The nonlinearity of restrictions of direct sums of monomials *

Serge Feukoua † Ana Sălăgean ‡ Pantelimon Stănică §

Abstract

We investigate how the nonlinearity of Boolean functions behaves when the input is restricted to an affine subspace of the original domain. We completely characterize the nonlinearity of such restrictions for the class of direct sums of monomials.

Keywords: Boolean functions, affine spaces, restriction, nonlinearity.

1 Introduction

The restriction of Boolean functions over affine spaces can significantly impact their cryptographic properties, potentially rendering them vulnerable to specific cryptanalytic attacks. In particular, a recent study [3] investigates the stability of the algebraic degree of Boolean functions under such restrictions. This stability is crucial for ensuring robustness against *guess-and-determine attacks*, where an adversary constrains the function's input to a specific affine subspace, thereby reducing the complexity of the attack.

In this paper, we extend this line of research by examining another fundamental cryptographic property, namely the *nonlinearity*. For a Boolean function f, we introduce a notion that captures the minimal possible nonlinearity that f can have when restricted to affine spaces of codimension at most k and analyze this minimal value within an important class of Boolean functions, namely the *direct sum of monomials*. Previous results considered the nonlinearity of such functions when restricted to only certain affine spaces, namely the ones defined by equations of the form $x_i = 0$ or $x_i = 1$, see [7], or to the set of vectors of a specified Hamming weight (such sets are not affine spaces) – see [4].

A key insight from [2] is that for any *bent function* f (a function achieving optimal nonlinearity), the restriction of f to any hyperplane of $\mathbb{F}_2^n$ remains *nearly bent*. This suggests that within the class of bent functions, nonlinearity remains relatively stable under hyperplane restrictions. We will demonstrate that this phenomenon also holds for the classes of *direct sum of monomials*, i.e. their nonlinearity does not decrease much.

*The research of the first two-named authors is supported by EPSRC, UK (EPSRC grant EP/W03378X/1); The work of the third-named author was started during a visit at University of Loughborough in the Spring of 2024. He thanks the host department for the excellent working conditions during his visit.

†Department of Computer Science, University of Loughborough, UK & National Advanced School of Public Work, Cameroon. E-mail: S.C.Feukoua-Jonzo@lboro.ac.uk, feukouaf@yahoo.fr

‡Department of Computer Science, University of Loughborough, UK; E-mail: A.M.Salagean@lboro.ac.uk

§Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943, USA; E-mail: pstanica@nps.edu

2 Preliminaries

We let $\mathbb{F}_2$ be the finite field with two elements and $\mathbb{F}_2^n$ be the vector space over $\mathbb{F}_2$ of dimension n. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is an n-variable Boolean function. It can be uniquely represented in *Algebraic Normal Form* (ANF), that is, as a polynomial function of degree at most one in each variable, $f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i$, with $a_I \in \mathbb{F}_2$ (see e.g. [1]).

The *algebraic degree* of a Boolean function f, denoted by $\deg(f)$, is the degree of its ANF representation. Those functions of algebraic degree at most one (respectively, two) are called *affine* (respectively *quadratic*).

Definition 2.1. *Two Boolean functions f and g in n variables are said to be affinely equivalent if there exists an affine automorphism L of $\mathbb{F}_2^n$, such that $f = g \circ L$, where '$\circ$' is the composition. The functions f and g are said to be EA-equivalent, if there exists an affine automorphism L of $\mathbb{F}_2^n$ and an affine Boolean function ℓ in n variables, such that $f = g \circ L + \ell$.*

The functions of algebraic degree 2 are fully characterized up to affine equivalence:

Lemma 2.2. [6, Chapter 15, Theorem 8] *Every quadratic non-affine function in n variables is EA-equivalent to $x_1x_2 + \cdots + x_{2t-1}x_{2t}$, for some $t \leq \frac{n}{2}$.*

Notation 2.3. *For every n-variable Boolean function f, we denote by $\mathrm{Var}(f)$ the set consisting of all the elements $i \in \{1, \ldots, n\}$ such that x_i appears in at least one term with nonzero coefficient in the ANF of f. For any hyperplane H, $\mathrm{Var}(H)$ will be the set of variables that occur in the defining equation of H.*

Recall that the Walsh-Hadamard transform of a Boolean function f is the function $W_f : \mathbb{F}_2^n \to \mathbb{R}$ defined as $W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u \cdot x}$, for all $u \in \mathbb{F}_2^n$, where "$\cdot$" denotes the usual inner product. The nonlinearity $\mathrm{nl}(f)$ of a Boolean function f over $\mathbb{F}_2^n$ is the minimum Hamming distance $d_H(f, h) = |\{x \in \mathbb{F}_2^n; f(x) \neq h(x)\}|$ between f and affine functions h. We have $\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \left|W_f(a)\right|$ (see, for example [5]).

