Properties and constructions of coincident functions

Morgan Barbier, Hayat Cheballah, Jean-Marie Le Bars

Noname manuscript No.
(will be inserted by the editor)

Properties and constructions of coincident functions

Morgan Barbier · **Hayat Cheballah** ·
Jean-Marie Le Bars

the date of receipt and acceptance should be inserted later

Abstract Extensive studies of Boolean functions are carried in many fields. The Mobius transform is often involved for these studies. In particular, it plays a central role in coincident functions, the class of Boolean functions invariant by this transformation. This class – which has been recently introduced – has interesting properties, in particular if we want to control both the Hamming weight and the degree. We propose an innovative way to handle the Mobius transform which allows the composition between several Boolean functions and the use of Shannon or Reed-Muller decompositions. Thus we benefit from a better knowledge of coincident functions and introduce new properties. We show experimentally that for many features, coincident functions look like any Boolean functions.

Keywords Boolean functions, Möbius transform, Coincident functions, Shannon and Reed-Muller decompositions

1 Introduction

Numerous studies with Boolean functions have been conducted in various fields like cryptography and error correcting codes (Carlet (2010)), Boolean circuits and Boolean Decision Diagram (Bryant (1986)), Boolean logic (Boole (1848)) or constraint satisfaction problems (Creignou et al. (2001)). There are many ways to represent a Boolean function which depends of the domain. For instance, on propositional logic one usually uses the conjunctive normal form or the disjunctive normal form, while we often use the BDD in Boolean circuits. Most of the time these studies involve several criteria. In cryptography, the (algebraic) degree and the (Hamming) weight are crucial criteria.

M. Barbier · Hayat Cheballah · J.-M. Le Bars
ENSICAEN - UNICAEN - GREYC
E-mail: morgan.barbier@ensicaen.fr
E-mail: hayat.cheballah@gmail.com
E-mail: jean-marie.lebars@unicaen.fr

Unfortunately, the best representation for the degree is the Algebraic Normal Form (sum of monomials), while the weight requires the truth table (sum of minterms). Thus the Reed-Muller decomposition (or expansion) allows us to perform recursive decomposition (Kasami and Tokura (1970)), enumeration and random generation among the degree whereas the Shannon decomposition (or expansion) does the same task among the weight Shannon (1949) shows the switching network interpretation of this identity, but (Boole (1854)) will be the first to mentioned it. These decompositions allow us to decompose a Boolean function with n variables into two Boolean functions with $n-1$ variables or equivalently to build a Boolean function with n variables with two Boolean functions with $n-1$ variables.

Since these decompositions appear to be orthogonal, it seems unreachable to consider them simultaneously or to perform enumeration or random generation with both criteria. This is why we propose the study of coincident functions for which we have a correspondence between the monomials and the minterms.

In Pieprzyk et al. (2011), the author defined for the first time the class of coincident functions, the boolean functions invariant by Mobius transform (see Guillot (1999) phd Thesis for a deep study of this property). We revisit their results with a new point of view more convenient, in particular we introduce a Mobius transform conditioned by the number of variables which gives a recursive (Reed-Muller and Shannon) decomposition of Mobius transform, linking the two decompositions. We investigate the distribution of degree and weight and provide a uniform random generator of these functions. We also benefit to the structure of lattice of the valuations to study the monotonic coincident functions and to provide a complete construction of symmetric coincident ones.

The paper is organized as follows. We recall the basic definitions related to boolean functions and to Mobius transform in Section 2. We introduce our new point of view and the resulting properties concerning Mobius transform and coincident in Section 3. Thanks to lattices, we exhibit, in Section 4, links between coincident functions with monotonic and symmetric functions, and also the random generation of coincident functions. Finally, we propose in Section 5 a set of experiment resulting on coincident functions.

2 Definition and first properties of Boolean functions and Mobius transform

2.1 Boolean function

Let $\mathcal{F}_n$ be the set of the boolean functions with n variables. Monomials and minterms play a role of canonical element in the different writings.

Definition 1 (Monomials and minterms) Let us to denote $x = (x_1, \ldots, x_n)$. For any $u = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$, x^u will be denoted the monomial $x_1^{u_1} \ldots x_n^{u_n}$. The minterm M_u is the Boolean function with n variables defined by

$$M_u(a) = \begin{cases} 1, & \text{if } u = a; \\ 0, & \text{otherwise.} \end{cases}$$

The two following definitions provide two different point of views what we wish to link.

Definition 2 (Algebraic Normal Form – ANF) A boolean function f can be viewed as the exclusive sum of a subset of the set of monomials in variables $x_1, \ldots, x_n$.

$$f = \bigoplus_{u \in \mathcal{F}_2^n} \alpha_u x^u.$$

Definition 3 (Truth table or valuations of f) A boolean function f can be viewed as the exclusive sum of a subset of the set of minterms in variables $x_1, \ldots, x_n$.

$$f = \bigoplus_{u \in \mathcal{F}_2^n} \beta_u M_u.$$

Notation 1 *Let u and $v \in \mathbb{F}_2^n$. We will write $u \preceq v$ when $u_i \leq v_i$, for any $i \in \{1, \ldots, n\}$ and $u \prec v$ when $u \preceq v$ and $u \neq v$.*

The previous partially ordered set provides connection between these notions.

Proposition 1 *Let $u \in \mathbb{F}_2^n$, then*

$$x^u = \bigoplus_{u \preceq v} M_v. \tag{1}$$

Proof Let $f = x^u$ and $a \in \mathbb{F}_2^n$, $f(a) = 1$ if and only if $a_i = 1$ for all i such that $u_i = 1$, *ie* $u \preceq a$. Hence $f = \bigoplus_{u \preceq v} M_v$.

Proposition 2 *Let $u \in \mathbb{F}_2^n$, then*

$$M_u = \bigoplus_{u \preceq v} x^v. \tag{2}$$

Proof Let $u = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$. It is easily seen that M_u is equal to the product $\prod_{i=1}^n (x_i \oplus u_i \oplus 1)$. Let $I_0(u) = \{i \in \{1, \ldots, n\} : u_i = 0\}$ and $I_1(u) = \{i \in \{1, \ldots, n\} : u_i = 1\}$, it follows

$$\begin{aligned} M_u &= \textstyle\prod_{i \in I_1(u)} x_i \prod_{i \in I_0(u)} (1 \oplus x_i) \\ &= \textstyle\bigoplus_{u \preceq v} x^v. \end{aligned}$$

Notation 2 *There are several natural ways to encode f by a binary word of length 2^n.*

We will choose the following natural encodings directly derived by the previous definition.

$$T(f) = t_1 \ldots t_{2^n},$$

where t_k, with $\sum_{i=1}^n u_i \, 2^{i-1}$ the 2-adic representation of k and $t_k = \beta_u$.

$$A(f) = a_1 \ldots a_{2^n},$$

where $a_k = \alpha_u$.

We denote by ψ the bijection $\psi(A(f)) = T(f)$.

The two definitions below introduce crucial parameters of a boolean function.

Definition 4 (Hamming weight) Let $f \in \mathcal{F}_n$ be a boolean function, we will write $w_H(f)$ the (Hamming) weight of f, *ie* the number of 1 of $T(f)$.

Definition 5 (Algebraic degree) Let $f \in \mathcal{F}_n$ be a boolean function, we will write $d(f)$ the (algebraic) degree of f, *ie* the maximal degree of the monomials in the ANF of f.

While the Reed-Muller decomposition is related to the algebraic normal form, the Shannon one is associated to truth table.

Definition 6 (Reed-Muller decomposition) Let $f \in \mathcal{F}_n$. The *Reed-Muller decomposition*, consists in rewriting the boolean function as

$$f = f_R^0 \oplus x_n f_R^1,$$

where $f_R^0, f_R^1 \in \mathcal{F}_{n-1}$ and are unique.

Definition 7 (Shannon decomposition) Let $f \in \mathcal{F}_n$. The *Shannon decomposition*, consists in rewriting the boolean function as

$$f = (1 + x_n) f_S^0 \oplus x_n f_S^1,$$

where $f_S^0, f_S^1 \in \mathcal{F}_{n-1}$ and are unique.

Remark 1 Let $f \in \mathcal{F}_n$. Clearly, we have by identification $f_R^0 = f_S^0$ and $f_R^1 = f_S^0 \oplus f_S^1$.

Remark 2 The Shannon decomposition is the natural decomposition for manipulating the minterms since $T(f) = T(f_S^0) \mid T(f_S^1)$, where $\mid$ denotes the concatenation. This trivially implies

$$w_H(f) = w_H(f_S^0) + w_H(f_S^1).$$

Remark 3 The Reed-Muller decomposition is the natural decomposition for manipulating the monomials since $A(f) = A(f_R^0) \mid A(f_R^1)$. This implies

$$d(f) = max(d(f_R^0), d(f_R^1) + 1).$$

Notation 3 *From now one, we will write* 0_n *the valuation of* $\mathbb{F}_2^n$ $(0, \ldots, 0)$ *and* $\mathbf{0}_n$ *(resp.* $\mathbf{1}_n$*) the Boolean function with* n *variables which takes the value* 0 *(resp.* 1*) for any valuation.*

2.2 Mobius transform

The Mobius transform is at the heart of this article.

