MöBIUS-α COMMUTATIVE FUNCTIONS AND PARTIALLY COINCIDENT FUNCTIONS

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

Abstract. The Möbius transform of Boolean functions is often involved in cryptographic design and analysis. As studied previously, a Boolean function f is said to be coincident if it is identical with its Möbius transform f_μ, i.e., $f = f_\mu$. In this paper we study more general problems. We denote the function $f(x \oplus \alpha)$ by f_α. We prove that for each vector α with $HW(\alpha) \neq 1$, there exist a large number of functions such that $(f_\alpha)_\mu = (f_\mu)_\alpha$ and a large number of functions such that $f_\mu = f_\alpha$. We derive a series of results related to the conversion between f and f_μ.

Key Words: Boolean Functions, Möbius Transform

1. **Introduction**

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 $(0,\dots,0,0) = \alpha_0$, $(0,\dots,0,1) = \alpha_1$, ..., $(1,\dots,1,1) = \alpha_{2^n-1}$, and call α_i the *binary representation* of integer i, $i = 0,1,\dots,2^n-1$. 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 $f(x_1,\dots,x_n)$ where $x = (x_1,\dots,x_n)$. The *truth table* of a function f on $(GF(2))^n$ is a

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

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 $HW(f)$.

The following statement is well known (see, for example, [1]):

Theorem 1.1. [1] *A function f on $(GF(2))^n$ can be uniquely represented as:*

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

where $\alpha=(a_1,\ldots,a_n)$ and g is also a function on $(GF(2))^n$ satisfying $g(\alpha)=\bigoplus_{\beta\preceq\alpha} f(\beta)$ for all $\alpha\in(GF(2))^n$ where $(b_1,\ldots,b_n)\preceq(a_1,\ldots,a_n)$ means that if $b_j=1$ then $a_j=1$.

(1) is called the *Algebraic Normal Form* (ANF) of f. The function g is called the ***Möbius transform*** 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 $deg(f)=\max_{(a_1,\ldots,a_n)}\{HW(a_1,\ldots,a_n)\mid g(a_1,\ldots,a_n)=1\}$.

Notation 1. *Let $\mathcal{R}_n$ denote the set of all functions on $(GF(2))^n$. If $g\in\mathcal{R}_n$ is the Möbius transform of $f\in\mathcal{R}_n$ we write $\mu(f)=g$ [2]. However in this work, we rewrite $g=\mu(f)$ as $g=f_\mu$ for convenience.*

The classical Möbius function, 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 (see, for example, [3]).

Lemma 1.2. [2] *Define $2^n\times 2^n$ binary matrix T_n by the following recurrence. Let $T_0=1$ and $T_s=\begin{bmatrix} T_{s-1} & T_{s-1}\\ O_{2^{s-1}} & T_{s-1}\end{bmatrix}$, where $0_{2^{s-1}}$ is the $2^{s-1}\times 2^{s-1}$ zero matrix, $s=1,2,\ldots$. Then (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) $T_s(T_s\oplus I_{2^s})=(T_s\oplus I_{2^s})T_s=I_{2^s}\oplus T_s$, where $s=1,2,\ldots$.*

Theorem 1.3. [2] *Let $f,g\in\mathcal{R}_n$. Denote the truth tables of f and g by ξ and η, respectively. Then the following statements are equivalent: (i) $g=f_\mu$, (ii) $f=g_\mu$, (iii) $\eta T_n=\xi$, (iv) $\xi T_n=\eta$.*

We illustrate Theorem 1.3 by an example. From the ANF of $f(x_1, x_2, x_3) = x_3 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2x_3$, we immediately have the truth table of f_μ: (0, 1, 0, 1, 1, 0, 0, 1). By using Theorem 1.3, we know that the truth table of f is $(0,1,0,1,1,0,0,1)T_3 = (0,1,0,0,1,0,1,0)$. From the truth table of f, we can directly write the ANF of $f_\mu(x_1, x_2, x_3) = x_3 \oplus x_1 \oplus x_1x_2$.

The concept of coincident functions was introduced in [2].

Definition 1.4. Let $f \in \mathcal{R}_n$. If f and f_μ 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*.

For example, $f(x_1, x_2, x_3, x_4) = x_2x_4 \oplus x_2x_3 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_2x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_3x_4$ is a coincident function on $(GF(2))^4$ because f and f_μ have the same truth table that is (0000 0111 0000 1111).

Theorem 1.5. [2] *Let $f \in \mathcal{R}_n$. Then f is coincident if and only if there exists some $h \in \mathcal{R}_n$ such that $f = h \oplus h_\mu$.*

Theorem 1.6. [2] *There precisely exist $2^{2^{n-1}}$ coincident functions on $(GF(2))^n$ that form 2^{n-1}-dimensional linear subspace of $\mathcal{R}_n$.*

In this work we develop the theory initiated in [2] by viewing two large classes of functions satisfying $(f_\alpha)_\mu = (f_\mu)_\alpha$ and $f_\mu = f_\alpha$ respectively. The definitions will be given later.

2. Relations between P_α and T_n

Some proofs in this section are easy and some can be found in the Appendix.

Notation 2. *For any given $\alpha \in (GF(2))^n$, we define a $2^n \times 2^n$ matrix P_α, whose rows (columns) from top (left) to bottom (right) indexed by $0, 1, \ldots, 2^n - 1$, such that the entry on the position (i, j) is $\begin{cases} 1 & \text{if } \alpha_i \oplus \alpha_j = \alpha \\ 0 & \text{otherwise} \end{cases}$ where α_i is the binary representation of integer i.*

Clearly each row (column) of P_α has exactly one nonzero entry.

Notation 3. *Let $f \in \mathcal{R}_n$ and $\alpha \in (GF(2))^n$. Define $f_\alpha \in \mathcal{R}_n$ such that $f_\alpha(x) = f(x \oplus \alpha)$ for any $x \in (GF(2))^n$.*

Lemma 2.1. *Let ξ denote the truth table of $f \in \mathcal{R}_n$. Then for any $\alpha \in (GF(2))^n$, ξP_α is the truth table of f_α.*

Proof. It is noted that the ith coordinate of ξP_α is $f(\alpha_i \oplus \alpha)$, where α_i is the binary representation of integer i, and then ξP_α is the truth table of $f(x \oplus \alpha) = f_\alpha(x)$. $\square$

Lemma 2.2. *(i) $P_0 = I_{2^n}$, (ii) $P_\alpha^2 = I_{2^n}$, for any $\alpha \in (GF(2))^n$.*

Lemma 2.3. *Let $\alpha \in (GF(2))^n$. Then*

(i) $P_\alpha T_n \oplus T_n P_\alpha = T_n(P_\alpha T_n \oplus T_n P_\alpha)T_n = P_\alpha(P_\alpha T_n \oplus T_n P_\alpha)P_\alpha$,
(ii) $T_n \oplus P_\alpha = T_n(T_n \oplus P_\alpha)P_\alpha = P_\alpha(T_n \oplus P_\alpha)T_n$,
(iii) $(T_n \oplus P_\alpha)^2 = P_\alpha T_n \oplus T_n P_\alpha$.

Lemma 2.4. *Let $\alpha = (a_1, a_2, \ldots, a_n) \in (GF(2))^n$ and $\beta = (a_2, \ldots, a_n) \in (GF(2))^{n-1}$. Then $P_\alpha = \begin{bmatrix} P_\beta & O_{2^{n-1}} \\ O_{2^{n-1}} & P_\beta \end{bmatrix}$ when $a_1 = 0$, and $P_\alpha = \begin{bmatrix} O_{2^{n-1}} & P_\beta \\ P_\beta & O_{2^{n-1}} \end{bmatrix}$ when $a_1 = 1$.*

Notation 4. *Let A be a $p \times p$ matrix over $GF(2)$. Then $\{\alpha | \alpha \in (GF(2))^p,\ \alpha A = 0\}$ is a linear subspace of $(GF(2))^p$ whose dimension is called the* nullity *of A, denoted by $nu(A)$.*

By linear algebra, $rank(A) + nu(A) = p$.

