Möbius Transforms, Coincident Boolean Functions and Noncoincidence Property of Boolean Functions [⋆]

Josef Pieprzyk[1], Huaxiong Wang[1,2], and Xian-Mo Zhang[1]

[1] Centre for Advanced Computing - Algorithms and Cryptography
Department of Computing, Macquarie University
Sydney , NSW 2109, Australia
[2] Division of Mathematical Science, School of Physical and Mathematical Science,
Nanyang Technological University, Singapore
josef.pieprzyk,hwaxiong.wang,xianmo.zhang@.mq.edu.au

Abstract. Boolean functions and their Möbius transforms are involved in logical calculation, digital communications, coding theory and modern cryptography. So far, little is known about the relations of Boolean functions and their Möbius transforms. This work is composed of three parts. In the first part we present relations between a Boolean function and its Möbius transform so as to convert the truth table/ANF to the ANF/truth table of a function in different conditions. In the second part we focus on the special case when a Boolean function is identical to its Möbius transform. We call such functions coincident. In the third part we generalise the concept of coincident functions and indicate that any Boolean function has the coincidence property even if it is not coincident.

Key Words: Boolean Functions, Möbius Transform, Coincident Functions, h-noncoincident Functions, Anti-coincident Functions, Noncoincident Weight.

1 Introduction

Boolean functions and their Möbius Transform have interests in logical calculations [9], digital communications [9] and coding theory [4] Boolean functions play a basic role in questions of complexity [3]. The properties of Boolean functions play a critical role in modern cryptography [2]. However, little is known about the relations of Boolean functions and their Möbius Transforms. In the practice we need covert the ANF of a Boolean function to its truth table and vice versa. We know that both translations are equivalent to the Möbius transform [1].

Throughout this paper we use the following notations. The vector space of n-tuples 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

[⋆] Part of this work was presented in *Boolean Functions: Cryptography and Application 2007 (BFCA'07)* [5] *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 binary vector defined by $(f(\alpha_0),\ f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$. The *Hamming weight* of a binary vector 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 $HW(f)$. A function 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 $d(f, g) = HW(f \oplus g)$ where $\oplus$ denotes the Boolean sum.

A function f can be uniquely represented by its *Algebraic Normal Form* (ANF):

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

where $\bigoplus$ denotes the binary sum, $\alpha = (a_1, \ldots, a_n)$ and g is also a function on $(GF(2))^n$. The function g is called the **<u>Möbius transform</u>** of f. Each $x_1^{a_1} \cdots x_n^{a_n}$ is called a *monomial (term)* of f. The *algebraic degree*, or *degree*, of f, denoted by $deg(f)$, is defined as $deg(f) = \max_{(a_1,\ldots,a_n)} \{HW(a_1, \ldots, a_n) \mid g(a_1, \ldots, a_n) = 1\}$.

It is noted that the classical Möbius functions, used in combinatorics and number theory, was first introduced in 1831 by A. F. Möbius. By the principle of the classical Möbius function, the Möbius transform of Boolean functions was proposed 1950s (see, for example, [7]).

Besides using Formula (1), in this work we derive relations between a Boolean function and its Möbius transform. By using those relations, we can compute the Möbius transform of a Boolean function in different conditions. Those relations also enable us to find new properties of Boolean functions. We further propose the concept of coincident functions. A Boolean function f is called coincident if it is identical to its Möbius transform. 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 coefficient $g(a_1, a_2, a_3)$ of each term $x_1^{a_1} x_2^{a_2} x_3^{a_3}$. For example, since the coefficient of $x_1^1 x_2^0 x_3^1$ is 1, $g(1, 0, 1) = 1$. In this way we obtain the truth table of g: (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 $(GF(2))^3$. For any coincident function, we do not need to compute its Möbius transform because its Möbius transform is exactly itself. Although coincident functions seem to be special Boolean functions, any Boolean function is related to a coincident function. This can been observed, for instance, from the fact that for an arbitrary Boolean function f and its Möbius transform g, the expression $f \oplus g$ is coincident. We extensively study the algebraic properties of coincident functions, especially, their characterisations. We generalise the concept of coincident functions so that the coincident property is applicable to all Boolean functions. We call the number of the vectors α such that $f(\alpha) \neq g(\alpha)$, noncoincident weight of f, denoted by $NCW(f)$. Here we study the decomposition of Boolean functions into their coincident and noncoincident components and we are going to investigate properties associated with NCW such as noncoincident indicator functions, h-noncoincident functions, anti-coincident functions and NCW-balanced functions. Those let us investigate Boolean functions from new perspectives and propose more questions in the applications of Boolean functions.

2 Part I: Möbius Transforms of Boolean Functions

By definition, converting f to its Möbius transform g (see Formula (1)) is equivalent to converting the truth table of f to its ANF. In this work we suggest three methods to compute the Möbius transform of a Boolean function: using matrices, using polynomials and using recursive formulas.

2.1 Computing $\mu(f)$ by Matrices

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

Notation 1 *Let $\mathcal{R}_n$ denote the set of all functions on $(GF(2))^n$. We define a mapping, denoted by μ, from $\mathcal{R}_n$ to $\mathcal{R}_n$ by the following rule: $\mu(f) = g$ if and only if g is the Möbius transform of f (see Formula (1)).*

By definition, it is easy to verify

Theorem 1. *μ, defined in Notation 1, is a one-to-one linear mapping from $\mathcal{R}_n$ to $\mathcal{R}_n$.*

Proof. For any $f_1, f_2 \in \mathcal{R}_n$ with $f_1 \neq f_2$, from (1), we know that $\mu(f_1) \neq \mu(f_2)$. Conversely, for any $g_1, g_2 \in \mathcal{R}_n$ with $g_1 \neq g_2$, from (1), we know that $f_1 \neq f_2$ where f_1 and f_2 are translated from g_1 and g_2 by (1) respectively. Therefore μ is a one-to-one correspondence between $\mathcal{R}_n$ and $\mathcal{R}_n$. Finally, from (1), we know that μ^{-1} is a linear transformation on $\mathcal{R}_n$ so is μ. The proof is completed. □

Notation 2 *We define $2^n \times 2^n$ (0, 1)-matrix, denoted by T_n, such that the ith row of T_n ($n \geq 1$) 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. In addition, we define $T_0 = 1$.*

Theorem 2. *T_n, defined in Notation 2, satisfies $T_s = \begin{bmatrix} T_{s-1} & T_{s-1} \\ O_{2^{s-1}} & T_{s-1} \end{bmatrix}$, 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. By definition, the 0th row of T_1 is the truth table of the constant function $f(x_1) = x_1^0 = 1$ and the 1st row of T_1 is the truth table of the function $f(x_1) = x_1$. Then $T_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. We call Notation 2 where $T_0 = 1$. Then the theorem holds for $n = 1$. 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 $x_1^{a_1}\cdots x_s^{a_s}= x_1x_2^{a_2}\cdots x_s^{a_s}$. 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 1. By using Theorem 2, 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 $x_1^1x_2^0x_3^1=x_1x_3$.

