IMPROVING THE LOWER BOUND ON THE HIGHER ORDER NONLINEARITY OF BOOLEAN FUNCTIONS WITH PRESCRIBED ALGEBRAIC IMMUNITY

SIHEM MESNAGER

Abstract. The recent algebraic attacks have received a lot of attention in cryptographic literature. The algebraic immunity of a Boolean function quantifies its resistance to the standard algebraic attacks of the pseudo-random generators using it as a nonlinear filtering function. Very few relevant results have been found concerning its relation with the other cryptographic parameters especially with the standard nonlinearity or with the r-th order nonlinearity. As recalled by Carlet in his Crypto'06 paper, many papers have illustrated the importance of the rth-order nonlinearity profile (which includes the first-order nonlinearity). The role of this parameter relatively to the currently known attacks has been also shown for block ciphers. Recently, two lower bounds involving the algebraic immunity on the rth-order nonlinearity have been shown by Carlet and Carlet et al. None of them improves upon the other one in all situations. In this paper, we prove a new lower bound on the rth-order nonlinearity profile of Boolean functions, given their algebraic immunity, that improves significatively the previous lower bounds.

Keywords. stream cipher, block cipher, algebraic attack, Boolean function, algebraic immunity, algebraic degree, higher order nonlinearity, annihilator.

Introduction

The Boolean functions defined on the vector space $\mathbb{F}_2^n$ of binary vectors of a given length n are used in the pseudo-random generators of stream ciphers. The generation of the keystream consists, in many stream ciphers, of a linear part, producing a sequence with a large period, usually composed of one or several LFSR's, and a nonlinear combining or filtering function f which produces the output, given the state of the linear part. The most usual representation of an n-variable Boolean function f is called the *algebraic normal form*, that is, the representation of f as a multivariate polynomial over $\mathbb{F}_2$. This representation is unique and its degree, that we denote by $\deg(f)$, is called the *algebraic degree* of f.

Stream ciphers, which are very efficient, in particular in hardware, have been the objects of a lot of cryptanalyses; resist those attacks, different

Date: March 30, 2007.

Member of MAATICAH, Department of Mathematics, University of Paris 8. *email* : hachai@math.jussieur.fr.

design criteria have been proposed. One of the most basic requirements concerning a Boolean function f used in cryptosystems is to be of high algebraic degree.

Recently, a new kind of attacks drawn from an original idea of Shannon [13] have emerged that are called *algebraic attacks* [10]. They proceed by modelling the problem of recovering the secret key by means of an over-defined systems of multivariate nonlinear equations of algebraic degree $\deg(f)$. Those attacks can be used even if the algebraic degree of f is high. The core of those attacks is to find out low degree Boolean functions $g \neq 0$ and h such that $fg = h$. Meier, Pasalic and Carlet [11] have shown that it is equivalent to the existence of low degree *annihilators* of f, that is, of n-variable Boolean functions g such that $fg = 0$ or $(1 \oplus f)g = 0$. The minimum degree of such g is often called the *algebraic immunity* of f, that we denote it by $AI(f)$, and it must be as high as possible (the maximum being equal to the minimum between $\deg(f)$ and $\lceil \frac{n}{2} \rceil$). We know that having a high algebraic immunity is not only a necessary condition for a resistance to standard algebraic attacks but also for a resistance to fast algebraic attacks.

Very little is known about the relation between the algebraic immunity of a Boolean function and its other cryptographic parameters. The question of finding Boolean functions with a high algebraic immunity that are balanced remains open (*a fortiori* if we look forward a Boolean function with a high order of resiliency). Carlet introduced in [1] the notion of *nonlinearity profile* of Boolean functions, which is the sequence whose rth-order term, for r from r to $n-1$, equals the rth-order nonlinearity of the function that we denote by $nl_r(f)$ and that is, the minimum distance between f and all n-variable Boolean functions of algebraic degrees at most r. Several papers [4, 6, 7, 8, 12] have shown the role played by this parameter in relation to some cryptanalyses (note that, contrary to the (first order) nonlinearity, it must have low value for allowing the attacks to be realistic). Also, as explained in [1], the knowledge of lower and upper bounds on the rth-order nonlinearity simplifies the question of designing cryptographic Boolean function meeting all necessary criteria. The values of the nonlinearity profile are known for very few functions and these functions have little cryptographic interest.

