Nonlinarity of Boolean functions and hyperelliptic curves
Eric Férard, François Rodier

To cite this version:
Eric Férard, François Rodier. Nonlinarity of Boolean functions and hyperelliptic curves. 2007. hal-00145890

HAL Id: hal-00145890
https://hal.science/hal-00145890
Preprint submitted on 11 May 2007

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Nonlinearity of Boolean functions
and hyperelliptic curves

Eric Férard, François Rodier

Boolean functions is an important tool in computer sciences. It is especially useful in private key cryptography for designing stream ciphers. For security reasons, and also because Boolean functions need also to have other properties than nonlinearity such as balancedness or high algebraic degree, it is important to have the possibility of choosing among many Boolean functions, not only bent functions, that is functions with the highest possible nonlinearity, but also functions which are close to be bent in the sense that their nonlinearity is close to the nonlinearity of bent functions. For \( m \) odd, it would be particularly interesting to find functions with nonlinearity larger than the one of quadratic Boolean functions (called almost optimal in [1]). This has been done for instance in the work of Patterson and Wiedemann [9] and also of Langevin-Zanotti [4].

Let \( q = 2^m \) and \( \mathbb{F}_{2^m} \) assimilated as a vector space to \( \mathbb{F}_2^m \). In this talk, we want to study functions of the form \( \text{Tr} G(x) \), where \( G \) is a polynomial on \( \mathbb{F}_{2^m} \) and Tr the trace of \( \mathbb{F}_{2^m} \) over \( \mathbb{F}_2 \).

For \( m \) even, many people got interested in finding bent functions of this form. To only mention the case of monomials, one can get the known cases (Gold, Dillon/Dobbertin, Niho exponents) in the paper of Leander [5].

For \( m \) odd, one might have expected that among the functions \( f : x \mapsto \text{Tr} G(x) \) where \( G \) is a polynomial of degree 7, there are some functions which are close to being bent in the previous sense. This happens not to be the case, but we will show that for \( m \) odd such functions have rather good nonlinearity or autocorrelation properties. We use for that recent results of Maisner and Nart [7] about zeta functions of supersingular curves of genus 2.

\* Université de Polynésie française, Tahiti; e-mail ferard@upf.pf
\dagger Institut de Mathématiques de Luminy – C.N.R.S. 163 avenue de Luminy, Case 907, Marseille Cedex 9, France; e-mail rodier@iml.univ-mrs.fr
On the other hand, vectorial Boolean functions are used in cryptography to construct block ciphers. An important criterion on these functions is a high resistance to the differential cryptanalysis. Nyberg has introduced the notion of almost perfect nonlinearity (APN) to study differential attacks. We relate this notion to the notion above, and we will give some criterion for a function not to be almost perfect nonlinear.

1 Preliminaries

1.1 Boolean functions

Let \( m \) be a positive integer and \( q = 2^m \).

**Definition 1.1** A Boolean function with \( m \) variables is a map from the space \( V_m = \mathbb{F}_q^m \) into \( \mathbb{F}_2 \).

A Boolean function is linear if it is a linear form on the vector space \( V_m \). It is affine if it is equal to a linear function up to addition of a constant.

1.2 Nonlinearity

**Definition 1.2** We call nonlinearity of a Boolean function \( f : V_m \rightarrow \mathbb{F}_2 \) the distance from \( f \) to the set of affine functions with \( m \) variables:

\[
\text{nl}(f) = \min_{h \text{ affine}} d(f, h)
\]

where \( d \) is the Hamming distance.