Definition 8 (Mobius transform) The *Mobius transform*, noted μ is defined by the following bijection

$$\begin{aligned} \mu : \mathcal{F}_n &\longleftrightarrow \mathcal{F}_n \\ f &\longmapsto \mu(f), \end{aligned}$$

such that, for any $f \in \mathcal{F}_n$

$$f = \bigoplus_{u \in \mathbb{F}_2^n} \mu(f)(u) x^u.$$

The statements of the following proposition derives directly from the definition of the Mobius transform.

Proposition 3 *(Pieprzyk et al. 2011, Theorem 1 and Lemma 3) Let $f, g \in \mathcal{F}_n$ and $u \in \mathbb{F}_2^n$,*

$$\mu(f \oplus g) = \mu(f) \oplus \mu(g) \text{ and } \mu(f)(0_n) = f(O_n).$$

Proof Both results are direct implication of the definition of μ, let $f = \bigoplus_{u \in \mathbb{F}_2^n} \mu(f)(u)x^u$ and $g = \bigoplus_{u \in \mathbb{F}_2^n} \mu(g)(u)x^u$. Then $f \oplus g = \bigoplus_{u \in \mathbb{F}_2^n} (\mu(f)(u) \oplus \mu(g)(u))x^u$ and $\mu(f \oplus g)(u) = \mu(f)(u) \oplus \mu(g)(u)$. Therefore let $a = 0_n$, $a^u = 0$ for any $a \prec u$, then $f(0_n) = \mu(f)(a)$.

Proposition 4 *(Pieprzyk et al. 2011, Lemma 2) Let $u \in \mathbb{F}_2^n$, then $\mu(x^u) = M_u$ and $\mu(M_u) = x^u$.*

Proof Let $u = (u_1, \ldots, u_n) \in \mathbb{F}_2^n$ and $f = x^u$. $f = \bigoplus_{v \in \mathbb{F}_2^n} \mu(f)(v)x^v$. Then $\mu(f)(v)$ is equal to 1 if $v = u$ and equal to 0 otherwise, which is the definition of M_u.

$$\begin{aligned} M_u &= \textstyle\bigoplus_{u \preceq v} x^v \text{ by (2)} \\ \mu(M_u) &= \textstyle\bigoplus_{u \preceq v} \mu(x^v) \\ &= \textstyle\bigoplus_{u \preceq v} M_v \\ &= x^u \text{ by (1)}. \end{aligned}$$

Proposition 5 *The Mobius transform is a involution, ie $\mu^2(f) = f$ and $\mu(f) = g$ if and only if $\mu(g) = f$.*

Proof

$$\begin{aligned} f &= \textstyle\bigoplus_{u \in \mathbb{F}_2^n} \mu(f)(u)x^u \\ \mu(f) &= \textstyle\bigoplus_{u \in \mathbb{F}_2^n} \mu(f)(u)M_u \\ \mu^2(f) &= \textstyle\bigoplus_{u \in \mathbb{F}_2^n} \mu(f)(u)x^u. \end{aligned}$$

3 New properties on Mobius transform and coincident functions

Let us start this section by the following remark, which is one of main statement of this paper.

Notation 4 *Let $f \in \mathcal{F}_n$, we will denote by $P(f)$ the polynomial form of f.*

Remark 4 The polynomial form contains only the variables which play a role for the evaluation of the function. We will denote by indeterminates these variables. We may increase the numbers of variables by keeping the same number of indeterminates. Let $f_n \in \mathcal{F}_n$ then for all $k > 0$, it exists $f_{n+k} \in \mathcal{F}_{n+k}$, such that f_n and f_{n+k} share the same polynomial form, $P(f_n) = P(f_{n+k})$. Furthermore $T(f_{2+k}) = T(f_2) * 2^k$ (we repeat 2^k times the word $T(f_2)$).

For instance, the Boolean function with two variables f_2 such that $T(f_2) = 0110$ has the polynomial form $P = P(f_2) = x_1 \oplus x_2$ and f_3 such that $T(f_3) = 01100110$ satisfies $P(f_3) = x_1 \oplus x_2$.

We were wondering if the Mobius transforms of function see as n variables and $n+k$ are equals. Let $f_n \in \mathcal{F}_n$ and $f_m \in \mathcal{F}_m$ such that $n < m$ and $P(f_n) = P(f_m)$. Does the following equality holds?

$$\mu(f_n) = \mu(f_m)? \tag{3}$$

We propose to look on a particular toy example.

Example 1 Let $f_1 = x_1 \oplus 1 \in \mathcal{F}_1$ be a boolean function with one indeterminate and $f_2 = x_1 \oplus 1 \in \mathcal{F}_2$ be the same function see as a boolean function with two variables. Very simple computations give us that $\mu(f_1) = 1$ and $\mu(f_2) = x_2 \oplus 1$.

3.1 New insights of the Mobius transform

The example 1 provides a counterexample (3). Then we have to use the Mobius transform carefully if we manipulate the polynomial form of a Boolean function. In this setting, we introduce the following notation.

Notation 5 *Let $f \in \mathcal{F}_n$ be a Boolean function with n variables. We will write $\mu_n(f)$ instead of $\mu(f)$.*

Example 1 implies $\mu(x_1 \oplus 1) = \mu_1(x_1 \oplus 1) = 1$ and $\mu_2(x_1 \oplus 1) = x_2 \oplus 1$. In other words, the Mobius transform depends on the variables, not on the indeterminates.

We obtain the following result, which permits us to manipulate the Mobius transform easily, hence this is one of key ingredient.

The following theorem contains three key ingredients to manipulate properly the Mobius transform.

Theorem 1 *Let $f \in \mathcal{F}_{n-1}$. We have*

$$\mu_n(f) = (1 \oplus x_n)\mu_{n-1}(f), \tag{4}$$

$$\mu_n(x_n f) = x_n \mu_{n-1}(f), \tag{5}$$

$$\mu_n((1 \oplus x_n) f) = \mu_{n-1}(f). \tag{6}$$

Proof It is straightforward to prove Equation (4) from the definition of the Mobius transform. Indeed, we can see the computation of the Mobius transform as an interpolation problem. Since the coefficients of the monomials where occurs x_{n+1} must be null, thus the statement.
The definition of the Mobius transform give us

$$\begin{aligned}
\mu_n(x_n f) &= \mu_n(f) - \mu_{n-1}(f) \\
&= (1 \oplus x_n)\mu_{n-1}(f) - \mu_{n-1}(f) \\
&= x_n \mu_{n-1}(f),
\end{aligned}$$

which is exactly Equation (5).

Let us to compute Equality (6):

$$\begin{aligned}
\mu_n((1 \oplus x_n) f) &= \mu_n(f) \oplus \mu_n(x_n f) \\
&= (1 \oplus x_n)\mu_{n-1}(f) \oplus x_n \mu_{n-1}(f) \\
&= \mu_{n-1}(f).
\end{aligned}$$

The Reed-Muller decomposition is related to algebraic normal form, whereas the Shannon one is related to truth table. Since the Mobius transform allows us to switch from one to the other; it is natural to see the relationship between the previous decompositions and the Mobius transform.

Proposition 6 *(Pieprzyk et al. 2011, Theorem 5). Let $f \in \mathcal{F}_n$ be a boolean function and $f_R^0, f_R^1 \in \mathcal{F}_{n-1}$ be the terms of the Reed-Muller decomposition. Then*

$$\mu_n(f) = (1 \oplus x_n)\mu_{n-1}(f_R^0) \oplus x_n\mu_{n-1}(f_R^1).$$

Proof

$$\begin{aligned}\mu_n(f) &= \mu_n(f_R^0) \oplus \mu_n(x_n f_R^1)\\ &= (1 \oplus x_n)\mu_{n-1}(f_R^0) \oplus x_n\mu_{n-1}(f_R^1).\end{aligned}$$

Proposition 7 *Let $f \in \mathcal{F}_n$ be a boolean function and $f_S^0, f_S^1 \in \mathcal{F}_{n-1}$ be the terms of the Shannon decomposition. Then*

$$\mu_n(f) = \mu_{n-1}(f_S^0) \oplus x_n\mu_{n-1}(f_S^1).$$

Proof

$$\begin{aligned}\mu_n(f) &= \mu_n\left((1 \oplus x_n)f_S^0\right) \oplus \mu_n(x_n f_S^1)\\ &= (1 \oplus x_n)\mu_{n-1}\left(f_S^0\right) \oplus x_n\mu_{n-1}\left(f_S^0\right) \oplus x_n\mu_{n-1}\left(f_S^1\right)\\ &= \mu_{n-1}(f_S^0) \oplus x_n\mu_{n-1}(f_S^1)\end{aligned}$$

We find again that the Reed-Muller decomposition of the Mobius transform is the Mobius transform of the Shannon decomposition; and vice versa.

The first step to try to make a link between the algebraic degree of a boolean function and its hamming weight is given by the following proposition.

