COMPUTING MÖBIUS TRANSFORMS OF BOOLEAN FUNCTIONS AND CHARACTERISING COINCIDENT BOOLEAN FUNCTIONS

Josef Pieprzyk[1] and Xian-Mo Zhang[1]

Abstract. The Möbius transform of Boolean functions is often involved in cryptographic design and analysis. This work is composed of two parts. In the first part we compute Möbius transform by different methods and study its cryptographic properties. In the second part we focus on the special case when a Boolean function is identical with its Möbius transform. We call such functions coincident. We further characterise coincident functions and study their cryptographic properties.

Key Words: Boolean Functions, Möbius transform, Coincident Functions

1. Introduction to This Work

Recent developments in algebraic analysis of ciphers put an emphasis on methods and techniques that treat a cryptographic system as a collection of Boolean functions, describe them by their algebraic normal forms (ANFs), and then examine their algebraic properties such as sparseness, algebraic degree, number of overdefined relations, number of monomials, etc. A prerequisite for an efficient algebraic analysis is the ability to represent Boolean functions and their relations by their short algebraic forms. Moreover, most of time the designers of Boolean functions are working with their truth tables and the translation from a truth table to its

[1] Centre for Advanced Computing - Algorithms and Cryptography, Department of Computing, Macquarie University, Sydney , NSW 2109, Australia, email: josef,xianmo@ics.mq.edu.au

unique algebraic normal form (ANF) is not immediate. The aim of this work is to investigate the Möbius transform and its significance in Cryptography. What is interesting about the Möbius transform is that it allows to define a class of Boolean functions whose ANFs can be written easily from their truth tables (and vice versa). This nice property can be useful for analysis and design of small cryptographic S-boxes. More importantly, it could be used to justify security level of a cryptographic scheme if its truth table is big enough so it is impossible to construct its truth table and as the results, it is impossible to determine its ANF. It is a well-known fact that a Boolean function f of n variables $(x_1, \ldots, x_n)$ can be uniquely represented a polynomial in Formula (1) where g is also a function of n variables that characterises f. We call g the Möbius transform of f. In this work we denote this relation by $g = \mu(f)$. We present three methods to compute $\mu(f)$. We then study cryptographic properties of $\mu(f)$. We further propose the concept of coincident functions. A Boolean function f is called coincident if f is identical with $\mu(f)$. We consider an example, $f(x_1, x_2, x_3) = x_3 \oplus x_2 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3$. From the ANF of f, we know that the truth table of $\mu(f)$ is (01101101). On the other hand, by computing, we know that the truth table of f is also (01101101). Then f is a coincident function on $(GF(2))^3$. In general if the ANF/truth table of a coincident function is given then we know its truth table/ANF without computing. We characterise the coincident functions and examine their cryptographic properties such as algebraic degree and nonlinearity.

The rest of the paper is organised as follows. Section 2 is a brief introduction to Boolean functions. We compute the Möbius transform $\mu(f)$ of a Boolean function f by using matrix, polynomial and recursive formulas in Sections 3, 4 and 5 respectively. In Section 6, we compute $\mu(f)$ after the variables are permuted. In Section 7 we prove that $deg(f) + deg(\mu(f)) \geq n$ where n is the number of the variables. We propose so-called coincident functions in Section 8 and then we characterise coincident functions by using matrix, polynomial and recursive relations in Sections 9, 15 and 16 respectively. We study operations of coincident functions in Section 10. In Section 11 we divide Boolean functions into cosets with respect to coincident functions and then we enumerate coincident functions in Section 12. In Section 13 we show a basis of coincident functions so as to get all coincident functions simply. In Section 14 we illustrate coincident functions by examples. Based on the

above results, we propose more properties of coincident functions in Section 17. To show the high degree of coincident functions, we give a lower bound on the degree of coincident functions in Section 18. Based on special properties of coincident functions, we study their nonlinearity and algebraic degree in Sections 19. Section 20 concludes the work.

2. Introduction to Boolean Functions

Throughout the paper we use the following notations. The vector space of n-tuples of elements from $GF(2)$ is denoted by $(GF(2))^n$. We write all vectors in $(GF(2))^n$ as $(0,\ldots,0,0) = \alpha_0$, $(0,\ldots,0,1) = \alpha_1$, ..., $(1,\ldots,1,1) = \alpha_{2^n-1}$, and call α_i the *binary representation* of integer i, $i = 0,1,\ldots,2^n-1$. A Boolean function f is a mapping from $(GF(2))^n$ to $GF(2)$ or simply, a function f on $(GF(2))^n$. We write f more precisely as $f(x)$ or $f(x_1,\ldots,x_n)$ where $x = (x_1,\ldots,x_n)$. The *truth table* of a function f on $(GF(2))^n$ is a $(0,1)$-sequence defined by $(f(\alpha_0),\ f(\alpha_1),\ldots,\ f(\alpha_{2^n-1}))$, The *Hamming weight* of a (0, 1)-sequence ξ, denoted by $HW(\xi)$, is defined as the number of nonzero coordinates of ξ. In particular, if ξ is the truth table of a function f, then $HW(\xi)$ is called the *Hamming weight* of f, denoted by $HW(f)$. f is said to be *balanced* if $HW(f) = 2^{n-1}$. The *Hamming distance* between functions f and g on $(GF(2))^n$, denoted by $d(f,g)$ is defined as $d(f,g) = HW(f \oplus g)$. The function f can be uniquely represented by a polynomial

$$f(x_1,\ldots,x_n) = \bigoplus_{\alpha\in(GF(2))^n} g(a_1,\ldots,a_n)x_1^{a_1}\cdots x_n^{a_n} \qquad (1)$$

where $\alpha = (a_1,\ldots,a_n)$, and g is also a function on $(GF(2))^n$, called the ***Möbius transform*** of f. The polynomial representation of f is called the *algebraic normal form* (ANF) of the function f and each $x_1^{a_1}\cdots x_n^{a_n}$ is called a *monomial (term)* in the ANF of f. The *algebraic degree*, or simply *degree*, of f, denoted by $deg(f)$, is defined as $deg(f) = \max_{(a_1,\ldots,a_n)}\{HW(a_1,\ldots,a_n) \mid g(a_1,\ldots,a_n) = 1\}$. f is called *affine* if its ANF has the following form: $f(x) = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus c$ where $x = (x_1,\ldots,x_n)$, $a_1,\ldots,a_n,c \in GF(2)$ are constant. In particular f is called *linear* if $c = 0$.

3. Computing $\mu(f)$ by Matrix

In this section we describe the Möbius Transform by using matrix.

Notation 1. *Let $\mathcal{R}_n$ denote the set of all functions on $(GF(2))^n$. In this work we write $\mu(f) = g$ where g is the* Möbius transform *of f, defined in Formula (1).*

By definition, it is easy to verify that the Möbius Transform μ is a one-to-one linear mapping from $\mathcal{R}_n$ to $\mathcal{R}_n$.

