21st International Symposium on
Mathematical Theory of Networks and Systems
July 7-11, 2014. Groningen, The Netherlands

A note on linear codes and algebraic immunity of Boolean functions

Sihem Mesnager[1*]

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 a more general kind 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.

keywords: Boolean functions, Algebraic immunity, Cyclic code.

1. Introduction

Due to the great success of algebraic attacks [1, 2], the notion of algebraic immunity has been introduced in [3] to measure the ability of functions used as building blocks of key stream generators resisting 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). For an n-variable Boolean function, its algebraic immunity is upper bounded by $\lceil \frac{n}{2} \rceil$ (see [2]). Several constructions of Boolean functions having high algebraic immunity have been proposed in the literature. Among these constructions, the one due to Carlet and Feng [4] was obtained from the BCH bound from coding theory. That work motivates to push further the approach initiated in [4]. Indeed, it shows that is seems possible to translate the problem of studying the annihilators of a Boolean function into studying a linear code. In section 3, we associate annihilators of a Boolean function to codewords of a cyclic code (Definition 3). We then show that a lower bound on the algebraic immunity of a Boolean function can be derived from the minimal distance of that code (Theorem 15).

2. 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) :

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

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 equals the global degree of its

*[1] Department of Mathematics, University of Paris VIII, LAGA (Laboratoire Analyse, Géometrie et Applications), UMR 7539, CNRS, University of Paris XIII. *E-mail: smesnager@univ-paris8.fr*

[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 $\mathbb{Z}$.

ISBN: 978-90-367-6321-9

(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 equals by definition the number of 1's in its binary expansion.

Because of standard algebraic attacks [5], the study of the set of annihilators of a Boolean function has become very important. We now recall the definition of an annihilator of a Boolean function.

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 $x\in\mathbb{F}_{2^n}$.*

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 of f [5].

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, the algebraic immunity of f can be written as: $AI(f)=\min(\mathrm{LDA}(f),\mathrm{LDA}(1+f))$.*

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 [6], the algebraic immunity of any n-variable function is bounded by $\lceil n/2\rceil$. Moreover, it was shown in [7] 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 linear code of length n is a vector subspace of $\mathbb{F}_{2^n}$. 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 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 vectors of the linear code; it equals the minimum nonzero weight among all the vectors of the code. 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 $(c_{n-1},c_0,\cdots,c_{n-2})$.

3. Algebraic immunity from coding point of view

Let $p:\mathbb{F}_{2^n}\to\mathbb{F}_2$ be an annihilator of a Boolean function f defined over $\mathbb{F}_{2^n}$. One can represent p as a polynomial in one variable over $\mathbb{F}_{2^n}$: $p(x)=\sum_{i=0}^{2^n-1}a_i x^i$. Introduce now the linear code 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 $(a_1,a_2,\cdots,a_{2^n-2},a_{2^n-1})$ 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 4 *Let $S\subset\mathbb{F}_{2^n}$. Then $\mathcal{C}(S)$ is a cyclic code of length 2^n-1.*

The linearity of the code simply comes from the fact that the common zeros of two polynomials are also 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 $xp(x)=\sum_{i=1}^{2^n-1}a_i x^{i+1}=\sum_{i=2}^{2^n-1}a_{i-1}x^i+a_{2^n-1}x^{2^n}=a_{2^n-1}x+\sum_{i=2}^{2^n-1}a_{i-1}x^i$, that is, $(a_{2^n-1},a_1,\cdots,a_{2^n-2})$ is a codeword of $\mathcal{C}(S)$ proving that it is a cyclic code.