Lemma 2.5. *Let $\alpha = (0, a_2, \ldots, a_n) \in (GF(2))^n$ and $\beta = (a_2, \ldots, a_n) \in (GF(2))^{n-1}$. Then $nu(T_n P_\alpha \oplus P_\alpha T_n) = 2 \cdot nu(T_{n-1} P_\beta \oplus P_\beta T_{n-1})$.*

Lemma 2.6. *Let $\alpha = (0, a_2, \ldots, a_n) \in (GF(2))^n$ and $\beta = (a_2, \ldots, a_n) \in (GF(2))^{n-1}$. Then $nu(T_n \oplus P_\alpha) = nu(T_{n-1} P_\beta \oplus P_\beta T_{n-1})$.*

Notation 5. *Write $P_{\alpha_{2^n-1}} = L_n$ where $\alpha_{2^n-1} = (1, \ldots, 1) \in (GF(2))^n$.*

Lemma 2.7. *(i) $(T_n L_n)^2 = L_n T_n$, (ii) $(L_n T_n)^2 = T_n L_n$.*

Lemma 2.8. $nu(T_n L_n \oplus L_n T_n) = nu(I_{2^{n-1}} \oplus T_{n-1} L_{n-1} \oplus L_{n-1} T_{n-1})$.

Lemma 2.9. $nu(I_{2^n} \oplus T_n L_n \oplus L_n T_n) = 2^{n-1} + nu(T_{n-1} \oplus L_{n-1})$.

Lemma 2.10. $nu(T_n \oplus L_n) = nu(I_{2^{n-1}} \oplus T_{n-1} L_{n-1} \oplus L_{n-1} T_{n-1})$.

3. Relations between f_μ, f_π and f_α

Notation 6. *Let $f \in \mathcal{R}_n$. Let π be a permutation on $\{1, \ldots, n\}$. Define the function f_π as $f_\pi(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)})$.*

Theorem 3.1. [2] *For any* $f \in \mathcal{R}_n$ *and any permutation* π *on* $\{1, \ldots, n\}$, $(f_\pi)_\mu = (f_\mu)_\pi$.

Theorem 3.2. *Let* $f \in \mathcal{R}_n$, $\alpha \in (GF(2))^n$ *and* π *be a permutation* π *on* $\{1, \ldots, n\}$. *Then* $(f_\alpha)_\pi = (f_\pi)_{\pi^{-1}(\alpha)}$.

Proof. By definition, we have $(f(x \oplus \alpha))_\pi = f(\pi(x) \oplus \alpha)$. It is noted that any permutation on the indices of variables is a linear transformation on $(GF(2))^n$. Then $\pi(x) \oplus \alpha = \pi(x \oplus \pi^{-1}(\alpha))$ and then $f(\pi(x) \oplus \alpha)= f(\pi(x \oplus \pi^{-1}(\alpha))$. Summarily $(f(x \oplus \alpha))_\pi = f(\pi(x \oplus \pi^{-1}(\alpha))$. By definition, $(f_\alpha)_\pi = (f_\pi)_{\pi^{-1}(\alpha)}$. □

Lemma 3.3. *Let* $f \in \mathcal{R}_n$, $\alpha, \alpha' \in (GF(2))^n$. *Then (i)* $(f_\alpha)_{\alpha'} = f_{\alpha \oplus \alpha'}$, *(ii)* $(f_\alpha) = f_{\alpha'}$ *if and only if* $f_{\alpha \oplus \alpha'} = f$.

Proof. By definition, (i) is true. Due to (i) of the lemma, we can easily prove (ii). □

Lemma 3.4. *Let* $f \in \mathcal{R}_n$ *and* $\alpha \in (GF(2))^n$. *Then* $(f_\mu)_\mu = f$ *and* $(f_\alpha)_\alpha = f$.

Proof. $(f_\mu)_\mu = f$ due to Theorem 1.3. $(f_\alpha)_\alpha = f$ due to (i) of Lemma 3.3. □

Lemma 3.5. *Let* $f, f' \in \mathcal{R}_n$. *Then* $f_\pi = f'_\pi$ *if and only if* $f = f'$.

Proof. The sufficiency is obviously true. Conversely assume that $f_\pi = f'_\pi$. Then $(f_\pi)_{\pi^{-1}} = (f'_\pi)_{\pi^{-1}}$. We have $f = f'$. □

4. **Möbius-α Commutative Functions**

Definition 4.1. Let $\alpha \in (GF(2))^n$. Then $f \in \mathcal{R}_n$ is called a *Möbius-α commutative function* if $(f_\alpha)_\mu = (f_\mu)_\alpha$.

Example 4.2. Let $f(x_1, x_2, x_3) = 1 \oplus x_3 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3$ and $\alpha = (0, 1, 1)$. It is noted that $f_\alpha = 1 \oplus x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2 \oplus x_1x_2x_3$. Due to Theorem 1.3, we have $(f_\alpha)_\mu = 1 \oplus x_3 \oplus x_2x_3$. Again, due to Theorem 1.3, $f_\mu = 1 \oplus x_2 \oplus x_2x_3$ and then $(f_\mu)_\alpha = 1 \oplus x_3 \oplus x_2x_3$. Then $(f_\alpha)_\mu = (f_\mu)_\alpha$, i.e., f is a Möbius-α commutative function. □

Notation 7. *For a given* $\alpha \in (GF(2))^n$, *denote the set of all Möbius-α commutative functions by* $\mathcal{U}_\alpha$.

Lemma 4.3. *For any given* $\alpha \in (GF(2))^n$, $\mathcal{U}_\alpha$ *is a linear subspace of* $\mathcal{R}_n$.

Theorem 4.4. *Let $f \in \mathcal{R}_n$ and $\alpha = (a_1, \dots, a_n) \in (GF(2))^n$ and π be a permutation on $\{1, \dots, n\}$. Then $f \in \mathcal{U}_\alpha$ if and only if $f_\pi \in \mathcal{U}_{\pi^{-1}(\alpha)}$, where $\pi^{-1}(\alpha) = (a_{\pi^{-1}(1)}, \dots, a_{\pi^{-1}(n)})$.*

Proof. Assume that $f \in \mathcal{U}_\alpha$, i.e., $(f_\alpha)_\mu = (f_\mu)_\alpha$ and then $((f_\alpha)_\mu)_\pi = ((f_\mu)_\alpha)_\pi$. Due to Theorems 3.1 and 3.2, we have $((f_\alpha)_\pi)_\mu = ((f_\mu)_\pi)_{\pi^{-1}(\alpha)}$. Again, due to Theorems 3.1 and 3.2, we have $((f_\pi)_{\pi^{-1}(\alpha)})_\mu = ((f_\pi)_\mu)_{\pi^{-1}(\alpha)}$. For clarity, set $g = f_\pi$. Then $(g_{\pi^{-1}(\alpha)})_\mu = (g_\mu)_{\pi^{-1}(\alpha)}$. This means that $g \in \mathcal{U}_{\pi^{-1}(\alpha)}$, i.e., $f_\pi \in \mathcal{U}_{\pi^{-1}(\alpha)}$. □