Proposition 8 *(Pieprzyk et al. 2011, Theorem 7) Let $f \in \mathcal{F}_n \setminus \{\mathbf{0}_n\}$. Then*

$$\deg(f) + \deg(\mu_n(f)) \geq n.$$

Proof Let $f = f_R^0 \oplus x_n f_R^1$. By Proposition 6,

$$\begin{aligned}\mu_n(f) &= \mu_{n-1}(f_R^0) \oplus x_n(\mu_{n-1}(f_R^0) \oplus \mu_{n-1}(f_R^1))\\ &= \mu_{n-1}(f_R^0) \oplus x_n(\mu_{n-1}(f_R^0 \oplus f_R^1)).\end{aligned}$$

Since $f \neq \mathbf{0}_n, f_R^0$ and f_R^1 cannot be null in same time, then it is easily seen that the property holds for $n = 1$.

Let $n > 1$. Assume that the property holds for $n - 1$.
Case 1) $\deg(f_R^0) \neq \deg(f_R^1)$. Then

$$\deg(f_R^0 \oplus f_R^1) = \max(\deg(f_R^0), \deg(f_R^1)) \leq \deg(f).$$

Since $\deg(f_R^0) \neq \deg(f_R^1)$, then $\deg(x_n\mu_{n-1}\left(f_R^0 \oplus f_R^1\right)) \geq \deg(\mu_{n-1}\left(f_R^0 \oplus f_R^1\right))$, so we deduce

$$\begin{aligned}\deg(f) + \deg(\mu_n(f)) &\geq \deg(f_R^0 \oplus f_R^1) + \deg(\mu_{n-1}(f_R^0 \oplus f_R^1)) + 1\\ &\geq n - 1 + 1 \qquad\qquad \text{by hypothesis of recurrence}\\ &\geq n\end{aligned}$$

Case 2) Hence $\deg(f_R^0) = \deg(f_R^1)$; moreover $\deg(f) = \deg(f_R^0) + 1$ and $\deg(\mu_n(f)) \geq \deg(\mu_{n-1}(f_R^0))$, and by hypothesis of recurrence, $\deg(f_R^0) + \deg(\mu_{n-1}(f_R^0)) \geq n-1$, hence $\deg(f) + \deg(\mu_n(f)) \geq n$.

Always with the same intended target: draw a link between algebraic degree and the Hamming weight of a boolean function; the following result gives us the probability that the Mobius transform has degree n.

Proposition 9 *Let $f \in \mathcal{F}_n$ built uniformly at random. Then*

$$\Pr(\deg(\mu_n(f)) = n \mid \deg(f) = n) = \Pr(\deg(\mu_n(f)) = n \mid \deg(f) < n)$$
$$= \Pr(\deg(\mu_n(f)) = n) = \tfrac{1}{2}.$$

Proof One may easily check the property for $n = 1$. Assume the property holds for $n-1$.

Let $f = f_R^0 \oplus x_n f_R^1$ built uniformly at random. Then $\deg(f) = n$ if and only if $x_1 \dots x_n$ occurs in the ANF of f. Since it is the case for half of the Boolean functions, $\Pr(\deg(f) = n) = \frac{1}{2}$. On the one hand $\deg(f) = n$ if and only if $d(f_R^1) = n-1$ and on the other hand, by Proposition 6, $\deg(\mu_n(f)) = n$ if and only if $\deg(\mu_{n-1}(f_R^0 \oplus f_R^1)) = n-1$. Hence

$$\Pr(\deg(\mu_n(f)) = n \mid \deg(f) = n) = \Pr(\deg(\mu_{n-1}(f_R^0 \oplus f_R^1)) = n-1 \mid \deg(f_R^1) = n-1).$$

Moreover, $\deg(\mu_{n-1}(f_R^0 \oplus f_R^1)) = n-1$ if $\deg(\mu_{n-1}(f_R^0)) = n-1$ and $\deg(\mu_{n-1}(f_R^1)) < n-1$ or $\deg(\mu_{n-1}(f_R^0)) < n-1$ and $\deg(\mu_{n-1}(f_R^1)) = n-1$.

The degree of $\mu_{n-1}(f_R^0)$ and $\mu_{n-1}(f_R^1)$ are clearly independent and $\Pr(\deg(\mu_{n-1}(f_R^0)) = n-1) = \frac{1}{2}$. It follows

$$\Pr(\deg(\mu_{n-1}(f_R^0)) = n-1 \text{ and } \deg(\mu_{n-1}(f_R^1)) < n-1 | \deg(f_R^1) = n-1)$$
$$= \Pr(\deg(\mu_{n-1}(f_R^0)) = n-1) \Pr(\deg(\mu_{n-1}(f_R^1)) < n-1 \mid \deg(f_R^1) = n-1)$$
$$= \tfrac{1}{2} \cdot \tfrac{1}{2} = \tfrac{1}{4}.$$

Similarly, we find

$$\Pr(\deg(\mu_{n-1}(f_R^0)) < n-1 \text{ and } \deg(\mu_{n-1}(f_R^1)) = n-1 | \deg(f_R^1) = n-1) = \frac{1}{4}.$$

Hence $\Pr(\deg(\mu_{n-1}(f_R^0 \oplus f_R^1)) = n-1 \mid \deg(f_R^1) = n-1) = \frac{1}{2}$.

The following proposition can be view as a new decomposition related to Mobius transform.

Proposition 10 *(Pieprzyk et al. 2011, Lemma 7). Let $n \in \mathbb{N}$ and $0 < k < n$. We will denote respectively the tuples $x = (x_1, \dots, x_n)$, $y = (x_1, \dots, x_k)$ and $z = (x_{k+1}, \dots, x_n)$. Let $f_1(y) \in \mathcal{F}_k$, $f_2(z) \in \mathcal{F}_{n-k}$ and $f(x) = f_1(y) \cdot f_2(z)$ and $g(x) = f_1(y) \oplus f_2(z)$. Then*

$$\mu_n(f(x)) = \mu_{n-k}(f_2(z)) \cdot \mu_k(f_1(y));$$
$$\mu_n(g(x)) = \textstyle\prod_{i=k+1}^{n}(1 \oplus x_i)\mu_k((f_1(y)) \oplus \prod_{i=1}^{k}(1 \oplus x_i)\mu_{n-k}(f_2(z)).$$

Proof Let $u = (u_{k+1}, \dots, u_n) \in \mathbb{F}_2^k$. By applying (4) and (5) of Proposition 1, it follows

$$\mu_{n-k}(z^u f_1(y)) = M_u(z) \cdot \mu_k(f_1(y)).$$

Hence

$$\begin{aligned}\mu_n(f(x)) &= \bigoplus_{u\in\mathbb{F}_2^n} M_u(z)\cdot\mu_k(f_1(y))\\ &= \mu_{n-k}(\bigoplus_{u\in\mathbb{F}_2^n} z^u)\cdot\mu_k(f_1(y))\\ &= \mu_{n-k}(f_2(z))\cdot\mu_k(f_1(y)).\end{aligned}$$

First $\mu_n(g(x)) = \mu_n(f_1(y)) \oplus \mu_n(f_2(z))$. Furthermore (4) of Proposition 1 implies $\mu_n(f_1(y)) = \prod_{i=k+1}^n (1\oplus x_i)\mu_k((f_1(y))$ and $\mu_n(f_2(z)) = \prod_{i=1}^k (1\oplus x_i)\mu_{n-k}(f_2(z))$.

3.2 Coincident functions

The notion of coincident function was previously introduced in Pieprzyk et al. (2011). A coincident function is a boolean function which is equal to its Mobius transform.

Definition 9 (Coincident function) Let $f \in \mathcal{F}_n$, f is called *coincident* if and only if

$$f = \mu_n(f).$$

We will denote by $\mathcal{C}_n$ the set of coincident functions with n variables.

For this particular subset of boolean functions the monomial and the associated minterms are directly related; this is the result of the following proposition. Let $f \in \mathcal{F}_n$, by Proposition 5, $f \oplus \mu_n(f) \in \mathcal{C}_n$. Here we propose an improvement of (Pieprzyk et al. 2011, Lemma 11).

Proposition 11 *Let $u \in \mathbb{F}_2^n$ and $h_u = x^u \oplus M_u$. Then h_u is coincident and*

$$h_u = \bigoplus_{u\prec v} x^v = \bigoplus_{u\prec v} M_v.$$

Proof Since $\mu_n(x^u) = M_u$, $h_u = x^u \oplus \mu_n(x^u)$ is coincident. By (2), $M_u = \bigoplus_{u\preceq v} x^v$ hence $h_u = \bigoplus_{u\prec v} x^v$.

Remark 5 We propose another point of view of the previous proposition: let $f_k = \prod_{i=1}^k x_i$, the function with all multiples of f_k, except f_k itself, give a coincident function; that is

$$f_k\left(1\oplus\prod_{i=k+1}^{n}(1\oplus x_i)\right).$$

Hence for particular coincident functions, it becomes trivial to compute their hamming weight.

Corollary 1 *Let $k = w_H(a)$. It follows $w_H(h_a) = 2^{n-k} - 1$.*

Coincident functions had a lower bound on its algebraic degree, this is a trivial consequence from Proposition 8.