Notation 2. *We define $2^n \times 2^n$ (0, 1)-matrix, denoted by T_n, such that the ith row of T_n is the truth table of $x_1^{a_1} \cdots x_n^{a_n}$ where $(a_1, \ldots, a_n)$ is the binary representation of the integer i.*

Theorem 3.1. *T_n, defined in Notation 2, satisfies the following recursive relation: $T_0 = 1$, $T_s = \begin{bmatrix} T_{s-1} & T_{s-1} \\ O_{2^{s-1}} & T_{s-1} \end{bmatrix}$, where $O_{2^{s-1}}$ denotes the $2^{s-1} \times 2^{s-1}$ zero matrix, $s = 1, 2, \ldots$.*

Proof. We prove the theorem by induction on n. Since $T_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, it is easy to verify that the theorem is true when $n = 1$. More precisely, the 0th row $(1, 1)$ of T_1 is the truth table of the constant function $f(x_1) = x_1^0 = 1$ and the 1st row $(0, 1)$ of T_1 is the truth table of the function $f(x_1) = x_1$. Assume that the lemma is true when $1 \leq n \leq s - 1$. Let $n = s$. Consider the monomial $x_1^{a_1} \cdots x_s^{a_s}$. There exist two cases to be considered: $a_1 = 0$ (Case 1) and $a_1 = 1$ (Case 2). In Case 1 $x_1^{a_1} \cdots x_s^{a_s} = x_2^{a_2} \cdots x_s^{a_s}$. By the induction assumption, the ith row of T_{s-1} is the truth table of $x_2^{a_2} \cdots x_s^{a_s}$. Due to the relation between T_s and T_{s-1}, it is easy to verify that the ith row of T_s is the truth table of $x_1^{a_1} x_2^{a_2} \cdots x_s^{a_s}$ with $a_1 = 0$. In Case 2 $x_1^{a_1} \cdots x_s^{a_s} = x_1 x_2^{a_2} \cdots x_s^{a_s}$. Due to the relation between T_s and T_{s-1}, it is easy to verify that the ith row of T_s is the truth table of $x_1^{a_1} x_2^{a_2} \cdots x_s^{a_s}$ with $a_1 = 1$. □

Example 3.2. By using Theorem 16.1, we can construct T_1, T_2, T_3, ... T_1 has two rows (1 1) and (0 1). T_2 has four rows (1 1 1 1), (0 1 0 1), (0 0 1 1) and (0 0 0 1). T_3 has eight rows: (1 1 1 1 1 1 1 1), (0 1 0 1 0 1 0 1), (0 0 1 1 0 0 1 1), (0 0 0 1 0 0 0 1), (0 0 0 0 1 1 1 1), (0 0 0 0 0 1 0 1), (0 0 0 0 0 0 1 1) and (0 0 0 0 0 0 0 1). It is noted that (1, 0, 1) is the binary representation of integer 5. By the definition of T_n, the 5th row of T_3, (0 0 0 0 0 1 0 1), is the truth table of $x_1^1 x_2^0 x_3^1 = x_1 x_3$. □

Lemma 3.3. *(i)* $T_s^2 = I_{2^s}$ *where* I_{2^s} *is the* $2^s \times 2^s$ *identity matrix, (ii)* $(T_s \oplus I_{2^s})^2 = 0_{2^s}$ *where* 0_{2^s} *is the* $2^s \times 2^s$ *zero matrix, (iii)* $T_s(T_s \oplus I_{2^s}) = (T_s \oplus I_{2^s})T_s = T_s \oplus I_{2^s}$, *where* $s = 1, 2, \ldots$.

Proof. (i) can be proved by induction. (ii) and (iii) are immediate consequences of (i). □

Theorem 3.4. *Let* f *and* g *be functions on* $(GF(2))^n$. *Denote the truth tables of* f *and* g *by* ξ *and* η *respectively. Then the following statements are equivalent: (i)* $g = \mu(f)$, *(ii)* $f = \mu(g)$, *(iii)* $\eta T_n = \xi$, *(iv)* $\xi T_n = \eta$.

Proof. Assume that (i) holds. We now prove (iii). It is noted that ηT_n is a linear combination of the rows of T_n. Recall that $\eta = (g(\alpha_0), g(\alpha_1), \ldots, g(\alpha_{2^n-1}))$. By the definition of T_n, ηT_n is the truth table of f. Then $\eta T_n = \xi$. This proves that (iii) holds. Assume that (iii) holds. Let $g' = \mu(f)$ and η' be the truth table of g'. Since we have proved (i) $\Longrightarrow$ (iii), we know that $\eta' T_n = \xi$. Comparing $\eta' T_n = \xi$ with $\eta T_n = \xi$, since T_n is invertible, we know $\eta' = \eta$ and then $g' = g$. We then have proved that (i) holds. Therefore we have proved (i) $\Longleftrightarrow$ (iii). Symmetrically, (ii) $\Longleftrightarrow$ (iv). Due to (i) of Lemma 3.3, (iii) $\Longleftrightarrow$ (iv). The proof is completed. □

It is noted that the equivalence between (i) and (ii) of Theorem 3.4 was previously proved in [4]. However we regain it here by using a different concept. Theorem 3.4 enables us to compute the truth table/ANF from the ANF/truth table of a function by using the matrix T_n.

Example 3.5. Assume that we know the ANF of f on $(GF(2))^3$: $f(x_1, x_2, x_3) = 1 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_2x_3$. Set $g = \mu(f)$. From the ANF of f, we know that g has the truth table (10111001). By using Theorem 3.4, $(10111001)T_3 = (11010011)$ is the truth table of f. Conversely, assume that we know the truth table of function f on $(GF(2))^3$: (11010011). By using Theorem 3.4, $(11010011)T_3 = (10111001)$ is the truth table of the $\mu(f)$. Therefore we obtain the ANF of f: $f(x_1, x_2, x_3) = 1 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_2x_3$. □

Theorem 3.6. μ^2 *is identity transformation, or in other words,* $\mu^{-1} = \mu$.

Proof. The theorem is true due to (i) of Lemma 3.3. □

4. Computing $\mu(f)$ by Polynomials

In this section we express Möbius Transform by using polynomials.

Notation 3. *For any $\alpha \in (GF(2))^n$, we define a function D_α on $(GF(2))^n$ as follows: $D_\alpha(x) = (1 \oplus a_1 \oplus x_1) \cdots (1 \oplus a_n \oplus x_n)$ where $x = (x_1, \ldots, x_n)$, $\alpha = (a_1, \ldots, a_n)$.*

Furthermore, it is known that for any function f on $(GF(2))^n$, we have

$$f(x) = \bigoplus_{\alpha \in (GF(2))^n} f(\alpha) D_\alpha(x) \tag{2}$$

For any two functions f and f' on $(GF(2))^n$, $f(x) \oplus f'(x) = \bigoplus_{\alpha \in (GF(2))^n} (f(\alpha) \oplus f'(\alpha)) D_\alpha(x)$ and $f(x) \cdot f'(x) = \bigoplus_{\alpha \in (GF(2))^n} (f(\alpha) \cdot f'(\alpha)) D_\alpha(x)$ where the second formula holds due to $D_\alpha(\beta) = \begin{cases} 1 & \text{if } \beta = \alpha \\ 0 & \text{if } \beta \neq \alpha \end{cases}$,

Lemma 4.1. *For any $\alpha \in (GF(2))^n$, we have (i) $\mu(D_\alpha)(x) = x_1^{a_1} \cdots x_n^{a_n}$ where $\alpha = (a_1, \ldots, a_n)$, (ii) $\mu(x_1^{a_1} \cdots x_n^{a_n}) = D_\alpha(x)$.*

Proof. Due to Theorem 3.6, (i) and (ii) are equivalent. Therefore we only need to prove (i). It is noted that the truth table ξ of $D_\alpha(x)$ is all-zero vector of length 2^n except for the ith coordinate where α is the binary representation of i. Set $\eta = \xi T_n$. Clearly η is exactly the ith row of T_n. According to Theorem 3.4, η is the truth table of $\mu(D_\alpha(x))$. On the other hand, due to the definition of T_n, the ith row of T_n is the truth table of $x_1^{a_1} \cdots x_n^{a_n}$. Thus we have proved that $\mu(D_\alpha)(x)$ and $x_1^{a_1} \cdots x_n^{a_n}$ have the same truth table and thus (i) holds. □

The following conclusion is true due to Formula (2) and Lemma 4.1.

