On the nonlinearity of Boolean functions

François Rodier

Institut de Mathématiques de Luminy – C.N.R.S.
Marseille – France
rodier@iml.univ-mrs.fr

1 Introduction

Boolean functions on the space $\mathbf{F}_2^m$ are not only important in the theory of error-correcting codes, but also in cryptography, where they occur in private key systems. In both cases, the properties of these systems depend on the nonlinearity of a Boolean function. The nonlinearity is linked to the covering radius of the Reed-Muller codes. It is also an important parameter for symmetric cryptosystems (cf. the thesis by C. Fontaine [8] or the recent papers by C. Carlet [2, 3]).

It is useful to have at one's disposal Boolean functions with highest nonlinearity as have shown W. Meier and O. Staffelbach in [12], and K. Nyberg in [14]. These functions have been studied in the case where m is even, and have been called "bent" functions (cf. J. Dillon [5]). For these, the nonlinearity is well known, we know how to construct several series of them, but we do not know yet their number, nor their classification (cf. works by Carlet, in particular the paper of C. Carlet and A. Klapper [4]).

In the case where m is odd, the situation is quite different. We do not know the value of the maximal nonlinearity except for $m = 3, 5, 7$, and we have only an asymptotic conjecture (cf. for instance P. Langevin [10]).

In this article, I want to show that one can get some insight in this theory from the study of random polynomials, which have been a subject of study since as far as the works of Paley and Zygmund. Indeed, the problem of the research of the maximum of the nonlinearity comes down to minimize the Fourier transform of Boolean functions. It is a problem analogous to Fourier series on the real torus, where one wants to minimize the transform of these functions on $\mathbf{Z}$ which take values ± 1 for a finite set (and 0 elsewhere), or one wants to minimize the values of polynomials with coefficients ± 1 (random polynomials) on the set of complex numbers of module 1.

In this work, we have been inspired by the works of R. Salem and A. Zygmund [18] and by J-P. Kahane [9] on random polynomials, and we have transposed them on Boolean functions. In this way, we find an evaluation of the mean of the maximum of the absolute values of the Fourier transforms of Boolean functions, which is not very far from the theoretical minimum value $2^{m/2}$. This gives an evaluation of the average nonlinearity of these functions. We find again in particular the fact that most of the Boolean functions have a high nonlinearity, a result already proved recently by D. Olejar and M. Stanek [15] and independently by C. Carlet [3] (see theorem 4.1 and remark after it).

Moreover, by transposing a work of D. Newman and J. Byrnes [13] on the norms in L_4 of polynomials, we studied also a weaker conjecture about the *sum-of-square indicator* of

Boolean functions. This criterion has been introduced by Xian-Mo Zhang et Yuliang Zheng [19] and it is linked to propagation criterion for the Boolean functions. Its relation with nonlinearity has been studied in [1].

This paper is an extended abstract of the paper [17] which contains complete proofs of these results.

2 Preliminaries

2.1 Boolean functions

Let m be a positive integer and $q = 2^m$.

Definition 2.1 *A Boolean function with m variables is a map from the space $V_m = \mathbf{F}_2^m$ into $\mathbf{F}_2$.*

A Boolean function is linear if it is a linear form on the vector space $\mathbf{F}_2^m$. It is affine if it is equal to a linear function up to addition of a constant.

2.2 Nonlinearity

Definition 2.2 *We call nonlinearity of a Boolean function $f : V_m \longrightarrow \mathbf{F}_2$ the distance from f to the set of affine functions with m variables:*

$$nl(f) = \min_{h\ affine} d(f, h)$$

where d is the Hamming distance.

One can show that the nonlinearity is equal to

$$nl(f) = 2^{m-1} - \frac{1}{2} S(f)$$

where

$$S(f) = \max_{v \in V_m} \Big| \sum_{x \in V_m} (-1)^{(f(x)+v\cdot x)} \Big|$$

and $v \cdot x$ denote the usual scalar product in V_m. We call $S(f)$ the spectral amplitude of the Boolean function f.