Example 4.5. We now illustrate Theorem 4.4. Reconsider $f(x_1, x_2, x_3) = 1 \oplus x_3 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3$ and $\alpha = (0, 1, 1)$ in Example 4.2. Let π be a permutation on $\{1, 2, 3\}$ such that $\pi(1) = 2$, $\pi(2) = 3$, $\pi(3) = 1$. By definition, $f_\pi(x_1, x_2, x_3) = 1 \oplus x_1 \oplus x_3x_1 \oplus x_2 \oplus x_2x_1 \oplus x_2x_3x_1$. Clearly $\pi^{-1}(1) = 3$, $\pi^{-1}(2) = 1$, $\pi^{-1}(3) = 2$. Then $\pi^{-1}(\alpha) = \pi^{-1}(0, 1, 1) = (1, 0, 1)$. By definition, $(f_\pi)_{\pi^{-1}(\alpha)} = 1 \oplus x_3 \oplus x_2 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3$. Due to Theorem 1.3, $((f_\pi)_{\pi^{-1}(\alpha)})_\mu = 1 \oplus x_1 \oplus x_1x_3$. Again, due to Theorem 1.3, $(f_\pi)_\mu = 1 \oplus x_3 \oplus x_1x_3$. It follows that $((f_\pi)_\mu))_{\pi^{-1}(\alpha)} = 1 \oplus x_1 \oplus x_1x_3$. Therefore $((f_\pi)_{\pi^{-1}(\alpha)})_\mu = ((f_\pi)_\mu))_{\pi^{-1}(\alpha)}$. Then $f_\pi \in \mathcal{U}_{\pi^{-1}(\alpha)}$. □

Theorem 4.6. *Let $\alpha \in (GF(2))^n$, $f \in \mathcal{R}_n$ and ξ be the truth table of f. Then $f \in \mathcal{U}_\alpha$ if and only if $\xi(P_\alpha T_n \oplus T_n P_\alpha) = 0$.*

Theorem 4.7. *Let $\alpha \in (GF(2))^n$. Then $dim(\mathcal{U}_\alpha) = nu(P_\alpha T_n \oplus T_n P_\alpha)$.*

Theorem 4.8. *For any fixed integer t with $0 \leq t \leq n$, both $nu(P_\alpha T_n \oplus T_n P_\alpha)$ and $dim(\mathcal{U}_\alpha)$ are invariant over all $\alpha \in (GF(2))^n$ with $HW(\alpha) = t$.*

Proof. Due to Theorem 4.7, we only need to prove the theorem on $dim(\mathcal{U}_\alpha)$. Let $\alpha, \alpha' \in (GF(2))^n$ with $HW(\alpha) = HW(\alpha') = t$. Then there exists a permutation π on $\{1, \dots, n\}$ such that $\pi(\alpha') = \alpha$, i.e., $\alpha' = \pi^{-1}(\alpha)$. Due to Lemma 3.5 and Theorem 4.4, there exists a one-to-one correspondence between $\mathcal{U}_\alpha$ and $\mathcal{U}_{\alpha'}$ such that $f \in \mathcal{U}_\alpha \leftrightarrow f_\pi \in \mathcal{U}_{\alpha'}$. Then $\#\mathcal{U}_\alpha = \#\mathcal{U}_{\alpha'}$. Since both $\mathcal{U}_\alpha$ and $\mathcal{U}_{\alpha'}$ are linear subspaces of $\mathcal{R}_n$, $dim(\mathcal{U}_\alpha) = dim(\mathcal{U}_{\alpha'})$. We have proved the theorem. □

Theorem 4.9. (i) *$f \in \mathcal{U}_\alpha$ if and only if $f_\mu \in \mathcal{U}_\alpha$,*
(ii) *$f \in \mathcal{U}_\alpha$ if and only if $f_\alpha \in \mathcal{U}_\alpha$.*

Proof. It is noted that $f \in \mathcal{U}_\alpha$, i.e, $(f_\mu)_\alpha = (f_\alpha)_\mu \iff ((f_\mu)_\alpha)_\mu = ((f_\alpha)_\mu)_\mu \iff ((f_\mu)_\alpha)_\mu = f_\alpha$ (Lemma 3.4) $\iff ((f_\mu)_\alpha)_\mu = ((f_\mu)_\mu))_\alpha$ (Lemma 3.4), i.e., $f_\mu \in \mathcal{U}_\alpha$. Then (i) holds. It is also noted that $f \in \mathcal{U}_\alpha$, i.e., $(f_\mu)_\alpha = (f_\alpha)_\mu \iff ((f_\mu)_\alpha)_\alpha = ((f_\alpha)_\mu)_\alpha \iff f_\mu = ((f_\alpha)_\mu)_\alpha$ (Lemma 3.4) $\iff ((f_\alpha)_\alpha)_\mu = ((f_\alpha)_\mu)_\alpha$ (Lemma 3.4), i.e., $f_\alpha \in \mathcal{U}_\alpha$. Then (ii) holds. □

5. Partially Coincident Functions

Definition 5.1. $f \in \mathcal{R}_n$ is said to be *partially coincident* with respect to a vector $\alpha \in (GF(2))^n$ if $f_\mu = f_\alpha$.

Example 5.2. Let $f(x_1, x_2, x_3) = x_1 \oplus x_1x_3 \oplus x_1x_2x_3$ and $\alpha = (0, 1, 1)$. Due to Theorem 1.3, we have $f_\mu(x_1, x_2, x_3) = x_1 \oplus x_1x_2 \oplus x_1x_2x_3$. On the other hand, $f_\alpha = x_1 \oplus x_1x_2 \oplus x_1x_2x_3$. Then $f_\mu = f_\alpha$ and then f is a partially coincident function with respect to $\alpha = (0, 1, 1)$. □

Notation 8. *Denote the set of all partially coincident functions on $(GF(2))^n$ with respect to α by $\mathcal{V}_\alpha$.*

Lemma 5.3. *$\mathcal{V}_\alpha$ is a linear subspace of $\mathcal{R}_n$ for any $\alpha \in (GF(2))^n$.*

Clearly a partially coincident function with respect to the zero vector 0 is a coincident function. For clarity, we state as follows.

Lemma 5.4. *$\mathcal{V}_0$, in Notation 8, is the set of all coincident functions on $(GF(2))^n$ and then $\#\mathcal{V}_0 = 2^{2^{n-1}}$ or $dim(\mathcal{V}_0) = 2^{n-1}$.*

Theorem 5.5. *Let $f \in \mathcal{R}_n$, $\alpha = (a_1, \ldots, a_n) \in (GF(2))^n$ and π be a permutation on $\{1, \ldots, n\}$. Then $f \in \mathcal{V}_\alpha$ if and only if $f_\pi \in \mathcal{V}_{\pi^{-1}(\alpha)}$ where $\pi^{-1}(\alpha) = (a_{\pi^{-1}(1)}, \ldots, a_{\pi^{-1}(n)})$.*

Proof. Assume that $f \in \mathcal{V}_\alpha$, i.e., $f_\mu = f_\alpha$ and then $(f_\mu)_\pi = (f_\alpha)_\pi$. Due to Theorems 3.1 and 3.2, it follows that $(f_\pi)_\mu = (f_\pi)_{\pi^{-1}(\alpha)}$. For clarity, set $g = f_\pi$. It follows that $g_\mu = g_{\pi^{-1}(\alpha)}$. Then $g \in \mathcal{V}_{\pi^{-1}(\alpha)}$, i.e., $f_\pi \in \mathcal{V}_{\pi^{-1}(\alpha)}$. We have proved the necessity. Since the deduction can be inverted, the sufficiency holds, □

