Des Codes Crypt (2006) 40:59–70
DOI 10.1007/s10623-005-6363-8

Asymptotic nonlinearity of Boolean functions

François Rodier

Received: 30 March 2005 / Revised: 22 November 2005 /
Accepted: 28 November 2005
© Springer Science+Business Media, LLC 2006

Abstract Boolean functions on the space $\mathbb{F}_2^m$ are not only important in the theory of error-correcting codes, but also in cryptography. In these two cases, the nonlinearity of these functions is a main concept. Carlet, Olejár and Stanek gave an asymptotic lower bound for the nonlinearity of most of them, and I gave an asymptotic upper bound which was strictly larger. In this article, I improve the bounds and get an exact limit for the nonlinearity of most of Boolean functions. This article is inspired by a paper of G. Halász about the related problem of real polynomials with random coefficients.

Keywords Error correcting code · Cryptography · Nonlinearity · Boolean function · Fourier transform

AMS Classification (2000) Primary: 11T71 · Secondary: 06E30 · 42A05 · 94C10

1. Introduction

The nonlinearity of a Boolean function $f:\mathbb{F}_2^m \longrightarrow \mathbb{F}_2$ is the distance from f to the set of affine functions with m variables (see Section 2.2). It is an important concept. It occurs in cryptography (cf. [1, 2, 4]) to construct strong cryptosystems (symmetric ciphers), and in coding theory with the old problem of the covering radius of the first order Reed–Muller codes (cf. [3, 8]).

The nonlinearity is bounded above by $2^{m-1} - 2^{m/2-1}$. This bound is reached by bent functions [6, Ch. 14. Section 5, Theorem 6] which exist only if the number of variables m of the Boolean functions is even. Except the paper by Chuan-Kun Wu [11] who studies the distribution of Boolean functions with nonlinearity $\leq 2^{m-2}$, the distribution of nonlinearity was not known until there appeared papers by Carlet [1, 2] and independently Olejár and Stanek [7] who proved that most of the Boolean functions have a nonlinearity greater than

Communicated by J.D. Key.

F. Rodier (✉)
Institut de Mathématiques de Luminy – C.N.R.S. Marseille – France
e-mail: rodier@iml.univ-mrs.fr

$2^{m-1} - 2^{m/2-1}\sqrt{2m\log 2}$. Then I got more precise results in [9, 10], proving that the nonlinearity of most of them was contained in the interval $[2^{m-1} - 2^{m/2-1}\sqrt{2m\log 2}, 2^{m-1} - 2^{m/2-2}\sqrt{m\log 2}]$.

Here I show that most of them have indeed a nonlinearity close to $2^{m-1} - 2^{m/2-1}\sqrt{2m\log 2}$ (see Section 3.3). For this, I use the link between random polynomials and nonlinearity of Boolean functions, already stressed in my previous papers, and ideas from a paper by Halász [5] which solves an analogous problem in the case of random polynomials. Using this method, we have to study the distribution of the spectral amplitude $S(f)$ of a Boolean function f, or rather that of a random variable η which measures the difference between $S(f)$ and $2^{m/2}\sqrt{2m\log 2}$, and to find clever estimations of the first two moments of η.

After some preliminaries in Section 2, I state the results in Section 3 and I leave some proofs for the following sections.

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 $V_m = \mathbb{F}_2^m$ into $\mathbb{F}_2$.

A Boolean function is linear if it is a linear form on the vector space $\mathbb{F}_2^m$. 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 $f{:}V_m \longrightarrow \mathbb{F}_2$ 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

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

where

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

and $v \cdot x$ denote the usual scalar product in V_m. We call $S(f)$ the *spectral amplitude* of the Boolean function f. It is just formed by taking the maximum of the absolute value of the Fourier transform of $(-1)^f$. This transform is also called Walsh, or Hadamard transform.

We will state the results in terms of spectral amplitude rather than nonlinearity, as it is linked to it by a simple formula (1).

