Cryptogr. Commun. (2019) 11:63–76
https://doi.org/10.1007/s12095-018-0293-6

On the nonlinearity of Boolean functions with restricted input

Sihem Mesnager[1,2,3] · **Zhengchun Zhou**[4] ·
Cunsheng Ding[5]

Received: 30 October 2017 / Accepted: 7 March 2018 / Published online: 13 March 2018

Abstract Very recently, Carlet, Méaux and Rotella have studied the main cryptographic features of Boolean functions when, for a given number n of variables, the input to these functions is restricted to some subset E of $\mathbb{F}_2^n$. Their study includes the particular case when E equals the set of vectors of fixed Hamming weight, which is important in the robustness of the Boolean function involved in the FLIP stream cipher. In this paper we focus on the nonlinearity of Boolean functions with restricted input and present new results related to the analysis of this nonlinearity improving the upper bound given by Carlet et al.

Keywords Boolean functions · Nonlinearity · Walsh Hadamard transform · FLIP cipher

Mathematics Subject Classification (2010) 11T71 · 11T06

This article is part of the Topical Collection on *Special Issue on Boolean Functions and Their Applications*

✉ Sihem Mesnager
smesnager@univ-paris8.fr

Zhengchun Zhou
zczhou@126.com

Cunsheng Ding
cding@cse.ust.hk

[1] Department of Mathematics, University of Paris VIII, Saint-Denis, France

[2] LAGA, UMR 7539, CNRS, University of Paris XIII, Villetaneuse, France

[3] Telecom ParisTech, Paris, France

[4] Department of Mathematics, Sothwest Jiaotong University, Chengdu, China

[5] Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong, China

1 Introduction

The cryptographic criterion of interest in this manuscript is that of *nonlinearity* which characterizes the distance between a Boolean function and the set of affine functions (i.e. those of algebraic degree 0 or 1) and is naturally defined using the Hamming distance. More precisely, the nonlinearity of f is the minimum distance to affine functions (in terms of Reed-Muller codes, it is equal to the minimum distance of the linear code Reed-Muller code $\mathrm{RM}(1,n) \cup (f + \mathrm{RM}(1,n))$ where $\mathrm{RM}(1,n)$ denotes the Reed-Muller code of order 1 and length 2^n). It can be shown that the nonlinearity of a Boolean function in n variables is upper bounded by $2^{n-1} - 2^{n/2-1}$. In order to provide confusion, cryptographic functions must lie at large Hamming distance (in the sense, close to the maximum value $2^{n-1} - 2^{n/2-1}$) to all affine functions, equivalently must be of a large nonlinearity (in the sense, close to the upper bound $2^{n-1} - 2^{n/2-1}$). Boolean functions achieving maximal nonlinearity are called *bent functions* introduced by Rothaus [8] in 1976 but already studied by Dillon [5] since 1974. For of their own sake as interesting combinatorial objects, but also for their relations to coding theory (Reed-Muller codes), combinatorics (difference sets) and applications in cryptography (design of stream ciphers), they have attracted a lot of research for more than four decades. Two references devoted especially to bent functions and containing a complete survey on bent functions are [3, 7]. It is important to point out that bent functions can not be directly used in the filter and combiner models; in particular, they are not balanced and their algebraic degree does not exceed $\frac{n}{2}$, which make them weak against fast algebraic attacks [9] even after modifying a number of values small enough to keep good nonlinearity.

In 2016, Méaux, Journault, Standaert and Carlet [6] introduced the cipher FLIP in the context of homomorphic encryption. FLIP is one of the encryption schemes specifically designed to be combined with an homomorphic encryption scheme to improve the efficiency of somewhat homomorphic encryption frameworks. It has been shown that in the context of the FLIP cipher, the important criteria of Boolean functions are the classical ones (balancedness, nonlinearity, algebraic immunity) when, for a given number n of variables, the input to these functions is restricted to some subset E of $\mathbb{F}_2^n$. In 2017, Carlet, Méaux and Rotella [4] studied Boolean functions with restricted input and their robustness in the framework of FLIP cipher. In this manuscript, we focus on one parameter of Boolean functions: the nonlinearity with restricted input. We derive new results on the analysis of the nonlinearity with restricted input improving the upper bound given by Carlet, Méaux and Rotella. The paper is organized as follows. In Section 2, we recall some background related to Boolean functions as well as some preliminaries on the nonlinearity of Boolean functions. In Section 3, we focus ourselves on the nonlinearity of Boolean functions with restricted input. Using the moments of the Walsh transform, we first derive in Section 3.1 an upper bound on that nonlinearity (Theorem 7). Next, we push further the analysis of the power sums involved in Theorem 7 and establish a new upper bound on the nonlinearity of Boolean functions with constant weight inputs improving the results of Carlet et al. (Theorem 16).

2 Preliminaries

We denote by $|I|$ the cardinality of a finite set I. Let n be any positive integer. In this paper, we shall denote by $\mathcal{B}_n$ the set of all n-variable Boolean functions over $\mathbb{F}_2^n$ [1]. Any n-variable