A Boolean function p is an annihilator of f according to Definition 1 if and only if $p(x)=0$ for every $x\in\mathrm{supp}(f)$. Let us write $p(x)=\sum_{i=0}^{2^n-1}a_i x^i$. If $f(0)=1$, then $a_0=0$, that is, there is no constant term in the representation of p : $p(x)=\sum_{i=1}^{2^n-1}a_i x^i$. If $f(0)=1$, then $(a_1,\ldots,a_{2^n-1})$ 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, to be an annihilator, $\sum_{i=1}^{2^n-1}a_i x^i$ must be the representation of a Boolean function, that is, one must have that $a_{2i}=a_i^2$ for every $i\neq 2^n-1$. The authors of [4] have neglected in their approach the fact that codewords of $\mathcal{C}(\mathrm{supp}(f))$ are not necessarily associated to annihilators. Let us denote $\mathcal{B}$ the set of all vectors $(a_1,\cdots,a_{2^n-2},a_{2^n-1})\in\mathbb{F}_{2^n}^{2^n-2}\times\mathbb{F}_2$ such that

$a_{2i \mod 2^n-1} = a_i$ for every integer i ranging from 1 to 2^n-2. Therefore, one has more precisely

Lemma 5 *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$ be such that $f(0)=1$. Then the set of annihilators of f is the intersection of $\mathcal{C}(\mathrm{supp}(f))\cap\mathcal{B}$. It is a linear sub-code of $\mathcal{C}(\mathrm{supp}(f))$.*

It is a linear code because $\mathcal{B}$ and $\mathcal{C}(\mathrm{supp}(f))$ are linear codes.

The question then arises from knowing what we could say when $f(0)=0$. To that effect we prove the following result that shows that the algebraic immunities of two Boolean functions differ of at most 1 if they differ only at 0 (note that a similar result can be obtain from [11]).

Proposition 6 *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$. Let $\epsilon\in\mathbb{F}_2$. Let f^ϵ be the Boolean function defined as $f^\epsilon(0)=\epsilon$ and $f^\epsilon(x)=f(x)$ for every $x\in\mathbb{F}_{2^n}^\star$. Then, it holds*

$$\mathrm{LDA}(f)-1\le\mathrm{LDA}(f^\epsilon)\le\mathrm{LDA}(f)+1$$

and

$$\mathrm{LDA}(1+f)-1\le\mathrm{LDA}(1+f^\epsilon)\le\mathrm{LDA}(1+f)+1$$

Let p be an annihilator of f of algebraic degree $\mathrm{LDA}(f)$. Clearly, $xp(x)f^\epsilon(x)=0$ for every $x\in\mathbb{F}_{2^n}$ proving that $\mathrm{LDA}(f^\epsilon)\le\mathrm{LDA}(f)+1$. Similarly, exchanging f and f^ϵ, one can prove $\mathrm{LDA}(f)\le\mathrm{LDA}(f^\epsilon)+1$, that is, $\mathrm{LDA}(f^\epsilon)\ge\mathrm{LDA}(f)-1$.

Let p be an annihilator of $1+f$ of algebraic degree $\mathrm{LDA}(1+f)$. Note that than $1+f^\epsilon(x)=f(x)+(1+f(0)+\epsilon)(1+x^{2^n-1})+x^{2^n-1}=(1+f(x))+(f(0)+\epsilon)(1+x^{2^n-1})$ for every $x\in\mathbb{F}_{2^n}$. Therefore, $q(x)=xp(x)$ is an annihilator of $1+f^\epsilon$ since $x+x^{2^n}=0$ for every $x\in\mathbb{F}_{2^n}$. Hence $\mathrm{LDA}(1+f^\epsilon)\le\mathrm{LDA}(1+f)+1$. One can get by similar arguments $\mathrm{LDA}(1+f)\le\mathrm{LDA}(1+f^\epsilon)+1$, that is, $\mathrm{LDA}(f^\epsilon)\ge\mathrm{LDA}(f)-1$.

The following statement is an immediate corollary (see also [11]). The result follows from the definition of the algebraic immunity : $AI(f)=\min(\mathrm{LDA}(f),\mathrm{LDA}(1+f))$.

Corollary 7 *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$. Let $\epsilon\in\mathbb{F}_2$. Let f^ϵ be the Boolean function defined as $f^\epsilon(0)=\epsilon$ and $f^\epsilon(x)=f(x)$ for every $x\in\mathbb{F}_{2^n}^\star$. Then $AI(f)-1\le AI(f^\epsilon)\le AI(f)+1$.*

Set $S_f=\mathrm{supp}(f)\cap\mathbb{F}_{2^n}^\star$. Obviously, one has $\mathrm{supp}(f)=\{0\}\cup S_f$ if $f(0)=1$ while $\mathrm{supp}(f)=S_f$ if $f(0)=0$. Let us now state our first result about the algebraic immunity that we can deduce from the analysis of the code $\mathcal{C}(S_f)$.

