Cyclic codes and algebraic immunity of Boolean functions

Sihem Mesnager[13] and Gérard Cohen[23]
[1]Department of Mathematics, University of Paris VIII and University of Paris XIII
LAGA, UMR 7539, CNRS
[2]LTCI, UMR 5141, CNRS
[3]Telecom ParisTech, Paris, France
Email: smesnager@univ-paris8.fr,cohen@enst.fr

***Abstract*—Since 2003, algebraic attacks have received a lot of attention in the cryptography literature. In this context, algebraic immunity quantifies the resistance of a Boolean function to the standard algebraic attack of the pseudo-random generators using it as a nonlinear Boolean function. A high value of algebraic immunity is now an absolutely necessary cryptographic criterion for a resistance to algebraic attacks but is not sufficient, because of more general kinds of attacks so-called Fast Algebraic Attacks. In view of these attacks, the study of the set of annihilators of a Boolean function has become very important. We show that studying the annihilators of a Boolean function can be translated into studying the codewords of a linear code. We then explain how to exploit that connection to evaluate or estimate the algebraic immunity of a cryptographic function. Direct links between the theory of annihilators used in algebraic attacks and coding theory are established using an atypical univariate approach.**

***Keywords*—Linear codes, Cyclic codes, Boolean functions, Algebraic immunity, Annihilators.**

I. Introduction

Due to the great success of algebraic attacks [2], [3], the notion of algebraic immunity has been introduced to measure the ability of functions used as building blocks of key stream generators to resist this new kind of attacks. The algebraic immunity of a Boolean function is the smallest possible degree of nonzero Boolean functions that can annihilate the Boolean function or its complement (such a Boolean function is called an annihilator of the Boolean function; Definition 1). Usually, the annihilator of a Boolean function is described using a multivariate approach, i.e. one searches for a Boolean function g (in multivariate description) of low degree that annihilates f. For an n-variable Boolean function, its algebraic immunity is upper bounded by $\lceil \frac{n}{2} \rceil$ (see [3]). Several constructions of Boolean functions having high algebraic immunity have been proposed in the literature. Among these, the one due to Carlet and Feng [1] was obtained from the BCH bound from coding theory. That work motivates to push further the approach initiated in [1]. Indeed, it shows that it seems possible to translate the problem of studying the annihilators of a Boolean function into studying a linear code. Recently, using a univariate approach, Helleseth and Ronjom [7] have connected the problem of estimating algebraic immunity to determining low-weight codewords in certain cyclic codes. Interesting applications of their results can be found in [5]. In this paper, we use the univariate representation of a Boolean function. We present an alternative approach from a coding theory point of view to study the algebraic immunity of a Boolean function. As in [7], direct relations between the theory of annihilators of Boolean functions and coding theory are established. The paper is organized as follows. In Section II, we give some preliminaries. In Section III, we present our results. In particular, we associate annihilators of a Boolean function to codewords of a cyclic code (Definition 3). Next, we show that studying the annihilators of a Boolean function can be translated into studying the codewords of a linear code. We then prove that lower bounds on the algebraic immunity of a Boolean function can be derived from the minimal distance of that code (Theorem 2, Theorem 4). We also show that one can recover from that lower bound a key result of Carlet and Feng [1] leading to the construction of Boolean functions achieving the maximum value of the algebraic immunity in even dimension (Theorem 5).

II. Notation and preliminaries

Let n be a positive integer. A Boolean function f is a map from the vector space $\mathbb{F}_2^n$ of all binary vectors of length n to the finite field with two elements $\mathbb{F}_2$.

The *Hamming weight of a Boolean function* f on $\mathbb{F}_2^n$, denoted by $\mathrm{wt}(f)$, is the size of the support of the function, that is, the cardinality of $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$. The *Hamming distance* $d_H(f, g)$ between two functions f and g is the size of the set $\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}$, which is equal to $\mathrm{wt}(f \oplus {}^1 g)$.