2.3. The space of Boolean functions with an infinity of variables

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

We recall that $V_m = \mathbb{F}_2^m$. We define V_∞ as being the space of infinite sequences of elements of $\mathbb{F}_2$ 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 uniform probability $\underline{\mathrm{P}}$ on $\mathcal{B}_m$ and we will endow $\mathcal{B}$ with a probability still denoted $\underline{\mathrm{P}}$ such that, for each $f \in \mathcal{B}_m$, the probability of the event $\pi_m^{-1} f$, which is the set of those elements h of $\mathcal{B}$ such that $h \mid_{V_m} = f$, is equal to $\frac{1}{2^q}$ where $q = |V_m| = 2^m$. In other words, the probability on $\mathcal{B}$ is the Haar measure on it with total mass 1.

2.4. Fourier transform of Boolean functions

As usual I call a character of V_m an homomorphism from the additive group of V_m to the group of multiplicative complex numbers. It is a function μ on V_m with complex values which is of the form

$$\mu(x) = (-1)^{x \cdot y}$$

where y is a given element of V_m. Let us denote by $\widehat{V_m}$ the set of characters of V_m. The preceding relation shows that it is isomorphic as a group to V_m.

The Fourier transform is defined on the set of functions on V_m with complex values: to the function f on V_m into $\mathbb{C}$, there corresponds a function $\widehat{f}$ on $\widehat{V_m}$ into $\mathbb{C}$ by

$$\widehat{f}(\mu) = \sum_{x \in V_m} f(x)\mu(x)$$

if μ runs in $\widehat{V_m}$. One has

$$f(x) = \frac{1}{q} \sum_{\mu \in \widehat{V_m}} \widehat{f}(\mu)\mu(x)$$

which will be denoted by $\int_{\mu \in \widehat{V_m}} \widehat{f}(\mu)\mu(x) d\mu$ to remind us that the space $\widehat{V_\infty}$ of characters of V_∞ is no more discrete.

3. Distribution of the spectral amplitude $S(f)$

3.1. Some auxiliary functions

For f a Boolean function on V_m, we have

$$S(f) = \max_{y \in V_m} \left| \sum_{x \in V_m} (-1)^{(f(x) + y \cdot x)} \right| = \|\widehat{\chi_f}\|_\infty,$$

where

$$\chi_f(x) = (-1)^{f(x)}$$

denotes the sign function associated to the Boolean function f and $\|\widehat{\chi_f}\|_\infty$ is the maximum of the absolute value of the function $\widehat{\chi_f}$ on the set $\widehat{V_m}$.

We want to compare $\|\widehat{\chi_f}\|_\infty$ with some real number M that we choose such that

$$M = \sqrt{2q \log q}(1-\beta) \tag{2}$$

with $0 < \beta < 1/4$. We take $\Delta = \sqrt{\frac{q}{\log q}}$.

We pick a monotonous infinitely differentiable real function α on $[0,\ 1]$ such that $\alpha(0) = 0$, $\alpha(1) = 1$, and such that the derivatives $\alpha^{(p)}(0)$ and $\alpha^{(p)}(1)$ are 0 for every p. Then we construct a function u, such that $0 \le u(x) \le 1$ for every $x \in \mathbb{R}$ and

$$u(x) = \begin{cases} 0 & \text{if } |x| \le M; \\ \alpha\left(\frac{|x|-M}{\Delta}\right) & \text{if } M \le |x| \le M + \Delta; \\ 1 & \text{if } |x| \ge M + \Delta. \end{cases}$$

We define the random variable

$$\eta = \int_{\widehat{V_m}} u(\widehat{\chi_f}(\mu))d\mu.$$

The function u is the real Fourier transform of a measure U on $\mathbb{R}$:

$$u(x) = \int_{\mathbb{R}} \exp(itx)dU(t)$$

whence

$$\eta = \int_{\widehat{V_m}} \int_{\mathbb{R}} \exp(it\widehat{\chi}_f(\mu))dU(t)\,d\mu = \int_{\mathbb{R}} \int_{\widehat{V_m}} \exp(it\widehat{\chi}_f(\mu))d\mu\,dU(t).$$

3.2. Lower bound of $S(f)$

Let us note that if f is a Boolean function on V_m such that $S(f) \le M$, then $\eta = 0$. We have then to compute the probability for η to be 0. Tchebitcheff's inequality gives an estimation of the probability that η deviate from the value $\mathcal{E}(\eta)$ of its expectation.

