Computing Möbius Transforms of Boolean Functions and Characterising Coincident Boolean Functions

Josef Pieprzyk and Xian-Mo Zhang

Department of Computing
Macquarie University, Australia

Outline

- The Möbius Transform of a Boolean Function f relates the truth table to its algebraic normal form (ANF).

- We compute the Möbius Transforms of Boolean Functions in different methods,

- We notice a special case when f is identical with its Möbius Transform. We call such a function coincident.

- We characterise coincident Boolean Functions in different ways.

Brief Introduction to Boolean Functions

- The vector space of n-tuples of elements from $GF(2)$ is denoted by $(GF(2))^n$.

- A Boolean function f is a mapping from $(GF(2))^n$ to $GF(2)$. We write f as $f(x)$ or $f(x_1, \ldots, x_n)$ where $x = (x_1, \ldots, x_n)$.

- We list all vectors in $(GF(2))^n$ as $(0, \ldots, 0, 0) = \alpha_0$, $(0, \ldots, 0, 1) = \alpha_1$, ..., $(1, \ldots, 1, 1) = \alpha_{2^n-1}$ and call α_i the binary representation of integer i.

- The truth table of a function f on $(GF(2))^n$ is a $(0, 1)$-sequence defined by $(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$,

Brief Introduction to Boolean Functions (Cont'd)

- The Hamming weight of $HW(\xi)$ is the number of nonzero coordinates of ξ.

- In particular, if ξ represents the truth table of a function f, then $HW(\xi)$ is called the Hamming weight of f, denoted by $HW(f)$.

Möbius Transforms of Boolean Functions

- The function f on $(GF(2))^n$ can be uniquely represented as

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

  where $\alpha = (a_1, \ldots, a_n)$ and g is also a function on $(GF(2))^n$.

- (1) is called the algebraic normal form (ANF) of f.

- g is called the Möbius transform of f, denoted by $g = \mu(f)$.

Computing $\mu(f)$ by Matrix

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

- Theorem 1 T_n satisfies : $T_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $T_s = \begin{bmatrix} T_{s-1} & T_{s-1} \\ O_{2^{s-1}} & T_{s-1} \end{bmatrix}$, where $O_{2^{s-1}}$ denotes the $2^{s-1} \times 2^{s-1}$ zero matrix, $s = 2, 3, \ldots$.

- Lemma 1 $T_n^{-1} = T_n$.

Computing $\mu(f)$ by Matrix (Cont'd)

- Example 1 $T_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$,

  $T_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ and

  $$T_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Computing $\mu(f)$ by Matrix (Cont'd)

- Theorem 2 The following are equivalent:

  (i) $g = \mu(f)$, (ii) $f = \mu(g)$,

  (iii) $(f(\alpha_0),\ f(\alpha_1), \ldots, f(\alpha_{2^n-1}))\, T_n = (g(\alpha_0),\ g(\alpha$ $g(\alpha_{2^n-1}))$,

  (iv) $(g(\alpha_0),\ g(\alpha_1), \ldots, g(\alpha_{2^n-1}))T_n = (f(\alpha_0),\ f(\alpha_1$ $f(\alpha_{2^n-1}))$.

- Example 2 Let $f(x_1, x_2, x_3) = 1 \oplus x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_2x_3$. Then $g = \mu(f)$ has the truth table (10111001) and f has the truth table: (11010011). (10111001)T_3= (11010011), (11010011)T_3= (10111001).

Computing $\mu(f)$ by Polynomials

- Define $D_\alpha(x) = (1 \oplus a_1 \oplus x_1) \cdots (1 \oplus a_n \oplus x_n)$ where $x = (x_1, \ldots, x_n)$, $\alpha = (a_1, \ldots, a_n)$.

- It is known that

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

- Lemma 2

(i) $\mu(D_\alpha)(x) = x_1^{a_1} \cdots x_n^{a_n}$ where $\alpha = (a_1, \ldots, a_n)$,

(ii) $\mu(x_1^{a_1} \cdots x_n^{a_n}) = D_\alpha(x)$.

- Theorem 3 Set $g = \mu(f)$. Then

$$\mu(f)(x) = \bigoplus_{\alpha \in (GF(2))^n} f(\alpha) x_1^{a_1} \cdots x_n^{a_n}$$

Computing $\mu(f)$ by Recursive Relations

- It is known that $f(x) = x_1 g(y) \oplus h(y)$ where $x = (x_1, \ldots, x_n)$ and $y = (x_2, \ldots, x_n)$.

