# The complexity of Boolean functions from cryptographic viewpoint

Claude Carlet*

**Abstract**

Cryptographic Boolean functions must be complex to satisfy Shannon's principle of confusion. But the cryptographic viewpoint on complexity is not the same as in circuit complexity. The two main criteria evaluating the cryptographic complexity of Boolean functions on $F_2^n$ are the nonlinearity (and more generally the $r$-th order nonlinearity, for every positive $r < n$) and the algebraic degree. Two other criteria have also been considered: the algebraic thickness and the non-normality. After recalling the definitions of these criteria and why, asymptotically, almost all Boolean functions are deeply non-normal and have high algebraic degrees, high ($r$-th order) nonlinearities and high algebraic thicknesses, we study the relationship between the $r$-th order nonlinearity and a recent cryptographic criterion called the algebraic immunity. This relationship strengthens the reasons why the algebraic immunity can be considered as a further cryptographic complexity criterion.

Index Terms - Boolean function, nonlinearity, Reed-Muller code.

## 1 Introduction

Let $n$ be any positive integer. We denote by $\mathcal{B}_n$ the set of all $n$-variable Boolean functions (from the vector space $F_2^n$ of binary vectors of length $n$ to $F_2$). We denote by $\oplus$ the additions in $F_2$, in $F_2^n$ and in $\mathcal{B}_n$. The representation of Boolean functions which is mostly used in cryptography is the *algebraic normal form* (ANF):

$$f(x_1, \cdots, x_n) = \bigoplus_{u \in F_2^n} a_u \left( \prod_{i=1}^{n} {x_i}^{u_i} \right) = \bigoplus_{u \in F_2^n} a_u \, x^u.$$

The (global) degree of the ANF (which exists and is unique, for every Boolean function) is called the *algebraic degree* of the function. It is *affine invariant*: the degree of any function $f$ equals that of any *affinely equivalent* function $f \circ A$ ($A$

*INRIA Projet CODES, BP 105, 78153 Le Chesnay Cedex, France; e-mail: Claude.Carlet@inria.fr; also with the University of Paris 8 (MAATICAH)



Dagstuhl Seminar Proceedings 06111
Complexity of Boolean Functions
http://drops.dagstuhl.de/opus/volltexte/2006/604

element of the general affine group, the set of all affine automorphisms of $F_2^n$). The Boolean functions whose algebraic degrees do not exceed 1 are the *affine* functions.

The Hamming weight of a Boolean function $f$ is the size of its support $\{x \in F_2^n;\ f(x) = 1\}$ and the Hamming distance between two functions $f$ and $g$ is the Hamming weight of the Boolean function $f \oplus g$. The *nonlinearity* $\mathcal{NL}(f)$ of a Boolean function $f$ is its minimum Hamming distance to affine functions. It is a natural complexity criterion: complex functions are supposed to be very different from the simplest (i.e. affine) Boolean functions, and the Hamming distance is a natural measure to evaluate this difference. Several years after the introduction of this notion by Rothaus [37] (the name came later), it has been confirmed as the main criterion quantifying the resistance of ciphers using the function to several kinds of attacks (linear and correlation attacks). The nonlinearity is affine invariant and can be expressed by means of the *Walsh* transform of $f$ (i.e. the discrete Fourier - or Hadamard - transform of the function $(-1)^f$):

$$\widehat{\mathrm{f}}(u) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus u \cdot x}$$

where $u \cdot x$ denotes the usual inner product $u \cdot x = u_1 x_1 \oplus \cdots \oplus u_n x_n$. We have:

$$\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2} \max_{u \in F_2^n} |\widehat{\mathrm{f}}(u)| \ . \tag{1}$$

Because of Parseval's relation:

$$\sum_{u \in F_2^n} \widehat{\mathrm{f}}^{\,2}(u) = 2^{2n},$$

any Boolean function $f$ on $n$ variables satisfies the so-called *covering radius bound* $\mathcal{NL}(f) \leq 2^{n-1} - 2^{n/2-1}$. This upper bound can be achieved for even values of $n$. The functions for which equality holds are called *bent functions*. These functions are used in coding theory for designing optimal error correcting codes (e.g. the Kerdock code), in combinatorics (their supports are *difference sets* and they can then be used in *designs*), and in telecommunications for generating *sequences* for CDMA. But in cryptography, they have the drawback of being unbalanced (they do not output as many 0's and 1's).

Nonlinearity is the most important criterion among those cryptographic criteria on Boolean functions (used in conventional cryptosystems) which are related to Shannon's principle of *confusion*. This principle [40] has been introduced in 1949. Since then, its relevance to modern cryptography has always been verified. It is related to the *complexity* of the Boolean functions involved in the cryptosystems (stream ciphers, block ciphers).
Nonlinearity is related to attacks on stream ciphers (cf. [6, 18]) and block ciphers as well (cf. the linear attack by Matsui [28]). Two other criteria play also important roles: the algebraic degree and the number of monomials in the ANF (i.e. the number of nonzero $a_u$'s). The complexity of the "higher order