Proposition 12 *(Pieprzyk et al. 2011, Theorem 31) Let $h \in \mathcal{C}_n \setminus \{0\}$ be a coincident function with n variables. Then a lower bound on its algebraic degree is*

$$\deg(h) \geq \frac{n}{2}.$$

Proof Since h is a coincident function and Proposition 8, we have that

$$\begin{aligned} \deg(h) + \deg(\mu(h)) &\geq n \\ 2\deg(h) &\geq n \\ \deg(h) &\geq \frac{n}{2}. \end{aligned}$$

Notation 6 *Let $f \in \mathcal{F}_n$. We define the operators φ_n and $\mathcal{C}_n$ by*

$$\begin{aligned} \varphi_n(f) &= f \oplus \mu_n(f) \\ \mathcal{C}_n(f) &= \left\{ f' \in \mathcal{F}_n : \varphi_n(f') = \varphi_n(f) \right\}. \end{aligned}$$

3.3 A construction of coincident functions

The following proposition gives us a simple way to build a coincident functions.

Proposition 13 *(Pieprzyk et al. 2011, Theorem 24) Let $h \in \mathcal{C}_n$, there exists a unique $g \in \mathcal{F}_{n-1}$ such that*

$$\begin{aligned} h &= g \oplus \mu_n(g) \\ &= \varphi_{n-1}(g) \oplus x_n\mu_{n-1}(g) \\ &= (1 \oplus x_n)\varphi_{n-1}(g) \oplus x_n g. \end{aligned}$$

Proof Let $h = h_R^0 \oplus x_n h_R^1 \in \mathcal{C}_{n-1}$. Then $\mu_n(h) = \mu_{n-1}(h_R^0) \oplus x_n\mu_{n-1}(h_R^0 \oplus h_R^1)$. Since $h = \mu_n(h)$, it follows $h_R^0 \in \mathcal{C}_{n-1}$ and $h_R^1 = h_R^0 \oplus \mu_{n-1}(h_R^1)$, which implies $h_R^0 = \varphi_{n-1}(h_R^1)$. Let $g = \mu_{n-1}(h_R^1)$, hence

$$\begin{aligned} g \oplus \mu_n(g) &= \mu_{n-1}(h_R^1) \oplus (1 \oplus x_n)h_R^1 \\ &= \varphi_{n-1}(h_R^1) \oplus x_n h_R^1 \\ &= h_R^0 \oplus x_n h_R^1 = h. \end{aligned}$$

Since $\varphi_{n-1}(g) = h_R^0$, we also have

$$\begin{aligned} h &= \varphi_{n-1}(g) \oplus x_n\mu_{n-1}(g) \\ &= (1 \oplus x_n)\varphi_{n-1}(g) \oplus x_n g. \end{aligned}$$

Since we have a one to one correspondence between the Boolean functions with $n-1$ variables and the coincident functions with n variables, we trivially deduce that $card(\mathcal{C}_n) = 2^{2^{n-1}}$; see (Pieprzyk et al. 2011, Theorem 18). We also show that $\mathcal{C}_n$ has a vectorial space structure.

Proposition 14 *The set $\mathcal{C}_n$ is a vectorial space of dimension 2^{n-1}.*

Proof Let h_1 and $h_2 \in \mathcal{C}_n$. We consider f_1 and $f_2 \in \mathcal{F}_2^n$ such that $h_1 = \varphi_n(f_1)$ and $h_2 = \varphi_n(f_2)$. Let $h = h_1 \oplus h_2$.

$$h = g_1 \oplus \mu_n(g_1) \oplus g_2 \oplus \mu_n(g_2) = (g_1 \oplus g_2) \oplus \mu_n(g_1 \oplus g_2),$$

hence $h = \varphi_n(f_1 \oplus f_2)$.

Corollary 2 *(Random generation of a coincident function) Let $uniform(E)$ a function which returns with the uniform distribution an element of a finite set E. The following algorithm returns with the uniform distribution a coincident function from $\mathcal{C}_n$.*

Algorithm 1: Uniform random generation of a coincident function

Input: The integer n, the number of variables.
Output: $h \in \mathcal{C}_n$ a coincident function with n variables.

begin
  $g \leftarrow$ uniform$(\mathcal{F}_{n-1})$
  $f \leftarrow \mu_n(g)$
  $h \leftarrow g \oplus f$
return h

Proposition 15 *Let $h \in C_n$ be a coincident function, then $h(0_n) = 0$.*

Proof Let f such that $h = \varphi_n(f)$, by Proposition 3, $\mu(f)(0_n) = f(0_n)$, then $h(0_n) = 0$.

Here is a strong connection between the Mobius transform of a boolean function and this one of its Reed-Muller decomposition.

Proposition 16 *Let $f = f_R^0 \oplus x_n f_R^1 \in \mathcal{F}_n$ and $h^0 = \varphi_{n-1}(f_R^0)$, $h^1 = \varphi_{n-1}(f_R^1)$ then*

$$\varphi_n(f) = h^0 + x_n(h^0 \oplus h^1 \oplus f_R^0).$$

Proof Let $h = \varphi_n(f)$. Let us to compute h

$$\begin{aligned} h &= f \oplus \mu_n(f) \\ &= f_R^0 \oplus x_n f_R^1 \oplus (1 + x_n)\mu_{n-1}(f_R^1) \oplus x_n \mu_{n-1}(f_R^1) \\ &= h^0 \oplus x_n(h^1 \oplus \mu_{n-1}(f_R^0)) \\ &= h^0 \oplus x_n(h^0 \oplus h^1 \oplus f_R^0). \end{aligned}$$

Remark 6 Proposition 13 and 16 imply $h^0 = \varphi_{n-1}(g)$ and $g = h^1 \oplus f_R^0$, *ie* $f_R^0 \in \mathcal{C}_{n-1}(g)$.

Remark 7 Let $h \in \mathcal{F}_n$, then h is coincident if and only if $h \in \mathcal{C}_n(0)$.

Corollary 3 *Let $g_1, g_2 \in \mathcal{F}_{n-1}$, $f_1 \in \mathcal{C}_n(g_1)$ and $f_2 \in \mathcal{C}_n(g_2)$. Then*

$$f_1 \oplus f_2 \in \mathcal{C}_n(g_1 \oplus g_2).$$

From the linearity, the Mobius transform of the sum of function is the sum of the Mobius transforms. We propose to look on the multiplicativity.

Proposition 17 *(Pieprzyk et al. 2011, Theorem 7) Let $n \in \mathbb{N}$ and $0 < k < n$. We will denote respectively the tuples $x = (x_1, \ldots, x_n)$, $y = (x_1, \ldots, x_k)$ and $z = (x_{k+1}, \ldots, x_n)$. Let $f_1(y) \in \mathcal{F}_k$, $f_2(z) \in \mathcal{F}_{n-k}$ and $f(x) = f_1(y) \cdot f_2(z)$. Then f is coincident if and only if f_1 and f_2 are.*

Proof This is a direct application of Proposition 10:

$$\mu_n(f(x)) = \mu_{n-k}(f_2(z)) \cdot \mu_k(f_1(y)).$$

Clearly if f_1 and f_2 are coincident functions, then $\mu_n(f(x)) = f_2(z) \cdot f_1(y) = f(z)$ and f is a coincident function. Conversely, $\mu_n(f(x)) = f(z)$ implies $\mu_{n-k}(f_2(z)) = f_2(z)$ and $\mu_k(f_1(y)) = f_1(y)$.

We exhibit now some constructions of coincident functions available for any number of variables.

Proposition 18 *Let $n \in \mathbb{N}^*$ be a positive integer, the boolean functions:*

1. $\mu_n(0_n) = 0_n$,
2. $\prod_{i=1}^{n} x_i$,
3. $1 \oplus \prod_{i=1}^{n}(1 \oplus x_i)$,

are coincident.

Proof Let us to prove the three assertions.
The definition of Mobius transform gives us directly 1.
For the next assertion 2, we have $\prod_{i=1}^{n} x_i = x^{\mathbf{1}} = M_{\mathbf{1}}$, we conclude by applying Proposition 4.
Concerning the assertion3; $\prod_{i=1}^{n}(1 \oplus x_i) = M_{\mathbf{0}}$ and $1 = x^{\mathbf{0}}$, then $\prod_{i=1}^{n}(1 \oplus x_i) = \mu_n(1)$ and $1 = \mu_n(\prod_{i=1}^{n}(1 \oplus x_i))$. Hence $1 \oplus \prod_{i=1}^{n}(1 \oplus x_i) = \varphi_n(1)$.

Since the Mobius transform of a coincident function provides a connection between the minterms and the monomials, we deduce the following corollary.

Corollary 4 *Let h be a coincident function, then $w(h) = N(h)$, where $N(h)$ gives the number of monomials of the h.*

We introduce now the dual of a coincident function.

Definition 10 Let $h \in \mathcal{C}_n$. The dual of h is the coincident function $\overline{h}^* = h \oplus \varphi_n(1)$.

