Fast algebraic immunity of Boolean functions and LCD codes

Sihem Mesnager[1] and Chunming Tang[2]

[1] Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, University Sorbonne Paris Cité, Laboratory Analysis, Geometry and Applications (LAGA), UMR 7539, CNRS, 93430 Villetaneuse, and Telecom Paris, 91120 Palaiseau, France
smesnager@univ-paris8.fr
[2] School of Mathematics and Information, China West Normal University Nanchong, Sichuan, 637002, China
tangchunmingmath@163.com

Abstract. Nowadays, the resistance against algebraic attacks and fast algebraic attacks are considered as an important cryptographic property for Boolean functions used in stream ciphers. Both attacks are very powerful analysis concepts and can be applied to symmetric cryptographic algorithms used in stream ciphers. The notion of algebraic immunity has received wide attention since it is a powerful tool to measure the resistance of a Boolean function to standard algebraic attacks. Nevertheless, an algebraic tool to handle the resistance to fast algebraic attacks is not clearly identified in the literature. In the current paper, we propose a new parameter to measure the resistance of a Boolean function to fast algebraic attack. We also introduce the notion of fast immunity profile and show that it informs both on the resistance to standard and fast algebraic attacks. Further, we evaluate our parameter for two secondary constructions of Boolean functions. Moreover, A coding-theory approach to the characterization of perfect algebraic immune functions is presented. Via this characterization, infinite families of binary linear complementary dual codes (or LCD codes for short) are obtained from perfect algebraic immune functions. The binary LCD codes presented in this paper have applications in armoring implementations against so-called side-channel attacks (SCA) and fault non-invasive attacks, in addition to their applications in communication and data storage systems.

Keywords Boolean function · (Fast) Algebraic immunity · Algebraic attack · Fast algebraic attack · Reed-Muller code · LCD code · Side-channel attack · Fault injection attack.

1 Introduction

Boolean functions have important applications in the combiner model and the filter model of stream ciphers. A function used in such an application should mainly possess balancedness, a high algebraic degree, a high nonlinearity and, in the case of the combiner model, a high correlation immunity. In 2003, new kinds of attacks drawn from an original idea of Shannon [37] emerged; these attacks are called *algebraic attacks* and *fast algebraic attacks* [14,15,33]. Since 2003, the designers of cryptosystems in symmetric cryptography need also to ensure resistance to the algebraic attack (they need in practice optimal or almost optimal algebraic immunity) and good resistance to fast algebraic attacks and to the Rønjom-Helleseth attack [20,22], and its improvements. A first nice primary construction of an infinite class of functions satisfying all the cryptographic criteria (balancedness, the algebraic degree the algebraic immunity and the non-linearity) is the so-called Carlet-Feng construction [5]. Note that its good resistance to fast algebraic attacks has first been checked by computer for $n \leq 12$, using an algorithm from [1], and later shown mathematically in [26] for all n. Later, classes of functions have been proposed in the literature in which the authors suggested some modifications of the Carlet-Feng functions and other constructions (see for instance [3,12] and the references therein).

(Fast-) algebraic attacks have changed the situation in symmetric cryptography for the steam ciphers by adding a new criterion of considerable importance to the above list. They proceed by modeling the problem of recovering the secret key through an over-defined system of multivariate nonlinear equations of algebraic degree at most $\deg(f)$. The core of algebraic attacks is to find out low degree Boolean functions $g \neq 0$ and h such that $fg = h$. It is shown in [33] that this is equivalent to the existence of low algebraic degree *annihilators* of f, that is, of n-variable Boolean functions g such that $f \cdot g = 0$ or $(1 + f) \cdot g = 0$. The minimum degree of such g is called the *algebraic immunity* of f, and we denote it by $AI(f)$. It must be as high as possible (the optimum value of $AI(f)$ being equal to $\lceil \frac{n}{2} \rceil$). In 2020, a novel application of Boolean functions with high algebraic immunity in minimal codes has been derived in [13]. Fast algebraic attacks proceed differently and exploit the existence of function g of small degree such that the degree of $f \cdot g$ is not too large. Many authors have indicated that having a high algebraic immunity is not only a necessary condition for resistance to standard algebraic attacks but also for resistance to fast algebraic attacks. Nevertheless, having a high algebraic immunity may not be sufficient in the design of pseudo-random generators using a Boolean function as filter or combiner (see [2]). That motivates to define a new parameter to measure the resistance of the Boolean function f used in such generators to fast algebraic attacks. Such a parameter has been proposed in [12,17,25]. Very recently, Méaux has studied in [31,32] the fast algebraic immunity of interesting families of cryptographic Boolean functions, namely the so-called majority functions (which have been intensively studied in the area of cryptography, because of their practical advantages and good properties), and Threshold functions (which are a sub-family of symmetric Boolean functions, which means that the output is independent of the order of the input binary variables). In 2020, Tang [38] has derived a relation on the fast algebraic immunity between a Boolean function and its modifications, by introducing a new concept called partial fast algebraic immunity. As applications of this relation, he derived some upper bounds on the fast algebraic immunity of several known classes of modified majority functions with optimal algebraic immunity. These bounds show that these modified majority functions still have low fast algebraic immunity, which is coincident with the relation. A very nice reference on this topic is the excellent book of Carlet [4] (which will appear soon).

In this paper, we provide for the first time a link between fast algebraic immune Boolean functions and the so-called *linear complementary dual code* (abbreviated LCD). An LCD code is defined as a linear code $\mathcal{C}$ whose (Euclidean) dual code $\mathcal{C}^\perp$ satisfies $\mathcal{C} \cap \mathcal{C}^\perp = \{\mathbf{0}\}$. LCD codes have been widely applied in data storage, communications systems, consumer electronics, and cryptography. In [30], Massey showed that LCD codes provide an optimum linear coding solution for the two-user binary adder channel. In 2014, Carlet and Guilley [6] investigated an interesting application of binary LCD codes against side-channel attacks (SCA) and fault injection attacks (FIA) and presented several constructions of LCD codes. It was shown non-binary LCD codes in characteristic 2 can be transformed into binary LCD codes by expansion. It is then important to keep in mind that, for SCA, the most interesting case is when the code is defined over an alphabet of size q with q even. The recent literature is abundant about LCD codes. One of the most important results on the classification of LCD codes is that any linear code over $\mathbb{F}_q$ $(q > 3)$ is equivalent to an (Euclidean) LCD code [11]. A complete state-of-the-art on LCD codes can be found in the recent article [7] and the references therein.

This paper is organized as follows. In Subsection 3.1, we modify the parameter proposed in [17,25] so that it does not depend on the algebraic immunity as in [17,25] that we denote by $FAI(f)$. We show that the value of the modified parameter is less or equal to the one proposed in [17] and [25] for every Boolean function. In Subsection 3.2, we introduce the notion of the immunity profile of a Boolean function and show that both the algebraic immunity and the FAI of a Boolean function can be deduced from this immunity profile. In Subsection 4.1, we show that if a function is at low Hamming distance from a low algebraic degree function, then it is weak against fast algebraic attacks and we study further the behavior of FAI. In Subsection 4.2, we study the FAI of a classical secondary construction of Boolean function, which it called concatenation Boolean function. We prove that the FAI of the concatenation of the Boolean function can be bounded from below and above by the FAI of its sub-functions. Finally, in Section 5 we present a coding-theory characterization of perfect algebraic immune Boolean functions by means of the LCD-ness of punctured Reed-Muller codes and derive some new infinite families of LCD codes.

2 Preliminaries and notation

In this section, we give a brief introduction to algebraic immunity, Reed-Muller codes and linear complementary dual codes, which are the foundations of other sections.

2.1 Algebraic immunity of Boolean functions

Let n be any positive integer. In this paper, we shall denote by $\mathcal{B}_n$ the set of all n-variable Boolean functions over $\mathbb{F}_2^n$. Any n-variable Boolean function f (that is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$) admits a unique *algebraic normal form* (ANF), that is, a representation as a multivariate polynomial over $\mathbb{F}_2$

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i,$$

where the a_I's are in $\mathbb{F}_2$. The terms $\prod_{i\in I} x_i$ are called *monomials*. The *algebraic degree* $\deg(f)$ of a Boolean function f equals the maximum degree of those monomials whose coefficients are nonzero in its algebraic normal form.

