Open access • Journal Article • DOI:10.1007/S12095-013-0090-1

Asymptotic nonlinearity of vectorial Boolean functions — Source link

Stéphanie Dib

Published on: 01 Jun 2014 - Cryptography and Communications (Springer US)

Asymptotic Nonlinearity of Vectorial Boolean Functions

Stephanie Dib

Asymptotic Nonlinearity of Vectorial Boolean Functions

Stéphanie DIB
Institut de Mathématiques de Luminy, Marseille, France

Abstract. We investigate the nonlinearity of functions from $\mathbb{F}_2^m$ to $\mathbb{F}_2^n$. We give asymptotic bounds for almost all these functions.

1 Introduction

Let m and n be two positive integers. Functions from the vectorspace $V_m = \mathbb{F}_2^m$ to the vectorspace $V_n = \mathbb{F}_2^n$, where $\mathbb{F}_2$ is the finite field with two elements, are called (m, n)-functions or more generally, vectorial Boolean functions. For a cryptographic use, such functions need to fulfill many criteria in order to ensure the robustness of the cryptosystems in which they are involved [1]. Among these criteria and one very important notion is the nonlinearity of these functions that must be as high as possible in order to resist to linear cryptanalysis. A (m, n)-function is affine if and only if it is a $\mathbb{F}_2$-linear map plus a constant. The nonlinearity $\mathcal{NL}(f)$ of a (m, n)-function f equals the minimum Hamming distance between all the component functions of f, that is $v.f$ where $v \in V_n^* = V_n \setminus \{0\}$, and all affine (m, n)-functions. It can be computed through the Walsh transform of these components. For a given $v \in V_n^*$, the Walsh transform of $v.f$ is the Fourier transform of $\chi_{v \cdot f}(x) = (-1)^{(v.f)(x)}$ the ± 1-representation of $v.f$. Let us denote by $\widehat{V}_m$ the set of characters of V_m. For every $\mu \in \widehat{V}_m$, we have

$$\widehat{\chi_{v \cdot f}}(\mu) = \sum_{x \in V_m} (-1)^{(v.f)(x)} \mu(x),$$

where $\mu(x) = (-1)^{x \cdot y}$ for some y in V_m. And the nonlinearity of f is

$$\mathcal{NL}(f) = 2^{m-1} - \frac{1}{2} \max_{\substack{v \in V_n^* \\ \mu \in \widehat{V}_m}} \left| \widehat{\chi_{v \cdot f}}(\mu) \right|.$$

Hence a function has high nonlinearity if all of its components Walsh values have low magnitudes. The covering radius bound is valid for every (m, n)-function

$$\mathcal{NL}(f) \leq 2^{m-1} - 2^{m/2-1}, \quad (1)$$

and can be achieved with equality only if m is even and $n \leq m/2$. For $n \geq m$, we have a better bound [4], and when n is sufficiently greater than m, other bounds are given in [2]. Finding better bounds than (1) in the other cases remains an open problem. Besides that, we don't have information about the distribution of the nonlinearity of (m, n)-functions. When $n = 1$, the distribution was studied by [8, 3, 10, 7].

In this paper, we propose asymptotic bounds which are valid for almost all (m, n)-functions. Let $0 < \beta < 1/4$, when m tends to infinity and $n \leq m$, we show in theorem 2.1 that the nonlinearity of almost all (m, n)-functions is bounded from above by $2^{m-1} - 2^{\frac{m-1}{2}}\sqrt{(m+n)\log 2}\,(1-\beta)$. And in theorem 3.1, we prove that for any positif real β, when $(m + n)$ tends to infinity and without any order for m and n, almost all (m, n)-functions have nonlinearity greater than $2^{m-1} - 2^{\frac{m-1}{2}}\sqrt{(m+n)\log 2}\,(1+\beta)$.

To obtain the first result, we use G. Halász method in [6] concerning random trigonometric polynomials. This work inspired F. Rodier [10] to prove that almost all m-variable Boolean functions ($(m, 1)$-functions) have nonlinearities in the neighbourhood of $2^{m-1} - 2^{m/2-1}\sqrt{2m\log 2}$. We use the same scheme of proof, however, it was necessary to take more precise approximations in the case of (m, n)-functions. As for the second result, it is a generalization of F. Rodier's result [9] on Boolean functions inspired by the work of R. Salem and A. Zygmund [11] on trigonometric series.

We begin by proving the lower bound of $\max\limits_{v \in V_n^*; \mu \in \widehat{V}_m} |\widehat{\chi_{v\cdot f}}(\mu)|$ which is more difficult.