Proposition 19 *We have a one to one correspondence between coincident functions with odd Hamming weight and even Hamming weight.*

Proof A Boolean function has Hamming weight odd if and only if $\prod_{i=1}^{n} x_i$ occurs in its ANF. Let $h \in \mathcal{C}_n$. It follows $A(f) = T(f) = t_1 \dots t_{2^n}$, and $w_H(h)$ odd if and only if $t_{2^n} = 1$. Hence we a have partition of $\mathcal{C}_n = (\mathcal{C}_n^o, \mathcal{C}_n^e)$, where $\mathcal{C}_n^o$ (resp. $\mathcal{C}_n^e$) are coincident functions of Hamming weight odd (resp. even) and a one to one correspondence between $\mathcal{C}_n^o$ and $\mathcal{C}_n^e$ with $h' = h \oplus \prod_{i=1}^{n} x_i$, $\prod_{i=1}^{n} x_i$ is the coincident function which changes the parity of a coincident function.

Thanks to the previous propositions, we propose to exhibit different coincident functions of any number of variables.

Proposition 20 *Table of some coincident functions*
The following words codes table (or equivalently ANF) of coincident functions:

1. $\mathbf{0}_n \iff 0 \dots 0$;
2. $\prod_{i=1}^{n} x_i \iff 0 \dots 01$;
3. $1 \oplus \prod_{i=1}^{n}(1 \oplus x_i) \iff 01 \dots 1$;
4. $1 \oplus \prod_{i=1}^{n}(1 \oplus x_i) \oplus \prod_{i=1}^{n} x_i = \overline{\prod_{i=1}^{n} x_i}^* \iff 01 \dots 10$;
5. $\forall u \in \mathbb{F}_2^n,\ \bigoplus_{u \prec v} x^v$.

4 Constructions of coincident functions based on the Boolean lattice

4.1 Boolean lattice properties of coincident functions

The set of valuations in n variables forms a Boolean lattice with the partial order $\preceq$ already defined. The process of placing the minterms (or the monomials) which appears in a Boolean function over this lattice may be useful for some studies. In Guillot (1999) PHD Thesis Boolean lattice is already considered for the study of Mobius transform.

We first provide a new caracterisation of coincident functions. Let $n \in \mathbb{N}$, we define the complete Boolean lattice $\mathcal{L}_n = (\mathbb{F}_2^n, \preceq)$ such that, for any $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$, the supremum and the infimum are defined by

$$\begin{aligned} sup(u, v) &= u \vee v = (u_1 \vee v_1, \ldots, u_n \vee v_n); \\ inf(u, v) &= u \wedge v = (u_1 \wedge v_1, \ldots, u_n \wedge v_n). \end{aligned}$$

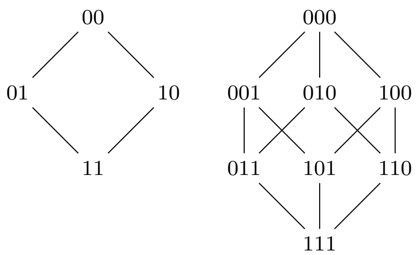
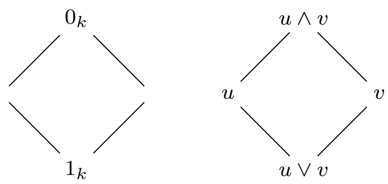


Fig. 1 The lattices $\mathcal{L}_2$ and $\mathcal{L}_3$.



The Boolean lattice $\mathcal{L}_k$ The Boolean lattice $\mathcal{L}(u, v)$

Fig. 2 Isomorphism between $\mathcal{L}_k$ and $\mathcal{L}(u, v)$.

The lattice is complete in the sense that any sublattice $(\mathcal{U}, \preceq)$ has the supremum $\bigvee_{u \in \mathcal{U}} u$ and the infimum $\bigwedge_{u \in \mathcal{U}} u$. $\mathcal{L}_n$ is also called the n-cube (Palmer et al. (1992)). Let u and $v \in \mathbb{F}_2^n$ and $k = d_h(u \vee v, u \wedge v)$. Then $\mathcal{L}(u, v) = \{w \in \mathbb{F}_2^n | u \preceq w \preceq v\}$ is isomorph to $\mathcal{L}_k$ (we remove the identical components in u and v), see Fig. 2.

Definition 11 Let $f \in \mathcal{F}_n$, we define $\mathcal{L}_n(f) = (\mathcal{U}, \preceq)$ the sublattice of $\mathcal{L}_n$ by $\mathcal{U} = support(f) = \{u \in \mathbb{F}_2^n | f(u) = 1\}$.

Then f can be viewed as a 2 coloring of the $\mathcal{L}_n$.

Let $a = (a_1, \ldots, a_n)$ and $f \in \mathcal{F}_n$, $f(a) = \bigoplus_{u \in \mathbb{F}_2^n} \mu_n(f)(u) a^u$. Since $a^u = 0$ for any u such that $u \npreceq a$ and $a^u = 1$, it follows

$$f(a) = \bigoplus_{u \preceq a} \mu_n(f)(u). \tag{7}$$

Proposition 21 *(Pieprzyk et al. 2011, Theorem 23) Let $f \in \mathcal{F}_n$ be a boolean function with n variables. Then f is coincident if and only if*

$$\bigoplus_{v \prec u} f(v) = 0, \text{ for any } u \in \mathbb{F}_2^n. \tag{8}$$

In other words, for each $u \in \mathbb{F}_2^n$, we have an even number of $v \prec u$ such that $f(v) = 1$.

Proof Let f be a coincident function, then $f(u) = \bigoplus_{v \preceq u} f(v) = f(u) \oplus \bigoplus_{v \prec u} f(v)$.

Proposition 22 *Recall that $h_a = x^a \oplus M_a$, for any $a \in \mathbb{F}_2^n$. Then $(h_a)_{a \in \mathbb{F}_2^n,\ a_n = 0}$ forms a basis of $\mathcal{C}_n$.*

Proof Let $h \in \mathcal{C}_n$ and $g \in \mathcal{F}_{n-1}$ such that $h = g \oplus \mu_n(g)$. Let $\mathcal{U} \subset \mathbb{F}_2^n$ such that $g = \bigoplus_{a \in \mathcal{U}} x^a$. Then $a_n = 0$ for any $a \in \mathcal{U}$ and

$$\begin{aligned} h &= \textstyle\bigoplus_{a \in \mathcal{U}} x^a \oplus \mu_n(\bigoplus_{a \in \mathcal{U}} x^a) \\ &= \textstyle\bigoplus_{a \in \mathcal{U}} x^a \oplus \bigoplus_{a \in \mathcal{U}} M_a \\ &= \textstyle\bigoplus_{a \in \mathcal{U}} h_a. \end{aligned}$$

The following proposition gives a link between a Boolean function f and the corresponding coincident function $\varphi_n(f) = f \oplus \mu_n(f)$.

Proposition 23 *Let f a Boolean function, $\mathcal{U} = support(f)$ and $h = \varphi_n(f)$, then $h(a) = 1$ if and only if there is an odd number of $u \in \mathcal{U}$ such that $u \prec a$.*

Proof Let $u \in \mathcal{U}$, $h_u = x^u \oplus M_u = \bigoplus_{u \prec v} M_v$. Hence $h = \bigoplus_{u \in \mathcal{U}} (\bigoplus_{u \prec v} M_v)$. Let $\mathcal{U}_{\prec a} = \{u \in \mathcal{U}, u \prec a\}$, for any $a \in \mathbb{F}_2^n$. Since $h(a) = \bigoplus_{u \in \mathcal{U}_{\prec a}} 1$, $h(a) = 1$ if and only if the cardinality of $\mathcal{U}_{\prec a}$ is odd.

Proposition 24 *The Boolean function with n variables $x_1 \oplus \ldots \oplus x_n$ is coincident.*

Proof Let $f = \prod_{i=1}^n (1 \oplus x_i)$. $f(u) = 1$ if and only if $u = 0_n$. Let $0_n = (0, \ldots, 0)$ and $u^j = (u_1^j, \ldots, u_n^j)$ for any $j \in \{1, \ldots, n\}$, where $u_i^j = 1$ if and only if $i = j$; hence $x^{u^j} = x_i$. We check Proposition 23. There is no $u \prec 0_n$ and for any u_i^j, the unique $u \prec x^{u^j}$ is 0_n and $f(0_n) = 1$.

Proposition 25 *Let $h = \varphi_n(f) \in \mathcal{C}_n$. Either the $ANF(h)$ contains all the terms $x_1, \ldots, x_n$ either it contains none of these terms.*

Proof The proof is similar that Proposition 24. If $f(0_n) = 1$ (resp. 0), then all the monomials x_i has an odd (resp. even) number of $u \prec u^j$ such that $f(u) = 1$.

4.2 Monotonic coincident functions

Monotonic Boolean functions are commonly involved as instances of constraint satisfaction problems like the NP-complete SAT or 3-SAT problems, Creignou et al. (2001). Indeed these problems are monotonic in the sense where an instance of a set of constraints $\mathcal{C}$ is also an instance of any subset of $\mathcal{C}$.

