{w}) \in \mathbb{F}_2^{n+m} : \boldsymbol{v} \in \mathbb{F}_2^n, \boldsymbol{w} = S(\boldsymbol{v}) \text{ and } \sum_{i=1}^n a_i v_i + \sum_{j=1}^m b_j w_j = 0\}.$$

Let $\boldsymbol{u} = (u_1, u_2, \ldots, u_{n+m}) \in \mathbf{V}_{\mathbb{F}_2}(\lambda I_S(\boldsymbol{a}, \boldsymbol{b}))$. Since $\mathbf{V}_{\mathbb{F}_2}(\lambda I_S(\boldsymbol{a}, \boldsymbol{b})) = \mathbf{V}_{\mathbb{F}_2}(F)$, then $f(\boldsymbol{u}) = 0$ for all $f \in F$. This implies that $(u_{n+1}, \ldots, u_{n+m}) = S(u_1, \ldots, u_n)$ (by the definition of F_S) and $\sum_{i=1}^n a_i u_i + \sum_{j=1}^m b_j u_{n+j} = 0$. The converse inclusion is obvious since the condition $\boldsymbol{w} = S(\boldsymbol{v})$ implies $f(\boldsymbol{v} \parallel \boldsymbol{w}) = 0$ for all $f \in F_S$ and clearly $(\boldsymbol{v} \parallel \boldsymbol{w})$ is a solution for the polynomial $\sum_{i=1}^n a_i x_i + \sum_{j=1}^m b_j y_j$. Thus, $(\boldsymbol{v} \parallel \boldsymbol{w}) \in \mathbf{V}_{\mathbb{F}_2}(F) = \mathbf{V}_{\mathbb{F}_2}(\lambda I_S(\boldsymbol{a}, \boldsymbol{b}))$.

Since $\mathsf{FP}(\mathcal{R}) \subset \lambda I_S(\boldsymbol{a}, \boldsymbol{b})$, by 1) and 2) of Proposition 8.5, the ideal $\lambda I_S(\boldsymbol{a}, \boldsymbol{b})$ is zero-dimensional and radical. We then have the following relation

$$|\mathbf{V}_{\overline{\mathbb{F}_2}}(\lambda I_S(\boldsymbol{a}, \boldsymbol{b}))| = \dim_{\mathbb{F}_2}(\mathcal{R}/\lambda I_S(\boldsymbol{a}, \boldsymbol{b})) = |\mathbf{V}_{\mathbb{F}_2}(\lambda I_S(\boldsymbol{a}, \boldsymbol{b}))|.$$

where the first equality is implied by Proposition 8.3 and the second equality is implied by 3) of Proposition 8.5. Therefore we have

$$\lambda_S(\boldsymbol{a}, \boldsymbol{b}) = \dim_{\mathbb{F}_2}(\mathcal{R}/\lambda I_S(\boldsymbol{a}, \boldsymbol{b})) - 2^{n-1} \tag{8.1}$$

and the bias of the linear approximation is equal to $2^{-n} \cdot (\dim_{\mathbb{F}_2}(\mathcal{R}/\lambda I_S(\boldsymbol{a}, \boldsymbol{b})) - 2^{n-1})$. ∎

In the following lemma, for a given $\boldsymbol{a} \in \mathbb{F}_2^n$, we denote by $\ell_{\boldsymbol{a}}$ the n-variable Boolean function $\ell_{\boldsymbol{a}}(x) = \boldsymbol{a} \cdot x$ and for any n-variable Boolean functions f, g we define $d(f, g) = |\{\boldsymbol{x} \in \mathbb{F}_2^n : f(\boldsymbol{x}) \neq g(\boldsymbol{x})\}|$ to be the *Hamming distance* of f and g.

Lemma 8.10. *Let $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$. We have the following equality*

$$\mathcal{W}_{S_{\boldsymbol{b}}}(\boldsymbol{a}) = 2^n - 2 \cdot d(S_{\boldsymbol{b}}, \ell_{\boldsymbol{a}}).$$

Proof. Recall that $\mathcal{W}_{S_{\boldsymbol{b}}}(\boldsymbol{a}) = \sum_{\boldsymbol{x}\in\mathbb{F}_2^n}(-1)^{\widehat{S_{\boldsymbol{b}}}(\boldsymbol{x})}(-1)^{\widehat{\ell_{\boldsymbol{a}}}(\boldsymbol{x})}$. For any $\boldsymbol{x} \in \mathbb{F}_2^n$ such that $S_{\boldsymbol{b}}(\boldsymbol{x}) = \ell_{\boldsymbol{a}}(\boldsymbol{x})$ we have $(-1)^{\widehat{S_{\boldsymbol{b}}}(\boldsymbol{x})}(-1)^{\widehat{\ell_{\boldsymbol{a}}}(\boldsymbol{x})} = 1$ and -1 otherwise. The number of -1 in the summation is equal to $|\{\boldsymbol{x} \in \mathbb{F}_2^n : S_{\boldsymbol{b}}(\boldsymbol{x}) \neq \ell_{\boldsymbol{a}}(\boldsymbol{x})\}| = d(S_{\boldsymbol{b}}, \ell_{\boldsymbol{a}})$. On the other hand, the number of $+1$ in the summation is equal to $2^n - d(S_{\boldsymbol{b}}, \ell_{\boldsymbol{a}})$. Therefore $\mathcal{W}_{S_{\boldsymbol{b}}}(\boldsymbol{a}) = 2^n - 2 \cdot d(S_{\boldsymbol{b}}, \ell_{\boldsymbol{a}})$. ■

Theorem 8.11. *Let $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and $\mathcal{R} = \mathbb{F}_2[x_1, \ldots, x_n, y_1, \ldots, y_m]$. For any $\boldsymbol{b} \in \mathbb{F}_2^m$, we have the following*

$$\mathcal{W}_{S_{\boldsymbol{b}}}(\boldsymbol{a}) = 2 \cdot \dim_{\mathbb{F}_2}(\mathcal{R}/\lambda I_S(\boldsymbol{a}, \boldsymbol{b})) - 2^n, \tag{8.2}$$

$$\mathcal{F}_{S_{\boldsymbol{b}}}(\boldsymbol{a}) = 2^{n-1}(\delta(\boldsymbol{a}) + 1) - \dim_{\mathbb{F}_2}(\mathcal{R}/\lambda I_S(\boldsymbol{a}, \boldsymbol{b})) \tag{8.3}$$

where $\delta(\boldsymbol{a}) = 1$ if $\boldsymbol{a} = \boldsymbol{0}$ and 0 otherwise.