In coding theory and cryptography, the most usual representation of these functions is the *algebraic Normal Form* (ANF) defined as

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

where the a_I's are in $\mathbb{F}_2$. The terms $\prod_{i \in I} x_i$ are called monomials. The *algebraic degree* of a Boolean function f

[1]We denote by $\oplus$ the addition in $\mathbb{F}_2$ (but we denote by $+$ the addition in the field $\mathbb{F}_{2^n}$ and in the vector space $\mathbb{F}_2^n$, since there will be no ambiguity) and by $+$ the addition in $\mathbb{Z}$.

equals the global degree of its (unique) ANF, that is, the maximum degree of those monomials whose coefficients are nonzero.

There is another common way to write down Boolean functions, that is, another representation using a finite field. To this end, we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$, the Galois field of characteristic 2 with 2^n elements. Another representation of Boolean functions using such an identification is to view any Boolean function as a polynomial in one variable over $\mathbb{F}_{2^n}$ of the form $f(x) = \sum_{j=0}^{2^n-1} a_j x^j$. This representation exists for every function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ and such function f is Boolean if and only if a_0 and a_{2^n-1} belong to $\mathbb{F}_2$ and $a_{2j} = a_j^2$ for every $j \neq 0$, $2^n - 1$, where $2j$ is taken modulo $2^n - 1$.

The *degree* of f is then equal to the maximum 2-weight of exponent j for which $a_j \neq 0$. Recall that the 2-weight $w_2(j)$ of an integer j is the number of 1's in its binary expansion.

Equation systems derived from stream ciphers are too difficult to solve directly. The criterion that any cipher should be highly nonlinear usually makes sure that the equations describing the encryption process look complex. Some ciphers (such as filter and combiner generators based on linear and nonlinear feedback shift registers) may be described by a single Boolean function with a time-variable input.

Because of standard algebraic attacks ([2], [3], [9]), the study of the set of *annihilators* of a Boolean function has become very important. An element of such sets is defined as follows.

Definition 1. Let f be a Boolean function defined over $\mathbb{F}_{2^n}$. A nonzero Boolean function p is called an annihilator of f if $f(x)p(x) = 0$ for every $x \in \mathbb{F}_{2^n}$.

The purpose of an annihilator is to reduce the number of variables in solving a multivariate nonlinear equation system. It has been highlighted that an important property of a Boolean function is the lowest possible degree of its annihilators or of the annihilators of its complement, that is called the *algebraic immunity*. In fact, the algebraic immunity consists on one way of measuring how hard it is to solve the equations describing some ciphers.

Definition 2. The algebraic immunity of f, denoted by $AI(f)$, is the minimum value of d such that f or its complement $1+f$ admits an annihilator of algebraic degree d. If we denote $\mathrm{LDA}(f)$ the lowest algebraic degree of nonzero annihilators of f, then $AI(f) = \min(\mathrm{LDA}(f), \mathrm{LDA}(1+f))$.

Clearly, the algebraic immunity of a Boolean function f is less than or equal to its algebraic degree since $1 \oplus f$ is an annihilator of f. As shown in [3], the algebraic immunity of any n-variable function is upper bounded by $\lceil n/2 \rceil$. Moreover, it was shown in [4] that the Hamming weight of a Boolean function f with given algebraic immunity satisfies : $\sum_{i=0}^{AI(f)-1} \binom{n}{i} \leq \mathrm{wt}(f) \leq \sum_{i=0}^{n-AI(f)} \binom{n}{i}$. In particular, if n is odd and f has optimum algebraic immunity then f is balanced.

Let us now recall the basic notation and facts about linear codes. A q-ary linear code of length n and dimension k is a linear subspace $\mathcal{C}$ with dimension k of the vector space $\mathbb{F}_q^n$, where $\mathbb{F}_q$ is the finite field with q elements. The Hamming weight (for short, weight) of a vector v is the number of its nonzero entries and is denoted $\mathrm{wt}(v)$. The Hamming distance $\mathrm{dist}(v, w)$ between two vectors v and w is the weight of $v+w$. The minimum distance of a linear code is the minimum Hamming distance between two of its vectors; its equals the minimum nonzero weight of its vectors. A linear code $\mathcal{C}$ is said to be cyclic if any cyclic shift of a vector belongs to $\mathcal{C}$, that is, whenever $(c_0, c_1, \cdots, c_{n-1})$ is in $\mathcal{C}$ then so is $(c_{n-1}, c_0, \cdots, c_{n-2})$.