A lower bound has been established on the (first-order) nonlinearity of a Boolean functions f with given algebraic immunity [9], and that we denote $nl(f)$ instead of nl_1. Lobanov [9] proved that $nl(f) \geq 2\sum_{i=0}^{AI(f)-2} \binom{n-1}{i}$ for every n-variable Boolean functions. Moreover, by constructing a family of Boolean function achieving the equality $nl(f) = 2\sum_{i=0}^{AI(f)-2} \binom{n-1}{i}$, he proved that this lower bound cannot be improved further . Lobanov's result has been extended to the rth-order nonlinearity $nl_r(f)$ of an n-variable Boolean function f in two different lower bounds [1, 2]. None of the two lower bounds improves upon the other one in all situations. Basically, those lower bounds say that the rth-order nonlinearity of an n-variable Boolean function is greater than or equal to $\max\left(\sum_{i=0}^{AI(f)-r-1} \binom{n}{i}, 2\sum_{i=0}^{AI(f)-r-1} \binom{n-r}{i}\right)$. In

this paper, we prove a lower bound that improves further the lower bound of [2] for all orders and the lower bound of [1] for the first orders (which are the most important from a practical point of view) : for every n-variable Boolean function f, we have $nl_r(f) \geq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i} + \sum_{i=AI(f)-2r}^{AI(f)-r-1} \binom{n-r}{i}$.

The paper is organized as follows. Firstly, we begin with fixing our main notation in Section 1. Secondly, we study in Section 2 the dimension of the annihilators with prescribed algebraic degrees of Boolean functions with given algebraic degrees. The results of this Section are crucial to obtain in Section 3 a new lower bound on the rth-order nonlinearity of a Boolean function of given algebraic immunity (Theorem 7).

1. Preliminaries

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 an application from $\mathbb{F}_2^n$ to $\mathbb{F}_2$) admits a unique *algebraic normal form*, that is, a representation as a multivariate polynomial over $\mathbb{F}_2$

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

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. A slightly different form for the algebraic normal form is $f(x) = \bigoplus_{u\in\mathbb{F}_2^n} a_u x^u$, where $a_u \in \mathbb{F}_2$ and where $x^u = \prod_{i=1}^n x_i^{u_i}$. Then $\deg(f)$ equals $\max_{a_u \neq 0} \mathrm{wt}(u)$, where $\mathrm{wt}(u)$ denotes the Hamming weight $|\{i = 1, \ldots, n \mid u_i = 1\}|$ of u. Given a positive integer r, we make an abuse of notation and denote by $\mathrm{RM}(r, n)$ the set of all n-variable Boolean functions of algebraic degrees at most r, that is, the so-called r-th order Reed-Muller code of length 2^n. We recall that $\mathrm{RM}(r, n)$ is a vector subspace over $\mathbb{F}_2$ of dimension $\sum_{i=0}^r \binom{n}{i}$.

The Hamming weight $\mathrm{wt}(f)$ of a Boolean function is the size of its support $\{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ that we denote by $\mathrm{supp}(f)$. The Hamming distance between two n-variable Boolean functions is the Hamming weight of $f \oplus g$, that is $\mathrm{dist}(f, g) = |\{x \in \mathbb{F}_2^n \mid f(x) \neq g(x)\}|$.

Definition 1 (rth-order nonlinearity)**.** Let f be an n-variable Boolean function. Let r be a positive integer such that $r \leq n$. The *r-th order nonlinearity* of f is the minimum Hamming distance between f and all n-variable Boolean functions from $\mathrm{RM}(r, n)$. We shall denote the r-th order nonlinearity of f by $nl_r(f)$.

The first-order nonlinearity of f is simply called the nonlinearity of f and is denoted by $nl(f)$. Clearly we have $nl_r(f) = 0$ if and only if f has degree at most r. So, the knowledge of the nonlinearity profile (i.e. of all the nonlinearities of orders $r \geq 1$) of a Boolean function includes the knowledge of its algebraic degree. It is in fact a much more complete cryptographic

parameter than are the single (first-order) nonlinearity and the algebraic degree. Very little is known on $nl_r(f)$. The best known upper bound on $nl_r(f)$ has asymptotic version [3] :

$$nl_r(f) \leq 2^{n-1} - \frac{\sqrt{15}}{2}(1+\sqrt{2})^{r-2}2^{\frac{n}{2}} + O(n^{r-2})$$

for every n-variable Boolean functions f.

The algebraic immunity [11] of a Boolean function f quantifies the resistance to the standard algebraic attack of the pseudo-random generators using it as a nonlinear function. It is defined as follows.

Definition 2 (Algebraic immunity)**.** Let f be an n-variable Boolean function. An n-variable Boolean function g is said to be an *annihilator* of f if the product $f \cdot g$ is null (that is, the support of g is included in the support of $1 \oplus f$). We denote by $An(g)$ the vector space of all annihilators of g The algebraic immunity of f is the minimum algebraic degree of all the nonzero annihilators of f or of $f \oplus 1$. The *algebraic immunity* of f, is denoted by $AI(f)$.

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 [10], we have $AI(f) \leq \lceil \frac{n}{2} \rceil$. It was shown in [5] 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.

