A lower bound on the higher order nonlinearity of algebraic immune functions

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

Abstract

We extend the lower bound, obtained by M. Lobanov, on the first order nonlinearity of functions with given algebraic immunity, into a bound on the higher order nonlinearities.

1 Introduction

Let n and r be positive integers such that $r \leq n$. The *r-th order nonlinearity* of a Boolean function $f : F_2^n \rightarrow F_2$ is the minimum Hamming distance $d(f,h) = |\{x \in F_2^n \,/\, f(x) \neq h(x)\}|$ between f and all functions h of algebraic degrees at most r, that is, whose algebraic normal forms $h(x) = \sum_{I\subseteq\{1,\dots,n\}} a_I \left(\prod_{i\in I} x_i\right)$; $a_I \in F_2$, are such that $\max\limits_{a_I\neq 0} |I| \leq r$. In this paper, 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 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 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 (first order) nonlinearity and the algebraic degree: the former is not sufficient for knowing the cryptographic behavior of a function (since we need for instance to know what is the algebraic degree to quantify the resistance to Berlekamp-Massey attack) and the latter is not sufficient either, since changing one single output bit, in a function of degree less than n, moves its degree to n, while it clearly does not much improve the cryptographic strength of the function.
The algebraic immunity of a Boolean function f quantifies the resistance of pseudo-random generators using it as a nonlinear function (with no memory) to the standard algebraic attack. It equals, cf. [13], the minimum algebraic degree of nonzero annihilators of f (that is, of those functions $g : F_2^n \rightarrow F_2$ whose products with f are null) or of $f+1$. It is denoted in this paper by $AI(f)$.

In [11], M. Lobanov has improved upon the lower bound obtained in [8], on the (first order) nonlinearity of functions with given algebraic immunity, which was: $nl(f) \geq \sum_{i=0}^{AI(f)-2} \binom{n}{i}$. He obtained that:

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

In the present paper, we extend this lower bound into a bound on the general r-th order nonlinearity. We obtain a bound which improves in a majority of cases (for reasonable numbers of variables) upon the lower bound obtained in [4], which was: $nl_r(f) \geq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i}$.

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

In the next lemma, we extend a result from [11], which dealt only with affine functions.

Lemma 1 *Let n, r and k be positive integers. Let h be an 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 $h(x) = x_1 x_2 \cdots x_r + k(x)$, where k has degree at most r and where the term $x_1 x_2 \cdots x_r$ 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 it has weight at least 1. For every $(u_{r+1}, \ldots, u_n) \in F_2^{n-r}$, let us 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 $g(x) = \sum_{\substack{u \in F_2^n \\ wt(u) \leq k}} a_u x^u$ 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 $An_k(h)$ equals the number of variables

of the system S, minus its rank, and is therefore upper bounded by $\sum_{i=0}^{k}\binom{n}{i}-\sum_{i=0}^{k}\binom{n-r}{i}$.
$\square$

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, $h+1$ is then the indicator of an $(n-r)$-dimensional flat (see e.g. [12]), and we may without loss of generality assume that $h(x)=x_1x_2\cdots x_r+1$. Then the elements of $An_k(h)$ are the products of $h(x)+1=x_1x_2\cdots x_r$ 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 1, that is, the value obtained by Lobanov.

3 The lower bound on the r-th order nonlinearity

Theorem 1 *Let f be a Boolean function in n variables and let r be a positive integer. The nonlinearity of order r of f satisfies:*

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

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 $f(h+1)$ and $(f+1)h$ satisfy $wt(f(h+1))+wt((f+1)h)=d$, we have $\min(wt(f(h+1)),wt((f+1)h))\leq d/2$. If $\min(wt(f(h+1)),wt((f+1)h))=wt(f(h+1))$, let $f_1=f$ and $h_1=h+1$. Otherwise, let $f_1=f+1$ 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: $\dim(An_k(f_1h_1))\geq\sum_{i=0}^{k}\binom{n}{i}-d/2$.
According to Lemma 1, we have $\dim(An_k(h_1))\leq\max_{j=1}^{r}\left(\sum_{i=0}^{k}\binom{n}{i}-\sum_{i=0}^{k}\binom{n-j}{i}\right)=\sum_{i=0}^{k}\binom{n}{i}-\sum_{i=0}^{k}\binom{n-r}{i}$.
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. $\square$

Remarks:
1. The bound of Theorem 1 improves upon the bound $nl_r(f) \geq \sum_{i=0}^{AI(f)-r-1} \binom{n}{i}$ of [4] for $r = 1$ (in which case it is Lobanov's bound) and for greater values of r as well, except when n is large, $AI(f)$ is large and r is neither small nor near $AI(f)-1$. For instance, the bound of Theorem 1 is better than the bound of [4] for every $n \leq 12$ and for every value of $AI(f)$ and r. We give in Table 1 at the end of the paper, for each value of $13 \leq n \leq 30$, the few values of $AI(f)$ and of r for which the bound of Theorem 1 is worse than the bound of [4].
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 (see e.g. [10, 2]) 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 Theorem 1, with $r \geq 2$, shows 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 linear attacks. Indeed, the complexity of such attacks increases fastly with the order.
3. If $r \geq AI(f)$, then the bound of Theorem 1 and the bound of [4] give no information; we have then no lower bound on $nl_r(f)$. But if f is balanced, we have an upper bound: as shown in [3], we have indeed $nl_r(f) \leq 2^{n-1} - 2^{n-r}$.

References

[1] F. Armknecht. Improving Fast Algebraic Attacks. In *FSE 2004*, number 3017 in Lecture Notes in Computer Science, pages 65–82. Springer Verlag, 2004.

[2] A. Canteaut and M. Trabbia. Improved fast correlation attacks using parity-check equations of weight 4 and 5. In *EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pages 573–588. Springer Verlag, 2000.

[3] C. Carlet. On bent and highly nonlinear balanced/resilient functions and their algebraic immunities. To appear in the proceedings of AAECC 16.

[4] C. Carlet, D. Dalai, K. Gupta and S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. Submitted.

[5] 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.

[6] 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.

[7] 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.

[8] 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

[9] 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.

[10] R. Forré. A fast correlation attack on nonlinearly feedforward filtered shift register sequences. *Advances in cryptology –EUROCRYPT '89, Lecture Notes in Comput. Sci.* 434, pp. 586-595, Springer, 1990.

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

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

[13] 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.

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 [4] is better than the bound of Theorem 1, for $n \leq 27$