differential attack" on block ciphers due to Knudsen and Lai [22, 23] depends on the algebraic degrees of the Boolean functions involved in the system. The linear complexity of a sequence generated by several Linear Feedback Shift Registers (LFSR) combined by a nonlinear function, or of a single one, filtered by a nonlinear function, depends on the degree of the function and on the number of monomials in its ANF (these parameters condition therefore the resistance to Berlekamp-Massey algorithm, cf. [27, 38], see also [30], page 208).
But these two criteria do not fit perfectly with the cryptographic reality.
Indeed, in the case of the first one, changing a few bits in the output to a function of low degree does not change much its robustness, and it can move the degree up to $n$ (or to $n-1$ if the original function was balanced and if we want to keep balancedness, since we need then to change at least two output bits). The proper criterion is the *nonlinearity profile*: let $\mathcal{NL}_r(f)$ denote the distance between $f$ and the set of all functions of degrees at most $r$ (the so-called Reed-Muller code), we call $\mathcal{NL}_r(f)$ the $r$-th order nonlinearity of $f$, and the nonlinearity profile is the sequence of $\mathcal{NL}_r(f)$ for $r = 1, \ldots, n-1$. For $r > 1$, it must be large but not necessarily almost optimum[1]. The optimum, that is, the maximum possible value of $\mathcal{NL}_r(f)$ is unkown for $r > 1$ and $n \geq 8$ (and also for $r = 1$ and $n \geq 9$ odd); the best known asymptotic upper bound has been given in [12]: $\max_f \mathcal{NL}_r(f) \leq 2^{n-1} - \frac{\sqrt{15}}{2} \cdot (1+\sqrt{2})^{r-2} \cdot 2^{n/2} + O(n^{r-2})$.
The number of monomials in the ANF of the function is not a proper criterion either: as pointed out by W. Meier and O. Staffelbach in [29], the general complexity criteria which are mostly interesting in cryptographic framework are affine invariant because the attacks on cryptosystems using Boolean functions (e.g. filtered Linear Feedback Shift Registers, block ciphers) often work with the same complexity when the functions are replaced by affinely equivalent ones. The number of monomials in the ANF is not affine invariant. An extreme example (given by Meier and Staffelbach) of a function with many monomials in its ANF and whose behavior is similar to a function with few monomials is the function whose ANF contains all monomials: it equals $\prod_{i=1}^{n}(x_i \oplus 1)$ and is affinely equivalent to the single monomial $\prod_{i=1}^{n} x_i$.

**Definition 1** *The* algebraic thickness $\mathcal{T}(f)$ *of a Boolean function $f$ is the minimum number of monomials with nonzero coefficients in the ANF of the functions $f \circ A$, where $A$ ranges over the general affine group.*

Equivalently, for every Boolean function $f(x) = \bigoplus_{u \in F_2^n} a_u \, (\prod_{i=1}^{n} {x_i}^{u_i})$, the parameter $\mathcal{T}(f)$ is the minimum number of monomials in the ANF of the functions $\bigoplus_{u \in F_2^n} a_u \, (\prod_{i=1}^{n} (l_i(x))^{u_i})$ where the $l_i$'s are affine functions whose linear parts are linearly independent.
For instance, the indicator $1_E$ of any $k$-dimensional flat $E$ (defined by $1_E(x) = 1$ if $x \in E$; 0 otherwise) being affinely equivalent to $\prod_{i=1}^{n-k} x_i$, we have $\mathcal{T}(1_E) = 1$. This is true in particular for $k \geq n-1$, that is, for every nonzero affine function. Every non-affine quadratic function (i.e. any function of degree 2) being affinely

[1] For $r = 1$, a good approximation of the function by an affine function leads to very efficient attacks. So the nonlinearity must be very high.

equivalent to $x_1x_2 \oplus \cdots \oplus x_{2k-1}x_{2k} \oplus x_{2k+1}$ (where $2k+1 \leq n$) if the function is balanced and to $x_1x_2 \oplus \cdots \oplus x_{2k-1}x_{2k}$ or to $x_1x_2 \oplus \cdots \oplus x_{2k-1}x_{2k} \oplus 1$ (where $2k \leq n$) otherwise (cf. [26]), we have $\mathcal{T}(f) \leq \lfloor n/2 \rfloor + 1$, where $\lfloor\ \rfloor$ denotes the integer part.

A fourth criterion can be considered. It already plays a role in the research on general (non-cryptographic) complexity of Boolean functions. It also generalizes a notion introduced by H. Dobbertin in [19].

**Definition 2** *Let $k \leq n$. A Boolean function $f$ on $F_2^n$ is called $k$-normal (resp. weakly-$k$-normal) if there exists a $k$-dimensional flat on which $f$ is constant (resp. affine).*

Clearly, $k$-normality implies weak-$k$-normality and weak-$k$-normality implies $(k-1)$-normality. The complexity criterion we are interested in is *non-$k$-normality with small $k$* (smaller is $k$, harder is the criterion).
Non-normality is a natural complexity criterion to consider in cryptography: since any affine function is constant on an affine hyperplane, it is natural to expect from a complex function to be non-constant on any flat of some low dimension.
This complexity criterion is not yet related to explicit attacks on ciphers. But the situation of the degree and of the nonlinearity, when they were first considered, was similar (for instance, the linear attack has been discovered by Matsui [28] sixteen years after Rothaus [37] introduced the idea, but not the term, of nonlinearity). Moreover, there is a relation (cf. Proposition 1) between (non)-normality and nonlinearity which shows that to have a chance to be highly nonlinear, a function must be non-(weakly)-normal at a reasonably deep level.