2. Some results on the dimension of the vector space of prescribed degree annihilators of a Boolean function

An important parameter for evaluating the complexity of algebraic attacks on the systems using this function is the number of linearly independent low degree annihilators of a given Boolean function g and of the function $g \oplus 1$. We shall see in the next Section that it plays also an important role in relation to the r-th order nonlinearity.

Definition 3. Let g be a Boolean function and let k be a positive integer. We denote by $An_k(g)$ the vector space of those annihilators of degrees at most k of g and by $d_{k,g}$ the dimension of $An_k(g)$.

The dimension $d_{k,g}$ is an affine invariant, that is, we have $d_{k,g} = d_{k,g\circ A}$ for every affine automorphism A of $\mathbb{F}_2^n$ (this comes from the affine invariance of the algebraic degree and the fact that p is an annihilator of g if and only if $p \circ A$ is an annihilator of $g \circ A$). Little is known on the behavior of $d_{k,g}$. Carlet [1] proved the following upper bound on $d_{k,g}$: for every n-variable Boolean function g of algebraic degree at most r, we have $d_{k,g} \leq \sum_{i=0}^{k} \binom{n}{i} - \sum_{i=0}^{k} \binom{n-r}{i}$. This upper bound is achieved by the indicators of an $(n-r)$-dimensional affine subspace of $\mathbb{F}_2^n$ for which the dimension $d_{k,g}$ is exactly equal to $\sum_{i=0}^{k} \binom{n}{i} - \sum_{i=0}^{k} \binom{n-r}{i}$. We can derive from this upper

bound a lower bound on $d_{k,g}$. Let us introduce some notation before. For every n-variable Boolean function g and every positive integer k, we denote by $Mul_k(g)$ the vector space of all n-variable Boolean functions p that can be written as $p = gh$ where h is of algebraic degree at most k. There exists a simple relation between $d_{k,g}$ and $\dim Mul_k(g)$.

Lemma 1. *Let g be an n-variable Boolean function of algebraic degree r. Let k be any positive integer less than n. Then* $\dim Mul_k(g) = \sum_{i=0}^{k} \binom{n}{i} - d_{k,g}$.

Proof. Let ϕ_g be the linear map from $\mathrm{RM}(k,n)$ to $Mul_k(g)$ which maps h to gh. Clearly, this map is onto and its kernel equals $An_k(g)$. Thus, $\sum_{i=0}^{k} \binom{n}{i} = \dim \mathrm{Im}(\phi_g) + \dim \ker(\phi_g) = \dim Mul_k(g) + d_{k,g}$. □

The upper bound of [1] and Lemma 1 will lead us to a lower bound on $d_{k,g}$ achived by some classes of Boolean functions. More precisely,

Lemma 2. *Let g be an n-variable Boolean function of algebraic degree at most r. Then, for every positive integer k, one has*

$$d_{k,g} \geq \sum_{i=0}^{k-r} \binom{n-r}{i}$$

If g is the complement of an indicator of an $(n-r)$-dimensional affine subspace of $\mathbb{F}_2^n$ then $d_{k,g} = \sum_{i=0}^{k-r} \binom{n-r}{i}$.

Proof. Let g be an n-variable Boolean function of algebraic degree at most r. We can assume that $k \geq r$ (indeed otherwise the lower bound is trivial). Take $h \in An_r(g)$. Now, according to Lemma 1, $\dim Mul_{k-r}(h) = \sum_{i=0}^{k-r} \binom{n}{i} - d_{k-r,h} \geq \sum_{i=0}^{k-r} \binom{n-r}{i}$ since $\dim Mul_{k-r}(h) \geq \sum_{i=0}^{k-r} \binom{n-r}{i}$. Moreover, we have the inclusion $Mul_{k-r}(h) \subseteq An_k(g)$. Therefore, it holds that $d_{k,g} \geq \dim Mul_{k-r}(h) \geq \sum_{i=0}^{k-r} \binom{n-r}{i}$. This latter inequality becomes an equality whenever g is the complement of an $(n-r)$-dimensional affine subspaces of $\mathbb{F}_2^n$. Indeed, it has been shown in [1] that $d_{k,g}$ is equal to $\sum_{i=0}^{k-r} \binom{n-r}{i}$ for such Boolean functions. □

We prove a result that we shall use to improve the lower bound of [1, 2]. To this aim, we need to introduce some additional notation. We shall use the word partial ordering $\preceq$ on $\mathbb{F}_2^n$ defined as follows :

$$u, v \in \mathbb{F}_2^n, \quad (u \preceq v) \iff (\mathrm{supp}(u) \subset \mathrm{supp}(v))$$