2 The lower bound

Let $u(x)$, that will be completely constructed in section 2.3, be a function on $\mathbb{R}$ satisfying

$$0 \leq u(x) \leq 1 \quad \forall x \in \mathbb{R}, \quad u(x) = \begin{cases} 0 & \text{for} \quad |x| \leq M \\ 1 & \text{for} \quad |x| \geq M + \Delta, \end{cases}$$

where $M = 2^{\frac{m+1}{2}}\sqrt{(m+n)\log 2}(1-\beta)$ with $0 < \beta < 1/4$ and $\Delta = \sqrt{\frac{2^m}{\log 2^m}}$.
We consider the random variable η on the space of (m,n)-functions

$$\eta(f) = \int_{V_n^*}\int_{\widehat{V}_m} u\left(\widehat{\chi_{v.f}}(\mu)\right) d\mu dv,$$

where $d\mu$ (resp. dv) is a uniform measure over $\widehat{V}_m$ (resp. V_n^*) of total mass 1. $\eta(f) = 0$ is equivalent to $\max_{v\in V_n^*;\,\mu\in\widehat{V}_m} |\widehat{\chi_{v\cdot f}}(\mu)| \leq M$. When $n \leq m$, we shall prove by applying Chebyshev's inequality that this occurs with probability tending to 0 for large enough m.
The function $u(x)$ is the real Fourier transform of a measure U on $\mathbb{R}$

$$u(x) = \int_{\mathbb{R}} \exp\left(-2\pi i t x\right) dU(t).$$

Hence

$$\eta(f) = \int_{V_n^*}\int_{\widehat{V}_m}\int_{\mathbb{R}} \exp\left(-2\pi i t\, \widehat{\chi_{v.f}}(\mu)\right) dU(t) d\mu dv.$$

Before evaluating the first and second moment of η, some estimations are necessary but we chose to give the proof later. The following proposition is given in [6] and [10] but we repeat it for the reader's convenience.

Proposition 2.1. *When m tends to infinity, we have the following estimations:*

$$\int_{\mathbb{R}} |dU(t)| = O(m), \tag{2}$$

$$\int_{\mathbb{R}} |t|^p |dU(t)| = O\left(\frac{m}{2^m}\right)^{p/2} \quad for \quad 1 \leq p \leq 32, \tag{3}$$

$$\left|\int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2 t^2\right) t^p dU(t)\right| = O\left(2^{-m\frac{p}{2}-(m+n)(1-2\beta)} m^{p/2-1/2}\right) for 0 \leq p \leq 24. \tag{4}$$

Proof. See section 2.3.

2.1 Expectation of η

Lemma 2.1.

$$E(\eta) = \int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2 t^2\right) dU(t) + O\left(2^{-2m-n+2\beta(m+n)} m^{3/2}\right) + O\left(2^{-2m} m^4\right). \tag{5}$$

Proof. We have

$$E(\eta) = \int_{V_n^*} \int_{\widehat{V}_m} \int_{\mathbb{R}} E\left(\exp\left(-2\pi it\,\widehat{\chi_{v.f}}(\mu)\right)\right) dU(t) d\mu dv.$$

The random variables $\chi_{v.f}(x)\mu(x)$ are independent in x and take values $+1$ and -1 with probability $1/2$. Thus

$$\begin{aligned} E\left(\exp\left(-2\pi it\,\widehat{\chi_{v.f}}(\mu)\right)\right) &= E\Big(\prod_{x\in V_m} \exp\left(-2\pi it\chi_{v.f}(x)\mu(x)\right)\Big) \\ &= \prod_{x\in V_m} E\left(\exp\left(-2\pi it\chi_{v.f}(x)\mu(x)\right)\right) \\ &= \cos^{2^m}(2\pi t) \qquad (6) \\ &= \exp\Big(-2^{m+1}\pi^2t^2 - \frac{4}{3}\pi^4 2^m t^4\Big) + O(2^m t^6) \end{aligned}$$

for $|t| \le \frac{1}{3\pi}$, by applying on (6)

$$\log\cos y = -\frac{y^2}{2} - \frac{y^4}{12} + O\left(y^6\right) \quad \text{for} \quad |y| \le 1$$

and

$$\exp(-a) = \exp(-b) + O(b-a) \quad \text{for} \quad a, b \ge 0. \qquad (7)$$

For $|t| > \frac{1}{3\pi}$, we use the trivial bound 1 for the integrand. This gives

$$\begin{aligned} &\int_{\mathbb{R}} E\left(\exp\left(-2\pi it\,\widehat{\chi_{v.f}}(\mu)\right)\right) dU(t) \\ &= \int_{-\frac{1}{3\pi}}^{\frac{1}{3\pi}} \exp\Big(-2^{m+1}\pi^2t^2 - \frac{4}{3}\pi^4 2^m t^4\Big) dU(t) + O\Big(2^m \int_{\mathbb{R}} t^6 |dU(t)|\Big) \\ &\quad + O\Big(\int_{|t|\ge\frac{1}{3\pi}} |dU(t)|\Big). \end{aligned}$$