Lemma 1. *The matrix T_s over GF(2) has the following properties: (i) $T_s^2=I_{2^s}$ where I_{2^s} is the $2^s\times 2^s$ identity matrix, (ii) $(T_s\oplus I_{2^s})^2=0_{2^s}$, (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. *Let $f,g\in\mathcal{R}_n$ where $\mathcal{R}_n$ is defined in Notation 1. 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). We 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 (iii). 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 (i). Therefore (i) $\Longleftrightarrow$ (iii). Symmetrically, (ii) $\Longleftrightarrow$ (iv). Due to (i) of Lemma 1, (iii) $\Longleftrightarrow$ (iv). The proof is completed. □

It is noted that a computationally efficient method to compute the ANF from the truth table of a function and vice versa were previously provided by Carlet, consequently, he already found the equivalence between (i) and (ii) of Theorem 3. These were surveyed in [1]. However we regain the equivalence here by using a different concept. Theorem 3 enables us to compute the truth table/ANF from the ANF/truth table of a function by using the matrix T_n.

Example 2. Assume that we know the ANF of $f\in\mathcal{R}_3$: $f(x_1,x_2,x_3)=1\oplus x_2\oplus x_1\oplus x_2x_3\oplus x_1x_2x_3$. Set $g=\mu(f)$. From the coefficient of $x_1^{a_1}x_2^{a_2}x_3^{a_3}$, we know $g(a_1,a_2,a_3)$. For example, since the coefficient of $x_1^1x_2^1x_3^0$ is 0, $g(1,1,0)=0$. In this way we know that g or $\mu(f)$ has the truth table (10111001). By using Theorem 3, (10111001)T_3= (11010011) is the truth table of f.

In the next example we consider the converse of the problem in Example 2.

Example 3. Assume that we know the truth table of function $f \in \mathcal{R}_3$: (11010011). By using Theorem 3, (11010011)T_3= (10111001) is the truth table of g or $\mu(f)$. From $g(a_1, a_2, a_3)$, we know the coefficient of $x_1^{a_1} x_2^{a_2} x_3^{a_3}$. For example, since $g(0, 1, 1) = 1$, $x_1^0 x_2^1 x_3^1$ appears in the ANF of f. In this way we obtain the ANF of f: $f(x_1, x_2, x_3) = 1 \oplus x_2 \oplus x_1 \oplus x_2 x_3 \oplus x_1 x_2 x_3$.

2.2 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 $D_\alpha \in \mathcal{R}_n$ 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 $f \in \mathcal{R}_n$, we have

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

For any two functions $f, f' \in \mathcal{R}_n$, $f(x) \oplus f'(x) = \bigoplus_{\alpha \in (GF(2))^n} (f(\alpha) \oplus f'(\alpha)) D_\alpha(x)$ 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 the fact that $D_\alpha(\beta) = \begin{cases} 1 \text{ if } \beta = \alpha \\ 0 \text{ if } \beta \neq \alpha \end{cases}$.

Lemma 2. *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 the equivalence between (i) and (ii) in Theorem 3, (i) and (ii) in the lemma are equivalent. Therefore we only need to prove (ii). Let $\alpha = (a_1, \ldots, a_n)$ be the binary representation of an integer i. It is noted that the truth table of $D_\alpha(x)$ is all-zero vector of length 2^n except for the ith coordinate. By the definition of T_n, the truth table ξ of $x_1^{a_1} \cdots x_n^{a_n}$ is the ith row of T_n. According to Theorem 3, $\eta = \xi T_n$ is the truth table of $\mu(x_1^{a_1} \cdots x_n^{a_n})$. Due to (i) of Lemma 1, η is all-zero vector of length 2^n except for the ith coordinate. Therefore $\mu(x_1^{a_1} \cdots x_n^{a_n})$ and $D_\alpha(x)$ have the same truth table and then (ii) holds. □

Due to Formula (2) and Lemma 2, we can state as follows.

Theorem 4. *Let $f \in \mathcal{R}_n$. Then $\mu(f)(x) = \bigoplus_{\alpha \in (GF(2))^n} f(\alpha) x_1^{a_1} \cdots x_n^{a_n}$.*

2.3 Computing $\mu(f)$ by Recursive Formulas

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

Theorem 5. *As we know, any function $f \in \mathcal{R}_n$ can be expressed 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, 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, 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 $\mu(f)(x) = x_1(\mu(g)(y) \oplus \mu(h)(y)) \oplus \mu(h)(y)$. □

By Theorem 5, we can reduce the size of Möbius Transform.

2.4 Properties of Möbius Transforms

According to the relations between the truth table and the ANF of a Boolean function, we can find more properties of Boolean functions via their Möbius transforms.

Lemma 3. *$f(0) = \mu(f)(0)$ for every Boolean function f.*

Proof. Let $f \in \mathcal{R}_n$ and $g = \mu(f)$. It is noted that $g(0) = 1 \Longrightarrow x_1^0 \cdots x_n^0$ or constant 1 appears in the ANF of $f \Longrightarrow f(0) = 1$. □

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

Theorem 6. *Let $f \in \mathcal{R}_n$ and $g = \mu(f)$. Then $\mu(f_P) = g_P$ where P is defined in Notation 4.*

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, $\mu(f_P) = g_P$. □

We note that the permutation P in Theorem 6 defined on $\{1, \ldots, n\}$ cannot be extended to be a permutation on $(GF(2))^n$. This can be seen from the following example. It is easy to verify that $f(x_1, x_2) = x_1 \oplus x_1 x_2$ has the Möbius Transform $\mu(f)(x_1, x_2) = x_2$. Set a nonsingular linear transformation on $(GF(2))^2$: $x_1 = y_2$, $x_2 = y_1 \oplus y_2$. It is easy to see that $f(x_1, x_2) = f(y_2, y_1 \oplus y_2) = y_1 y_2$ whose Möbius Transform is $y_1 y_2$.

The following theorem explores a relation between degrees of a Bollean function and its Möbius transform.

Theorem 7. *Let $f \in \mathcal{R}_n$ be nonzero. 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 $f \in \mathcal{R}_n$. We can express f as $f(x) = x_1 g(y) \oplus h(y)$ where $x = (x_1, \ldots, x_s)$, $y = (x_2, \ldots, x_s)$, $g, h \in \mathcal{R}_{s-1}$. According to Theorem 5, $\mu(f)(x) = x_1(\mu(g)(y) \oplus \mu(h)(y)) \oplus \mu(h)(y)$. 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 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 2, $\mu(f)$ is the constant one. Then $deg(f) + deg(\mu(f)) = n + 0 = n$.

3 Part II: Coincident Boolean Functions

3.1 Concept of Coincident Boolean Functions

In this section we propose a special kind of Boolean functions - so called coincident functions.

Definition 1. *Let $f \in \mathcal{R}_n$. 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.