The normality has a nice relationship with the nonlinearity:

**Proposition 1** *Let $f$ be a weakly-$k$-normal Boolean function on $F_2^n$. Then*

$$\mathcal{NL}(f) \leq 2^{n-1} - 2^{k-1}, \tag{2}$$

*or equivalently*

$$k \leq \log_2[2^{n-1} - \mathcal{NL}(f)] + 1.$$

We refer to [8] for a survey of the different proofs of this result.

# 2 Random functions are almost surely highly complex

Recall that, asymptotically, almost all Boolean functions have high circuit complexities (more precisely, the density of the set of $n$-variable Boolean functions with high complexity tends to 1 when $n$ tends to infinity). Lupanov [25] calls this the *Shannon effect* (Shannon [41] observed it in 1949).
It is a simple matter to check the Shannon effect also for the algebraic degree:

almost all Boolean functions have degrees at least $n-1$ since the number of $n$-variable Boolean functions of degrees at most $n-2$ equals $2^{\sum_{i=0}^{n-2}\binom{n}{i}} = 2^{2^n-n-1}$ and is negligible with respect to the number $2^{2^n}$ of all $n$-variable Boolean functions.
In [32], D. Olejár and M. Stanek showed the same Shannon effect on the nonlinearity: almost all Boolean functions on $F_2^n$ have nonlinearities greater than $2^{n-1} - c_1\sqrt{n}\ 2^{\frac{n}{2}}$, where $c_1 = \sqrt{\ln 2(1+\epsilon_0)/2}$ (where $\epsilon_0 > 0$ is arbitrary).
Let us generalize their result to the nonlinearity profile. We shall need the following well-known lemma (see [1, 26]):

**Lemma 1** *Let $N$ be any positive integer and $0 < \lambda < 1/2$. Then*

$$\frac{2^{NH_2(\lambda)}}{\sqrt{8N\lambda(1-\lambda)}} \leq \sum_{0\leq i\leq \lambda N}\binom{N}{i} \leq 2^{NH_2(\lambda)} < 2^N e^{-2N(1/2-\lambda)^2}$$

*where $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function.*

**Theorem 1** *Let $c$ be any strictly positive real number. For every $r$, the density of the set of functions such that*

$$\mathcal{NL}_r(f) > 2^{n-1} - c\sqrt{\sum_{i=0}^{r}\binom{n}{i}}\ \ 2^{\frac{n-1}{2}}$$

*is greater than*

$$1 - 2^{(1-c^2\log_2 e)\sum_{i=0}^{r}\binom{n}{i}}$$

*and, if $c^2\log_2 e > 1$, it tends to 1 when $n$ tends to $\infty$.*

*Proof*: The number of functions of degrees at most $r$ equals $2^{\sum_{i=0}^{r}\binom{n}{i}}$. For every such function $h$, the number of Boolean functions $f$ whose Hamming distance to $h$ is upper bounded by some number $D$ equals

$$\sum_{0\leq i\leq D}\binom{2^n}{i}.$$

Hence, the number of Boolean functions $f$ such that

$$d_H(f,h) \leq 2^{n-1} - c\sqrt{\sum_{i=0}^{r}\binom{n}{i}}\ 2^{\frac{n-1}{2}}$$

equals

$$\sum_{0\leq i\leq 2^{n-1}-c\sqrt{\sum_{i=0}^{r}\binom{n}{i}}\ 2^{\frac{n-1}{2}}}\binom{2^n}{i}.$$

This number is upper bounded by $2^{2^n - c^2 \sum_{i=0}^{r} \binom{n}{i} \log_2 e}$, according to Lemma 1. Thus, the number of those Boolean functions which have $r$-th order nonlinearity smaller than or equal to $2^{n-1} - c\sqrt{\sum_{i=0}^{r} \binom{n}{i}}\ 2^{\frac{n-1}{2}}$ is smaller than $2^{(1-c^2 \log_2 e) \sum_{i=0}^{r} \binom{n}{i} + 2^n}$. □

Note that $\sqrt{\sum_{i=0}^{r} \binom{n}{i}}$ can be replaced by $\sqrt{\binom{n}{r}}$ in Theorem 1, since $\sum_{i=0}^{r} \binom{n}{i}$ is equivalent to $\binom{n}{r}$.

The Shannon effect works also for the two other criteria:

**Theorem 2 ([7])** *Let $c$ be any strictly positive real number. The density in $\mathcal{B}_n$ of the subset $\{f \in \mathcal{B}_n \mid \mathcal{T}(f) \geq 2^{n-1} - c\, n\, 2^{\frac{n-1}{2}}\}$ is greater than $1 - 2^{n^2+n}\ e^{-c^2 n^2}$ and, if $c^2 \log_2 e > 1$, then this density tends to 1 when $n$ tends to infinity. For every $n \geq 3$, a Boolean function $f$ such that $\mathcal{T}(f) \geq 2^{n-1} - n\ 2^{\frac{n-1}{2}}$ exists.*

Theorem 2 implies that, for every $\lambda < 1/2$, there exists $N$ such that, for every $n \geq N$, a Boolean function $f$ such that $\mathcal{T}(f) \geq \lambda\ 2^n$ exists. But, unless $\lambda$ is small, $N$ is greater than 3. We can take $N = 9$ for $\lambda = \frac{1}{4}$ and $N = 12$ for $\lambda = \frac{3}{8}$.