We extend the first integral over the real line making the same error as the third term, that can be included in the second one. This yields

$$\int_{\mathbb{R}} \exp\Big(-2^{m+1}\pi^2t^2 - \frac{4}{3}\pi^4 2^m t^4\Big) dU(t) + O\Big(2^m \int_{\mathbb{R}} t^6 |dU(t)|\Big).$$

By (3), the remainder equals $O\left(2^{-2m}m^3\right)$. As for the main term, we use

$$\exp(-a) = 1 - a + O(a^2) \quad \text{for} \quad a > 0,$$

in addition to (3) and (4) as follows

$$\begin{aligned}
&\int_{\mathbb{R}} \exp\Big(-2^{m+1}\pi^2 t^2 - \frac{4}{3}\pi^4 2^m t^4\Big) dU(t)\\
&= \int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2 t^2\right)\Big(1-\frac{4}{3}\pi^4 2^m t^4 + O\left(2^{2m}t^8\right)\Big) dU(t)\\
&= \int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2 t^2\right) dU(t) + O\left(2^{-2m-n+2\beta(m+n)}m^{3/2}\right) + O\Big(2^{2m}\int_{\mathbb{R}} t^8 |dU(t)|\Big)\\
&= \int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2 t^2\right) dU(t) + O\left(2^{-2m-n+2\beta(m+n)}m^{3/2}\right) + O\left(2^{-2m}m^4\right).
\end{aligned}$$

The proof is complete recalling that the total mass over V_n^* and $\widehat{V}_m$ is 1. □

2.2 The second moment

$\eta^2(f)$ consists of three sums

$$\begin{aligned}
\eta^2(f) &= \int_{\substack{V_n^{*2}\times\widehat{V}_m^2\\(v,\mu)=(v',\mu')}} u\left(\widehat{\chi_{v.f}}(\mu)\right) u\left(\widehat{\chi_{v'.f}}(\mu')\right) d\mu dv d\mu' dv'\\
&+ \int_{\substack{V_n^{*2}\times\widehat{V}_m^2\\ v=v'\\ \mu\neq\mu'}} u\left(\widehat{\chi_{v.f}}(\mu)\right) u\left(\widehat{\chi_{v'.f}}(\mu')\right) d\mu dv d\mu' dv'\\
&+ \int_{\substack{V_n^{*2}\times\widehat{V}_m^2\\ v\neq v'}} u\left(\widehat{\chi_{v.f}}(\mu)\right) u\left(\widehat{\chi_{v'.f}}(\mu')\right) d\mu dv d\mu' dv',
\end{aligned}$$

which we denote respectively by $\eta_1^2(f)$, $\eta_2^2(f)$ et $\eta_3^2(f)$.

Lemma 2.2.

$$E(\eta_1^2) \leq \frac{1}{2^m(2^n-1)}\, E(\eta).$$

Proof.

$$\begin{aligned}
\eta_1^2(f) &= \int_{\substack{V_n^{*2}\times\widehat{V}_m^2\\(v,\mu)=(v',\mu')}} u\left(\widehat{\chi_{v.f}}(\mu)\right) u\left(\widehat{\chi_{v'.f}}(\mu')\right) d\mu dv d\mu' dv'\\
&= \frac{1}{2^m(2^n-1)} \int_{V_n^*\times\widehat{V}_m} u^2\left(\widehat{\chi_{v.f}}(\mu)\right) d\mu dv\\
&\leq \frac{1}{2^m(2^n-1)} \int_{V_n^*\times\widehat{V}_m} u\left(\widehat{\chi_{v.f}}(\mu)\right) d\mu dv = \frac{1}{2^m(2^n-1)}\, \eta(f)
\end{aligned}$$

noting that $0 \leq u(x) \leq 1$, $\forall x \in \mathbb{R}$. □

For $E(\eta_2^2)$ (resp. $E(\eta_3^2)$), we use the representation of u as a Fourier transform

$$E(\eta_2^2) = E\Bigg(\int_{\substack{V_n^{*2}\times\widehat{V}_m^2 \\ v=v' \\ \mu\neq\mu'}} u\left(\widehat{\chi_{v.f}}(\mu)\right) u\left(\widehat{\chi_{v.f}}(\mu')\right) d\mu dv d\mu' dv' \Bigg)$$

$$= \int_{\substack{V_n^{*2}\times\widehat{V}_m^2 \\ v=v' \\ \mu\neq\mu'}} \int_{\mathbb{R}^2} E\left(\exp\left(-2\pi it\, \widehat{\chi_{v.f}}(\mu) - 2\pi it'\, \widehat{\chi_{v.f}}(\mu')\right)\right) dU(t)dU(t')d\mu dv d\mu' dv'.$$

We evaluate the integrand in the following lemma.