Theorem 8 *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$ such that $f(0)=1$. Let δ be the minimum distance of $\mathcal{C}(S_f)$. Let d be a positive integer such that $\sum_{i=1}^d\binom{n}{i}<\delta$. Then there is no nonzero annihilator of f of algebraic degree at most d.*

Note first that any annihilator p of f vanishes at 0 since $f(0)=1$ and therefore can be represented as $p(x)=\sum_{i=1}^{2^n-1}a_ix^i$. 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 $c=(a_1,\cdot,a_{2^n-2},a_{2^n-1})$ of $\mathcal{C}(S_f)$ where $a_i=0$ for every i such that $w_2(i)\ge d+1$. Therefore, c has at most $\sum_{i=1}^d\binom{n}{i}$ 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 at most d.

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

Theorem 9 *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$ be such that $f(0)=1$. Let δ be the minimum distance of $\mathcal{C}(S_f)$. Let d be the lowest positive integer such that $\sum_{i=1}^d\binom{n}{i}\ge\delta$. Then $\mathrm{LDA}(f)\ge d$.*

Suppose that $\sum_{i=1}^e\binom{n}{i}<\delta$. Then, according to Theorem 8, f has no annihilator of algebraic degree at most e proving that $\mathrm{LDA}(f)\ge e+1$. Now, if d is the smallest possible positive integer such that $\sum_{i=1}^d\binom{n}{i}\ge\delta$. Then $\sum_{i=1}^{d-1}\binom{n}{i}<\delta$ and thus $\mathrm{LDA}(f)\ge d-1+1=d$.

In the case where a Boolean function vanishes at 0, one has

Theorem 10 *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$ such that $f(0)=0$. Let δ be the minimum distance of $\mathcal{C}(S_f)$. Let d be the lowest positive integer such that $\sum_{i=1}^d\binom{n}{i}\ge\delta$. Then $\mathrm{LDA}(f)\ge d-1$.*

Proposition 6 states that $\mathrm{LDA}(f)\ge\mathrm{LDA}(f^1)-1$ where $f^1:\mathbb{F}_{2^n}\to\mathbb{F}_2$ is the Boolean function taking the same values than f at every point of $\mathbb{F}_{2^n}^\star$ and equals 1 at 0. One then conclude thanks to Theorem 9 that $\mathrm{LDA}(f^1)\ge d$ from which one deduces the desired result.

Collecting together Theorem 9 and Theorem 10, we now prove that

Theorem 11 *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$. Let δ be the minimum distance of $\mathcal{C}(S_f)$ and δ' be the minimum distance of $\mathcal{C}(S_{1+f})$. Let d be the lowest positive integer such that $\sum_{i=1}^d\binom{n}{i}\ge\delta$ and d' be the lowest positive integer such that $\sum_{i=1}^{d'}\binom{n}{i}\ge\delta'$. Then $AI(f)\ge$*

$\min(d,d'-1)$ *if* $f(0)=1$ *or* $AI(f)\geq\min(d-1,d')$ *if* $f(0)=0$.

If $f(0)=1$, one gets the first lower bound on the algebraic immunity of f applying Theorem 9 to f and Theorem 10 to $1+f$. Similarly, if $f(0)=0$, one gets the second lower bound applying Theorem 10 to f and Theorem 9 to $1+f$.

