THREE PARAMETERS OF BOOLEAN FUNCTIONS RELATED TO THEIR CONSTANCY ON AFFINE SPACES

CLAUSE CARLET

LAGA, Department of Mathematics, University of Paris 8 (and Paris 13 and CNRS)
Saint–Denis cedex 02, France
and University of Bergen, Norway

SERGE FEUKOUA*

University of Yaoundé 1
Faculty of Sciences, Department of Mathematics
P.O.BOX 812 Yaoundé, Cameroon

(Communicated by Sihem Mesnager)

Abstract. The $k$-normality of Boolean functions is an important notion initially introduced by Dobbertin and studied in several papers. The parameter related to this notion is the maximal dimension of those affine spaces contained in the support $\text{supp}(f)$ of the function or in its co-support $\text{cosupp}(f)$. We denote it by $\text{norm}(f)$ and call it the norm of $f$.

The norm concerns only the affine spaces contained in either the support or the co-support; the information it provides on $f$ is then somewhat incomplete (for instance, two functions constant on a hyperplane will have the same very large parameter value, while they can have very different complexities). A second parameter which completes the information given by the first one is the minimum between the maximal dimension of those affine spaces contained in $\text{supp}(f)$ and the maximal dimension of those contained in $\text{cosupp}(f)$ (while $\text{norm}(f)$ equals the maximum between these two maximal dimensions). We denote it by $\text{cons}(f)$ and call it the (affine) constancy of $f$.

The value of $\text{cons}(f)$ gives global information on $f$, but no information on what happens around each point of $\text{supp}(f)$ or $\text{cosupp}(f)$. We define then its local version, equal to the minimum, when $a$ ranges over $\mathbb{F}_2^n$, of the maximal dimension of those affine spaces which contain $a$ and on which $f$ is constant.

We denote it by $\text{stab}(f)$ and call it the stability of $f$.

We study the properties of these three parameters. We have $\text{norm}(f) \geq \text{cons}(f) \geq \text{stab}(f)$, then for determining to which extent these three parameters are distinct, we exhibit four infinite classes of Boolean functions, which show that all cases can occur, where each of these two inequalities can be strict or large.

We consider the minimal value of $\text{stab}(f)$ (resp. $\text{cons}(f)$, $\text{norm}(f)$), when $f$ ranges over the Reed-Muller code $\text{RM}(r, n)$ of length $2^n$ and order $r$, and we denote it by $\text{stab}_{\text{RM}}(r, n)$ (resp. $\text{cons}_{\text{RM}}(r, n)$, $\text{norm}_{\text{RM}}(r, n)$). We give upper bounds for each of these three integer sequences, and determine the exact values of $\text{stab}_{\text{RM}}(r, n)$ and $\text{cons}_{\text{RM}}(r, n)$ for $r \in \{1, 2, n - 2, n - 1, n\}$, and of $\text{norm}_{\text{RM}}(r, n)$ for $r = 1, 2$.

2010 Mathematics Subject Classification: 06E30, 94C10, 94A60, 11T71, 05E99.
Key words and phrases: Boolean functions, affine spaces, normality.

* The work of this author was partially supported by PRMAIS.
1. Introduction

Let \( n \) and \( k \) be two positive integers with \( k \leq n \). An \( n \)-variable Boolean function \( f \) is called \( k \)-normal if it is constant on at least one \( k \)-dimensional affine subspace of \( \mathbb{F}_2^n \), that is, if the support of \( f \) (denoted by \( \text{supp}(f) \)) or the co-support of \( f \) (denoted by \( \text{cosupp}(f) \)) contains an affine space of dimension \( k \). H. Dobbertin introduced this notion in [15] by calling normal those \( n \)-variable Boolean functions with \( n \) even which are called \( n/2 \)-normal in the terminology above. All known bent functions (a category of functions which plays a role in cryptography and in error correcting codes like Kerdock codes, see [8, 19]) were normal and the question solved (positively) by Dobbertin was the existence of non-normal bent functions (see [4]). He also showed how constructing balanced functions with high nonlinearities from normal bent functions and its construction is generalizable to normal functions of high nonlinearity. These functions therefore have a cryptographic advantage. However, the high normality of a function used in an algorithm is a potential weakness because the fact that the function is constant over a large space is likely to be used for example in a “guess and determine” type attack, where the attacker would make the assumption that the entry of the function is in the affine space where it is constant.

A natural parameter related to the notion of normality is the maximal dimension of affine spaces on which \( f \) is constant. We denote it by \( \text{norm}(f) \).

The fact that a given function \( f \) is \( k \)-normal gives information on its support or on its co-support but not on both. It seems then also interesting to consider the possibility that both the support and the co-support of the function contain affine spaces of dimension \( k \). This leads to the parameter that we shall denote by \( \text{cons}(f) \), equal to the minimum between the maximum dimension of affine spaces contained in the support of \( f \) and the maximum of those contained in its co-support.

But \( \text{cons}(f) \) gives no information, for each point \( a \) of \( \mathbb{F}_2^n \), on the maximal dimension of those affine spaces containing \( a \) and on which \( f \) is constant. We denote by \( \text{stab}(f) \) and call stability of \( f \) the minimum for all \( a \in \mathbb{F}_2^n \) of the maximal dimension of affine spaces containing \( a \) on which \( f \) is constant.

Studying these three parameters for general Boolean functions should allow increasing our knowledge on the supports of Boolean functions (one of the approaches to cryptographic weaknesses of Boolean functions consists in studying their local affinity, and the most basic and easiest to handle case of affinity is constance). Such study in the case of bounded algebraic degree (i.e. in Reed-Muller codes) would be also useful.