Lemma 2.3. *Given $v \in V_n^*$ and μ, $\mu' \in \widehat{V}_m$ such that $\mu \neq \mu'$. For t and t' of absolute value smaller than $\frac{1}{3\pi}$, we have*

$$E\left(\exp\left(-2\pi it\, \widehat{\chi_{v.f}}(\mu) - 2\pi it'\, \widehat{\chi_{v.f}}(\mu')\right)\right) = \exp\left(-2^m \sum_{i=1}^{4}\sum_{j=0}^{i} c_{i,j} t^{2i-2j} t'^{2j}\right) + 2^m O(|t|+|t'|)^{10},$$

where $c_{i,j}$ are positive reals.

Proof. The random variables $\chi_{v.f}(x)\left(t\mu(x) + t'\mu'(x)\right)$ are independent in x, and take values $\left(t\mu(x) + t'\mu'(x)\right)$ and $-\left(t\mu(x) + t'\mu'(x)\right)$ with probability $1/2$. Thus

$$\begin{aligned}
&E\left(\exp\left(-2\pi it\, \widehat{\chi_{v.f}}(\mu) - 2\pi it'\, \widehat{\chi_{v.f}}(\mu')\right)\right) \\
&= E\Big(\prod_{x\in V_m} \exp\left(-2\pi i\chi_{v.f}(x)\left(t\mu(x) + t'\mu'(x)\right)\right) \Big) \\
&= \prod_{x\in V_m} E\left(\exp\left(-2\pi i\chi_{v.f}(x)\left(t\mu(x) + t'\mu'(x)\right)\right)\right) \\
&= \prod_{x\in V_m} \cos(2\pi(t\mu(x) + t'\mu'(x))).
\end{aligned}$$

Since $\mu \neq \mu'$, they agree (resp. disagree) 2^{m-1} times

$$\begin{aligned}
&\prod_{x\in V_m} \cos(2\pi(t\mu(x) + t'\mu'(x))) \\
&= \cos^{2^{m-1}}(2\pi(t + t'))\cos^{2^{m-1}}(2\pi(t - t')) \\
&= \exp\Bigg(-2^m \Bigg(\sum_{i=1}^{4} c_i(t + t')^{2i} + O(t + t')^{10} + \sum_{i=1}^{4} c_i(t - t')^{2i} + O(t - t')^{10} \Bigg)\Bigg),
\end{aligned}$$

for $|t| \leq \frac{1}{3\pi}$, $|t'| \leq \frac{1}{3\pi}$, by applying

$$\log\cos y = -\frac{y^2}{2} - \frac{y^4}{12} - \frac{y^6}{45} - \frac{17y^8}{2520} + O\left(y^{10}\right) \quad \text{for} \quad |y| \leq 1.$$

Simplifying and using (7) give the result. $\square$

Lemma 2.4.

$$E(\eta_2^2) = \frac{1}{2^n-1}\left(\int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2 t^2\right) dU(t)\right)^2 + O\left(2^{-3m-3n+4\beta(m+n)}m\right) + O\left(2^{-4m-n}m^9\right).$$

Proof. Using the previous lemma together with the trivial bound 1 for the integrand outside the square $|t| \geq \frac{1}{3\pi}$, $|t'| \geq \frac{1}{3\pi}$ give

$$\begin{aligned}
&\int_{\mathbb{R}^2} E\left(\exp\left(-2\pi i t\,\widehat{\chi_{v.f}}(\mu) - 2\pi i t'\,\widehat{\chi_{v.f}}(\mu')\right)\right) dU(t)dU(t') \\
&= \int_{-\frac{1}{3\pi}}^{\frac{1}{3\pi}}\int_{-\frac{1}{3\pi}}^{\frac{1}{3\pi}} \exp\Bigg(-2^m\sum_{i=1}^{4}\sum_{j=0}^{i} c_{i,j}t^{2i-2j}t'^{2j}\Bigg) dU(t)dU(t') \\
&\quad + O\Bigg(2^m\int_{\mathbb{R}^2}(|t|+|t'|)^{10}|dU(t)||dU(t')|\Bigg) \qquad (8)\\
&\quad + O\Bigg(\int_{|t|\geq\frac{1}{3\pi}}\int_{\mathbb{R}}|dU(t)||dU(t')|\Bigg).
\end{aligned}$$