We exhibit in this part 2^{n+1} monotonic coincident functions. We also provide a general characterization of the class of monotonic coincident functions in order to build more such functions.

Definition 12 A Boolean function f is monotonic if for any $u \in \mathbb{F}_2^n$ such that $f(u) = 1$ we have $f(v) = 1$ for any $v \prec u$.

As far as we know, the number of such functions on n variables is known as the Dedekind number of n and the exact values are known only for $n \leq 8$.

Proposition 26 *A Boolean function f is monotonic if there exists $Inf(f) \subset \mathbb{F}_2^n$ which satisfies $f(v) = 1$ if and only if there exists $u \in Inf(f)$ with $u \preceq v$.*

Proof We define $Inf(f) = \{u \in \mathbb{F}_2^n \mid f(u) = 1 \text{ and } f(v) = 0 \text{ for any } v \prec u\}$. Assume that f is monotonic. Let $v \notin Inf(f)$ and $f(v) = 1$. Then there exists a unique $u \in Inf(f)$ such that $u \prec v$. Conversely assume that $f(v) = 1$ for any $v \preceq u$, for some $u \in Inf(f)$, then f is clearly monotonic.

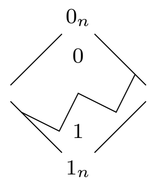


Fig. 3 Lattice for monotonic boolean functions.

Since $f = \bigoplus_{u \in \mathbb{F}_2^n} \beta_u M_u$, f is monotonic when for any u such that $\beta_u = 1$, $\beta_v = 1$ for any $v \prec u$.

For example, $x^u = \bigoplus_{u \preceq v} M_v$ are monotonic functions and $h_u = \bigoplus_{u \prec v} M_v$ are monotonic coincident functions.

Proposition 27 *Let $u \in \mathbb{F}_2^n$ and $\overline{u} = (u_1 \oplus 1, \ldots, u_n \oplus 1)$. Then $f_u = h_u \oplus h_{\overline{u}} \oplus x_1 \ldots x_n$ is a monotonic coincident function.*

Proof Let $v \in \mathbb{F}_2^n$. If $h_u(v) = h_{\overline{u}}(v) = 1$ then $u \prec v$ and $\overline{u} \prec v$, hence $v = (1, \ldots, 1)$ and $f_u(v) = 1$. Assume that $v \neq (1, \ldots, 1)$, if $h_u(v) = 1$ or $h_{\overline{u}}(v) = 1$ then $f_u(w) = 1$, for any $v \preceq w$.

We have yet exhibit 2^{n+1} monotonic coincident functions but other constructions over the Boolean lattice could be performed.

4.3 Construction of the class of coincident symmetric Boolean functions

Symmetric Boolean functions have good implementation since the number of required gates is linear in the number of variables. In Canteaut and Videau (2005), the authors proposed an extensive study combined with cryptographic parameters like degree, correlation-immunity, non-linearity. We present here an algorithm to generate all the $2^{\lfloor \frac{n}{2} \rfloor + 1}$ coincident symmetric functions.

Definition 13 (Symmetric (Boolean) functions) Let $k \leq n$, Σ_k^n will denote the Boolean function with n variables which is the sum of monomials of degree k. A symmetric function f of $\mathcal{F}_n$ is defined by

$$f = \sum_{k=0}^{n} \lambda_k \Sigma_k^n,$$

where $(\lambda_0, \dots, \lambda_n) \in F_2^n$ satisfies

$$\lambda_i = \begin{cases} 1, & \text{if all the monomials of degree } i \text{ occur in the ANF of f;} \\ 0, & \text{otherwise.} \end{cases}$$

We will note $\lambda(f) = (\lambda_0, \dots, \lambda_n)$.

Since a symmetric function is invariant by permutation of the variables, we have another definition of a symmetric function over the valuations. Let $a = (a_1, \dots a_n) \in \mathcal{F}_2^n$,

$$f(a_1, \dots, a_n) = f(a_{\sigma(1)}, \dots, a_{\sigma(n)}),$$

for any permutation σ of $\{1, \dots n\}$.

Then the value of $f(a)$ only depends of the weight of the valuation a. Let $v(f) = (v_0, \dots, v_n)$, where $v_k = f(a)$, for any $a \in \mathcal{F}_2^n$ of weight k.

Since a symmetric Boolean function may be defined by fixing $\lambda(f) = (\lambda_0, \dots, \lambda_n)$ or $v(f_n) = (v_0, \dots, v_n)$, we have 2^{n+1} symmetric Boolean functions. Furthermore, $d(f)$ is the largest i such that $\lambda_i = 1$ and $w_H(f)$ is $\sum_{i=0}^{n} \lambda_i \binom{n}{i}$.

Let $f = f_R^0 \oplus x_n f_R^1$ be a symmetric function with n variables, where f_R^0 and f_R^1 are Boolean functions with $n-1$ variables.

For $i \in \{1, \dots, n-1\}$, the ANF of f contains all the monomials of degree i if and only if the ANF of f_R^0 contains all the monomials of degree i. Thus f_R^0 is a symmetric function. Furthermore for $i \in \{0, \dots, n-1\}$ the ANF of f contains all the monomials of degree $i+1$ if and only if the ANF of f_R^1 contains all the monomials of degree i. Hence f_R^1 is also a symmetric function.

We define

$$\begin{aligned} \lambda(f) &= (\lambda_0, \dots, \lambda_n); \\ \lambda(f_R^0) &= (\lambda_0^0, \dots, \lambda_{n-1}^0); \\ \lambda(f_R^1) &= (\lambda_0^1, \dots, \lambda_{n-1}^1). \end{aligned}$$

We have $\lambda_i = \lambda_i^0 = \lambda_{i-1}^1$, for any $i \in \{1, \dots, n-1\}$, $\lambda_n = \lambda_{n-1}^1$ and $\lambda_n = 1$ if and only if the ANF of f contains the monomial $x_1 \dots x_n$.

Definition 14 (Luca's coefficients) Let k, $j \in \mathbb{N}$ and $p(k, j) = \begin{pmatrix} k \\ j \end{pmatrix}$ mod 2.

Proposition 28 *Let f be a symmetric Boolean function with n variables, $v(f) = (v_0, \ldots, v_n)$ and $\lambda(f) = (\lambda_0, \ldots, \lambda_n)$. The following system holds*

$$v_j = \sum_{k=0}^{j} \lambda_k \, p(k, j).$$

Proof Clearly $v_0 = \lambda_0$. Let $j \in \{0, \ldots, n\}$ and $a = (a_1, \ldots, a_n) \in \mathcal{F}_2^n$ such that $w_H(a) = j$. By (7),

$$f(a) = \bigoplus_{u \preceq a} \mu_n(f)(u) a^u.$$

For $k \leq j$, we have $\binom{k}{j}$ $b \in \mathbb{F}_2^n$ such that $w_H(b) = k$ and $b \preceq a$. We have to deal with two cases

1. $\lambda_k = 1$ and $\mu_n(f)(b) = 1$ for any $b \preceq a$ such that $w_H(b) = k$.
2. $\lambda_k = 0$ and $\mu_n(f)(b) = 0$ for any $b \preceq a$ such that $w_H(b) = k$.

It follows

$$f(a) = \bigoplus_{k=0}^{j} \lambda_k \binom{k}{j}.$$

Notation 7 *Let $k = \sum_{i \in \mathbb{N}} k_i \; 2^i$ and $j = \sum_{i \in \mathbb{N}} j_i \; 2^i$ the 2-adic representation of k and respectively j. We will write $j \preceq k$ when $j_i = 1$ implies $k_i = 1$, for any $i \in \mathbb{N}$.*

By Lucas' Theorem $p(k, j) = 1$ if and only if $j \preceq k$ and by definition of Mobius transform,

$$v(f) = \lambda(\mu_n(f)) \text{ and } \lambda(f) = v(\mu_n(f)).$$

Proposition 29 *With the previous notations, we have $\lambda(\mu_n(\Sigma_n^k)) = (v_0^k, \ldots, v_n^k)$, where*

$$\begin{cases} v_j^k = 0, \; \textit{for } j < k \\ v_k^k = 1 \\ v_j^k = p(j, k), \; \textit{for } k < j \leq n. \end{cases} \tag{9}$$

We have already seen the symmetric coincident functions $1 \oplus x_1 \oplus \ldots \oplus x_n$ (Proposition 24) which corresponds to $v(f) = (0, 1, 0, \ldots, 0)$. We are looking for the whole class of such functions.

Recall that $h(\Sigma_k^n) = \Sigma_k^n \oplus \mu_n(\Sigma_n^k)$, $\lambda(h(\Sigma_n^k)) = (w_0^k, \ldots, w_n^k)$, where $w_i^k = v_i^k$, for any $i \neq k$ and $w_k^k = 0$.

Since a sum of symmetric functions still a symmetric function, a sum of symmetric coincident functions still a symmetric coincident function. Hence $\mathcal{SC}_n$ the set of symmetric coincident function is generated by the $h(\Sigma_k^n)$ is a vector space of dimension 2^l, for some $l \in n + 1$. Remark that for some k_1 and $k_2 \in \{0, \ldots, n\}$, $k_1 < k_2$, we may have $h(\Sigma_n^{k_1}) = h(\Sigma_n^{k_2})$.