Example 5.6. We now illustrate Theorem 5.5. In Example 5.2 we know that $f(x_1, x_2, x_3) = x_1 \oplus x_1x_3 \oplus x_1x_2x_3 \in \mathcal{V}_\alpha$ with $\alpha = (0, 1, 1)$. Let π be a permutation on $\{1, 2, 3\}$ such that $\pi(1) = 3$, $\pi(2) = 1$, $\pi(3) = 2$. By definition, $f_\pi(x_1, x_2, x_3) = x_3 \oplus x_3x_2 \oplus x_3x_1x_2$. Due to $\pi^{-1}(1) = 2$, $\pi^{-1}(2) = 3$, $\pi^{-1}(3) = 1$, we know that $\pi^{-1}(\alpha) = \pi^{-1}(0, 1, 1) = (1, 1, 0)$. It is noted that $(f_\pi)_{\pi^{-1}(\alpha)} =$

$x_3 \oplus x_1x_3 \oplus x_1x_2x_3$. By using Theorem 1.3, we have $(f_\pi)_\mu = x_3 \oplus x_1x_3 \oplus x_1x_2x_3$. Therefore $(f_\pi)_\mu = (f_\pi)_{\pi^{-1}(\alpha)}$. This means that $f_\pi \in \mathcal{V}_{\pi^{-1}(\alpha)}$. $\square$

Theorem 5.7. *Let $\alpha \in (GF(2))^n$. Let $f \in \mathcal{R}_n$ and ξ be the truth table of f. Then $f \in \mathcal{V}_\alpha$ if and only if $\xi(T_n \oplus P_\alpha) = 0$.*

Theorem 5.8. (i) *$f \in \mathcal{V}_\alpha$ if and only if $f_\mu \in \mathcal{V}_\alpha$,*
(ii) *$f \in \mathcal{V}_\alpha$ if and only if $f_\alpha \in \mathcal{V}_\alpha$.*

Proof. It is noted that $f \in \mathcal{V}_\alpha$, i.e., $f_\mu = f_\alpha \iff (f_\mu)_\alpha = (f_\alpha)_\alpha \iff (f_\mu)_\alpha = f$ (Lemma 3.4) $\iff (f_\mu)_\alpha = (f_\mu)_\mu$ (Lemma 3.4), i.e., $f_\mu \in \mathcal{V}_\alpha$. Then (i) holds. It is also noted that $f \in \mathcal{V}_\alpha$, i.e., $f_\mu = f_\alpha \iff (f_\mu)_\mu = (f_\alpha)_\mu \iff f = (f_\alpha)_\mu$ (Lemma 3.4) $\iff (f_\alpha)_\alpha = (f_\alpha)_\mu$ (Lemma 3.4), i.e., $f_\alpha \in \mathcal{V}_\alpha$. Then (ii) holds. $\square$

According to Theorem 5.7, we can state as follows.

Theorem 5.9. *Let $\alpha \in (GF(2))^n$. Then $dim(\mathcal{V}_\alpha) = nu(T_n \oplus P_\alpha)$.*

Theorem 5.10. *Let $f \in \mathcal{R}_n$ and further $f \in \mathcal{V}_\alpha$. Then $f \in \mathcal{V}_{\alpha'}$ if and only if $f_{\alpha \oplus \alpha'} = f$.*

Proof. Assume that $f \in \mathcal{V}_{\alpha'}$, i.e., $f_\mu = f_{\alpha'}$. Since $f \in \mathcal{V}_\alpha$, i.e., $f_\mu = f_\alpha$, it follows that $f_\alpha = f_{\alpha'}$. Due to Lemma 3.3, we know that $f_{\alpha \oplus \alpha'} = f$. We have proved the necessity. Conversely, we assume that $f_{\alpha \oplus \alpha'} = f$. Due to Lemma 3.3, we have $f_\alpha = f_{\alpha'}$. Since $f \in \mathcal{V}_\alpha$, i.e., $f_\mu = f_\alpha$. it follows that $f_\mu = f_{\alpha'}$, i.e., $f \in \mathcal{V}_{\alpha'}$. This proves the sufficiency. $\square$

Theorem 5.11. *For any given integer t with $0 \le t \le n$, both $nu(T_n \oplus P_\alpha)$ and $dim(\mathcal{V}_\alpha)$ are invariant over all $\alpha \in (GF(2))^n$ with $HW(\alpha) = t$.*

Proof. Due to Theorem 5.9, we only need to prove the theorem on $dim(\mathcal{V}_\alpha)$. Let $\alpha, \alpha' \in (GF(2))^n$ with $HW(\alpha) = HW(\alpha') = t$. Then there exists a permutation π on $\{1, \dots, n\}$ such that $\pi(\alpha') = \alpha$, i.e., $\alpha' = \pi^{-1}(\alpha)$. Due to Lemma 3.5 and Theorem 5.5, there exists a one-to-one correspondence between $\mathcal{V}_\alpha$ and $\mathcal{V}_{\alpha'}$ such that $f \in \mathcal{V}_\alpha \leftrightarrow f_\pi \in \mathcal{V}_{\alpha'}$. Then $\#\mathcal{V}_\alpha = \#\mathcal{V}_{\alpha'}$. Since both $\mathcal{V}_\alpha$ and $\mathcal{V}_{\alpha'}$ are linear subspaces of $\mathcal{R}_n$, $dim(\mathcal{V}_\alpha) = dim(\mathcal{V}_{\alpha'})$. We have proved the theorem. $\square$

Lemma 5.12. *Let $f \in \mathcal{V}_\alpha$. Then $f \oplus f_\alpha$ is coincident.*

Proof. Since $f \in \mathcal{V}_\alpha$, we know that $f \oplus f_\alpha = f \oplus f_\mu$. Due to Theorem 1.5, $f \oplus f_\mu$ is coincident and then $f \oplus f_\alpha$ is coincident. $\square$

Theorem 5.13. [2] *Let f be a nonzero 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.*

We have an analogous result for partially coincident functions,

Theorem 5.14. *Let $f \in \mathcal{R}_n$. If $f \in \mathcal{V}_\alpha$ ($\alpha \neq 0$) but f is not coincident then $deg(f) \geq 1 + \lceil \frac{1}{2}n \rceil$. More precisely, (i) $deg(f) \geq 1 + \frac{1}{2}n$ where n is even, (ii) $deg(f) \geq 1 + \frac{1}{2}(n+1)$ where n is odd.*

Proof. Due to Lemma 5.12, $f \oplus f_\alpha$ is coincident. Since $f \in \mathcal{V}_\alpha$, $f \oplus f_\alpha = f \oplus f_\mu$. Since f is not coincident, $f \oplus f_\mu$ is nonzero and then $f \oplus f_\alpha$ is nonzero coincident. Due to Theorem 5.13, $deg(f \oplus f_\alpha) \geq \lceil \frac{1}{2}n \rceil$. It is noted that $deg(f \oplus f_\alpha) \leq deg(f) - 1$. We then have proved the theorem. □

Theorem 5.14 gives a larger lower bound than Theorem 5.13.

6. Relations between Möbius-α Commutative Functions and Partially Coincident Functions

Theorem 6.1. *$\mathcal{V}_\alpha \subseteq \mathcal{U}_\alpha$ for any $\alpha \in (GF(2))^n$.*

Proof. Let $f \in \mathcal{V}_\alpha$, i.e., $f_\mu = f_\alpha$. Then $(f_\mu)_\alpha = (f_\alpha)_\alpha$. Due to Lemma 3.3, we have $(f_\mu)_\alpha = f$. On the other hand, from $f_\mu = f_\alpha$, we have $(f_\mu)_\mu = (f_\alpha)_\mu$. Again, due to Lemma 3.3, we have $f = (f_\alpha)_\mu$. Summarily $(f_\mu)_\alpha = (f_\alpha)_\mu$. Then $f \in \mathcal{U}_\alpha$. Since f is arbitrarily from $\mathcal{V}_\alpha$, $\mathcal{V}_\alpha \subseteq \mathcal{U}_\alpha$. □

However the equality in Theorem 6.1 does not necessarily hold.