For our purpose it is useful to use normalized versions of the Walsh-Hadamard transform and nonlinearity.

Definition 2.4. *The normalized Walsh-Hadamard transform of a Boolean function f in n variables, denoted here by NW_f, is the function $\mathrm{NW}_f : \mathbb{F}_2^n \to \mathbb{R}$ defined as $\mathrm{NW}_f(a) = \frac{1}{2^n} W_f(a)$, for all $a \in \mathbb{F}_2^n$. The normalized nonlinearity of f is defined as follows:* $\mathrm{nnl}(f) = \frac{1}{2^n}\mathrm{nl}(f) = \frac{1}{2}\left(1 - \max_{a \in \mathbb{F}_2^n} \left|\mathrm{NW}_f(a)\right|\right)$.

Note that the (normalized) Walsh-Hadamard transform and (normalized) nonlinearity are invariant under EA-equivalence. The (normalized) nonlinearity satisfies the bounds $\mathrm{nl}(f) \leq 2^{n-1} - 2^{n/2-1}$ and $\mathrm{nnl}(f) \leq \frac{1}{2}\left(1 - \frac{1}{2^{\frac{n}{2}}}\right)$, respectively; functions that attain the upper bound are called *bent functions* (in which case n must be even). When n is odd, functions f with $\mathrm{nnl}(f) = \frac{1}{2}\left(1 - \frac{1}{2^{\frac{n-1}{2}}}\right)$ are called *nearly bent* functions.

Remark 2.5. *We can easily check from the definition of the Walsh-Hadamard transform that if a function f in n variables is viewed as a function in $m > n$ variables, that it, as a function $g(x_1, \ldots, x_n, \ldots, x_m) = f(x_1, \ldots, x_n)$ we have $W_g(a, b) = 2^{m-n} W_f(a)$ for all $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^{m-n}$, and $\mathrm{nl}(g) = 2^{m-n}\mathrm{nl}(f)$. However, the normalized versions remain unchanged; namely, $\mathrm{NW}_g(a, b) = \mathrm{NW}_f(a)$ and $\mathrm{nnl}(g) = \mathrm{nnl}(f)$.*

When f is a monomial function of algebraic degree $r \geq 2$, we have $\mathrm{nnl}(f) = \frac{1}{2^r}$. When a function f is a direct sum of two functions g and h in n and m variables, respectively (i.e. $f = g + h$ and $\mathrm{Var}(g) \cap \mathrm{Var}(h) = \emptyset$), it is known that $W_f(a,b) = W_g(a)W_h(b)$ for all $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^{m-n}$ (see [5] for example). This means we also have $\mathrm{NW}_f(a,b) = \mathrm{NW}_g(a)\mathrm{NW}_h(b)$ and therefore, $\mathrm{nnl}(f) = \frac{1}{2}(1 - (1 - 2\mathrm{nnl}(g))(1 - 2\mathrm{nnl}(h))) = \mathrm{nnl}(g) + \mathrm{nnl}(h) - 2\mathrm{nnl}(g)\mathrm{nnl}(h)$. In particular, when $f = f_1 + \cdots + f_m$ is a direct sum of m monomials of degree at least two,

$$\mathrm{nnl}(f) = \frac{1}{2}\left(1 - \prod_{i=1}^{m}\left(1 - \frac{1}{2^{\deg(f_i)-1}}\right)\right). \tag{1}$$

The restriction of a function f to an affine space A will be denoted by $f_{|A}$. If A is defined by k affine equations, that are, after Gaussian elimination: $x_{i_1} = a_{i_1}(y), \ldots, x_{i_k} = a_{i_k}(y)$, where $i_1, \ldots, i_k$ are distinct and $a_j(y)$ are affine functions in $y = (y_1, \ldots, y_{n-k})$, where $\{y_1, \ldots, y_{n-k}\} = \{x_1, \ldots, x_n\} \setminus \{x_{i_1}, \ldots, x_{i_k}\}$. The ANF of $f_{|A}$ is thus a function in the $n-k$ variables $\{y_1, \ldots, y_{n-k}\}$, whose expression depends on the equations used for defining A, although all choices yield functions which are affinely equivalent.