Theorem 4.2. *Let f be a function on $(GF(2))^n$.*

(i) *if the truth table $(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$ of f, where α_i is the binary representation of integer i, $i = 0, 1, \ldots, 2^n - 1$, is known then $\mu(f)(x) = \bigoplus_{\alpha \in (GF(2))^n} f(\alpha) x_1^{a_1} \cdots x_n^{a_n}$,*

(ii) *if the ANF of f, or, $f(x) = \bigoplus_{\alpha \in (GF(2))^n} g(\alpha) x_1^{a_1} \cdots x_n^{a_n}$, where $\alpha = (a_1, \ldots, a_n)$, and $g = \mu(f)$, is given then $\mu(f)(x) = \bigoplus_{\alpha \in (GF(2))^n} g(\alpha) D_\alpha(x)$.*

Theorem 4.2 enables us to write the ANF/truth table from the truth table/ANF by using polynomials.

5. Computing $\mu(f)$ by Recursive Relations

In this section we compute the Möbius Transform of a function by recursive formulas.

Theorem 5.1. *It is noted that any function f on $(GF(2))^n$ as $f(x) = x_1 g(y) \oplus h(y)$ where $x = (x_1, \ldots, x_n)$ and $y = (x_2, \ldots, x_n)$. Then $\mu(f)(x) = x_1(\mu(g)(y) \oplus \mu(h)(y)) \oplus \mu(h)(y)$.*

Proof. Let ξ, η, ζ denote the truth tables of f, g and h respectively. It is easy to verify that $\xi = (\zeta, \eta \oplus \zeta)$. Let ξ' denote the truth table of $\mu(f)$. According to Theorem 3.4, the truth table of $\mu(f)$ can be computed as $\xi T_n = (\zeta, \eta \oplus \zeta)T_n = (\zeta T_{n-1}, \eta T_{n-1})$. Again, due to Theorem 3.4, ζT_{n-1} and ηT_{n-1} are the truth tables of $\mu(h)$ and $\mu(g)$ respectively. Therefore, it is easy to verify that $\mu(f)(x) = x_1(\mu(g(y) \oplus h(y)) \oplus \mu(h)(y)$. □

Theorem 5.1 changes the Möbius Transform into the same problem with a less dimension.

6. Computing $\mu(f)$ after a Permutations on Variables

Notation 4. *Let f be a function on $(GF(2))^n$. Let P be a permutation on $\{1, \ldots, n\}$. Define the function f_P as $f_P(x_1, \ldots, x_n) = f(x_{P(1)}, \ldots, x_{P(n)})$.*

Theorem 6.1. *Let f be a function on $(GF(2))^n$ and $g = \mu(f)$. Then $\mu(f_P) = g_P$.*

Proof. Due to (1), f can be expressed as $f(x_1, \ldots, x_n) = \bigoplus_{\alpha \in (GF(2))^n} g(a_1, \ldots, a_n) x_1^{a_1} \cdots x_n^{a_n}$ where $\alpha = (a_1, \ldots, a_n)$. Then $f_P(x_1, \ldots, x_n) = \bigoplus_{\alpha \in (GF(2))^n} g(a_1, \ldots, a_n) x_{P(1)}^{a_1} \cdots x_{P(n)}^{a_n}$. It is noted that $x_{P(1)}^{a_1} \cdots x_{P(n)}^{a_n}$ is identical with $x_1^{a_{P^{-1}(1)}} \cdots x_n^{a_{P^{-1}(n)}}$ where P^{-1} denotes the inverse of P. Set $a_{P^{-1}(i)} = b_i$ and then $a_i = b_{P(i)}$, $i = 1, \ldots, n$. Therefore $g(a_1, \ldots, a_n) x_{P(1)}^{a_1} \cdots x_{P(n)}^{a_n}$ is identical with $g(b_{P(1)}, \ldots, b_{P(n)}) x_1^{b_1} \cdots x_n^{b_n}$. Then we have proved that $f_P(x_1, \ldots, x_n) = \bigoplus_{\beta \in (GF(2))^n} g(b_{P(1)}, \ldots, b_{P(n)}) x_1^{b_1} \cdots x_n^{b_n}$ where $\beta = (b_1, \ldots, b_n)$. By definition, we know that the Möbius transform of f_P is g_P, or in other words, $\mu(f_P) = g_P$. □

It should be noted that the permutation P in Theorem 6.1 is defined on the set of indexes $\{1, \ldots, n\}$ but P cannot be extended to be a permutation on the vector space $(GF(2))^n$.

7. A Lower Bound on $deg(f) + deg(\mu(f))$

In this section we present a result: the sum of degree of any nonzero Boolean function with n variables and the degree of its Möbius transform is lower bounded by n.

Theorem 7.1. *Let f be a nonzero function on $(GF(2))^n$. Then $deg(f) + deg(\mu(f)) \geq n$.*

Proof. We prove the theorem by induction on n. It is easy to verify the theorem is true for $n = 1$ because $\mu(f_1) = f_2$, $\mu(f_2) = f_1$ and $\mu(f_3) = f_3$ where $f_1(x_1) = 1 \oplus x_1$, $f_2(x_1) = 1$ and $f_3(x_1) = x_1$. We assume that the theorem holds for $1 \leq n \leq s - 1$. Consider the case of $n = s$. Let f be a function on $(GF(2))^s$. We can express f as $f(x) = x_1 g(y) \oplus h(y)$ where $x = (x_1, \ldots, x_n)$, $y = (x_2, \ldots, x_n)$, g and h are functions on $(GF(2))^{n-1}$. According to Theorem 5.1, $\mu(f)(x) = x_1(\mu(g)(y) \oplus \mu(h)(y)) \oplus \mu(h)(y)$. There exist two cases to be considered: $g \neq h$ (Case 1) and $g = h$ (Case 2). We now consider Case 1. Case 1 is composed of three cases: $deg(\mu(g)) > deg(\mu(h))$ (Case 1.1), $deg(\mu(g)) < deg(\mu(h))$ (Case 1.2) and $deg(\mu(g)) = deg(\mu(h))$ (Case 1.3). For Case 1.1, $deg(f) + deg(\mu(f)) \geq 1 + deg(g) + 1 + deg(\mu(g) \oplus \mu(h)) = 1 + deg(g) + 1 + deg(\mu(g))$. By the induction assumption, $deg(g) + deg(\mu(g)) \geq s-1$ and then $deg(f)+deg(\mu(f)) \geq 1+s$. For Case 1.2, $deg(f)+deg(\mu(f)) \geq deg(h)+1+deg(\mu(g) \oplus \mu(h)) = deg(h)+1+deg(\mu(h))$. By the induction assumption, $deg(h) + deg(\mu(h)) \geq s - 1$ and then $deg(f) + deg(\mu(f)) \geq s$. For Case 1.3, $deg(f) + deg(\mu(f)) \geq 1 + deg(g) + deg(\mu(h)) = 1 + deg(h) + deg(\mu(h))$. By the induction assumption, $deg(h) + deg(\mu(h)) \geq s - 1$ and then $deg(f) + deg(\mu(f)) \geq s$. We next consider Case 2. In Case 2, $deg(f)+deg(\mu(f)) = 1+deg(g)+deg(\mu(h)) = 1+deg(h)+deg(\mu(h))$. By the induction assumption, $deg(h)+deg(\mu(h)) \geq s-1$ and then $deg(f) + deg(\mu(f)) \geq s$. We have proved that the theorem is true for $n = s$. Therefore we have proved the theorem. □

It is noted that the lower bound in Theorem 7.1 can be reached. For example, if $f(x) = (1 \oplus x_1) \cdots (1 \oplus x_n) = D_{\alpha_0}(x)$ where α_0

denotes the zero vector in $(GF(2))^n$, according to Lemma 4.1, $\mu(f)$ is the constant one. Then $deg(f) + deg(\mu(f)) = n + 0 = n$.

8. Concept of Coincident Boolean Functions

In this section we propose a special kind of Boolean functions.