2.3 The covering radius of the Reed-Muller code of the first order

This spectral amplitude is linked to the covering radius of the Reed-Muller code.

Indeed the Reed-Muller code $\mathcal{R}_m$ of order 1 on V_m is the vector space of affine Boolean functions on V_m. The covering radius r_m of the code is the highest nonlinearity of Boolean functions on V_m.

2.4 Known results, conjecture

The covering radius of the Reed-Muller code of the first order is well known. For an even dimension m, bent functions reach the lower bound $2^{m/2}$ of spectral amplitude. For odd m, $2^{m/2}\sqrt{2}$ has been a long time the only known lower bound of $S(f)$.

In 1983, Patterson and Wiedemann [16] have shown that one can do better for $m \geq 15$. They have exhibited a Boolean function f in V_{15} such that

$$S(f) = \frac{27}{32}\, 2^{15/2}\sqrt{2}.$$

They have conjectured that

$$\min_f S(f) \sim 2^{m/2} \tag{1}$$

2.5 Case of the torus on R

The Fourier series on the torus (that is on the group of complex numbers of module equal to 1) present an analogous problem. Let us replace the functions $x \longmapsto (-1)^{v\cdot x}$ for $v \in V_m$, which are characters of V_m by characters of the torus $x \longmapsto e^{isx}$ for $s \in \mathbf{Z}$.

An analogous conjecture is then

$$\lim_n \min \frac{\| \sum_0^n a_{s,n} e^{isx}\|_\infty}{\sqrt{n}} = 1$$

where $a_{s,n} = \pm 1$. So, it claims that there exists a sequence of polynomials $P_n(z) = \sum_{s=0}^n a_{s,n} z^s$ with $a_{s,n} = \pm 1$, and a sequence of positive numbers ϵ_n which tend to zero such that for all $|z| = 1$, $|P_n(z)| \leq (1+\epsilon_n)\sqrt{n}$.

Several authors such as J. E. Littlewood [11], and P. Erdös [7] have asked for the same problem. The latter has conjectured that on the contrary there exists $\delta > 1$ such that for all integer n and complex number z of module 1, one has $|P_n(z)| \geq \delta\sqrt{n}$. J-P. Kahane ([9]) solved the problem for complex coefficients $a_{s,n}$ of module 1. He has proved that in this case, $\lim_n \min \frac{\|P_n\|_\infty}{\sqrt{n}} = 1$. But nothing has been done for the initial problem. Moreover, Kahane used to solve this problem exponentials of the form $e^{\pi i n^2/a}$. He then works out a polynomial which solves almost the problem and he adjusts this polynomial by using a probabilistic argument. The exponentials Kahane uses are exponentials of quadratic forms in n, but in our case they do not give any complete result for odd dimensions m.

3 The space of Boolean functions with an infinity of variables

To study asymptotically Boolean functions, we will need the notion of Boolean functions with an infinity of variables and we will introduce a probability measure on them to be able to state almost sure results.

3.1 The space $\mathcal{B}$

We recall that $V_m = \mathbf{F}_2^m$. We define V_∞ as being the space of infinite sequences of elements of $\mathbf{F}_2$ which are almost all equal to zero. We define then $\mathcal{B}_m$ as being the algebra of Boolean

functions on V_m and $\mathcal{B} = \mathcal{B}_\infty$ as being the algebra of Boolean functions on V_∞. We have the restriction mappings

$$\pi_m : \mathcal{B}_\infty \longrightarrow \mathcal{B}_m : f \longmapsto f_m = f \mid_{V_m} .$$

We will consider the equiprobability on $\mathcal{B}_m$ and we will endow $\mathcal{B}$ with a probability which will be the Haar measure on it with total mass 1. In other words, for each $f \in \mathcal{B}_m$, the probability of the event $\pi_m^{-1} f = \{g \in \mathcal{B} \mid g \mid_{V_m} = f\}$ is given by

$$\underline{\mathrm{P}}(\pi_m^{-1} f) = \frac{1}{2^q}$$

where $q = |V_m| = 2^m$.