By Definition 1 and Theorem 3, we can conclude

Theorem 8. *Let $f \in \mathcal{R}_n$ and $g = \mu(f)$. Denote the truth tables of f and g by ξ and η respectively. 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 4. Consider the function $f \in \mathcal{R}_4$:
$f(x_1, x_2, x_3, x_4) = x_2x_4 \oplus x_2x_3 \oplus x_1x_2 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3$. Set $g = \mu(f)$. From the coefficient of the term $x_1^{a_1}x_2^{a_2}x_3^{a_3}x_4^{a_4}$, we know $g(a_1, a_2, a_3, a_4)$. For

example, since coefficient of the term $x_1^1x_2^1x_3^1x_4^0$ is 1, $g(1,1,1,0)=1$. In this way we obtain the truth table of g or $\mu(f)$: (0000011000011110). By computing, the truth table of f is also (0000011000011110). Then $f \in \mathcal{R}_4$ is coincident.

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

3.2 Characterisations and Constructions of Coincident Functions (by Matrices)

In this section we characterise coincident functions by using matrices so as to construct a coincident function directly from the matrix T^*.

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

Due to Theorem 8, we can state as follows.

Theorem 9. *Let* $f \in \mathcal{R}_n$ *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 4. *(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)* $T_nT_n^* = T_n^*T_n = T_n^*$.

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 1 respectively. □

Theorem 10. *Let* $f \in \mathcal{R}_n$. *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 a (0, 1)-vector of length* 2^{n-1}.

Proof. Assume that (i) holds. Denote the truth table of f by (ξ_1, ξ_2) where each ξ_i is a (0, 1)-vector of length 2^{n-1}. Due to Theorem 9, we know that $(\xi_1, \xi_2)T_n^* = (\xi_1, \xi_2)\begin{bmatrix} T_{n-1}^* & T_{n-1} \\ O_{2^{n-1}} & T_{n-1}^* \end{bmatrix} = 0$ where 0 denotes the all-zero vector of length 2^n. Therefore $\xi_1 T_{n-1}^* = 0$ and $\xi_1 T_{n-1} \oplus \xi_2 T_{n-1}^* = 0$. From the two equations, we know that $\xi_1(T_{n-1}^* \oplus T_{n-1}) \oplus \xi_2 T_{n-1}^* = 0$ and then $\xi_1 \oplus \xi_2 T_{n-1}^* = 0$ or $\xi_1 = \xi_2 T_{n-1}^*$. Thus the truth table of f can be expressed as $(\xi_2 T_{n-1}^*, \xi_2)$. This proves that (ii) holds. We then have proved (i) $\Longrightarrow$ (ii). Assume that (ii) holds, i.e., the truth table of f can be expressed as $(\zeta T_{n-1}^*, \zeta)$. Let ϑ be any (0, 1)-vector of length 2^{n-1}. Set $\zeta = \zeta' \oplus \vartheta T_{n-1}^*$. Due to Lemma 4, $\zeta T_{n-1}^* = \zeta' T_{n-1}^*$. Therefore

$(\zeta T^*_{n-1}, \zeta)$= $(\zeta' T^*_{n-1}, \zeta' \oplus \vartheta T^*_{n-1})$ and then (iii) holds. We then have proved (ii) $\Longrightarrow$ (iii). Assume that (iii) holds, i.e., the truth table of f can be expressed as $(\zeta T^*_{n-1}, \zeta \oplus \vartheta T^*_{n-1})$ where both ζ and ϑ are (0, 1)-vector of length 2^{n-1}. By using Lemma 4, we know that $(\zeta T^*_{n-1}, \zeta \oplus \vartheta T^*_{n-1})T^*_n = 0$. Due to Theorem 9, f is coincident. This proves (iii) $\Longrightarrow$ (i). □

Theorem 11. *Let $f \in \mathcal{R}_n$. 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.*

Proof. The sufficiency is true due to Theorem 9 and Lemma 4. We now prove the necessity. Assume that f is coincident. According to Theorem 10, 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}. By using Lemma 4, it is easy to verify that $(\zeta T^*_{n-1}, \zeta) = (\zeta T_{n-1}, 0)T^*_n$. This proves the necessity. □

We can state Theorem 11 equivalently.

Theorem 12. *Let $f \in \mathcal{R}_n$. Then f is coincident if and only if the truth table of f is a linear combination of rows of T^*_n.*

By using Theorem 12, we can construct coincident functions by using Theorems 10, 11 and 12.

3.3 Operations of Coincident Functions

According to Theorem 11, the following statement holds.

Corollary 1. *If both $f, g \in \mathcal{R}_n$ are coincident then $f \oplus g$ is coincident.*

But, $f \cdot g$ is not necessarily coincident even both f and g are coincident. For example, both $f_1 = x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3 \in \mathcal{R}_3$ and $f_2 = x_2x_3 \oplus x_1x_2 \oplus x_1x_2x_3 \in \mathcal{R}_3$ are coincident but $f_1f_2 = x_2x_3 \in \mathcal{R}_3$ is not coincident. 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 [10].

Lemma 5. *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 6. *$T_n = T_p \times T_{n-p}$, $p = 1, 2, \ldots, n-1$, 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 7. *Let $f_1 \in \mathcal{R}_m$ and $f_2 \in \mathcal{R}_n$. Define a function $\in \mathcal{R}_{m+n}$ 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 f.*

Theorem 13. *Let $f_1 \in \mathcal{R}_m$ and $f_2 \in \mathcal{R}_n$ be coincident. Define a function $f \in \mathcal{R}_{m+n}$ as $f(y,z) = f_1(y) \cdot f_2(z)$. Then $f \in \mathcal{R}_{m+n}$ is coincident.*

Proof. Let ξ_1 and ξ_2 denote the truth tables of f_1 and f_2 respectively. Due to Lemma 7, $\xi_1 \times \xi_2$ is the truth table of a coincident function f. By using Lemmas 6 and 5, $(\xi_1 \times \xi_2)T_{m+n}$= $(\xi_1 \times \xi_2)(T_m \times T_n)$= $(\xi_1 T_m) \times (\xi_2 T_n)$. According to Theorem 8, $\xi_1 T_m = \xi_1$ and $\xi_2 T_n = \xi_2$. Therefore $(\xi_1 \times \xi_2)T_{m+n}$= $\xi_1 \times \xi_2$. Again, Theorem 8, we know that $\xi_1 \times \xi_2$ is the truth table of a coincident function $\in \mathcal{R}_{m+n}$. □

Although the product of two coincident functions is not necessarily coincident, the operation is special.

Theorem 14. *Let both $f, f' \in \mathcal{R}_n$ be coincident 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. □

3.4 A Classification and Enumeration of Coincident Functions

Although coincident functions are very special Boolean functions, any Boolean function is related to a coincident function.

Definition 2. *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 2, Ψ is a linear mapping.

Notation 7 *For each coincident h, set $\aleph_h = \{f | \Psi(f) = h\}$.*

Lemma 8. *$\aleph_0$ is the collection of all coincident functions $\in \mathcal{R}_n$ and $\aleph_0$ is a linear subspace of $\mathcal{R}_n$ where $\mathcal{R}_n$ is defined in Notation 1.*

Proof. Let $f \in \mathcal{R}_n$ and ξ be the truth table of f. Then $f \in \aleph_0 \iff \Psi(f) = 0 \iff \xi T_n^* = 0 \iff f$ is coincident. This proves that $\aleph_0$ is the collection of all coincident functions. According to Corollary 1, all coincident functions form a linear subspace of $\mathcal{R}_n$. □

Since Ψ is a linear mapping, applying linear algebra to Ψ, $\aleph_0$ and $\mathcal{R}_n$, we obtain the following results (Theorems 15, 16 and Corollary 2).