Proposition 3.1 *One has*

$$\underline{P}(\eta = 0) \le \underline{P}(|\eta - \mathcal{E}(\eta)| \ge \mathcal{E}(\eta)) \le \frac{\mathcal{E}(\eta^2) - \mathcal{E}^2(\eta)}{\mathcal{E}^2(\eta)}.$$

So, we have to compute the expectation of η and of η^2.

Proposition 3.2 *One has the following estimations, for q tending to infinity,*

$$\begin{aligned} \mathcal{E}(\eta) &= \int_{\mathbb{R}} \exp\Big(-q\frac{t^2}{2}\Big)dU(t) + O\Big(\frac{\log^2 q}{q}\Big); \\ \frac{1}{\mathcal{E}(\eta)} &= O(q^{1-2\beta}\sqrt{\log q}); \\ \mathcal{E}(\eta^2) &\le \Big(\int_{\mathbb{R}} \exp\Big(-\frac{qt^2}{2}\Big)dU(t)\Big)^2 + \frac{\mathcal{E}(\eta)}{q} + O\Big(\frac{\log^5 q}{q^2}\Big). \end{aligned} \tag{3}$$

Proof The proposition is shown in Section 5. □

Proposition 3.3 *One has, if β is fixed*

$$\underline{P}(S(f) \leq M) \leq \underline{P}(\eta = 0) = O\Big(\frac{1}{\log^2 q}\Big).$$

Proof By the previous propositions, one has

$$\underline{\mathrm{P}}(\eta = 0) \leq \frac{O(\mathcal{E}(\eta)\log^2 q/q) + O\left(\frac{\log^5 q}{q^2}\right)}{\mathcal{E}^2(\eta)} = \frac{O(\log^2 q)}{q\mathcal{E}(\eta)} + O\left(\frac{\log^5 q}{q^2\mathcal{E}^2(\eta)}\right)$$

We have, by the relation (3),

$$\frac{O(\log^2 q)}{q\mathcal{E}(\eta)} = O(q^{-2\beta}\log^{5/2} q)$$

and

$$O\Big(\frac{\log^5 q}{q^2\mathcal{E}^2(\eta)}\Big) = O(q^{-4\beta}\log^6 q).$$

This gives the desired conclusion. □

We then get the following asymptotic result.

Theorem 3.1 *If f is a Boolean function in $\mathcal{B}_\infty$, its restriction to V_m fulfills almost surely, for m big enough*:

$$S(f_m) > \sqrt{2q\log q}(1 - \beta).$$

Proof Indeed, summing up for $m \in \mathbb{N}$ both sides of the inequalities given by the previous proposition, we get

$$\sum_m \underline{\mathrm{P}}(S(f_m) \leq M) \leq O\left(\sum_m \frac{1}{m^2}\right) < \infty.$$

Borel-Cantelli's lemma tells us that almost surely $S(f_m) > M$ except for a finite number of m. □

3.3. Limit of $S(f)$

Theorem 3.2 *If f is a Boolean function in $\mathcal{B}_\infty$, then almost surely*:

$$\lim_{m\to\infty} \frac{S(f_m)}{\sqrt{2q\log q}} = 1.$$

Proof One uses the previous theorem, letting β tending to 0, and Corollary 4.1 of [9] (cf. also Corollary 4.1 of [10]) which gives an upper bound for the limit. □

Corollary 3.1 *If f is a Boolean function in $\mathcal{B}_\infty$, then almost surely*:

$$\lim_{m\to\infty} \frac{2^{m-1} - nl(f_m)}{2^{m/2-1}\sqrt{2m\log 2}} = 1.$$

3.4. Remark 1

One could with more work obtain a result like this one similar to Halácz's [5].

Theorem 3.3 *For almost every Boolean function f in $\mathcal{B}_\infty$, one has*

$$\left|\frac{S(f_m)}{2^{m/2}\sqrt{m}} - \sqrt{2\log 2}\right| \le C\frac{\log m}{m}$$

for m large enough, for some constant C.

3.5. Remark 2

The expression *almost surely* in Theorem 3.1 or 3.2 or in Corollary 3.1 and the expression *almost every* in Theorem 3.3 mean that the results are true only for f belonging to a set of $\mathcal{B}_\infty$ of measure 1.

4. Some estimations

The proofs of the following estimations of integrals in proposition 4.1 are similar to Halász's ones. I recall them for the convenience of the reader.