**Open problem**:
We do not know if there exist functions $f$ such that $\mathcal{T}(f) > 2^{n-1}$. ◇

We know (cf. [33]) that, for $n$ odd $\geq 15$, there exist Boolean functions with nonlinearities strictly greater than $2^{n-1} - 2^{\frac{n-1}{2}}$. According to Proposition 1, these functions cannot be weakly-$\frac{n+1}{2}$-normal (and *a fortiori* they cannot be $\frac{n+1}{2}$-normal). S. Blackburn and H. Dobbertin, using a counting argument, have also observed (see [19]) that for every even $n \geq 12$, there exist non-$\frac{n}{2}$-normal Boolean functions on $F_2^n$. In fact, a stronger Shannon effect exists for the non-normality criterion:

**Theorem 3 ([7])** *Let $k_n$ be a sequence of integers (greater than 2) such that $\frac{2^{k_n}}{n k_n}$ tends to infinity. The density in $\mathcal{B}_n$ of the set of all Boolean functions on $F_2^n$ which are not weakly-$k_n$-normal is greater than $1 - 2^{n(k_n+1)-2^{k_n}}$ and tends to 1 when $n$ tends to infinity.*
*For every $n \geq 12$, there exist non-weakly-$\lfloor \frac{n}{2} \rfloor$-normal functions; for every $n \geq 16$, there exist non-weakly-$\left(\lfloor \frac{n}{2} \rfloor - 1\right)$-normal functions.*

This result implies that, if we have $\alpha > 1$ and $\alpha \log_2 n \leq k_n$ for every $n$, then asymptotically, almost all Boolean functions are non-weakly-$k_n$-normal.
*We have also checked that for every $n \geq 12$, there exist non-$\lfloor \frac{n}{2} \rfloor$-normal functions with $\mathcal{T}(f) > \max(\frac{3}{8}2^n, 2^{n-1} - n\ 2^{\frac{n-1}{2}})$ and nonlinearity $\mathcal{NL}(f) \geq 2^{n-1} - \sqrt{n}\ 2^{\frac{n-1}{2}}$.*
But we know that for $n \leq 7$, all Boolean functions are $\lfloor \frac{n}{2} \rfloor$-normal (cf. [20]). In fact, $k$-normality for $k \approx n/2$, which is unusual for large $n$, is common for low

$n$.
As usual, the proof of existence of non-normal functions does not give examples of such functions. Alon, Goldreich, Hastad and Peralta give in [2] several constructions of functions that are nonconstant on flats of dimension $n/2$. This is not explicitly mentioned in the paper. What they actually show is that the functions (they say, the sets) are not constant on flats defined by equations $x_{i_1} = a_1, ..., x_{i_{n/2}} = a_{n/2}$. To prove that, they use however the fact that the sets have small bias with respect to linear tests. As this property is invariant w.r.t. affine transformations, it implies the result.
There are also explicit constructions that work for dimensions $(1/2 - \epsilon)\, n$, for some small $\epsilon > 0$ very recently found by Jean Bourgain [4].
Functions that are nonconstant on flats of dimensions $n^\delta$ for every $\delta > 0$ are also given in [3]. These constructions are very good asymptotically (but may not be usable to obtain functions in explicit numbers of variables).
As far as we know, no construction is known below $n^\delta$.

**Remark**:
Theorem 3 remains essentially valid (except for the number "12") if, in the definition of weakly-$k$-normal functions, we replace "there exists a $k$-dimensional flat on which the function is affine" by "there exists a $k$-dimensional flat such that the restriction of the function to this flat has degree $\leq l$", where $l$ is some fixed positive integer. $\diamond$

So, almost all Boolean functions are deeply non-normal. On the contrary, quadratic functions are $\frac{n}{2}$-normal if $n$ is even and weakly-$\frac{n+1}{2}$-normal if $n$ is odd, according to the properties of these functions recalled in the introduction. What about functions of degree 3? Do they behave similarly to quadratic functions or do they behave more as general functions, with respect to normality (and to nonlinearity when $n$ is odd)? For nonlinearity, this is an open problem. But for normality, we know the existence of non-$k_n$-normal Boolean functions of degree 3, where $k_n$ is negligible with respect to $n$.

**Proposition 2 ([7])** *Let $l_n$ be any sequence of positive integers such that $\frac{l_n}{\sqrt{n}}$ tends to infinity. The density of the set of all Boolean functions of degrees at most 3 on $F_2^n$ which are not weakly-$l_n$-normal in the set of all Boolean functions of degrees at most 3 is greater than or equal to $1 - 2^{n(l_n+1)-{l_n}^2-\binom{l_n}{2}-\binom{l_n}{3}}$ and it tends to 1 when $n$ tends to infinity. For every $n \geq 15$, there exist non-weakly-$\left\lceil \frac{n}{2} \right\rceil$-normal functions of degree 3.*

Same remark as above can be done for Proposition 2, with $l = 2$. And this proposition can also be generalized to higher fixed degrees.

All the results above are essentially valid if we restrict ourselves to balanced functions. Indeed, the number of balanced functions on $F_2^n$ equals $\binom{2^n}{2^{n-1}} = \Theta(2^{2^n - n/2})$, according to Stirling's formula, and all the arguments used in the proofs still work.