We extend integration in the first term over $\mathbb{R}^2$ making the same error as the third term, that is smaller than the second one.
Noting that $c_{1,0} = c_{1,1} = 2\pi^2$, and applying

$$\exp(-a) = 1 - a + \frac{a^2}{2} - \frac{a^3}{6} + O(a^4), \quad \text{for} \quad a > 0,$$

the first term then becomes

$$\begin{aligned}
&\int_{\mathbb{R}^2} \exp(-2^{m+1}\pi^2t^2)\exp(-2^{m+1}\pi^2t'^2)\Bigg(1 - 2^m\sum_{i=2}^{4}\sum_{j=0}^{i}c_{i,j}t^{2i-2j}t'^{2j} + 2^{2m}\sum_{i=4}^{8}\sum_{j=0}^{i}l_{i,j}t^{2i-2j}t'^{2j} \\
&- 2^{3m}\sum_{i=6}^{12}\sum_{j=0}^{i}p_{i,j}t^{2i-2j}t'^{2j} + 2^{4m}O\Bigg(\sum_{i=8}^{16}\sum_{j=0}^{i}r_{i,j}t^{2i-2j}t'^{2j}\Bigg)\Bigg)dU(t)dU(t')
\end{aligned}$$

and by (4), we get

$$\begin{aligned}
&\left(\int_{\mathbb{R}}\exp(-2^{m+1}\pi^2t^2)dU(t)\right)^2 - 2^m\sum_{i=2}^{4}\sum_{j=0}^{i}O\left(2^{-mi-2(m+n)(1-2\beta)}m^{i-1}\right) \\
&+ 2^{2m}\sum_{i=4}^{8}\sum_{j=0}^{i}O\left(2^{-mi-2(m+n)(1-2\beta)}m^{i-1}\right) - 2^{3m}\sum_{i=6}^{12}\sum_{j=0}^{i}O\left(2^{-mi-2(m+n)(1-2\beta)}m^{i-1}\right) \\
&+ 2^{4m}O\left(\sum_{i=8}^{16}\sum_{j=0}^{i}r_{i,j}\int_{\mathbb{R}}t^{2i-2j}|dU(t)|\int_{\mathbb{R}}t'^{2j}|dU(t')|\right). \qquad (9)
\end{aligned}$$

Terms in (9) with $i = j$ or $j = 0$ are equal $2^{4m} O(m)\, O\left(\frac{m}{2^m}\right)^8$ by (2) and (3). The other terms are equal $2^{4m} O\left(\frac{m}{2^m}\right)^8$ by (3). This gives

$$\left(\int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2 t^2\right) dU(t)\right)^2 + O\left(2^{-3m-2n+4\beta(m+n)} m\right) + O\left(2^{-4m} m^9\right).$$

As for (8), it can be estimated just like (9) using (2) and (3), yielding $O\left(2^{-4m} m^6\right)$. We end the calculations by integrating over the other variables. □

Lemma 2.5.

$$E(\eta_3^2) = \left(1 - \frac{1}{2^n - 1}\right) E^2(\eta).$$

Proof. We have

$$E(\eta_3^2) = \int_{\substack{V_n^{*2} \times \widehat{V}_m^2 \\ v \neq v'}} \int_{\mathbb{R}^2} E\left(\exp\left(-2\pi i t\, \widehat{\chi_{v.f}}(\mu) - 2\pi i t'\, \widehat{\chi_{v'.f}}(\mu')\right)\right) dU(t) dU(t') d\mu dv d\mu' dv'.$$

Since $v \neq v'$, the random variables $\widehat{\chi_{v.f}}(\mu)$ and $\widehat{\chi_{v'.f}}(\mu')$ are independent. Thus

$$\begin{aligned}
&E\left(\exp\left(-2\pi i t\, \widehat{\chi_{v.f}}(\mu) - 2\pi i t'\, \widehat{\chi_{v'.f}}(\mu')\right)\right) \\
&= E\left(\exp\left(-2\pi i t\, \widehat{\chi_{v.f}}(\mu)\right)\right) E\left(\exp\left(-2\pi i t'\, \widehat{\chi_{v'.f}}(\mu')\right)\right) \\
&= \cos^{2^m}(2\pi t) \cos^{2^m}(2\pi t'),
\end{aligned}$$

as calculated previously in (6). And,

$$\begin{aligned}
E(\eta_3^2) &= \int_{\substack{V_n^{*2} \times \widehat{V}_m^2 \\ v \neq v'}} d\mu dv d\mu' dv' \left(\int_{\mathbb{R}} \cos^{2^m}(2\pi t) dU(t)\right)^2 \\
&= \left(1 - \frac{1}{2^n - 1}\right) E^2(\eta).
\end{aligned}$$

□

Lemma 2.6.

$$\frac{1}{E(\eta)} = O\left(2^{(m+n)(1-\beta)^2} \sqrt{m}\right). \tag{10}$$

Proof. We have

$$E(\eta) = \int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2 t^2\right) dU(t) + O\left(2^{-2m-n+2\beta(m+n)} m^{3/2}\right) + O\left(2^{-2m} m^4\right).$$