- Theorem 4
  $\mu(f)(x) = x_1(\mu(g)(y) \oplus \mu(h)(y)) \oplus \mu(h)(y)$.

Properties of $\mu(f)$

- Corollary 1 $\mu^{-1} = \mu$.

- Let P be a permutation on $\{1, \ldots, n\}$. Define the function f_P as
  $f_P(x_1, \ldots, x_n) = f(x_{P(1)}, \ldots, x_{P(n)})$.

- Theorem 5 $\mu(f_P) = g_P$.

- Note: P in Theorem 5 is a permutation on $\{1, \ldots, n\}$ but P cannot be extended to be a permutation on $(GF(2))^n$.

Properties of $\mu(f)$ (Cont'd)

- Theorem 6 $deg(f) + deg(\mu(f)) \geq n$.

- Note: the lower bound in Theorem 6 can be reached.

- Example 3 $f(x) = (1 \oplus x_1) \cdots (1 \oplus x_n)$. By Lemma 2, $\mu(f)$ is the constant one. Then $deg(f) + deg(\mu(f)) = n + 0 = n$.

Concept of Coincident Boolean Functions

- If f and $g = \mu(f)$ are identical, i.e., $f = \mu(f)$, Then f is called a coincident function on $(GF(2))^n$.

- Example 4 Set $f(x_1, x_2, x_3, x_4) = x_2x_4 \oplus x_2x_3 \oplus x_1x_2 \oplus x_1x_3x_4 \oplus x_1x_2x_4 \oplus x_1x_2x_3$. Then the truth table of $\mu(f)$ is (0000011000011110). By computing, the truth table of f is also (0000011000011110). Then f is coincident and $\mu(f) = f$.

- Theorem 7 Let ξ and η be the truth tables of f and $g = \mu(f)$. Then the following 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.

Characterisations and Constructions of Coincident Functions (by Matrix)

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

- Theorem 8 Let ξ and η be the truth tables of f and $g = \mu(f)$ respectively. Then the following are equivalent: (i) f is coincident, (ii) g is coincident, (iii) $\xi T_n^* = 0$, (iv) $\eta T_n^* = 0$.

- Theorem 9 f is coincident $\Longleftrightarrow$ its truth table satisfies $(\zeta T_{n-1}^*, \zeta)$.

Characterisations and Constructions of Coincident Functions (by Matrix)-Cont'd

- Theorem 10 f is coincident $\Longleftrightarrow$ its truth table ξ can be expressed as $\xi = \eta T_n^*$.

- Theorem 11 f is coincident $\Longleftrightarrow$ its truth table is a linear combination of rows of T_n^*.

Characterisations and Constructions of Coincident Functions (by Matrix)-Cont'd

- Example 5 $T_3^* = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$.

- Consider $f(x_1, x_2, x_3) = x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3$.

- By definition, f is coincident because f and $\mu(f)$ have the same truth table (00000111).

- (00000111)T_3^* = (00000000). By Theorem 8, f is coincident.

- (00000111) = (01110000)T_3^*. By Theorem 11, f is coincident.

Enumeration of Coincident Functions

- Theorem 12

  (1) T_n^* has a rank 2^{n-1}, (ii) all the top 2^{n-1} rows of T_n^* form a basis of rows of T_n^*.

- Theorem 13 f is coincident $\Longleftrightarrow$ its truth table of f is a linear combination of top 2^{n-1} rows of T_n^*.

- Theorem 14

  (i) There precisely exist $2^{2^{n-1}}$ coincident functions of n variables, (ii) they form 2^{n-1}-dimensional linear space.

Enumeration of Coincident Functions (Cont'd)

- Example 6 The top 4 rows of T_3^*:

$$\begin{matrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{matrix}$$

  All ($2^{2^{3-1}} = 16$) linear combinatios: (01111111), (00010101), (00010011), (00000001), (0000011 (00000110), (01101010), (00010100), (0110110 (01101011), (01111110), (01101100), (0111100 (01111001), (00010010), (00000000).

- They have the ANFs: $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3$, $x_2x_3 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_1x_2x_3$, $x_1x_3 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_1x_3 \oplus x_1x_2$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_2$, $x_2x_3 \oplus x_1x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_2 \oplus x_1x_2x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2$, $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3$, $x_3 \oplus x_2 \oplus x_1 \oplus x_2x_3 \oplus x_1x_2x_3$, $x_2x_3 \oplus x_1x_2$, 0

Characterisations and Constructions of Coincident Functions (by Polynomial)

- Define a mapping Ψ as $\Psi(f) = h \iff f \oplus \mu(f) = h$.