4 Distribution of $S(f)$

We have by Parseval identity, for $f \in \mathcal{B}_m$:

$$\sqrt{q} \leq S(f) \leq q$$

We will show that in fact $S(f)$ is rather close to $\sqrt{q}$.

4.1 Upper bound of $S(f)$

The following result shows that few Boolean function have a high spectral amplitude.

Theoreme 4.1 *If f is a Boolean function on V_m, and η a positive real, one has*

$$\underline{P}\left(S(f) \geq (1+\eta)\sqrt{2q \ln q}\right) \leq \frac{1}{q^{2\eta}}.$$

Remark 4.1 *This theorem is a particular case of a theorem by J-P. Kahane (Theorem 1, Chapter 6 in [9]) which we have stated here in the case of Boolean function with optimized constants. Recently, Olejar and Stanek in one hand, and Carlet in the other hand proved this result by independent proofs, using approximations of sums of binomial coefficients [15, 3].*

Corollary 4.1 *We have almost surely*

$$\limsup_q \frac{S(f_m)}{2^{m/2}\sqrt{m}} \leq \sqrt{2 \ln 2}$$

where f is in the space $\mathcal{B}$.

4.2 Lower bound of $S(f)$

The following theorem shows that the spectral amplitudes of most Boolean functions are not too small. It is inspired by Salem and Zygmund [18] who deal with the real torus.

Theoreme 4.2 *If f is a Boolean function on V_m, for all η such that $0 < \eta < 0.2$ there exists a constant B positive and depending only of η such that*

$$\underline{P}\left(S(f) < \left(\frac{1}{2} - 2\eta\right)\sqrt{q \ln q}\right) < \frac{B}{q^\eta}$$

Corollary 4.2 *We have almost surely*

$$\liminf_m \frac{S(f_m)}{2^{m/2}\sqrt{m}} \geq \frac{\sqrt{\ln 2}}{2}$$

where f is in the space $\mathcal{B}$.

4.3 Sketches of the proofs

Here I explain the main ideas of the proof. Complete proofs can be found in [17].

They come from the following three ingredients. We denote by $\mathcal{E}(X)$ the expectation of a random variable X on $\mathcal{B}_m$.

- If X is a positive square integrable random variable, if $0 < a < 1$ and $b > 1$, one gets these simple formulas (see for instance [9], Chapter 1):

$$(1-a)^2 \frac{\mathcal{E}^2(X)}{\mathcal{E}(X^2)} \leq \underline{\mathrm{P}}\Big(X \geq a\mathcal{E}(X)\Big) \tag{2}$$

$$\underline{\mathrm{P}}\Big(X \geq b\mathcal{E}(X)\Big) \leq \frac{1}{b}. \tag{3}$$

- In the previous relations, we take $X = \exp \lambda S(f)$. We have to estimate $\mathcal{E}(\exp \lambda S(f))$. We first introduce

$$\widehat{\chi_f}(u) = \sum_{x \in V_m} (-1)^{(f(x)+u\cdot x)} \quad \text{and} \quad I_q = \frac{1}{q}\sum_u \exp(\lambda \widehat{\chi_f}(u)). \tag{4}$$

  We can compare $\mathcal{E}(I_q)$ with $\mathcal{E}(\exp \lambda S(f))$:

$$\mathcal{E}(I_q) \leq \mathcal{E}(\exp \lambda S(f)) \leq 2q\mathcal{E}(I_q).$$

  The first inequality is obvious, the second comes from the fact that $S(f) = \widehat{\chi_f}(u)$ or $-\widehat{\chi_f}(u)$ for at least one value of $u \in V_m$.