Given an element u of $\mathbb{F}_2^n$, we call the support of u, that we denote by $\mathrm{supp}(u)$, the subset $\{i \in \{1, \ldots, n\} \mid u_i = 1\}$. The Hamming weight of u, denoted by $\mathrm{wt}(u)$, is the cardinality of $\mathrm{supp}(u)$. Moreover, for every pair (u, v) of elements of $\mathbb{F}_2^n$, we denote by $u \vee v$ the element of $\mathbb{F}_2^n$ defined as: $\forall i = 1, \ldots, n$, $(u \vee v)_i = \max(u_i, v_i)$, that is, the element of $\mathbb{F}_2^n$ whose support is the union of the two supports $\mathrm{supp}(u)$ and $\mathrm{supp}(v)$. We say that an element u of a subset Π of $\mathbb{F}_2^n$ is a maximal element of Π with respect to the word partial ordering $\preceq$ if : $v \in \Pi$, $u \preceq v \Rightarrow v = u$. For every element

u of $\mathbb{F}_2^n$, we denote by $\bar{u}$ the bitwise complement of u, that is, the element of $\mathbb{F}_2^n$ defined by : $\forall i \in \{1, \ldots, n\}, \bar{u}_i = 1 \oplus u_i$. We begin with proving the following key Lemma.

Lemma 3. *Let g be an n-variable Boolean function whose algebraic normal form is : $\forall x \in \mathbb{F}_2^n$, $g(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u$. Set $\Pi = \{u \in \mathbb{F}_2^n \mid a_u = 1\}$. Let $\mathbf{u}$ a maximal element of Π with respect to the word partial ordering $\preceq$. Set $\Theta = \{v \in \mathbb{F}_2^n \mid v \preceq \bar{\mathbf{u}}\}$. Then $\{x^v \cdot g, v \in \Theta\}$ is a linearly independent family of $\mathcal{B}_n$.*

Proof. Let $(c_v)_{v \in \Theta}$ be a collection of elements of $\mathbb{F}_2$ such that : $\forall x \in \mathbb{F}_2^n$, $\bigoplus_{v \in \Theta} c_v x^v g(x) = 0$. Replacing g by its algebraic normal form yields to : $\forall x \in \mathbb{F}_2^n$, $\bigoplus_{(u,v) \in \Pi \times \Theta} c_v x^{u \vee v} = 0$. We now prove that, for every $v \in \Theta$, the monomial $x^{\mathbf{u} \vee v}$ appears only once in the sum $\bigoplus_{(u,v) \in \Pi \times \Theta} c_v x^{u \vee v}$. To this end, let us fix $v \in \Theta$ and let us look forward $v' \in \Theta$ and $u \in \Pi$ such that $u \vee v' = \mathbf{u} \vee v$. This requires that $\mathbf{u} \preceq u \vee v'$. The support of $\mathbf{u}$ being disjoint from the support of v', we must have $\mathbf{u} \preceq u$ which is possible only if $u = \mathbf{u}$ because $\mathbf{u}$ is a maximal element of Π with respect to the word ordering $\preceq$. The equality $u \vee v' = \mathbf{u} \vee v$ becomes $\mathbf{u} \vee v' = \mathbf{u} \vee v$ from which we deduce that $v = v'$ (since they are both disjoint from $\mathbf{u}$). We hence prove that, for every $v \in \Theta$, the monomial $x^{\mathbf{u} \vee v}$ appears only once in the sum $\bigoplus_{(u,v) \in \Pi \times \Theta} c_v x^{u \vee v}$ which vanishes for every word x in $\mathbb{F}_2^n$. That requires that $x \mapsto c_v x^{\mathbf{u} \vee v}$ is null on $\mathbb{F}_2^n$ yielding to $c_v = 0$. The element v being arbitrary, that proves that the collection $\{x^v \cdot g, v \in \Theta\}$ is a linearly independent family of $\mathcal{B}_n$. □

We then use the preceding lemma to show the following result.

Proposition 4. *Let k be a positive integer. Let g be an n-variable Boolean function of algebraic degree at most r whose algebraic normal form is : $\forall x \in \mathbb{F}_2^n$, $g(x) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u$. Set $\Pi = \{u \in \mathbb{F}_2^n \mid a_u = 1\}$. Let $\mathbf{u}$ a maximal element of Π with respect to the word partial ordering $\preceq$. Then*

1. *The vector space $An_k(g \oplus 1)$ is contained in $Mul_k(g)$.*
2. *$\dim Mul_k(g) \geq \sum_{i=k-\mathrm{wt}(\mathbf{u})+1}^{k} \binom{n-\mathrm{wt}(\mathbf{u})}{i} + d_{k,1 \oplus g}$.*
3. *If g is the complement of the indicator of an $(n-r)$-dimensional affine subspace of $\mathbb{F}_2^n$ then $\dim Mul_k(g) = \sum_{i=k-r+1}^{k} \binom{n-r}{i} + d_{k,1 \oplus g}$.*

Proof.