III. Algebraic immunity from coding point of view

In [7], the authors have presented a direct connection between the annihilators used in algebraic attacks and the minimum distance of a specific 2^n-ary code. More precisely, they have proved the following main result.

Theorem 1. *([7]) Let $f(x)$ be a Boolean function (in univariate form). Then any annihilator of $f(x)$ belongs to the 2^n-ary cyclic code with generator polynomial $G_f(x)$ given by*

$$G_f(x) = gcd(f(x) + 1, x^{2^n-1} + 1).$$

The previous result shows that the annihilators of f belong to a 2^n-ary cyclic code with generator polynomial determined by f. A direct consequence of Theorem 1 is the following corollary related to the notion of algebraic immunity. More precisely, the next corollary shows that the problem of estimating the algebraic immunity is closely connected to determining low-weight height codewords in cyclic codes. The weight height of a polynomial p given by $p(x) = \sum_{i=0}^{2^n-2} a_i x^i$ is equal to $max\{wt(i) \mid a_i \neq 0\}$. Thus, the weight height is equal to the highest 2-weight of an i where the coefficient a_i is nonzero.

Corollary 1. *([7]) The algebraic immunity of a Boolean function function is equal to the minimal weight height of a codeword $g(x)$ in the cyclic codes generated by $gcd(f(x), x^{2^n-1} + 1)$ and $gcd(f(x) + 1, x^{2^n-1} + 1)$ where $g(x)^2 \equiv g(x) \pmod{x^{2^n-1} + 1}$ and the weight height of a polynomial $p(x) = \sum_{i=0}^{2^n-2} c_i x^i$ denoted by $wh(p)$ is defined as $wh(p) = max\{wt(i) \mid c_i \neq 0\}$.*

In the following, we adopt a different univariate approach from a coding point of view for evaluating or estimating the algebraic immunity of a cryptographic function. To this end, we provide a new connection between the annihilators and some cyclic codes.

In this section, given a subset S of $\mathbb{F}_{2^n}$, we shall denote by $S^\star$ the subset $S \setminus \{0\}$. Let f be a Boolean function on $\mathbb{F}_{2^n}$ and $p : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be an annihilator of f (see Definition 1). One can represent p as a polynomial in one variable over $\mathbb{F}_{2^n}$: $p(x) = \sum_{i=0}^{2^n-1} a_i x^i$. We now introduce two linear codes over $\mathbb{F}_{2^n}$.

Definition 3. Given a subset S of $\mathbb{F}_{2^n}$, let $\mathcal{C}(S)$ be the set of all tuples $(a_0, a_1, a_2, \cdots, a_{2^n-2}, a_{2^n-1})$ of $\mathbb{F}_{2^n}^{2^n}$ such that $\sum_{i=0}^{2^n-1} a_i x^i = 0$ for every $x \in S$. Let $\overline{\mathcal{C}}(S)$ be the set

of all tuples $(a_1, a_2, \cdots, a_{2^n-2}, a_{2^n-1})$ of $\mathbb{F}_{2^n}^{2^n-1}$ such that $\sum_{i=1}^{2^n-1} a_i x^i = 0$ for every $x \in S$.