Boolean function f (that is, a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$) admits a unique *algebraic normal form* (ANF), that is, a representation as a multivariate polynomial over $\mathbb{F}_2$:

$$f(x_1,\ldots,x_n)=\bigoplus_{I\subseteq\{1,\ldots,n\}} a_I \prod_{i\in I} x_i,$$

where the a_I's are in $\mathbb{F}_2$. The terms $\prod_{i\in I} x_i$ are called *monomials*. The *algebraic degree* $\deg(f)$ of a Boolean function f equals the maximum degree of those monomials whose coefficients are nonzero in its algebraic normal form. A slightly different form for the algebraic normal form is $f(x)=\bigoplus_{u\in\mathbb{F}_2^n} a_u x^u$, where $a_u\in\mathbb{F}_2$ and where $x^u=\prod_{i=1}^n x_i^{u_i}$. Then $\deg(f)$ equals $\max\limits_{a_u\neq 0} \mathrm{wt}(u)$, where $\mathrm{wt}(u)$ denotes the Hamming weight of u, that is, $\mathrm{wt}(u)=|\{i=1,\ldots,n \mid u_i=1\}|$. Given a positive integer r, we make an abuse of notation and denote by $\mathrm{RM}(r,n)$ the set of all n-variable Boolean functions of algebraic degrees at most r, that is, the so-called r-th order Reed-Muller code of length 2^n. We recall that $\mathrm{RM}(r,n)$ is a vector subspace over $\mathbb{F}_2$ of dimension $\sum_{i=0}^r \binom{n}{i}$.

The Hamming weight $\mathrm{wt}(f)$ of a Boolean function is the size of its support $\{x\in\mathbb{F}_2^n \mid f(x)=1\}$ that we denote by $\mathrm{supp}(f)$. The Hamming distance between two n-variable Boolean functions is the Hamming weight of $f\oplus g$, that is $\mathrm{dist}(f,g)=|\{x\in\mathbb{F}_2^n \mid f(x)\neq g(x)\}|$.

Definition 1 (rth-order nonlinearity) Let f be an n-variable Boolean function. Let r be a positive integer such that $r\leq n$. The *r-th order nonlinearity* of f is the minimum Hamming distance between f and all n-variable Boolean functions from $\mathrm{RM}(r,n)$. We shall denote the r-th order nonlinearity of f by $nl_r(f)$.

We have

$$nl_r(f)=2^{n-1}-\frac{1}{2}\max_{g\in RM(r,n)}\left|\sum_{x\in F_2^n}(-1)^{f(x)+g(x)}\right|. \tag{1}$$

The first-order nonlinearity of f is simply called the nonlinearity of f and is denoted by $nl(f)$ (instead of $nl_1(f)$). Clearly we have $nl_r(f)=0$ if and only if f has degree at most r. So, the knowledge of the nonlinearity profile (i.e. 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 the single (first-order) nonlinearity and the algebraic degree. The best known upper bound on $nl_r(f)$ has an asymptotic version [2]:

$$nl_r(f)\leq 2^{n-1}-\frac{\sqrt{15}}{2}(1+\sqrt{2})^{r-2}2^{\frac{n}{2}}+O(n^{r-2})$$

for every n-variable Boolean function f.

3 Results on the nonlinearity with restricted input

3.1 An upper bound derived from power sums of Walsh transform

Let n be a positive integer. Let E be any subset of $\mathbb{F}_2^n$ and let f be any Boolean function defined over E. We define

$$\widehat{\chi_{f,E}}(a)=\sum_{x\in E}(-1)^{f(x)+a\cdot x},\quad a\in\mathbb{F}_2^n,$$

where "·" denotes the standard inner product in $\mathbb{F}_2^n$. In [4], the authors have introduced the following definition of the nonlinearity of a Boolean function with restricted input:

$$NL_E(f) = \frac{|E|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} |\widehat{\chi_{f,E}}(a)|.$$

Clearly, NL_E is invariant under the addition by a Boolean function g whose restriction to E is affine, that is, $g(x) = \gamma \cdot x + \beta$. Indeed,

$$\widehat{\chi_{f+g,E}}(a) = \sum_{x\in E}(-1)^{f(x)+\gamma\cdot x+\beta+a\cdot x} = (-1)^{\beta}\sum_{x\in E}(-1)^{f(x)+x\cdot(a+\gamma)} = (-1)^{\beta}\,\widehat{\chi_{f,E}}(a+\gamma).$$

Thus, we have the following.

Lemma 2 *Let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ such that $g(x) = \gamma \cdot x + \beta$ for every $x \in E$ where $\gamma \in \mathbb{F}_2^n$ and $\beta \in \mathbb{F}_2$. Then $NL_E(f + g) = NL_E(f)$.*

In [4], it is established the following upper bound on this nonlinearity.

Theorem 3 ([4, Proposition 6]) *We have*

$$NL_E(f) \le \frac{|E|}{2} - \frac{\sqrt{|E| + \lambda}}{2},$$

where

$$\lambda = \max_{F\in\mathcal{F}}\left|\sum_{\substack{(x,y)\in E^2\\ x+y\in F^{\perp}\setminus\{0\}}} (-1)^{f(x)+f(y)}\right|.$$

Herein $\mathcal{F}$ is a family of vector spaces F for each of which there exists $v \in \mathbb{F}_2^n$ such that $v \cdot (x + y) = 1$ for all $(x, y) \in E^2$ such that $x + y \in F^{\perp} \setminus \{0\}$. Herein and hereafter, $F^{\perp}$ denotes the dual space of the vector space F.

Remark 4 If $E = \mathbb{F}_2^n$, Theorem 3 is the classical "covering radius bound" $2^{n-1} - 2^{\frac{n}{2}-1}$ (since $F^{\perp} = \{0\}$).

Remark 5 Without giving the calculation, we indicate that the theorem above is a direct consequence of the following identity where F is a vector space:

$$\sum_{a\in F}\left(\widehat{\chi_{f,E}}(a)\right)^2 = |F| \sum_{\substack{(x,y)\in E^2\\ x+y\in F^{\perp}}} (-1)^{f(x)+f(y)}.$$

The most important feature is that Theorem 3 does not relies on any property on E but only on the fact that we sum over a vector space.