If we identify $\mathbb{F}_2^n$ with the Galois field $\mathbb{F}_{2^n}$ of order 2^n, Boolean functions of n-variables are then the binary functions over the Galois field $\mathbb{F}_{2^n}$ (one can always endow this vector space with the structure of a field, thanks to the choice of a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$) of order 2^n. The *support* of f, denoted by $supp(f)$, is the set of elements of $\mathbb{F}_{2^n}$ whose image under f is 1, that is, $supp(f) = \{x \in \mathbb{F}_{2^n} : f(x) = 1\}$. The *weight* of f, denoted by $wt(f)$, is the *Hamming weight* of the image vector of f, that is, the cardinality of its support $supp(f) := \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.

For any positive integer k, and r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$, denoted by Tr_r^k, is the mapping defined as: $\forall x \in \mathbb{F}_{2^k}, \quad Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}}$. In particular, we denote the *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ by $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. Every non-zero Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion of the form:

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1})$$

called its polynomial form, where Γ_n is the set of integers obtained by choosing one element in each cyclotomic class of 2 modulo $2^n - 1$, $o(j)$ is the size of the cyclotomic coset of 2 modulo $2^n - 1$ containing j, $a_j \in \mathbb{F}_{2^{o(j)}}$ and, $\epsilon = wt(f)$ modulo 2. The algebraic degree of f is equal to the maximum 2-weight of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$. We recall that the 2-weight of an exponent j, that we denote by $w_2(j)$, is the number of 1 in its binary expansion.

An n-variable Boolean function g is said to be an *annihilator* of an n-variable Boolean function f if $f \cdot g = 0$, where $f \cdot g$ is the Boolean function whose output equals the product in $\mathbb{F}_2$ of the outputs of f and g. The set of all non-zero annihilators of a Boolean function f shall be denoted by $AN(f)$. We shall denote by $AN^c(f)$ the complement of the set $AN(f)$, that is, the set of n-variable Boolean function f such that $f \cdot g \neq 0$. We shall denote by $LDA(f)$ the minimum degree of non-zero annihilators of f [33]. The *algebraic immunity* $AI(f)$ of f is the minimum value between $LDA(f)$ and $LDA(1+f)$. Obviously, for a Boolean function f, we have $AI(1 + f) = AI(f)$. In addition, algebraic immunity is invariant under affine transformations. More specifically, if f is an n-variable Boolean function and A is an affine automorphism of $\mathbb{F}_2^n$ then, $AI(f) = AI(f \circ A)$.

2.2 Linear codes and Reed-Muller codes

An $[\ell, k]$ code $\mathcal{C}$ over the finite field $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^\ell$ with dimension k. For convenience, we will denote by $\dim_{\mathbb{F}_q}(\mathcal{C})$ the dimension of the code $\mathcal{C}$. The dual code, denoted by $\mathcal{C}^\perp$, of $\mathcal{C}$ is a linear code with dimension $\ell - k$ and is defined by

$$\mathcal{C}^\perp = \left\{ (w_i)_{i=1}^\ell \in \mathbb{F}_q^\ell : \begin{array}{l} c_1 w_1 + \cdots + c_\ell w_\ell = 0 \\ \text{for all } (c_1, \cdots, c_\ell) \in \mathcal{C} \end{array} \right\}.$$

Puncturing and shortening are classical techniques used to obtain codes of length less than ℓ from mother codes having length ℓ, thus decreasing the length of codes. These constructions will be useful for understanding fast algebraic immunity. Given an $[\ell, k]$ code $\mathcal{C}$, we can puncture it by deleting the same coordinate i in each codeword. The resulting code is denoted by $\mathcal{C}^{\{i\}}$. For any set D of coordinates in $\mathcal{C}$, we use $\mathcal{C}^D$ to denote the code obtained by puncturing $\mathcal{C}$ in all coordinates in D. Let $\mathcal{C}(D)$ be the set of codewords which are $\mathbf{0}$ on D. Then the shortened code of $\mathcal{C}$ in all coordinates in D, denoted by $\mathcal{C}_D$, is the code obtained by puncturing the coordinates of $\mathcal{C}(D)$ in D. Puncturing a code is equivalent to shortening the dual code, as explained by the following proposition, whose proof can be found in [21, Theorem 1.5.7].

Proposition 1. *Let $\mathcal{C}$ be an $[\ell, k]$ code over $\mathbb{F}_q$ and let D be any set of coordinates of $\mathcal{C}$. Then*

$$\left(\mathcal{C}^D\right)^\perp = \left(\mathcal{C}^\perp\right)_D \text{ and } \left(\mathcal{C}_D\right)^\perp = \left(\mathcal{C}^\perp\right)^D.$$

Reed-Muller codes first appeared in print in 1954 and remain "$\cdots$ one of the oldest and best understood families of codes" [29, p. 370]. As stated in [4], we use $\mathrm{RM}(d, n)$ to denote the dth-order Reed-Muller code of length 2^n. Each codeword in $\mathrm{RM}(d, n)$ is defined by evaluating an n-variable Boolean function h of degree at most d at all points in $\mathbb{F}_2^n$. The Reed-Muller codes $\mathrm{RM}(d, n)$ have been shown to be equivalent to primitive cyclic codes (codes of length $2^n - 1$) with an overall parity check added [24]. Let α be a primitive element of $\mathbb{F}_{2^n}$. Let $P_0 = 0$ and $P_j = \alpha^{j-1}$, where $1 \le j \le 2^n - 1$. Then $P_0, ..., P_{2^n-1}$ is an enumeration of the points of the vector space $\mathbb{F}_{2^n}$. Under this enumeration, the Reed-Muller code $\mathrm{RM}(d, n)$ of order d in n variables may be written as

$$\mathrm{RM}(d, n) = \left\{ (f(P_0), \cdots, f(P_{2^n-1})) : f \in \mathcal{B}_n, \deg(f) \le d \right\}.$$

We summarize the results on the properties of the Reed-Muller codes in the following theorem. For the details of proof we refer the reader to [24,29].

Theorem 1. *Let n be any positive integer and let $0 \le d \le n$.*

(1) The Reed-Muller code $\mathrm{RM}(d, n)$ is a binary linear code of dimension $\sum_{i=0}^d \binom{n}{i}$.
(2) The dual code of $\mathrm{RM}(d, n)$ is the code $\mathrm{RM}(n - d - 1, n)$.

2.3 Linear complementary dual codes and self-orthogonal codes

The *hull* of a linear code $\mathcal{C}$ is defined to be $\mathrm{Hull}(\mathcal{C}) = \mathcal{C} \cap \mathcal{C}^{\perp}$. When $\mathrm{Hull}(\mathcal{C}) = \mathcal{C}$, $\mathcal{C}$ is said to be *self-orthogonal.* In particular, if $\mathrm{Hull}(\mathcal{C}) = \mathcal{C} = \mathcal{C}^{\perp}$, then $\mathcal{C}$ is called a self-dual code. The code $\mathcal{C}$ is called a *linear complementary dual code* (in brief, an *LCD* code) if $\mathrm{Hull}(\mathcal{C})$ is the zero space. These codes have been extensively studied recently [8,9,11,23,27,28,35].

For a matrix G, G^T denotes the transposed matrix of G. The *Gram matrix* of G is defined to be GG^T. The Gram matrix of a generator of a linear code plays an important role in the study of the hulls of linear codes [19,41].

Proposition 2. *Let $\mathcal{C}$ be an $[\ell, k]$ linear code over $\mathbb{F}_q$ with generator matrix G. Then*

$$\dim_{\mathbb{F}_q}(\mathrm{Hull}(\mathcal{C})) = k - \mathrm{Rank}\left(GG^T\right).$$

In particular, $\mathcal{C}$ is LCD (resp. self-orthogonal) if and only if GG^T is nonsingular (resp. $GG^T = 0$).

A vector $\mathbf{x} = (x_1, x_2, \ldots, x_\ell)$ in $\mathbb{F}_2^\ell$ is even-like if $\sum_{i=1}^{\ell} x_i = 0$. A binary code is said to be *even-like* if it has only even-like codewords. The following proposition gives a necessary condition for an even-like code being LCD [10].

Proposition 3. *Let $\mathcal{C}$ be an even-like binary code with parameters $[\ell, k]$. If $\mathcal{C}$ is LCD then k is an even integer.*

3 Fast algebraic immunity and fast immunity profile

3.1 A new definition of fast algebraic immunity and its consequences

In the literature, different criteria have been proposed to characterize the immunity of Boolean functions against fast algebraic attacks; some of those characterizations do not define a parameter but a property that should satisfy a Boolean function to resist to fast algebraic attacks [18,26,36].