1. Every annihilator h of $1 \oplus g$ satisfies $gh = h$ and thus is an element of $Mul_k(g)$.
2. The algebraic normal form of g can be rewritten as : $\forall x \in \mathbb{F}_2^n$, $g(x) = \bigoplus_{u \in \Pi} x^u$.

   Let $\mathbf{u}$ be a maximal element of Π with respect to the word partial ordering $\preceq$. Define $\Theta = \{v \in \Pi \mid v \preceq \bar{\mathbf{u}}\}$. Let Σ be the subset of Θ defined by $\Sigma = \{v \in \Theta \mid k - \mathrm{wt}(\mathbf{u}) + 1 \leq \mathrm{wt}(v) \leq k\}$. Now, $\{x^v \cdot g, v \in \Sigma\}$ is a subfamily of $\{x^v \cdot g, v \in \Theta\}$ which is a linearly independent family of $\mathcal{B}_n$ according to Lemma 3. Thus, $\{x^v \cdot g, v \in$

$\Sigma\}$ is also a linearly independent family of $\mathcal{B}_n$. Moreover, every element of this family belongs to $Mul_k(g)$ since, for every $v \in \Sigma$, we have that $\mathrm{wt}(v) \leq k$.

Now, let V be the vector subspace spanned by all the Boolean functions $x^v g$ where v ranges over Σ. The vector subspace V is by construction a vector subspace of $Mul_k(g)$ and its dimension over $\mathbb{F}_2$ equals the cardinality of the family $\{x^v \cdot g, v \in \Sigma\}$, that is, its dimension equals $\sum_{i=k-\mathrm{wt}(\mathbf{u})+1}^{k} \binom{n-\mathrm{wt}(\mathbf{u})}{i}$.

We are now going to prove that the vector sum $V + An_k(1 \oplus g)$ is a direct sum of $Mul_k(g)$. Every element of V is of the form $\bigoplus_{(u,v)\in \Pi\times\Sigma} c_v x^{u\vee v}$ where $(c_v)_{v\in\Sigma}$ is any collection of elements of $\mathbb{F}_2$. The algebraic degree of such a Boolean function is at least $k+1$. Indeed, for every $v \in \Sigma$, the monomial $x^{\mathbf{u}\vee v}$ appears only once in the sum $\bigoplus_{(u,v)\in \Pi\times\Sigma} c_v x^{u\vee v}$ (see proof of Lemma 3) and is of algebraic degree $\mathrm{wt}(\mathbf{u})+\mathrm{wt}(v) \geq k+1$. Hence, the intersection $V \cap An_k(1\oplus g)$ is reduced to $\{0\}$ because every non null element of V is of algebraic degree at least $k+1$ while every non null element of $An_k(1 \oplus g)$ is of algebraic degree at most k. This proves that the vector sum $V + An_k(1 \oplus g)$ is a direct sum. This implies that $\dim Mul_k(g) \geq \dim V + \dim An_k(1\oplus g) = \dim V + d_{k,1\oplus g} = \sum_{i=k-\mathrm{wt}(\mathbf{u})+1}^{k} \binom{n-\mathrm{wt}(\mathbf{u})}{i} + d_{k,1\oplus g}$.

(3) Let g be the complement of an $(n-r)$-dimensional affine subspace of $\mathbb{F}_2^n$. We have that $d_{k,1\oplus g} = \sum_{i=0}^{k}\binom{n}{i} - \sum_{i=0}^{k}\binom{n-r}{i}$ and $d_{k,g} = \sum_{i=0}^{k-r}\binom{n-r}{i}$. According to Lemma 1, $\dim Mul_k(g) = \sum_{i=0}^{k}\binom{n}{i} - d_{k,g} = \sum_{i=0}^{k}\binom{n}{i} - \sum_{i=0}^{k-r}\binom{n-r}{i} = \sum_{i=0}^{k}\binom{n}{i} - \sum_{i=0}^{k}\binom{n-r}{i} + \sum_{i=k-r+1}^{k}\binom{n-r}{i} = d_{k,1\oplus g} + \sum_{i=k-r+1}^{k}\binom{n-r}{i}$.

□

We can deduce from the preceding Proposition the following lower bound on the difference $\dim Mul_k(g) - d_{k,1\oplus g}$.