Proposition 4.1 *One has the following estimations:*

$$\int_{\mathbb{R}} |dU(t)| = O(\log q); \tag{4}$$

$$\int_{\mathbb{R}} |t|^p |dU(t)| = O\left(\frac{\log q}{q}\right)^{p/2} \quad \textit{for} \quad 1 \le p \le 8; \tag{5}$$

$$\left|\int_{\mathbb{R}} \exp\left(-\frac{qt^2}{2}\right) t^p\, dU(t)\right| = O\big(q^{-1+2\beta-p/2}\log^{p/2-1/2} q\big) \quad \textit{for} \quad 0 \le p \le 8. \tag{6}$$

Proof The measure U, as u is its Fourier transform, is the sum of the Dirac measure at the origin and of a measure whose density is the indefinitely differentiable function

$$v(t) = \frac{1}{2\pi}\int_{\mathbb{R}} (u(x) - 1)\exp(-itx)dx,$$

which is rapidly decreasing at infinity.

By using the fact that $u(x) = 1$ if $|x| \ge M + \Delta$ we get

$$|v(t)| \le \frac{1}{2\pi}\int_{|x|\le M+\Delta} |u(x) - 1|dx \le \frac{1}{\pi}(M + \Delta) = O(M). \tag{7}$$

The formula of Fourier transform of derivatives gives for $1 \le p \le 8$:

$$|2\pi t^p v(t)| \le \int_{\mathbb{R}} |u^{(p)}(x)|dx \le 2\Delta\|u^{(p)}(x)\|_\infty \le 2\|\alpha^{(p)}(x)\|_\infty \frac{1}{\Delta^{p-1}} = O\Big(\frac{1}{\Delta^{p-1}}\Big). \tag{8}$$

To prove the first two estimations of the Proposition 4.1, we split the integration interval in two pieces: $|t| \le \frac{1}{\Delta}$ and $|t| \ge \frac{1}{\Delta}$. For the first piece, we get an upper bound of $|t^p dU(t)|$ with (7) or (8). For the second, we get an upper bound of that expression with (8) for $p + 2$ and use it to obtain an estimation of the integral $\int_{|t|\ge\frac{1}{\Delta}} t^p |dU(t)|$.

To prove the third (6), we use the fact that the Fourier transform of the measure t^pU is $i^{-p}u^{(p)}(x)$ and that of $\exp(-\frac{q}{2}t^2)$ is $\sqrt{\frac{2\pi}{q}}\exp\left(-\frac{x^2}{2q}\right)$. By Parseval formula, we have

$$\Big|\int_{\mathbb{R}} \exp\left(-\frac{q}{2}t^2\right) t^p dU(t)\Big| = \frac{1}{\sqrt{2\pi q}}\Big|\int_{\mathbb{R}} \exp\left(-\frac{x^2}{2q}\right) u^{(p)}(x)dx\Big|$$
$$= O\left(\frac{1}{\Delta^p\sqrt{q}}\int_{|x|\geq M} \exp\left(-\frac{x^2}{2q}\right)dx\right)$$

and by using an estimation for the previous integral

$$= O\left(\frac{\sqrt{q}}{M\Delta^p}\exp\left(-\frac{M^2}{2q}\right)\right)$$
$$= O\left(q^{-1+2\beta-p/2}\log^{p/2-1/2}\right). \qquad \square$$

Remark 4.1 Actually we can check that we used the fact that the auxiliary function α was 8 times continuously differentiable, and not infinitely differentiable, as we supposed in the section just for simplicity.

5. Proof of Proposition 3.2

Lemma 5.1 *Let t be a real number and μ a character of $\mathbb{F}_2^m$, then, for f running in the space of Boolean functions on $\mathbb{F}_2^m$, one has, for x fixed in V_m :*

$$\mathcal{E}(\exp(it\chi_f(x)\mu(x))) = \cos(t).$$

Proof Half of Boolean function on V_m are such that $\chi_f(x)\mu(x) = 1$, half of them are such that $\chi_f(x)\mu(x) = -1$. □

Lemma 5.2 *For μ given, one has*

$$\mathcal{E}(\exp(it\widehat{\chi_f}(\mu))) = \exp\Big(-q\frac{t^2}{2}\Big) + O(qt^4)$$

for $|t| \leq 1$.