One can show that the nonlinearity is equal to

\[
\text{nl}(f) = 2^m - 1 - \frac{1}{2} \| \hat{f} \|_{\infty}
\]

where

\[
\| \hat{f} \|_{\infty} = \sup_{v \in V_m} \left| \sum_{x \in V_m} \chi(f(x) + v \cdot x) \right|
\]

where \( v \cdot x \) denote the usual scalar product in \( V_m \) and \( \chi(f) = (-1)^f \). It is the maximum of the Fourier transform of \( \chi(f) \) (the Walsh transform of \( f \)):

\[
\hat{f}(v) = \sum_{x \in V_m} \chi(f(x) + v \cdot x).
\]
Parseval identity can be written
\[ \|\hat{f}\|_2^2 = \frac{1}{q} \sum_{v \in V_m} \hat{f}(v)^2 = q \]
and we get, for \( f \) a Boolean function on \( V_m \):
\[ \sqrt{q} \leq \|\hat{f}\|_\infty \leq q. \]

1.3 The sum-of-square indicator

Let \( f \) be a Boolean function on \( V_m \). Zhang and Zheng introduced the sum-of-square indicator \([14]\), as a measure of the global avalanche criterion:
\[ \sigma_f = \frac{1}{q} \sum_{x \in V_m} \hat{f}(x)^4 = \|\hat{f}\|_4^4. \]

We remark that
\[ \|\hat{f}\|_2 \leq \|\hat{f}\|_4 \leq \|\hat{f}\|_\infty. \] (1)
Hence the values of \( \|\hat{f}\|_4 \) may be considered as a first approximation of \( \|\hat{f}\|_\infty \) and in some cases they may be easier to compute. The relationship of this function with non-linearity was studied by A. Canteaut et al.\([6]\).

2 The functions \( f : x \rightarrow \text{Tr}(G(x)) \) where \( G \) is a polynomial

2.1 Divisibility of \( \|\hat{f}\|_\infty \)

Let \( G(x) \) be the polynomial \( \sum_{i=0}^{s} a_i x^i \) with coefficients in \( \mathbb{F}_q \) and \( f \) the Boolean function \( \text{Tr} \circ G \).

Definition 2.1 The binary degree of \( G \) is the maximum value of \( \sigma(i) \) for \( 0 \leq i \leq s \), where \( \sigma(i) \) is the sum of the binary digits of \( i \).

One has the following proposition, due to C. Moreno and O. Moreno \([6]\).

Proposition 2.1 Let \( G \) be a polynomial with coefficients in \( \mathbb{F}_q \) and binary degree \( d \). Then \( \|\hat{f}\|_\infty \) is divisible by \( 2^{|\frac{m}{\pi}|} \).
2.2 Case where $G$ is a polynomial of binary degree 2

The $\|\hat{f}\|_\infty$ are multiple of $2^{\lceil \frac{m}{2} \rceil}$. Therefore, if $m$ is even $\|\hat{f}\|_\infty$ is a multiple of $q^{1/2}$, and if $m$ is odd, of $\sqrt{2q}$. In particular, if $m$ is odd, the spectral amplitude is higher or equal to $\sqrt{2q}$ which is equal to that of the quadratic Boolean functions, of the maximum rank.

3 The functions $f : x \to \text{Tr}(G(x))$ where $G$ is a binary polynomial of degree 3

One simply will study the case where $G$ is a binary polynomial of degree 2 to which one adds a monomial of degree 7:

$$G = a_7 x^7 + \sum_{i=0}^{s} b_i x^{2i+1}$$

where $a_7 \neq 0$ a polynomial of degree 7 with coefficients in $k$. We would like to evaluate $\|\hat{f}\|_4$ on $F_{2^m}$, for $f(x) = \text{Tr}(G(x))$ where $\text{Tr}$ indicates the function trace of $F_{q^n}$ on $F_2$:

$$\text{Tr}(x) = \sum_{i=0}^{m-1} x^{2^i}.$$ 

One obtains the simple expression of $\|\hat{f}\|_4$ (cf [10, 11]):

$$\|\hat{f}\|_4^4 = \sum_{x_1 + x_2 + x_3 + x_4 = 0} \chi(f(x_1) + f(x_2) + f(x_3) + f(x_4)) = q^2 + \sum_{\alpha \in k^*} X_\alpha$$

with

$$X_\alpha = \left( \sum_{x \in k} \chi \circ \text{Tr}(G(x) + G(x + \alpha)) \right)^2.$$