Proof. By the definition of $\lambda_S(\boldsymbol{a}, \boldsymbol{b})$, we can express it as

$$\begin{aligned}\lambda_S(\boldsymbol{a}, \boldsymbol{b}) &= |\{(\boldsymbol{v} \parallel S(\boldsymbol{v})) \in \mathbb{F}_2^{n+m} : \boldsymbol{a} \cdot \boldsymbol{v} = \boldsymbol{b} \cdot S(\boldsymbol{v})\}| - 2^{n-1} \\ &= 2^n - d(S_{\boldsymbol{b}}, \ell_{\boldsymbol{a}}) - 2^{n-1} \\ &= 2^{n-1} - d(S_{\boldsymbol{b}}, \ell_{\boldsymbol{a}})\end{aligned}$$

and by Lemma 8.10 we have $\mathcal{W}_{S_{\boldsymbol{b}}}(\boldsymbol{a}) = 2 \cdot \lambda_S(\boldsymbol{a}, \boldsymbol{b})$. From this, the proof of (8.2) is immediate from (8.1), i.e.,

$$\mathcal{W}_{S_{\boldsymbol{b}}}(\boldsymbol{a}) = 2 \cdot \lambda_S(\boldsymbol{a}, \boldsymbol{b}) = 2 \cdot \dim_{\mathbb{F}_2}(\mathcal{R}/\lambda I_S(\boldsymbol{a}, \boldsymbol{b})) - 2^n.$$

The proof of (8.3) is a straightforward implication of Proposition 8.7 and (8.2). ■

Input: A vectorial Boolean function $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$
Input: An input mask $\boldsymbol{a} \in \mathbb{F}_2^n$
Input: An output mask $\boldsymbol{b} \in \mathbb{F}_2^m$
Output: The bias of the linear approximation $\boldsymbol{a} \cdot x = \boldsymbol{b} \cdot S(x)$.
1 $\mathcal{R} \leftarrow \mathbb{F}_2[x_1, \ldots, x_n, y_1, \ldots, y_m]$
2 $F_S \leftarrow$ Algebraic Normal Form of S
3 $\lambda I_S(\boldsymbol{a}, \boldsymbol{b}) \leftarrow \langle F_S, \sum_{i=1}^n a_i x_i + \sum_{j=1}^m b_j y_j, \mathsf{FP}(\mathcal{R})\rangle$
4 $G \leftarrow$ GröbnerBasis($\lambda I_S(\boldsymbol{a}, \boldsymbol{b})$)
5 $\mathsf{RM}(\lambda I_S(\boldsymbol{a}, \boldsymbol{b})) \leftarrow$ ReducedMonomials(G)
6 **return** $2^{-n} \cdot (|\mathsf{RM}(\lambda I_S(\boldsymbol{a}, \boldsymbol{b}))| - 2^{n-1})$

Algorithm 8.2: An algorithm to compute the bias of a linear approximation on S using a Gröbner bases algorithm.

Theorem 8.12. *Given $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$, $\boldsymbol{a} \in \mathbb{F}_2^n$ and $\boldsymbol{b} \in \mathbb{F}_2^m$, Algorithm 8.2 computes the bias of a linear approximation on S with input mask $\boldsymbol{a}$ and output mask $\boldsymbol{b}$.*

Proof. Termination: Since each step in line 1-4 terminates, then eventually the algorithm terminates.*

* The termination of a Gröbner bases algorithm is due to the Noetherianity of $\mathcal{R}$ (see for example the proof of Theorem 2 in [CLO15, pg. 91]) and the termination of ReducedMonomials is due to the fact that the ideal $\lambda I_S(\boldsymbol{a}, \boldsymbol{b})$ is zero-dimensional (see Proposition 8.1 and 4) of Proposition 3.46).

Correctness: By Proposition 8.2, the set $\{\mathfrak{m} + \lambda I_S(\boldsymbol{a}, \boldsymbol{b}) : \mathfrak{m} \in \mathsf{RM}(\lambda I_S(\boldsymbol{a}, \boldsymbol{b}))\}$ is a basis of the $\mathbb{F}_2$-vector space $\mathcal{R}/\lambda I_S(\boldsymbol{a}, \boldsymbol{b})$. It follows from Theorem 8.9, that the bias of the linear approximation $\boldsymbol{a} \cdot x = \boldsymbol{b} \cdot S(x)$ is equal to $2^{-n} \cdot (|\mathsf{RM}(\lambda I_S(\boldsymbol{a}, \boldsymbol{b}))| - 2^{n-1})$. ■

Example 8.13. *Let S be the mapping defined in Table 20. Let $\boldsymbol{a} = \boldsymbol{F} = (1,1,1,1), \boldsymbol{b} = \boldsymbol{\mathcal{S}} = (0,0,0,1)$ and $I = \lambda I_S(\boldsymbol{a}, \boldsymbol{b})$. The reduced Gröbner basis of the ideal I w.r.t. degree-reverse lexicographic ordering consists of the following polynomials*

$$\begin{array}{lll} y_1^2 + y_1, & y_2y_4 + y_2, & x_3 + y_1 + y_2 + y_4, \\ y_1y_2, & y_4^2 + y_4, & x_4 + y_1 + y_4, \\ y_2^2 + y_2, & x_1, & y_3 + y_4, \\ y_1y_4, & x_2 + y_2 + y_4. & \end{array}$$

The basis of the $\mathbb{F}_2$-vector space $\mathcal{R}/I$ is the following

$$\{y_4 + I, y_2 + I, y_1 + I, 1 + I\}.$$

Therefore $\lambda_S(\boldsymbol{F}, \boldsymbol{\mathcal{S}}) = \dim_{\mathbb{F}_2}(\mathcal{R}/I) - 2^3 = -4$ (see also Table 21).

8.3 Multivariate Ideals and Differential Property

In this section we present relations between ideals in multivariate polynomial ring and properties of vectorial Boolean functions that are relevant for *differential cryptanalysis*. Differential cryptanalysis is one class of attacks applicable to wide-range of symmetric-key primitives, particularly block ciphers and hash functions. The attack studies how a difference in two inputs to a vectorial Boolean function affects differences of their corresponding outputs. The common difference operation is bitwise exclusive-or (XOR) operation, which corresponds to vector addition in $\mathbb{F}_2^n$. This is also the difference operation considered throughout this chapter.

Let $\boldsymbol{\alpha} \in \mathbb{F}_2^n, \boldsymbol{\beta} \in \mathbb{F}_2^m$ be differences in the input and output of $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ respectively. We refer to the pair $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ as a *differential* of S and its probability is defined as

$$\mathsf{Pr}[\boldsymbol{\alpha} \xrightarrow{S} \boldsymbol{\beta}] = \frac{|\{\boldsymbol{v} \in \mathbb{F}_2^n : S(\boldsymbol{v} + \boldsymbol{\alpha}) + S(\boldsymbol{v}) = \boldsymbol{\beta}\}|}{2^n} = \frac{\delta_S(\boldsymbol{\alpha}, \boldsymbol{\beta})}{2^n}.$$

Note that for small n, m, the values $(\delta_S(\boldsymbol{\alpha}, \boldsymbol{\beta}))_{\boldsymbol{\alpha} \in \mathbb{F}_2^n, \boldsymbol{\beta} \in \mathbb{F}_2^m}$ are typically stored in a two-dimensional array called the *difference distribution table* of S. An example of a difference distribution table is provided in Table 22. Another relevant parameter to determine the resistance of a vectorial Boolean function against differential cryptanalysis is *differential uniformity* [Nyb93].