Considering the case where F is a hyperplane (in that case, the condition of Theorem 3 is satisfied), we have the following most simple bound established in [4]:

Corollary 6 *We have*

$$NL_E(f) \le \frac{|E|}{2} - \frac{1}{2}\sqrt{|E| + \lambda},$$

where

$$\lambda = \max_{a\in\mathbb{F}_2^n,\, a\neq 0}\left|\sum_{\substack{x,y\in E\\ x+y=a}}(-1)^{D_a f(x)}\right|$$

and $D_a f$ is the derivative of f in the direction of a whose expression is given as follows:

$$D_a f(x) = f(x+a) + f(x).$$

We are going to show that Theorem 3 is a particular case of a more general result. To this end, set

$$S_\ell(f, E, F) = \sum_{a\in F}\left(\widehat{\chi_{f,E}}(a)\right)^\ell .$$

Observe that $S_\ell(f, E, F) = 0$ if and only if $\widehat{\chi_{f,E}}$ vanishes on F when ℓ is even. Next,

$$\begin{aligned} S_{2\ell+2}(f, E, F) &= \sum_{a\in F}\left(\widehat{\chi_{f,E}}(a)\right)^{2\ell+2}\\ &\leq \left(\max_{a\in F}|\widehat{\chi_{f,E}}(a)|\right)^2 \sum_{a\in F}\left(\widehat{\chi_{f,E}}(a)\right)^{2\ell}\\ &= \left(\max_{a\in F}|\widehat{\chi_{f,E}}(a)|\right)^2 S_{2\ell}(f, E, F) \end{aligned}$$

Thus we arrive at

$$\frac{S_{2\ell+2}(f, E, F)}{S_{2\ell}(f, E, F)} \leq \left(\max_{a\in F}|\widehat{\chi_{f,E}}(a)|\right)^2 \tag{2}$$

A direct generalization of Theorem 3 is therefore the following upper bound.

Theorem 7 *Let f be a Boolean function over $\mathbb{F}_2^n$. Let F be a vectorspace of $\mathbb{F}_2^n$ such that $\widehat{\chi_{f,E}}$ does not vanish on F. Then, every positive integer ℓ,*

$$NL_E(f) \leq \frac{|E|}{2} - \frac{1}{2}\sqrt{\frac{S_{2\ell+2}(f, E, F)}{S_{2\ell}(f, E, F)}}. \tag{3}$$

Remark 8 With our framework, the approach of [4] corresponds to take $\ell = 0$ in (2) and to consider particular subspaces F. Indeed, if $\ell = 0$, one has

$$\begin{aligned} \frac{S_{2\ell+2}(f, E, F)}{S_{2\ell}(f, E, F)} &= \frac{1}{|F|}\sum_{a\in F}\left(\widehat{\chi_{f,E}}(a)\right)^2\\ &= \sum_{(x,y)\in E^2, x+y\in F^\perp}(-1)^{f(x)+f(y)}. \end{aligned}$$

To get the absolute value, it suffices to use Lemma 2 with $f_v(x) = f(x)+v\cdot x$. According to Lemma 2, one has $NL_E(f) = NL_E(f_v)$ On the other hand,

$$\begin{aligned}\sum_{\substack{(x,y)\in E^2\\ x+y\in F^\perp}} (-1)^{f_v(x)+f_v(y)} &= \sum_{\substack{(x,y)\in E^2\\ x+y\in F^\perp}} (-1)^{f(x)+f(y)+v\cdot(x+y)}\\ &= |E| + \sum_{\substack{(x,y)\in E^2\\ x+y\in F^\perp\setminus\{0\}}} (-1)^{f(x)+f(y)+v\cdot(x+y)}.\end{aligned}$$

Now, if v is chosen such that $v\cdot(x+y) = 1$ for every $(x, y) \in E^2$ such that $x + y \in F^\perp$, then

$$\sum_{\substack{(x,y)\in E^2\\ x+y\in F^\perp}} (-1)^{f_v(x)+f_v(y)} = |E| - \sum_{\substack{(x,y)\in E^2\\ x+y\in F^\perp\setminus\{0\}}} (-1)^{f(x)+f(y)}.$$

Remark 9 Another approach would have been to use the following naive upper bound:

$$S_{2\ell}(f, E, F) \le |F| \left(\max_{a\in F} |\widehat{\chi_{f,E}}(a)|\right)^{2\ell}. \tag{4}$$

But it will not give a better upper bound. Indeed, using the Hölder inequality (that is, $\sum_{a\in F} |u_a v_a| \le \left(\sum_{a\in F} |u_a|^p\right)^{\frac{1}{p}} \left(\sum_{a\in F} |u_a|^q\right)^{\frac{1}{q}}$, where $\frac{1}{p} + \frac{1}{q} = 1$) with $p = \frac{\ell+1}{\ell}$ and $q = \ell + 1$, we get

$$S_{2\ell}(f, E, F) = \sum_{a\in F} \left(\widehat{\chi_{f,E}}(a)\right)^{2\ell} \le \left(\sum_{a\in F} \left(\widehat{\chi_{f,E}}(a)\right)^{2\ell+2}\right)^{\frac{\ell}{\ell+1}} \left(\sum_{a\in F} 1\right)^{\frac{1}{\ell+1}}.$$

That implies that

$$|F| \left(S_{2\ell+2}(f, E, F)\right)^{\ell} \ge \left(S_{2\ell}(f, E, F)\right)^{\ell+1},$$

that is,

$$\frac{S_{2\ell+2}(f, E, F)}{S_{2\ell}(f, E, F)} \ge \left(\frac{1}{|F|} S_{2\ell}(f, E, F)\right)^{\frac{1}{\ell}}.$$

Remark 10 An important feature of Theorem 7 is that the right-hand side is a decreasing sequence. Indeed, by the Cauchy-Schwarz inequality,

$$\left(S_{2\ell+2}(f, E, F)\right)^2 \le S_{2\ell}(f, E, F) S_{2\ell+4}(f, E, F)$$

which implies that the sequence $\left(\frac{S_{2\ell+2}(f,E,F)}{S_{2\ell}(f,E,F)}\right)_{\ell\in\mathbb{N}^\star}$ is an increasing sequence. Since Theorem 3 corresponds to the case where $\ell = 0$, that says that (3) may be a better upper bound than Theorem 3 for every positive integers ℓ and the particular subspaces F considered in that Theorem.