Theorem 15. *Let $f_1, f_2 \in \mathcal{R}_n$. 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 16. *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 2. *$\mathcal{R}_n$, 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 $h \neq h'$.*

Lemma 9. *All the 2^{n-1} rows of the matrix $\left[T_{n-1}^* \; T_{n-1}\right]$ form a basis of rows of T_n^*, where $n = 1, 2, \ldots$.*

Proof. Due to Lemma 4, $T_n^* = \begin{bmatrix} T_{n-1}^* & T_{n-1} \\ 0_{2^{n-1}} & T_{n-1}^* \end{bmatrix}$. Again, due to Lemma 4, $\begin{bmatrix} I_{2^{n-1}} & 0_{2^{n-1}} \\ T_{n-1}^* & I_{2^{n-1}} \end{bmatrix} \begin{bmatrix} T_{n-1}^* & T_{n-1} \\ 0_{2^{n-1}} & 0_{2^{n-1}} \end{bmatrix} = \begin{bmatrix} T_{n-1}^* & T_{n-1} \\ 0_{2^{n-1}} & T_{n-1}^* \end{bmatrix}$. It is noted that T_{n-1} has a rank 2^{n-1}. The proof is completed. □

Due to Theorem 12 and Lemma 9, we have Theorems 17 and 18 where Theorem 17 is an improvement on Theorem 12.

Theorem 17. *Let $f \in \mathcal{R}_n$. Then f is coincident if and only if the truth table of f is a linear combination of rows of $\left[T_{n-1}^* \; T_{n-1}\right]$, where $n = 1, 2, \ldots$.*

Theorem 18. *There precisely exist $2^{2^{n-1}}$ coincident functions $\mathcal{R}_n$ that form a 2^{n-1}-dimensional linear subspace of $\mathcal{R}_n$ where $\mathcal{R}_n$ is defined in Notation 1.*

Example 5. According to Theorem 18, there precisely exist $2^{2^{3-1}} = 16$ coincident functions on $(GF(2))^3$. According to Theorem 17, all the linear combinations of rows of $[T_2^*, T_2] = \begin{bmatrix} 0\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,0\,1\,0\,1\,0\,1 \\ 0\,0\,0\,1\,0\,0\,1\,1 \\ 0\,0\,0\,0\,0\,0\,0\,1 \end{bmatrix}$ are the truth tables of coincident functions of 3 variables: (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 of 3 variables: $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3$, $x_2x_3 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_1x_2x_3$, $x_1x_3 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_1x_3 \oplus x_1x_2$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_2$, $x_2x_3 \oplus x_1x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_2x_3$, $x_2x_3 \oplus x_1x_2$, 0

It is noted that $\#\aleph_h = \#\aleph_0$ for all $h \in \alpha_0$ where $\#X$ denotes the cardinality of the set X, i.e., the number of elements in the set X. Due to Corollary 2, we can state as follows.

Theorem 19. *$\mathcal{R}_n$, the set of all functions on $(GF(2))^n$, can be divided into $2^{2^{n-1}}$ cosets: $\mathcal{R}_n = \bigcup_{h\in\aleph_0} \aleph_h$, where $\aleph_h$ is defined in Notation 7 and $\#\aleph_h = 2^{2^{n-1}}$ for each $h \in \alpha_0$.*

By using the term of linear algebra [6], we can call $\{\aleph_h | h \in \aleph_0\}$ *quotient space*, denoted by $\mathcal{R}_n/\aleph_0$ (read " $\mathcal{R}_n$ mod $\aleph_0$"). Theorem 19 means that $\#(\mathcal{R}_n/\aleph_0)$ $= \#\aleph_0 = 2^{2^{n-1}}$.

3.5 Characterisations and Constructions of Coincident Functions (by Polynomials)

In this section we characterise coincident functions by using polynomials so as to write the Möbius transform of a Boolean function immediately.

Lemma 10. *Let $f \in \mathcal{R}_n$. Then $\Psi(f) = h$ if and only if $f \oplus \mu(f) = h$ where Ψ is defined in Definition 2.*

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

Theorem 20. *Let $h \in \mathcal{R}_n$. Then the following statements are equivalent: (i) h is coincident, (ii) there exists a function $f \in \mathcal{R}_n$ such that $h = \Psi(f)$, i.e., $h = f \oplus \mu(f)$, (iii) $\Psi(h)$ is the zero function.*

Proof. Due to Theorem 11, (i) $\iff$ (ii). Due to Theorem 9, (i) $\iff$ (iii). □

Due to Lemma 2 and Theorem 20, we can state as follows.

Lemma 11. *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.*

Again, by using Theorem 20 and Lemma 2, we can state more generally.

Theorem 21. *Let $h \in \mathcal{R}_n$. 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 $\alpha = (a_1, \ldots, a_n) \in (GF(2))^n$.*

Due to Formulas (1), (2) and Definition 1, we conclude

Theorem 22. *Let $f \in \mathcal{R}_n$ 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) $f(x) = \bigoplus_{\alpha\in(GF(2))^n} g(\alpha)D_\alpha(x)$.*

By the way, we can construct coincident functions by using Theorems 20, 21 and 22.

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 can be found in p.372 of [4].

Lemma 12. *Let $f \in \mathcal{R}_n$ 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 $\bigoplus_{\beta \preceq \alpha} f(\beta) = 1$.*

Theorem 23. *Let $f \in \mathcal{R}_n$. Then f is coincident if and only if for any $\alpha \in (GF(2))^n$, $\bigoplus_{\beta \prec \alpha} f(\beta) = 0$.*

Proof. Let $g = \mu(f)$. Due to Lemma 12, $g(\alpha) = \bigoplus_{\beta \preceq \alpha} f(\beta)$ for any $\alpha \in (GF(2))^n$. Then f is coincident $\Longleftrightarrow$ $f = g$ $\Longleftrightarrow$ for each $\alpha \in (GF(2))^n$, $f(\alpha) = \bigoplus_{\beta \preceq \alpha} f(\beta)$ or $\bigoplus_{\beta \prec \alpha} f(\beta) = 0$. □

3.6 Characterisations and Constructions of Coincident Functions (by Recursive Formulas)

In this section we characterise coincident functions by recursive relations so as to show the relation between coincident functions and arbitrary functions.

Theorem 24. *Let $f \in \mathcal{R}_n$. Then f is coincident if and only if f can be expressed as $f(x) = x_1 g(y) \oplus \Psi(g)(y)$ where $g \in \mathcal{R}_{n-1}$ and Ψ has been defined in Definition 2. 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 $g, h \in \mathcal{R}_{n-1}$, due to Theorem 5, $\mu(f)(x) = x_1 \mu(g \oplus h)(y) \oplus \mu(h)(y)$. 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 20). Due to Lemma 10, $g \oplus \mu(g) = \Psi(g)$. This proves the main part of the theorem. Clearly if f is nonzero then g is nonzero. □

Recursively applying Theorem 24, we state as follows.