Definition 8.14. *Let $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$. The function S has differential uniformity equal to δ_S if*

$$\delta_S = \max_{0 \neq \boldsymbol{\alpha} \in \mathbb{F}_2^n, \boldsymbol{\beta} \in \mathbb{F}_2^m} \delta_S(\boldsymbol{\alpha}, \boldsymbol{\beta}).$$

In order to study the properties relevant for differential cryptanalysis, we first need to construct the required polynomial ring. Recall that in differential cryptanalysis, we consider two inputs to a vectorial Boolean function $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$. Let $x'_1, \ldots, x'_n$ and $x''_1, \ldots, x''_n$ be two sets of variables that represent two

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
1	–	–	–	4	–	–	2	2	–	–	–	4	2	2	–	–
2	–	–	–	–	–	2	–	2	–	2	–	2	2	2	2	2
3	–	–	2	–	2	2	2	–	2	–	2	2	2	–	–	–
4	–	–	–	–	–	2	2	–	–	4	4	–	2	–	–	2
5	–	2	2	–	–	2	–	2	–	2	2	–	2	–	2	–
6	–	–	4	2	–	2	2	2	2	–	–	–	–	–	–	2
7	–	2	–	2	2	2	–	–	–	–	–	–	2	–	4	2
8	–	–	–	2	–	–	–	2	–	–	2	–	2	2	4	2
9	–	4	–	–	2	–	–	2	2	–	–	2	–	4	–	–
A	–	4	–	2	–	2	–	–	–	2	2	2	–	–	2	–
B	–	–	2	–	–	2	4	–	4	–	2	–	–	2	–	–
C	–	2	–	2	2	–	4	2	2	2	–	–	–	–	–	–
D	–	–	2	–	4	–	–	2	–	–	–	2	–	4	2	–
E	–	2	–	–	2	–	–	–	4	2	–	–	2	–	–	4
F	–	–	4	2	2	–	–	–	–	2	2	2	–	–	–	2

Table 22: *Difference distribution table of S defined in Table 20. The entries denoted by '–' are equal to zero.*

inputs to S. Their respective output are denoted by variables $y'_1, \ldots, y'_m$ and $y''_1, \ldots, y''_m$. Thus, for notions related to differential cryptanalysis, we will use the following ring

$$\mathcal{R} = \mathbb{F}_2[x'_1, \ldots, x'_n, y'_1, \ldots, y'_m, x''_1, \ldots, x''_n, y''_1, \ldots, y''_m]. \tag{8.4}$$

However, we stress that the results of this chapter are independent from the choice of variable ordering and the monomial ordering in $\mathcal{R}$.

Definition 8.15 (Differential ideal)**.** *Let $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and let $\mathcal{R}$ be a polynomial ring defined in* (8.4)*. For any $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_2^n, \boldsymbol{\beta} = (\beta_1, \ldots, \beta_m) \in \mathbb{F}_2^m$ we define the differential ideal $\delta I_S(\boldsymbol{\alpha}, \boldsymbol{\beta}) \subseteq \mathcal{R}$ of S w.r.t. the differential $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ as*

$$\delta I_S(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \langle F'_S, F''_S, \{x'_i + x''_i + \alpha_i \ : 1 \le i \le n\}, \\ \{y'_j + y''_j + \beta_j : 1 \le j \le m\}, \mathsf{FP}(\mathcal{R})\rangle$$

where F'_S and F''_S are the sets of polynomials that represent S in variables x'_i, y'_j and x''_i, y''_j respectively.

Theorem 8.16. *Let $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and let $\mathcal{R}$ be a polynomial ring defined in* (8.4)*. The probability of a differential $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ is equal to*

$$\mathsf{Pr}[\boldsymbol{\alpha} \xrightarrow{S} \boldsymbol{\beta}] = \frac{\dim_{\mathbb{F}_2}(\mathcal{R}/\delta I_S(\boldsymbol{\alpha}, \boldsymbol{\beta}))}{2^n}.$$

Proof. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_2^n$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_m) \in \mathbb{F}_2^m$. Suppose that the following system of equations

$$F = F'_S \cup F''_S \cup \{x'_i + x''_i + \alpha_i : 1 \le i \le n\} \cup \{y'_j + y''_j + \beta_j : 1 \le j \le m\} \cup \mathsf{FP}(\mathcal{R})$$

has a solution in $\mathbb{F}_2^{2(n+m)}$. Let $\Delta_S(\boldsymbol{\alpha}, \boldsymbol{\beta})$ be the following set

$$\Delta_S(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \{(\boldsymbol{v} \parallel S(\boldsymbol{v}) \parallel \boldsymbol{v} + \boldsymbol{\alpha} \parallel S(\boldsymbol{v} + \boldsymbol{\alpha})) : \boldsymbol{v} \in \mathbb{F}_2^n, S(\boldsymbol{v} + \boldsymbol{\alpha}) + S(\boldsymbol{v}) = \boldsymbol{\beta}\}.$$

We will first show that $\mathbf{V}_{\mathbb{F}_2}(\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta})) = \Delta_S(\boldsymbol{\alpha},\boldsymbol{\beta})$.