Little is known on the structure of the support and of the co-support of a Boolean function of given algebraic degree, except for the results by Assmus [1] and those of J. C. C. McKinsey [21] (on the continuity of Boolean functions).

The behavior of Boolean and vectorial functions on flats (i.e. affine spaces) has been studied in [18], but in a different way (by studying those flats on which the function is affine - which is of course close to our study but happens to be quite different in practice, or whose images by a given vectorial function are flats, which is also a very interesting question).

The uniform continuity defined in [21, Definition 6], which may look apparently close to what we do in this paper, is in fact very different also, because it is based on a metric space topology, not at all the same as ours (if we consider that stability can be considered as a form of continuity); in our case, the “neighborhoods” are affine subspaces.
The paper is organized as follows:
- in Section 2, we give some basic definitions and properties on Boolean functions useful for our results;
- in Section 3, we study these three parameters and their properties. We develop an approach using the Walsh transform and the Poisson summation formula (see e.g. [8, Relation 28]). We also study the behavior of the three parameters in the subcase of bent functions since normality has been first defined in the framework of these functions;
- by definition, we have \( \text{stab}(f) \leq \text{cons}(f) \leq \text{norm}(f) \) for general functions, and we need to know if the three parameters are distinct but can also coincide in some cases. In Section 4, we search then four examples of classes of Boolean functions showing that each of these two inequalities can be strict or large independently of the other. We exhibit such examples thanks to the study of the three parameters in the two sets of quadratic functions and of Kasami-Tokura functions (see [17]);
- in Section 5, we consider the minimal value of \( \text{stab}(f) \) (resp. \( \text{cons}(f) \), resp. \( \text{norm}(f) \)), when \( r \) ranges over the Reed-Muller code \( RM(r,n) \) of length \( 2^n \) and order \( r \), and we denote it by \( \text{stab}_{RM(r,n)} \) (resp. \( \text{cons}_{RM(r,n)} \), resp. \( \text{norm}_{RM(r,n)} \)).

In [13], Cohen and Tal generalize the minimum \( \text{norm}_{RM(r,n)} \) in \( \mathbb{F}_q \) denoted by \( k_q(n,r) \) and they link this minimum to the good affine dispersers (recall that an affine disperser for dimension \( k \) is a function \( f : \mathbb{F}_q^k \rightarrow \mathbb{F}_q \) with the following property. For every affine subspace \( u_0 + U \subseteq \mathbb{F}_q^k \) of dimension \( k \), \( f \) restricted to \( u_0 + U \) is not constant). They also study an approach of the minimum \( \text{stab}_{RM(r,n)} \) but most of their work consists to provide bounds for these minima and they do not give exact values for them. Here we focus on the case \( q = 2 \) and give a formal study when \( n \) is fixed.

The idea is to see if a Boolean function \( f \) is all the more “stable” (i.e. that \( \text{stab}(f) \), \( \text{cons}(f) \) and \( \text{norm}(f) \) are larger), as \( f \) has low algebraic degree. We shall also see that the nonlinearity of a function \( f \) (that is the Hamming distance between \( f \) and the set of all affine functions) is all the more small as \( \text{stab}(f) \), \( \text{cons}(f) \) and \( \text{norm}(f) \) are larger. Such connections between some of the most important cryptographic and coding theoretic parameters of Boolean functions (their algebraic degree and their nonlinearity) and a mix of topology and linear algebra seems interesting to study, but happens to be difficult to evaluate. Note that the parameter \( \text{stab} \) which is local, corresponds better to “guess and determine” attacks since the attacker does not have the choice of the affine space in which the input to the Boolean function will be. Besides Boyar and Find in [2] related normality to another cryptographic feature called algebraic thickness, introduced by Carlet in [6] and which is related to the so called “higher order differential attack”. In fact our three parameters can be related to this parameter. We give an upper bound for each sequence above, determine the exact values of \( \text{stab}_{RM(r,n)} \) and \( \text{cons}_{RM(r,n)} \) for \( r \in \{1, 2, n-2, n-1, n\} \), and the exact values of \( \text{norm}_{RM(r,n)} \) for \( r = 1, 2 \).

2. Preliminaries

In this document, \( \mathbb{F}_2^n \) denotes the vector space over the field \( \mathbb{F}_2 \) of all binary vectors of length \( n \). We call Boolean function on \( \mathbb{F}_2^n \), or \( n \)-variable Boolean function, every function from \( \mathbb{F}_2^n \) to \( \mathbb{F}_2 \). The set of all Boolean functions on \( \mathbb{F}_2^n \) is denoted by \( 2^{\mathbb{F}_2^n} \). There is a bijective correspondence between the set \( 2^{\mathbb{F}_2^n} \) and the quotient group \( \mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n) \); a Boolean function can then be seen as an element of this quotient group (see e.g. [8]). The representation in this quotient ring...
is called the *Algebraic Normal Form* (in brief, ANF) of the Boolean function. Note that every coordinate $x_i$ in the ANF appears with exponent at most 1, because every bit in $\mathbb{F}_2$ is its own square. The *algebraic degree* of a Boolean function $f$, denoted by $\deg(f)$, is the degree of its ANF. Those functions of algebraic degree 2 (resp. 3) are called *quadratic* (resp. *cubic*). The set of all $n$-variable Boolean functions of algebraic degree at most $r$ is denoted by $\text{RM}(r,n)$ and called the Reed-Muller code of order $r$. For every binary vector $x \in \mathbb{F}_2^n$, the Hamming weight $w_H(x)$ of $x$ being the number of its non zero coordinates (i.e. the size of the set $\{ i \in N/ x_i \neq 0 \}$, called the support of $x$ denoted by $\text{supp}(x)$), where $N$ denotes the set $\{1,\ldots,n\}$, the Hamming weight $w_H(f)$ of a Boolean function $f$ on $\mathbb{F}_2^n$ is also the size of the support of the function, i.e. of the set $\{ x \in \mathbb{F}_2^n / f(x) = 1 \}$, denoted by $\text{supp}(f)$. We denote then by $\text{cosupp}(f)$ the set $\{ x \in \mathbb{F}_2^n / f(x) = 0 \}$. Moreover, the nonlinearity 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 $h$ (in other words, the distance from $f$ to $\text{RM}(1,n)$, the Reed-Muller code of order 1, since this code equals the set of functions of algebraic degree at most 1, viewed as binary vectors of length $2^n$). In general, the $r$-th order nonlinearity (where $r$ is a positive integer) of a Boolean function $f$ over $\mathbb{F}_2^n$ denoted by $n_{l_r}(f)$, is the minimum distance between $f$ and the set $\text{RM}(r,n)$. A Boolean function $f$ over $\mathbb{F}_2^n$ is called *balanced* if its Hamming weight equals $2^{n-1}$. Let us give the following definitions and propositions, useful to understand our subject and needed in our proofs:

**Definition 1.** [15] Let $n$ be an integer. An $n$-variable Boolean function is called $k$-normal if its restriction to some $k$-dimensional affine subspace of $\mathbb{F}_2^n$ is constant.

**Proposition 1.** [19] Let $n,r$ be two integers such that $r \leq n$. Then for all $f \in \text{RM}(r,n)$, we have $w_H(f) \geq 2^{n-r}$. Furthermore, if $n \geq 1$, $\text{RM}(n-1,n)$ equals the set of those Boolean functions such that $w_H(f)$ is even.

The functions of algebraic degree $r$ and of minimal Hamming weight $2^{n-r}$ are characterized in [19]:

**Proposition 2.** [19] The Boolean functions of algebraic degree $r$ and of minimal Hamming weight $2^{n-r}$ are the indicators of $(n-r)$-dimensional flats (i.e. the functions whose supports are $(n-r)$-dimensional affine subspaces of $\mathbb{F}_2^n$).

**Definition 2.** [22, 23] A Boolean function over $\mathbb{F}_2^n$ ($n$ even) is bent if its Hamming distance to the set of all $n$-variable affine Boolean functions (the nonlinearity of $f$) equals $2^{r-1} - 2^{n/2-1}$ (which is optimal).

**Proposition 3.** [22, 23] An $n$-variable Boolean function is bent if and only if its Hamming distance to any affine function equals $2^{n-1} \pm 2^{n/2-1}$. In particular, if $f$ is a bent Boolean function over $\mathbb{F}_2^n$, then $w_H(f) = 2^{n-1} \pm 2^{n/2-1}$. If $f$ is quadratic, the converse is true.

We shall need the next result:

**Proposition 4.** [7] Let $f$ be an $n$-variable Boolean function, $r$ a positive integer smaller than $n$ and $H$ an affine hyperplane of $\mathbb{F}_2^n$. Then the $r$-th order nonlinearity of the restriction $f_0$ of $f$ to $H$ (viewed as an $n-1$-variable function) satisfies:

$$n_{l_r}(f_0) \geq n_{l_r}(f) - 2^{n-2}$$

**Definition 3.** The Fourier-Hadamard transform of a Boolean function $f$, or more generally of an integer-valued function over $\mathbb{F}_2^n$, is the function denoted by $\hat{f}$ and
defined by:
\[ \hat{f}(u) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{u \cdot x} \text{ for all } u \in \mathbb{F}_2^n \text{ (sum in } \mathbb{Z}) , \]
where “\( \cdot \)” is some chosen inner product, that is, where \( x \cdot y \) is a bilinear form and \( x \cdot y = 0 \) for every \( y \in \mathbb{F}_2^n \) if and only if \( x = 0 \) (i.e. the only element orthogonal to \( \mathbb{F}_2^n \) is 0). Moreover, the Walsh transform of \( f \), denoted by \( W_f \), is the Fourier-Hadamard transform of the sign function \( f(x) = (-1)^{f(x)} \):
\[ W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u \cdot x} \text{ for all } u \in \mathbb{F}_2^n . \]

The Poisson summation formula will be useful

**Proposition 5.** [7] For every \( n \)-variable Boolean or more generally integer-valued function \( f \) on \( \mathbb{F}_2^n \), for every vector subspace \( E \) of \( \mathbb{F}_2^n \), and for every elements \( a \) and \( b \) of \( \mathbb{F}_2^n \), we have:
\[ \sum_{u \in b+E^\perp} (-1)^{a \cdot u} \hat{f}(u) = |E^\perp| (-1)^{a \cdot b} \sum_{x \in a+E} (-1)^{b \cdot x} f(x) . \]

We define in what follows the notions of affine equivalence, of affine invariance and some notation useful in Section 3.

**Definition 4.** Two Boolean functions \( f \) and \( g \) are said affinely equivalent if there exists \( L \), an affine automorphism of \( \mathbb{F}_2^n \), such that \( f = g \circ L \) where \( \circ \) is the operation of composition.

Recall that an affine automorphism of \( \mathbb{F}_2^n \) is a function \( L : \)
\[ \left( \begin{array}{c} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{array} \right) \rightarrow M \left( \begin{array}{c} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{array} \right) \]
\[ + \left( \begin{array}{c} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{array} \right) \text{ where } M \text{ is a nonsingular } n \times n \text{ matrix.} \]

A parameter associated to a function is called an affine invariant if it is preserved by affine equivalence. For instance, the Hamming weight and the algebraic degree are affine invariants.