In this work, we are interested in how the normalized nonlinearity of a function changes when we restrict the function to an affine subspace. It turns out that it can decrease, increase, or stay unchanged:

Example 2.6. *Let $f = f_1 + \cdots + f_m$ be a direct sum of monomials of degree $r \geq 2$. We can easily check that for any hyperplane H defined by an equation $x_i = 0$ with $i \in \mathrm{Var}(f_j)$ we have $f_{|H} = f_1 + \cdots + f_{j-1} + f_{j+1} + \ldots + f_k$ and, using* (1)*, we have* $\mathrm{nnl}(f_{|H}) < \mathrm{nnl}(f)$.

Let $S_{r,n}$ be the homogeneous symmetric function of degree r in n variables and let $H_{i,\epsilon}$ be the hyperplane defined by the equation $x_1 + x_2 + \cdots + x_i + \epsilon = 0$, with $\epsilon \in \mathbb{F}_2$. By direct computation, we observe that $\mathrm{nnl}(S_{3,5}) < \mathrm{nnl}((S_{3,5})_{|H_{4,1}})$, $\mathrm{nnl}(S_{3,5}) > \mathrm{nnl}((S_{3,5})_{|H_{4,0}})$ *and* $\mathrm{nnl}(S_{4,5}) = \mathrm{nnl}((S_{4,5})_{|H_{3,0}})$.

We are particularly interested in functions for which the nonlinearity does not decrease much on any of the subspaces of a given codimension k. We are therefore led to define the following notion.

Definition 2.7. *Let f be a Boolean function in n variables and $0 \leq k < n$. The k-restriction nonlinearity of f is defined as* $\mathrm{rnnl}_k(f) = \min_{\mathrm{codim}(A) \leq k}(\mathrm{nnl}(f_{|A}))$, *where A are affine spaces of $\mathbb{F}_2^n$.*

Note that $\mathrm{nnl}(f) = \mathrm{rnnl}_0(f) \geq \mathrm{rnnl}_1(f) \geq \mathrm{rnnl}_2(f) \geq \ldots \geq \mathrm{rnnl}_{n-1}(f) = 0$. Other than the trivial case of affine (including constant) functions, which have nonlinearity zero, we do not know if there are any functions with $\mathrm{nnl}(f) = \mathrm{rnnl}_1(f)$. We will be interested in functions for which $\mathrm{rnnl}_1(f)$ is not much lower than $\mathrm{nnl}(f)$.

We consider first the bent functions, as they have maximal nonlinearity. In [2, Theorem 5.2] it is shown that a Boolean function f in n variables is bent if and only if for every hyperplane H of $\mathbb{F}_2^n$, the restrictions of f to H and $\mathbb{F}_2^n \setminus H$ (viewed as Boolean functions on $\mathbb{F}_2^{n-1}$) are nearly bent and therefore $\mathrm{rnnl}_1(f) = \frac{1}{2}\left(1 - \frac{1}{2^{\frac{n}{2}-1}}\right)$, only slightly lower that $\mathrm{nnl}(f) = \frac{1}{2}\left(1 - \frac{1}{2^{\frac{n}{2}}}\right)$. This means that the nonlinearity of bent functions is relatively stable under restrictions to hyperplane.

3 Direct sums

Theorem 3.1. *Let f be the direct sum of two functions, $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_r) + h(x_{r+1}, \ldots, x_n)$. Let H be a hyperplane such that the equation which defines H contains at least one of the variables that g depends on (i.e.* $\mathrm{Var}(g) \cap \mathrm{Var}(H) \neq \emptyset$*). Then* $\mathrm{nnl}(f_{|H}) \geq \mathrm{nnl}(h)$. *Consequently,* $\mathrm{rnnl}_1(f) \geq \min(\mathrm{nnl}(g), \mathrm{nnl}(h))$.

Proof. Without loss of generality, we can assume that $x_1 \in \mathrm{Var}(g) \cap \mathrm{Var}(H)$; we write the equation of H as

$$x_1 = \mathbf{a}^{(1)} \cdot \mathbf{x}^{(1)} + \mathbf{a}^{(2)} \cdot \mathbf{x}^{(2)} + \epsilon, \tag{2}$$

where $\mathbf{x}^{(1)} = (x_2, \ldots, x_r)$, $\mathbf{x}^{(2)} = (x_{r+1}, \ldots, x_n)$, $\mathbf{a}^{(1)} \in \mathbb{F}_2^{r-1}$, $\mathbf{a}^{(2)} \in \mathbb{F}_2^{n-r}$ and $\epsilon \in \mathbb{F}_2$. Writing g as $g(x_1, \ldots, x_r) = x_1 g_1(\mathbf{x}^{(1)}) + g_2(\mathbf{x}^{(1)})$ for suitable functions g_1, g_2, we obtain $f_{|H}$ by substituting x_1 in f using (2), that is,

$$f_{|H}\left(\mathbf{x}^{(1)}, \mathbf{x}^{(2)}\right) = (\mathbf{a}^{(1)} \cdot \mathbf{x}^{(1)} + \mathbf{a}^{(2)} \cdot \mathbf{x}^{(2)} + \epsilon) g_1(\mathbf{x}^{(1)}) + g_2(\mathbf{x}^{(1)}) + h(\mathbf{x}^{(2)}).$$