The Fourier transform of $\exp\left(-2^{m+1}\pi^2t^2\right)$ is $\dfrac{1}{\sqrt{2^{m+1}\pi}}\exp\left(-\dfrac{x^2}{2^{m+1}}\right)$. Hence, by Plancherel's theorem, and the left-hand inequality of (13), we have

$$\begin{aligned}
\int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2t^2\right) dU(t) &= \frac{1}{\sqrt{2^{m+1}\pi}} \int_{\mathbb{R}} \exp\left(-\frac{x^2}{2^{m+1}}\right) u(x)dx \\
&\geq \frac{1}{\sqrt{2^{m+1}\pi}} \int_{|x|\geq M+\Delta} \exp\left(-\frac{x^2}{2^{m+1}}\right) dx \\
&= \frac{1}{\sqrt{\pi}} \int_{|y|\geq \frac{M+\Delta}{\sqrt{2^{m+1}}}} \exp(-y^2)dy \\
&\geq \sqrt{\frac{2^{m+1}}{\pi}}\, \frac{\exp\left(-\frac{(M+\Delta)^2}{2^{m+1}}\right)}{M+\Delta} \left(1-\frac{2^m}{(M+\Delta)^2}\right) \\
&\geq C_1\sqrt{2^{m+1}}\, \frac{\exp\left(-\frac{M^2}{2^{m+1}}\right)}{M+\Delta} \\
&\geq C_2\, 2^{-(m+n)(1-\beta)^2} m^{-1/2}.
\end{aligned}$$

Adding the fact that

$$O\left(2^{-2m-n+2\beta(m+n)}m^{3/2}\right) + O\left(2^{-2m}m^4\right) = o\left(2^{-(m+n)(1-\beta)^2}m^{-1/2}\right),$$

proves the result. □

Theorem 2.1. *Let $0 < \beta < \frac{1}{4}$ and γ any positive real. When m tends to infinity and $n \leq m$, we have*

$$P\Big(\max_{\substack{v\in V_n^* \\ \mu\in\widehat{V}_m}} |\widehat{\chi_{v\cdot f}}(\mu)| \leq 2^{\frac{m+1}{2}}\sqrt{(m+n)\log 2}\,(1-\beta)\Big) = P(\eta=0) = O\left(m^{-\gamma}\right).$$

Proof. When $\eta = 0$, η deviates from its expectation by $E(\eta)$, and by Tchebitcheff's inequality

$$P(\eta = 0) \leq P\big(|\eta - E(\eta)| \geq E(\eta)\big) \leq \frac{E(\eta^2)-E^2(\eta)}{E^2(\eta)}.$$

We have

$$\begin{aligned}
E(\eta^2)-E^2(\eta) \leq \frac{E(\eta)}{2^m(2^n-1)} + \frac{1}{2^n-1}\left(\left(\int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2t^2\right) dU(t)\right)^2 - E^2(\eta)\right) \\
+ O\left(2^{-3m-3n+4\beta(m+n)}m\right) + O\left(2^{-4m-n}m^9\right),
\end{aligned}$$

and by (5), we get

$$E(\eta^2) - E^2(\eta) \leq \frac{E(\eta)}{2^m(2^n-1)} + \frac{1}{2^n-1}\left(\left(\int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2t^2\right) dU(t)\right) O\left(2^{-2m-n+2\beta(m+n)}m^{3/2}\right) + O\left(2^{-4m}m^8\right) + E(\eta)O\left(2^{-2m}m^4\right) \right) + O\left(2^{-3m-3n+4\beta(m+n)}m\right) + O\left(2^{-4m-n}m^9\right)$$

When divided by $E^2(\eta)$, we can check using (10) and (4) that every term is smaller than $O\left(m^{-\gamma}\right)$. □

2.3 Proof of proposition 2.1

Before giving the proof, we first complete the construction of u. Let us fix a 34 times continuously differentiable function α on $[0,1]$, which takes 0 at 0, 1 at 1, takes values between 0 and 1, and with vanishing derivatives up to the 18th order at 0 and 1. By choosing $u(x)$ to be equal $\alpha\left(\frac{|x|-M}{\Delta}\right)$ for $M \leq |x| \leq M+\Delta$, $u(x)$ is then a 34 times differentiable function on $\mathbb{R}$ with $|u^r(x)| \leq \dfrac{\text{constant}}{\Delta^r}$, for $r = 0, 1, ..., 34$.