To compute $X_\alpha$, one can remark that the curve of equation $y^2 + y = G(x + \alpha) + G(x)$ is isomorphic to

$$y^2 + y = G(\alpha) + (a_7 \alpha^6 + a_7^{1/4} \alpha^{3/4} + a_7^{1/2} \alpha^{5/2} + \sum (b_i \alpha)^{2-i} + \sum b_i \alpha^{2i}) x + (a_7 \alpha^4 + a_7^{1/2} \alpha^{1/2}) x^3 + a_7 \alpha^2 x^5$$

which is an equation of a curve $C_1$ of genus 2 for $\alpha \neq 0$. One has

$$X_\alpha = (\# C_1 - q - 1)^2.$$

To compute $X_\alpha$, we will need results of Van der Geer - van der Vlugt and of Maisner - Nart.
3.1 Van der Geer and van der Vlugt theory

Let $C_1$ the curve with affine equation:

$$C_1 : y^2 + y = ax^5 + bx^3 + cx + d$$

with $a \neq 0$. Let $R$ be the linearized polynomial $ax^4 + bx^2 + c^2x$. The map

$$Q : k \rightarrow \mathbb{F}_2 \quad x \mapsto \text{Tr}(xR(x))$$

is the quadratic form associated to the symplectic form

$$k \times k \rightarrow \mathbb{F}_2 \quad (x,y) \mapsto < x, y >_R = \text{Tr}(xR(y) + yR(x)).$$

The number of zeros of $Q$ determines the number of points of $C_1$:

$$\#C_1(k) = 1 + 2\#Q^{-1}(0).$$

Let $W$ be the radical of the symplectic form $<,>_R$, and $w$ be its dimension over $\mathbb{F}_2$. The codimension of the kernel $V$ of $Q$ in $W$ is equal to 0 or 1.

**Theorem 3.1** *(van der Geer - van der Vlugt [13])*  
*If $V \neq W$, then $\#C_1(k) = 1 + q$.  
*If $V = W$, then $\#C_1(k) = 1 + q \pm \sqrt{2^wq}$.*

3.2 Values of $X_\alpha$

In [3], we study the factorization of $P$ which determines $V$ and $W$ (see Maisner-Nart [5]). Thanks to the work of van der Geer - van der Vlugt, we can compute the number of points of the curves $y^2 + y = G(x + \alpha) + G(x)$.

**Proposition 3.1** Suppose that $m$ is odd. Then

$$X_\alpha = 0 \quad \text{or} \quad 2q \quad \text{or} \quad 8q.$$

Let $\ell = a^{-1/3}\alpha^{-7/3}$. Then

$$X_\alpha = 8q \quad \text{if and only if} \quad \text{Tr} \ell = 0$$

and

$$X_\alpha = 8q \quad \text{if and only if} \quad \text{Tr} \ell = v + v^4 \quad \text{with} \quad \text{Tr} v = 0,$$


$$X_\alpha = 2q \quad \text{if and only if} \quad \text{Tr} \ell = 1$$

and

$$X_\alpha = 0 \quad \text{in the remaining cases}.$$
4 Evaluation of $\|\hat{f}\|_4$

**Proposition 4.1** The value of $\|\hat{f}\|_4$ on $\mathbb{F}_{2^m}$ when $m$ is odd and $f(x) = \text{Tr}(G(x))$ is such that

$$\|\hat{f}\|_4^4 - 3q^2 \leq 185.2^{s-1}q^{3/2}.$$

**Proof**

One can evaluate the number of $\alpha$ which gives each case of the preceding proposition. The proves of these evaluations are linked with the computations of exponential sums over the curve $v + v^4 = \gamma x^7$. We get

$$|\#\{\alpha \mid X_\alpha = 8q\} - \frac{1}{8}| \leq 23.2^{s-1}q^{1/2}$$

$$|\#\{\alpha \mid X_\alpha = 2q\} - \frac{1}{2}| \leq 3q^{1/2} + 1$$

One deduce easily the evaluation of $\|\hat{f}\|_4^4$. The details of the proof will appear in [3].