Definition 8.1. Let f be a function on $(GF(2))^n$. If f and $\mu(f)$ are identical, or in other words, $f(\alpha) = 1$ if and only if $x_1^{a_1} \cdots x_n^{a_n}$ is a monomial in the ANF of f, for any $\alpha = (a_1, \ldots, a_n) \in (GF(2))^n$, then f is called a *coincident function*.

According to the definition of coincident functions and Theorem 3.4, we conclude as follows.

Theorem 8.2. *Let f be a function on $(GF(2))^n$ and $g = \mu(f)$. Denote the truth tables of f and g by ξ and η. Then the following statements are equivalent: (i) f is coincident, (ii) g is coincident, (iii) $\xi T_n = \xi$, (iv) $\eta T_n = \eta$, (v) f and g are identical, (vi) ξ and η identical.*

Example 8.3. Consider the function f on $(GF(2))^4$: $f(x_1, x_2, x_3, x_4)= x_2x_4 \oplus x_2x_3 \oplus x_1x_2 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3$. From the ANF of f, we know that the truth table of $\mu(f)$ is (0000011000011110). By computing, the truth table of f is also (0000011000011110). Then f is coincident on $(GF(2))^4$.

Since any coincident function is identical with its Möbius Transform, we can have the truth table/ANF of a coincident function from its ANF/truth table without computing.

9. Characterisations and Constructions of Coincident Boolean Functions (by Matrix)

In this section we characterise coincident functions by using matricies.

Notation 5. *Set $T_n^* = T_n \oplus I_{2^n}$, $n = 1, 2, \ldots$.*

Due to Theorem 8.2, we can state as follows.

Theorem 9.1. *Let f be a function on $(GF(2))^n$ and $g = \mu(f)$. Then the following statements are equivalent: (i) f is coincident, (ii) g is coincident, (iii) the truth table ξ of f satisfies $\xi T_n^* = 0$*

where 0 *denotes the all-zero vector of length* 2^n*, (iv) the truth table* η *of* g *satisfies* $\eta T_n^* = 0$*.*

Lemma 9.2. *(i)* $T_n^* = \begin{bmatrix} T_{n-1}^* & T_{n-1} \\ O_{2^{n-1}} & T_{n-1}^* \end{bmatrix}$*,* $n = 1, 2, \ldots$*, (ii)* $(T_n^*)^2 = 0_{2^n}$*, (iii)* $T_n T_n^* = T_n^* T_n = T_n^*$*.*

Proof. (i) is obvious due to the relation between T_n and T_n^*. (ii) and (iii) are equivalent to (ii) and (iii) of Lemma 3.3 respectively. □

We prove Theorems 9.3 and 9.4 in the full paper.

Theorem 9.3. *Let* f *be a function on* $(GF(2))^n$*. Then the following statements are equivalent:*

(i) f *is coincident,*
(ii) *the truth table of* f *can be expressed as* $(\zeta T_{n-1}^*, \zeta)$ *where* ζ *is a (0, 1)-vector of length* 2^{n-1}*,*
(iii) *the truth table of* f *can be expressed as* $(\zeta T_{n-1}^*, \zeta \oplus \vartheta T_{n-1}^*)$ *where* ϑ *is any (0, 1)-vector of length* 2^{n-1}*.*

Theorem 9.4. *Let* f *be a function on* $(GF(2))^n$*. Then* f *is coincident if and only if the truth table of* f *can be expressed as* ηT_n^* *where* η *is a (0, 1)-vector of length* 2^n*.*

Clearly we can give Theorem 9.4 an equivalent statement as follows.

Theorem 9.5. *Let* f *be a function on* $(GF(2))^n$*. Then* f *is coincident if and only if the truth table of* f *is a linear combination of rows of* T_n^**.*

Theorems 9.3, 9.4 and 9.5 can be applied to construct coincident functions.

10. Operations of Coincident Functions

According to Theorem 9.4, the following statement holds.

Corollary 10.1. *If both* f *and* g *are coincident functions on* $(GF(2))^n$ *then* $f \oplus g$ *is coincident.*

But, $f \cdot g$ is not necessarily coincident even both f and g are coincident. For example, both $f_1 = x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3$ and $f_2 = x_2x_3 \oplus x_1x_2 \oplus x_1x_2x_3$ are coincident functions on $(GF(2))^3$ but $f_1 f_2 = x_2x_3$ is not coincident on $(GF(2))^3$. However, when f and g have disjoint variables the conclusion is right.

Notation 6. *Let $A = (a_{ij})$ an $m \times n$ matrix over $GF(2)$ and B be a $p \times q$ matrix over $GF(2)$. The* Kronecker product *of A and B, denoted by $A \times B$, is an $mp \times nq$ matrix, defined as* $A \times B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ a_{21}B & a_{22}B & \cdots & a_{2m}B \\ & & \cdots & \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{bmatrix}$.

The following lemma is a special case of Formula (23) in [3].

Lemma 10.2. *Let A and B be $m \times m$ and $n \times n$ matrices over $GF(2)$ respectively, ξ and η be vectors in $(GF(2))^m$ and $(GF(2))^n$ respectively. Then $(\xi \times \eta)(A \times B) = (\xi A) \times (\eta B)$.*

Lemma 10.3. *$T_n = T_p \times T_{n-p}$, $p = 0, 1, \ldots, n$, where $\times$ is the Kronecker Product.*

Proof. It is noted that $T_n = T_1 \times T_{n-1}$. Therefore the lemma can be proved by induction □

By a straightforward verification, we can prove the following Lemma.

Lemma 10.4. *Let f_1 and f_2 on $(GF(2))^m$ and $(GF(2))^n$ respectively. Define a function on $(GF(2))^{m+n}$ as $f(y, z) = f_1(y) \cdot f_2(z)$ where $y \in (GF(2))^m$ and $z \in (GF(2))^n$. Let ξ_1 and ξ_2 denote the truth tables of f_1 and f_2 respectively. Then $\xi_1 \times \xi_2$ is the truth table of a coincident function f.*

Theorem 10.5. *Let f_1 and f_2 be coincident functions on $(GF(2))^m$ and $(GF(2))^n$ respectively. Define a function f on $(GF(2))^{m+n}$ as $f(x, y) = f_1(x) \cdot f_2(y)$. Then f is a coincident function f on $(GF(2))^{m+n}$.*

Proof. Let ξ_1 and ξ_2 denote the truth tables of f_1 and f_2 respectively. Due to Lemma 10.4, $\xi_1 \times \xi_2$ is the truth table of a coincident function f. By using Lemmas 10.3 and 10.2, $(\xi_1 \times \xi_2)T_{m+n} = (\xi_1 \times \xi_2)(T_m \times T_n) = (\xi_1 T_m) \times (\xi_2 T_n)$. According to Theorem 8.2, $\xi_1 T_m = \xi_1$ and $\xi_2 T_n = \xi_2$. Therefore $(\xi_1 \times \xi_2)T_{m+n} = \xi_1 \times \xi_2$. Again, Theorem 8.2, we know that $\xi_1 \times \xi_2$ is the truth table of a coincident function on $(GF(2))^{m+n}$. □

In general, the product of two coincident functions is not necessarily coincident. However the operation is special.

Theorem 10.6. *Let f and f' be both coincident functions on $(GF(2))^n$ whose ANFs are given as $f(x) = \bigoplus_{\alpha\in(GF(2))^n} g(\alpha)x_1^{a_1}\cdots x_n^{a_n}$ and*
$f'(x) = \bigoplus_{\alpha\in(GF(2))^n} g'(\alpha)x_1^{a_1}\cdots x_n^{a_n}$ respectively where $g = \mu(f)$ and $g' = \mu(f')$. Then $f(x)\cdot f'(x) = \bigoplus_{\alpha\in(GF(2))^n} g(\alpha)g'(\alpha)D_\alpha(x)$.