**Notation 1.** Let \( f \) and \( g \) be two Boolean functions, the notation \( f \sim g \) will be used for “\( f \) and \( g \) are affinely equivalent”.

For every Boolean function \( f \), we denote by \( Var(f) \) the set:
\[ \{ i \mid x_i \text{ appears in the ANF of } f \} . \]

The next lemma will be useful in the study of the three parameters for the quadratic functions.

**Lemma 1.** [19, 8] Every quadratic non-affine function is affinely equivalent to \( x_1 x_2 + \cdots + x_{2t-1} x_{2t} \) (where \( t \leq \frac{n}{2} \)) if it has weight smaller than \( 2^{n-1} \), to \( x_1 x_2 + \cdots + x_{2t-1} x_{2t} + 1 \) (where \( t \leq \frac{n}{2} \)) if it has weight greater than \( 2^{n-1} \) and to \( x_1 x_2 + \cdots + x_{2t-1} x_{2t} + x_{2t+1} \) (where \( t \leq \frac{n-1}{2} \)) if it is balanced. 

---

Advances in Mathematics of Communications

Volume XX, No. X (2019), XXX–XXX
We recall now a more general equivalence relation:

**Definition 5.** Two functions $f$ and $g$ are said extended-affine equivalent (in brief, EA-equivalent) if they are affine equivalent up to the addition of an affine Boolean function.

**Proposition 6.** [19, 23] For every even $n$, all quadratic bent functions over $\mathbb{F}_2^n$ are known. For $n \geq 2$, they are the functions EA-equivalent to the function $x_1x_2 + \cdots + x_{n-1}x_n$.

We show in the following that the parameters $\text{stab}(\cdot)$, $\text{cons}(\cdot)$ and $\text{norm}(\cdot)$ are not EA-invariant.

We recall in what follows a class of Boolean functions already used in [10].

**Definition 6.** [10] Let $n$, $p$ and $s$ be three integers such that $p \geq 2$, $s \geq 2$ and $n \geq ps$. We denote by $K_{n,p,s}$ the class of all those Boolean functions on $\mathbb{F}_2^n$ which are the sum of a function of algebraic degree at most $s-1$ and of the direct sum of $p$ monomials of algebraic degree $s$, that is, whose ANF is given by:

$$f(x) = \sum_{i=1}^{p} m_i(x) + h(x)$$

where $\text{deg}(h(x)) \leq s-1$ and $(m_i)_{i=1,...,p}$ is a sequence of monomials with the same algebraic degree $s$ satisfying the condition: $\text{Var}(m_i(x)) \cap \text{Var}(m_j(x)) = \emptyset$ for all $i \neq j$.

We shall need the following result.

**Theorem 1.** ([10], Theorem 1) Let $k$ be a positive integer. Then for every function $f$ of Class $K_{n,p,s}$ with $p \geq k+1$ and $s \geq k+1$, and any affine subspace $E$ of $\mathbb{F}_2^n$ of codimension $k$, the algebraic degree $\text{deg}(f|_E)$ of the restriction $f|_E$ of $f$ to $E$ equals $\text{deg}(f)$.

We observe that if an $n$-variable Boolean function keeps its algebraic degree when restricted to any affine space of some dimension, then its algebraic degree can not decrease when restricted to an affine space of larger dimension. Hence, if for any affine subspace $E$ of $\mathbb{F}_2^n$ of codimension $k$, we have $\text{deg}(f|_E) = \text{deg}(f)$, then $\text{deg}(f|_E) = \text{deg}(f)$ for all affine subspace $E$ of $\mathbb{F}_2^n$ of codimension at most $k$.

Now, we show that Theorem 1 remains true for $p \geq k+1$ and $s = 2$, which shall be needed in the sequel. To this aim, we need the next lemma. Recall that the rank of a quadratic function $f$ denoted by $\text{rk}(f)$ is the rank of the symplectic (i.e. bilinear and null on the diagonal) form $\varphi_f(x,y) = f(x)f(y) + f(x+y) + f(0)$. It is also the even value $2k$ such that $f$ is EA-equivalent to $x_1x_2 + x_3x_4 + \cdots + x_{2k-1}x_{2k}$, see [19]. We have:

**Lemma 2.** Let $f$ be a quadratic Boolean function on $\mathbb{F}_2^n$ and $H$ an affine hyperplane of $\mathbb{F}_2^n$. Then we have:

$$\text{rk}(f) - 2 \leq \text{rk}(f|_H) \leq \text{rk}(f).$$

We give the proof for the paper to be self-contained.

**Proof.** Let $f$ be a quadratic Boolean function on $\mathbb{F}_2^n$ and $H$ be an affine hyperplane of $\mathbb{F}_2^n$. Since $H \subset \mathbb{F}_2^n$, then the inequality $\text{rk}(f|_H) \leq \text{rk}(f)$ holds and it remains to show that $\text{rk}(f|_H) \geq \text{rk}(f) - 2$. By the formula $\text{nl}(f) = 2^{n-1} - 2^{n-\text{rk}(f)/2} - 1$ for all $n$-variable Boolean functions $f$ (see e.g. [19]), this is equivalent to saying that if $\text{nl}(f) = 2^{n-1} - 2^{k-1}$, then we have $\text{nl}(f|_H) \geq 2^{n-2} - 2^{k-1}$ that is,
$nl(f_{|H}) \geq nl(f) - 2^{n-2}$. But this last inequality holds by Proposition 4 and the result follows.