Lemma 1. *Let $S \subset \mathbb{F}_{2^n}$. Then $\mathcal{C}(S)$ is a linear code of length 2^n and $\overline{\mathcal{C}}(S)$ is a cyclic code of length $2^n - 1$.*

Proof: The linearity of the codes simply comes from the fact that the common zeros of two polynomials are zeros of their sum. Suppose now that $p(x) = \sum_{i=1}^{2^n-1} a_i x^i$ vanishes on S, that is, $p(x) = 0$ for every $x \in S$. Note now that $xp(x) = \sum_{i=1}^{2^n-1} a_i x^{i+1} = \sum_{i=2}^{2^n-1} a_{i-1} x^i + a_{2^n-1} x^{2^n} = a_{2^n-1} x + \sum_{i=2}^{2^n-1} a_{i-1} x^i = 0$ for every $x \in S$, that is, $(a_{2^n-1}, a_1, \cdots, a_{2^n-2})$ is a codeword of $\overline{\mathcal{C}}(S)$ proving that it is a cyclic code. ∎

Clearly, $(a_0, a_1, \ldots, a_{2^n-1})$ is a codeword of $\mathcal{C}(\mathrm{supp}(f))$. Conversely, one has to take care that not all the codewords of $\mathcal{C}(\mathrm{supp}(f))$ can be associated to an annihilator of f. Indeed, $\sum_{i=0}^{2^n-1} a_i x^i$ has to be the representation of a Boolean function, that is, one must have that a_0, a_{2^n-1} are in $\mathbb{F}_2$ and $a_{2i \mod 2^n-1} = a_i^2$ for every $i \in \{1, \ldots, 2^n - 2\}$.

Let us denote $\mathcal{B}$ the set of all vectors $(a_0, a_1, \cdots, a_{2^n-2}, a_{2^n-1}) \in \mathbb{F}_2 \times \mathbb{F}_{2^n}^{2^n-2} \times \mathbb{F}_2$ such that $a_{2i \mod 2^n-1} = a_i^2$ for every integer i ranging from 1 to $2^n - 2$. Note that $\mathcal{C}(\mathrm{supp}(f)) \cap \mathcal{B}$ is a linear sub-code of $\mathcal{C}(\mathrm{supp}(f))$. By the above we have

Lemma 2. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Then the map which associates to each codeword $(a_0, a_1, \cdots, a_{2^n-1})$ the polynomial $\sum_{i=0}^{2^n-1} a_i x^i$ is a linear isomorphism from $\mathcal{C}(\mathrm{supp}(f)) \cap \mathcal{B}$ to the set of annihilators of f.*

We now show the link between $\mathcal{C}(\mathrm{supp}(f))$ and $\overline{\mathcal{C}}(\mathrm{supp}(f)^\star)$ when $f(0) = 1$.

Lemma 3. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Suppose $f(0) = 1$. Then $\mathcal{C}(\mathrm{supp}(f)) = \{0\} \times \overline{\mathcal{C}}(\mathrm{supp}(f)^\star)$.*

Proof: Note first that $\mathcal{C}(\mathrm{supp}(f)) \supset \{0\} \times \overline{\mathcal{C}}(\mathrm{supp}(f)^\star)$. It remains therefore to prove the converse inclusion. Let $(a_0, a_1, \ldots, a_{2^n-1})$ be a codeword of $\mathcal{C}(\mathrm{supp}(f))$. One has $\sum_{i=0}^{2^n-1} a_i x^i = 0$ for every $x \in \mathrm{supp}(f)$. This implies that $a_0 = 0$ since $0 \in \mathrm{supp}(f)$. Therefore, we have that $\sum_{i=1}^{2^n-1} a_i x^i = 0$ for every $x \in \mathrm{supp}(f)^\star$ yielding that $(a_0, a_1, a_2, \ldots, a_{2^n-1})$ is a codeword of $\{0\} \times \overline{\mathcal{C}}(\mathrm{supp}(f)^\star)$. ∎

A quite natural question is then what happens when $f(0) = 0$. To this end, note that, for every element $(1, a_1, \ldots, a_{2^n-1})$ of $\mathcal{C}(S)$, we have $\sum_{i=1}^{2^n-1} a_i x^i = 1$ for every $x \in S$.