But above, it is known that $\frac{\sum_i \lambda_i^{k+1}}{\sum_i \lambda_i^k}$ tends to $\max_i \lambda_i$ as k tends to infinity for any finite sequence of positive numbers λ_i. That says that, the right-hand side of (4) is a decreasing sequence which tends to $\frac{|E|}{2} - \frac{1}{2}\max_{a\in F} |\widehat{\chi_{f,E}}(a)|$ as ℓ tends to infinity.

At this stage, Theorem 7 does not give enough insight on NL_E because it does not rely on the structure of E. To understand more deeply what restricting inputs implies on the nonlinearity of a Boolean function, we shall consider particular subsets E in the sequel. But before doing this, we shall push further a bit more the analysis of the power sums $S_{2\ell}(f, E, F)$ involved in Theorem 7 in the next subsection.

3.2 Analysis of the power sums involved in Theorem 7

3.2.1 A decomposition formula

We begin with a classical calculation:

$$\begin{aligned} S_{2\ell}(f, E, F) &= \sum_{a\in F}\sum_{x_1,\dots,x_{2\ell}\in E} (-1)^{\sum_{i=1}^{2\ell} f(x_i)+a\cdot\left(\sum_{i=1}^{2\ell} x_i\right)} \\ &= \sum_{x_1,\dots,x_{2\ell}\in E} (-1)^{\sum_{i=1}^{2\ell} f(x_i)} \sum_{a\in F}(-1)^{a\cdot\left(\sum_{i=1}^{2\ell} x_i\right)} \\ &= |F| \sum_{\substack{x_1,\dots,x_{2\ell}\in E \\ x_1+\dots+x_{2\ell}\in F^\perp}} (-1)^{\sum_{i=1}^{2\ell} f(x_i)}. \end{aligned} \tag{5}$$

Let us now split the latter sum as follows

$$\begin{aligned} S_{2\ell}(f, E, F) = |F| &\sum_{\substack{x_1,\dots,x_{2\ell}\in E \\ x_1+x_2, x_3+\dots+x_{2\ell}\in F^\perp}} (-1)^{\sum_{i=1}^{2\ell} f(x_i)} + |F| \sum_{\substack{x_1,\dots,x_{2\ell}\in E \\ x_1+x_2, x_3+\dots+x_{2\ell}\notin F^\perp \\ x_1+\dots+x_{2\ell}\in F^\perp}} (-1)^{\sum_{i=1}^{2\ell} f(x_i)} \\ = |F| &\left(\sum_{\substack{x_1,x_2\in E \\ x_1+x_2\in F^\perp}} (-1)^{f(x_1)+f(x_2)} \right)\left(\sum_{\substack{x_1,\dots,x_{2\ell-2}\in E \\ x_1+\dots+x_{2\ell-2}\in F^\perp}} (-1)^{\sum_{i=1}^{2\ell-2} f(x_i)} \right) \\ &+|F| \sum_{\substack{x_1,\dots,x_{2\ell}\in E \\ x_1+x_2, x_3+\dots+x_{2\ell}\notin F^\perp \\ x_1+\dots+x_{2\ell}\in F^\perp}} (-1)^{\sum_{i=1}^{2\ell} f(x_i)}. \end{aligned} \tag{6}$$

We then deduce from the above calculation

Proposition 11 *Let f be a Boolean function over $\mathbb{F}_2^n$. Let F be a vectorspace of $\mathbb{F}_2^n$ such that $\widehat{\chi_{f,E}}$ does not vanish on F. Let ℓ be a positive integer. Then*

$$\frac{S_{2\ell+2}(f, E, F)}{S_{2\ell}(f, E, F)} = \sum_{u\in F^\perp} T_2(f, E, u) + R_\ell(f, E, F), \tag{7}$$

where

$$R_\ell(f, E, F) = \frac{\sum_{\substack{u+v\in F^\perp \\ u,v\notin F^\perp}} T_2(f, E, u) T_{2\ell}(f, E, v)}{\sum_{u\in F^\perp} T_{2\ell}(f, E, u)} \geq 0$$

and

$$T_{2\ell}(f, E, u) = \sum_{\substack{x_1,\dots,x_{2\ell}\in E\\ x_1+\dots+x_{2\ell}=u}} (-1)^{\sum_{i=1}^{2\ell} f(x_i)}.$$

Proof Let ℓ be a positive integer. Equation (6) implies that

$$S_{2\ell+2}(f, E, F)=\left(\sum_{\substack{x_1,x_2\in E\\ x_1+x_2\in F^\perp}} (-1)^{f(x_1)+f(x_2)}\right)S_{2\ell}(f, E, F)+|F| \sum_{\substack{x_1,\dots,x_{2\ell+2}\in E\\ x_1+x_2,x_3+\dots+x_{2\ell+2}\notin F^\perp\\ x_1+\dots+x_{2\ell+2}\in F^\perp}} (-1)^{\sum_{i=1}^{2\ell} f(x_i)}.$$