Let $\boldsymbol{u} = (u_1,\ldots,u_{2(n+m)}) \in \mathbf{V}_{\mathbb{F}_2}(\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta}))$. Since $\mathbf{V}_{\mathbb{F}_2}(\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta})) = \mathbf{V}_{\mathbb{F}_2}(F)$ then $f(\boldsymbol{u}) = 0$ for all $f \in F$. Thus, $(u_{n+1},\ldots,u_{n+m}) = S(u_1,\ldots,u_n)$ by the definition of F'_S, $(u_{n+m+1},\ldots,u_{2n+m}) = (u_1+\alpha_1,\ldots,u_n+\alpha_n)$ due to $u_i + u_{n+m+i} + \alpha_i = 0$ for $1 \le i \le n$, and $(u_{2n+m+1},\ldots,u_{2(n+m)}) = S(u_{n+m+1},\ldots,u_{2n+m})$ by the definition of F''_S such that $u_{n+j}+u_{2n+m+j}+\beta_j = 0$ for $1 \le j \le m$. Conversely, let $(\boldsymbol{v} \parallel S(\boldsymbol{v}) \parallel \boldsymbol{v}+\boldsymbol{\alpha} \parallel S(\boldsymbol{v}+\boldsymbol{\alpha})) \in \Delta_S(\boldsymbol{\alpha},\boldsymbol{\beta})$ where $\boldsymbol{v} \in \mathbb{F}_2^n$. Clearly $f'(\boldsymbol{v} \parallel S(\boldsymbol{v})) = 0$ for all $f' \in F'_S$ and $f''(\boldsymbol{v}+\boldsymbol{\alpha} \parallel S(\boldsymbol{v}+\boldsymbol{\alpha})) = 0$ for all $f'' \in F''_S$. Similarly, $(\boldsymbol{v} \parallel \boldsymbol{v}+\boldsymbol{\alpha})$ is a solution of $x'_i + x''_i + \alpha_i$ for $1 \le i \le n$ and $(S(\boldsymbol{v}) \parallel S(\boldsymbol{v}+\boldsymbol{\alpha}))$ is also a solution for $y'_j + y''_j + \beta_j = 0$ for $1 \le j \le m$ by the condition $S(\boldsymbol{v}+\boldsymbol{\alpha}) + S(\boldsymbol{v}) = \boldsymbol{\beta}$. Thus $(\boldsymbol{v} \parallel S(\boldsymbol{v}) \parallel \boldsymbol{v}+\boldsymbol{\alpha} \parallel S(\boldsymbol{v}+\boldsymbol{\alpha})) \in \mathbf{V}_{\mathbb{F}_2}(F) = \mathbf{V}_{\mathbb{F}_2}(\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta}))$.

Since $\mathsf{FP}(\mathcal{R}) \subset \delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta})$, by 1) and 2) of Proposition 8.5, the ideal $\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta})$ is zero-dimensional and radical. We then have the following relation

$$|\mathbf{V}_{\overline{\mathbb{F}_2}}(\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta}))| = \dim_{\mathbb{F}_2}(\mathcal{R}/\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta})) = |\mathbf{V}_{\mathbb{F}_2}(\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta}))|$$

where the first equality is an implication of Proposition 8.3 and the second equality is an implication of 3) in Proposition 8.5. Since it is trivial to see that $\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta}) = |\Delta_S(\boldsymbol{\alpha},\boldsymbol{\beta})|$, therefore we have the following

$$\delta_S(\boldsymbol{\alpha},\boldsymbol{\beta}) = \dim_{\mathbb{F}_2}(\mathcal{R}/\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta})). \tag{8.5}$$

■

Remark 8.17. *From* (8.5) *and Definition 8.14, computing the differential uniformity of S is equivalent to finding an $\mathbb{F}_2$-vector space $\mathcal{R}/\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta})$, for $\boldsymbol{0} \neq \boldsymbol{\alpha} \in \mathbb{F}_2^n$ and $\boldsymbol{\beta} \in \mathbb{F}_2^m$, of maximum dimension.*

In the following, we shall apply the result from Theorem 8.16 to compute the probability of a differential using a Gröbner basis algorithm.

Theorem 8.18. *Given $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and a differential $(\boldsymbol{\alpha},\boldsymbol{\beta}) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$, Algorithm 8.3 computes the differential probability of $(\boldsymbol{\alpha},\boldsymbol{\beta})$.*

Input: A vectorial Boolean function $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$
Input: A differential $(\boldsymbol{\alpha},\boldsymbol{\beta}) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$
Output: The probability $\mathsf{Pr}[\boldsymbol{\alpha} \to^S \boldsymbol{\beta}]$
1 $\mathcal{R} \leftarrow \mathbb{F}_2[x'_1,\ldots,x'_n,y'_1,\ldots,y'_m,x''_1,\ldots,x''_n,y''_1,\ldots,y''_m]$
2 $F'_S \leftarrow$ Algebraic Normal Form of S in $x'_1,\ldots,x'_n,y'_1,\ldots,y'_m$
3 $F''_S \leftarrow$ Algebraic Normal Form of S in $x''_1,\ldots,x''_n,y''_1,\ldots,y''_m$
4 $A \leftarrow \{x'_i + x''_i + \alpha_i : 1 \le i \le n\}$
5 $B \leftarrow \{y'_j + y''_j + \beta_j : 1 \le j \le m\}$
6 $\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta}) \leftarrow \langle F'_S, F''_S, A, B, \mathsf{FP}(\mathcal{R})\rangle$
7 $G \leftarrow$ GröbnerBasis($\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta})$)
8 $\mathsf{RM}(\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta})) \leftarrow$ ReducedMonomials(G)
9 **return** $|\mathsf{RM}(\delta I_S(\boldsymbol{\alpha},\boldsymbol{\beta}))|/2^n$

Algorithm 8.3: An algorithm to compute the probability of a differential on S using a Gröbner bases algorithm.

Proof. Termination : The termination of the above algorithm is obvious since the computation of algebraic normal form of S, Gröbner basis of $\delta I_S(\boldsymbol{\alpha}, \boldsymbol{\beta})$, and the ReducedMonomials terminates where the latter is due to the ideal $\delta I_S(\boldsymbol{\alpha}, \boldsymbol{\beta})$ being a zero-dimensional.
Correctness : By Proposition 8.2, the set $\{\mathfrak{m} + \delta I_S(\boldsymbol{\alpha}, \boldsymbol{\beta}) : \mathfrak{m} \in \mathsf{RM}(\delta I_S(\boldsymbol{\alpha}, \boldsymbol{\beta}))\}$ is a basis of the $\mathbb{F}_2$-vector space $\mathcal{R}/\delta I_S(\boldsymbol{\alpha}, \boldsymbol{\beta})$ and clearly by Theorem 8.16, $\mathsf{Pr}[\boldsymbol{\alpha} \xrightarrow{S} \boldsymbol{\beta}] = |\mathsf{RM}(\delta I_S(\boldsymbol{\alpha}, \boldsymbol{\beta}))|/2^n$. ■

Example 8.19. *Let S be the mapping defined in Table 20. Let $\boldsymbol{\alpha} = \boldsymbol{6} = (0,1,1,0) \in \mathbb{F}_2^4, \boldsymbol{\beta} = \boldsymbol{2} = (0,1,0,0) \in \mathbb{F}_2^4$ and let $I = \delta I_S(\boldsymbol{\alpha}, \boldsymbol{\beta}) \subset \mathcal{R}$ where $\mathcal{R}$ is a polynomial ring defined in* (8.4) *with $n = m = 4$. The reduced Gröbner basis of I w.r.t. degree-reverse lexicographic ordering consists of the following polynomials*

$$
\begin{array}{llll}
y_2''^2 + y_2'', & x_3' + y_2'' + y_3'' + 1, & y_3' + y_3'', & x_3'' + y_2'' + y_3'', \\
y_3''^2 + y_3'', & x_4' + y_3'', & y_4' + 1, & x_4'' + y_3'', \\
x_1' + y_3'' + 1, & y_1', & x_1'' + y_3'' + 1, & y_1'', \\
x_2' + y_2'', & y_2' + y_2'' + 1, & x_2'' + y_2'' + 1, & y_4'' + 1.
\end{array}
$$

The basis of the $\mathbb{F}_2$-vector space $\mathcal{R}/I$ consists of the following elements

$$1 + I, y_2'' + I, y_3'' + I, y_2'' y_3'' + I.$$

Therefore $\delta_S(\boldsymbol{6}, \boldsymbol{2}) = \dim_{\mathbb{F}_2}(\mathcal{R}/I) = 4$ (see also Table 22).