Lemma 4. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Suppose $f(0) = 0$. Let $(c_1, \ldots, c_{2^n-1})$ be any element of $\mathbb{F}_{2^{2^n}}^{2^n-1}$ such that $\sum_{i=1}^{2^n-1} c_i x^i = 1$ for every $x \in S$. Set $c = (c_1, \ldots, c_{2^n-1}) \in \mathbb{F}_{2^{2^n}}^{2^n-1}$. Then*

$$\mathcal{C}(\mathrm{supp}(f)) = \{0\} \times \overline{\mathcal{C}}(\mathrm{supp}(f)) \cup \{1\} \times \{c + a, a \in \overline{\mathcal{C}}(\mathrm{supp}(f))\}.$$

Proof: Let $a = (a_0, a_1, \ldots, a_{2^n-1})$ be a codeword of $\mathcal{C}(\mathrm{supp}(f)$.

- Suppose that $a_0 = 0$. Then $\sum_{i=1}^{2^n-1} a_i x^i = 0$ for every $x \in \mathrm{supp}(f)$, that is, $(a_1, \ldots, a_{2^n-1}) \in \overline{\mathcal{C}}(\mathrm{supp}(f))$.
- Suppose that $a_0 = 1$. Then, $\sum_{i=1}^{2^n-1} a_i x^i = 1$ for every $x \in \mathrm{supp}(f)$ which is equivalent to say that $\sum_{i=1}^{2^n-1} (a_i + c_i) x^i = 0$ for every $x \in \mathrm{supp}(f)$, that is, $(a_1, \ldots, a_{2^n-1}) + (c_1, \ldots, c_{2^n-1})$ is in $\overline{\mathcal{C}}(\mathrm{supp}(f))$.

∎

Let us now state the following result about the algebraic immunity deduced from the analysis of the code $\mathcal{C}(\mathrm{supp}(f))$.

Theorem 2. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Let δ be the minimum distance of $\mathcal{C}(\mathrm{supp}(f))$. Let d be a positive integer such that $\sum_{i=0}^{d} \binom{n}{i} < \delta$. Then there is no nonzero annihilator of f of algebraic degree less than or equal to d, that is, any annihilator of f is of algebraic degree at least $d + 1$.*

Proof: Any annihilator p can be represented as $p(x) = \sum_{i=0}^{2^n-1} a_i x^i$. Suppose that p is an annihilator of algebraic degree at most d, that is, $a_i = 0$ for every i of 2-weight greater than d. It is associated to a codeword $c = (a_0, \cdots, a_{2^n-2}, a_{2^n-1})$ of $\mathcal{C}(\mathrm{supp}(f))$ where $a_i = 0$ for every i such that $w_2(i) \geq d + 1$. Therefore, c has at most $\sum_{i=0}^{d} \binom{n}{i}$ nonzero components, that is, the weight of c is less than δ. It implies that c is the null codeword proving thus that f has no nonzero annihilator of algebraic degree less than or equal to d. ∎

The preceding theorem leads thus to a lower bound for $\mathrm{LDA}(f)$.

Corollary 2. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Let δ be the minimum distance of $\mathcal{C}(\mathrm{supp}(f))$. Let e be the lowest positive integer such that $\sum_{i=0}^{e} \binom{n}{i} \geq \delta$. Then $\mathrm{LDA}(f) \geq e$.*

Proof: It holds that $\sum_{i=0}^{e-1} \binom{n}{i} < \delta \leq \sum_{i=0}^{e} \binom{n}{i}$. Then, according to Theorem 2, the algebraic degree of a nonzero annihilator f is at least e. ∎

We are now going to consider a particular case. Let α be a primitive element of $\mathbb{F}_{2^n}$. Let l and t be two nonnegative integers. Denote then $V(\alpha; l; t) = \{\alpha^l, \alpha^{l+1}, \cdots, \alpha^{l+t-1}\}$. Let us now recall a classical result about the minimum distance of cyclic codes (Bose-Ray Chaudhuri-Hocquenghem, [8, Theorem 8]).

Theorem 3. *([8]) Let α be a primitive element of $\mathbb{F}_{2^n}$. Let r be a nonnegative integer and t a positive integer greater or equals 2. Let $\mathcal{C} \subset \mathbb{F}_{2^n}$ be a cyclic code having t consecutive zeros α^r, α^{r+1}, $\cdots$, α^{r+t-1}. Then the minimum distance of $\mathcal{C}$ greater than t.*

Theorem 3 is usually called the BCH bound. Now, using the previous notation, one can prove the following result.