- One can compute the expectation of $\exp(\lambda\widehat{\chi_f}(u))$, using the fact that the random variables $\exp(\lambda(-1)^{(f(x)+u\cdot x)})$ (on the space $\mathcal{B}_m$) are independent:

$$\mathcal{E}(\exp(\lambda\widehat{\chi_f}(u))) = \prod_{x\in V_m} \mathcal{E}(\exp(\lambda(-1)^{(f(x)+u\cdot x)})) = \prod_{x\in V_m} \cosh(\lambda).$$

  From this, one gets by elementary computations:

$$\exp\Big(\frac{\lambda^2 q}{2} - \lambda^4 q\Big) \leq \mathcal{E}(I_q) \leq \exp\left(\frac{\lambda^2 q}{2}\right);$$

  One gets in the same way

$$\mathcal{E}(I_q^2) \leq \Big(1 + \frac{\exp\left(q\lambda^2\right)}{q}\Big)\exp\left(q\lambda^2\right).$$

4.3.1 Proofs of upper bound

We plug in these estimations into relation (3) to get

$$\underline{\mathrm{P}}\Big(\exp\left(\lambda S(f)\right) \geq 2qb\exp\left(q\lambda^2/2\right)\Big) \leq \frac{1}{b}$$

A good choice of the parameter λ leads to the proof.

4.3.2 Proofs of lower bound

In this case, we have to plug in the estimations of $\mathcal{E}(\exp\lambda S(f))$ into relation (2):

$$(1-a)^2\frac{\exp\left(\lambda^2 q - 2\lambda^4 q\right)}{\left(1+\frac{\exp(q\lambda^2)}{q}\right)\exp\left(q\lambda^2\right)} \leq \underline{\mathrm{P}}\Big(\exp\lambda S(f) \geq a\exp\left(\frac{\lambda^2 q}{2} - \lambda^4 q\right)\Big)$$

whence

$$(1-2a)\exp\left(-2\lambda^4 q\right)\Big(1-\frac{\exp\left(q\lambda^2\right)}{q}\Big) \leq \underline{\mathrm{P}}\Big(S(f) \geq \frac{\ln a}{\lambda} + \frac{\lambda q}{2} - \lambda^3 q\Big)$$

if $\frac{\exp(q\lambda^2)}{q} < 1$. Again a good choice of the parameter λ leads to the proof.

4.3.3 Proofs of the corollaries

One uses the Borel-Cantelli lemma (cf. [9], § 1.6).

5 The sum-of-square indicator

Let us go back using an idea of D. Newman and J. Byrnes [13]. They have remarked that, in the case of Fourier series on $\mathbf{Z}$, the norm in L^4 of $\sum_n \pm e^{int}$ had a nice expression. It is the same for Boolean functions. For f a Boolean function on V_m, let us denote

$$\sigma_f = \frac{1}{q}\sum_{x\in V_m} \widehat{\chi_f}(x)^4 = \|\widehat{\chi_f}\|_4^4$$

where $\widehat{\chi_f}$ is defined in (4). It happens to be the sum-of-square indicator introduced by Zhang and Zheng [19]. We remark that $2^{2m} \leq \sigma_f \leq S(f)^4$. Consequently, the conjecture (1) implies a weaker conjecture:

Conjecture 5.1 *If f runs over the Boolean functions on V_m, one has*

$$\lim_m \min_{f\in V_m} \frac{\sigma_f}{2^{2m}} = 1.$$

We have the following simple expression for σ_f.

Lemme 5.1 *If f is a Boolean function on V_m,*

$$\sigma_f = q^2 + \sum_{\substack{a\neq 0\\ a\in V_m}} X_a \qquad \textit{with} \qquad X_a = \left(\sum_{x\in V_m} (-1)^{f(x)+f(x+a)}\right)^2$$

5.1 Distribution of σ_f

From lemma 5.1, one can compute the expectations $\mathcal{E}(\sigma_f)$ and $\mathcal{E}(\sigma_f^2)$. This computation reduces to the computation of expressions like $\mathcal{E}\left((-1)^{f(x_1)+f(x_2)+f(x_3)+\cdots+f(x_r)}\right)$ for $x_i \in V_m$.