The normalized Walsh-Hadamard transform of $f_{|H}$ at $(\mathbf{u}^{(1)}, \mathbf{u}^{(2)})$ with $\mathbf{u}^{(1)} \in \mathbb{F}_2^{r-1}$, $\mathbf{u}^{(2)} \in \mathbb{F}_2^{n-r}$ is

$$\begin{aligned} \mathrm{NW}_{f_{|H}}\left(\mathbf{u}^{(1)}, \mathbf{u}^{(2)}\right) &= \frac{1}{2^{n-1}} \sum_{\mathbf{x}^{(1)} \in \mathbb{F}_2^{r-1}} \sum_{\mathbf{x}^{(2)} \in \mathbb{F}_2^{n-r}} (-1)^{f_{|H}\left(\mathbf{x}^{(1)}, \mathbf{x}^{(2)}\right) + \mathbf{u}^{(1)} \cdot \mathbf{x}^{(1)} + \mathbf{u}^{(2)} \cdot \mathbf{x}^{(2)}} \\ &= \frac{1}{2^{r-1}} \sum_{\mathbf{x}^{(1)} \in \mathbb{F}_2^{r-1}} (-1)^{(\mathbf{a}^{(1)} \cdot \mathbf{x}^{(1)} + \epsilon) g_1(\mathbf{x}^{(1)}) + g_2(\mathbf{x}^{(1)}) + \mathbf{u}^{(1)} \cdot \mathbf{x}^{(1)}} S(\mathbf{x}^{(1)}, \mathbf{u}^{(2)}, \mathbf{a}^{(2)}), \end{aligned} \tag{3}$$

where

$$S\left(\mathbf{x}^{(1)}, \mathbf{u}^{(2)}, \mathbf{a}^{(2)}\right) = \frac{1}{2^{n-r}} \sum_{\mathbf{x}^{(2)} \in \mathbb{F}_2^{n-r}} (-1)^{(\mathbf{a}^{(2)} \cdot \mathbf{x}^{(2)}) g_1(\mathbf{x}^{(1)}) + \mathbf{u}^{(2)} \cdot \mathbf{x}^{(2)} + h(\mathbf{x}^{(2)})} = \mathrm{NW}_h\left(\mathbf{u}^{(2)} + g_1(\mathbf{x}^{(1)}) \mathbf{a}^{(2)}\right),$$

which implies

$$\left| S\left(\mathbf{x}^{(1)}, \mathbf{u}^{(2)}, \mathbf{a}^{(2)}\right) \right| \leq \max_{\mathbf{u}^{(2)} \in \mathbb{F}_2^{n-r}} \left| \mathrm{NW}_h\left(\mathbf{u}^{(2)}\right) \right|. \tag{4}$$

From (3) and (4) we have therefore

$$\begin{aligned} \max_{(\mathbf{u}^{(1)}, \mathbf{u}^{(2)})} \left| \mathrm{NW}_{f_{|H}}\left(\mathbf{u}^{(1)}, \mathbf{u}^{(2)}\right) \right| &\leq \frac{1}{2^{r-1}} \sum_{\mathbf{x}^{(1)} \in \mathbb{F}_2^{r-1}} \left| S\left(\mathbf{x}^{(1)}, \mathbf{u}^{(2)}, \mathbf{a}^{(2)}\right) \right| \\ &\leq \frac{1}{2^{r-1}} 2^{r-1} \max_{\mathbf{u}^{(2)} \in \mathbb{F}_2^{n-r}} \left| \mathrm{NW}_h\left(\mathbf{u}^{(2)}\right) \right| \\ &= \max_{\mathbf{u}^{(2)} \in \mathbb{F}_2^{n-r}} \left| \mathrm{NW}_h\left(\mathbf{u}^{(2)}\right) \right|, \end{aligned}$$

and consequently $\mathrm{nnl}(f_{|H}) \geq \mathrm{nnl}(h)$. □

Corollary 3.2. *Let $f = f_1 + \cdots + f_m$ be a function that is the direct sum of the functions $f_1, \ldots, f_m$. We have:* $\mathrm{rnnl}_1(f) \geq \min_{I \subseteq \{1, \ldots, m\}} \mathrm{nnl}\left(\sum_{i \in I} f_i\right)$.