# 3 A recent criterion: the algebraic immunity

The recent algebraic attacks [14] have led to further characteristics that a cryptographic Boolean function must have. These attacks cleverly use over-defined systems of multivariate nonlinear equations to recover the secret key (or to recover the initialization of the cipher, which is sufficient for breaking it, since all the rest is supposed to be public). The idea of using such systems comes from C. Shannon, but the improvement in the efficiency of the method is recent. The core of the analysis in the standard algebraic attack is to find out low degree functions $g \neq 0$ and $h$ such that $fg = h$ (where $fg$ is the product of $f$ and $g$, i.e. has support the intersection of their supports). It has been shown in [31] that this is equivalent to the existence of a low degree nonzero annihilator of $f$ or of $1 \oplus f$, that is, of a function $g$ such that $fg = 0$ or $(1 \oplus f)g = 0$. The algebraic immunity of a Boolean function $f$, quantifying the resistance to the standard algebraic attack of the pseudo-random generators using it as a nonlinear function is then defined as follows.

**Definition 3** *Let $f$ be any $n$-variable Boolean function. Its algebraic immunity $AI(f)$ equals the minimum algebraic degree of all the nonzero annihilators of $f$ and of all the nonzero annihilators of $f \oplus 1$.*

Clearly, since $f$ is an annihilator of $f \oplus 1$ (and $f \oplus 1$ is an annihilator of $f$), the algebraic immunity is upper bounded by the degree.
As shown in [14], we always have $AI(f) \leq \lceil \frac{n}{2} \rceil$. This bound is tight. Also, we know that almost all Boolean functions have algebraic immunities close to this optimum; more precisely, for all $a < 1$, $AI(f)$ is almost surely greater than $\frac{n}{2} - \sqrt{\frac{n}{2} \ln\left(\frac{n}{a \ln 2}\right)}$: see [17]. Hence, in the case of this criterion too, almost all Boolean functions are highly complex.

In [15] is given an lower bound on the (first order) nonlinearity of functions with given algebraic immunity. Let us recall how this bound can be proven and what it is: we clearly have $\sum_{i=0}^{AI(f)-1} \binom{n}{i} \leq wt(f) \leq \sum_{i=0}^{n-AI(f)} \binom{n}{i}$, since otherwise, the linear system expressing that a function $g$ of degree at most $AI(f)-1$ is an annihilator of $f$ (resp. of $f \oplus 1$) would have non-trivial solutions (indeed, its number of equations would be strictly smaller than its number of unknowns); it is a simple matter to show that, for every affine function $h$, the algebraic immunity of $f \oplus h$ is at least $AI(f) - 1$; this implies that $\mathcal{NL}(f) \geq \sum_{i=0}^{AI(f)-2} \binom{n}{i}$.
As observed in [10], this bound can easily be generalized to the higher order nonlinearity: it is a simple matter to show that, for every function $h$ of degree at most $r$, the algebraic immunity of $f \oplus h$ is at least $AI(f) - r$; this implies that $\mathcal{NL}_r(f) \geq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i}$.
In [24], M. Lobanov has improved upon the lower bound obtained in [15]. He obtained that:

$$\mathcal{NL}(f) \geq 2 \sum_{i=0}^{AI(f)-2} \binom{n-1}{i}.$$

We extend this lower bound into a bound on the general $r$-th order nonlinearity. We obtain a bound which is asymtotically slightly better than the lower bound obtained in [10], and which improves upon it in a majority of cases, for the numbers of variables used in cryptographic practice. The way of proving this more difficult result may also present some interest.

## 3.1 A preliminary result on the dimension of the vector space of prescribed degree annihilators of a function

In the next lemma, we extend to all Boolean functions a result from [24] which dealt only with affine functions.

**Lemma 2** *Let $n$, $r$ and $k$ be positive integers. Let $h$ be any $n$-variable Boolean function of algebraic degree $r$. The dimension of the set $An_k(h)$ of those annihilators of degrees at most $k$ of $h$ is at most $\sum_{i=0}^{k}\binom{n}{i}-\sum_{i=0}^{k}\binom{n-r}{i}$.*

*Proof*:
Since $h$ has degree $r$ and since the dimension of $An_k(h)$ is invariant under affine equivalence, we can assume without loss of generality that $h(x)=x_1x_2\cdots x_r\oplus k(x)$, where $k$ has degree at most $r$ and where the term $x_1x_2\cdots x_r$ has null coefficient in its ANF. For any choice of $n-r$ bits $u_{r+1},\ldots,u_n$, the restriction $h_{u_{r+1},\ldots,u_n}$ of $h$ obtained by fixing the variables $x_{r+1},\ldots,x_n$ to the values $u_{r+1},\ldots,u_n$ (respectively) has degree $r$, and has therefore odd weight (i.e. has a support of odd size), since $r$ is the number of its variables. Hence $h_{u_{r+1},\ldots,u_n}$ has weight at least 1. For every $(u_{r+1},\ldots,u_n)\in F_2^{n-r}$, let us then denote by $x_{u_{r+1},\ldots,u_n}$ a vector $x$ such that $(x_{r+1},\ldots,x_n)=(u_{r+1},\ldots,u_n)$ and $h(x)=1$. Let $g$ be an element of $An_k(h)$, and let $g(x)=\sum_{\substack{u\in F_2^n\\ wt(u)\leq k}}a_ux^u$ be its ANF (where $x^u=\prod_{i=1}^n x_i^{u_i}$ and where $wt$ denotes the Hamming weight).
Since we have $h(x)=1\Rightarrow g(x)=0$ and since $g(x)=\sum_{u\preceq x}a_u$, where $u\preceq x$ means that every coordinate of $u$ is upper bounded by the corresponding coordinate of $x$, the coefficients $a_u$ are the solutions of the system $S$ of linear equations $\sum_{u\preceq x_{u_{r+1},\ldots,u_n}}a_u=0$. If, in each equation, we transfer all unknowns $a_u$ such that $(u_1,\ldots,u_r)\neq(0,\ldots,0)$ to the right hand side, we obtain a system $S'$ in the unknowns $a_u$ such that $(u_1,\ldots,u_r)=(0,\ldots,0)$. Replacing the right hand sides of the resulting equations by 0 (i.e. considering the corresponding homogeneous system $S'_0$) gives the system that we obtain when we characterize the $(n-r)$-variable annihilators of degrees at most $k$ of the constant function 1, considered as a function in the variables $x_{r+1},\ldots,x_n$. Since the constant function 1 admits only the null function as annihilator, this means that the matrix of $S'_0$ has full rank $\sum_{i=0}^{k}\binom{n-r}{i}$. Hence, $S$ has rank at least $\sum_{i=0}^{k}\binom{n-r}{i}$. The dimension of $An_k(h)$ is therefore upper bounded by $\sum_{i=0}^{k}\binom{n}{i}-\sum_{i=0}^{k}\binom{n-r}{i}$. □