Since for any affine space $E$ of codimension $k$ there exist $k$ affine hyperplanes $H_1, H_2, \ldots, H_k$ (of equations which are linearly independent) such that $E = H_1 \cap H_2 \cap \cdots \cap H_k$, and by the fact that for any function $f$, the restriction $f|_E$ can be given by the equality $f|_E = ((f|_{H_1})|_{H_2})|_{H_3} \ldots|_{H_k}$, Lemma 2 yields:

**Corollary 1.** Let $f$ be a quadratic Boolean function on $\mathbb{F}_2^n$. Then, for all affine spaces $E$ of codimension $k$ of $\mathbb{F}_2^n$ with $k \leq \frac{rk(f)}{2}$, we have:

$$rk(f|_E) \geq rk(f) - 2k.$$  

Then, we have the following Lemma:

**Lemma 3.** Let $n \geq 2$ and $p \geq 1$ be two integers. Then, for every function $f$ in $K_{n,p,2}$ and for any affine subspace $E$ of $\mathbb{F}_2^n$ of codimension at most $p - 1$, we have $deg(f|_E) = 2$.

**Proof.** Thanks to the observation following Theorem 1, we will just prove this result for any affine subspace $E$ of $\mathbb{F}_2^n$ of codimension $k = p - 1$. Now, since for all $f \in K_{n,p,v}$, we have $rk(f) = 2p$ and by taking $k = p - 1$ in Corollary 1, we have $rk(f|_E) \geq 2p - 2(p - 1) = 2$ that is, $deg(f|_E) = 2$.

We need also to recall the class of Kasami and Tokura functions (see [17]). We shall say that an $n$-variable Boolean function $f$ of degree $\nu \geq 2$ is a Kasami-Tokura function (in brief a K-T function), if there exists an integer $\mu \geq 2$ such that:

- $n \geq \nu + \mu$, $\nu \geq \mu$ and $f \sim x_1 x_2 \ldots x_{\nu-\mu} x_{\nu-\mu+1} \ldots x_{\nu} + x_{\nu+1} \ldots x_{\nu+\mu}$, (Note that $f$ is not the 0-function if $\nu - \mu = 0$)

or

- $n \geq \nu + 2\mu - 2$ and $f \sim x_1 x_2 \ldots x_{\nu-2} x_{\nu-1} x_{\nu} + x_{\nu+1} x_{\nu+2} + \cdots + x_{\nu+2\mu-3} x_{\nu+2\mu-2}$.

3. THE THREE PARAMETERS AND THEIR PROPERTIES

In this section, we define the three parameters and give their properties. We give an approach by using poisson summation formula and we give an upper bound for each of them within the class of bent Boolean functions.

**Definition 7.** Let $f$ be a non constant Boolean function on $\mathbb{F}_2^n$. The numbers $\text{norm}(f)$, $\text{cons}(f)$ and $\text{stab}(f)$ are respectively:

$$\text{norm}(f) = \max \{\dim A : A \text{ is an affine subspace of } \mathbb{F}_2^n \text{ such that } f|_A = \text{cst}\},$$

$$\text{cons}(f) = \min_{\epsilon \in \{0, 1\}} \max \{\dim A : A \text{ is an affine subspace of } \mathbb{F}_2^n \text{ such that } f|_A = \epsilon\},$$

$$\text{stab}(f) = \min_{a \in \mathbb{F}_2^n} \max \{\dim A : A \text{ is an affine subspace of } \mathbb{F}_2^n \text{ such that } f|_A = \text{cst and } a \in A\}.$$  

Note that we do not define these three parameters for the constant function 0 (resp. 1) since its support (resp. co-support) is empty and contains then no affine space.

**Remark 1.** From Definition 7, for all $n$-variable Boolean functions $f$, we have $\text{stab}(f) \leq \text{cons}(f) \leq \text{norm}(f)$. Moreover, $\text{stab}(f) = k$ means $k$ is the greatest dimension such that both $\text{supp}(f)$ and $\text{cosupp}(f)$ are covered (exactly) by affine hyperplanes.
spaces of dimensions at least \( k \). In the literature, little is known about affine spaces covering sets, except for the work of Jamison in [16] where is counted, given an \( n \)-dimensional vector space \( V \), the number of \( k \)-dimensional affine spaces covering exactly the non zero elements of \( V \).

**Remark 2.** It is shown in [6] that, for every real \( c > 1 \) and every sequence \((k_n)_{n \in \mathbb{N}}\) of positive integers such that \( c \log_2 n < k_n \leq n \), the density in the set of \( n \)-variable Boolean functions of those \( f \) such that \( \text{norm}(f) \leq k_n \) tends to 1 when \( n \) tends to infinity. Hence, in probability terms, almost all \( n \)-variable functions \( f \) have parameter \( \text{norm}(f) \) lower than or comparable to the base-2-logarithm of their number of variables, which is quite low. Since the two other parameters are not larger, the same is true for them.

**Remark 3.** An affine space \( A \) is included in the support of a Boolean function \( f \) or in its co-support if and only if the indicator \( 1_A \) is an annihilator of \( f \oplus 1 \) or of \( f \) (recall that \( g \) is called an annihilator of \( f \) if and only if the product \( fg \) is the null function) and its dimension is maximal if and only if the algebraic degree of \( 1_A \) (which equals the complement to \( n \) of this dimension) is minimal. Determining \( \text{norm}(f) \) is then a problem similar to determining the algebraic immunity \( AI(f) \) (i.e. the minimal algebraic degree of nonzero annihilators of \( f \) or \( f \oplus 1 \), see e.g. [8]), but when reducing the space of annihilators to the set of minimum weight elements of Reed-Muller codes (which is no more a vector space). Note that, since the minimum is taken over a subset, then for every Boolean function \( f \), we have that \( n = \text{norm}(f) \geq AI(f) \). An interesting question, that we leave open, is the determination of all the Boolean functions for which there is equality.