Definition 1. *Let f be an n-variable Boolean function. We call fast algebraic immunity of f, denoted by $FAI(f)$, the smallest value taken by* $\deg(g)+\deg(f\cdot g)$ *when $g \not\equiv 1$ ranges over the set $AN^c(f)$. We say that such a g achieves $FAI(f)$.*

Remark 1. It has been shown in [14, Theorem 7.2.1] that, for any n-variable Boolean function f and for every positive integers d and e such that $d + e \geq n$, there exists g of algebraic degree at most d and h of algebraic degree at most e such that $f \cdot g = h$. It implies that $FAI(f) \leq n$. Now, one has $\deg(f \cdot g) \geq \deg(g)$ if $\deg(f \cdot g) + \deg(g) = FAI(f)$ (indeed, suppose that $\deg(f \cdot g) < \deg(g)$ then g cannot achieve $\deg(f \cdot g) + \deg(g) = FAI(f)$, because, denoting $h = f \cdot g$, we have $f \cdot h = h$ and then $h \neq 0$ and $\deg(f \cdot h) + \deg(h) < \deg(f \cdot g) + \deg(g)$). Hence, if g achieves $FAI(f)$ then, necessarily, $\deg(g) \leq \frac{n}{2}$ since $\deg(g) + \deg(f \cdot g) = FAI(f) \leq n$ and $\deg(g) \leq \deg(f \cdot g)$ implies that $\deg(g) \leq \frac{n}{2}$.

Remark 2. In [16,26], the authors proposed different criteria that should satisfy a Boolean function to be (almost) resistant to fast algebraic attacks. Those criteria are very similar. Indeed, in [16, Definition 1], it is defined that an n-variable Boolean function f would be *almost optimal resistant* against fast algebraic attacks if, for $1 \leq e < \frac{n}{2}$, $\deg(f \cdot g) \geq n - e - 1$ whenever $\deg(g) \leq e$ and $f \cdot g \neq 0$. In [26, Definition 2], the authors defined *perfect algebraic immune functions* as the n-variable Boolean function f such that, for every $1 \leq e < \frac{n}{2}$, $\deg(f \cdot g) \geq n - e$ for any n-variable Boolean function g of algebraic degree at most e.

Observe that the *almost optimal resistance* defined in [16] is equivalent to $FAI(f) \geq n - 1$ while the *perfect algebraic immune functions* of [26] are those such that $FAI(f) \geq n$.

We first derive from the definition of FAI an upper bound on the algebraic degree of Boolean function achieving FAI.

Proposition 4. *Let n be a positive integer. Let f be an n-variable function. Let g an n-variable function achieving $FAI(f)$. Then* $\deg(g) \leq \left\lfloor \frac{FAI(f)}{2} \right\rfloor$ *and* $\deg(f \cdot g) \geq \left\lceil \frac{FAI(f)}{2} \right\rceil$

Proof. Let $g \in AN^c(f)$ achieving $FAI(f)$, that is, $\deg(g) + \deg(f.g) = FAI(f)$. Necessarily $\deg(f \cdot g) \geq \deg(g)$ (see Remark 2). Hence $2\deg(g) \leq FAI(f)$, that is, $\deg(g) \leq \left\lfloor \frac{FAI(f)}{2} \right\rfloor$. Thus $\deg(f \cdot g) = FAI(f) - \deg(g) \geq FAI(f) - \left\lfloor \frac{FAI(f)}{2} \right\rfloor = \left\lceil \frac{FAI(f)}{2} \right\rceil$.

□

In [25], it has been proposed another definition than ours for the fast algebraic immunity. Indeed, in [25], the authors give the following definition for the fast algebraic immunity of a Boolean function:

$$\min\left(2AI(f), \min_{1 \leq \deg(g) < AI(f)} (\deg(g) + \deg(f \cdot g))\right). \tag{1}$$

Remark 3. Using the definition above, an upper bound of fast algebraic immunity of power functions has been established by Mesnager and Cohen [34]. More precisely, let $f(x) = Tr_1^n(\gamma x^d)$ where $\gamma \in \mathbb{F}_{2n}$ and d is a positive integer. Suppose that $AI(f) \geq \left\lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \right\rceil + 1$. Then

$$FAI(f) \leq u\lfloor \sqrt{n} \rfloor + 2\left\lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \right\rceil - 1$$

where u is the number of runs of 1 in the binary representation of d.

Note that $AN^c(f)$ contains all n-variable Boolean functions g such that $1 \leq \deg(g) < AI(f)$ because any g of algebraic degree less than $AI(f)$ cannot be an annihilator of f. Hence

$$\min_{1\leq\deg(g)<AI(f)} (\deg(g) + \deg(f \cdot g)) \geq FAI(f).$$

Furthermore, $AN^c(f)$ may contain Boolean function of algebraic degree greater than or equal to $AI(f)$, that is, $\{g : \mathbb{F}_2^n \to \mathbb{F}_2 \mid 1 \leq \deg(g) < AI(f)\}$ is strictly contained in $AN^c(f)$. However, (1) is less than $FAI(f)$ if and only only if $2AI(f) < FAI(f)$. We are now going to show that the FAI of a Boolean function or its complement is necessarily less than or equal to (1). To this end, we first show that the FAI of a function can be bounded from above and below with the lowest degree of the non-zero annihilators of its complement.

Proposition 5. *Let f be a non-zero n-variable Boolean function. Then*

$$LDA(1 + f) + 1 \leq FAI(f) \leq 2LDA(1 + f).$$

Proof. Note that $g \notin AN^c(f)$ says only that $f \cdot g \neq 0$. Hence, $AN^c(f)$ contains all the non-zero annihilators of $1+f$ since $f \cdot g = g$ for every $g \in AN(1+f)$. Now, if g is an non-zero annihilator of $1+f$ then $f \cdot g = g$ proving that $FAI(f) \leq 2\deg(g)$ from which we deduce that $FAI(f) \leq 2LDA(1 + f)$.

On the other hand, observe that, if $f \cdot g \neq 0$, then $f \cdot g$ is an non-zero annihilator of $1 + f$. Thus $\deg(g) + \deg(f \cdot g) \geq 1 + LDA(1 + f)$. □

Remark 4. The lower bound and the upper bound in Proposition 5 are achieved. Indeed, let f be an n-variable Boolean function whose support strictly contains the support of an affine Boolean function l. Then $fl = l$ which implies that $LDA(1 + f) = 1$ since $(1 + f) \cdot l = 0$. Thus $\deg(l) + \deg(f \cdot l) = 2\deg(l) = 2 = LDA(1 + f) + 1 = 2LDA(1 + f)$.

Proposition 5 says that, for any n-variable Boolean function, $FAI(f) \leq 2LDA(1+f)$. Thus, if $LDA(1+f) > LDA(f)$, $FAI(1+f) \leq 2LDA(f) = 2AI(f)$ while $FAI(f) \leq 2AI(f) = 2LDA(1 + f)$ if $LDA(1 + f) \leq LDA(f)$. Summarizing:

Corollary 1. *Let f be an n-variable Boolean function. Then*

$$\min(FAI(f), FAI(1 + f)) \leq 2AI(f).$$

Based on this observation, an extension of fast algebraic immunity is given by Definition 2.

Definition 2. *Let f be an n-variable Boolean function. The $\mathcal{FAI}$ of f is the minimum value between $FAI(f)$ and $FAI(1 + f)$:*

$$\mathcal{FAI}(f) = \min(FAI(f), FAI(1 + f)).$$

A direct consequence of Proposition 5 is then that the $\mathcal{FAI}$ of an n-variable function is less than or equal to (1). But above, one deduces from Proposition 5.

Proposition 6. *Let f be an n-variable Boolean function. Then*

$$\min\left(LDA(f)+1, LDA(1+f)+1\right) \leq \mathcal{FAI}(f) \leq 2AI(f).$$

Another property of FAI is that it is invariant under affine transformations like the standard algebraic immunity.