Theorem 25. *Let $f \in \mathcal{R}_n$. Then f is coincident if and only if there exists a function $f_i \in \mathcal{R}_{n-i}$, $i = 1, \ldots, n$, 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*
$x_i f_i(x_{i+1}, \ldots, x_n) \oplus \cdots \oplus x_{n-1} f_{n-1}(x_n) \oplus f_n(x_n) =$
$\Psi(x_{i-1} f_{i-1}(x_i, \ldots, x_n) \oplus \cdots \oplus x_{n-1} f_{n-1}(x_n) \oplus f_n(x_n))$, $i = 2, \ldots, n$.

By the way, we can construct coincident functions by using Theorems 24 and 25.

3.7 Properties of Coincident Functions

Coincident functions have some interesting properties.

Theorem 26. *Let $f \in \mathcal{R}_n$ 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 $f_P = g_P$. By Theorem 6, $\mu(f_P) = g_P$. Then we have $\mu(f_P) = f_P$ and then f_P is coincident. The converse is true because we can set $f_P = f'$ then $f'_{P^{-1}} = f$. □

We note that the permutation P in Theorem 26 defined on $\{1,\ldots,n\}$ cannot be extended to be a permutation on $(GF(2))^n$. This can be seen from the following example. From Example 5, $f(x_1,x_2,x_3) = x_1x_2x_3 \in \mathcal{R}_3$ is coincident. Set a nonsingular linear transformation on $(GF(2))^3$: $x_1 = y_1 \oplus y_2$, $x_2 = y_2$, $x_3 = y_3$. It is easy to see that $f(x_1,x_2,x_3) = y_1y_2y_3 \oplus y_2y_3 \in \mathcal{R}_3$ is not coincident.

Theorem 27. *Let $f \in \mathcal{R}_n$ 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 22. □

A difference between Theorems 26 and 27 is that the permutation P in Theorem 26 replaces x_j by $x_{P(j)}$ while P in Theorem 27 regards $x_{P(j)}$ as the jth variable but does not change the function f. For example, if $f(x_1,x_2,x_3) = x_1x_2 \oplus x_2x_3$, $P(1) = 2$, $P(2) = 3$ and $P(3) = 1$, then $f_P(x_1,x_2,x_3) = x_2x_3 \oplus x_3x_1$ but $f'(x_2,x_3,x_1) = x_1x_2 \oplus x_2x_3$ where f' is mentioned in Theorem 27.

Theorem 28. *Let $f \in \mathcal{R}_n$ be nonzero and coincident. Then each variable x_j appears in a monomial of the ANF of f.*

Proof. By Theorem 24, $f(x) = x_1g(y) \oplus \Psi(g)(y)$ where $g \in \mathcal{R}_{n-1}$. 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, By Theorem 27, 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. □

Corollary 3. *Any coincident function h satisfies $h(0) = 0$.*

Proof. According to Theorem 20, there exists a function $f \in \mathcal{R}_n$ $h = f \oplus \mu(f)$. Due to Lemma 3, $h(0) = 0$. □

Theorem 29. *Let $f \in \mathcal{R}_n$ be coincident. 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 $1 \leq j_0 \leq n$. 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 Theorem 23, $\bigoplus_{\beta \prec \gamma_{i_0,j_0}} g(\beta) = 0$. More precisely, $g(0) \oplus g(\gamma_{j_0}) \oplus g(\gamma_{i_0}) = 0$. Due to Corollary 3, $g(0) = 0$. 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. □

Lemma 13. *Let $f \in \mathcal{R}_n$ be coincident. 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 in $\mathcal{R}_{n-r}$.*

Proof. According to Theorem 24, $f(x) = x_1 g(y) \oplus \Psi(g)(y)$ where Ψ has been defined in Definition 2. Then $f(0, x_2, \ldots, x_n) = \Psi(g)(x_2, \ldots, x_n)$. Due to Theorem 20, $\Psi(g)$ is a coincident function in $\mathcal{R}_{n-1}$, i.e., $f(0, x_2, \ldots, x_n)$ is a coincident function in $\mathcal{R}_{n-1}$. Applying the same reasoning to $\Psi(g)$, we know that $f(0, 0, x_3, \ldots, x_n)$ is a coincident function on $\mathcal{R}_{n-2}$. Repeatedly, we can prove that $f(0, \ldots, 0, x_{r+1}, \ldots, x_n)$ is a coincident function in $\mathcal{R}_{n-r}$. □

Theorem 30. *Let $f \in \mathcal{R}_n$ be coincident. 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 in $\mathcal{R}_{n-r}$.*

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 27, f' is coincident. Applying Lemma 13 to f', we have proved the theorem. □

Lemma 14. *There precisely exist $2^{2^{n-1}-1}$ coincident functions of n variables having a degree n and there precisely exist $2^{2^{n-1}-1}$ coincident functions of n variables having a degree less than n.*

Proof. Due to Theorem 12, the truth table of a coincident function $f \in \mathcal{R}_n$ 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. By Definition 1, for any coincident function $f \in \mathcal{R}_n$, $deg(f) = n$ if and only if $f(1, \ldots, 1) = 1$. Therefore there precisely 50% coincident functions $\in \mathcal{R}_n$ having a degree n. Therefore, due to Theorem 18, 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 31. *Let $f \in \mathcal{R}_n$ be nonzero and coincident. 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, $deg(f) + deg(\mu(f)) \geq n$. 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 bound in Theorem 31 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 $\in \mathcal{R}_3$ 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 $\in \mathcal{R}_3$ having a degree two.

3.8 Coincident Functions with High Nonlinearity and High Degree

The *nonlinearity* N_f of $f \in \mathcal{R}_n$ is defined as $N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f, \psi_i)$ where ψ_1, ψ_2, ..., $\psi_{2^{n+1}}$ are all the affine functions $\in \mathcal{R}_n$. It is well-known that for any function $f \in \mathcal{R}_n$, 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 [8], equivalently as follows: a function $f \in \mathcal{R}_n$ is said to be *bent* if the nonlinearity N_f reaches the maximum value $N_f = 2^{n-1} - 2^{\frac{1}{2}n-1}$. Therefore bent functions of n variables exist for even n only.

Construction 1 (for Case of Even Variables) The following statement can be verified straightforwardly.

Lemma 15. *Let f_1, f_2 and $f_3 \in \mathcal{R}_n$. Then $d(f_1, f_3) \leq d(f_1, f_2) + d(f_2, f_3)$.*

Theorem 32. *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 (i) $h \in \mathcal{R}_{2k}$ is coincident, (ii) $N_h \geq 2^{2k-1} - 2^{k-1} - k$, (iii) $deg(h) \geq 2k-2$.*

Proof. Due to Theorem 20, 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 $\psi \in \mathcal{R}_{2k}$ be affine 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 15, $d(\xi, \ell) \leq d(\xi, \xi \oplus \eta) + d(\xi \oplus \eta, \ell)$. 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, $deg(f) \oplus deg(\mu(f)) \geq 2k$. Since $deg(f) = 2$, we know that $deg(\mu(f)) \geq 2k-2$. Clearly $deg(h) = deg(\mu(f))$, We have proved the theorem. □

Construction 2 (for Case of Odd Variables)

Theorem 33. *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 (i) $h \in \mathcal{R}_{ak+1}$ is coincident, (ii) $N_h \geq 2^{2k} - 2^k - k$, (iii) $deg(h) \geq 2k-1$.