Example 6.2. Recall Example 4.2. $f(x_1, x_2, x_3) = 1 \oplus x_3 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3 \in \mathcal{U}_\alpha$ for $\alpha = (0, 1, 1)$ and $f_\alpha = 1 \oplus x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2 \oplus x_1x_2x_3$ and $f_\mu = 1 \oplus x_2 \oplus x_2x_3$. Then $f_\mu \neq f_\alpha$, i.e., $f \notin \mathcal{V}_\alpha$. Summarily $f \in \mathcal{U}_\alpha$ but $f \notin \mathcal{V}_\alpha$. □

Theorem 6.3. *Let $\alpha \in (GF(2))^n$. Then*

(i) $dim(\mathcal{U}_0) = 2 \cdot dim(\mathcal{V}_0) = 2^n$,
(ii) $dim(\mathcal{U}_\alpha) = 2 \cdot dim(\mathcal{V}_\alpha)$ *when* $1 \leq HW(\alpha) \leq n-1$,
(iii) $\mathcal{U}_{\alpha_{2^n-1}} = \mathcal{V}_{\alpha_{2^n-1}}$ *where* $\alpha_{2^n-1} = (1, \dots, 1)$.

Proof. It is noted that $P_0 = I_{2^n}$. Then $T_nP_0 \oplus P_0T_n = 0$ and then $nu(T_nP_0 \oplus P_0T_n) = 2^n$. Due to Theorem 4.7, $dim(\mathcal{U}_0) = 2^n$. Due to Lemma 5.4, $dim(\mathcal{V}_0) = 2^{n-1}$. Then (i) holds. We now prove (ii). Let $\alpha' = (0, a_2, \dots, a_n) \in (GF(2))^n$ with $HW(\alpha') = HW(\alpha)$.

Combing Lemmas 2.5 and 2.6, we know that $nu(T_nP_{\alpha'} \oplus P_{\alpha'}T_n) = 2 \cdot nu(T_n \oplus P_{\alpha'})$. Due to Theorems 4.8 and 5.11, $nu(T_nP_\alpha \oplus P_\alpha T_n) = 2 \cdot nu(T_n \oplus P_\alpha)$. Due to Theorems 4.7 and 5.9, (ii) holds. Due to Lemmas 2.8 and 2.10, $nu(T_nL_n \oplus L_nT_n) = nu(T_n \oplus L_n)$ where $L_n = P_{\alpha_{2^n-1}}$. Therefore, according to Theorems 4.7 and 5.9, $dim(\mathcal{U}_{\alpha_{2^n-1}})= dim(\mathcal{V}_{\alpha_{2^n-1}})$. Due to Theorem 6.1, $\mathcal{V}_\alpha \subseteq \mathcal{U}_\alpha$. Then $dim(\mathcal{U}_{\alpha_{2^n-1}}) = dim(\mathcal{V}_{\alpha^{2^n-1}})$ and $\mathcal{V}_\alpha \subseteq \mathcal{U}_\alpha$ together imply that $\mathcal{V}_{\alpha_{2^n-1}} = \mathcal{U}_{\alpha_{2^n-1}}$. Then (iii) holds. □

Corollary 6.4. *$\mathcal{V}_\alpha \subseteq \mathcal{U}_\alpha$ for any $\alpha \in (GF(2))^n$, furthermore, $\mathcal{V}_\alpha = \mathcal{U}_\alpha$ if and only if $\alpha = (1, \dots, 1)$.*

Theorem 6.5. *Let $f \in \mathcal{R}_n$ and $f \in \mathcal{U}_\alpha$. If f further satisfies one of the following two conditions:*

(i) *there exists some $h \in \mathcal{U}_\alpha$ such that $f = h_\mu \oplus h_\alpha$ when $HW(\alpha) < n$, or*
(ii) *$HW(\alpha) = n$, i.e., $\alpha = (1, \dots, 1)$.*

then $f \in \mathcal{V}_\alpha$.

Proof. Assume that $HW(\alpha) < n$, $h \in \mathcal{U}_\alpha$ and $f = h_\mu \oplus h_\alpha$. It is noted that $f_\mu = (h_\mu)_\mu \oplus (h_\alpha)_\mu$. Due to Lemma 3.4, $f_\mu = h \oplus (h_\alpha)_\mu$. It is also noted that $f_\alpha = (h_\mu)_\alpha \oplus (h_\alpha)_\alpha$. Again, due to Lemma 3.4, $f_\alpha = (h_\mu)_\alpha \oplus h$. Since $h \in \mathcal{U}_\alpha$, i.e., $(h_\alpha)_\mu. = (h_\mu)_\alpha$, it follows that $f_\mu = f_\alpha$, i.e., $f \in \mathcal{V}_\alpha$. We have proved (i). (ii) holds due to (iii) of Theorem 6.3. □

We next prove the converse of Theorem 6.5.

Theorem 6.6. *Let $f \in \mathcal{R}_n$ and further $f \in \mathcal{V}_\alpha$. Then*

(i) *either there exists some $h \in \mathcal{U}_\alpha$ such that $f = h_\mu \oplus h_\alpha$ when $HW(\alpha) < n$,*
(ii) *or $HW(\alpha) = n$, i.e., $\alpha = (1, \dots, 1)$.*

Proof. If $HW(\alpha) = n$ then (ii) takes place. Assume that $HW(\alpha) < n$. Set $W = \{h_\mu \oplus h_\alpha | h \in \mathcal{U}_\alpha\}$. Combing Theorems 6.5 and 6.1, $W \subseteq \mathcal{V}_\alpha \subseteq \mathcal{U}_\alpha$. We define a linear mapping Φ from $\mathcal{U}_\alpha$ to $\mathcal{U}_\alpha$: $\Phi(g) = g'$ if and only $g' = g_\mu \oplus g_\alpha$ where $g \in \mathcal{U}_\alpha$. Clearly $g' \in W \subseteq \mathcal{V}_\alpha \subseteq \mathcal{U}_\alpha$. Due to the definition of $\mathcal{V}_\alpha$, Theorems 6.5 and 6.1, it is easy to verify that $\Phi^{-1}(0) = \mathcal{V}_\alpha$ where $\Phi^{-1}(0)$ denotes the kernel of Φ. It is noted that W is the range of Φ. By using linear algebra, $dim(\mathcal{V}_\alpha) + dim(W) = dim(\mathcal{U}_\alpha)$. Due to Theorem 6.3, $dim(\mathcal{U}_\alpha) = 2 \cdot dim(\mathcal{V}_\alpha)$. Therefore $dim(W) = dim(\mathcal{V}_\alpha)$. Recall that $W \subseteq \mathcal{V}_\alpha$. Then $dim(W) = dim(\mathcal{V}_\alpha)$ and $W \subseteq \mathcal{V}_\alpha$ together imply that $W = \mathcal{V}_\alpha$. Therefore any $f \in \mathcal{V}_\alpha$ can be expressed as $f = h_\mu \oplus h_\alpha$ where $h \in \mathcal{U}_\alpha$. □

7. Enumeration of Möbius-α Commutative Functions

Some proofs in this section can be found in the Appendix.

By a straightforward verification, we can conclude as follows.