Theorem 4. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Let l be a nonnegative integer and δ be a positive integer. Suppose that $\mathrm{supp}(f) \supset V(\alpha; l; t-1)$ with $t \geq 2$. Then $\mathrm{LDA}(f) \geq e$ where e is the lowest possible integer such $\sum_{i=0}^{e} \binom{n}{i} \geq t - 1$.*

Proof: Note that $\mathcal{C}(\mathrm{supp}(f))$ contains $\{0\} \times \overline{\mathcal{C}}(\mathrm{supp}(f)^\star)$. Now, $\overline{\mathcal{C}}(\mathrm{supp}(f)^\star)$ is a cyclic code having $t - 1$ consecutive zeros. According to Theorem 3, the minimum distance of $\overline{\mathcal{C}}(\mathrm{supp}(f)^\star)$ is greater than $t - 1$.

Let us now establish a lower bound on the minimum distance δ' of $\mathcal{C}(\mathrm{supp}(f))$ involving the minimum distance δ

of $\overline{\mathcal{C}}(\mathrm{supp}(f)^\star)$. If $f(0)=1$ then, according to Theorem 3, we have $\delta'=\delta$. Let us now consider the case where $f(0)=0$. By definition, $\delta'=\min_{a,a'\in\mathcal{C}(\mathrm{supp}(f)),a\neq a'}\mathrm{dist}(a,a')$. Theorem 4 show that $\mathcal{C}(\mathrm{supp}(f))$ can be decomposed as $\mathcal{C}(\mathrm{supp}(f))=\{0\}\times\overline{\mathcal{C}}(\mathrm{supp}(f))\cup\{1\}\times\{c+a,a\in\overline{\mathcal{C}}(\mathrm{supp}(f))\}$ where $c\in\mathcal{S}=\{(c_1,\ldots,c_{2^n-1})\in\mathbb{F}_{2^{2^n}}^{2^n}\mid\sum_{i=1}^{2^n-1}c_ix^i=1 \text{ for every } x\in\mathrm{supp}(f)\}$. Now,

- suppose that $a=(0,a_1,\ldots,a_{2^n-1})$ and $a'=(0,a'_1,\ldots,a'_{2^n-1})\neq a$ are in $\{0\}\times\overline{\mathcal{C}}(\mathrm{supp}(f))$, then $\mathrm{dist}(a,a')=\mathrm{wt}(a+a')=\mathrm{wt}((a_1+a'_1,\ldots,a_{2^n-1}+a'_{2^n-1}))\geq\delta$.
- suppose that $a=(1,a_1,\ldots,a_{2^n-1})$ and $a'=(1,a'_1,\ldots,a'_{2^n-1})\neq a$ with $c+(a_1,\ldots,a_{2^n-1})$ and $c+(a'_1,\ldots,a'_{2^n-1})$ belonging to $c+\overline{\mathcal{C}}(\mathrm{supp}(f))$, then $\mathrm{dist}(a,a')=\mathrm{wt}((a_1+a'_1,\ldots,a_{2^n-1}+a'_{2^n-1}))\geq\delta$.
- suppose that $a=(0,a_1,\ldots,a_{2^n-1})\in\{0\}\times\overline{\mathcal{C}}(\mathrm{supp}(f))$ and $a'=(1,a'_1,\ldots,a'_{2^n-1})$ with $c+(a'_1,\ldots,a'_{2^n-1})$ belonging to $c+\overline{\mathcal{C}}(\mathrm{supp}(f))$. Then $\mathrm{dist}(a,a')=1+wt((a_1+a'_1+c_1,\ldots,a_{2^n-1}+a'_{2^n-1}+c_{2^n-1}))$. Note then that $(a_1+a'_1+c_1,\ldots,a_{2^n-1}+a'_{2^n-1}+c_{2^n-1})\in\mathcal{S}$ since $\sum_{i=1}^{2^n-1}(a_i+a'_i+c_i)x^i=1$ for every $x\in\mathrm{supp}(f)$. Let us now study the Hamming weights of the elements of $\mathcal{S}$. To this end, note that, since $0\notin\mathrm{supp}(f)$, we have, for every $c\in\mathcal{S}$, $\sum_{i=1}^{2^n-1}c_ix^i=1,\forall x\in\mathrm{supp}(f)$ if and only if, $x\sum_{i=1}^{2^n-1}c_ix^i=x,\forall x\in\mathrm{supp}(f)$ if and only if, $(c_{2^n-1}+1)x+\sum_{i=2}^{2^n-1}c_{i-1}x^i=0,\forall x\in\mathrm{supp}(f)$ that is, $(c_{2^n-1}+1,c_1,\ldots,c_{2^n-2})\in\overline{\mathcal{C}}(\mathrm{supp}(f))$. Then $\mathrm{wt}(c)\geq\mathrm{wt}((c_{2^n-1}+1,c_1,\ldots,c_{2^n-2}))-1\geq\delta-1$.