**Remark**: If $h$ has weight $2^n-2^{n-r}$, then the dimension of $An_k(h)$ equals $\sum_{i=0}^{k-r}\binom{n-r}{i}$. Indeed, $h\oplus 1$ is then the indicator of an $(n-r)$-dimensional

flat (see e.g. [26]), and we may without loss of generality assume that $h(x) = x_1x_2\cdots x_r \oplus 1$. Then the elements of $An_k(h)$ are the products of $h(x) \oplus 1 = x_1x_2\cdots x_r$ with functions in the variables $x_{r+1}, \ldots, x_n$ whose degrees are at most $k-r$. The dimension of $An_k(h)$ equals then $\sum_{i=0}^{k-r} \binom{n-r}{i}$. Note that, in the case $r = 1$, this is the value of the upper bound given by Lemma 2, that is, the value obtained by Lobanov.

## 3.2 Relationship between the algebraic immunity and the nonlinearity profile

**Theorem 4** *Let $f$ be a Boolean function in $n$ variables and let $r$ be a positive integer. The nonlinearity of order $r$ of $f$ satisfies:*

$$\mathcal{NL}_r(f) \geq 2 \sum_{i=0}^{AI(f)-r-1} \binom{n-r}{i}.$$

*Proof*:
Let $h$ be any function of degree at most $r$ and let $d$ be the Hamming distance between $f$ and $h$. Since the Hamming weights of the functions $f(h\oplus 1)$ and $(f\oplus 1)h$ satisfy $wt(f(h\oplus 1))+wt((f\oplus 1)h) = d$, we have $\min(wt(f(h\oplus 1)), wt((f\oplus 1)h)) \leq d/2$. If $\min(wt(f(h\oplus 1)), wt((f\oplus 1)h)) = wt(f(h\oplus 1))$, let $f_1 = f$ and $h_1 = h\oplus 1$. Otherwise, let $f_1 = f \oplus 1$ and $h_1 = h$. We have then $wt(f_1h_1) \leq d/2$.
Let $k$ be any positive integer. A Boolean function of degree at most $k$ belongs to $An_k(f_1h_1)$ if and only if the coefficients in its ANF satisfy a system of $wt(f_1h_1)$ equations in $\sum_{i=0}^{k} \binom{n}{i}$ variables. Hence we have: $\dim(An_k(f_1h_1)) \geq \sum_{i=0}^{k} \binom{n}{i} - d/2$.
We have $\dim(An_k(h_1)) \leq \max_{j=1}^{r} \left(\sum_{i=0}^{k} \binom{n}{i} - \sum_{i=0}^{k} \binom{n-j}{i}\right) = \sum_{i=0}^{k} \binom{n}{i} - \sum_{i=0}^{k} \binom{n-r}{i}$, according to Lemma 2.
If $\dim(An_k(f_1h_1)) > \dim(An_k(h_1))$, then there exists an annihilator $g$ of $f_1h_1$ which is not an annihilator of $h_1$. Then, $gh_1$ is a nonzero annihilator of $f_1$ and has degree at most $k+r$. Thus, if $k = AI(f) - r - 1$, we arrive to a contradiction. We deduce that $\dim(An_{AI(f)-r-1}(f_1h_1)) \leq \dim(An_{AI(f)-r-1}(h_1))$. This implies: $\sum_{i=0}^{AI(f)-r-1} \binom{n}{i} - d/2 \leq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i} - \sum_{i=0}^{AI(f)-r-1} \binom{n-r}{i}$, that is:

$$d \geq 2 \sum_{i=0}^{AI(f)-r-1} \binom{n-r}{i}.$$

Hence the nonlinearity of order $r$ of $f$ is lower bounded by this same expression.□

**Remarks**:
1. The bound of Theorem 4 is better than the bound of [10] for every $n \leq 12$ and for every value of $AI(f)$ and $r$. We give in Table 1, for each value of $13 \leq n \leq 30$, the few values of $AI(f)$ and of $r$ for which the bound of Theorem 4 is worse than the bound of [10].