Proof. Due to Formula (2), $f(x) = \bigoplus_{\alpha\in(GF(2))^n} f(\alpha)D_\alpha(x)$ and $f'(x) = \bigoplus_{\alpha\in(GF(2))^n} f'(\alpha)D_\alpha(x)$. Then
$f(x)\cdot f'(x) = \bigoplus_{\alpha\in(GF(2))^n} f(\alpha)f'(\alpha)D_\alpha(x)$. Since both f and f' are coincident, f is identical with g and f' is identical with g'. We then have proved the theorem. □

11. A Classification of Boolean Functions

Definition 11.1. Define a mapping Ψ from $\mathcal{R}_n$ to $\mathcal{R}_n$, where $\mathcal{R}_n$ has been defined in Notation 1: $\Psi(f) = h$ if and only if $\xi T_n^* = \zeta$ where $f, h \in \mathcal{R}_n$, ξ and ζ are truth tables of f and h respectively.

By definition, the following statement is obvious.

Lemma 11.2. *Ψ, defined in Definition 11.1, is a linear mapping.*

Due to Theorem 9.4, we state as follows.

Lemma 11.3. *$\Psi(f)$ is coincident for any function f on $(GF(2))^n$.*

Notation 7. *For each coincident function h on $(GF(2))^n$, set $\aleph_h = \{f|\Psi(f) = h\}$.*

Lemma 11.4. *$\aleph_0$ is the collection of all coincident functions on $(GF(2))^n$ and $\aleph_0$ is a linear subspace of $(GF(2))^n$.*

Proof. Let f be a function on $(GF(2))^n$ and ξ be the truth table of f. Then $f \in \aleph_0 \Longleftrightarrow \Psi(f) = 0 \Longleftrightarrow \xi T_n^* = 0 \Longleftrightarrow f$ is coincident. This proves that $\aleph_0$ is the collection of all coincident functions. According to Corollary 10.1, all coincident functions form a linear subspace of of $(GF(2))^n$. □

Applying linear algebra to Ψ, $\aleph_0$ and $\mathcal{R}_n$, we obtain the following results (Theorems 11.5, 11.6 and Corollary 11.7).

Theorem 11.5. *Let f_1, f_2 be functions in $(GF(2))^n$. Then there exists some $h \in \aleph_0$ such that $f_1, f_2 \in \aleph_h$ if and only if $f_1 \oplus f_2 \in \aleph_0$.*

Theorem 11.6. *For any fixed $h \in \aleph_0$ and any fixed $f \in \aleph_h$, $\aleph_h = f \oplus \aleph_0$, where $f \oplus \aleph_0 = \{f \oplus h|h \in \aleph_0\}$.*

Corollary 11.7. *$\mathcal{R}_n$, the set of all functions on $(GF(2))^n$, can be partitioned as $\mathcal{R}_n = \bigcup_{h\in\aleph_0} \aleph_h$, where $\aleph_h \cap \aleph_{h'} = \emptyset$, where $\emptyset$ denotes the empty set, for any $h, h' \in \aleph_0$ with $h \neq h'$.*

12. Enumeration of Coincident Functions

Theorem 12.1. *$\#\aleph_h = 2^{2^{n-1}}$ for each $h \in \aleph_0$, where $\#X$ denotes the number of elements in the set X and n is the number of the variables of functions. In particular, $\#\aleph_0 = 2^{2^{n-1}}$, or in other words, there precisely exist $2^{2^{n-1}}$ coincident functions on $(GF(2))^n$.*

Proof. By linear algebra, $\#\aleph_h$ has a constant value N for all $h \in \aleph_0$. In particular, $\#\aleph_0 = N$. According to Corollary 11.7, we know that $\#\mathcal{R}_n = \sum_{h\in\aleph_0} \#\aleph_h$ and then $2^{2^n} = N \cdot N$. This proves that $N = 2^{2^{n-1}}$. □

Corollary 12.2. *The matrix T_n^* has a rank 2^{n-1}.*

Proof. According to Theorem 12.1, there precisely exist $2^{2^{n-1}}$ coincident functions on $(GF(2))^n$. Then the corollary is true due to Theorem 9.5. □

Corollary 12.3. *Let f be a function on $(GF(2))^n$. Then $\Psi(f) = h$ if and only if $f \oplus \mu(f) = h$ where Ψ has been defined in Definition 11.1.*

Proof. Let ξ and ζ be the truth tables of f and h respectively. It is clear that $\Psi(f) = h \iff \xi T_n^* = \zeta \iff \xi \oplus \xi T_n = \zeta \iff f \oplus \mu(f) = h$. □

13. A Basis of Coincident Functions

In this section we improve Theorem 9.5.

Lemma 13.1. *All the 2^{n-1} rows of the matrix $\begin{bmatrix} T_{n-1}^* & T_{n-1} \end{bmatrix}$ form a basis of rows of T_n^*.*

Proof. Due to Lemma 9.2, $T_n^* = \begin{bmatrix} T_{n-1}^* & T_{n-1} \\ 0_{2^{n-1}} & T_{n-1}^* \end{bmatrix}$. Then $\begin{bmatrix} T_{n-1}^* & T_{n-1} \end{bmatrix}$ is a submatrix of T_n^*. It is noted that $\begin{bmatrix} T_{n-1}^* & T_{n-1} \end{bmatrix}$ has a rank 2^{n-1} because T_{n-1} is nonsingular. On the other hand, due to Corollary 12.2, the rank of T_n^* is also 2^{n-1}. Therefore the Lemma holds. □

Combing Lemma 13.1 and Theorem 9.5, we state as follows.

Theorem 13.2. *All the 2^{n-1} functions on $(GF(2))^n$, whose truth tables are the rows of $\left[\begin{array}{cc} T^*_{n-1} & T_{n-1} \end{array}\right]$, form a basis of all the coincident functions on $(GF(2))^n$.*

According to Theorem 13.2, we can state as follows.

Theorem 13.3. *Let f be a function on $(GF(2))^n$. Then f is coincident if and only if the truth table of f is a linear combination of rows of $\left[\begin{array}{cc} T^*_{n-1} & T_{n-1} \end{array}\right]$.*

Theorem 13.3 is an improvement on Theorem 9.5.

14. Examples of Coincident Functions

Example 14.1. According to Theorem 12.1, there precisely exist $2^{2^{3-1}} = 16$ coincident functions on $(GF(2))^3$. According to Theorem 13.3, all the linear combinations of rows of $[T^*_2, T_2] = \left[\begin{array}{cccccccc} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$ are the truth tables of coincident functions on $(GF(2))^3$: (01111111), (00010101), (00010011), (00000001), (00000111), (00000110), (01101010), (00010100), (01101101), (01101011), (01111110), (01101100), (01111000), (01111001), (00010010), (00000000). We directly write the ANFs of the 16 coincident functions on $(GF(2))^3$: $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3$, $x_2x_3 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_1x_2x_3$, $x_1x_3 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_1x_3 \oplus x_1x_2$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_2$, $x_2x_3 \oplus x_1x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_2x_3$, $x_2x_3 \oplus x_1x_2$, 0 □

15. Characterisations and Constructions of Coincident Functions (by Polynomial)

In this section we characterise coincident functions in polynomial form. We prove Theorem 15.1 in the full paper.

Theorem 15.1. *Let h be a function on $(GF(2))^n$. Then the following statements are equivalent: (i) h is coincident, (ii) there exists a function f on $(GF(2))^n$ such that $h = f \oplus \mu(f)$ or $h = \Psi(f)$*

where Ψ has been defined in Definition 11.1, (iii) $\Psi(h)$ is the zero function.

Due to Lemma 4.1 and Theorem 15.1, we state as follows.