Proof. By using the same reasoning in the proof of Theorem 32, we have $N_h \geq N_f - k$. 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 of $2k$ variables 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, $deg(f) \oplus deg(\mu(f)) \geq 2k+1$. Since $deg(f) = 2$, we know that $deg(\mu(f)) \geq 2k+1-2 = 2k-1$. Clearly $deg(h) = deg(\mu(f))$. We have proved the theorem. □

Both coincident functions in Theorems 32 and 33 are highly nonlinear, comparing to the maximum nonlinearity $2^{n-1} - 2^{\frac{1}{2}n-1}$ of functions $\in \mathcal{R}_n$. Obviously the two coincident functions are also of high algebraic degree.

4 Part III: Noncoincidence Property of Boolean Functions

4.1 *h*-noncoincident Functions

In this section we examine general Boolean functions, that are not necessarily coincident, by viewing the coincident property.

Definition 3. *Let $f \in \mathcal{R}_n$. Define a $h \in \mathcal{R}_n$ such that $h(\alpha) = 1$ if and only if $f(\alpha) \neq \mu(f)(\alpha)$. Then h is called* noncoincident indicator function *of f and f is called a h-*noncoincident function.

For example, $f(x_1, x_2, x_3) = x_2x_3 \oplus x_1x_3 \oplus x_1x_2$ is a h-noncoincident function where $h(x_1, x_2, x_3) = x_1x_2x_3$ and then h is the noncoincident indicator function of f. Clearly a function is a 0-noncoincident function if and only it is a coincident function defined in Definition 1.

Theorem 34. *Given $f, h \in \mathcal{R}_n$ and their truth tables denoted by ξ and η respectively. Then the following statements are equivalent: (i) f is h-noncoincident, (ii) $\mu(f)$ is h-noncoincident, (iii) $f \oplus \mu(f) = h$, (iv) $\xi \oplus \xi T_n = \eta$, (v) $\xi T_n^* = \eta$ and (vi) $f \in \aleph_h$.*

Proof. By definition, (i) $\Longleftrightarrow$ (iii). By symmetry, we claim that (ii) $\Longleftrightarrow$ (iii). The equivalence (iii) $\Longleftrightarrow$ (iv) holds because of the relation between Boolean functions and their truth tables. The equivalence (iv) $\Longleftrightarrow$ (v) is true due to the definition of T_n^*. Due to the definition of $\aleph_f$, the relation (vi) $\Longleftrightarrow$ (iii) holds as well. □

Corollary 4. *(i) The indicator function h of any $f \in \mathcal{R}_n$ is coincident,*

(ii) for any coincident $h \in \mathcal{R}_n$, there precisely exist $2^{2^{n-1}}$ h-noncoincident functions $\in \mathcal{R}_n$.

Proof. (i) holds due to Theorems 34 and 20. (ii) holds due to Theorems 34 and 18. □

Corollary 5. *For any $f \in \mathcal{R}_n$, there uniquely exists a coincident $h \in \mathcal{R}_n$ such that f is a h-noncoincident function, or in other words, any $f \in \mathcal{R}_n$ has a unique noncoincident indicator function h.*

Proof. According to Theorem 34, there uniquely exists a $h \in \mathcal{R}_n$ such that $f \in \aleph_h$. Due to Theorem 34, f is h-noncoincident. □

4.2 Finding All *h*-noncoincident Functions

Given a coincident function h, we show how to find all Boolean functions with noncoincident indicator function h. Due to Theorem 34, finding all h-noncoincident functions is equivalent to finding $\aleph_h$.

Lemma 16. *Let $h \in \mathcal{R}_n$ be coincident and (η_1, η_2) be its truth table where each η_j is a binary vector of length 2^{n-1}. Set $\zeta = \eta_2 T_{n-1}$. Then $(\zeta, 0)$, where 0 is the all-zero vector of length 2^{n-1}, is the truth table of a h-noncoincident function $\in \mathcal{R}_n$.*

Proof. Note that

$$(\zeta, 0)T_n^* = (\zeta, 0)\begin{bmatrix} T_{n-1}^* & T_{n-1} \\ O_{2^{n-1}} & T_{n-1}^* \end{bmatrix} = (\zeta T_{n-1}^*, \zeta T_{n-1}) = (\eta_2 T_{n-1} T_{n-1}^*, \eta_2).$$

According to Lemma 4, $\eta_2 T_{n-1} T_{n-1}^* = \eta_2 T_{n-1}^*$. Therefore, $(\zeta, 0)T_n^* = (\eta_2 T_{n-1}^*, \eta_2)$. Since h is coincident, due to Theorem 10, $\eta_1 = \eta_2 T_{n-1}^*$. Consequently, $(\zeta, 0)T_n^* = (\eta_1, \eta_2)$. According to Theorem 34, $(\zeta, 0)$ is the truth table of a h-noncoincident function $\in \mathcal{R}_n$. □

Theorem 35. *Let $h \in \mathcal{R}_n$ be coincident and (η_1, η_2) be its truth table where each η_j is a binary vector of length 2^{n-1}. Set $\zeta = \eta_2 T_{n-1}$. Let $f \in \mathcal{R}_n$. Then the function f is h-noncoincident if and only if its truth table ξ can be expressed as $\xi = (\zeta, 0) \oplus \varsigma$, where ς is the truth table of a coincident function $\in \mathcal{R}_n$.*

Proof. Assume that $\xi = (\zeta, 0) \oplus \varsigma$, where ς is the truth table of a coincident function $\in \mathcal{R}_n$. Due to the proof of Lemma 16 and Theorems 9, $\xi T_n^* = (\zeta, 0)T_n^* \oplus \varsigma T_n^*$ $= (\eta_1, \eta_2) \oplus 0$. Due to Theorems 34, f is h-noncoincident function. Conversely, assume that f is h-noncoincident function. Due to Theorem 34, $\xi T_n^* = (\eta_1, \eta_2)$. On the other hand, according to the proof of Lemma 16, $(\zeta, 0)T_n^* = (\eta_1, \eta_2)$. Summarily, $(\xi \oplus (\zeta, 0))T_n^* = 0$. Due to Theorem 9, $\xi \oplus (\zeta, 0)$ is the truth table of a coincident function $\in \mathcal{R}_n$. Therefore $\xi = (\zeta, 0) \oplus \varsigma$. □

4.3 Anti-coincident Functions

In this section we introduce new functions that are opposite to coincident functions.

Definition 4. *Let $f \in \mathcal{R}_n$. If $f(\alpha) \oplus \mu(f)(\alpha) = 1$ for all nonzero $\alpha \in (GF(2))^n$, or in other words, $f(\alpha) = 1$ if and only if $x_1^{a_1} \cdots x_n^{a_n}$ is not a monomial in the ANF of f, for any nonzero $\alpha = (a_1, \ldots, a_n) \in (GF(2))^n$, then f is called an* anti-coincident function.