2. Lobanov's bound does not guarantee that having a high algebraic immunity implies a high resistance to the correlation attacks. Indeed, such resistance needs a high (first order) nonlinearity and even for $AI(f) = (n+1)/2$, which is the highest possible algebraic immunity of an $n$-variable function, a nonlinearity of $2\sum_{i=0}^{(n+1)/2-2}\binom{n-1}{i} = 2^{n-1} - \binom{n-1}{(n-1)/2} \approx 2^{n-1} - \frac{2^n}{\sqrt{2\pi n}}$ (the minimum ensured by Lobanov's bound) is not quite satisfactory. But the bound of [10] and Theorem 4, with $r \geq 2$, show that having a high algebraic immunity is a strong property, not only with respect to the resistance to algebraic attacks, but also with respect to the resistance to higher order attacks. Indeed, the complexity of such attacks increases fastly with the order.
3. If $r \geq AI(f)$, then the bound of Theorem 4 and the bound of [10] give no information; we have then no lower bound on $\mathcal{NL}_r(f)$. But if $f$ is balanced, we have an upper bound: as shown in [9], we have indeed $\mathcal{NL}_r(f) \leq 2^{n-1} - 2^{n-r}$.

*Acknowledgement*

We are indebted to Pavel Pudlak for very useful information on the constructions of non-normal functions.

# References

[1] N. Alon and J.H. Spencer. *The probabilistic method*. Wiley-VCH, 2000 (second edition).

[2] N. Alon, O. Goldreich, J. Hastad and R. Peralta. Simple constructions of almost k-wise independent random variables. Random Stuctures and Algorithms, Vol 3, No 3, pp 289-304, 1992.

[3] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov and A. Wigderson. Simulating Independence: New Constructions of Condensers, Ramsey Graphs, Dispersers, and Extractors. Preprint available at http://www.math.ias.edu/ boaz/Papers/BKSSW.html

[4] J. Bourgain. On the construction of affine extractors. Preprint 2005.

[5] A. Canteaut, M. Daum, H. Dobbertin and G. Leander. *Normal and Non Normal Bent Functions*. Proceedings of the Workshop on Coding and Cryptography 2003, pp. 91-100, 2003.

[6] A. Canteaut and M. Trabbia. *Improved fast correlation attacks using parity check equations of weight 4 and 5*. Advances in Cryptology - EUROCRYPT 2000, number 1805 in Lecture Notes in Computer Science, pp. 573-588. Springer-Verlag, 2000.

[7] C. Carlet. On the degree, nonlinearity, algebraic thickness and non-normality of Boolean functions, with developments on symmetric functions. *IEEE Transactions on Information Theory*, vol. 50, pp. 2178-2185, 2004.

[8] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, to appear in 2006. Prelimnary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html

[9] C. Carlet. On bent and highly nonlinear balanced/resilient functions and their algebraic immunities. Proceedings of AAECC 16, LNCS 3857, pp. 1-28, 2006.

[10] C. Carlet, D. Dalai, K. Gupta and S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. To appear in IEEE Transactions on Information Theory.

[11] C. Carlet and P. Gaborit. On the construction of balanced Boolean functions with a good algebraic immunity. Proceedings of BFCA (First Workshop on Boolean Functions: Cryptography and Applications), Rouen, France, March 2005, pp. 1-14. See also the extended abstract entitled "On the construction of balanced Boolean functions with a good algebraic immunity" in the proceedings of ISIT 2005.

[12] C. Carlet and S. Mesnager. Improving the upper bounds on the covering radii of binary Reed-Muller codes. C. Carlet et S. Mesnager. To appear in IEEE Transactions on Information Theory, 2006.

[13] N. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology - CRYPTO 2003*, number 2729 in Lecture Notes in Computer Science, pages 176–194. Springer Verlag, 2003.

[14] N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology - EUROCRYPT 2003*, number 2656 in Lecture Notes in Computer Science, pages 345–359. Springer Verlag, 2003.

[15] D. K. Dalai, K. C. Gupta and S. Maitra. Results on Algebraic Immunity for Cryptographically Significant Boolean Functions. Indocrypt 2004, Chennai, India, December 20–22, pages 92–106, number 3348 in Lecture Notes in Computer Science, Springer Verlag, 2004

[16] D. K. Dalai, K. C. Gupta and S. Maitra. Cryptographically Significant Boolean functions: Construction and Analysis in terms of Algebraic Immunity. Fast Software Encryption 2005, to be published in Lecture Notes in Computer Science, Springer Verlag.

[17] F. Didier. A new upper bound on the block error probability after decoding over the erasure channel. Preprint available at http://www-rocq.inria.fr/codes/Frederic.Didier/
A revised version will appear in IEEE Transactions on Information Theory, 2006.

[18] C. Ding, G.-Z. Xiao and W. Shan. *The stability theory of stream ciphers*, vol. LNCS 561, Springer Verlag, 1991.

[19] H. Dobbertin. *Construction of bent functions and balanced Boolean functions with high nonlinearity.* Fast Software Encryption Proceedings of the 1994 Leuven Workshop on Cryptographic Algorithms, Lecture Notes in Computer Science 1008, Springer Verlag, pp. 61-74, 1995.

[20] S. Dubuc. *Etude des propriétés de dégénérescence et de normalité des fonctions booléennes et construction de fonctions q-aires parfaitement non linéaires.* PhD thesis, University of Caen, 2001.