Lemma 15.2. *For any $\alpha = (a_1, \ldots, a_n) \in (GF(2))^n$, $D_\alpha(x) \oplus x_1^{a_1} \cdots x_n^{a_n}$ is coincident.*

Combing Theorem 15.1 and Lemma 4.1, we state as follows.

Theorem 15.3. *Let h be a function on $(GF(2))^n$. Then h is coincident if and only if h is a linear combination of all the functions in the form $D_\alpha(x) \oplus x_1^{a_1} \cdots x_n^{a_n}$ where $\alpha = (a_1, \ldots, a_n) \in (GF(2))^n$.*

Proof. The sufficiency holds due to Lemma 15.2. We only prove the necessity. Assume that f is coincident. Due to Theorem 15.1, $h = f \oplus \mu(f)$ where f is a function on $(GF(2))^n$. From Formula (2), $f(x) = \bigoplus_{\alpha \in (GF(2))^n} f(\alpha) D_\alpha(x)$. According to Theorem 4.2, $\mu(f)(x) = \bigoplus_{\alpha \in (GF(2))^n} f(\alpha) x_1^{a_1} \cdots x_n^{a_n}$. Then $f(x) \oplus \mu(f)(x) = \bigoplus_{\alpha \in (GF(2))^n} f(\alpha)\ (D_\alpha(x) \oplus x_1^{a_1} \cdots x_n^{a_n})$. This proves the necessity. □

Theorem 15.4. *Let f be a function on $(GF(2))^n$ whose ANF of f is given as $f(x) = \bigoplus_{\alpha \in (GF(2))^n} g(\alpha) x_1^{a_1} \cdots x_n^{a_n}$ where $\alpha = (a_1, \ldots, a_n) \in (GF(2))^n$ and $g = \mu(f)$. Then the following statements are equivalent: (i) f is coincident,*
(ii) $f(x) = \bigoplus_{\alpha \in (GF(2))^n} f(\alpha) x_1^{a_1} \cdots x_n^{a_n}$,
(iii) $f(x) = \bigoplus_{\alpha \in (GF(2))^n} g(\alpha) D_\alpha(x)$.

Proof. Due to Formula 2, $f(x) = \bigoplus_{\alpha \in (GF(2))^n} f(\alpha) D_\alpha(x)$. On the other hand, due to Formula 1, $f(x) = \bigoplus_{\alpha \in (GF(2))^n} g(\alpha) x_1^{a_1} \cdots x_n^{a_n}$ where $\alpha = (a_1, \ldots, a_n)$. Then f is coincident $\iff$ f and g are identical. Thus we have proved the theorem. □

Theorems 15.1, 15.3 and 15.4 can be applied to construct coincident functions.

Notation 8. *Let $\beta = (b_1, \ldots, b_n)$ and $\alpha = (a_1, \ldots, a_n)$ be (0, 1)-vectors. Then $\beta \preceq \alpha$ means that if $b_j = 1$ then $a_j = 1$. In particular, $\beta \prec \alpha$ means that $\beta \preceq \alpha$ but $\beta \neq \alpha$.*

The following result is well-known to coding theorists (see p.372 of [1]):

Lemma 15.5. *Let f be a function on $(GF(2))^n$ and $\alpha = (a_1, \ldots, a_n)$ be a vector in $(GF(2))^n$. Then the term $x_1^{a_1} \cdots x_n^{a_n}$ appears in the ANF of f if and only if $\bigoplus_{\beta \preceq \alpha} f(\beta) = 1$.*

Lemma 15.6. *Let f be a function on $(GF(2))^n$. Then f is coincident if and only if $f(\alpha) = \bigoplus_{\beta \preceq \alpha} f(\beta)$.*

Proof. Let $g = \mu(f)$. Due to Lemma 15.5, $g(\alpha) = \bigoplus_{\beta \preceq \alpha} f(\beta)$ for any $\alpha \in (GF(2))^n$. It is noted that f is coincident $\Longleftrightarrow f = g \Longleftrightarrow f(\alpha) = \bigoplus_{\beta \preceq \alpha} f(\beta)$ for each $\alpha \in (GF(2))^n$. □

Theorem 15.7. *Let f be a function on $(GF(2))^n$. Then f is coincident if and only if for any $\alpha \in (GF(2))^n$, $\bigoplus_{\beta \prec \alpha} f(\beta) = 0$.*

Proof. It is noted that $f(\alpha) = \bigoplus_{\beta \preceq \alpha} f(\beta) \Longleftrightarrow \bigoplus_{\beta \prec \alpha} f(\beta) = 0$. Therefore the theorem is true due to Lemma 15.6. □

Due to Theorem 8.2, f is coincident if and only if $\mu(f)$ is coincident. Then the following conclusions follow Lemma 15.6 and Theorem 15.7 respectively.

Corollary 15.8. *Let f be a function on $(GF(2))^n$ and $g = \mu(f)$. Then f is coincident if and only if $g(\alpha) = \bigoplus_{\beta \preceq \alpha} g(\beta)$.*

Corollary 15.9. *Let f be a function on $(GF(2))^n$ and $g = \mu(f)$. Then f is coincident if and only if for any $\alpha \in (GF(2))^n$, $\bigoplus_{\beta \prec \alpha} g(\beta) = 0$.*

16. Characterisations and Constructions of Coincident Functions (by Recursive Formulas)

In this section we characterise coincident functions by recursive relations.

Theorem 16.1. *Let f be a function on $(GF(2))^n$. Then f is coincident if and only if there exists a function g on $(GF(2))^{n-1}$ such that $f(x) = x_1 g(y) \oplus \Psi(g)(y)$ where Ψ has been defined in Definition 11.1. Furthermore, if f is nonzero then g is nonzero.*

Proof. Since f can be expressed as $f(x) = x_1 g(y) \oplus h(y)$ where both g and h are functions on $(GF(2))^{n-1}$, due to Theorem 5.1, $\mu(f)(x) = x_1 \mu(g \oplus h)(y) \oplus \mu(h)(y)$. It is noted that f is coincident $\Longleftrightarrow f = \mu(f) \Longleftrightarrow g = \mu(g \oplus h)$ and $h = \mu(h) \Longleftrightarrow h = \mu(h)$ and $h = \mu(g) \oplus g \Longleftrightarrow h = \mu(g) \oplus g$ (due to Theorem 15.1). Due to Corollary 12.3, $g \oplus \mu(g) = \Psi(g)$. This proves the main part of the theorem. Therefore if f is nonzero then g is nonzero then g is nonzero. □

Recursively applying Theorem 16.1, we state as follows.

Theorem 16.2. *Let f be a function on $(GF(2))^n$. Then f is coincident if and only if there exists a function f_i on $(GF(2))^{n-i}$, $i = 1, \ldots, n$, such that $f(x_1, \ldots, x_n) = x_1 f_1(x_2, \ldots, x_n) \oplus x_2 f_2(x_3, \ldots, x_n) \oplus \cdots \oplus x_{n-1} f_{n-1}(x_n) \oplus f_n(x_n)$ where $x_i f_i(x_{i+1}, \ldots, x_n) \oplus \cdots \oplus x_{n-1} f_{n-1}(x_n) \oplus f(x_n) = \Psi(x_{i-1} f_{i-1}(x_i, \ldots, x_n) \oplus \cdots \oplus x_{n-1} f_{n-1}(x_n) \oplus f_n(x_n))$, $i = 2, \ldots, n$.*

Theorems 16.1, 16.2 and 15.4 can be applied to construct coincident functions.