Corollary 5. *Let k be a positive integer. Then, for every n-variable Boolean function g of algebraic degree at most r, we have*

$$\dim Mul_k(g) - d_{k,1\oplus g} \geq \sum_{i=k-r+1}^{k} \binom{n-r}{i}$$

Proof. Assume that the algebraic normal form of g is : $\forall x \in \mathbb{F}_2^n$, $g(x) = \bigoplus_{u\in\mathbb{F}_2^n} a_u x^u$. Set $\Pi = \{u \in \mathbb{F}_2^n \mid a_u = 1\}$. The algebraic degree of g equals r then there exists at least one maximal element $\mathbf{u}$ of Π with respect to the word partial ordering $\preceq$ whose hamming weight equals r. We then deduce the result from Proposition 4. □

Remark 1. Proposition 4 says that, for every $w \leq r$,

$$\dim Mul_k(g) - d_{k,1\oplus g} \geq \sum_{i=k-w+1}^{k} \binom{n-w}{i}$$

if the algebraic normal form of g contains a monomial x^ω, with $\mathrm{wt}(\omega) = w$, which is not contained in any another monomial of g. Now, we have

$$\sum_{i=k-w+1}^{k} \binom{n-w}{i} \geq \sum_{i=k-r+1}^{k} \binom{n-r}{i}$$

Indeed, using the identity $\binom{n-w}{i} = \sum_{p=i-r+w}^{i} \binom{n-r}{p}\binom{r-w}{i-p}$, we get $\sum_{i=k-w+1}^{k} \binom{n-w}{i} = \sum_{i=k-w+1}^{k} \sum_{p=i-r+w}^{i} \binom{n-r}{p}\binom{r-w}{i-p} = \sum_{p=k-r+1}^{k} \binom{n-r}{p} \sum_{i=\max(p,k-w+1)}^{\min(p-w+r,k)} \binom{r-w}{i-p} \geq \sum_{p=k-r+1}^{k} \binom{n-r}{p}$.

Therefore, the preceding lower bound on $\dim Mul_k(g) - d_{k,1\oplus g}$ is better than that of Corollary 5 if we take $w < r$. However, it requires more information on the n-variable Boolean function g than that of Corollary 5 that simply depends on the algebraic degree of g. Now, we shall need a lower bound that does not depend on the n-variable Boolean function g to get our result. This is the reason why we shall restrict ourselves to use Corollary 5 rather than Proposition 4 in the sequel.

3. A new lower bound on the r-th-order nonlinearity of n-variable Boolean function with respect to their algebraic immunity

In this Section, we shall see that the dimension of the vector subspace of all annihilators with prescribed algebraic degree of a Boolean function plays also an important role in relation to the r-th order nonlinearity of this Boolean function.

Given an n-variable Boolean function f and a positive integer r, we denote by $\Re_f(r,n)$ the restriction of the generator matrix of the rth-order Reed-Muller code to the support of f. Clearly, an n-variable Boolean function f has no annihilator of algebraic degree at most k if and only if all the matrices $\Re_f(r,n)$, $r \leq k-1$, are of full rank. Moreover, one has, for every positive integer $k \leq n$,

$$d_{k,f} + \mathrm{rank}\,(\Re_f(k,n)) \;=\; \sum_{i=0}^{k} \binom{n}{i}. \tag{1}$$

The rth-order nonlinearity of a Boolean function g is the minimum Hamming distance from f to an n-variable Boolean function g of algebraic degree at most r. Our approach is to establish a lower bound on $\mathrm{dist}(f,g)$ holding for every Boolean function g of algebraic degree r. To this end, we first

establish a lower bound on $\mathrm{dist}(f,g)$ involving the sum of the two dimensions $d_{k-1,g}$ and $d_{k-1,1\oplus g}$. This is the key result that will enable to improve further the lower bound of [2, 1].

Lemma 6. *Let f be an n-variable Boolean function. Suppose that $AI(f) = k$. Let r be a positive integer less than k. Then, for every n-variable boolean function g of algebraic degree at most r, we have*

$$\mathrm{dist}(f,g) \geq d_{k-1,g} + d_{k-1,1\oplus g}.$$

Proof. Denote by d the number of bits to be modified in the truth table of f to obtain g. Denote by d_i, $i \in \{0,1\}$, the number of words of $\mathrm{supp}(i \oplus f)$ for which we modify the output value of $i \oplus f$. Clearly, we have $\mathrm{dist}(f,g) = d = d_0 + d_1$.

Now, for every positive integer ℓ, The matrix $\Re_g(\ell, n)$ is deduced from the matrix $\Re_f(\ell, n)$ by deleting d_0 rows and adding d_1 rows. The matrix $\Re_f(k-1,n)$ being of full rank, we hence have that $\mathrm{rank}(\Re_g(k-1,n)) \geq \sum_{i=0}^{k-1} \binom{n}{i} - d_0$ and thus that $d_0 \geq \sum_{i=0}^{k-1} \binom{n}{i} - \mathrm{rank}(\Re_g(k-1,n)) = d_{k-1,g}$.