Example 6. $f(x_1, x_2, x_3) = 1 \oplus x_2x_3 \oplus x_1x_3$ is an anti-coincident function $\in \mathcal{R}_3$. This can be seen from the fact that f has the truth table (1, 1, 1, 0, 1, 0, 1, 1) and $\mu(f)$ has the truth table (1, 0, 0, 1, 0, 1, 0, 0).

According to Lemma 3, $f(0) = \mu(f)(0)$ for every function f. For this reason, Definition 4 excludes the zero vector.

For clarity, we formulate the following lemma.

Lemma 17. *(i) The 2^n-bit vector $(0, 1, \ldots, 1)$ is the truth table of a coincident function of n variables, denoted by h^*,*

(ii) for any coincident function h of n variables, $h^* \oplus h$ is a coincident function with $HW(h^* \oplus h) = 2^n - 1 - HW(h)$.

Proof. It is noted that the 2^n-bit vector $(0, 1, \ldots, 1)$ is the top row of T_n^*. According to Theorem 12, it is the truth table of a coincident function h^* of n variables. We have proved (i). According to Theorem 12, $h^* \oplus h$ is a coincident function of n variables. Due to Corollary 3, $h(0) = 0$. Therefore $HW(h^* \oplus h) = HW(h^*) - HW(h)$. We have proved (ii). □

Theorem 36. *Let $f \in \mathcal{R}_n$ with its truth table ξ and $h^* \in \mathcal{R}_n$ be coincident, mentioned in Lemma 17, with its truth table $(0, 1, \ldots, 1)$. Then the following statements are equivalent: (i) f is anti-coincident, (ii) f is a h^*-noncoincident function, (iii) $\mu(f)$ is anti-coincident, (iv) $\mu(f)$ is a h^*-noncoincident function, (v) $f \oplus \mu(f) = h^*$, (vi) $\xi \oplus \xi T_n = (0, 1, \ldots, 1)$, (vii) $\xi T_n^* = (0, 1, \ldots, 1)$ and (viii) $f \in \aleph_{h^*}$, (ix) $1 \oplus f$ is coincident.*

Proof. The equivalence between (i), (ii), (iii) and (iv) and the equivalence between (v), (vi), (vii) and (viii) are obvious. Due to Definition 4, (i) $\Longleftrightarrow$ (v). It is easy to verify that $(0, 1, \ldots, 1)$ is also the truth table of $1 \oplus \mu(1)$. Then $1 \oplus \mu(1) = h^*$. It is noted that $1 \oplus f$ is a coincident function of n variables $\Longleftrightarrow$ $\mu(1 \oplus f) = 1 \oplus f \Longleftrightarrow f \oplus \mu(f) = 1 \oplus \mu(1) = h^* \Longleftrightarrow f$ is h^*-noncoincident. This proves (ix) $\Longleftrightarrow$ (ii). We have proved the theorem. □

According to Theorem 36, f is anti-coincident if and only if $1 \oplus f$ is coincident. Therefore we can obtain all properties of anti-coincident functions from coincident functions. For example, according to Theorem 3, we can state as follows.

Corollary 6. *Any anti-coincident function h satisfies $h(0) = 1$.*

Coincident and anti-coincident functions satisfy the following rules.

Theorem 37. *(i) if both f_1 and f_2 are coincident functions of n variables then $f_1 \oplus f_2$ is coincident,*

(ii) if f_1 is a coincident function of n variables and f_2 is an anti-coincident function of n variables then $f_1 \oplus f_2$ is anti-coincident,

(iii) if both f_1 and f_2 are anti-coincident functions of n variables then $f_1 \oplus f_2$ is coincident,

Proof. (i) is easily known from Theorem 12. Assume that f_1 is a coincident function of n variables and f_2 is an anti-coincident function of n variables. Due to Theorem 36, $1 \oplus f_2$ is a coincident function of n variables. Since we have proved (i), $f_1 \oplus (1 \oplus f_2)$ is a coincident function of n variables. Again, due to Theorem 36, $f_1 \oplus f_2$ is anti-coincident function of n variables. We have proved (ii). Assume that both f_1 and f_2 are anti-coincident functions of n variables. Due to Theorem 36, both $1 \oplus f_1$ and $1 \oplus f_2$ are coincident functions of n variables. According to (i), $(1 \oplus f_1) \oplus (1 \oplus f_2)$, i.e., $f_1 \oplus f_2$, is coincident function of n variables. We have proved (iii). □

Due to Theorem 18, we can state as follows.

Corollary 7. *There precisely exist $2^{2^{n-1}}$ anti-coincident functions of n variables.*

Theorem 38. *The set W of all the coincident functions and all the anti-coincident functions of n variables is a $(2^{n-1}+1)$-dimensional subspace of $\mathcal{R}_n$ where $\mathcal{R}_n$ is defined in Notation 1.*

Proof. According to Theorem 37, W is subspace of $\mathcal{R}_n$. Since there precisely exist $2^{2^{n-1}}$ coincident functions and $2^{2^{n-1}}$ anti-coincident functions of n variables, $\#W = 2^{2^{n-1}} + 2^{2^{n-1}} = 2^{2^{n-1}+1}$. This proves that W is $(2^{n-1}+1)$-dimensional. □

4.4 Noncoincident Weight of a Boolean Function

In this section we further generalise the concept of coincident functions. The noncoincident weight in the next definition is to measure how different between a Boolean function and its Möbius transform.

Definition 5. *Let $f \in \mathcal{R}_n$. The value of $d(f, \mu(f))$ is called the* noncoincident weight *of f, denoted by $NCW(f)$.*

Example 7. Let $f(x_1,x_2,x_3,x_4) = x_4 \oplus x_3 \oplus x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2 \oplus x_1x_2x_3$ then $\mu(f)(x_1,x_2,x_3,x_4) = x_4 \oplus x_3 \oplus x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_4 \oplus x_1x_2 \oplus x_1x_2x_4$. Note that $f(\alpha) \neq \mu(f)(\alpha)$ if and only if $\alpha = (1101)$ or (1110). Therefore $NCW(f) = 2$.

For clarity, we state as follows.

Theorem 39. *Let $f \in \mathcal{R}_n$ and ξ denote the truth table of f. Denote the noncoincident indicator function of f by h. Then $NCW(f) = HW(h) = HW(\xi T_n^*)$ or $\#h^{-1}(1) = NCW(f)$ or $\#h^{-1}(0) = 2^n - NCW(f)$, where $h^{-1}(1) = \{\alpha | \alpha \in (GF(2))^n,\ h(\alpha) = 1\}$ and $h^{-1}(0) = \{\alpha | \alpha \in (GF(2))^n,\ h(\alpha) = 0\}$.*

Proof. Due to Theorem 34, $f \oplus \mu(f) = h$. Then $NCW(f) = HW(h)$. Denote the truth table h by η. Again, due to Theorem 34, $HW(\xi T_n^*) = HW(\eta) = HW(h)$. □

Corollary 8. *Any Boolean function f satisfies $NCW(f) = NCW(\mu(f))$.*

Proof. Due to Theorem 34, f and $\mu(f)$ have the same noncoincident indicator function h. Applying Theorem 39 to both f and $\mu(f)$, we have proved the corollary. □

Theorem 40. *Let $n > 0$ be an integer. Then for any $f \in \mathcal{R}_n$,*

(i) $0 \leq NCW(f) \leq 2^n - 1$*,*
(ii) $NCW(f) = 0$ *if and only if f is a coincident function of n variables,*
(iii) $NCW(f) = 2^n - 1$ *if and only if f is an anti-coincident function of n variables.*

Proof. By definition, $NCW(f) = 0$ if and only if f is a coincident function of n variables. Due to Corollary 3, $f(0) = \mu(f)(0)$ holds for any function f. This proves that $NCW(f) \leq 2^n - 1$. Furthermore, due to Theorem 36, $NCW(f) = 2^n - 1$ if and only if f is an anti-coincident function of n variables. □

For further study, we present a new property of coincident function.