17. More Properties of Coincident Functions

Theorem 17.1. *Let f be a function on $(GF(2))^n$ and P be a permutation on $\{1, \ldots, n\}$. Then f is coincident if and only if f_P is coincident, where f_P is defined in Notation 4, i.e., $f_P(x_1, \ldots, x_n) = f(x_{P(1)}, \ldots, x_{P(n)})$.*

Proof. Set $g = \mu(f)$. Assume that f is coincident. Then g is identical with f and then $f_P = g_P$. On the other hand, according to Theorem 6.1, $\mu(f_P) = g_P$. Therefore we have $\mu(f_P) = f_P$ and then f_P is coincident. The inverse is true because if we set $f_P = f'$ then $f'_{P^{-1}} = f$. □

It should be noted that the permutation P in Theorem 17.1 is defined on the set of indexes $\{1, \ldots, n\}$ instead of the vector space $(GF(2))^n$. For example, $f(x_1, x_2, x_3) = x_1 x_2 x_3$ is coincident on $(GF(2))^3$. Set a nonsingular linear transformation Q on $(GF(2))^3$: $x_1 = y_1 \oplus y_2$, $x_2 = y_2$, $x_3 = y_3$. It is seay to see that $f(Q(x_1, x_2, x_3)) = y_1 y_2 y_3 \oplus y_2 y_3$ that is not coincident on $(GF(2))^3$.

Theorem 17.2. *Let f be a function on $(GF(2))^n$ and P be a permutation on $\{1, \ldots, n\}$. Set $f'(x_{P(1)}, \ldots, x_{P(n)}) = f(x_1, \ldots, x_n)$. Then f is coincident if and only if f' is coincident.*

Proof. The theorem is true due to the equivalence between (i) and (iii) in Theorem 15.4. □

A difference between Theorems 17.1 and 17.2 is that the permutation P in Theorem 17.1 replaces x_j by $x_{P(j)}$ while P in Theorem 17.2 regards $x_{P(j)}$ as the jth variable but does not change the function f. For example, if $f(x_1, x_2, x_3) = x_1 x_2 \oplus x_2 x_3$, $P(1) = 2$, $P(2) = 3$ and $P(3) = 1$, then $f_P(x_1, x_2, x_3) = x_2 x_3 \oplus x_3 x_1$ but $f'(x_2, x_3, x_1) = x_2 x_3 \oplus x_3 x_1$.

Theorem 17.3. *Let f be a nonzero coincident function on $(GF(2))^n$. Then each variable x_j must appear in a monomial of the ANF of f.*

Proof. According to Theorem 16.1, $f(x) = x_1 g(y) \oplus \Psi(g)(y)$ where g is a function on $(GF(2))^{n-1}$. Since f is nonzero, g is nonzero. Then x_1 appears in a monomial of the ANF of f. Therefore, if we regard any other variable x_j as the 1st variable, according to Theorem 17.2, the new function f' is also coincident. By the same reasoning, x_j appears in a monomial of the ANF of f' as well as x_1 in f. □

Theorem 17.4. *Let f be a coincident function on $(GF(2))^n$. Then either the ANF of f has every linear term x_j, or, the ANF does not have any linear term.*

Proof. Assume that the ANF of f has a linear term x_{j_0} where $1 \le j_0 \le n$. Let $i_0 \in \{1, \ldots, n\} - \{j_0\}$. Without loss of generality, we assume that $i_0 < j_0$. Let γ_i denote the vector in $(GF(2))^n$ whose ith coordinate is one and all other coordinates are zero. Let $\gamma_{i,j}$ denote the vector in $(GF(2))^n$ whose ith and jth coordinates are one and all other coordinates are zero. According to Corollary 15.9, $\bigoplus_{\beta \prec \gamma_{i_0,j_0}} g(\beta) = 0$. More precisely, $g(\gamma_{j_0}) \oplus g(\gamma_{i_0}) = 0$. Since the ANF of f has a linear term x_{j_0}, $g(\gamma_{j_0}) = 1$. Therefore we know that $g(\gamma_{i_0}) = 1$. This means that the ANF of f has a linear term x_{i_0}. Since i_0 is arbitrarily included in $\{1, \ldots, n\} - \{j_0\}$, we have proved the theorem. □

Theorem 17.5. *Let f be any nonzero function on $(GF(2))^n$. Then there exists a nonzero function f' on $(GF(2))^n$ such that $f \cdot f'$ is coincident.*

Proof. For fixed f, let f' go through all the functions on $(GF(2))^n$. Since $\#\mathcal{R}_n = 2^{2^n}$ and $\#\aleph_0 = 2^{2^{n-1}}$, there must exit two distinct functions f_1 and f_2 such that $f \cdot f_1 \in \aleph_h$ and $f \cdot f_2 \in \aleph_h$ for some $h \in \aleph_0$. According to Theorem 11.5, $f \cdot (f_1 \oplus f_2)$ is coincident. Set $f' = f_1 \oplus f_2$. Clearly f' is nonzero and then f' is required in the theorem. □

Corollary 17.6. *If f is a coincident function then $f(0) = 0$.*

Proof. Due to Theorem 9.4, the truth table of f can be expressed as ξT_n^*. It is noted that the leftmost column of T_n^* is the all-zero column. Then the first coordinate of ξT_n^* turns out to be zero. This proves that $f(0) = 0$. □

Lemma 17.7. *Let f be a coincident function on $(GF(2))^n$. Then for any integer r with $1 \leq r \leq n-1$ and the r-subset $\{1,\ldots,r\}$ of $\{1,\ldots,n\}$, $f(x_1,\ldots,x_n)|_{x_1=0,\ldots,x_r=0}$ is a coincident function on $(GF(2))^{n-r}$.*

Proof. According to Theorem 16.1, $f(x) = x_1 g(y) \oplus \Psi(g)(y)$ where Ψ has been defined in Definition 11.1. Then $f(0, x_2, \ldots, x_n) = \Psi(g)(x_2, \ldots, x_n)$. Due to Theorem 15.1, $\Psi(g)$ is a coincident function on $(GF(2))^{n-1}$, i.e., $f(0, x_2, \ldots, x_n)$ is a coincident function on $(GF(2))^{n-1}$. Applying the same reasoning to $\Psi(g)$, we know that $f(0, 0, x_3, \ldots, x_n)$ is a coincident function on $(GF(2))^{n-2}$. Repeatedly, we can prove that $f(0, \ldots, 0, x_{r+1}, \ldots, x_n)$ is a coincident function on $(GF(2))^{n-r}$. □

Theorem 17.8. *Let f be a coincident function on $(GF(2))^n$. Then for any integer r with $1 \leq r \leq n-1$ and any r-subset $\{j_1,\ldots,j_r\}$ of $\{1,\ldots,n\}$, $f(x_1,\ldots,x_n)|_{x_{j_1}=0,\ldots,x_{j_r}=0}$ is a coincident function on $(GF(2))^{n-r}$.*

Proof. Let $\{j_1,\ldots,j_r\} \cup \{j_{r+1},\ldots,j_n\} = \{1,\ldots,n\}$. We define a function f': $f'(x_{j_1},\ldots,x_{j_n}) = f(x_1,\ldots,x_n)$. According to Theorem 17.2, f' is coincident. Applying Lemma 17.7 to f', we have proved the theorem. □

18. A Lower Bound on Degree of Coincident Functions

Lemma 18.1. *Let f be a coincident function on $(GF(2))^n$. Then $deg(f) = n$ if and only if $f(1,\ldots,1) = 1$.*

Proof. From the definition of coincident functions, $deg(f) = n \Longleftrightarrow x_1 \cdots x_n$ is a monomial in the ANF of $f \Longleftrightarrow f(1,\ldots,1) = 1$. □

Corollary 18.2. *There precisely exist $2^{2^{n-1}-1}$ coincident functions on $(GF(2))^n$ having a degree n and there precisely exist $2^{2^{n-1}-1}$ coincident functions on $(GF(2))^n$ having a degree less than n.*

Proof. Due to Theorem 9.5, the truth table of a coincident function f on $(GF(2))^n$ is a linear combination of rows of T_n^*. It is noted that the rightmost column of T_n^* contains ones. Then there precisely 50% such linear combinations whose last coordinate is one. Then according to Lemma 18.1, there precisely 50% coincident functions on $(GF(2))^n$ having a degree n. Therefore, due to Theorem 12.1, we have proved the corollary. □

We next indicate that all coincident functions have a high degree even for coincident functions whose degree are less than n.