Proposition 7. *Let f be an n-variable Boolean function and A an automorphism of $\mathbb{F}_2^n$. Then $FAI(f \circ A) = FAI(f)$.*

Proof. Note that $\{\deg(g)+\deg(f\cdot g) \mid g \in AN^c(f)\} = \{\deg(g\circ A)+\deg(f\circ A\cdot g\circ A) \mid g \in AN^c(f)\}$. Observe now, that $f\cdot g \neq 0$ if and only if $f\circ A\cdot g\circ A \neq 0$, that is, $g \in AN^c(f)$ if and only if $g\circ A \notin AN^c(f\circ A)$. Thus $FAI(f) = FAI(f\circ A)$. □

One can extend Proposition 7 to $\mathcal{FAI}$.

Proposition 8. *Let f be an n-variable Boolean function and A an automorphism of $\mathbb{F}_2^n$. Then $\mathcal{FAI}(f \circ A) = \mathcal{FAI}(f)$.*

3.2 Fast immunity profile

Set $MUL_k(f) = \{f \cdot g \mid \deg(g) \leq k\}$ and $\mu_k(f) = mindegMUL_k(f)$, where *mindeg* denotes the minimum degree of the non-zeros elements of the set. Clearly $(\mu_k(f)_{1\leq k\leq n}$ is a non-increasing sequence of integers. We shall call it the *fast immunity profile* of f. Note that $MUL_k(f \circ A) = \{f \circ A \cdot g \mid \deg(g \circ A) \leq k\} = \{f \cdot h \mid \deg(h) \leq k\} \circ A = MUL_k(f) \circ A$ for every affine automorphism of $\mathbb{F}_2^n$, proving that

Lemma 1. *Let f be an n-variable Boolean function and A an automorphism of $\mathbb{F}_2^n$. Then $\mu_k(f) = \mu_k(f \circ A)$ for every $1 \leq k \leq n$.*

We now show that the algebraic immunity and the fast algebraic immunity of f can be expressed by means of the immunity profile. We first recall the relationship between the annihilators of a function f and the multiples of $f + 1$.

Proposition 9. *Let f be an n-variable Boolean function. Then*

$$LDA(f) = \min_{1\leq k\leq n} \mu_k(f+1).$$

Furthermore, if $k \geq LDA(f)$, $\mu_k(f+1) = LDA(f)$.

Proof. For any integer k ranging from 1 to n, we have $\mu_k(1+f) = mindegMUL_k(1+f) \geq LDA(f)$ since every nonzero element of $MUL_k(1+f)$ is a non-zero annihilator of f. It follows that $\min_{1\leq k\leq n}\mu_k(f+1) \geq LDA(f)$.

Conversely, let g be an annihilator of f of algebraic degree $LDA(f)$. Then one has $(1+f)\cdot g = g$ and thus $\mu_{LDA(f)}(1+f) \leq LDA(f)$ implying that $\min_{1\leq k\leq n}\mu_k(f+1) \leq LDA(f)$. Consequently, $LDA(f) = \min_{1\leq k\leq n}\mu_k(f+1)$.

Furthermore, note that $(\mu_k(1+f))_{1\leq k\leq n}$ is a nonincreasing sequence of integers. Hence, since $\mu_{LDA(f)}(1+f) \leq LDA(f)$, one has necessarily $\mu_k(1+f) = LDA(f)$ when $k \geq LDA(f)$. □

Recalling that $AI(f) = \min(LDA(f), LDA(1+f))$, we deduce:

Proposition 10. *Let f be an n-variable Boolean function. Then*

$$AI(f) = \min(\min_{1\le k\le n} \mu_k(f+1), \min_{1\le k\le n} \mu_k(f))$$

Proposition 11. *Let f be an n-variable Boolean function. Then*

$$FAI(f) = \min_{1\le k\le n}(k + \mu_k(f)).$$

Proof. Let $1 \le k \le n$ be arbitrary. By definition, $\mu_k(f)$ is the lowest algebraic degree of all nonzero elements of $MUL_k(f)$. Thus, for $g \ne 0$, $\deg(g) = k$, $f \cdot g \ne 0$, one has $\deg(f \cdot g) + \deg(g) \ge \mu_k(f) + k$. Hence, one gets that $FAI(f) \ge \min_{1\le k\le n}(k + \mu_k(f))$. Conversely, let $1 \le j \le n$ be such that $j + \mu_j(f) = \min_{1\le k\le n}(k+\mu_k(f))$. Let h be a function with $\deg(h) = j$ achieving $\mu_j(f)$ (such that $\mu_j(f) = \deg(f \cdot h)$ and $f \cdot h \ne 0$). Then $\deg(h) + \deg(f \cdot h) = j + \mu_j(f) \ge FAI(f)$. $\square$

4 Fast algebraic immunity, approximation and concatenation of functions

4.1 Fast algebraic immunity and approximation of functions

In [40] the algebraic complement of a Boolean function and its algebraic immunity have been studied.

Definition 3. *Given a Boolean function f defined on $\mathbb{F}_2^n$, the algebraic complement of f, denoted by f^c, is the function that contains all the monomials that are not in the algebraic normal form of f.*

In [40, Theorem 2], the authors have shown that the algebraic immunities of a Boolean function and its algebraic complement are close:

$$|AI(f) - AI(f^c)| \le 1.$$

Let us denote by δ_0 the indicator of the singleton $\{0\}$. It is well-known and easily checked that the algebraic normal form of δ_0 equals $\sum_{I\subseteq\{1,\dots,n\}} \prod_{i\in I} x_i$. The algebraic complement of a function f is then the function $f + \delta_0$. Since the algebraic immunity is invariant under affine transformations, there is no reason to privilege δ_0 rather than any other indicator of a singleton δ_a (except that the ANF of the algebraic complement is nicely simple). Moreover, functions $f + \delta_a$, $a \in \mathbb{F}_2^n$, are all functions at Hamming distance 1 from f, and it seems natural to consider more generally functions at low Hamming distance from f. A nice observation has been made in [39]: if a function is at low Hamming distance from a low algebraic degree function, then it is weak against fast algebraic attacks. We show now that if a function is at low Hamming distance from a low algebraic immunity function, then it is weak against (standard) algebraic attacks:

Proposition 12. *let k and d be two positive integers. Let f be any n-variable Boolean function such that $AI(f) = k$. Let δ be any Boolean function such that $w_H(\delta) < \min(2^{n-k}, 2^{d+1} - 1)$. Then:*

$$|AI(f + \delta) - AI(f)| \leq d.$$

Proof. There exists by hypothesis a nonzero annihilator g of f or of $f + 1$ whose algebraic degree is k. Let a_0 be any element such that $\delta(a_0) = 0$ and $g(a_0) = 1$. Such an element exists because the Hamming weight of g is larger than or equal to 2^{n-k}.

Write $\mathrm{Supp}(\delta) = \{x \in \mathbb{F}_2^n : \delta(x) = 1\}$ and $w = w_H(\delta)$. Let the points of $\mathrm{Supp}(\delta)$ be $a_1, \cdots, a_w$. Let π be the linear mapping given by

$$\begin{aligned} \pi : \mathrm{RM}(d, n) &\longrightarrow \mathbb{F}_2^{w+1} \\ (h(x))_{x \in \mathbb{F}_2^n} &\mapsto (h(a_i))_{i=0}^{w}. \end{aligned}$$

We next claim that the mapping π is surjective. Suppose the claim was false. Then the image of π lies in a hyperplane of $\mathbb{F}_2^{w+1}$ and thus we could find a non-zero vector $(c_{a_i})_{i=0}^{w} \in \mathbb{F}_2^{w+1}$ such that $c_{a_0} h(a_0) + \cdots c_{a_w} h(a_w) = 0$ for any n-variable Boolean function h of degree at most d. It follows that the vector $(c_x)_{x \in \mathbb{F}_2^n}$ defined by $c_x = \begin{cases} c_{a_i}, & \text{if } x = a_i \\ \\ 0, & \text{otherwise} \end{cases}$ belongs to the dual code $\mathrm{RM}(d, n)^{\perp} = \mathrm{RM}(n - d - 1, n)$ of $\mathrm{RM}(d, n)$. Note that the weight of the codeword $(c_x)_{x \in \mathbb{F}_2^n}$ of $\mathrm{RM}(n - d - 1, n)$ is less or equal to $w + 1$, which contradicts the facts that the minimum distance of $\mathrm{RM}(n - d - 1, n)$ is at least 2^{d+1} and $w + 1 \leq 2^{d+1} - 1$. Thus π is a surjective mapping. In particular, there exists a polynomial h of degree at most d such that $h(a_0) = 1$ and $h(a_i) = 0$ for $1 \leq i \leq w$. We have then $(f + \delta) \cdot gh = 0$ or $(f + 1 + \delta) \cdot gh = 0$ and gh is an annihilator of $f + \delta$ or of $f + 1 + \delta$ and it is nonzero since $(gh)(a_0) = 1$. This implies that $AI(f + \delta) \leq AI(f) + d$ and applying this result to $f + \delta$ instead of f gives $AI(f) \leq AI(f + \delta) + d$, which completes the proof. □

Note that this result and the result from [39] mentioned above are complementary of each other since the condition of being at low Hamming distance from a low algebraic immunity function is a weaker assumption than being at low Hamming distance from a function of low algebraic degree, and moreover the weakness against standard algebraic attacks is still worse than the weakness against fast algebraic attacks (because when they apply, algebraic attacks are more efficient than fast algebraic attacks), but the result from [39] still applies for functions at low Hamming distance from a function whose algebraic degree is not necessarily low, but is not high either; indeed it says that if $w_H(\delta) < \sum_{i=0}^{d} \binom{n}{i}$ and f has algebraic degree k then $FAI(f + \delta) \leq k + 2d$.