Similarly, the matrix $\Re_{1\oplus g}(\ell, n)$ is deduced from the matrix $\Re_{1\oplus f}(\ell, n)$ by deleting d_1 rows and adding d_0 rows. The matrix $\Re_f(k-1,n)$ being also of full rank, we hence deduce by similar arguments as those exposed previously that $d_1 \geq d_{k-1,1\oplus g}$. □

Remark 2. Collecting together Lemma 2 applied to affine Boolean functions and Lemma 6 leads to $\mathrm{dist}(f,l) \geq d_{k-1,l} + d_{k-1,1\oplus l} = 2\sum_{i=0}^{k-2} \binom{n-1}{i}$ for every n-variable affine Boolean functions, that is, we recover the lower bound of [9].

Similarly, Applying Lemma 6 to n-variable Boolean functions of algebraic degree at most r leads to $\mathrm{dist}(f,g) \geq 2\sum_{i=0}^{k-r-1} \binom{n-r}{i}$, that is, we recover the first lower bound of [1, Theorem 1].

We then deduce from Lemma 6, thanks to Lemma 4 and 6 our lower bound on the rth-order linearity of an n-variable Boolean function with prescribed algebraic immunity. Our idea is to get a lower bound on this sum rather than considering separately the two dimensions $d_{k-1,g}$ and $d_{k-1,1\oplus g}$.

Theorem 7. *Let f be an n-variable Boolean function of algebraic immunity k and let r be a positive integer less than k. Then*

$$nl_r(f) \geq \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}$$

Proof. Let g be an arbitrary n-variable Boolean function of algebraic degree at most r. According to Lemma 6, we have

$$\mathrm{dist}(f,g) \geq d_{k-1,g} + d_{k-1,1\oplus g}.$$

Now, note that $An_{k-1}(g \oplus 1) \supset Mul_{k-r-1}(g)$ and $An_{k-1}(g) \supset Mul_{k-r-1}(1 \oplus g)$. Hence

$$\mathrm{dist}(f,g) \geq d_{k-1,g} + d_{k-1,1\oplus g} \geq \dim Mul_{k-r-1}(g) + \dim Mul_{k-r-1}(1 \oplus g)$$

Next, thanks to Lemma 1, we get

$$\begin{aligned}\mathrm{dist}(f,g) &\geq \dim Mul_{k-r-1}(g) + \dim Mul_{k-r-1}(1 \oplus g) \\ &= \sum_{i=0}^{k-r-1} \binom{n}{i} + \dim Mul_{k-r-1}(g) - d_{k-r-1,1\oplus g}.\end{aligned}$$

We finally conclude thanks to Corollary 5 that says that

$$\dim Mul_{k-r-1}(g) - d_{k-r-1,1\oplus g} \geq \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i}$$

□

References

1. C. Carlet, *On the higher order nonlinearities of algebraic immune Boolean functions*, CRYPTO 2006, Lecture notes in Computer Science, vol. 4117, 2006, pp. 584–601.
2. C. Carlet, D. K. Dalai, K. C. Gupta, and S. Maitra., *Algebraic immunity for cryptographically significant boolean functions: Analysis and construction*, IEEE Transactions on Information Theory **52** (2006), no. 7, 3105–3121.
3. C. Carlet and S. Mesnager, *Improving the upper bounds on thecovering radii of binary Reed-Muller codes*, IEEE Transactions on Information Theory (2007), To appear.
4. N. Courtois, *Higher Order Correlation Attacks, XL algorithm, and Cryptanalysis of Toyocrypt*, ICISC 2002, Lecture notes in Computer Science, vol. 2587, Spinger-Verlag, 2002, The extended version of the paper can be found on `http://eprint.iacr.org/2002/087/`, pp. 182–199.
5. D. K. Dalai, K. C. Gupta, and S. Maitra, *Notion of algebraic immunity and its evaluation related to fast algebraic attacks*, International Workshop on Boolean Functions : Cryptography and Applications, 2006, 13–15 March, Rouen, France, 2006.
6. J. Golic, *Fast low order approximation of cryptographic functions*, EUROCRYPT'96, Lecture notes in Computer Science, vol. 1070, Spinger-Verlag, 1996, pp. 268–282.
7. T. Iwata and K. Kurosawa, *Probabilistic higher order differential attack and higher order bent functions*, ASIACRYPT'99, Lecture notes in Computer Science, vol. 1716, Spinger-Verlag, 1999, pp. 62–74.
8. L. R. Knudsen and M. J. B. Robshaw, *Nonlinear approximations in linear cryptanalysis*, EUROCRYPT'96, Lecture notes in Computer Science, vol. 1070, Spinger-Verlag, 1996, pp. 224–236.
9. M. Lobanov, *Tight bound between nonlinearity and algebraic immunity*, Cryptology ePrint Archive, Report 2005/441, 2005, `http://eprint.iacr.org/`.
10. W. Meier and N. Courtois, *Algebraic Attacks on Stream Ciphers with Liner Feedback*, Eurocrypt 2003, Lecture notes in Computer Science, vol. 2656, Spinger-Verlag, 2003, This attack has been now implemented by Nicolas Courtois, see the extended version of the paper at `http://www.minrank.org/toyolili.pdf`. Also reproduced (illegally) at `http://www.esat.kuleuven.ac.be/~jlano/stream/papers/coumei03.pdf`, pp. 345–359.
11. W. Meier, E. Pasalic, and C. Carlet, *Algebraic Attacks and Decomposition of Boolean Functions*, Eurocrypt 2004, Lecture notes in Computer Science, vol. 3027, Spinger-Verlag, 2004, Slides at `http://www.zurich.ibm.com/eurocrypt2004/slides/session14talk1.pdf`, pp. 474–491.
12. W. Millan, *Low order approximations of cipher functions*, Cryptographic Policy and Algortihms, Lecture notes in Computer Science, vol. 1029, Springer-Verlag, 1996, pp. 144–155.