Theorem 41. *Let $n > 0$ be an integer. Then for any integer t with $0 \leq t \leq 2^n - 1$, there exists a coincident function h of n variables with $HW(h) = t$.*

Proof. We prove the theorem by induction on n. When $n = 1$. There precisely are two coincident functions of one variables whose truth tables are (0, 0) and (0, 1) respectively. Then the theorem is true for $n = 1$. We assume that the theorem holds for n with $1 \leq n \leq k - 1$. We now consider the case $n = k$. Let t be an integer with $0 \leq t \leq 2^k - 1$. There are two cases to be considered: $0 \leq t \leq 2^{k-1} - 1$ (Case 1) and $2^{k-1} \leq t \leq 2^k - 1$ (Case 2). We first consider Case 1, i.e., $0 \leq t \leq 2^{k-1} - 1$. By the induction assumption, there exists a coincident function h of $k - 1$ variables with $HW(h) = t$. Denote the truth table of h by η. Due to Theorems 9 and 10, $(0, \eta)$, where 0 denotes the all-zero vector of length 2^{k-1}, is the truth table of a coincident function f of k variables. Clearly $HW(f) = t$. We then have proved the theorem in Case 1. We turn to Case 2, i.e., $2^{k-1} \leq t \leq 2^k - 1$. Since $0 \leq 2^k - 1 - t \leq 2^{k-1} - 1$, due to (i), there exists a coincident function h' of k variables with $HW(h') = 2^k - 1 - t$. Let $h^* \in \mathcal{R}_k$ whose truth table is (0, 1, ..., 1). According to Lemma 17, h^* is a coincident function of k variables, furthermore, $h' \oplus h^*$ is a coincident function of k variables with $HW(h' \oplus h^*) = (2^k - 1) - (2^k - 1 - t) = t$. We have proved the theorem in Case 2. □

Corollary 9. *Let $n > 0$ be an integer. Then for any integer t with $0 \leq t \leq 2^n - 1$, there exists at least $2^{2^{n-1}}$ functions of n variables with noncoincident weight t.*

Proof. Due to Theorem 41, there exists at least one coincident function h of n variables with $HW(h) = t$. Due to Corollary 4, there precisely exist $2^{2^{n-1}}$ h-noncoincident functions of n variables. According to Theorem 39, any h-noncoincident function f has $NCW(f) = t$. We have proved the corollary. □

Theorem 42. *Let $n > 0$ be an integer. Then for any integer t with $0 \leq t \leq 2^n - 1$, there exists a balanced $f \in \mathcal{R}_n$ such that $NCW(f) = t$.*

Proof. There exist two cases to be considered: $t = 0$ and $1 \leq t \leq 2^n - 1$. For the case that $t = 0$, due to Theorem 41 there exists a coincident function h of n variables with $HW(h) = 2^{n-1}$. Then $h \in \mathcal{R}_n$ is balanced and $NCW(h) = t = 0$. We turn to the case $1 \leq t \leq 2^n - 1$. Due to Theorem 41, there exists a coincident function h' of n variables with $HW(h') = t$. Write the truth table of h' as $\eta = (\eta_1, \eta_2)$, where each η_j is a binary vector of length 2^{n-1}. Set $\zeta = \eta_2 T_{n-1}$. By using Theorem 41, there exists a coincident function r of $n-1$ variables with $HW(r) = 2^{n-1} - HW(\zeta)$. Denote the truth table of r by ϱ. Due to Theorem 10, $(0, \varrho)$, where 0 denotes the zero vector of length 2^{n-1}, is the truth table of a coincident function of n variables. According to Theorem 35, $(\zeta, 0) \oplus (0, \varrho)$ $= (\zeta, \varrho)$ is the truth table of a h'-noncoincident function, denoted by f. Clearly $HW(f) = HW(\zeta) + HW(\varrho)$ and then $HW(f) = 2^{n-1}$. Summarily f is balanced and $NCW(f) = HW(h') = t$. □

Assume that there exists a subset U of $\{1, \ldots, m\}$ such that for each $u \in U$, the value of $NCW(f_u)$ is either small or large. We further assume that the analysts know which f_u has small $NCW(f_u)$ and which f_u has large $NCW(f_u)$ for each $u \in U$.

5 Conclusions

In this work we have presented relations between a Boolean function and its Mӧbius transform, i.e., relations between the truth table of a Boolean function and its ANF so as to compute the ANF/truth table from the truth table/ANF of a function in different conditions. We have proposed a special kind of Boolean functions, so-called coincident functions, and extensively studied such functions especially their characteristic properties. We have generalised the concept of coincident functions and investigated general Boolean functions from the coincidence property.

Acknowledgement

The first author was supported by the Australian Research Council Grant DP0987734. The second author was supported by the Australian Research Council Grant DP0665035, the Singapore National Research Foundation Grant NRF-CRP2-2007-03 and the Singapore Ministry of Education Research Grant T206B2204. All the authors would like to thank the anonymous referees whose comments have helped improve this paper.

References

1. C. Carlet. Boolean functions for cryptography and error correcting codes. Chapter of the monography “Boolean Models and Methods in Mathematics, Computer Science, and Engineering” published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.). In press.

2. J. Katz and Y. Lindell. *Introduction to Modern Cryptography.* CRC Press, Boca Raton, FL, 2007.
3. S. Lloyd. *Programming the Universe: A Quantum Computer Scientist Takes on The Cosmos.* Alfred A. Knopf, ISBN 978-1400040926, 2006.
4. F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, New York, Oxford, 1978.
5. Josef Pieprzyk and Xian-Mo Zhang. Computing Möbius transforms of boolean functions and characterising coincident boolean functions. In J-B Yunès J-F Michon, P. Valarcher, editor, *Proceedings of Third International Workshop on Boolean Functions: Cryptography and Applications (BFCA'07)*, pages 127–143, 2007.
6. R. Piziak and P. L. Odell. *Matrix Theory.* Chapman & Hall/CRC, Boca Raton, London, New York, 2007.
7. G. C. Rota. On the foundations of combinatorial theory I. theory of möbius functions. *Probability Theory and Ralated Fields*, Vol 2, No 4:340–368, 1964.
8. O. S. Rothaus. On “bent” functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.
9. G. E. Shannon and W. Weaver. *The Mathematical Theory of Communication.* The University of Illinois Press, Urbana, Illinois, 1949.
10. R. Yarlagadda and J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceedings (Part E)*, 136:112–123, 1989.