Let us now investigate if $FAI(f)$ and $FAI(f^c)$ are close or not. To this end, we shall need the following Lemma.

Lemma 2. *Let $f \neq \delta_0$ be an n-variable Boolean function. Let g achieving $FAI(f)$. Then there exists an n-variable affine function l vanishing at 0 such that $f \cdot g \cdot l \neq 0$.*

Proof. Suppose that for every n-variable affine Boolean function l vanishing at 0, $f \cdot g \cdot l = 0$. Then, for any $1 \leq i \leq n$, $f \cdot g \cdot l_i = 0$ where $l_i(x_1, \ldots, x_n) = x_i$, that is, $f \cdot g = (1 + l_i)h_i$ for some n-variable Boolean function h_i. Therefore, $f \cdot g = \delta_0 = \prod_{i=1}^{n} l_i$. Now, $FAI(f) = \deg(f \cdot g) + \deg(g) = n + \deg(g) \leq n$. Hence, $g = 1$ contradicting $f \neq \delta_0$. □

We begin with showing.

Proposition 13. *Let f be an n-variable Boolean function. Suppose $f \neq \delta_0$ and $f^c \neq \delta_0$. Then*

$$|FAI(f^c) - FAI(f)| \leq 2.$$

Proof. According to Proposition 11, $FAI(f) = \min_{1 \leq k \leq n}(k + \mu_k(f))$. Let $k \geq 1$ achieving $FAI(f)$: $k + \mu_k(f) = FAI(f)$. Let g achieving $\mu_k(f)$: $\deg(f \cdot g) = \mu_k(f)$.

Now, observe that, for any n-variable Boolean function p,

$$f^c \cdot p = f \cdot p + \delta_0 \cdot p = \begin{cases} f \cdot p & \text{if } p(0) = 0 \\ f \cdot p + \delta_0 & \text{if } p(0) = 1 \end{cases}$$

But in all cases, for any n-variable affine Boolean function l vanishing at 0, $f \cdot g \cdot l = f^c \cdot g \cdot l$ since $\delta_0 \cdot l = 0$. According to Lemma 2, there exists l such that $f \cdot g \cdot l = f^c \cdot g \cdot l \neq 0$. Then

$$\begin{aligned} FAI(f^c) &\leq \deg(f^c \cdot g \cdot l) + \deg(g \cdot l) \\ &\leq \deg(f^c \cdot g) + \deg(g) + 2 = FAI(f) + 2. \end{aligned}$$

Now, since the algebraic complement of f^c is f itself. One can exchange the role of f and its algebraic complement f^c in the above arguments and prove

$$FAI(f) \leq FAI(f^c) + 2.$$

□

Remark 5. Following the above proof, if the n-Boolean function g achieving $FAI(f)$ vansihes at 0. Then, one has $FAI(f^c) \leq \deg(f^c \cdot g) + \deg(g) = \deg(f \cdot g) + \deg(g) = FAI(f)$. Therefore, if $FAI(f^c)$ is also achieved by an n-variable Boolean function vanishing at 0 then, $FAI(f^c) \geq FAI(f)$. Therefore, we might have $FAI(f) = FAI(f^c)$ for some subclasses of n-variable Boolean functions.

Remark 6. Observe that the condition $f \neq \delta_0$ is not restrictive since $AI(\delta_0) = 1$ ($\delta_0 \cdot l = 0$ if $l(0) = 0$ and $\deg(l) = 1$).

4.2 Fast algebraic immunity and concatenation of Boolean functions

A classical secondary constructions of Boolean functions from Boolean functions in lower dimension is the following.

Definition 4. *Let f_0 and f_1 be two $(n-1)$-variable Boolean functions. The concatenation of f_0 with f_1 is the n-variable Boolean function defined, for $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, by*

$$\begin{aligned} f(x_1, \ldots, x_n) &= (x_n + 1) f_0(x_1, \ldots, x_{n-1}) \\ &\quad + x_n f_1(x_1, \ldots, x_{n-1}) \\ &= \begin{cases} f_0(x_1, \ldots, x_{n-1}) & \text{if } x_n = 0 \\ f_1(x_1, \ldots, x_{n-1}) & \text{if } x_n = 1. \end{cases} \end{aligned} \tag{2}$$

Any n-variable Boolean function of algebraic degree k can be written

$$\begin{aligned} g(x_1, \ldots, x_n) &= (x_n + 1) g_0(x_1, \ldots, x_{n-1}) \\ &\quad + x_n g_1(x_1, \ldots, x_{n-1}) \end{aligned} \tag{3}$$

where g_0 and g_1 are $(n-1)$-Boolean function and

$$\deg(g) = \max(\deg(g_0), \deg(g_0 + g_1) + 1).$$

Observe that, the product $f \cdot g$, where f is given by (2) and g is given by (3), is

$$\begin{aligned} &f(x_1, \ldots, x_n) g(x_1, \ldots, x_n) \\ &\quad = (x_n + 1) f_0(x_1, \ldots, x_{n-1}) g_0(x_1, \ldots, x_{n-1}) \\ &\quad\quad + x_n f_1(x_1, \ldots, x_{n-1}) g_1(x_1, \ldots, x_{n-1}). \end{aligned}$$

Hence

$$\begin{aligned} \deg(f \cdot g) + \deg(g) = \max\Big(&\deg(f_0 g_0) + \deg(g_0), \\ &\deg(f_0 g_0) + \deg(g_0 + g_1) + 1, \\ &\deg(f_0 g_0 + f_1 g_1) + \deg(g_0) + 1, \\ &\deg(f_0 g_0 + f_1 g_1) + \deg(g_0 + g_1) + 2\Big). \end{aligned} \tag{4}$$

Based on this observation, we prove

Proposition 14. *Let n be a positive integer greater than 1. Let f_0 and f_1 be two $(n-1)$-variable Boolean functions. Let f be the n-variable Boolean function obtained by concatenating f_0 with f_1. Then*

$$FAI(f) \geq \min(FAI(f_0), FAI(f_1) + 1),$$

and

$$FAI(f) \leq \min(FAI(f_0), FAI(f_1)) + 2.$$

Proof. Let g an n-variable Boolean function achieving $FAI(f)$: $FAI(f) = \deg(f\cdot g) + \deg(g)$ and $f \cdot g \neq 0$. This Boolean function can be written as (3). Since $f \cdot g \neq 0$, either $f_0 \cdot g_0 \neq 0$ either $f_1 \cdot g_1 \neq 0$. If $f_0 \cdot g_0 \neq 0$ then, according to (4), $FAI(f) \geq \deg(f_0g_0) + \deg(g_0) \geq FAI(f_0)$. If $f_0g_0 = 0$ and $f_1g_1 \neq 0$, then (4) rewrites as

$$\begin{aligned}\deg(f \cdot g) + \deg(g) = \max\Big(&\deg(f_1g_1) + \deg(g_0) + 1,\\ &\deg(f_1g_1) + \deg(g_0 + g_1) + 2\Big).\end{aligned}$$

The result follows then from nothing that

- either $\deg(g_0 + g_1) < \deg(g_1)$, wich implies $\deg(g_0) = \deg(g_1)$ and thus $FAI(f) \geq \deg(f_1g_1) + \deg(g_0) + 1 \geq FAI(f_1) + 1$,
- either $\deg(g_0 + g_1) \geq \deg(g_1)$ which implies that $FAI(f) \geq \deg(f_1g_1) + \deg(g_1) + 2 \geq FAI(f_1) + 2 \geq FAI(f) + 1$.