8.4 Multivariate Ideals and Autocorrelation

In this section we shall describe the relation of autocorrelation of vectorial Boolean functions and ideals in multivariate polynomial ring. The notion of autocorrelation is related to the derivative of Boolean functions. The derivative of an n-variable Boolean function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ with respect to $\boldsymbol{\alpha} \in \mathbb{F}_2^n$ is the Boolean function $D_{\boldsymbol{\alpha}} f(x) = f(x + \boldsymbol{\alpha}) + f(x)$.

Definition 8.20 (Autocorrelation)**.** *Let $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$. The autocorrelation of a component function $S_{\boldsymbol{b}}$ at $\boldsymbol{\alpha}$ is defined as*

$$\tau_S(\boldsymbol{\alpha}, \boldsymbol{b}) = \sum_{\boldsymbol{v} \in \mathbb{F}_2^n} (-1)^{\widehat{D_{\boldsymbol{\alpha}} S_{\boldsymbol{b}}}(\boldsymbol{v})}.$$

If n and m are relatively small, it is possible to exhaustively compute $\tau_S(\boldsymbol{\alpha}, \boldsymbol{b})$ for all $\boldsymbol{\alpha} \in \mathbb{F}_2^n, \boldsymbol{b} \in \mathbb{F}_2^m$. We refer to $(\tau_S(\boldsymbol{\alpha}, \boldsymbol{b}))_{\boldsymbol{\alpha} \in \mathbb{F}_2^n, \boldsymbol{b} \in \mathbb{F}_2^m}$ as the *autocorrelation table* of S. An example of autocorrelation table is provided in Table 23.

The work in [CKL+19] demonstrates that autocorrelation is closely related to the differential-linear cryptanalysis [LH94]. For instance, the notion of *differential-linear connectivity table* (DLCT) introduced in [BDKW19] to examine the differential-linear property of S-Boxes, coincides with the autocorrelation table. Other related cryptographic weaknesses is the notion of *linear structures* which we will describe in Subsection 8.4.1.

We will now present the construction of an ideal that corresponds to the autocorrelation of a component function of S.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	-8	-8	8	-	-8	-8	8	-	-	-8	-	-	-	8	-
2	16	-8	-	-	-8	-	-	-	-8	-	-	-	-	8	-	-
3	16	8	-	-	-	-	-8	-	-	-	-	-8	-8	-	-	-
4	16	-	-	-8	-	-	-	-8	-8	-	-	-	-8	-	-	16
5	16	-	-	-8	-	-	-	-8	-	-8	-	-	-	8	-	-
6	16	-	-8	-	-	8	-	-	8	-	-8	-8	-	-	-8	-
7	16	-	-	-	-8	-8	-	-	-	-8	8	-	8	-	-8	-
8	16	-	-8	-	-8	-	-	-	-8	-8	-	8	8	-	-	-
9	16	-8	8	-	-	-	-	-	-	-	-	-	-	-8	8	-16
A	16	-8	-	-8	8	-8	-	-	-	-8	8	-	-	-	-	-
B	16	8	-	-8	-	8	-	8	-	-	-8	-8	-8	-8	-	-
C	16	-	-	-	-	-8	8	-	8	-	-8	-	-8	-8	-	-
D	16	-	-	-	-8	-	-8	-	-	8	-	8	-	-	-	-16
E	16	-	8	8	-	-	8	-8	-8	-	-	-8	-	-8	-8	-
F	16	-	-8	-	8	-	-8	-8	-	8	-	-	-	-	-8	-

Table 23: *Autocorrelation table of S defined in Table 20. The entries denoted by '-' are equal to zero.*

Definition 8.21 (Autocorrelation ideal)**.** *Let $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and let $\mathcal{R}$ be a polynomial ring defined in* (8.4)*. For any $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_2^n$ and $\boldsymbol{b} = (b_1, \ldots, b_m) \in \mathbb{F}_2^m$ we define the autocorrelation ideal $\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}) \subseteq \mathcal{R}$ of S with input difference $\boldsymbol{\alpha}$ and output mask $\boldsymbol{b}$ as*

$$\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}) = \langle F'_S, F''_S, \{x'_i + x''_i + \alpha_i : 1 \le i \le n\}, \sum_{j=1}^{m} b_j(y'_j + y''_j) + 1, \mathsf{FP}(\mathcal{R})\}\rangle.$$

where F'_S and F''_S are the set of polynomials that represent S in variables x'_i, y'_j and x''_i, y''_j respectively.

Theorem 8.22. *Let $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and let $\mathcal{R}$ be a polynomial ring defined in* (8.4)*. The autocorrelation of a component function $S_{\boldsymbol{b}}$ at $\boldsymbol{\alpha}$ is equal to*

$$\tau_S(\boldsymbol{\alpha}, \boldsymbol{b}) = 2^n - 2 \cdot \dim_{\mathbb{F}_2}(\mathcal{R}/\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b})).$$

Proof. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_2^n$ and $\boldsymbol{b} = (b_1, \ldots, b_m) \in \mathbb{F}_2^m$. Suppose that the following system of equations

$$F = F'_S \cup F''_S \cup \{x'_i + x''_i + \alpha_i : 1 \le i \le n\} \cup \{\textstyle\sum_{j=1}^{m} b_j(y'_j + y''_j) + 1\} \cup \mathsf{FP}(\mathcal{R})$$

has a solution in $\mathbb{F}_2^{2(n+m)}$. We first define the following set

$$\mathrm{T}_S(\boldsymbol{\alpha}, \boldsymbol{b}) = \{(\boldsymbol{v} \parallel S(\boldsymbol{v}) \parallel \boldsymbol{v} + \boldsymbol{\alpha} \parallel S(\boldsymbol{v} + \boldsymbol{\alpha})) : \boldsymbol{v} \in \mathbb{F}_2^n, S_{\boldsymbol{b}}(\boldsymbol{v} + \boldsymbol{\alpha}) + S_{\boldsymbol{b}}(\boldsymbol{v}) = 1\}$$

and we will show that $\mathbf{V}_{\mathbb{F}_2}(\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b})) = \mathrm{T}_S(\boldsymbol{\alpha}, \boldsymbol{b})$.