Recall that, for every \( n \)-variable Boolean function, we have \( AI(f) \leq \left\lceil \frac{n}{2} \right\rceil \). This does not give information on \( \text{norm}(f) \). But the knowledge of \( AI(f) \) provides the upper bound \( \text{norm}(f) \leq n - AI(f) \). For instance, the majority function (whose output equals 1 if and only if its input has Hamming weight at least \( \frac{n}{2} \)) has optimal algebraic immunity \( \left\lceil \frac{n}{2} \right\rceil \), and it is easily seen that its norm reaches the upper bound, that is, that \( \text{norm}(f) = \left\lceil \frac{n}{2} \right\rceil \) (since the support contains the affine space of equations \( x_i + x_{n+1-i} = 1, \ i \leq \frac{n}{2} \) and, for \( n \) odd, \( x_{n+1} = 1 \)).

The parameter \( \text{cons}(f) \) is also related to \( AI(f) \) since it considers as \( AI(f) \), the support and the co-support of \( f \).

Denoting by \( RM(1,n)^* \) the set of all non constant affine functions, for every \( f \) in \( RM(1,n)^* \), both \( \text{supp}(f) \) and \( \text{cosupp}(f) \) are affine hyperplanes (affine subspaces of codimension 1), and we have then the obvious:

**Lemma 4.** Let \( n \geq 2 \) be an integer. Then, for every \( f \) in \( RM(1,n)^* \) we have,

\[
\text{norm}(f) = \text{cons}(f) = \text{stab}(f) = n - 1.
\]

Let \( f \) be an \( n \)-variable (with \( n \geq 2 \)) function of degree at most \( n - 1 \). It is known that \( \text{Card}(\text{supp}(f)) \) and \( \text{Card}(\text{cosupp}(f)) \) are even (see e.g. [8]). Thus, for all \( a \in \mathbb{F}_2^n \) (where \( a \) belongs to \( \text{supp}(f) \) or to \( \text{cosupp}(f) \) ), there exists \( b \neq a \) such that \( f(b) = f(a) \); \( \{a,b\} \) is an affine space of dimension 1. Therefore, we have an obvious lower bound on the three parameters.

**Lemma 5.** Let \( n \) be an integer such that \( n \geq 2 \). Then for every \( f \) of degree at most \( n - 1 \), we have:

\[
\text{norm}(f) \geq \text{cons}(f) \geq \text{stab}(f) \geq 1.
\]
Remark 4. Let $f$ be an $n$-variable Boolean function and let $A$ and $A'$ be affine subspaces of maximal dimension and respectively included in the support of $f$ and its co-support. We have by definition $\text{cons}(f) = \min (\text{dim } A, \text{dim } A')$. Then we have $2^{\text{cons}(f)} \leq \text{Card}(A) \leq w_H(f)$ and $2^{\text{cons}(f)} \leq \text{Card}(A') \leq 2^n - w_H(f)$ (and one of these two inequalities on the left is an equality) which implies $2^{\text{stab}(f)} \leq 2^{\text{cons}(f)} \leq w_H(f) \leq 2^n - 2^{\text{cons}(f)} \leq 2^n - 2^{\text{stab}(f)}$. Thus, we have: $\text{stab}(f) \leq \text{cons}(f) \leq \log_2(\min \{w_H(f), 2^n - w_H(f)\})$.

Moreover, we have $\text{norm}(f) = \max (\text{dim } A, \text{dim } A')$ and we deduce then that $\text{norm}(f) \leq \log_2(\max \{w_H(f), 2^n - w_H(f)\})$.

3.1. Affine invariance of the three parameters. Since the set of affine subspaces of $\mathbb{F}_2^n$ of a given dimension is affine invariant, we shall easily show that the three parameters are also affine invariants. They are a little more than affine invariant since, for all non constant Boolean function $f$, we have by definition $\text{stab}(f) = \text{stab}(1+f)$, $\text{cons}(f) = \text{cons}(1+f)$ and $\text{norm}(f) = \text{norm}(1+f)$. However, we observe that none is EA invariant:

Lemma 6. The parameter $\text{stab}(\cdot)$ (resp. $\text{cons}(\cdot)$, resp. $\text{norm}(\cdot)$) is an affine invariant but is not EA-invariant.

Proof. It is easy to check the affine invariance. For the non EA-invariance, for all $k, n$ two integers such that $2 < k < n$, consider $f_k, g_k \in \text{RM}(k, n)$ defined by $f_k(x) = \prod_{i=1}^k x_i$ and $g_k(x) = f_k(x) + x_n$. Then $f_k$ and $g_k$ are EA-equivalent by definition, and we can easily check that $\text{cons}(g_k) = n - 2 \neq n - k = \text{cons}(f_k)$ and $\text{norm}(g_k) = n - 2 \neq n - 1 = \text{norm}(f_k)$. However, we do not have necessarily $\text{stab}(f_k) \neq \text{stab}(g_k)$. For example, for $k = n - 1$ we can easily check that $\text{stab}(f_{n-1}) = 1 = \text{stab}(g_{n-1})$ and we need then another function for the parameter $\text{stab}(\cdot)$. Thus, for all $n \geq 3$, we consider the functions $f_n = \prod_{i=1}^n x_i$ and $h_n = f_n + x_n$ which are EA-equivalent and clearly, we have $\text{stab}(f_n) = 0$ since $w_H(f_n) = 1$. Moreover, since $\text{supp}(h_n)$ and $\text{cosupp}(h_n)$ contain each at least two elements, then $\text{stab}(h_n) \geq 1 > \text{stab}(f_n)$ which ends the proof.\[\Box\]

3.2. Viewing an $n$-variable function as a function in $n+1$ variables. Adding a dummy (i.e. non-effective) variable $x_{n+1}$ to an $n$-variable Boolean function $f(x_1, \ldots, x_n)$ increases by 1 the value of each parameter $\text{stab}(\cdot)$, $\text{cons}(\cdot)$ and $\text{norm}(\cdot)$:

Lemma 7. Let $f$ be an $n$-variable Boolean function and $g$ the $(n+1)$-variable function defined by $g(x_1, \ldots, x_n, x_{n+1}) = f(x_1, \ldots, x_n)$. Then we have,

$\text{norm}(g) = \text{norm}(f) + 1$ (resp. $\text{cons}(g) = \text{cons}(f) + 1$, resp. $\text{stab}(g) = \text{stab}(f) + 1$).