Proof. The measure U, having u as its Fourier transform, can be written as the sum of the Dirac measure at the origin and

$$g(t) = \int_{\mathbb{R}} \exp(-2\pi itx)(u(x)-1)dx = \int_{-M-\Delta}^{M+\Delta} \exp(-2\pi itx)(u(x)-1)dx.$$

We have

$$|g(t)| \leq 2(M+\Delta) = O(M). \tag{11}$$

And integration by parts gives

$$|t^r g(t)| \leq \int_{-M-\Delta}^{M+\Delta} |u^{(r)}(x)|dx = O\left(\frac{1}{\Delta^{r-1}}\right) \quad \text{for} \quad r = 1, ..., 34. \tag{12}$$

To prove (2), we use (11) for $|t| \leq \dfrac{1}{\Delta}$ and (12) with $r=2$ for $|t| \geq \dfrac{1}{\Delta}$

$$\int_{\mathbb{R}} |dU(t)| = 1 + \int_{\mathbb{R}} |g(t)|dt = O\left(\frac{M}{\Delta}\right) = O(m).$$

To prove (3), we use (12) with $r = p$ for $|t| \leq \dfrac{1}{\Delta}$ and with $r = p+2$ for $|t| \geq \dfrac{1}{\Delta}$

$$\int_{\mathbb{R}} |t^p||dU(t)| = \int_{\mathbb{R}} |t^p||g(t)|dt = O\left(\frac{1}{\Delta^p}\right) = O\left(\frac{m}{2^m}\right)^{p/2} \quad \text{for} \quad p = 1, ..., 32.$$

To prove (4), we use the Plancherel's theorem. The Fourier transform of $t^p U$ is $\dfrac{i^p}{(2\pi)^p} u^{(p)}(x)$ and that of $\exp\left(-2^{m+1}\pi^2 t^2\right)$ is $\dfrac{1}{\sqrt{2^{m+1}\pi}} \exp\left(-\dfrac{x^2}{2^{m+1}}\right)$,

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

To evaluate the integral of the exponential, we have [5]

$$\left(1 - \frac{1}{2y^2}\right) \frac{\exp(-y^2)}{-2y} < \int_{-\infty}^{y} \exp(-x^2) dx < \frac{\exp(-y^2)}{-2y}, \qquad (13)$$

for every $y < 0$. Using the right-hand inequality of (13), we get

$$\left| \int_{\mathbb{R}} \exp\left(-2^{m+1}\pi^2 t^2\right) t^p dU(t) \right| = O\left(2^{\left(-m\frac{p}{2} - (m+n)(1-\beta)^2\right)} m^{p/2-1/2}\right). \qquad (14)$$

□

3 The upper bound

Lemma 3.1. *Let λ be a real number, $v \in V_n^*$ and $\mu \in \widehat{V}_m$. Then, for f running in the space of (m,n)-functions*

$$E\left(\exp\left(\lambda\,\widehat{\chi_{v.f}}(\mu)\right)\right) \leq \exp\left(2^{m-1}\lambda^2\right).$$

Proof. The random variables $\chi_{v.f}(x)\mu(x)$ are independent in x and take values $+1$ and -1 with probability $1/2$. Thus

$$E\left(\exp\left(\lambda\,\widehat{\chi_{v.f}}(\mu)\right)\right) = E\left(\prod_{x\in V_m} \exp\left(\lambda\,\chi_{v.f}(x)\mu(x)\right)\right)$$
$$= \prod_{x\in V_m} E\left(\exp\left(\lambda\,\chi_{v.f}(x)\mu(x)\right)\right)$$
$$= \prod_{x\in V_m} \cosh\lambda.$$

And

$$\cosh\lambda \leq \exp\frac{\lambda^2}{2}.$$

□

Theorem 3.1. *Let m and n be any positive integers and β any positif real. Then*

$$P\Big(\max_{\substack{v\in V_n^*\\ \mu\in\widehat{V}_m}} |\widehat{\chi_{v\cdot f}}(\mu)| \geq 2^{\frac{m+1}{2}}\sqrt{(m+n)\log 2}\,(1+\beta)\Big) \leq 2^{-(m+n)(2\beta+\beta^2)+1}.$$

Proof. There exists (v_0,μ_0) in $V_n^*\times\widehat{V}_m$ such that $\max_{\substack{v\in V_n^*\\ \mu\in\widehat{V}_m}} |\widehat{\chi_{v\cdot f}}(\mu)| = |\widehat{\chi_{v_0\cdot f}}(\mu_0)|$.