Let $\boldsymbol{u} = (u_1, \ldots, u_{2(n+m)}) \in \mathbf{V}_{\mathbb{F}_2}(\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}))$. Since $\mathbf{V}_{\mathbb{F}_2}(\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b})) = \mathbf{V}_{\mathbb{F}_2}(F)$, then $f(\boldsymbol{u}) = 0$ for all $f \in F$. Thus, $(u_{n+m+1}, \ldots, u_{2n+m}) = (u_1 + \alpha_1, \ldots, u_n + \alpha_n)$ by the polynomials in $\{x'_i + x''_i + \alpha_i : 1 \le i \le n\}$. Moreover, we have $(u_{n+1}, \ldots, u_{n+m}) = S(u_1, \ldots, u_n)$ and at the same time $(u_{2n+m+1}, \ldots u_{2(n+m)}) = S(u_{n+m+1}, \ldots, u_{2n+m})$ by the definition of F'_S, F''_S respectively such that

$$\sum_{j=1}^{m} b_j(u_{j+n} + u_{j+2n+m}) + 1 = S_{\boldsymbol{b}}(u_1, \ldots, u_n) + S(u_1 + \alpha_1, \ldots, u_n + \alpha_n) + 1 = 0.$$

Therefore, $\boldsymbol{u} \in \mathrm{T}_S(\boldsymbol{\alpha}, \boldsymbol{b})$. Conversely, let $(\boldsymbol{v} \parallel S(\boldsymbol{v}) \parallel \boldsymbol{v} + \boldsymbol{\alpha} \parallel S(\boldsymbol{v} + \boldsymbol{\alpha})) \in \mathrm{T}_S(\boldsymbol{\alpha}, \boldsymbol{b})$ where $\boldsymbol{v} \in \mathbb{F}_2^n$ and $S_{\boldsymbol{b}}(\boldsymbol{v}) + S_{\boldsymbol{b}}(\boldsymbol{v} + \boldsymbol{\alpha}) = 1$. Clearly $f'(\boldsymbol{v} \parallel S(\boldsymbol{v})) = 0$ for all $f' \in F'_S$ and $f''(\boldsymbol{v} + \boldsymbol{\alpha} \parallel S(\boldsymbol{v} + \boldsymbol{\alpha})) = 0$ for all $f'' \in F''_S$. Similarly, $(\boldsymbol{v} \parallel \boldsymbol{v} + \boldsymbol{\alpha})$ is a solution of $x'_i + x''_i + \alpha_i = 0$ for all $1 \leq i \leq n$ and the condition $S_{\boldsymbol{b}}(\boldsymbol{v}) + S_{\boldsymbol{b}}(\boldsymbol{v} + \boldsymbol{\alpha}) = 1$ implies that $(S(\boldsymbol{v}) \parallel S(\boldsymbol{v} + \boldsymbol{\alpha}))$ is a solution for $\sum_{j=1}^{m} b_j(y'_j + y''_j) + 1 = 0$. Thus $(\boldsymbol{v} \parallel S(\boldsymbol{v}) \parallel \boldsymbol{v} + \boldsymbol{\alpha} \parallel S(\boldsymbol{v} + \boldsymbol{\alpha})) \in \mathbf{V}_{\mathbb{F}_2}(F) = \mathbf{V}_{\mathbb{F}_2}(\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}))$.

Since $\mathsf{FP}(\mathcal{R}) \subseteq \tau I_S(\boldsymbol{\alpha}, \boldsymbol{b})$, by 1) and 2) of Proposition 8.5 the ideal $\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b})$ is zero-dimensional and radical. We then have the following relation

$$|\mathbf{V}_{\overline{\mathbb{F}_2}}(\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}))| = \dim_{\mathbb{F}_2}(\mathcal{R}/\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b})) = |\mathbf{V}_{\mathbb{F}_2}(\tau I_S(\boldsymbol{\alpha}, \boldsymbol{\beta}))|$$

where the first equality is an implication of Proposition 8.3 and the second equality is an implication of 3) in Proposition 8.5.

By the definition of Hamming weight, clearly $\mathsf{wt}(D_{\boldsymbol{\alpha}} S_{\boldsymbol{b}}) = |\mathbf{V}_{\mathbb{F}_2}(\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}))|$ and for any n-variable Boolean function f, $\sum_{\boldsymbol{v} \in \mathbb{F}_2^n} (-1)^{\widehat{f(\boldsymbol{v})}} = 2^n - 2 \cdot \mathsf{wt}(f)$ holds. Therefore

$$\tau_S(\boldsymbol{\alpha}, \boldsymbol{b}) = 2^n - 2 \cdot \mathsf{wt}(D_{\boldsymbol{\alpha}} S_{\boldsymbol{b}}) = 2^n - 2 \cdot \dim_{\mathbb{F}_2}(\mathcal{R}/\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}).$$

■

Theorem 8.23. *Given $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$, $\boldsymbol{\alpha} \in \mathbb{F}_2^n$, and $\boldsymbol{b} \in \mathbb{F}_2^m$, Algorithm 8.4 computes the autocorrelation $\tau_S(\boldsymbol{\alpha}, \boldsymbol{b})$.*

Input: A vectorial Boolean function $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$
Input: An input difference $\boldsymbol{\alpha} \in \mathbb{F}_2^n$
Input: An output mask $\boldsymbol{b} \in \mathbb{F}_2^m$
Output: The autocorrelation $\tau_S(\boldsymbol{\alpha}, \boldsymbol{b})$

1 $\mathcal{R} \leftarrow \mathbb{F}_2[x'_1, \ldots, x'_n, y'_1, \ldots, y'_m, x''_1, \ldots, x''_n, y''_1, \ldots, y''_m]$
2 $F'_S \leftarrow$ Algebraic Normal Form of S in $x'_1, \ldots, x'_n, y'_1, \ldots, y'_m$
3 $F''_S \leftarrow$ Algebraic Normal Form of S in $x''_1, \ldots, x''_n, y''_1, \ldots, y''_m$
4 $A \leftarrow \{x'_i + x''_i + \alpha_i : 1 \leq i \leq n\}$
5 $f \leftarrow \sum_{j=1}^{m} b_j(y'_j + y''_j) + 1$
6 $\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}) \leftarrow \langle F'_S, F''_S, A, f, \mathsf{FP}(\mathcal{R}) \rangle$
7 $G \leftarrow$ GröbnerBasis($\tau I_S(\boldsymbol{\alpha}, \boldsymbol{\beta})$)
8 $\mathsf{RM}(\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b})) \leftarrow$ ReducedMonomials(G)
9 **return** $2^n - 2 \cdot |\mathsf{RM}(\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}))|$

Algorithm 8.4: An algorithm to compute the autocorrelation $\tau_S(\boldsymbol{\alpha}, \boldsymbol{\beta})$ using a Gröbner bases algorithm.