Decomposition (7) follows then from (5) and

$$\sum_{\substack{x_1,\dots,x_{2\ell+2}\in E\\ x_1+x_2,x_3+\dots+x_{2\ell+2}\notin F^\perp\\ x_1+\dots+x_{2\ell+2}\in F^\perp}} (-1)^{\sum_{i=1}^{2\ell} f(x_i)} = \sum_{\substack{u+v\in F^\perp\\ u,v\notin F^\perp}} T_2(f, E, u)T_{2\ell}(f, E, v),$$

where $T_2(f, E, u) = \sum_{\substack{x_1,x_2\in E\\ x_1+x_2=u}}(-1)^{f(x_1)+f(x_2)}$. Now, according to Remark 10, $\frac{S_{2\ell+2}(f,E,F)}{S_{2\ell}(f,E,F)} \geq \frac{S_2(f,E,F)}{S_0(f,E,F)} = \sum_{\substack{x_1,x_2\in E\\ x_1+x_2\in F^\perp}} (-1)^{f(x_1)+f(x_2)}$ which implies that $R_\ell(f, E, F) \geq 0$. □

Remark 12 Remark 10 implies also that the sequence $(R_\ell(f, E, F))_{\ell\in\mathbb{N}}$ is a non-decreasing sequence. Note that the sum $\sum_{\substack{u+v\in F^\perp\\ u,v\notin F^\perp}} T_2(f, E, u)T_{2\ell}(f, E, v)$ is also nonnegative because $\sum_{u\in F^\perp} T_{2\ell}(f, E, u) = \frac{1}{|F|}S_{2\ell}(f, E, F) > 0$ when $\widehat{\chi_{f,E}}$ does not vanish on F. Furthermore, if $\sum_{\substack{u+v\in F^\perp\\ u,v\notin F^\perp}} T_2(f, E, u)T_{2\ell}(f, E, v) = 0$, then we have $\frac{S_{2\ell+2}(f,E,F)}{S_{2\ell}(f,E,F)} = \frac{S_2(f,E,F)}{S_0(f,E,F)}$. Thus, according to Remark 10, the preceding equality implies that $\frac{S_4(f,E,F)}{S_2(f,E,F)} = \frac{S_2(f,E,F)}{S_0(f,E,F)}$. Next, since equality is achieved in Cauchy-Schwarz inequality if and only the two sequences involved in the inequality are proportional, $(\widehat{\chi_{f,E}})^2$ is therefore constant on F. The converse is also true. Hence,

$$\sum_{\substack{u+v\in F^\perp\\ u,v\notin F^\perp}} T_2(f, E, u)T_{2\ell}(f, E, v) = 0 \iff (\widehat{\chi_{f,E}})^2 \text{ is constant on } F.$$

3.2.2 *The case $\ell = 1$*

We are now going to turn our attention to the case where $\ell = 1$. As in Section 3.2.1, in the sequel, F denotes a vectorspace of $\mathbb{F}_2^n$ such that $\widehat{\chi_{f,E}}$ does not vanish on F. In that case, Proposition 11 says that:

$$\frac{S_4(f, E, F)}{S_2(f, E, F)} = \sum_{u\in F^\perp} T_2(f, E, u) + \frac{\sum_{\substack{u+v\in F^\perp\\ u,v\notin F^\perp}} T_2(f, E, u)T_2(f, E, v)}{\sum_{u\in F^\perp} T_2(f, E, u)}, \tag{8}$$

where

$$T_2(f, E, u) = \sum_{\substack{x,y \in E \\ x+y=u}} (-1)^{f(x)+f(y)}, \tag{9}$$

$$\sum_{\substack{u+v \in F^{\perp} \\ u,v \notin F^{\perp}}} T_2(f, E, u)T_2(f, E, v) \geq 0.$$

Observe next that

$$\sum_{u \in F^{\perp}} T_2(f, E, u) = |E| + \sum_{u \in F^{\perp}\setminus\{0\}} T_2(f, E, u). \tag{10}$$

Note that this term is involved in the upper bound stated by Theorem 3. At this stage, we observe that one should deduce from Equation (8) an upper bound on NL_E and this upper bound should be better than Theorem 3 provided that the second-term at the right-hand side is positive. Thus, we are now going to study when this term vanishes, that is, when

$$\sum_{\substack{u+v \in F^{\perp} \\ u,v \notin F^{\perp}}} T_2(f, E, u)T_2(f, E, v) = 0. \tag{11}$$

We have restricted ourselves to suppose that $\widehat{\chi_{f,E}}$ does not vanish on F. We therefore indicate that (11) is always true when F is a vectorspace such that $\widehat{\chi_{f,E}}$ vanishes on F according to Remark 12. We have

Proposition 13 *Let $n > 1$ be a positive integer. Let F be a vector space of $\mathbb{F}_2^n$ and E be a subset of $\mathbb{F}_2^n$. Let $R_1(f, E, F)$ be defined in Proposition 11. Then $R_1(f, E, F) = 0$ for every hyperplane F if and only if $T_2(f, E, u) = 0$ for every $u \neq 0$.*

Proof Clearly, if $T_2(f, E, u) = 0$ for every $u \neq 0$, (11) holds. Suppose now that (11) holds. Every hyperplane F can be written as $F = \{0, \gamma\}^{\perp}$. Therefore, (11) rewrites as

$$\sum_{\substack{u+v \in \{0,\gamma\} \\ u,v \notin \{0,\gamma\}}} T_2(f, E, u)T_2(f, E, v) = 0.$$