Proof. The inequalities $\text{norm}(g) \geq \text{norm}(f) + 1$, $\text{cons}(g) \geq \text{cons}(f) + 1$ and $\text{stab}(g) \geq \text{stab}(f) + 1$ hold since for every affine subspace $A$ of $\mathbb{F}_2^n$ of a given dimension $k$ on which $f$ equals 0 (resp. 1), we have that $g$ equals 0 (resp. 1) on the affine subspace $A \times \{0, 1\}$ of $\mathbb{F}_2^{n+1}$ of dimension $k + 1$.

Moreover, let $B$ be an affine subspace of $\mathbb{F}_2^{n+1}$ of dimension $k + 2$, then by considering the hyperplanes $H_0 = \{x : x_{n+1} = 0\}$ and $H_1 = \{x : x_{n+1} = 1\}$ of $\mathbb{F}_2^{n+1}$, we have $\text{dim}(B \cap H_0) \geq k + 1$ or $\text{dim}(B \cap H_1) \geq k + 1$. So, if $g$ is equal to 0 (resp. 1) on $B$, then identifying as an affine subspace $A$ of $\mathbb{F}_2^n$ the one of these two intersections which has dimension at least $k + 1$, we have $f|_A = 0$ (resp. 1). Thus, replacing $k$ by the parameter $\text{norm}(f)$ (resp. $\text{cons}(f)$), we have that supposing $\text{norm}(g) \geq \text{norm}(f) + 2$ (resp. $\text{cons}(g) \geq \text{cons}(f) + 2$) leads to a
contradiction, since there exists then such $B$, either included in the support of $f$ or in its co-support (resp. there exists then such $B_1$ in the support of $f$ and $B_2$ in its co-support). Hence, we have $\text{norm}(g) \leq \text{norm}(f) + 1$ and $\text{cons}(g) \leq \text{cons}(f) + 1$. We have also $\text{stab}(g) \leq \text{stab}(f) + 1$ since otherwise, for every $a \in \mathbb{F}_2^n$, taking $B$ containing for instance $(a,0)$, we arrive to a contradiction as well. \hfill $\Box$

3.3. Restricting a function to an affine space.

**Lemma 8.** Let $f$ be an $n$-variable Boolean function and let $B$ be an affine space such that $B \subseteq \mathbb{F}_2^n$ and $f|_B$ is not constant. Then we have:

$$\text{norm}(f) \geq \text{norm}(f|_B); \text{cons}(f) \geq \text{cons}(f|_B).$$

But we do not have necessarily “$\text{stab}(f|_B) \geq \text{stab}(f)$” or “$\text{stab}(f|_B) \leq \text{stab}(f)$”.

**Proof.** One can easily prove the two first inequalities. Moreover, taking $f(x) = x_1x_2x_3x_4 + x_5 \in RM(4,5)$ and $g(x) = x_1x_2 + x_3 \in RM(2,3)$ and considering the affine spaces $B_1 = \{x \in \mathbb{F}_2^n : x_1 = 0\}$ and $B_2 = \{x \in \mathbb{F}_2^n : x_3 = 0\}$, we have, by a simple verification, $\text{stab}(f|_{B_1}) = 3 > 1 = \text{stab}(f)$ and $\text{stab}(g|_{B_2}) = 0 < 1 = \text{stab}(g)$ which ends the prove. \hfill $\Box$

3.4. Expressing $\text{norm}(\cdot), \text{cons}(\cdot)$ and $\text{stab}(\cdot)$ by means of the Walsh transform. By the Poisson summation formula (see Proposition 5) applied to the sign function $(-1)^{f(x)}$ instead of $f$ and with $b = 0$, a Boolean function $f$ is constant on an affine space $A = a + E$, where $E$ is a vector subspace of $\mathbb{F}_2^n$, if and only if:

$$\sum_{u \in E^\perp} (-1)^{a \cdot u} W_f(u) = \pm 2^n.$$ 

Indeed, if $A$ is $k-$dimensional, we have $\sum_{u \in E^\perp} (-1)^{a \cdot u} W_f(u) = 2^{n-k} \sum_{x \in a + E} (-1)^{f(x)}$.

Denoting by $\mathcal{F}$ the set of all vector subspaces of $\mathbb{F}_2^n$, then we look for those $F$ in $\mathcal{F}$ of minimal dimension, for which there exists $a \in \mathbb{F}_2^n$ such that $\sum_{u \in F} (-1)^{a \cdot u} W_f(u) = \pm 2^n$.