Proof. Termination: Clearly Algorithm 8.4 terminates since the computation of the algebraic normal form of S, Gröbner basis, and the ReducedMonomials eventually terminate.
Correctness: By Proposition 8.2, $\{\mathfrak{m} + \tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}) : \mathfrak{m} \in \mathsf{RM}(\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}))\}$ is a basis of the $\mathbb{F}_2$-vector space $\mathcal{R}/\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b})$ and clearly by Theorem 8.22, $\tau_S(\boldsymbol{\alpha}, \boldsymbol{b}) = 2^n - 2 \cdot |\mathsf{RM}(\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b}))|$. ■

Example 8.24. *Let S be the mapping defined in Table 20. Let $\boldsymbol{\alpha} = \mathtt{5} = (1, 0, 1, 0) \in \mathbb{F}_2^4, \boldsymbol{b} = \mathtt{D} = (1, 0, 1, 1) \in \mathbb{F}_2^4$. The reduced Gröbner basis of the*

ideal $I = \tau I_S(\boldsymbol{\alpha}, \boldsymbol{b})$ *w.r.t. degree-reverse lexicographic ordering consists of the following polynomials*

$$
\begin{array}{lll}
y_1''^2 + y_1'', & x_1' + y_1'' + y_3'' + y_4'' + 1, & y_3' + y_3'', \\
y_1''y_3'' + y_1'', & x_2' + y_3'', & y_4' + y_3'' + y_4'' + 1, \\
y_3''^2 + y_3'', & x_3' + y_1'' + y_3'' + y_4'' + 1, & x_1'' + y_1'' + y_3'' + y_4'', \\
y_1''y_4'', & x_4', & x_2'' + y_3'', \\
y_3''y_4'', & y_1' + y_1'' + y_3'', & x_3'' + y_1'' + y_3'' + y_4'', \\
y_4''^2 + y_4'', & y_2' + y_3'' + y_4'' + 1, & \\
x_4'', & y_2'' + y_4'', &
\end{array}
$$

and the basis of the $\mathbb{F}_2$*-vector space* $\mathcal{R}/I$ *consists of the following elements*

$$y_4'' + I, y_3'' + I, y_1'' + I, 1 + I.$$

Therefore $\tau_S(\mathtt{5}, \mathtt{D}) = 2^4 - 2 \cdot \dim_{\mathbb{F}_2}(\mathcal{R}/I) = 8$ *(see also Table 23).*

8.4.1 Linear Structures and Ideal Membership Problem

One particular application of autocorrelation is to determine whether a vectorial Boolean function has a linear structure. The vector $\boldsymbol{\alpha}$ is a linear structure of an n-variable Boolean function f if $D_{\boldsymbol{\alpha}} f$ is a constant function. If the constant function $D_{\boldsymbol{\alpha}} f$ is equal to $c \in \mathbb{F}_2$, we say that $\boldsymbol{\alpha}$ is a c-linear structure of f. A Boolean function f is said to have a linear structure if there exists a nonzero $\boldsymbol{\alpha} \in \mathbb{F}_2^n$ such that $D_{\boldsymbol{\alpha}} f$ is a constant function [Eve87, Lai94]. This definition was generalized for the case of vectorial Boolean functions in [MS89b, pg. 4].

Definition 8.25. *A vectorial Boolean function* $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ *is said to have a linear structure if one of its nontrivial component function has a linear structure, i.e., there exists a nonzero* $\boldsymbol{b} \in \mathbb{F}_2^m$ *and a nonzero* $\boldsymbol{\alpha} \in \mathbb{F}_2^n$ *such that* $S_{\boldsymbol{b}}(x + \boldsymbol{\alpha}) + S_{\boldsymbol{b}}(x)$ *is a constant function.*

Clearly, S has a linear structure if and only if there exists a nonzero $\boldsymbol{\alpha} \in \mathbb{F}_2^n$ and a nonzero $\boldsymbol{b} \in \mathbb{F}_2^m$ such that $\tau_S(\boldsymbol{\alpha}, \boldsymbol{b}) = \pm 2^n$. The magnitude of $\tau(\boldsymbol{\alpha}, \boldsymbol{b})$ tells about the constant function $D_{\boldsymbol{\alpha}} S_{\boldsymbol{b}}$, i.e., it is a 0-linear structure (resp. 1-linear structure) if and only if $\tau_S(\boldsymbol{\alpha}, \boldsymbol{b}) = 2^n$ (resp. $\tau_S(\boldsymbol{\alpha}, \boldsymbol{b}) = -2^n$). From the autocorrelation table in Table 23, one can see that the function defined in Table 20 has a linear structure (see the entries in the column `F`). The following corollary is an immediate consequences of Theorem 8.22.

Corollary 8.26. *Let* $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$*. A vector* $\boldsymbol{\alpha} \in \mathbb{F}_2^n$ *is a linear structure of the component function* $S_{\boldsymbol{b}}$ *if and only if* $\dim_{\mathbb{F}_2}(\mathcal{R}/\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b})) \in \{0, 2^n\}$.

We will now discuss other possible means to characterize whether a vectorial Boolean functions has a linear structure. We first recall the following result that describes the relation of a linear structure, when viewed as an input difference to S, and the set of all its possible output differences.

Proposition 8.27. *Let* $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$*. The vector* $\boldsymbol{\alpha} \in \mathbb{F}_2^n$ *is a* c*-linear structure of the component function* $S_{\boldsymbol{b}}$ *if and only if* $\boldsymbol{b} \cdot \boldsymbol{\beta} = c$ *for all* $\boldsymbol{\beta} \in \mathbb{F}_2^m$ *such that* $\delta_S(\boldsymbol{\alpha}, \boldsymbol{\beta}) > 0$.

Proof. See the proof of Theorem 7 in [MT14, pg. 17]. ■

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_2^n$, $\boldsymbol{b} = (b_1, \ldots, b_m) \in \mathbb{F}_2^m$. In the construction of autocorrelation ideals $\tau I_S(\boldsymbol{\alpha}, \boldsymbol{b})$, we look at the implication of the derivative of $S_{\boldsymbol{b}}$ w.r.t. $\boldsymbol{\alpha}$. However, the construction of this ideal is too restrictive when we want to characterize $\boldsymbol{\alpha}$ as a linear structure of some component functions of S because in this case $\boldsymbol{\alpha}$ is the only relevant parameter.