Proof As the random variables $\chi_f(x)$ are independent in x, we have

$$\mathcal{E}(\exp(it\widehat{\chi_f}(\mu))) = \mathcal{E}\bigg(\prod_{x\in\mathbb{F}_2^m} \exp\Big(it\chi_f(x)\mu(x)\Big)\bigg)$$
$$= \prod_{x\in\mathbb{F}_2^m} \mathcal{E}\bigg(\exp\Big(it\chi_f(x)\mu(x)\Big)\bigg) = \exp\Big(q\log(\cos t)\Big).$$

We have

$$\exp(q\log\cos t) = \exp\Big(-q\frac{t^2}{2}\Big) + O\Big(q\frac{t^2}{2} + q\log\cos t\Big)$$

by the relation $e^{-a} = e^{-b} + O(b-a)$ if $a, b \geq 0$ and

$$q\frac{t^2}{2} + q\log\cos t = O(qt^4)$$

by the expansion $\log\cos t = -\frac{t^2}{2} + O(t^4)$ if $|t| \leq 1$. □

5.1. Expectation of η

Lemma 5.3 *The expectation of η is such that*

$$\mathcal{E}(\eta) = \int_{\mathbb{R}} \exp\Big(-q\frac{t^2}{2}\Big)dU(t) + O(\log^2/q).$$

Proof One has

$$\mathcal{E}(\eta) = \int_{\mathbb{R}}\int_{\widehat{V}_m} \mathcal{E}(\exp(it\widehat{\chi_f}(\mu)))d\mu\, dU(t).$$

By first computing the integral over the interval $[-1,\ 1]$ and using the previous estimation which is independent of μ, we get

$$\begin{aligned}
&\int_{-1}^{1}\int_{\widehat{V}_m} \mathcal{E}(\exp(it\widehat{\chi_f}(\mu)))d\mu\, dU(t)\\
&\quad= \int_{-1}^{1}\int_{\widehat{V}_m} \exp\Big(-q\frac{t^2}{2}\Big)d\mu\, dU(t) + \int_{-1}^{1}\int_{\widehat{V}_m} O(qt^4)d\mu|dU(t)|\\
&\quad= \int_{-1}^{1} \exp\Big(-q\frac{t^2}{2}\Big)dU(t) + \int_{-1}^{1} O(qt^4)|dU(t)|\\
&\quad= \int_{\mathbb{R}} \exp\Big(-q\frac{t^2}{2}\Big)dU(t) + O\Big(\int_{\mathbb{R}} qt^4|dU(t)|\Big)
\end{aligned}$$

as $\int_{|t|>1} \exp\big(-q\frac{t^2}{2}\big)|dU(t)| = O\Big(\int_{|t|>1}|dU(t)|\Big) = O\Big(\int_{\mathbb{R}} qt^4|dU(t)|\Big)$. The integral, outside the interval $[-1,\ 1]$, is

$$\int_{|t|>1}\int_{\widehat{V}_m} \mathcal{E}(\exp(it\widehat{\chi_f}(\mu)))d\mu\, dU(t) = O\Big(\int_{|t|>1}|dU(t)|\Big) = O\Big(q\int_{\mathbb{R}} t^4|dU(t)|\Big)$$

whence

$$\mathcal{E}(\eta) = \int_{\mathbb{R}} \exp\Big(-q\frac{t^2}{2}\Big)dU(t) + O\Big(q\int_{\mathbb{R}} t^4|dU(t)|\Big). \tag{9}$$

We then use the estimations of the Proposition 4.1 to get the result. □

Lemma 5.4 *We have*

$$\frac{1}{\mathcal{E}(\eta)} = O(q^{1-2\beta}\sqrt{\log q})$$

Proof We have to estimate $\mathcal{E}(\eta)$. By the Lemma 5.3, we begin by an estimation of $\int_{\mathbb{R}}\exp(-q\frac{t^2}{2})dU(t)$. The real Fourier transform of $\exp(-q\frac{t^2}{2})$ is $\sqrt{\frac{2\pi}{q}}\exp(-\frac{x^2}{2q})$. By Parseval formula one has therefore

$$\int_{\mathbb{R}} \exp\Big(-q\frac{t^2}{2}\Big)dU(t) = \frac{1}{\sqrt{2\pi q}}\int_{\mathbb{R}} \exp\Big(-\frac{x^2}{2q}\Big)u(x)dx$$