Lemma 7.1. *(i) $nu(T_1 \oplus L_1) = 0$, (ii) $nu(T_1L_1 \oplus L_1T_1) = 0$, (iii) $nu(I_{2^1} \oplus T_1L_1 \oplus L_1T_1) = 2$, (iv) $nu(T_2L_2 \oplus L_2T_2) = 2$, (v) $nu(I_{2^2} \oplus T_2L_2 \oplus L_2T_2) = 2$.*

Lemma 7.2. *Let $\alpha \in (GF(2))^n$ with $HW(\alpha) = 1$. Then $nu(T_nP_\alpha \oplus P_\alpha T_n) = 0$.*

Proof. Due to Theorem 4.8, without loss of generality, we can assume that $\alpha = (0, \ldots, 0, 1) \in (GF(2))^n$. Repeatedly using Lemma 2.5, we have $nu(T_nP_\alpha \oplus P_\alpha T_n) = 2^{n-1} \cdot nu(T_1L_1 \oplus L_1T_1)$. Due to Lemma 7.1, $nu(T_1L_1 \oplus L_1T_1) = 0$. We then have proved the lemma. □

Lemma 7.3. (i) $nu(I_{2^{2k+1}} \oplus T_{2k+1}L_{2k+1} \oplus L_{2k+1}T_{2k+1}) = \frac{2}{3}(2^{2k+1} + 1)$, $k = 0, 1, \ldots,$

(ii) $nu(I_{2^{2k}} \oplus T_{2k}L_{2k} \oplus L_{2k}T_{2k}) = \frac{2}{3}(2^{2k} - 1)$, $k = 1, 2, \ldots.$

Lemma 7.4. (i) $nu(T_{2k+1}L_{2k+1} \oplus L_{2k+1}T_{2k+1}) = \frac{2}{3}(2^{2k} - 1)$, $k = 1, 2, \ldots,$

(ii) $nu(T_{2k}L_{2k} \oplus L_{2k}T_{2k}) = \frac{2}{3}(2^{2k-1} + 1)$, $k = 1, 2, \ldots.$

Lemma 7.5. *Let $\alpha = (0, \ldots, 0, 1, \ldots, 1) \in (GF(2))^n$ with $1 \leq HW(\alpha) = t \leq n$. Then*

$$nu(T_nP_\alpha \oplus P_\alpha T_n) = \begin{cases} \frac{2}{3}(2^{n-1} - 2^{n-t}) & t = 1, 3, 5, \ldots \\ \frac{2}{3}(2^{n-1} + 2^{n-t}) & t = 2, 4, 6, \ldots \end{cases}.$$

By using Theorems 4.7 and 4.8, we can generalise Lemma 7.5 as follows.

Theorem 7.6. *Let $\alpha \in (GF(2))^n$ with $1 \leq HW(\alpha) = t \leq n$. Then* $dim(\mathcal{U}_\alpha) = \begin{cases} \frac{2}{3}(2^{n-1} - 2^{n-t}) & t = 1, 3, 5, \ldots \\ \frac{2}{3}(2^{n-1} + 2^{n-t}) & t = 2, 4, 6, \ldots \end{cases}.$

Due to Theorem 4.7, we know that Lemmas 7.2 and 7.4 are special cases of Theorem 7.6 when $t = 1$ and $t = n$ respectively.

Theorem 7.7. *Let $\alpha \in (GF(2))^n$. Then $0 \leq dim(\mathcal{U}_\alpha) \leq 2^n$ where (i) $dim(\mathcal{U}_\alpha) = 2^n$ if and only if $\alpha = 0$, (ii) $dim(\mathcal{U}_\alpha) = 0$ if and only if $HW(\alpha) = 1$.*

Proof. $0 \le dim(\mathcal{U}_\alpha) \le 2^n$ obviously holds. It is noted that $\alpha = 0 \Longrightarrow P_\alpha = I_{2^n}. \Longrightarrow T_n P_\alpha \oplus P_\alpha T_n = 0 \Longrightarrow dim(\mathcal{U}_\alpha) = 2^n$ (Theorem 4.7). Conversely, assume that $dim(\mathcal{U}_\alpha) = 2^n$. From Theorem 7.6, we know that α must be zero. We have proved (i). We next prove (ii). The sufficiency of (ii) holds because of Theorem 7.6. We next prove the necessity of (ii). Assume that $dim(\mathcal{U}_\alpha) = 0$. Due to (i) of the theorem, we know that $\alpha \ne 0$. Due to Theorem 7.6, we know that $HW(\alpha) = 1$. □

Corollary 7.8. *Let $\alpha \in (GF(2))^n$ with $1 \le HW(\alpha) = t \le n$. Then* $\#\mathcal{U}_\alpha = \begin{cases} 2^{\frac{2}{3}(2^{n-1}-2^{n-t})} & t = 1,3,5,\dots \\ 2^{\frac{2}{3}(2^{n-1}+2^{n-t})} & t = 2,4,6,\dots \end{cases}$.

According to Theorem 7.7, we can state as follows.

Corollary 7.9. *Let $\alpha \in (GF(2))^n$. Then $1 \le \#\mathcal{U}_\alpha \le 2^{2^n}$ where $\#\mathcal{U}_\alpha = 2^{2^n}$ if and only if $\alpha = 0$, $\#\mathcal{U}_\alpha = 1$ if and only if $HW(\alpha) = 1$.*

Theorem 7.6 and Corollary 7.8 are restricted by $\alpha \ne 0$. When $\alpha = 0$, we refer Theorem 7.7 and Corollary 7.9.

8. Enumeration of Partially Coincident Functions

Combing (ii) of Theorem 6.3 and Theorem 7.6, we state as follows.

Theorem 8.1. *Let $\alpha \in (GF(2))^n$ with $HW(\alpha) = t$ ($1 \le t \le n-1$). Then* $dim(\mathcal{V})_\alpha = \begin{cases} \frac{2}{3}(2^{n-2} - 2^{n-1-t}) & t = 1,3,5,\dots \\ \frac{2}{3}(2^{n-2} + 2^{n-1-t}) & t = 2,4,6,\dots \end{cases}$.

As for $t = n$, due to Lemma 7.4 and Theorem 5.9, we have the following conclusion.

Theorem 8.2. $dim(\mathcal{V})_{\alpha_{2^n-1}} = \begin{cases} \frac{2}{3}(2^{n-1} - 1) & n = 1,3,5,\dots \\ \frac{2}{3}(2^{n-1} + 1) & n = 2,4,6,\dots \end{cases}$ *where $\alpha_{2^n-1} = (1,\dots,1) \in (GF(2))^n$.*

Theorem 8.3. *Let $\alpha \in (GF(2))^n$. Then $0 \le dim(\mathcal{V}_\alpha) \le 2^{n-1}$ where (i) $dim(\mathcal{V}_\alpha) = 2^{n-1}$ if and only if $\alpha = 0$, (ii) $dim(\mathcal{V}_\alpha) = 0$ if and only if $HW(\alpha) = 1$.*

Proof. Combing Theorems 8.1, 8.2 and Lemma 5.4, we know that $0 \le dim(\mathcal{V}_\alpha) \le 2^{n-1}$ and (i) holds. We next prove (ii). The sufficiency of (ii) holds because of Theorem 8.1. We next prove the necessity of (ii). Assume that $dim(\mathcal{V}_\alpha) = 0$. Due to (i) of the theorem, we know that $\alpha \neq 0$. Due to Theorems 8.1 and 8.2, we know that $HW(\alpha) = 1$. □

Corollary 8.4. *Let $\alpha \in (GF(2))^n$ with $1 \leq HW(\alpha) = t \leq n-1$. Then* $\#\mathcal{V}_\alpha = \begin{cases} 2^{\frac{2}{3}(2^{n-2}-2^{n-1-t})} & t = 1,3,5,\ldots \\ 2^{\frac{2}{3}(2^{n-2}+2^{n-1-t})} & t = 2,4,6,\ldots \end{cases}$.

Corollary 8.5. $\#\mathcal{V}_{\alpha_{2^n-1}} = \begin{cases} 2^{\frac{2}{3}(2^{n-1}-1)} & k = 1,3,5,\ldots \\ 2^{\frac{2}{3}(2^{n-1}+1)} & k = 2,4,6,\ldots \end{cases}$ *where* $\alpha_{2^n-1} = (1,\ldots,1) \in (GF(2))^n$.