Conversely, if we take g_0 achieving $FAI(f_0)$ and $g_1 = 0$ in (4), then, we get

$$FAI(f) \leq \deg(g) = \deg(f_0g_0) + \deg(g_0) + 2 = FAI(f_0) + 2.$$

Likewise, if we take g_1 achieving $FAI(f_1)$ and $f_0 = 0$ then,

$$FAI(f) \leq \deg(g) = \deg(f_1g_1) + \deg(g_1) + 2 = FAI(f_1) + 2.$$

□

In [12], the authors have considered such construction to design Boolean functions suitable for the filter model of pseudo-random generator. More precisely, they have considered the particular case of the concatenation of an $(n-1)$-variable Boolean function f with its complement $1 + f$ to 1. Let us denote $\bar{f}$ such a concatenation:

$$\begin{aligned}\bar{f}(x_1, \ldots, x_n) &= x_n + f(x_1, \cdots, x_{n-1})\\ &= (x_n + 1)f(x_1, \cdots, x_{n-1})\\ &\quad + x_n(1 + f(x_1, \cdots, x_{n-1})).\end{aligned} \tag{5}$$

We then deduce from Proposition 14

Corollary 2. *Let f be an $(n-1)$-variable Boolean function. Let $\bar{f}$ be defined by (5). Then*

$$\min(FAI(f), FAI(1 + f) + 1) \leq FAI(\bar{f}) \leq \mathcal{FAI}(f) + 2.$$

Now, note that $1 + \bar{f}$ is the concatenation of $1 + f$ with f:

$$\begin{aligned}1 + \bar{f}(x_1, \ldots, x_n) &= 1 + x_n + f(x_1, \cdots, x_{n-1})\\ &= (x_n + 1)(1 + f(x_1, \cdots, x_{n-1}))\\ &\quad + x_nf(x_1, \cdots, x_{n-1}).\end{aligned}$$

Therefore

Corollary 3. *Let f be an $(n-1)$-variable Boolean function. Let $\bar{f}$ be defined by (5). Then*

$$\mathcal{FAI}(f) \leq \mathcal{FAI}(\bar{f}) \leq \mathcal{FAI}(f) + 2.$$

5 Fast algebraic immunity and LCD codes

In this section we shall establish the relation between fast algebraic immunity, perfect algebraic immune functions, punctured Reed-Muller codes and binary LCD codes.

The link between the algebraic immunity of Boolean functions and the dimensions of punctured Reed-Muller codes is described in the following.

Proposition 15. *Let e be a positive integer. Let f be an n-variable Boolean function and let D be its support. Then the algebraic immunity of f is greater than e if and only if the dimensions of the two punctured Reed-Muller codes* $\mathrm{RM}(e,n)^D$ *and* $\mathrm{RM}(e,n)^{\overline{D}}$ *are both equal to* $\dim_{\mathbb{F}_2}(\mathrm{RM(e,n)})$.

Proof. Let $AI(f) > e$. Assume by way of contradiction,

$$\dim_{\mathbb{F}_2}\left(\mathrm{RM}(e,n)^{\overline{D}}\right) < \dim_{\mathbb{F}_2}(\mathrm{RM(e,n)}). \tag{6}$$

Consider the linear transformation Res_D from $\mathrm{RM(e,n)}$ to the punctured code $\mathrm{RM}(e,n)^{\overline{D}}$ defined by

$$(g(x))_{\mathbb{F}_2^n} \mapsto (g(x))_{x\in D}.$$

By assumption in (6), there exists a nonzero function $g \in \mathcal{B}_n$ of degree at most e such that $Res_D(g) = (g(x))_{x\in D} = \mathbf{0}$. Then $fg = 0$, contrary to $AI(f) > e$. Hence $\dim_{\mathbb{F}_2}\left(\mathrm{RM}(e,n)^{\overline{D}}\right) = \dim_{\mathbb{F}_2}(\mathrm{RM(e,n)})$. By a similar argument, we can show that $\dim_{\mathbb{F}_2}\left(\mathrm{RM}(e,n)^{D}\right) = \dim_{\mathbb{F}_2}(\mathrm{RM(e,n)})$.

As for the converse, suppose the assertion is false. Then we could find a nonzero function g of degree at most e such that $fg = 0$ or $(1+f)g = 0$. By symmetry, one can assume that $fg = 0$. We then have $Res_D(g) = (g(x))_{x\in D}$ is the all zeros codeword of $\mathrm{RM}(e,n)^{\overline{D}}$. We conclude that the linear transformation Res_D is surjective but not injective. This clearly forces $\dim_{\mathbb{F}_2}\left(\mathrm{RM}(e,n)^{\overline{D}}\right) < \dim_{\mathbb{F}_2}(\mathrm{RM(e,n)})$, a contradiction. Therefore $AI(f) > e$. ☐

Given a nonzero Boolean function f, let $\left\langle \mathbf{1}_{wt(f)} \right\rangle$ denote the binary code generated by the all-ones vector $\mathbf{1}_{wt(f)}$ of length $wt(f)$. To treat fast algebraic immunity of Boolean functions, we need to invoke punctured Reed-Muller codes.

Lemma 3. *Let e, e' and n be positive integers. Let f be an n-variable nonzero Boolean function and let D be its support. Then the intersection of* $\mathrm{RM}(e,n)^{\overline{D}}$ *and* $\left(\mathrm{RM}(e',n)^{\overline{D}}\right)^{\perp}$ *is included in* $\left\langle \mathbf{1}_{wt(f)} \right\rangle$ *if and only if* $\deg(fg) \geq n - e'$ *holds for any n-variable nonzero Boolean function $g \in AN^c(f)\backslash(1 + AN(f))$ of degree at most e, where $1 + AN(f) = \{1 + h : h \in AN(f)\}$.*

Proof. By Proposition 1,

$$\left(\mathrm{RM}(e',n)^{\overline{D}}\right)^{\perp} = \left(\mathrm{RM}(e',n)^{\perp}\right)_{\overline{D}}.$$

Invoking Part (5) of Theorem 1, we get

$$\left(\mathrm{RM}(e',n)^{\overline{D}}\right)^{\perp} = \mathrm{RM}(n-e'-1,n)_{\overline{D}}. \tag{7}$$

Let us first prove the only if part, so let us suppose that $\mathrm{RM}(e,n)^{\overline{D}} \cap \left(\mathrm{RM}(e',n)^{\overline{D}}\right)^{\perp} \subseteq \langle \mathbf{1}_{wt(f)} \rangle$. If there existed a function $g \in AN^c(f) \backslash (1+AN(f))$ such that $\deg(g) \leq e$ and $\deg(fg) \leq n-e'-1$, we would have

$$(g(x))_{x\in D} \in \mathrm{RM}(e,n)^{\overline{D}}$$

and

$$(g(x)f(x))_{x\in D} \in \mathrm{RM}(n-e'-1,n)_{\overline{D}}.$$

Then, taking $g \in AN^c(f)$ and $supp(f) = D$ into account, one sees that the nonzero codeword $(g(x))_{x\in D}$ is not equal to $\mathbf{1}_{wt(f)}$ and lies in the intersection of the punctured code $\mathrm{RM}(e,n)^{\overline{D}}$ and the shortened code $\mathrm{RM}(n-e'-1,n)_{\overline{D}}$. From (7), we deduce that $\mathrm{RM}(e,n)^{\overline{D}} \cap \left(\mathrm{RM}(e',n)^{\overline{D}}\right)^{\perp}$ is not included in $\langle \mathbf{1}_{wt(f)} \rangle$, a contradiction. Hence the proof of the only if part is concluded.

For the converse, suppose the assertion of the lemma is false. Then we could find a function $g \in AN^c(f)$ of degree at most e such that

$$(g(x))_{x\in D} \in \left(\mathrm{RM}(e,n)^{\overline{D}} \cap \left(\mathrm{RM}(e',n)^{\overline{D}}\right)^{\perp}\right) \setminus \langle \mathbf{1}_{wt(f)} \rangle.$$

Thus, we can apply (7) to conclude that $1+g \notin AN(f)$ and

$$(g(x)f(x))_{x\in D} = (g(x))_{x\in D} \in \mathrm{RM}(n-e'-1,n)_{\overline{D}}.$$

We thus get $\deg(gf) \leq n-e'-1$, a contradiction. This completes the proof. □

Lemma 4. *Let f be an n-variable nonzero Boolean function and let D be its support. Then $\mathbf{1}_{wt(f)} \notin \left(\mathrm{RM}(e',n)^{\overline{D}}\right)^{\perp}$ if and only if* $\deg(f) \geq n-e'$.