We estimate this integral using

$$\int_{\mathbb{R}} \exp\Big(-\frac{x^2}{2q}\Big)u(x)dx \geq \int_{M+\Delta\leq|x|} \exp\Big(-\frac{x^2}{2q}\Big)dx.$$
$$\geq \frac{q}{2M+2\Delta}\exp\Big(-\frac{(M+\Delta)^2}{2q}\Big)$$

There is a constant C_1 such that this last terms is greater than

$$C_1\frac{q}{2M}\exp\Big(-\frac{M^2}{2q}\Big) = C_1\frac{\sqrt{q}}{2\sqrt{2\log q}(1-\beta)}q^{2\beta-1}$$

Therefore $\frac{1}{\sqrt{2\pi q}}\int_{\mathbb{R}}\exp\Big(-\frac{x^2}{2q}\Big)u(x)$ is bigger than the error term $O\Bigg(\frac{\log^2 q}{q}\Bigg)$ in the Lemma 5.3. Whence one has

$$\frac{1}{\mathcal{E}(\eta)} = O(q^{1-2\beta}\sqrt{\log q}).$$ □

5.2. Expectation of η^2

The computation of $\mathcal{E}(\eta^2)$ will be done in several steps. One decomposes η^2 in two integrals:

$$\eta^2 = \int_{\mu=\psi} u(\widehat{\chi_f}(\mu))u(\widehat{\chi_f}(\psi))d\mu\, d\psi + \int_{\mu\neq\psi} u(\widehat{\chi_f}(\mu))u(\widehat{\chi_f}(\psi))d\mu\, d\psi$$

where the integrals are computed for $\mu \in \widehat{V}_m$ and $\psi \in \widehat{V}_m$.

We evaluate the first term.

Lemma 5.5

$$\int_{\mu=\psi} u(\widehat{\chi_f}(\mu))u(\widehat{\chi_f}(\psi))d\mu\, d\psi \leq \frac{\eta}{q}.$$

Proof We simply remark that

$$\int_{\mu=\psi} u(\widehat{\chi_f}(\mu))u(\widehat{\chi_f}(\psi))d\mu\, d\psi = \int_{\mu=\psi} u^2(\widehat{\chi_f}(\mu))d\mu\, d\psi$$
$$= \frac{1}{q}\int_{V_m} u^2(\widehat{\chi_f}(\mu))d\mu \leq \frac{1}{q}\int_{V_m} u(\widehat{\chi_f}(\mu))d\mu = \frac{\eta}{q}.$$

□

For the other term, we first have by Fourier transform

$$\int_{\mu\neq\psi} u(\widehat{\chi_f}(\mu))u(\widehat{\chi_f}(\psi))d\mu\, d\psi = \int_{\mu\neq\psi}\int_{\mathbb{R}^2} \exp(i(t\widehat{\chi_f}(\mu) + r\widehat{\chi_f}(\psi)))dU(t)\, dU(r).$$

So we compute the expectation of the inner term $\exp(i(t\widehat{\chi_f}(\mu) + r\widehat{\chi_f}(\psi)))$

Lemma 5.6 *For t and r of absolute value smaller than $\frac{1}{2}$, and for $\mu \neq \psi$,*

$$\begin{aligned}
&\mathcal{E}\Big(\exp\Big(i(t\widehat{\chi_f}(\mu)+r\widehat{\chi_f}(\psi))\Big)\Big)\\
&\quad=\exp\Big(-\frac{q}{2}(t^2+r^2)\Big)-\frac{q(t^4+6t^2r^2+r^4)}{12}\exp\Big(-\frac{q}{2}(t^2+r^2)\Big)\\
&\qquad+qO\Big((|t|+|r|)^6\Big)+q^2O\Big((|t|+|r|)^8\Big).
\end{aligned}$$

Proof We decompose the Fourier transforms on V_m and use the independence in x of the random variables $\chi_f(x)(t\mu(x)+r\psi(x))$:

$$\begin{aligned}
\mathcal{E}\Big(\exp\Big(i(t\widehat{\chi_f}(\mu)+r\widehat{\chi_f}(\psi))\Big)\Big)&=\mathcal{E}\Big(\prod_{x\in V_m}\exp\Big(i\chi_f(x)(t\mu(x)+r\psi(x))\Big)\Big)\\
&=\prod_{x\in V_m}\mathcal{E}\Big(\exp\Big(i\chi_f(x)(t\mu(x)+r\psi(x))\Big)\Big)\\
&=\prod_{x\in V_m}\cos(t\mu(x)+r\psi(x)).
\end{aligned}$$