Now

$$\sum_{\substack{u+v \in \{0,\gamma\} \\ u,v \notin \{0,\gamma\}}} T_2(f, E, u)T_2(f, E, v)$$
$$= \sum_{u \notin \{0,\gamma\}} (T_2(f, E, u))^2 + \sum_{u \notin \{0,\gamma\}} T_2(f, E, u)T_2(f, E, u+\gamma). \tag{12}$$

Suppose that (12) holds for every $\gamma \neq 0$. Then

$$\begin{aligned}
0 &= \sum_{\gamma \neq 0} \sum_{u \notin \{0,\gamma\}} (T_2(f, E, u))^2 + \sum_{\gamma \neq 0} \sum_{u \notin \{0,\gamma\}} T_2(f, E, u) T_2(f, E, u+\gamma) \\
&= \sum_{u \neq 0} (T_2(f, E, u))^2 \sum_{\gamma \notin \{0,u\}} 1 + \sum_{u \neq 0} T_2(f, E, u) \sum_{\gamma \notin \{0,u\}} T_2(f, E, u+\gamma) \\
&= (2^n - 2) \sum_{u \neq 0} (T_2(f, E, u))^2 + \sum_{u \neq 0} T_2(f, E, u) \sum_{\gamma \notin \{0,u\}} T_2(f, E, \gamma) \\
&= (2^n - 2) \sum_{u \neq 0} (T_2(f, E, u))^2 + \left(\sum_{u \neq 0} T_2(f, E, u) \sum_{\gamma \neq 0} T_2(f, E, \gamma) - \sum_{u \neq 0} (T_2(f, E, u))^2 \right) \\
&= (2^n - 3) \sum_{u \neq 0} (T_2(f, E, u))^2 + \left(\sum_{u \neq 0} T_2(f, E, u) \right)^2 .
\end{aligned}$$

Hence, $\sum_{u \neq 0} (T_2(f, E, u))^2 = 0$ implying that $T_2(f, E, u) = 0$ for every $u \neq 0$. □

We immediately deduce the following corollary.

Corollary 14 *Let $n > 1$ be a positive integer. Let F be a vector space of $\mathbb{F}_2^n$ and E be a subset of $\mathbb{F}_2^n$. Let $R_\ell(f, E, F)$ be defined in Proposition 11. Then $R_\ell(f, E, F) = 0$ for every hyperplane F if and only if $T_2(f, E, u) = 0$ for every $u \neq 0$.*

Proof Clearly, if $T_2(f, E, u) = 0$ for every $u \neq 0$, then $R_\ell(f, E, F) = 0$ for any hyperplane F. Conversely, suppose that $R_\ell(f, E, F) = 0$ for every hyperplane F. According to Remark 12, we have $0 \leq R_1(f, E, F) \leq R_\ell(f, E, F) = 0$. We then conclude thanks to Proposition 13 that $T_2(f, E, u) = 0$ for every $u \neq 0$. □

4 Boolean functions with constant weight inputs

In this subsection, we shall consider the subsets $E = \{x \in \mathbb{F}_2^n \mid \mathrm{wt}(x) = k\}$ for $0 \leq k \leq n$. In the sequel, when x and y are in $\mathbb{F}_2^n$, we shall denote by $z = xy$ the element of $\mathbb{F}_2^n$ such that $z_i = x_i y_i$ for every $1 \leq i \leq n$. Set $E + E = \{x + y,\ (x, y) \in E^2\}$.

Let us investigate the particular cases where $k \in \{0, 1, n-1, n\}$. If $k = 0$, $\widehat{\chi_{f,E}}(a) = (-1)^{f(0)}$ while, if $k = n$, $\widehat{\chi_{f,E}}(a) = (-1)^{f(1)+\mathrm{wt}(a)}$. In both cases, it implies that $NL_E(f) = 0$. On the other hand, denote e_i the element of $\mathbb{F}_2^n$ whose all coordinates are equal to 0 except the ith coordinate. Then, if $k = 1$, $\widehat{\chi_{f,E}}(a) = \sum_{i=1}^n (-1)^{a_i + f(e_i)}$ where a_i stands for the ith-coordinate of a. Now, if $a_i = f(e_i)$ for every $1 \leq i \leq n$, then $\widehat{\chi_{f,E}}(a) = n$ and thus $NL_E(f) = \frac{n}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} |\widehat{\chi_{f,E}}(a)| \leq 0$. If $k = n-1$, given $x \in \mathbb{F}_2^n$, we denote $\bar{x}$ the element of $\mathbb{F}_2^n$ such that $\bar{x}_i = 1 + x_i$. Then, $\widehat{\chi_{f,E}}(a) = \sum_{i=1}^n (-1)^{a_i + \mathrm{wt}(a) + f(\bar{e}_i)}$. Hence, if $a_i = f(\bar{e}_i) + \mathrm{wt}(a) \mod 2$ for every $1 \leq i \leq n$ then, we can conclude as precedingly that $NL_E(f) = 0$. In the sequel, we shall therefore suppose that $2 \leq k \leq n-2$.

Let us now prove the following.

Lemma 15 $E+E=\{x+y,\ (x,y)\in E^2\}=\{a\in\mathbb{F}_2^n \mid \mathrm{wt}(a)\le\min(2k,n),\ \mathrm{wt}(a)=0 \bmod 2\}$. *Furthermore, for every $a\in\mathbb{F}_2^n$, x and $x+a$ are both in E if and only if* $\mathrm{wt}(x)=k$ *and* $\mathrm{wt}(ax)=\frac{\mathrm{wt}(a)}{2}$.