n \ r	2	3	4	5	6	7
18	**43556**	**17439**	**5518**	1976	344	38
19	**126008**	**57992**	**21592**	**6507**	2320	382
20	**188368**	**81404**	**28568**	8826	2702	422
21	**527900**	**257396**	**103784**	**34780**	15094	3124
22	**803860**	**369748**	**141064**	**44844**	18218	3588
23	**2195580**	**1123220**	**483680**	**176660**	**53954**	21806
24	**3396320**	**1645660**	**672784**	**233827**	**68071**	25902
25	**9080772**	**4838490**	**2202164**	**863975**	**289301**	136812
26	**14239032**	**7211198**	**3125248**	**1169920**	**374371**	167364
27	**37392864**	**20633040**	**9846132**	**4104275**	**1484042**	**458054**
28	**59333408**	**31214643**	**14221898**	**5670245**	**1963795**	**581338**
29	**153434536**	**87279291**	**43393566**	**19055725**	**7355234**	**2462995**
30	**246025562**	**133797407**	**63665462**	**26799567**	**9928262**	**3194667**

TABLE 1. Best lower bounds on $nl_r(f)$ for $18 \leq n \leq 30$, $AI(f) = \lceil \frac{n}{2} \rceil$, $r \leq 8$

n \ r	2	3	4	5	6	7
18	1.46	1.76	1.88	0.69	0.73	0.82
19	1.53	1.95	2.18	1.01	0.66	0.71
20	1.49	1.87	2.07	0.92	0.67	0.72
21	1.55	2.04	2.38	2.30	0.63	0.65
22	1.52	1.96	2.26	2.38	0.64	0.66
23	1.58	2.13	2.57	2.83	1.33	0.62
24	1.55	2.05	2.44	2.67	1.21	0.62
25	1.60	2.20	2.74	3.13	2.11	0.59
26	1.57	2.12	2.60	2.95	2.24	0.60
27	1.61	2.27	2.90	3.42	3.74	1.77
28	1.59	2.19	2.76	3.22	3.50	1.60
29	1.63	2.33	3.05	3.69	4.17	2.12
30	1.60	2.26	2.90	3.48	3.90	2.08

TABLE 2. The new lower bound over the Lower bound of [1] for $18 \leq n \leq 30$, $AI(f) = \lceil \frac{n}{2} \rceil$, $r \leq 8$

13. C.E. Shannon, *Communication theory of secrecy systems*, vol. 28, pp. 656–715, Bell system technical journal, 1949.

APPENDIX A. TABLES

Our result improves further the result of [2] for all orders and improves the result of [1] for all low orders (see the tables 1 and 2). We give in the next table the best lower bound between ours (that we write in bold text) and those of [1] for n ranging from 18 to 30, for optimum algebraic immunity $\lceil \frac{n}{2} \rceil$ and for r ranging from 2 to 7.

n \ r	2	3	4	5	6	7
18	1.40	1.38	1.36	1.38	1.46	1.63
19	1.34	1.32	1.30	1.29	1.33	1.41
20	1.37	1.35	1.32	1.31	1.35	1.44
21	1.31	1.30	1.26	1.25	1.26	1.30
22	1.34	1.32	1.28	1.27	1.28	1.32
23	1.29	1.27	1.24	1.21	1.21	1.23
24	1.32	1.29	1.25	1.23	1.23	1.25
25	1.28	1.26	1.22	1.19	1.18	1.18
26	1.30	1.27	1.23	1.20	1.19	1.20
27	1.26	1.24	1.20	1.17	1.15	1.15
28	1.28	1.26	1.22	1.18	1.17	1.16
29	1.25	1.23	1.19	1.16	1.14	1.13
30	1.27	1.24	1.20	1.17	1.15	1.14

TABLE 3. The new lower bound over the Lower bound of [2] for $18 \leq n \leq 30$, $AI(f) = \lceil \frac{n}{2} \rceil$, $r \leq 8$