Let CS_n the set of coincident symmetric Boolean functions. Since the sum of two coincident functions is a coincident function and the sum of two symmetric functions is a symmetric function, CS_n is a vector space.

Proposition 30

$$|CS_n| = 2^{\lfloor \frac{n}{2} \rfloor + 1}.$$

Proof We show that

$$\begin{cases} |CS_1| &= 2 \\ |CS_n| &= |CS_{n-1}| \text{ if } n \text{ is odd} \\ &= 2|CS_{n-1}| \text{ if } n \text{ is even.} \end{cases}$$

For $n = 1$, $f(x_1) = x_1$ is the unique coincident symmetric Boolean function different from $\mathbf{0}_1$, $\lambda(f) = (0, 1)$ and $\lambda(\mathbf{0}_1) = (0, 0)$.

Let $n \geq 1$ and $f = f_R^0 \oplus x_n f_R^1$ be a symmetric function with n variables, where f_R^0 and f_R^1 are Boolean functions with $n-1$ variables.

Let $\lambda(f) = (\lambda_0, \ldots, \lambda_n)$ and $v(f) = (v_0, \ldots, v_n)$, f is coincident if and only if $\lambda(f) = v(f)$.

Let j be any element of $\{0, \ldots, n\}$. By implying (9) we obtain

$$\begin{aligned} v_j &= \lambda_j \oplus \Big(\textstyle\bigoplus_{k=0}^{n} \lambda_k \; v_j \Big), \\ &= \lambda_j \oplus \Big(\textstyle\bigoplus_{k<j} \lambda_k \; p(j,k) \Big). \end{aligned}$$

Then f is coincident if and only if

$$\bigoplus_{k<j} \lambda_k \; p(j,k) = 0, \text{ for any } j \in \{0, \ldots, n\}. \tag{10}$$

We have seen that $\lambda(f_R^0) = (\lambda_0, \ldots, \lambda_{n-1})$. Furthermore

$$\begin{aligned} \mu_n(f) &= \mu_n(f_R^0) \oplus \mu_n(f_R^1) \\ &= (1 \oplus x_n)\mu_{n-1}(f_R^0) \oplus x_n \mu_{n-1}(f_R^1) \\ &= \mu_{n-1}(f_R^0) \oplus x_n \big(\mu_{n-1}(f_R^0) \oplus \mu_{n-1}(f_R^1)\big). \end{aligned}$$

Then f is coincident if and only if

$$\begin{cases} \mu_{n-1}(f_R^0) = f_R^0 \\ \mu_{n-1}(f_R^1) = f_R^0 \oplus f_R^1. \end{cases}$$

The first equation implies that f_R^0 is a symmetric coincident function and it just remains to check the last equation of (10)

$$\bigoplus_{k<n} \lambda_k \; p(n,k) = 0.$$

Case n is even

$p(n, 1) = 0$ and it is easily seen that $p(n, k) = 0$ for k odd and $p(n, k) = p(n-2, k-2)$, for k even. Then we have to check

$$\bigoplus_{k<n-2} \lambda_k \; p(n-2,k) = 0,$$

which is already satisfies by f_R^0. Hence we may choose $\lambda_n = 0$ or 1 and $CS_n = 2CS_{n-1}$.

Algorithm 2: Enumeration

Input: The number of variables: $n \in \mathbb{N}$.
Output: Enumeration of coincident symmetric functions with n variables.

```
if n = 1 then
    enumerate (0,0)
    enumerate (0,1)
else
    if n even then
        for (λ_0, ..., λ_{n-1}) of Enumeration(n − 1) do
            enumerate (λ_0, ..., λ_{n-1}, 0)
            enumerate (λ_0, ..., λ_{n-1}, 1)
    else
        for (λ_0, ..., λ_{n-1}) of Enum(n − 1) do
            if λ_0 p(n,n) ⊕ λ_2 p(n,n−2) ... ⊕ λ_{n-2} p(n,2) = λ_{n-1} then
                enumerate (λ_0, ..., λ_{n-1}, 0)
                enumerate (λ_0, ..., λ_{n-1}, 1)
```

Case n is odd
Since $p(n,1)=1$, $\lambda_0\ p(n,n) \oplus \lambda_2\ p(n,n-2)\ldots \oplus \lambda_{n-2}\ p(n,2) = \lambda_{n-1}$. Then we may chose $\lambda_n = 0$ or 1, but we have a unique possibility for λ_{n-1}. By the previous case, we know that half of the symmetric coincident function f^0_R satisfy $\lambda_{n-1}=0$. Clearly $|CS_n| = |CS_{n-1}|$.

Proposition 31 *Enumeration*
The Algorithm 2 provides an enumeration of coincident symmetric functions.

Proposition 32 *The Algorithm 3 provides random generation of coincident symmetric functions.*

Algorithm 3: UniformRandomGeneration

Input: The number of variables: $n \in \mathbb{N}$.
Output: Uniform random generation of a coincident symmetric functions with n variables

```
if n = 1 then
    return uniform( {(0,0), (0,1)})
else
    if n even then
        (λ_0, ..., λ_{n-1}) ← UniformRandomGeneration(n − 1)
        λ_n ← uniform ({0,1})
        return (λ_0, ..., λ_n).
    else
        (λ_0, ..., λ_{n-1}) ← UniformRandomGeneration(n − 1)
        λ_n ← uniform ({0,1}).
        if λ_0 p(n,n) ⊕ λ_2 p(n,n−2) ... ⊕ λ_{n-2} p(n,2) = λ_{n-1} then
            return (λ_0, ..., λ_{n-1}, λ_n).
        else
            return (λ_0, ..., 1 − λ_{n-1}, λ_n).
```

5 Experiments results

The usefulness of coincident functions for practical applications is not yet established. Therefore a deep investigation of other cryptographically significant properties of Boolean functions must be conducted from a cryptographic point of view. We show in this part that for some aspects a random coincident function looks like uniform random Boolean functions. We consider the Hamming weight, the distribution of the degrees (the number of monomials for each degree), the balancedness and the nonlinearity. Other investigation like propagation criteria, algebraic immunity may also be considered.

5.1 Correlation-immune Boolean functions

Correlation immunity of a Boolean function is a measure of the degree to which its outputs are uncorrelated with some subset of its inputs. In Siegenthaler (1984), the author shows the importance of this property in cryptography.

The table below gives the number of correlation-immune functions of order 1 for fix Hamming weight for $n \leq 5$. We write $cor_1(n)$ the total number of correlation-immune functions of order 1 with n variables.

Remark that the only 1-resilient in this table is the function with 2 variables $x_1 \oplus x_2$.

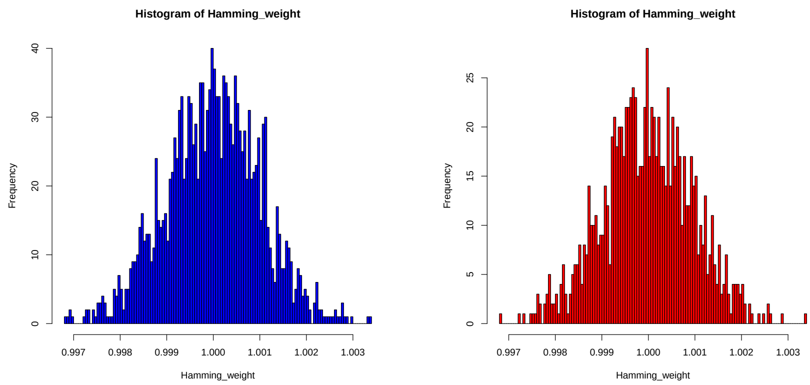
$n \setminus m$	0	2	4	6	8	10	12	14	18	22	30	Total	$cor_1(n)$
1	1											1	
2	1	1										2	4
3	1		1									2	18
4	1	3			3		1					8	648
5	1			5		70			70	5	1	152	3140062

5.2 Hamming weight distribution

We observe that $\mathcal{C}_n$ and $\mathcal{F}_n$ follows a similar weight distribution. The Figure 5 gives the distribution of Hamming weight for 1000 uniform random generated Boolean functions over $\mathcal{C}_n$ and $\mathcal{F}_n$, with $n = 20$. The Hamming weight w is normalized by the mean 2^{n-1}, so the abscissa will be $w' = w/2^{n-1}$. It is easily shown that the distributions are very similar.