Proof Recall that $\mathrm{wt}(x+y)=\mathrm{wt}(x)+\mathrm{wt}(y)-2\mathrm{wt}(xy)$. Now the latter equation in x has a solution in E for every a of even hamming weight at most $2k$. □

According to the above proposition, if u is of even Hamming weight at most $2k$,

$$T_2(f,E,u)=\sum_{\substack{x,y\in E\\ x+y=u}}(-1)^{f(x)+f(y)}=\sum_{\substack{x\in E\\ \mathrm{wt}(ux)=\frac{\mathrm{wt}(u)}{2}}}(-1)^{D_uf(x)}, \tag{13}$$

while $T_2(f,E,u)=0$ if $\mathrm{wt}(u)$ is odd or greater than $2k$. Note, that if $u=0$ then $T_2(f,E,0)=|E|$.

We then establish the following new upper bound on NL_E.

Theorem 16 *Let $2\le k\le n-2$. Set $E=\{x\in\mathbb{F}_2^n \mid \mathrm{wt}(x)=k\}$. Let f be a Boolean function over $\mathbb{F}_2^n$. Then,*

$$NL_E(f)\le\frac{\binom{n}{k}}{2}-\frac{1}{2}\sqrt{\binom{n}{k}+\lambda+\max\left(\theta,\frac{1}{\binom{n}{k}}\gamma-\lambda\right)}, \tag{14}$$

where

$$\lambda=\max_{\substack{u\neq 0\\ \mathrm{wt}(u)\equiv 0 \pmod 2}}\left|\sum_{\substack{x\in E\\ \mathrm{wt}(ux)=\frac{\mathrm{wt}(u)}{2}}}(-1)^{D_uf(x)}\right|, \tag{15}$$

$$\gamma=\sum_{\substack{u\neq 0\\ \mathrm{wt}(u)\equiv 0 \pmod 2}}\left(\sum_{\substack{x\in E\\ \mathrm{wt}(ux)=\frac{\mathrm{wt}(u)}{2}}}(-1)^{D_uf(x)}\right)^2 \tag{16}$$

and

$$\theta=\frac{1}{\binom{n}{k}+\lambda}\left(\gamma-\lambda^2\right)\ge 0. \tag{17}$$

Proof Let $\gamma\neq 0$ be such that $|T_2(f,E,\gamma)|=\lambda$. According to Equation (8), when $F=\{0,\gamma\}^\perp$:

$$\frac{S_4(f,E,F)}{S_2(f,E,F)}=|E|+T_2(f,E,\gamma)+\frac{\sum_{\substack{u+v\in\{0,\gamma\}\\ u,v\notin\{0,\gamma\}}}T_2(f,E,u)T_2(f,E,v)}{|E|+T_2(f,E,\gamma)}$$

We have to distinguish two cases depending on the sign of $T_2(f,E,\gamma)$:

- If $T_2(f, E, \gamma)$ is nonnegative, then
$$\frac{S_4(f,E,F)}{S_2(f,E,F)} = |E| + \lambda + \frac{\sum_{\substack{u+v\in\{0,\gamma\}\\ u,v\notin\{0,\gamma\}}} T_2(f,E,u)T_2(f,E,v)}{|E|+\lambda}$$
Now
$$\sum_{\substack{u+v\in\{0,\gamma\}\\ u,v\notin\{0,\gamma\}}} T_2(f,E,u)T_2(f,E,v) = \sum_{u\notin\{0,\gamma\}} (T_2(f,E,u))^2 + \sum_{u\notin\{0,\gamma\}} T_2(f,E,u)T_2(f,E,u+\gamma)$$
and therefore
$$\frac{S_4(f,E,F)}{S_2(f,E,F)} = |E| + \lambda + \frac{\sum_{u\notin\{0,\gamma\}} (T_2(f,E,u))^2 + \sum_{u\notin\{0,\gamma\}} T_2(f,E,u)T_2(f,E,u+\gamma)}{|E|+\lambda}$$
- If $T_2(f, E, \gamma)$ is negative, that is, $T_2(f, E, \gamma) = -\lambda$. Set $f_v(x) = f(x) + v\cdot x$ with $v \neq 0$. Observe that $T_2(f_v, E, u) = \sum_{\substack{x,y\in E\\ x+y=u}} (-1)^{f_v(x)+f_v(y)} = (-1)^{v\cdot u} T_2(f, E, u)$ for every $u \in \mathbb{F}_2^n$. If we choose v such that $v\cdot\gamma = 1$ (such v exists since $\gamma \neq 0$), then we have $T_2(f_v, E, \gamma) = -T_2(f, E, \gamma) = \lambda$. Furthermore,
$$\frac{S_4(f_v,E,F)}{S_2(f_v,E,F)} = |E| + \lambda + \frac{\sum_{u\notin\{0,\gamma\}} (T_2(f,E,u))^2 - \sum_{u\notin\{0,\gamma\}} T_2(f,E,u)T_2(f,E,u+\gamma)}{|E|+\lambda}$$

Now
$$(|E| - 2NL_E(f))^2 \geq \frac{S_4(f,E,F)}{S_2(f,E,F)}$$
and, according to Lemma 2, $NL_E(f_v) = NL_E(f)$. Thus
$$(|E| - 2NL_E(f))^2 \geq \frac{S_4(f_v,E,F)}{S_2(f_v,E,F)}$$
We therefore conclude from the two above decompositions of $\frac{S_4(f,E,F)}{S_2(f,E,F)}$ and $\frac{S_4(f_v,E,F)}{S_2(f_v,E,F)}$ that:
$$(|E| - 2NL_E(f))^2 \geq |E| + \lambda + \frac{\sum_{u\notin\{0,\gamma\}} (T_2(f,E,u))^2}{|E|+\lambda}$$
proving
$$NL_E(f) \leq \frac{|E|}{2} - \frac{1}{2}\sqrt{|E| + \lambda + \frac{\sum_{u\notin\{0,\gamma\}} (T_2(f,E,u))^2}{|E|+\lambda}}. \tag{18}$$