Theorem 18.3. *Let f be a coincident function on $(GF(2))^n$. Then $deg(f) \geq \lceil \frac{1}{2}n \rceil$. More precisely,*

(i) *$deg(f) \geq \frac{1}{2}n$ where n is even,*
(ii) *$deg(f) \geq \frac{1}{2}(n+1)$ where n is odd.*

Proof. According to Theorem 7.1, $deg(f)+deg(\mu(f)) \geq n$. On the other hand, since f is coincident, f and $\mu(f)$ are identical. Then $2deg(f) \geq n$ and then $deg(f) \geq \frac{1}{2}n$. In particular, when n is odd, it is noted that $deg(f) \geq \frac{1}{2}n$. Since n is odd and $deg(f)$ is integer, $deg(f) \geq \frac{1}{2}(n+1)$. Summarily, $deg(f) \geq \lceil \frac{1}{2}n \rceil$. □

We now indicate that the lower bounds in Theorem 18.3 is tight. For example, $f(x_1, x_2, x_3, x_4) = x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$ is a coincident function on $(GF(2))^4$ having a degree two. $f(x_1, x_2, x_3) = x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2$ is a coincident function on $(GF(2))^3$ having a degree two.

19. Coincident Functions with High Nonlinearity and High Degree

Definition 19.1. The *nonlinearity* of a function f on $(GF(2))^n$, denoted by N_f, is the minimal Hamming distance between f and all affine functions on $(GF(2))^n$, i.e., $N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f, \psi_i)$ where ψ_1, ψ_2, …, $\psi_{2^{n+1}}$ are all the affine functions on $(GF(2))^n$.

It is well-known that For any function f on $(GF(n))$, the nonlinearity N_f of f satisfies $N_f \leq 2^{n-1} - 2^{\frac{1}{2}n-1}$. We can define bent functions, introduced first by Rothaus [2], equivalently as follows: a function f on $(GF(n))$ is said to be *bent* if the nonlinearity N_f reaches the maximum value $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$. Obviously bent functions on $(GF(2))^n$ exist for even n.

19.1. Construction 1 (for Case of Even Variables)

The following statement can be verified straightforwardly.

Lemma 19.2. *Let f_1, f_2 and f_3 be functions on $(GF(2))^n$. Then $d(f_1, f_3) \leq d(f_1, f_2) + d(f_2, f_3)$.*

Theorem 19.3. *Let* $f(x_1, \ldots, x_{2k}) = x_1x_2 \oplus \cdots \oplus x_{2k-1}x_{2k}$. *Set* $h = f \oplus \mu(f)$. *Then* h *is a coincident function on* $(GF(2))^{2k}$ *satisfying (i)* $N_h \geq 2^{2k-1} - 2^{k-1} - k$, *(ii)* $deg(h) \geq 2k - 2$.

Proof. Due to Theorem 15.1, h is coincident. Let ξ and η be the truth tables of f and $\mu(f)$ respectively. Then $\xi \oplus \eta$ is the truth table of h. Let ψ be an affine function on $(GF(2))^{2k}$ and ℓ be the truth table of ψ. By the definition of nonlinearity, $d(\xi, \ell) \geq N_f$. On the other hand, it is obvious that $HW(\eta) = k$. Therefore $d(\xi \oplus \eta, \xi) = k$. Due to Lemma 19.2, $d(\xi, \ell) \leq d(\xi, \xi \oplus \eta) + d(\xi \oplus \eta, \ell)$. Then $N_f \leq k + d(\xi \oplus \eta, \ell)$ or $d(\xi \oplus \eta, \ell) \geq N_f - k$. Since ψ is an arbitrarily affine function, $N_h \geq N_f - k$. It is well-known that f is bent. Then $N_f = 2^{2k-1} - 2^{k-1}$. We then have proved that $N_h \geq 2^{2k-1} - 2^{k-1} - k$. Due to Theorem 7.1, $deg(f) \oplus deg(\mu(f)) \geq 2k$. From the fact $deg(f) = 2$, we know that $deg(\mu(f)) \geq 2k - 2$. Clearly $deg(h) = deg(\mu(f))$, We have proved the theorem. □

Comparing $N_h \geq 2^{2k-1} - 2^{k-1} - k$ in Theorem 19.3 to $2^{2k-1} - 2^{k-1}$, the maximum nonlinearity of functions on $(GF(2))^{2k}$, we know the coincident function in Theorem 19.3 is highly nonlinear.

19.2. **Construction 2 (for Case of Odd Variables)**

Theorem 19.4. *Let* $f(x_1, x_2, \ldots, x_{2k+1}) = x_2x_3 \oplus x_4x_5 \cdots \oplus x_{2k}x_{2k+1}$. *Set* $h = f \oplus \mu(f)$. *Then* h *is a coincident function on* $(GF(2))^{2k+1}$ *satisfying (i)* $N_h \geq 2^{2k} - 2^k - k$, *(ii)* $deg(h) \geq 2k - 1$.

Proof. Due to Theorem 15.1, h is coincident. Let ξ and η be the truth tables of f and $\mu(f)$ respectively. Then $\xi \oplus \eta$ is the truth table of h. Let ψ be an affine function on $(GF(2))^{2k+1}$ and ℓ be the truth table of ψ. By the definition of the nonlinearity, $d(\xi, \ell) \geq N_f$. On the other hand, since $HW(\eta) = k$, $d(\xi \oplus \eta, \xi) = k$. Due to Lemma 19.2, $d(\xi, \ell) \leq d(\xi, \xi \oplus \eta) + d(\xi \oplus \eta, \ell)$. Then $N_f \leq k + d(\xi \oplus \eta, \ell)$ or $d(\xi \oplus \eta, \ell) \geq N_f - k$. Since ψ is an arbitrarily affine function, $N_h \geq N_f - k$. Set $f'(x_2, \ldots, x_{2k+1}) = x_2x_3 \oplus x_4x_5 \cdots \oplus x_{2k}x_{2k+1}$. Then f' is a bent function on $(GF(2))^{2k}$ and then $N_{f'} = 2^{2k-1} - 2^{k-1}$. It is easy to see that $N_f = 2N_{f'} = 2^{2k} - 2^k$. Therefore we have proved that $N_h \geq 2^{2k} - 2^k - k$. Due to Theorem 7.1, $deg(f) \oplus deg(\mu(f)) \geq 2k + 1$. From the fact $deg(f) = 2$, we know that $deg(\mu(f)) \geq 2k + 1 - 2 = 2k + 1$. Clearly $deg(h) = deg(\mu(f))$, We have proved the theorem. □

The nonlinearity $N_h \geq 2^{2k} - 2^k - k$ in Theorem 19.4 is high compared to the maximum nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$ of functions on $(GF(2))^n$,

20. Conclusions

We have established relations between Boolean functions and their Möbius transforms so as to compute the truth table/ANF from the ANF/truth table of a function in different conditions. We have indicated $deg(f)+deg(\mu(f)) \geq n$ where n denotes the number of variables. We have proposed the concept of coincident functions whose ANF is identical with the ANF of its Möbius transforms. We have characterised coincident functions so as to obtain a coincident functions easily. We have studied cryptographic properties such as algebraic degree and nonlinearity.

References

[1] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, Amsterdam, New York, Oxford, 1978.

[2] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.

[3] R. Yarlagadda and J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceedings (Part E)*, 136:112–123, 1989.

[4] Y. Zheng, X. M. Zhang, and Hideki Imai. Restrictions, terms and nonlinearity of boolean functions. *Theoretical Computer Science*, 226:207–223, 1999.