[21] J. H. Evertse, *Linear structures in block ciphers*, Advances in Cryptology, EUROCRYPT' 87, Lecture Notes in Computer Science 304, pp. 249-266, Springer Verlag, 1988.

[22] L.R. Knudsen. *Truncated and higher order differentials.* Fast Software Encryption, Second International Workshop, Lecture Notes in Computer Science, n 1008. pp. 196–211. – Springer-Verlag, 1995.

[23] X. Lai. *Higher order derivatives and differential cryptanalysis.* Proc. "Symposium on Communication, Coding and Cryptography", in honor of J. L. Massey on the occasion of his 60'th birthday. 1994.

[24] M. Lobanov. Tight bound between nonlinearity and algebraic immunity. Paper 2005/441 in http://eprint.iacr.org/

[25] O. B. Lupanov. *On circuits of functional elements with delay.* Probl. Kibern. 23, pp. 43-81 , 1970.

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

[27] J.L. Massey. *Shift-register synthesis and BCH decoding.* IEEE Transactions on Information Theory, vol. 15, pp. 122–127, 1969.

[28] M. Matsui. *Linear cryptanalysis method for DES cipher.* Advances in Cryptology - EUROCRYPT'93, number 765 in Lecture Notes in Computer Science. Springer-Verlag, pp. 386-397, 1994.

[29] W. Meier and O. Staffelbach, *Nonlinearity Criteria for Cryptographic Functions*, Advances in Cryptology, EUROCRYPT' 89, Lecture Notes in Computer Science 434, pp. 549-562, Springer Verlag, 1990.

[30] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography.* CRC Press Series on Discrete Mathematics and Its Applications, 1996.

[31] W. Meier, E. Pasalic and C. Carlet. Algebraic attacks and decomposition of Boolean functions. In *Advances in Cryptology - EUROCRYPT 2004*, number 3027 in Lecture Notes in Computer Science, pages 474–491. Springer Verlag, 2004.

[32] D. Olejár and M. Stanek. *On cryptographic properties of random Boolean functions.* Journal of Universal Computer Science, vol. 4, No.8, pp. 705-717, 1998.

[33] N.J. Patterson and D.H. Wiedemann. *The covering radius of the* $[2^{15}, 16]$ *Reed-Muller code is at least 16276.* IEEE Trans. Inform. Theory, IT-29, pp. 354-356, 1983.

[34] N.J. Patterson and D.H. Wiedemann. *Correction to [33].* IEEE Trans. Inform. Theory, IT-36(2), pp. 443, 1990.

[35] V. S. Pless, W. C. Huffman, Eds, R. A. Brualdi, *Handbook of Coding Theory*, Amsterdam, the Netherlands: Elsevier, 1998.

[36] F. Rodier. On the nonlinearity of Boolean functions. *Proceedings of the Workshop on Coding and Cryptography 2003*, pp. 397-405, 2003.

[37] O. S. Rothaus. *On bent functions*, J. Comb. Theory, 20A, pp. 300-305, 1976.

[38] R. A. Rueppel *Analysis and design of stream ciphers* Com. and Contr. Eng. Series, Berlin, Heidelberg, NY, London, Paris, Tokyo, 1986

[39] C. E. Shannon. *A mathematical theory of communication.* Bell system technical journal, 27, pp. 379-423, 1948.

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

[41] C. E. Shannon. *The synthesis of two-terminal switching circuits.* Bell system technical journal, 28, pp. 59–98, 1949.

[42] I. Wegener. *The complexity of Boolean functions.* B.G. Teubner, Stuttgart. John Wiley and sons, 1987.

| $n$ | $AI(f)$ | $r$ |
|---|---|---|
| 13 | 7 | 3–4 |
| 14 | 7 | 3 |
| 15 | 8 | 2–5 |
| 16 | 8 | 3–5 |
| 17 | 8 | 3–4 |
| 17 | 9 | 2–6 |
| 18 | 8 | 3–4 |
| 18 | 9 | 2–6 |
| 19 | 8 | 3–4 |
| 19 | 9 | 2–6 |
| 19 | 10 | 2–7 |
| 20 | 9 | 3–5 |
| 20 | 10 | 2–7 |
| 21 | 9 | 3–5 |
| 21 | 10 | 2–7 |
| 21 | 11 | 2–8 |
| 22 | 9 | 3–5 |
| 22 | 10 | 2–7 |
| 22 | 11 | 2–8 |
| 23 | 9 | 3–5 |
| 23 | 10 | 3–7 |
| 23 | 11 | 2–8 |
| 23 | 12 | 2–9 |
| 24 | 9 | 4–5 |
| 24 | 10 | 3–6 |
| 24 | 11 | 2–8 |
| 24 | 12 | 2–9 |
| 25 | 9 | 4 |
| 25 | 10 | 3–6 |
| 25 | 11 | 2–8 |
| 25 | 12 | 2–9 |
| 25 | 13 | 2–10 |
| 26 | 10 | 3–6 |
| 26 | 11 | 3–8 |
| 26 | 12 | 2–9 |
| 26 | 13 | 2–10 |
| 27 | 10 | 3–6 |
| 27 | 11 | 3–7 |
| 27 | 12 | 2–9 |
| 27 | 13 | 2–10 |
| 27 | 14 | 2–11 |

Table 1: The few cases where the bound of [10] is better than the bound of Theorem 4, for $n \leq 27$