By using the relations

$$e^{-a}=e^{-b}+(b-a)e^{-b}+O((b-a)^2)\quad\text{if}\quad a,b\geq 0 \tag{10}$$

and the expansion

$$\log\cos(z)=-\frac{z^2}{2}-\frac{z^4}{12}+O(z^6)\quad\text{if}\quad |z|\leq 1. \tag{11}$$

we get for $|t|<\frac{1}{2}$ and $|r|<\frac{1}{2}$, by taking $a=-\sum_x \ln(cos(t\chi(x)+r\psi(x)))$ and $b=\sum_x\frac{(t\chi(x)+r\psi(x))^2}{2}$:

$$\begin{aligned}
\mathcal{E}\Big(\exp\Big(i(t\widehat{\chi_f}(\mu)+r\widehat{\chi_f}(\psi))\Big)\Big)&=\exp\sum_{x\in V_m}\log\cos(t\mu(x)+r\psi(x))\\
&=\exp\Big(-\sum_{x\in V_m}\frac{(t\mu(x)+r\psi(x))^2}{2}\Big)\\
&\quad-\frac{1}{12}\sum_{x\in V_m}(t\mu(x)+r\psi(x))^4\\
&\quad\times\exp\Big(-\sum_{x\in V_m}\frac{(t\mu(x)+r\psi(x))^2}{2}\Big)\\
&\quad+qO\Big((t\mu(x)+r\psi(x))^6\Big)+q^2O\Big((t\mu(x)+r\psi(x))^8\Big).
\end{aligned}$$

One can do the following computation by noticing that $\mu\neq\psi$:

$$\sum_{x\in V_m}\frac{(t\mu(x)+r\psi(x))^2}{2}=\frac{q}{2}(t^2+r^2)$$

and

$$\sum_{x\in V_m}(t\mu(x)+r\psi(x))^4 = q(t^4+6t^2r^2+r^4)$$

and we get the result. □

We can use this result to compute the integral over $\mathbb{R}^2$ of

$$\mathcal{E}\Bigg(\exp\Big(i(t\widehat{\chi_f}(\mu)+r\widehat{\chi_f}(\psi))\Big)\Bigg).$$

Lemma 5.7

$$\begin{aligned}\mathcal{E}\Big(\int_{\mathbb{R}^2}\exp(i(t\widehat{\chi_f}(\mu)+r\widehat{\chi_f}(\psi)))dU(t)\,dU(r)\Big)\\ =\Big(\int_{\mathbb{R}}\exp(-\frac{q}{2}(t^2))dU(t)\Big)^2 + O\Big(\frac{\log^5 q}{q^2}\Big).\end{aligned}$$

Proof One uses the previous lemma. One benefits from the fact that outside of the square $|t|<\frac{1}{2}$, $|r|<\frac{1}{2}$ the term $\exp(i(t\widehat{\chi_f}(\mu)+r\widehat{\chi_f}(\psi)))$ is bounded in absolute value by 1. So one has

$$\begin{aligned}&\mathcal{E}\Big(\int_{\mathbb{R}^2}\exp(i(t\widehat{\chi_f}(\mu)+r\widehat{\chi_f}(\psi)))dU(t)\,dU(r)\Big)\\ &=\int_{-1/2}^{1/2}\int_{-1/2}^{1/2}\exp\Big(-\frac{q}{2}(t^2+r^2)\Big)dU(t)\,dU(r)\\ &-\frac{q}{12}\int_{-1/2}^{1/2}\int_{-1/2}^{1/2}(t^4+6t^2r^2+r^4)\exp\Big(-\frac{q}{2}(t^2+r^2)\Big)dU(t)\,dU(r)\\ &+qO\Big(\int_{\mathbb{R}^2}(|t|+|r|)^6dU(t)\,dU(r)\Big)+q^2O\Big(\int_{\mathbb{R}^2}(|t|+|r|)^8dU(t)\,dU(r)\Big)\\ &+O\Big(\int_{\substack{|t|\geq 1/2\\ \text{or } |r|\geq 1/2}}\int_{\mathbb{R}}dU(t)\,dU(r)\Big).\end{aligned}\tag{12}$$