Proof. By (7), $\mathbf{1}_{wt(f)} \notin \left(\mathrm{RM}(e',n)^{\overline{D}}\right)^{\perp}$ if and only if $\mathbf{1}_{wt(f)} \notin \mathrm{RM}(n-e'-1,n)_{\overline{D}}$. The desired conclusion then follows from the definition of $\mathrm{RM}(n-e'-1,n)_{\overline{D}}$. □

The following theorem provides a characterization of fast algebraic immunity of n-variable higher degree Boolean functions by means of punctured Reed-Muller codes.

Theorem 2. *Let s be a positive integer. Let f be an n-variable nonzero Boolean function with* $\deg(f) \geq s-1$ *and let D be its support. Then the fast algebraic immunity of f is greater than or equal to s if and only if* $\mathrm{RM}(e,n)^{\overline{D}} \cap \left(\mathrm{RM}(e+n-s,n)^{\overline{D}}\right)^{\perp} = \{\mathbf{0}\}$ *holds for any* $1 \leq e \leq n$.

Proof. Let f be an n-variable Boolean function with $FAI(f) \geq s$. By the definition of fast algebraic immunity, we have

$$\deg(g) + \deg(gf) \geq s \text{ for any } g \in AN^c(f) \setminus \{1\}.$$

Now, as then, we can assert that $\deg(gf) \geq s - \deg(g) \geq n-(e+n-s)$ for any $g \in AN^c(f)$ with $1 \leq \deg(g) \leq e$. Therefore $\mathrm{RM}(e,n)^{\overline{D}} \cap \left(\mathrm{RM}(e+n-s,n)^{\overline{D}}\right)^{\perp} \subseteq \left\langle \mathbf{1}_{wt(f)} \right\rangle$ holds for any $1 \leq e \leq n$ by Lemma 3. As $\deg(f) \geq s-1 \geq n-(e+n-s)$ we have $\mathrm{RM}(e,n)^{\overline{D}} \cap \left(\mathrm{RM}(e+n-s,n)^{\overline{D}}\right)^{\perp} = \{\mathbf{0}\}$ from Lemma 4.

Conversely, assume that for any $1 \leq e \leq n$ one has

$$\mathrm{RM}(e,n)^{\overline{D}} \cap \left(\mathrm{RM}(e+n-s,n)^{\overline{D}}\right)^{\perp} = \{\mathbf{0}\}.$$

Suppose the theorem were false. Then we could find a Boolean function $g \in AN^c(f) \setminus \{1\}$ such that $\deg(g) + \deg(gf) < s$. It follows that $\deg(gf) < n - (e+n-s) \leq \deg(f)$ and $g(1+f) \not\equiv 0$, where $e = \deg(g)$. Lemma 3 now implies that $\mathrm{RM}(e,n)^{\overline{D}} \cap \left(\mathrm{RM}(e+n-s,n)^{\overline{D}}\right)^{\perp}$ is included in $\left\langle \mathbf{1}_{wt(f)} \right\rangle$, a contradiction. This completes the proof. □

The following theorem gives a characterization of perfect algebraic immune functions using the LCD-ness of the punctured codes of Reed-Muller codes by deleting the coordinates outside the supports of the Boolean functions.

Theorem 3. *Let f be an n-variable nonzero Boolean function and let D be its support. Then f is a perfect algebraic immune function if and only if* $\mathrm{RM}(e,n)^{\overline{D}}$ *is an LCD code for any* $1 \leq e \leq n$.

Proof. Let f be a perfect algebraic immune function. The perfect algebraic immune function f has degree at least $n-1$ (see [36]). By Theorem 2 and $FAI(f) = n$, $\mathrm{RM}(e,n)^{\overline{D}}$ is LCD for any $1 \leq e \leq n$.

Conversely, suppose that $\mathrm{RM}(e,n)^{\overline{D}}$ is an LCD code for any $1 \leq e \leq n$. The desired conclusion then follows from Theorem 2 and Lemma 4. This completes the proof. □

The following corollary has been proved in [26] and we give an alternative proof of it based on coding theory.

Corollary 4. *Let f be an n-variable perfect algebraic immune function. Then $n = 2^\tau + 1$ when $wt(f)$ is even and $n = 2^\tau$ when $wt(f)$ is odd, where τ is a positive integer.*

Proof. Let f be a perfect algebraic immune function and let D be its support. Then $AI(f) \geq n/2$ by Corollary 1. Theorem 3 shows that $\mathrm{RM}(e,n)^{\overline{D}}$ is an LCD code for any $1 \leq e \leq (n-1)/2$. Combining Proposition 15 with Theorem 1 yields $\dim_{\mathbb{F}_2}\left(\mathrm{RM}(e,n)^{\overline{D}}\right) = \sum_{i=0}^{e}\binom{n}{i}$. Since $\mathbf{1}_{wt(f)}$ lies in $\mathrm{RM}(e,n)^{\overline{D}}$, $\left(\mathrm{RM}(e,n)^{\overline{D}}\right)^{\perp}$ is an even-like LCD code with dimension $wt(f) - \sum_{i=0}^{e}\binom{n}{i}$. We conclude from Proposition 3 that $wt(f) \equiv \sum_{i=0}^{e}\binom{n}{i} \pmod 2$ for any $1 \leq e \leq (n-1)/2$. This clearly forces

$$n \equiv wt(f) + 1 \pmod 2 \text{ and } \binom{n}{e} \equiv 0 \pmod 2, \tag{8}$$

where $2 \leq e \leq (n-1)/2$.

Let us first consider the case $wt(f) \equiv 0 \pmod 2$. Write $n = 2^\tau + \sum_{i=0}^{\tau-1} a_i 2^i$. We have $a_0 = 1$, because $n \equiv 1 \pmod 2$. If there existed an a_i such that $a_i = 1$ and $1 \leq i \leq \tau - 1$, we would have $2 \leq 2^i \leq (n-1)/2$ and $\binom{n}{2^i} \equiv 1 \pmod 2$ by Lucas' Theorem, contrary to (8). Hence $a_i = 0$ and $n = 2^\tau + 1$.

Similar arguments apply to the case $wt(f) \equiv 1 \pmod 2$. Then we have $n = 2^\tau$ in this case.This completes the proof. □

As a corollary of Proposition 15 and Theorem 3, we have the following, which provides a way of constructing LCD codes via perfect algebraic immune function.

Corollary 5. *Let f be an n-variable perfect algebraic immune function and let D be its support. Let e be an integer with $1 \leq e \leq (n-1)/2$. Then $\mathrm{RM}(e,n)^{\overline{D}}$ is an LCD code of dimension $\sum_{i=0}^{e}\binom{n}{i}$.*

Plugging all the families of perfect algebraic immune functions presented in [5] and [26] into Corollary 5 will produce a lot of binary LCD codes.

Corollary 6. *Let $n = 2^\tau$ or $2^\tau + 1$. Let D be a subset of $\mathbb{F}_{2^n}$ given by*

$$D = \begin{cases} \{\alpha^\ell, \alpha^{\ell+1}, \cdots, \alpha^{\ell+2^{\tau-1}-1}\}, & \text{if } n = 2^\tau + 1, \\ \{0, \alpha^\ell, \alpha^{\ell+1}, \cdots, \alpha^{\ell+2^{\tau-1}-1}\}, & \text{if } n = 2^\tau, \end{cases}$$

where α is a primitive element of $\mathbb{F}_{2^n}$ and ℓ is an integer. Then $\mathrm{RM}(e,n)^{\overline{D}}$ is an LCD code of dimension $\sum_{i=0}^{e}\binom{n}{i}$ for any $1 \leq e \leq (n-1)/2$.