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 $V(\alpha;l,t)=\{\alpha^l,\alpha^{l+1},\cdots,\alpha^{l+t-1}\}$. We then begin with studying the case where S_f equals $V(\alpha;l,t)$. To this end, let us recall a classical result about the minimum distance of cyclic codes (Bose-Ray Chaudhuri-Hocquenghem, [8, Theorem 8])

Theorem 12 *Let α be a primitive element of $\mathbb{F}_{2^n}$. Let r be nonnegative integer and t a positive integer. Let $\mathcal{C}\subset\mathbb{F}_{2^n}$ be a cyclic codes having t consecutive zeros α^r, α^{r+1}, $\cdots$, α^{r+t-1}. Then the minimum distance of δ is greater than t.*

Theorem 12 is usually called the BCH bound. Note now that, when $x\neq 0$,

$$\sum_{i=1}^{2^n-1}a_ix^i=x\sum_{i=1}^{2^n-1}a_ix^{i-1}=0$$
$$\iff\sum_{i=0}^{2^n-2}a_{i+1}x^i=0.$$

Hence, since S_f does not contains 0, for any codeword $c=(a_1,a_2,\cdots,a_{2^n-1})$, it holds $g(x)=\sum_{i=0}^{2^n-2}a_ix^i=0$ for every $x\in S_f$. That proves in particular that

Lemma 13 *Let $f:\mathbb{F}_2\to\mathbb{F}_2$. Every element of S_f is a zero of $\mathcal{C}(S_f)$.*

Theorem 14 *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$. Let l be a nonnegative integer and δ be a positive integer. Suppose that $S_f=V(\alpha;l,\delta-1)$. Then* $\mathrm{LDA}(f)\geq d-1$ *where d is the lowest possible integer such $\sum_{i=1}^{d}\binom{n}{i}\geq\delta+1$.*

$\mathcal{C}(S_f)$ has δ consecutive powers of a primitive element as zeros. Therefore, according the BCH bound recalled in Theorem 12, its minimum distance is at least $\delta+1$. We then conclude thanks to Theorem 9 and Theorem 10.

Now, since Theorem 14 relies only on the number of powers of α, one can show the following result with similar arguments as those exposed in the proof of Theorem 12.

Theorem 15 *Let f be defined as in Theorem 14. Then $AI(f)\geq d-1$ where d is the lowest integer such that*

$$\sum_{i=1}^{d}\binom{n}{i}\geq\min(\delta+1,2^n-\delta+2).$$

According to Theorem 12, one has to show a similar result for $\mathrm{LDA}(1+f)$. To this end, note that

$$\begin{aligned}S_{1+f}&=\{1,\cdots,\alpha^{l-1},\alpha^{l+\delta-1},\cdots,\alpha^{2^n-2}\}\\&=\{\alpha^{l+\delta-1},\cdots,\alpha^{2^n-2},\alpha^{2^n-1},\cdots,\alpha^{2^n+l-2}\}\\&=\{\alpha^{l+\delta-1},\cdots,\alpha^{l+\delta-1+(2^n-\delta)-1}\}.\end{aligned}$$

S_{1+f} contains therefore $2^n-\delta+1$ consecutive powers of a primitive element. The minimum distance of $\mathcal{C}(S_{1+f})$ is hence at least $2^n-\delta+2$ according to the BCH bound (Theorem 12). We then get that $\mathrm{LDA}(1+f)\geq d-1$ from Theorem 9 and Theorem 10. The result follows then from the definition of the algebraic immunity : $AI(f)=\min(\mathrm{LDA}(f),\mathrm{LDA}(1+f))$.

Remark 16 *Let r be any positive integer relatively prime with n and b be any nonnegative integer. Let f be a Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ such that $S_f=\{\alpha^b,\alpha^{b+2r},\cdots,\alpha^{b+(\delta-2)r}\}$. Set $\beta=\alpha^r$. Thus β is a primitive element of $\mathbb{F}_{2^n}$ since r and n are relatively prime. Furthermore, $\alpha^b=\beta^l$ for some positive integer l and thus $S_f=\{\beta^l,\beta^{l+2},\cdots,\beta^{l+\delta-2}\}=V(\beta;l,\delta-1)$. Then, according to Theorem 15, one can prove that $AI(f)\geq d-1$ where d is the smallest possible positive integer such that $\sum_{i=1}^{d}\binom{n}{i}\geq\min(\delta+1,2^n-\delta+2)$.*

We now state a first result that one can deduce from Theorem 15.