For a function that is a direct sum of monomials, we can obtain a more explicit result than Corollary 3.2.

Theorem 3.3. *Let $f = f_1 + \cdots + f_m$ be a function that is the direct sum of the monomials $f_1, \ldots, f_m$ with $m \geq 2$ and $\deg(f_1) \geq \ldots \geq \deg(f_m) \geq 2$. We have:*

$$\mathrm{rnnl}_1(f) = \mathrm{nnl}(f_1 + \cdots + f_{m-1}) = \frac{1}{2}\left(1 - \prod_{i=1}^{m-1}\left(1 - \frac{1}{2^{\deg(f_i)-1}}\right)\right) = \mathrm{nnl}(f) - \frac{1}{2^{\deg(f_m)}} \prod_{i=1}^{m-1}\left(1 - \frac{1}{2^{\deg(f_i)-1}}\right).$$

Note that the last equality in the theorem above means that the nonlinearity decreases by only a relatively small amount when restricting a direct sum of monomials to a hyperplane. For example, if f is a direct sum of 5 monomials of degree 3, we have $\mathrm{nnl}(f) \approx 0.38$ and $\mathrm{nnl}_1(f) \approx 0.34$, a decrease of about 0.04.

Corollary 3.4. *If* $f(x_1, \ldots, x_{2t}) = x_1x_2 + \cdots + x_{2t-1}x_{2t}$, *then* $\mathrm{rnnl}_1(f) = \frac{1}{2}\left(1 - \frac{1}{2^{t-1}}\right) = \mathrm{nnl}(f) - \frac{1}{2^{t+1}}$.

The next result generalizes Theorem 3.3 to direct sums of m monomials restricted to affine spaces of codimension k, using a similar proof technique, combined with a careful choice of the variables that will be substituted. It suffices to consider the case $k < m$, since, when $k \geq m$, we obviously have $\mathrm{rnnl}_k(f) = 0$ as $f_{|A} = 0$ for the vector space A defined by the equations $x_{i_j} = 0$, $j = 1, \ldots, k$, where the variables x_{i_j} were picked ensuring that at least one is picked from each monomial of f.

Theorem 3.5. *Let* $m \geq 2$ *and* $0 < k < m$ *and* $f = f_1 + f_2 + \cdots + f_m$ *be a direct sum of monomials with* $\deg(f_1) \geq \ldots \geq \deg(f_m) \geq 2$. *Then,* $\mathrm{rnnl}_k(f) = \mathrm{nnl}(f_1 + f_2 + \cdots + f_{m-k}) = \frac{1}{2}\left(1 - \prod_{i=1}^{m-k}\left(1 - \frac{1}{2^{\deg(f_i)-1}}\right)\right)$.

Corollary 3.6. *If* $f(x_1, \ldots, x_{2t}) = x_1x_2 + \cdots + x_{2t-1}x_{2t}$, *then for all* $k \leq t$, $\mathrm{rnnl}_k(f) = \frac{1}{2}\left(1 - \frac{1}{2^{t-k}}\right)$.

Note that alternative proofs for Corollaries 3.4 and 3.6 can be obtained using the results in [3].

References

[1] C. Carlet. *Boolean Functions for Cryptography and Error Correcting Codes. Cambridge University Press*, 2021.

[2] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. "On cryptographic properties of the cosets of $R(1, m)$". IEEE Transactions on Information Theory 47 (2001), pp. 1494–1513.

[3] C. Carlet, S. Feukoua, and A. Sălăgean. "The stability of the algebraic degree of Boolean functions when restricted to affine spaces". *arXiv preprint arXiv:2409.20211* (2024).

[4] C. Carlet, P. Méaux, and Y. Rotella. "Boolean functions with restricted input and their robustness; application to the FLIP cipher". *Cryptology ePrint Archive* (2017).

[5] T. W. Cusick and P. Stănică. *Cryptographic Boolean functions and applications*. 2nd ed. Academic Press, 2017.

[6] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1978.

[7] P. Méaux, A. Journault, F. X. Standaert, and C. Carlet. "Towards stream ciphers for efficient FHE with low-noise ciphertexts". *Eurocrypt*. Springer. 2016, pp. 311–343.