Let λ be a positive real, we have

$$\begin{aligned}\exp\Big(\lambda \max_{\substack{v\in V_n^*\\ \mu\in\widehat{V}_m}} |\widehat{\chi_{v\cdot f}}(\mu)|\Big) &\leq \exp\left(\lambda\, \widehat{\chi_{v_0\cdot f}}(\mu_0)\right) + \exp\left(-\lambda\, \widehat{\chi_{v_0\cdot f}}(\mu_0)\right)\\ &\leq 2^{m+n}\int_{V_n^*}\int_{\widehat{V}_m} \left(\exp\left(\lambda\,\widehat{\chi_{v\cdot f}}(\mu)\right) + \exp\left(-\lambda\,\widehat{\chi_{v\cdot f}}(\mu)\right)\right) d\mu dv.\end{aligned}$$

When f ranges over the space of (m,n)-functions

$$E\Big(\exp\Big(\lambda \max_{\substack{v\in V_n^*\\ \mu\in\widehat{V}_m}} |\widehat{\chi_{v\cdot f}}(\mu)|\Big)\Big) \leq 2^{m+n}\int_{V_n^*}\int_{\widehat{V}_m} \mathrm{E}\left(\exp\left(\lambda\,\widehat{\chi_{v\cdot f}}(\mu)\right) + \exp\left(-\lambda\,\widehat{\chi_{v\cdot f}}(\mu)\right)\right) d\mu dv.$$

Using lemma 3.1 and recalling that the total mass over V_n^* and $\widehat{V}_m$ is 1, we have

$$\begin{aligned}E\Big(\exp\Big(\lambda \max_{\substack{v\in V_n^*\\ \mu\in\widehat{V}_m}} |\widehat{\chi_{v\cdot f}}(\mu)|\Big)\Big) &\leq 2^{m+n+1}\exp\left(2^{m-1}\lambda^2\right)\\ &= 2^{-(m+n)(2\beta+\beta^2)+1}\exp\left(2^{m-1}\lambda^2 + (m+n)(1+\beta)^2\log 2\right).\end{aligned}$$

Thus,

$$E\Big(\exp\Big(\lambda \max_{\substack{v\in V_n^*\\ \mu\in\widehat{V}_m}} |\widehat{\chi_{v\cdot f}}(\mu)| - 2^{m-1}\lambda^2 - (m+n)(1+\beta)^2\log 2\Big)\Big) \leq 2^{-(m+n)(2\beta+\beta^2)+1}.$$

Consequently,

$$P\Big(\exp\Big(\lambda \max_{\substack{v\in V_n^*\\ \mu\in\widehat{V}_m}} |\widehat{\chi_{v\cdot f}}(\mu)| - 2^{m-1}\lambda^2 - (m+n)(1+\beta)^2\log 2\Big) \geq 1\Big) \leq 2^{-(m+n)(2\beta+\beta^2)+1}.$$

And finally,

$$P\Big(\max_{\substack{v\in V_n^*\\ \mu\in\widehat{V}_m}} |\widehat{\chi_{v\cdot f}}(\mu)| \geq 2^{m-1}\lambda + \frac{(m+n)(1+\beta)^2\log 2}{\lambda}\Big) \leq 2^{-(m+n)(2\beta+\beta^2)+1}.$$

The best bound is obtained when $\lambda = 2^{\frac{1-m}{2}}\sqrt{(m+n)\log 2}\,(1+\beta)$, which gives the result. ☐

When $(m+n)$ tends to infinity, we obtain then a lower bound of the nonlinearity of almost all (m,n)-functions.

References

[1] C. Carlet, Vectorial Boolean Functions for Cryptography. Chapter of the monography “Boolean Models and Methods in Mathematics, Computer Science, and Engineering" published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), pp. 398-469, 2010.

[2] C. Carlet, C. Ding, Nonlinearities of S-boxes. Finite Fields Appl. 13 (2007), no. 1, 121Ð135.

[3] 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.

[4] F. Chabaud, S. Vaudenay, Links between differential and linear cryptanalysis. Advances in cryptology, EUROCRYPT ’94 (Perugia), 356Ð365, Lecture Notes in Comput. Sci., 950, Springer, Berlin, 1995.

[5] W. Feller, An introduction to probability theory and its applications. Vol. I. Third edition John Wiley & Sons, Inc., New York-London-Sydney 1968.

[6] G. Halász On a result of Salem and Zygmund concerning random polynomials. Studia Sci. Math. Hungar. 8 (1973), 369Ð377.

[7] S. Litsyn, A. Shpunt, On the distribution of Boolean function nonlinearity. SIAM J. Discrete Math. 23 (2008/2009), no. 1, 79–95

[8] D. Olejár et M. Stanek, On cryptographic properties of random Boolean functions, J.UCS 4 (1998), no. 8, 705–717.

[9] F. Rodier, Sur la non-linéarité des fonctions booléennes. Acta Arithmetica, vol 115, (2004), 1-22, disponible sur ArXiv: math.NT/0306395.

[10] F. Rodier, Asymptotic nonlinearity of Boolean functions. Designs, Codes and Cryptography, 40:1 2006,

[11] R. Salem, A. Zygmund, Some properties of trigonometric series whose terms have random signs. Acta Math. 91, (1954). 245Ð301.