**Remark 4.1** This result is to be compared with proposition 5.6 in [10] where the distribution of $\|\hat{f}\|_4^4$ for all Boolean function is shown to be concentrated around $3q^2$.

5 Bound for $\|\hat{f}\|_\infty$

From the theorem, we can deduce some lower bounds for $\|\hat{f}\|_\infty$.

**Proposition 5.1** For the functions $f : x \rightarrow \text{Tr}(G(x))$ on $\mathbb{F}_{2^m}$ where $G$ is the polynomial $G = a_7x^7 + \sum b_i x^{2^i+1}$ and $m$ is odd one has, for $m \leq 11 + 2s$:

$$\sqrt{2q} \leq \|\hat{f}\|_\infty.$$

For $m \geq 15 + 2s$, one has moreover:

$$\sqrt{2q} < \|\hat{f}\|_\infty.$$

**Proof**

The evaluation of the number of $\alpha$ such that $\text{Tr} \ell = 1$ in proposition [3.1] gives:

$$2q^2 - 6q^{3/2} \leq \|\hat{f}\|_4^4.$$
As it is easy to show that 
\[ \|\hat{f}\|^4 \leq q\|\hat{f}\|^2_{\infty} \]
we get \( 2q - 6q^{1/2} \leq \|\hat{f}\|^2_{\infty} \) whence the result, as \( \|\hat{f}\|_{\infty} \) is divisible by \( 2^{\lceil m/3 \rceil} \).

The second inequality is a consequence of theorem 4.1.

**Remark 5.1** So \( f \) is not almost optimal (in the sense of \([3]\)), for \( m \geq 15 + 2s \).

### 6 APN Functions

Let us consider a function \( G : \mathbb{F}_q \rightarrow \mathbb{F}_q \).

**Definition 6.1** The function \( G \) is said to be APN (almost perfect nonlinear) if for every \( a \in \mathbb{F}_q^* \) and \( b \in \mathbb{F}_q \), there exists at most 2 elements of \( \mathbb{F}_q \) such that \( G(z + a) + G(z) = b \).

**Proposition 6.1** The function \( G : \mathbb{F}_q \rightarrow \mathbb{F}_q \)

\[ x \mapsto a_7x^7 + \sum_{0}^{s} b_ix^{2i+1} \]
is not APN for \( m \geq 13 + 2s \).

**Proof**

For \( \gamma \in \mathbb{F}_q \), consider the function \( f_\gamma(x) = \text{Tr}(G(\gamma x)) \). The proposition follows from proposition 4.1 and the following result from Chabaud-Vaudenay [3].

**Proposition 6.2** One has \( \sum_{\gamma \in \mathbb{F}_q^*} \sigma(f_\gamma) \geq 2q^2(q - 1) \).

The function \( G \) is APN if and only if the equality is true.

For \( s \leq 2 \), one can even say more. The following theorem [12] proves that the function \( G \) is not APN for \( m \geq 11 \).

**Theorem 6.1** Let \( G \) be a polynomial from \( \mathbb{F}_{2^m} \) to \( \mathbb{F}_{2^m} \), \( d \) its degree. Let us suppose that the curve \( X_\infty \) of equation

\[ \frac{x_0^d + x_1^d + x_2^d + (x_0 + x_1 + x_2)^d}{(x_0 + x_1)(x_2 + x_1)(x_0 + x_2)} = 0 \]
is smooth. Then if \( m \geq 6 \) and \( d < q^{1/6} + 3.9 \), \( G \) is not APN.

\[ 7 \]
References