Corollary 8.6. *Let $\alpha \in (GF(2))^n$. Then $1 \leq \#\mathcal{V}_\alpha \leq 2^{2^{n-1}}$ where $\#\mathcal{V}_\alpha = 2^{2^{n-1}}$ if and only if $\alpha = 0$, $\#\mathcal{V}_\alpha = 1$ if and only if $HW(\alpha) = 1$.*

Theorems 8.1, 8.2, Corollaries 8.4 and 8.5 are restricted by $\alpha \neq 0$. As for $\alpha = 0$, we refer Lemma 5.4.

9. Conclusions

We have proposed and studied Möbius-α commutative functions and partially coincident functions. We have proved that for each vector α with $HW(\alpha) \neq 1$, there exist a large number of Möbius-α commutative functions and a large number of partially coincident functions with respect to α. The new results are related to conversion between Boolean functions and their Möbius transforms.

Acknowledgement

The authors were supported by Australian Research Council grants DP0663452, DP0558773 and DP0665035. The second author was also in part supported by the Ministry of Education of Singapore under grant T206B2204. We would like to thank the referees for helpful suggestions.

References

[1] J. F. Dillon. Möbius inversion and boolean functions. S12 Informal Note #219, 1968.

[2] 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, *Third International Workshop on Boolean Functions: Cryptography and Applications (BFCA'07), in Pre-proceedings and to appear in Proceedings*, 2007.
[3] G. C. Rota. *On the foundations of combinatorial theory I. Theory of Möbius functions, Z.Wahrsch.Verw. Gebiete, 340â ∼ @ ∼S368.* 1964.

Appendix

<u>Proof of Lemma 2.5</u> Due to the structure of T_n and Lemma 2.4, $T_nP_\alpha \oplus P_\alpha T_n = \begin{bmatrix} T_{n-1}P_\beta \oplus P_\beta T_{n-1} & T_{n-1}P_\beta \oplus P_\beta T_{n-1} \\ O_{2^{n-1}} & T_{n-1}P_\beta \oplus P_\beta T_{n-1} \end{bmatrix}$. Set $B = \begin{bmatrix} I_{2^{n-1}} & I_{2^{n-1}} \\ 0_{2^{n-1}} & I_{2^{n-1}} \end{bmatrix}$. It is noted that $(T_nP_\alpha \oplus P_\alpha T_n)B$ $= \begin{bmatrix} T_{n-1}P_\beta \oplus P_\beta T_{n-1} & O_{2^{n-1}} \\ O_{2^{n-1}} & T_{n-1}P_\beta \oplus P_\beta T_{n-1} \end{bmatrix}$. By linear algebra, multiplying a matrix by a nonsingular square matrix does not change its nullity. Therefore $nu(T_nP_\alpha \oplus P_\alpha T_n) = 2 \cdot nu(T_{n-1}P_\beta \oplus P_\beta T_{n-1})$. $\square$

<u>Proof of Lemma 2.6</u>

It is noted that $T_n \oplus P_\alpha = \begin{bmatrix} T_{n-1} \oplus P_\beta & T_{n-1} \\ O_{2^{n-1}} & T_{n-1} \oplus P_\beta \end{bmatrix}$. Set $B = \begin{bmatrix} T_{n-1} & O_{2^{n-1}} \\ O_{2^{n-1}} & T_{n-1} \end{bmatrix}$ and $C = \begin{bmatrix} I_{2^{n-1}} & 0_{2^{n-1}} \\ I_{2^{n-1}} \oplus T_{n-1}P_\beta & I_{2^{n-1}} \end{bmatrix}$. Then, it is easy to verify that

$CB(T_n \oplus P_\alpha) = \begin{bmatrix} I_{2^{n-1}} \oplus T_{n-1}P_\beta & I_{2^{n-1}} \\ (I_{2^{n-1}} \oplus T_{n-1}P_\beta)^2 & 0_{2^{n-1}} \end{bmatrix}$. By linear algebra, multiplying a matrix by a nonsingular square matrix does not change its nullity. Summarily $nu(T_n \oplus P_\alpha) = nu(I_{2^{n-1}} \oplus T_{n-1}P_\beta)^2$. We note that $nu((I_{2^{n-1}} \oplus T_{n-1}P_\beta)^2) = nu(T_{n-1}(I_{2^{n-1}} \oplus T_{n-1}P_\beta)^2P_\beta)$ where $T_{n-1}(I_{2^{n-1}} \oplus T_{n-1}P_\beta)^2P_\beta$ is identical with $T_{n-1}P_\beta \oplus P_\beta T_{n-1}$. We have proved the lemma. $\square$

<u>Proof of Lemma 2.7</u> We now prove (i) by induction on n. $T_1L_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ and then $(T_1L_1)^2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = L_1T_1$. Then (i) is true when $n = 1$. Assume that (i) is true for n with $1 \leq n \leq k$. Consider $n = k+1$. It is noted that $L_{k+1} = \begin{bmatrix} 0_{2^k} & L_k \\ L_k & 0_{2^k} \end{bmatrix}$. Then $T_{k+1}L_{k+1} = \begin{bmatrix} T_k & T_k \\ 0 & T_k \end{bmatrix}\begin{bmatrix} 0_{2^k} & L_k \\ L_k & 0_{2^k} \end{bmatrix} =$

$\begin{bmatrix} T_kL_k & T_kL_k \\ T_kL_k & 0_{2^k} \end{bmatrix}$. Then $(T_{k+1}L_{k+1})^2 = \begin{bmatrix} 0_{2^k} & (T_kL_k)^2 \\ (T_kL_k)^2 & (T_kL_k)^2 \end{bmatrix}$. By the induction assumption, $(T_kL_k)^2 = L_kL_k$. Therefore $T_{k+1}L_{k+1} = \begin{bmatrix} 0_{2^k} & L_kT_k \\ L_kT_k & L_kT_k \end{bmatrix}$ where the right side is identical with $L_{k+1}T_{k+1}$. Thus (i) is true for $n = k+1$. We then have proved (i). Due to the part (i), $(T_nL_n)^2 = L_nT_n$. Then $(T_nL_n)^2 \cdot L_nT_n = L_nT_n \cdot L_nT_n$ and then $T_nL_n = (L_nT_n)^2$. This proves (ii). □

<u>Proof of Lemma 2.8</u> Due to the structure of T_n and Lemma 2.4, $T_nL_n \oplus L_nT_n = \begin{bmatrix} T_{n-1}L_{n-1} & T_{n-1}L_{n-1} \oplus L_{n-1}T_{n-1} \\ T_{n-1}L_{n-1} \oplus L_{n-1}T_{n-1} & L_{n-1}T_{n-1} \end{bmatrix}$.
Set $B = \begin{bmatrix} L_{n-1}T_{n-1} & 0_{2^{n-1}} \\ 0_{2^{n-1}} & T_{n-1}L_{n-1} \end{bmatrix}$ and
$C = \begin{bmatrix} I_{2^{n-1}} & 0_{2^{n-1}} \\ I_{2^{n-1}} \oplus L_{n-1}T_{n-1} & I_{2^{n-1}} \end{bmatrix}$. Due to Lemma 2.7, $(L_{n-1}T_{n-1})^2 = T_{n-1}L_{n-1}$ and $(T_{n-1}L_{n-1})^2 = L_{n-1}T_{n-1}$. Then $CB(T_nL_n \oplus L_nT_n) = \begin{bmatrix} I_{2^{n-1}} & I_{2^{n-1}} \oplus T_{n-1}L_{n-1} \\ 0_{2^{n-1}} & I_{2^{n-1}} \oplus T_{n-1}L_{n-1} \oplus L_{n-1}T_{n-1} \end{bmatrix}$. Summarily $nu(T_nL_n \oplus L_nT_n) = nu(I_{2^{n-1}} \oplus T_{n-1}L_{n-1} \oplus L_{n-1}T_{n-1})$. □

<u>Proof of Lemma 2.9</u> Due to the structure of T_n and Lemma 2.4, $I_{2^n} \oplus T_nL_n \oplus L_nT_n$
$= \begin{bmatrix} I_{2^{n-1}} \oplus T_{n-1}L_{n-1} & T_{n-1}L_{n-1} \oplus L_{n-1}T_{n-1} \\ T_{n-1}L_{n-1} \oplus L_{n-1}T_{n-1} & I_{2^{n-1}} \oplus L_{n-1}T_{n-1} \end{bmatrix}$.