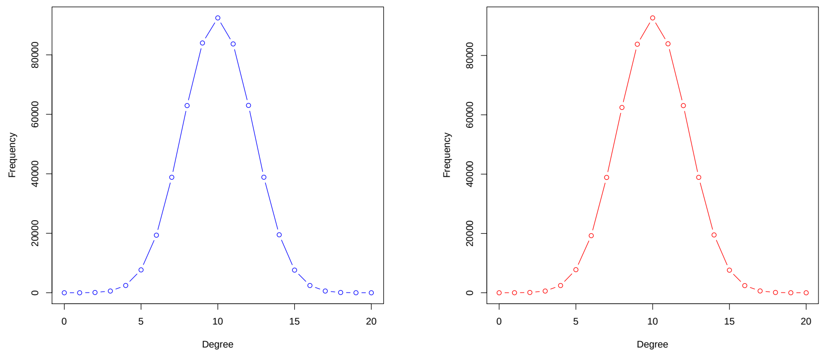
5.3 Algebraic degree distribution

We show experimentally that random coincident functions follow the same algebraic degree distribution than any random Boolean function. Let f and g be Boolean functions uniformly randomly generated over respectively $\mathcal{C}_n$ and $\mathcal{F}_n$, we consider the number of monomials of degree d for each $d \in \{0, \dots, n\}$. For any d, the expected value should be close to $\binom{n}{d}/2$ in the case of g. We have used several times the Kolmogorov-Smirnov statistical test to show that the distributions are very closed. Of course if we consider just one degree d, its is possible to distinguish



Random functions over $\mathcal{C}_{20}$ Random functions over $\mathcal{F}_{20}$

Fig. 4 Hamming weight distributions for coincident and boolean functions with 20 variables.



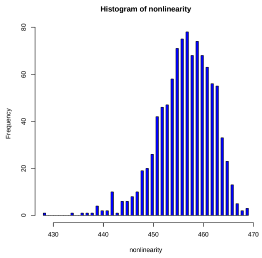
Random function over $\mathcal{C}_{20}$ Random functions over $\mathcal{F}_{20}$

Fig. 5 Degree distribution of Boolean functions with 20 variables.

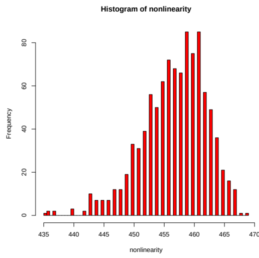
the distributions since in f we have either all the monomials of degree 1 or neither (Proposition 24). The Figure 5.3 in a single random generation of f and g.

5.4 Balancedness

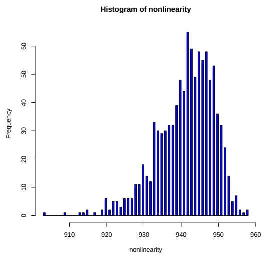
A Boolean function of n variables is balanced when $w_H(f_n) = 2^{n-1}$. It is easily seen that the probability that a random Boolean function is balanced is equal to $\frac{\binom{2^n}{2^{n-1}}}{2^{2^n}}$. We obtain every close frequencies when we generates random coincident function under $n \leq 20$. Further investigations should proved this statement for any $n \in \mathbb{N}$.



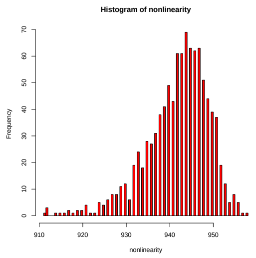
Random functions over $\mathcal{C}_{10}$



Random functions over $\mathcal{F}_{10}$



Random functions over $\mathcal{C}_{11}$



Random functions over $\mathcal{F}_{11}$

Fig. 6 Nonlinearity distributions for coincident and boolean function with 10 and 11 variables.

5.5 Non-linearity

The non-linearity is the Hamming weight distance to all the affine Boolean functions. It is shown that Boolean functions must have a high nonlinearity to ensure confusion, an important property in cryptographic context(Carlet (2010)), in particular to avoid fast correlation attacks(Canteaut and Trabbia (2000); Chepyzhov and Smeets (1991)). The functions which reach the best nonlinearity are called bent functions, they occur when n is even and they have nonlinearity $2^{n-1} - 2^{n/2-1}$. On the other hand, the best nonlinearity of Boolean functions in odd numbers of variables is strictly greater than the quadratic bound –$2^{n-1} - 2^{\frac{n-1}{2}}$– for any $n > 7$. See (Carlet (2010)) for a good introduction of the nonlinearity property and the bent functions.

Let $h \in \mathcal{C}_n$, there exists a unique $g \in \mathcal{F}_{n-1}$ such that $h = (1 \oplus x_n)\varphi_{n-1}(g) \oplus x_n g$ (Proposition 13). Let $l_n \in \mathcal{L}_n$, the set of affine functions with n variables. There is $l_{n-1} \in \mathcal{L}_{n-1}$ such that $l_n = (1 \oplus x_n)l_{n-1} \oplus x_n l_{n-1}$ or $l_n = (1 \oplus x_n)l_{n-1} \oplus x_n(l_{n-1} \oplus 1)$. Hence $d(h, l_n) = w_H(\varphi_{n-1}(g), l_{n-1}) + w_H(g, l_{n-1})$ or $d(h, l_n) = w_H(\varphi_{n-1}(g), l_{n-1}) + w_H(g \oplus 1, l_{n-1})$. A random h of $\mathcal{C}$ should have the same distance from the affine functions from any random Boolean function if the there is no correlation between the distances $w_H(\varphi_{n-1}(g), l_{n-1})$ and $w_H(g \oplus 1, l_{n-1})$.

We observe experimentally that this is the case. In Figure 6, we consider $n = 10$ and 11 and we build 1000 random functions over $\mathcal{C}_n$ and 1000 over $\mathcal{F}_n$ and we compute the frequency of each nonlinearity value. Remark that bent functions have nonlinearity $2^9 - 2^4 = 496$. We consider even and odd values of n because the nonlinearity behaviour is very different in these cases.

6 Conclusion

Our paper presents an innovative way to manipulate the Mobius transform, with the distinction between variables abd indeterminates. This allows us to highlight new properties of coincident functions. We may also move easily from Shannon decomposition to Reed-Muller decomposition or vice versa. We show how the Boolean lattice is colored in the case of coincident functions, which gives a method to build monotone functions, and we provide a method to build and generate uniformly the symmetric coincident functions. Thanks to a uniform random generator over all the coincident boolean functions, we establish experimentally that for the most common characteristics (Hamming weight, distributions of the monomials degree, balanceness), a coincident function looks like any Boolean function. This experimental work could be completed by further properties. Notice that our random generator of coincident functions requires the computation of a Mobius transform with $n-1$ variables. We may avoid this problem with the use of the basis of coincident functions but it is not an efficient way. Direct random generation and enumeration will be a challenge. Another promising perspective will be to propose algorithms which compute the Mobius transform with low complexity for a larger part of Boolean functions, standed by our new properties. Based on all these results, we therefore recommand to use this class of functions, especially in order to build Boolean functions with good cryptographic properties. Specific constructions with trade-off between cryptographic criteria seems really feasible.

References

Boole, Georges. 1848. The calculus of logic. *Cambridge and Dublin Mathematical Journal* III: 183–98.

Boole, Georges. 1854. An investigation of the laws of thought. MacMillan.

Bryant, Randal. 1986. Graph-based algorithms for boolean function manipulation. *IEEE Transactions on Computers* C-35 (8): 677–691.

Canteaut, Anne, and Michaël Trabbia. 2000. Improved fast correlation attacks using parity-check equations of weight 4 and 5. In *Advances in cryptology - EUROCRYPT 2000, international conference on the theory and application of cryptographic techniques, bruges, belgium, may 14-18, 2000, proceeding*, 573–588.

Canteaut, Anne, and Marion Videau. 2005. Symmetric boolean functions. *IEEE Transactions on Information Theory* 51 (8): 2791–2811.

Carlet, Claude. 2010. Boolean models and methods in mathematics, computer science, and engineering. Cambridge University Press.

Chepyzhov, Vladimir V., and Ben J. M. Smeets. 1991. On A fast correlation attack on certain stream ciphers. In *Advances in cryptology - EUROCRYPT '91, workshop on the theory and application of of cryptographic techniques, brighton, uk, april 8-11, 1991, proceedings*, 176–185.

Creignou, Nadia, Sanjeev Khanna, and Madhu Sudan. 2001. *Complexity classifications of boolean constraint satisfaction problems.* Philadelphia, PA, USA: Society for Industrial and Applied Mathematics.

Guillot, Philippe. 1999. Fonctions courbes binaires et transformation de Mobius. PhD diss, University of Caen Basse-Normandie.

Kasami, Tadao, and Nobuki Tokura. 1970. On the weight structure of reed-muller codes. *IEEE Transactions on Information Theory* 16 (6): 752–759.

Palmer, E. M., R. C. Read, and R. W. Robinson. 1992. Balancing the n-cube: A census of colorings. *Journal of Algebraic Combinatorics* 1 (3): 257–273.

Pieprzyk, Josef, Huaxiong Wang, and Xian-Mo Zhang. 2011. Möbius transforms, coincident boolean functions and non-coincidence property of boolean functions. *International Journal of Computer Mathematics* 88 (7): 1398–1416.

Shannon, Claude. E. 1949. The synthesis of two-terminal switching circuits. *Bell System Technical Journal* 28 Issue 1: 59–98.

Siegenthaler, Thomas. 1984. Correlation-immunity of nonlinear combining functions for crypthographic applications. *IEEE Transactions on Information Theory* IT-30 (5): 776–780.