Theorem 17 *Let $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$. Suppose that $S_f=\{1,\alpha,\alpha^2,\cdots,\alpha^{2^{n-1}-2}\}$. Then $AI(f)\geq\lceil\frac{n}{2}\rceil-1$.*

Note that $S_f=V(\alpha;0;2^{n-1}-1)$. Set $\delta=2^{n-1}$. Thus $\min(\delta+1,2^n-\delta+2)=2^{n-1}+1$. Recall then that, for every positive integer n, one has

$$\sum_{i=1}^{\lceil\frac{n}{2}\rceil-1}\binom{n}{i}<2^{n-1}+1<\sum_{i=1}^{\lceil\frac{n}{2}\rceil}\binom{n}{i}.$$

We then conclude by Theorem 15 that $AI(f)\geq\lceil\frac{n}{2}\rceil-1$.

Remark 18 *In [4], it is indicated that the algebraic immunity of f is optimal, that is, equals $\lceil\frac{n}{2}\rceil$, when $f(0)=0$.*

Remark 19 *Theorem 17 can be obtained for other Boolean functions. Indeed, let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function such that $S_f = V(\alpha; l, \delta - 1)$. The key point in the proof is then that one must have*

$$\sum_{i=1}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i} < \min(\delta + 1, 2^n - \delta + 2) \leq \sum_{i=1}^{\lceil \frac{n}{2} \rceil} \binom{n}{i}.$$

Suppose $\min(\delta + 1, 2^n - \delta + 2) = \delta + 1$, *that is,* $\delta \leq 2^{n-1}$. *Let us now indicate that* $\sum_{i=1}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i} < 2^{n-1} + 1 < \sum_{i=1}^{\lceil \frac{n}{2} \rceil} \binom{n}{i}$ *for every positive integer* n. *Therefore, if we take any* δ *such that* $\sum_{i=1}^{\lceil \frac{n}{2} \rceil - 1} \binom{n}{i} < \delta + 1 \leq 2^{n-1} + 1$, *then* $AI(f) \geq \lceil \frac{n}{2} \rceil - 1$.

We now recall a generalization of Theorem 12 proved in [9, 10]

Theorem 20 *Let α be a primitive element of $\mathbb{F}_{2^n}$. Let r and k be nonnegative integers, t be a positive integer and m an positive integer relatively prime to n. Let $\mathcal{C} \subset \mathbb{F}_{2^n}$ be a cyclic code having α^r, α^{r+1}, $\cdots$, α^{r+t-1}, α^{r+m}, α^{r+m+1}, $\cdots$, $\alpha^{r+m+t-1}$, $\cdots$, $\alpha^{r+km+t-1}$. Then the minimum distance of $\mathcal{C}$ is greater than $t + k$.*

Therefore, one can deduce from Theorem 20 by a similar proof of that of Theorem 14.

Theorem 21 *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$. Let l and k be two positive integers. Let δ be a positive integer and let m be a positive integer relatively prime to n. Suppose that S_f contains $V(\alpha; l, \delta - 1) \cup V(\alpha; l + m, \delta - 1) \cup \cdots \cup V(\alpha; l + km, \delta - 1)$. Then* $\mathrm{LDA}(f) \geq d$ *where g is the smallest possible positive integer such that* $\sum_{i=1}^{d} \binom{n}{i} \geq \delta + k$.

Open problem 1 *Prove a lower bound for* $\mathrm{LDA}(1 + f)$ *where f is defined as in Theorem 21.*

4. Conclusion

In this paper, we explain how to translate the study of the algebraic immunity of a Boolean function into studying the properties of a particular cyclic code. We show that it can be derived from the knowledge of the minimum distance of those cyclic codes lower bounds 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.

References

[1] 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.

[2] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in Advances in cryptology- *Eurocrypt 2003, Lecture Notes in Computer Science, volume 2656, Springer-Verlag*, pp. 345–349, 2002.

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

[4] 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.

[5] 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.

[6] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," in *EUROCRYPT, Lecture Notes in Computer Science, volume 2656. Springer-Verlag*, pp. 345–359, 2003.

[7] 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.

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

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

[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] 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.