Lemme 5.2 *One has*

$$\mathcal{E}\left((-1)^{f(x_1)+f(x_2)+f(x_3)+\cdots+f(x_r)}\right) = 0 \quad or \quad 1.$$

The expectation $\mathcal{E}\left((-1)^{f(x_1)+f(x_2)+f(x_3)+\cdots+f(x_r)}\right)$ *is equal to 1 if and only if for every* $y \in \mathbf{F}_2^n$ *there is an even number of* x_i *equal to* y*, that is if and only if there exists a partition of* $\{x_1, x_2, x_3, \ldots, x_r\}$ *in sets containing two equal elements.*

From this lemma, one gets

Proposition 5.1 *If* f *is a Boolean function on* V_m *then*

$$\begin{aligned} \mathcal{E}(\sigma_f) &= 3q^2 - 2q; \\ \mathcal{E}(\sigma_f^2) &\leq 64q - 100q^2 + 28q^3 + 9q^4. \end{aligned}$$

Using these expectations one can prove the following proposition, using the inequality of Bienaymé-Tchebicheff (See for instance [9], § 1.6.).

Proposition 5.2 *If* f *is a Boolean function on* V_m*, and* t *a positive real number,*

$$\underline{P}\left(\left|\frac{\sigma_f}{q^2} - 3 + \frac{2}{q}\right| \geq t\right) \leq \frac{40}{t^2 q}$$

Corollary 5.1 *If* $f \in \mathcal{B}$*, one has almost surely* $\lim_m \frac{\sigma_{f_m}}{2^{2m}} = 3.$

5.2 Asymptotic results

From lemma 5.1, we have

$$\frac{\sigma_f}{q^2} - 1 = \frac{1}{q}\sum_{a \neq 0} Y_a$$

with $Y_a = \frac{1}{q} X_a$. We can prove an asymptotical result about the distribution of the random variable Y_a, but we have only a conjecture about the distribution of σ_f.

5.2.1 Convergence of the distribution of the random variable Y_a

Using the fact that the random values $(-1)^{f(x)+f(x+a)}$ are independent on the hyperplane orthogonal to a, we deduce that the distribution of $\frac{1}{\sqrt{q}} \sum_{x \in \mathbf{F}_2^m} (-1)^{f(x)+f(x+a)}$ converge in law to a gaussian law. We deduce a limit for its square.

Proposition 5.3 *The distribution of* $Y_a = \frac{1}{q} X_a$ *converges in law to the distribution of density*

$$\frac{1}{2\sqrt{\pi x}} e^{-x/4} \mathbf{1}_{(x>0)}.$$

5.2.2 A conjecture about the distribution of σ_f

By the previous proposition, the random variables Y_a have almost the same distribution. They seem to be almost independent. In view of the central limit theorem, one may therefore conjecture, that the sequence $\frac{1}{\sqrt{q}} \sum_{a \neq 0} Y_a$ converges in law to the Gaussian law $\mathcal{N}(0, 40)$ with density $\frac{1}{\sqrt{80\pi}} e^{-x^2/80}$.

This conjecture and the conjecture that $\lim_m \min_{f \in V_m} \frac{\sigma_f}{2^{2m}} = 1$ would follow from a better understanding of $\mathcal{E}(\sigma_f^n)$, or of the $\mathcal{E}(X_{a_1}^{p_1} \dots X_{a_q}^{p_q})$. Indeed let us define

$$\phi_q(u) = \frac{1}{q} \ln \mathcal{E}\left(\exp\left(u \sum_{a \neq 0} Y_a \right) \right)$$

If we prove that $\phi(u) = \lim_{q \to \infty} \phi_q(u)$ exists for every $u \in \mathbf{R}$ (infinite values are allowed) plus some technical conditions, we would deduce by a theorem on large deviation [6], the conjecture 5.1, that is for given ϵ, for every q large enough, there exists f such that

$$\frac{\sigma_f}{q^2} - 1 < \epsilon.$$

References

[1] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine *Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions,* Advances in cryptology, EUROCRYPT 2000 (Bruges), 507–522, Lecture Notes in Comput. Sci., Vol. 1807, Springer, Berlin, 2000.