6 Conclusions

In this paper, we investigated some problems on fast algebraic immunity of Boolean functions and LCD codes. More specifically, we pushed further the general study of the fast algebraic immunity and investigated its behavior in particular for certain families of Boolean functions. We have also introduced the related fast immunity profile and showed that the algebraic immunity and the fast algebraic immunity of a Boolean function can be expressed by means of its immunity profile. In addition, we provided new characterizations of perfect algebraic immune functions by means of the LCD-ness of punctured Reed-Muller codes. We also contributed to the current work on binary LCD codes (which are the most important codes regarding its applications in armoring implementations against side-channel attacks and fault non-invasive attacks) by constructing a large class of binary LCD codes from perfect algebraic immune functions. The results show a novel application of perfect algebraic immune functions in addition to their contribution in symmetric cryptography. This offers a new direction of research in this context.

References

1. F. Armknecht, C. Carlet, P. Gaborit, S. Kunzli, W. Meier, and O. Ruatta. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. Proceedings of EUROCRYPT 2006, Lecture Notes in Computer Science 4004 , pp. 147-164, 2006.
2. C. Carlet. Boolean functions for Cryptography and Error Correcting Codes", in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. L. Hammer, Eds, Cambridge University Press, pages 257-397, 2010.
3. C. Carlet. A Survey on Nonlinear Boolean Functions with Optimal Algebraic Immunity suitable for Stream Ciphers. Proceedings of the SMF-VMS conference, Hu?e, Vietnam, August 20-24, 2012. Special issue of the Vietnam Journal of Mathematics 41 (4), pp. 527-541, 2013.
4. C. Carlet. Boolean functions for cryptography and coding theory. To appear in Cambridge University Press.
5. C. Carlet, K. Feng. An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, good Immunity to Fast Algebraic Attacks and Good Nonlinearity. In: Advances in Cryptology-ASIACRYPT 2008, Heidelberg Springer, LNCS, vol. 5350, pages 425-440, 2008.
6. C. Carlet, S. Guilley. Complementary dual codes for counter-measures to side-channel attacks, In: E. R. Pinto et al. (eds.), Coding Theory and Applications, CIM Series in Mathematical Sciences, vol. 3, pp. 97-105, Springer Verlag, 2014 and Journal Adv. in Math. of Comm. 10(1), pp. 131-150, 2016.
7. C. Carlet, C. Li, S. Mesnager. Some (almost) optimally extendable linear codes. Des. Codes Cryptogr. 87(12), 2813-2834, 2019.
8. C. Carlet, S. Mesnager, C. Tang, Y. Qi. Euclidean and Hermitian LCD MDS codes. Designs, Codes and Cryptography, 86(11), 2605-2618, 2018.
9. C. Carlet, S. Mesnager, C. Tang, Y. Qi. On σ-LCD codes. IEEE Transactions on Information Theory, 65(3), 1694-1704, 2018.
10. C. Carlet, S. Mesnager, C. Tang, Y. Qi. New characterization and parametrization of LCD codes. IEEE Transactions on Information Theory, 65(1), 39-49, 2018.
11. C. Carlet, S. Mesnager, C. Tang , Y. Qi, R. Pellikaan .Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$. IEEE Trans. Inf. Theory **64**(4), 3010-301, 2018.
12. C. Carlet and D. Tang. Enhanced Boolean functions suitable for the filter model of pseudo-random generator. Designs, Codes and Cryptography 76 (3), pp. 571-587, 2015.

13. H. Chen, C. Ding, S. Mesnager and C. Tang. A novel application of Boolean functions with high algebraic immunity in minimal codes. CoRR abs/2004.04932, 2020.
14. N. Courtois. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. *Advances in cryptology–CRYPTO 2003, Lecture Notes in Computer Science* 2729, pp. 177-194, Springer, 2003.
15. N. Courtois and W. Meier. Algebraic Attacks on Stream Ciphers with Linear Feedback. *Advances in cryptology, Eurocrypt 2003, Lecture Notes in Computer Science* 2656, pp. 346-359, Springer, 2002.
16. Y. Du, B. Wei, F. Zhang and H. Zhang. On the (Fast) Algebraic Immunity of Boolean Power Functions/ Cryptology ePrint Archive, Report 2015/435, 2015.
17. Y. Du, F. Zhang F and M. Liu. On the Resistance of Boolean Functions against Fast Algebraic Attacks. In: ICISC 2011, Heidelberg Springer, 2012, LNCS, vol. 7259, pp. 261-274, 2012.
18. G. Gong. *Sequences, DFT and Resistance against Fast Algebraic Attacks*, pages 197–218. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.
19. K. Guenda, S. Jitman, T. A. Gulliver. Constructions of good entanglement-assisted quantum error correcting codes, Des. Codes Cryptogr. 86, 121-136, 2018.
20. S. Rønjom and T. Helleseth. A new attack on the filter generator. *IEEE Transactions on Information Theory*, 53 (5), pp.1752-1758, 2007.
21. W. C. Huffman, V. Pless. Fundamentals of Error-Correcting Codes. 2003.
22. T. Helleseth and S. Rønjom. Simplifying algebraic attacks with univariate analysis. Proceedings of *Information Theory and Applications Workshop*, ITA 2011, San Diego, California, USA, February 6-11, 2011, pp. 153-159, 2011.
23. L. Jin, C. Xing. Algebraic geometry codes with complementary duals exceed the asymptotic Gilbert-Varshamov bound. IEEE Transactions on Information Theory, 64(9), 6277-6282, 2017.
24. T. Kasami, S. Lin, W. Peterson. New generalizations of the Reed-Muller codes I: Primitive codes. IEEE Transactions on Information Theory, 14(2), 189-199, 1968.
25. M. Liu, D. Lin and D. Pei. Fast Algebraic Attacks and Decomposition of Symmetric Boolean Functions. *IEEE Transactions on Information Theory*, 57 (7), pp. 4817-4821, 2011.
26. M. Liu, Y. Zhang, and D. Lin. *Perfect Algebraic Immune Functions*, pp. 172-189. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.
27. C. Li, C. Ding, and S. Li, LCD cyclic codes over finite fields, IEEE Trans. Inf. Theory, vol. 63, no. 7, pp. 4344-4356, Jul. 2017.
28. S. Li, C. Li, C. Ding, and H. Liu, Two families of LCD BCH codes, IEEE Trans. Inf. Theory, vol. 63, no. 9, pp. 5699-5717, Sep. 2017.
29. F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes. Amsterdam, The Netherlands: North-Holland, 1986.
30. J. L. Massey. Linear codes with complementary duals, Discrete Math., vol. 106-107, pp. 337-342, 1992.
31. P. Méaux. *On the fast algebraic immunity of majority functions*, *LATINCRYPT 2019*, pp. 86-105, 2019.
32. P. Méaux. *On the fast algebraic immunity of threshold functions*, IACR Cryptology ePrint Archive 2020: 273, 2020.
33. W. Meier, E. Pasalic, and C. Carlet. Algebraic Attacks and Decomposition of Boolean Functions. In *Eurocrypt 2004*, ser. Lecture notes in Computer Science, Vol. 3027, pp. 474-491, Springer-Verlag, 2004.
34. S. Mesnager, and G. D. Cohen. Fast algebraic immunity of Boolean functions. Adv. in Math. of Comm. 11(2), pp. 373-377, 2017.

35. S. Mesnager, C. Tang, Y. Qi. Complementary dual algebraic geometry codes. IEEE Transactions on Information Theory, 64(4), 2390-2397, 2017.
36. E. Pasalic. Almost Fully Optimized Infinite Classes of Boolean Functions Resistant to (Fast) Algebraic Cryptanalysis. In: ICISC 2008, Heidelbergn Springer LNCS, vol. 5461, pages 399-414, 2008.
37. C. Shannon, *Communication theory of secrecy systems*. Bell system technical journal, Vol. 28, pp. 656-715,1949.
38. D. Tang. A note on the fast algebraic immunity and its consequences on modified majority functions. Journal *Advances in Mathematics of Communications*, 14(1), pp. 111-125, 2020.
39. Q. Wang and T. Johansson. *A note on fast algebraic attacks and higher order nonlinearities*. In *Inscrypt 2010*, LNCS 6584, pp. 404-414, 2011.
40. X-M. Zhang, J. Pieprzyk, and Y. Zheng. *On Algebraic Immunity and Annihilators*, ICISC, Lecture Notes in Computer Science, volume 4296, pp. 65-80. Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.
41. Z. Zhou, X. Li, C. Tang, C. Ding. Binary LCD codes and self-orthogonal codes from a generic construction. IEEE Transactions on Information Theory, 65(1), 16-27, 2018.