That implies that $\delta'\geq\delta-1$ yielding that $\delta'\geq t-1$. One then concludes by Theorem 2. ∎

When $\mathrm{supp}(f)=V(\alpha;0;2^{n-1}-1)=\{1,\alpha,\cdots,\alpha^{2^n-2}\}$, it is proved in [1] that the algebraic immunity of f is optimal, that is, $AI(f)=\lceil\frac{n}{2}\rceil$. We now prove than one can recover that result from Theorem 4 when n is even.

Theorem 5. *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$. Let n be an even integer greater than 2. Suppose that $\mathrm{supp}(f)=V(\alpha;0;2^{n-1}-1)=\{1,\alpha,\cdots,\alpha^{2^n-2}\}$ where α is a primitive element of $\mathbb{F}_{2^n}$. Then $AI(f)=\frac{n}{2}$.*

Proof: Theorem 4 states that $\mathrm{LDA}(f)\geq e$ where e is the lowest possible integer such that $\sum_{i=0}^{e}\binom{n}{i}\geq 2^{n-1}-2$. Now, note that $\sum_{i=0}^{\frac{n}{2}}\binom{n}{i}\geq 2^{n-1}-2>\sum_{i=0}^{\frac{n}{2}-1}\binom{n}{i}$ for every even positive integer $n\geq 4$. We then deduce from Theorem 4 that $\mathrm{LDA}(f)\geq\frac{n}{2}$ when n is even and greater than 2. Now $\mathrm{supp}(1+f)=\{0,\alpha^{2^n-1},\cdots,\alpha^{2^n-2}\}\supset V(\alpha;2^{n-1}-1;2^{n-1})$. Therefore, if we apply Theorem 4 again, we conclude than $\mathrm{LDA}(1+f)\geq e$ where e is the lowest possible integer such that $\sum_{i=0}^{e}\binom{n}{i}\geq 2^{n-1}-1$. If $n\geq 4$ is even, one has $\sum_{i=0}^{\frac{n}{2}}\binom{n}{i}\geq 2^{n-1}-1>\sum_{i=0}^{\frac{n}{2}-1}\binom{n}{i}$ and therefore $\mathrm{LDA}(1+f)\geq\frac{n}{2}$. We conclude that $AI(f)=\frac{n}{2}$. We hence recover the result of [1]. ∎