- Theorem 15 The following are equivalent: (i) h is coincident, (ii) $h = \Psi(f)$ or $h = f \oplus \mu(f)$ for some f, (iii) $\Psi(h) = 0$.

- Lemma 3 $D_\alpha(x) \oplus x_1^{a_1} \cdots x_n^{a_n}$ is coincident.

- Theorem 16 h is coincident $\iff$ if and only if h is a linear combination of all $D_\alpha(x) \oplus x_1^{a_1} \cdots x_n^{a_n}$

Characterisations and Constructions of Coincident Functions (by Recursive Formula)

- Theorem 17 f is coincident $\iff f(x) = x_1 g(y) \oplus \Psi(g)(y)$ for some g. Furthermore, if f is nonzero then g is nonzero.

- Theorem 18 f is coincident $\iff f(x_1, \ldots, x_n) = x_1 f_1(x_2, \ldots, x_n) \oplus x_2 f_2(x_3, \ldots, x_n) \oplus \cdots \oplus x_{n-1} f_{n-1}(x_n) \oplus f_n(x_n)$ where $x_i f_i(x_{i+1}, \ldots, x_n) \oplus \cdots \oplus x_{n-1} f_{n-1}(x_n) \oplus f(x_n)$ $= \Psi(x_{i-1} f_{i-1}(x_i, \ldots, x_n) \oplus \cdots \oplus x_{n-1} f_{n-1}(x_n) \oplus f_n(x_n))$, $i = 2, \ldots, n$.

Properties of Coincident Functions

- <u>Theorem 19</u> f is coincident $\Longleftrightarrow$ f_P is coincident, where f_P is defined before, i.e., $f_P(x_1, \ldots, x_n) = f(x_{P(1)}, \ldots, x_{P(n)})$.

- <u>Theorem 20</u> If f is a nonzero coincident function then each variable x_j appears in a monomial of the ANF of f.

- <u>Theorem 21</u> If f be a coincident function on $(GF(2))^n$ then either the ANF of f has every linear term x_j, or, the ANF does not have any linear term.

- <u>Example 7</u> $x_3 \oplus x_2 \oplus x_1 \oplus x_1x_2 \oplus x_1x_2x_3$ and $x_2x_3 \oplus x_1x_2$ are both coincident.

Properties of Coincident Functions (Cont'd)

- Corollary 2 If f is a coincident function then $f(0) = 0$.

- Theorem 22 If f is 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 of $(n-r)$ variables.

A Lower Bound on Degree of Coincident Functions

- Theorem 23 If f be a coincident function on $(GF(2))^n$ then $deg(f) \geq \lceil \frac{1}{2}n \rceil$. More precisely,

  (i) $deg(f) \geq \frac{1}{2}n$ (n is even)

  (ii) $deg(f) \geq \frac{1}{2}(n+1)$ (n is odd).

- The lower bound in Theorem 23 is tight. For example, $f(x_1, x_2, x_3, x_4) = x_2x_4 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_3$ is a coincident function on $(GF(2))^4$ having a degree two.

Coincident Functions with High Nonlinearity and High Degree

- The nonlinearity N_f of a function f is defined as $N_f = \min_{i=1,2,\ldots,2^{n+1}} d(f, \psi_i)$ where ψ_1, ψ_2, $\ldots$, $\psi_{2^{n+1}}$ are all the affine functions on $(GF(2))^n$.

- It is known that $N_f \leq 2^{n-1} - 2^{\frac{1}{2}n-1}$.

- Construction 1 (Even Variables):

- Let $f(x_1, \ldots, x_{2k}) = x_1x_2 \oplus \cdots \oplus x_{2k-1}x_{2k}$. Set $h = f \oplus \mu(f)$.

- Theorem 24 In Construction 1

  (i) h is coincident function,

  (ii) $N_h \geq 2^{2k-1} - 2^{k-1} - k$,

  (iii) $deg(h) \geq 2k - 2$.

Coincident Functions with High Nonlinearity and High Degree (Cont'd)

- Construction 2 (Odd Variables):

- 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 $h = f \oplus \mu(f)$.

- Theorem 25 In Construction 2

  (i) h is coincident function,

  (ii) $N_h \geq 2^{2k} - 2^k - k$,

  (iii) $deg(h) \geq 2k - 1$.

Conclusion

- We presented different methods to compute $\mu(f)$ and studied properties of $\mu(f)$.

- We proposed the concept of coincident functions and characterised such functions.