Set $B = \begin{bmatrix} L_{n-1}T_{n-1} & 0_{2^{n-1}} \\ 0_{2^{n-1}} & T_{n-1}L_{n-1} \end{bmatrix}$, $C = \begin{bmatrix} I_{2^{n-1}} & 0_{2^{n-1}} \\ I_{2^{n-1}} & I_{2^{n-1}} \end{bmatrix}$ and $D = \begin{bmatrix} T_{n-1} & T_{n-1} \\ 0_{2^{n-1}} & L_{n-1} \end{bmatrix}$. Due to Lemma 2.7, $(L_{n-1}T_{n-1})^2 = T_{n-1}L_{n-1}$ and $(T_{n-1}L_{n-1})^2 = L_{n-1}T_{n-1}$. We then have

$CB(I_{2^n} \oplus T_nL_n \oplus L_nT_n)D = \begin{bmatrix} T_{n-1} \oplus L_{n-1} & 0_{2^{n-1}} \\ 0_{2^{n-1}} & 0_{2^{n-1}} \end{bmatrix}$. Summarily $nu(I_{2^n} \oplus T_nL_n \oplus L_nT_n) = 2^{n-1} + nu(T_{n-1} \oplus L_{n-1})$. □

<u>Proof of Lemma 2.10</u> Due to the structure of T_n and Lemma 2.4, $T_n \oplus L_n = \begin{bmatrix} T_{n-1} & T_{n-1} \oplus L_{n-1} \\ L_{n-1} & T_{n-1} \end{bmatrix}$. Set $B = \begin{bmatrix} T_{n-1} & 0_{2^{n-1}} \\ T_{2^{n-1}} & L_{n-1} \end{bmatrix}$. It is noted that
$B(T_n \oplus L_{n-1}) = \begin{bmatrix} I_{2^{n-1}} & I_{2^{n-1}} \oplus T_{n-1}L_{n-1} \\ 0_{2^{n-1}} & I_{2^{n-1}} \oplus T_{n-1}L_{n-1} \oplus L_{n-1}T_{n-1} \end{bmatrix}$. Summarily $nu(T_n \oplus L_n) = nu(I_{2^{n-1}} \oplus T_{n-1}L_{n-1} \oplus L_{n-1}T_{n-1})$. □

<u>Proof of Lemma 7.3</u> We first prove (i) by induction on k. Due to Lemma 7.1, (i) is true for $k = 0$. We assume that (i) is true

for k with $0 \le k \le s-1$. We next prove that (i) is true for $k = s$. Due to Lemma 2.9, $nu(I_{2^{2s+1}} \oplus T_{2s+1}L_{2s+1} \oplus L_{2s+1}T_{2s+1})$ $= 2^{2s} + nu(T_{2s} \oplus L_{2s})$. By using Lemma 2.10, $nu(T_{2s} \oplus L_{2s})$ $= nu(I_{2^{2s-1}} \oplus T_{2s-1}L_{2s-1} \oplus L_{2s-1}T_{2s-1})$. Due to the induction assumption, $nu(I_{2^{2s-1}} \oplus T_{2s-1}L_{2s-1} \oplus L_{2s-1}T_{2s-1}) = \frac{2}{3}(2^{2s-1}+1)$. Summarily $nu(T_{2s+1}L_{2s+1} \oplus L_{2s+1}T_{2s+1}) = 2^{2s} + \frac{2}{3}(2^{2s-1}+1)=$ $\frac{2}{3}(2^{2s+1}+1)$. Then (i) is true for $k = s$. We have proved (i).

We now prove (ii) by induction on k. Due to Lemma 7.1, (ii) is true for $k = 1$. We assume that (ii) is true for k with $0 \le k \le s-1$. We next prove that (ii) is true for $k = s$. Due to Lemma 2.9, $nu(I_{2^{2s}} \oplus T_{2s}L_{2s} \oplus L_{2s}T_{2s})$ is equal to $2^{2s-1} +$ $nu(T_{2s-1} \oplus L_{2s-1})$. By using Lemma 2.10, $nu(T_{2s-1} \oplus L_{2s-1})$ $= nu(I_{2^{2s-2}} + T_{2s-2}L_{2s-2} \oplus L_{2s-2}T_{2s-2})$. Due to the induction assumption, $nu(I_{2^{2s-2}} + T_{2s-2}L_{2s-2} \oplus L_{2s-2}T_{2s-2})$ $\frac{2}{3}(2^{2s-2}-1)$. Summarily $nu(I_{2^{2s}} \oplus T_{2s}L_{2s} \oplus L_{2s}T_{2s}) = 2^{2s-1} + \frac{2}{3}(2^{2s-2}-1)$ $= \frac{2}{3}(2^{2s}-1)$. Then (ii) is true for $k = s$. We have proved (ii). □

<u>Proof of Lemma 7.4</u> We first prove (i). Due to Lemma 2.8, $nu(T_{2k+1}L_{2k+1} \oplus L_{2k+1}T_{2k+1}) = nu(I_{2^{2k}} \oplus T_{2k}L_{2k} \oplus L_{2k}T_{2k})$. From Lemma 7.3, $nu(I_{2^{2k}} \oplus T_{2k}L_{2k} \oplus L_{2k}T_{2k}) = \frac{2}{3}(2^{2k}-1)$. Then (i) is true. We next prove (ii). Due to Lemma 2.8, $nu(T_{2k}L_{2k} \oplus L_{2k}T_{2k}) = nu(I_{2^{2k-1}} \oplus T_{2k-1}L_{2k-1} \oplus L_{2k-1}T_{2k-1})$. From Lemma 7.3, $nu(I_{2^{2k-1}} \oplus T_{2k-1}L_{2k-1} \oplus L_{2k-1}T_{2k-1}) = \frac{2}{3}(2^{2k-1}+1)$. Then we have proved (ii). □

<u>Proof of Lemma 7.5</u> Repeatedly using Lemma 2.5, we know that $nu(T_nP_\alpha \oplus P_\alpha T_n) = 2^{n-t} \cdot nu(T_tL_t \oplus L_tT_t)$. There exist two cases to be considered: $t = 2k+1$ (Case 1) and $t = 2k$ (Case 2). We first prove the lemma for $t = 2k+1$. When $t = 2k+1$, by using Lemma 7.4, we know that $2^{n-t} \cdot nu(T_tL_t \oplus L_tT_t) = 2^{n-t} \cdot \frac{2}{3}(2^{2k}-1)$ $= \frac{2}{3}(2^{n-1} - 2^{n-t})$. This proves the lemma for Case 1. We next prove the lemma for Case 2, i.e., $t = 2k$. By using Lemma 7.4, we know that $2^{n-t} \cdot nu(T_tL_t \oplus L_tT_t)$ is equal to $2^{n-t} \cdot \frac{2}{3}(2^{2k-1}+1)$ $= \frac{2}{3}(2^{n-1} + 2^{n-t})$. We have proved the lemma for Case 2. □