We may neglect the integrals outside the square $[-\frac{1}{2},\ \frac{1}{2}]$: the change in the integrals is smaller than the error terms in the formula. So is the last term (12). Therefore one gets

$$\mathcal{E}\Big(\int_{\mathbb{R}^2}\exp(i(t\widehat{\chi_f}(\mu)+r\widehat{\chi_f}(\psi)))dU(t)\,dU(r)\Big)$$

$$=\int_{\mathbb{R}^2}\exp\Big(-\frac{q}{2}(t^2+r^2)\Big)dU(t)\,dU(r)$$

$$-\frac{q}{12}\int_{\mathbb{R}^2}(t^4+6t^2r^2+r^4)\exp\Big(-\frac{q}{2}(t^2+r^2)\Big)dU(t)\,dU(r)\tag{13}$$

$$+qO\Big(\int_{\mathbb{R}^2}(|t|+|r|)^6dU(t)\,dU(r)\Big)\tag{14}$$

$$+q^2O\Big(\int_{\mathbb{R}^2}(|t|+|r|)^8dU(t)\,dU(r)\Big).\tag{15}$$

One evaluates the three last terms by Proposition 4.1 to get the result. Indeed the term (13) is a sum of 3 terms of the form:

$$q\int_{\mathbb{R}}t^a\exp\Big(-\frac{q}{2}(t^2)\Big)dU(t)\int_{\mathbb{R}}r^b\exp\Big(-\frac{q}{2}(r^2)\Big)dU(t)\,dU(r)$$

with $a+b=4$, each of which are

$$qO\left(\frac{\log q}{q^4}q^{4\beta}\right)=O\left(\frac{\log^5 q}{q^2}\right)$$

if $\beta<1/4$. The term (14) is a sum of several terms of the form:

$$q\int_{\mathbb{R}}|t|^a\,dU(t)\int_{\mathbb{R}}|r|^b\,dU(r)$$

with $a+b=6$, each of which are $qO\left(\frac{\log^4 q}{q^3}\right)$. In the same way, the term (15) is a sum of several terms, each of which is $q^2O\left(\frac{\log^5 q}{q^4}\right)$. □

5.3. End of proof of Proposition 3.2.

One has to collect the results of Lemmas 5.5 and 5.7 with the remark made at the beginning of the previous section. □

References

1. Carlet C (2002). On cryptographic complexity of Boolean functions, In: Mullen GL, Stichtenoth H and Tapia-Recillas H (eds), Proceedings of the Sixth Conference on Finite Fields with Applications to Coding Theory, Cryptography and Related Areas Springer, pp 53–69
2. Carlet C (2004). On the degree, nonlinearity, algebraic thickness and non-normality of Boolean functions, with developments on symmetric functions IEEE Trans Inform Theory 50:2178–2185
3. Cohen G, Honkala I, Litsyn S, Lobstein A (1997). Covering codes. North-Holland Mathematical Library, 54, North-Holland Publishing Co., Amsterdam
4. Fontaine C (1998). 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
5. Halász G (1973). On a result of Salem and Zygmund concerning random polynomials, Studia Sci Math Hungar 8:369–377
6. MacWilliams FJ, Sloane NJA (1977). The theory of error-correcting codes, North-Holland, Amsterdam.
7. Olejár D, Stanek M (1998). On cryptographic properties of random Boolean functions, J.UCS 4(8):705–717
8. Patterson N, Wiedemann D (1983). The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16 276, IEEE Trans Inform Theory 29(3):354–356
9. Rodier F (2004). Sur la non-linéarité des fonctions booléennes. Acta Arithmetica 115:1–22; preprint: arXiv: math.NT/0306395
10. Rodier F (2003). On the nonlinearity of Boolean functions, In: Augot D, Charpin P, Kabatianski G (eds), Proceedings of WCC2003, Workshop on coding and cryptography 2003 INRIA pp 397–405.
11. Wu, Chuan-Kun (1998). On distribution of Boolean functions with nonlinearity $\leq 2^{n-2}$ Australas J Combin 17:51–59