[2] C. Carlet, *On cryptographic complexity of Boolean functions*, Proceedings of the Sixth Conference on Finite Fields with Applications to Coding Theory, Cryptography and Related Areas. Springer, G.L. Mullen, H. Stichtenoth and H. Tapia-Recillas Eds, pp. 53-69, 2002.

[3] C. Carlet, *On the algebraic thickness and non-normality of Boolean functions, with developments on symmetric functions*, submitted to IEEE Trans. Inform. Theory.

[4] C. Carlet and A. Klapper, *Upper bounds on the numbers of resilient functions and of bent functions, Springer-Verlag*, Lecture Notes dedicated to Philippe Delsarte (to appear).

[5] J. Dillon, *Elementary Hadamard Difference sets*, Ph.D. thesis, University of Maryland, 1974.

[6] A. Dembo, O. Zeitouni, *Large deviations techniques and applications* Applications of Mathematics, 38. Springer-Verlag, New York, 1998.

[7] P. Erdös, *Some unsolved problems*, Michigan Math. J. 4 (1957), 291–300.

[8] C. Fontaine, *Contribution à la recherche de fonctions booléennes hautement non linéaires et au marquage d'images en vue de la protection des droits d'auteur*, Thèse, Université Paris VI, 1998.

[9] J-P. Kahane, *Some random series of functions*, Cambridge Studies in Advanced Mathematics, 5. Cambridge University Press, Cambridge-New York, 1985.

[10] P. Langevin, *Les sommes de caractères et la formule de Poisson dans la théorie des codes, des séquences et des fonctions booléennes*, Habilitation à Diriger les Recherches, Université de Toulon et du Var, 1999,
`http://www.univ-tln.fr/~langevin/`

[11] J. Littlewood, *On polynomials* $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta_i}$, J. London Math. Soc. 41 (1966), 367–376.

[12] W. Meier and O. Staffelbach, *Nonlinear criteria for cryptographic functions*, Advances in Cryptology, EUROCRYPT 89, Lecture Notes in Computer Science, vol. 434, J. J. Quisquater, J. Vandewalle eds., Springer-Verlag, (1990) p. 549–562.

[13] D. Newman et J. Byrnes, *The* L^4 *norm of a polynomial with coefficients* ± 1, Amer. Math. Monthly 97 (1990), no. 1, 42–45

[14] K. Nyberg, *Perfect nonlinear S-boxes*, Advances in Cryptology, Proc. Workshop, EUROCRYPT '91, Brighton/UK 1991, Lect. Notes Comput. Sci. 547 (1991), 378-386.

[15] D. Olejar, and M. Stanek, *On cryptographic properties of random Boolean functions* J .UCS 4 n° 8,(1998), 705–717.

[16] N. Patterson and D. Wiedemann, *The covering radius of the* $(2^{15}, 16)$ *Reed-Muller code is at least* 16 276, IEEE Trans. Inform. Theory 29, n° 3 (1983), 354–356.

[17] F. Rodier, *Sur la non-linéarité des fonctions booléennes*, submitted to Acta Arithmetica (2002), preprint:
`http://iml.univ-mrs.fr/editions/preprint2002/preprint2002.html`.

[18] R. Salem, A. Zygmund *Some properties of trigonometric series whose terms have random signs*, Acta Math. 91 (1954), 245–301

[19] Xian-Mo Zhang and Yuliang Zheng, *GAC —the Criterion for Global Avalanche Characteristics of Cryptographic Functions*, Journal of Universal Computer Science, vol. 1, no. 5 (1995), 316-333