Recall that we may view $\boldsymbol{\alpha}$ as an input difference to S. A set of polynomials in $\mathcal{R}$ that describes the application of $\boldsymbol{\alpha}$ to two different inputs of S is given by

$$F'_S \cup F''_S \cup \{x'_i + x''_i + \alpha_i : 1 \leq i \leq n\}$$

where F'_S and F''_S are the set of polynomials that represent S in variables x'_i, y'_j and x''_i, y''_j respectively, $1 \leq i \leq n, 1 \leq j \leq m$. If $\boldsymbol{\alpha}$ is a linear structure to some component functions of S, then the ideal

$$\langle F'_S \cup F''_S \cup \{x'_i + x''_i + \alpha_i : 1 \leq i \leq n\}\rangle$$

contains all polynomials that are implied by having $\boldsymbol{\alpha}$ as an input difference to S. One possible element of $\langle F'_S \cup F''_S \cup \{x'_i + x''_i + \alpha_i : 1 \leq i \leq n\}\rangle$ is the polynomial that represents Proposition 8.27, i.e.

$$\left(\sum_{j=1}^{m} b_j(y'_j + y''_j)\right) + c = \left(\sum_{j=1}^{m} b_j y'_j + b_j y''_j\right) + c. \tag{8.6}$$

Conjecture 8.28. *Let $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ and let $\mathcal{R}$ be a polynomial ring defined in* (8.4)*. A vector $\boldsymbol{\alpha} \in \mathbb{F}_2^n$ is a c-linear structure of the component function $S_{\boldsymbol{b}}$, $\boldsymbol{b} = (b_1, \ldots, b_m) \in \mathbb{F}_2^m$, if and only if*

$$\left(\sum_{j=1}^{m} b_j y'_j + b_j y''_j\right) + c \in \langle F'_S, F''_S, \{x'_i + x''_i + \alpha_i : 1 \leq i \leq n\}\rangle$$

where F'_S and F''_S are the set of polynomials that represent S in variables x'_i, y'_j and x''_i, y''_j respectively.

Note that by computing a Gröbner bases of the ideal $I = \langle F'_S, F''_S, \{x'_i + x''_i + \alpha_i : 1 \leq i \leq n\}\rangle$, we can determine whether the polynomial of the form (8.6) is in I (see Corollary 3.38). In the following, we provide an example that demonstrate Conjecture 8.28.

Example 8.29. *Let S be the mapping defined in Table 20 and let $\boldsymbol{\alpha} = 4 = (0, 0, 1, 0) \in \mathbb{F}_2^4$. We construct the polynomial ring $\mathcal{R}$ as in* (8.4) *with $n = m = 4$ and use lexicographic monomial ordering in $\mathcal{R}$. The reduced Gröbner basis G of*

$I = \langle F'_S, F''_S, \{x'_i + x''_i + \alpha_i : 1 \le i \le 4\}\rangle$ *consists of the following polynomials*

$$
\begin{aligned}
g_1 &= x'_1 + y''_1y''_2y''_4 + y''_1y''_3y''_4 + y''_1y''_3 + y''_1y''_4 + y''_2y''_4 + y''_2 + y''_3 + y''_4,\\
g_2 &= x'_2 + y''_1y''_2y''_3 + y''_1y''_2 + y''_1y''_3y''_4 + y''_2 + y''_3y''_4 + y''_3 + y''_4,\\
g_3 &= x'_3 + y''_1y''_2y''_4 + y''_1y''_2 + y''_1y''_3y''_4 + y''_1y''_4 + y''_1 + y''_2y''_4 + y''_3 + 1,\\
g_4 &= x'_4 + y''_1y''_2y''_3 + y''_1y''_3 + y''_1 + y''_2y''_3y''_4 + y''_2y''_3 + y''_2y''_4 + y''_2 + y''_3y''_4,\\
g_5 &= y'_1 + y''_1y''_2y''_3 + y''_1y''_2 + y''_1y''_3y''_4 + y''_1y''_3 + y''_2y''_3 + y''_2 + y''_3y''_4,\\
g_6 &= y'_2 + y''_1y''_2y''_3 + y''_1y''_3 + y''_2y''_3y''_4 + y''_2y''_4 + y''_3y''_4 + y''_3 + y''_4 + 1,\\
g_7 &= y'_3 + y''_1y''_3 + y''_2y''_3 + y''_2 + y''_3 + 1,\\
g_8 &= y'_4 + y''_1y''_2 + y''_1y''_3y''_4 + y''_1y''_3 + y''_1 + y''_2y''_3y''_4 + y''_2y''_4 + y''_2 + y''_3,\\
g_9 &= x''_1 + y''_1y''_2y''_4 + y''_1y''_3y''_4 + y''_1y''_3 + y''_1y''_4 + y''_2y''_4 + y''_2 + y''_3 + y''_4,\\
g_{10} &= x''_2 + y''_1y''_2y''_3 + y''_1y''_2 + y''_1y''_3y''_4 + y''_2 + y''_3y''_4 + y''_3 + y''_4,\\
g_{11} &= x''_3 + y''_1y''_2y''_4 + y''_1y''_2 + y''_1y''_3y''_4 + y''_1y''_4 + y''_1 + y''_2y''_4 + y''_3,\\
g_{12} &= x''_4 + y''_1y''_2y''_3 + y''_1y''_3 + y''_1 + y''_2y''_3y''_4 + y''_2y''_3 + y''_2y''_4 + y''_2 + y''_3y''_4,\\
g_{13} &= y''^2_1 + y''_1,\\
g_{14} &= y''^2_2 + y''_2,\\
g_{15} &= y''^2_3 + y''_3,\\
g_{16} &= y''^2_4 + y''_4.
\end{aligned}
$$

Let $\boldsymbol{b} = F = (1,1,1,1) \in \mathbb{F}_2^4$ *and let* $f = \sum_{i=1}^4 b_i y'_i + b_i y''_i + 0$. *We see that* $f \in I = \langle G\rangle$ *because* $f = g_5 + g_6 + g_7 + g_8$. *Therefore* $\boldsymbol{4}$ *is a* 0*-linear structure of the component function* $S_{\boldsymbol{b}}$ *(see also that* $\tau_S(\boldsymbol{4}, F) = 16$ *in Table 23).*

Note that if the ring $\mathcal{R}$ used a monomial ordering that respects the degree of monomials (e.g., degree-lexicographic or degree-reverse lexicographic ordering), it is possible that a polynomial of the form (8.6) is an element of the Gröbner basis. For instance, if we use the ring

$$\mathcal{R} = \mathbb{F}_2[x'_1, x'_2, x'_3, x'_4, x''_1, x''_2, x''_3, x''_4, y'_1, y'_2, y'_3, y'_4, y''_1, y''_2, y''_3, y''_4]$$

together with degree-lexicographic ordering, the polynomials f will appear in a Gröbner bases G of I. This, however, is not the case if we use different ordering of variables such as $\mathcal{R} = \mathbb{F}_2[x'_1, x'_2, x'_3, x'_4, y'_1, y'_2, y'_3, y'_4, x''_1, x''_2, x''_3, x''_4, y''_1, y''_2, y''_3, y''_4]$.

More generally, assuming Conjecture 8.28 is true, if $\mathcal{R}$ uses a monomial ordering that respects the degree of monomials and S has a linear structure, then there exists a polynomial of degree 1 in a Gröbner basis of $\langle F'_S, F''_S, \{x'_i + x''_i + \alpha_i : 1 \le i \le n\}\rangle$.