Remark 1. Let f be chosen as in Theorem 4 but with n odd greater than 1. Theorem 4 states that $\mathrm{LDA}(f)\geq e$ where e is the lowest possible integer such that $\sum_{i=0}^{e}\binom{n}{i}\geq 2^{n-1}-2$. Now, note that $\sum_{i=0}^{\lceil\frac{n}{2}\rceil-1}\binom{n}{i}\geq 2^{n-1}-2>\sum_{i=0}^{\lceil\frac{n}{2}\rceil-2}\binom{n}{i}$ for every odd integer $n\geq 3$. We can then deduce from Theorem 4 that $\mathrm{LDA}(f)\geq\lceil\frac{n}{2}\rceil-1$. Now, let us turn our attention on $1+f$. If we apply Theorem 4 again, we conclude than $\mathrm{LDA}(1+f)\geq e$ where e is the lowest possible integer such that $\sum_{i=0}^{e}\binom{n}{i}\geq 2^{n-1}-1$. When n is odd integer greater than 1, we have that $\sum_{i=0}^{\lceil\frac{n}{2}\rceil-1}\binom{n}{i}\geq 2^{n-1}-1>\sum_{i=0}^{\lceil\frac{n}{2}\rceil-2}\binom{n}{i}$. Thus, $\mathrm{LDA}(1+f)\geq\lceil\frac{n}{2}\rceil-1$ if n is odd proving that $AI(f)\geq\lceil\frac{n}{2}\rceil-1$ in that case.

IV. Conclusion

As in [7], direct links between the theory of annihilators used in algebraic attacks and coding theory are established in this paper using an atypical univariate approach. We firstly provide a new connection between the annihilators and some cyclic codes. We explain how to translate the study of the algebraic immunity of a Boolean function into studying the properties of particular cyclic codes. We show that, from the knowledge of the minimum distance of those cyclic codes, lower bounds can be derived on the algebraic immunity of the associated Boolean functions. The results presented in this paper highlight that it could be an alternative way for studying the algebraic immunity of Boolean functions. The new connections given in the paper can give new Boolean functions with good algebraic immunity by selecting Boolean functions in univariate representation such that the corresponding cyclic codes have good distance properties. Moreover, it should be possible to make use of some well-known linear codes to construct Boolean functions with good algebraic immunity.

References

[1] C. Carlet and K. Feng, "An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," in *ASIACRYPT, Lecture Notes in Computer Science, volume 5350. Springer-Verlag*, pp. 425–440, 2008.

[2] N. Courtois, "Higher order correlation attacks, XL algorithm, and Cryptanalysis of Toyocrypt," in *Information Security and Cryptology (ICISC 2002), Lecture Notes in Computer Science, volume 2587 Springer-Verlag*, pp. 182–199, 2003.

[3] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback", proceedings of *EUROCRYPT 2003, LNCS 2656, Springer*, pp. 345-359, 2003. An extended version is available at http ://www.cryptosystem.net/stream/

[4] D. K. Dalai, K. C. Gupta, and S. Maitra, "Notion of algebraic immunity and its evaluation related to fast algebraic attacks," in *International Workshop on Boolean Functions : Cryptography and Applications*, pp. 13–15, 2006.

[5] G. Gong, S. Ronjom and T. Helleseth and H. Honggang "Fast Discrete Fourier Spectra Attacks on Stream Ciphers," in *IEEE Transactions on Information Theory 57(8)*, pp. 5555–5565, 2011.

[6] C. Hartmann and K. Tzeng, "Generalizations of the BCH bound," *Inform. and Control*, volume 20, pp. 489–498, 1972.

[7] T. Helleseth and S. Ronjom "Simplifying Algebraic Attacks with Univariate Analysis," in *Proceedings of Information Theory and Applications Workshop (ITA)*, pp. 1–7, 2011.

[8] F. J. MacWilliams and N. J. Sloane, "The theory of error-correcting codes", *Amsterdam, North Holland*, 1977.

[9] W. Meier, E. Pasalic, and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," in *EUROCRYPT, Lecture Notes in Computer Science, volume 3027. Springer-Verlag*, pp. 474–491, 2004.

[10] K. Tzeng and C. Hartmann, "On the minimum distance of certain reversible cyclic codes," *IEEE Trans. Inform. Theory*, volume 16, pp. 644–646, 1970.

[11] B. Wu and J. Zheng, "A remark on algebraic immunity of Boolean functions", *CoRR*, vol. abs/1305.5919, 2013.

[12] X.M. Zhang, J. Pieprzyk, Y . Zheng, "On algebraic immunity and annihilators," *ICISC, Lecture Notes in Computer Science, volume 4296. Springer-Verlag*, pp. 65–80, 2006.