Next, according to (10), when $F = \{0,\gamma\}^\perp$ with γ of odd weight,
$$\frac{S_4(f,E,F)}{S_2(f,E,F)} = |E| + \frac{\sum_{\substack{u+v\in\{0,\gamma\}\\ u,v\notin\{0,\gamma\}}} T_2(f,E,u)T_2(f,E,v)}{|E|},$$
since $T_2(f, E, \gamma) = 0$. Now, if γ is of odd weight, then, for every $u \notin \{0, \gamma\}$, the weights of u and $u + \gamma$ are of different parity since $\mathrm{wt}(u + \gamma) = \mathrm{wt}(u) + \mathrm{wt}(\gamma) - 2\mathrm{wt}(u\gamma)$. Thus

$T_2(f, E, u)T_2(f, E, u+\gamma) = 0$ for every $u \notin \{0, \gamma\}$ according to Lemma 15. Then, we simply get in that case (since $T_2(f, E, \gamma) = 0$)

$$\frac{S_4(f, E, F)}{S_2(f, E, F)} = |E| + \frac{1}{|E|}\sum_{u \neq 0}(T_2(f, E, u))^2 .$$

yielding that

$$NL_E(f) \leq \frac{|E|}{2} - \frac{1}{2}\sqrt{|E| + \frac{1}{|E|}\sum_{u \neq 0}(T_2(f, E, u))^2} \tag{19}$$

Proposition 16 follows then from (18) and (19). □

Remark 17 Observe that

$$\begin{aligned}\theta - \left(\frac{1}{\binom{n}{k}}\gamma - \lambda\right) &= \frac{1}{\binom{n}{k} + \lambda}\left(\gamma - \lambda^2\right) - \left(\frac{1}{\binom{n}{k}}\gamma - \lambda\right)\\ &= \frac{\lambda}{\binom{n}{k}\left(\binom{n}{k} + \lambda\right)}\left(\binom{n}{k}^2 - \gamma\right).\end{aligned}$$

Thus

$$\max\left(\theta, \frac{1}{\binom{n}{k}}\gamma - \lambda\right) = \begin{cases}\theta & \text{if } \gamma \leq \binom{n}{k}^2\\ \frac{1}{\binom{n}{k}}\gamma - \lambda & \text{if } \gamma > \binom{n}{k}^2\end{cases}$$

We indicate that, if $\gamma > \binom{n}{k}^2$ then $\frac{1}{\binom{n}{k}}\gamma - \lambda > \binom{n}{k} - \lambda \geq 0$.

Remark 18 Observe that, if there exists $u_1 \neq u_2$ such that $|T_2(f, E, u_1)| = |T_2(f, E, u_2)| = \lambda$, $\gamma \geq 2\lambda^2 > \lambda^2$ yielding that $\theta > 0$. Therefore, $\max\left(\theta, \frac{1}{\binom{n}{k}}\gamma - \lambda\right) = 0$ if and only if there exists a unique $u \neq 0$ such that $|T_2(f, E, u)| = \lambda$ and $\theta = 0$, that is, $|T_2(f, E, v)| = 0$ for every $v \notin \{0, u\}$ (observe that $\gamma = T_2(f, E, u)^2 = \lambda^2$ and $\frac{1}{\binom{n}{k}}\gamma - \lambda = \frac{1}{\binom{n}{k}}\lambda(\lambda - \binom{n}{k}) \leq 0$). In other words, if we are not in this situation, $\max\left(\theta, \frac{1}{\binom{n}{k}}\gamma - \lambda\right)$ is positive.

5 Concluding remarks

In the line of the very recent work of Carlet, Méaux and Rotella, we provided a further study of Boolean functions with restricted input. Inspired by the work of Carlet and the first author on the covering radii of binary Reed-Muller codes, we firstly obtained upper bounds on the nonlinearity for Boolean functions with general restricted input. Next, we derived an upper bound in the particular case when the restricted input is the set of vectors of fixed Hamming weight. Our results improved the known upper bound given by Carlet et al. It would be interesting to construct Boolean functions approaching those developed bounds. But such construction would be a very hard work. The reader is kindly invited to join this adventure.

References

1. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, Cambridge (2010)
2. Carlet, C., Mesnager, S.: Improving the upper bounds on the covering radii of binary Reed-Muller codes. IEEE Trans. Inf. Theory **53**(1), 162–173 (2007)
3. Carlet, C., Mesnager, S.: Four decades of research on bent functions. Des. Codes Crypt. **78**(1), 5–50 (2016)
4. Carlet, C., Méaux, P., Rotella, Y.: Boolean functions with restricted input and their robustness; application to the flip cipher. IACR Transactions on Symmetric Cryptology (3), 192–227. https://doi.org/10.13154/tosc.v2017.i3.192-227 (2017)
5. Dillon, J.: Elementary Hadamard difference sets. PhD Thesis, University of Maryland (1974)
6. Méaux, P., Journault, A., Standaert, F.-X., Carlet, C.: Towards stream ciphers for efficient FHE with low-noise ciphertexts. In: EUROCRYPT 2016, pp. 311–343 (2016)
7. Mesnager, S.: Binary Bent Functions: Fundamentals and Results. Springer, Switzerland (2016)
8. Rothaus, O.S.: On “bent” functions. Journal of Combinatorial Theory, Series A **20**, 300–305 (1976)
9. Wang, Q., Johansson, T.: A note on fast algebraic attacks and higher order nonlinearities. In: International Conference on Information Security and Cryptology, Inscrypt 2010, pp. 404–414 (2010)