For every non constant function $f$, $\text{norm}(f)$ is then given by the formula:

$$(1) \quad \text{norm}(f) = n - \min_{a \in \mathbb{F}_2^n} \min_{F \in \mathcal{F}} \{ \text{dim } F; F \in \mathcal{F}, \sum_{u \in F} (-1)^{a \cdot u} W_f(u) = \pm 2^n \}.$$ 

We have similarly:

$$\text{cons}(f) = \min \{d, d'\},$$

where:

$$d = n - \min_{a \in \text{supp}(f)} \min_{F \in \mathcal{F}} \{ \text{dim } F; F \in \mathcal{F} \text{ such that } \sum_{u \in F} (-1)^{a \cdot u} W_f(u) = \pm 2^n \};$$

$$d' = n - \min_{a \in \text{cosupp}(f)} \min_{F \in \mathcal{F}} \{ \text{dim } F; F \in \mathcal{F} \text{ such that } \sum_{u \in F} (-1)^{a \cdot u} W_f(u) = \pm 2^n \}.$$ 

And $\text{stab}(f)$ is given by the formula:

$$\text{stab}(f) = n - \max_{a \in \mathbb{F}_2^n} \min_{F \in \mathcal{F}} \{ \text{dim } F; F \in \mathcal{F} \text{ such that } \sum_{u \in F} (-1)^{a \cdot u} W_f(u) = \pm 2^n \}.$$ 

These results will have interesting consequences, for instance on bent functions in the next subsection.
Remark 5. The inverse Walsh transform formula states (see e.g. [8]) that, for every \( a \in \mathbb{F}_2^n \) and every \( n \)-variable Boolean function \( f \), we have \( \sum_{u \in F} (-1)^{a \cdot u} W_f(u) = 2^n (-1)^{f(a)} \). So for \( \text{dim}(F) = n \), every element \( a \in \mathbb{F}_2^n \) fits.

Note that, according to the Poisson formula, for every Boolean function \( f \), every vector subspace \( F \) of \( \mathbb{F}_2^n \), and every \( a \in \mathbb{F}_2^n \), we have \( \sum_{u \in F} (-1)^{a \cdot u} W_f(u) \leq 2^n \). In fact, this is more generally true for every coset of \( F \), i.e., over every affine space, according to the general Poisson summation formula of Proposition 5.

Moreover, if \( F = E^⊥ \) is such that \( \sum_{u \in F} (-1)^{a \cdot u} W_f(u) = \pm 2^n \) then for all superspaces \( F' \) of \( F \), we have \( \sum_{u \in F'} (-1)^{a \cdot u} W_f(u) = \pm 2^n \) since \( f \) is constant on the subspace \( a + F'^⊥ \) of \( a + E \). A consequence of this observation is that if \( f \) is null (resp. equal to 1) on an affine space \( a + E \), then this affine space is maximal (i.e. there is no coset of \( a + E \) different from \( a + E \) on which \( f \) is constant) if and only if no function \( b \cdot x + f(x) \), such that \( b \) is not null and orthogonal to \( E \), is balanced on a hyperplane of \( E^⊥ \) containing \( b \). Indeed, denoting by \( E' \) the union of \( E \) and one of its cosets (this union is a vector space), and by setting \( F = E^⊥ \) and \( F' = E'^⊥ \) (which is a vectorial hyperplane of \( F \) since the dimension of \( F' \) equals the dimension of \( F \) minus 1), then the condition is equivalent to \( \sum_{u \in F'} (-1)^{a \cdot u} W_f(u) = 2^n \) (resp. \(-2^n\)), that is, \( \sum_{u \in F \cap F'} (-1)^{a \cdot u} W_f(u) \neq 0 \), which is equivalent to \( \sum_{x \in a + (F')⊥} (-1)^{b \cdot x + f(x)} \neq 0 \) where \( b \) is such that \( F \setminus F' = b + F' \), i.e. \( b \in F \setminus F' \).

In the following remark, we observe that a function \( f \) has low nonlinearity when it has large stability.

Remark 6. Let \( f \) be an \( n \)-variable Boolean function. Then we have:

\[
\text{nl}(f) \leq 2^{n-1} - 2^n \text{norm}(f) - 1 \leq 2^{n-1} - 2^n \text{cons}(f) - 1 \leq 2^{n-1} - 2^n \text{stab}(f) - 1.
\]

Indeed, let \( E \) and \( E' \) be subspaces of \( \mathbb{F}_2^n \) such that \( E \cap E' = \{0\} \) and whose direct sum equals \( \mathbb{F}_2^n \). Denote by \( k \) the dimension of \( E \). For every \( a \in E' \), let \( h_a \) be the restriction of \( f \) to the coset \( a + E \). It is known (see [3]) that \( \text{nl}(f) \leq 2^{n-1} - 2^{k-1} + \text{nl}(h_a) \) and the result follows since \( \text{nl}(h_a) = 0 \) if \( f \) is constant on \( a + E \).

3.5. Upper bounds within the class of bent Boolean functions. Let \( f \) be a bent function on \( \mathbb{F}_2^n \) where \( n \) is an even integer. Then, there exists a Boolean function (which is also bent) \( f \), called the dual of \( f \), see e.g. [22, 11], such that \( W_f(u) = 2^n (-1)^{f(u)} \). Now if \( F \) is a vector subspace of \( \mathbb{F}_2^n \), then for all \( a \in \mathbb{F}_2^n \), \( \sum_{u \in F} (-1)^{a \cdot u} W_f(u) = 2^n \sum_{u \in F} (-1)^{f(u) + a \cdot u} \), and we are looking then for \( a \) and \( E \) such that:

\[
\sum_{u \in E^⊥} (-1)^{f(u) + a \cdot u} = 2^n \cdot \text{dim} E \sum_{u \in a + E} (-1)^{f(x)} = \pm 2^n.
\]

It is well-known (see [5]) that for any \( n \)-variable bent function, we have \( \text{norm}(f) \leq \frac{n}{2} \). In the next proposition, we recall this result and we give upper bounds for each of the two other parameters in the class of bent Boolean functions, which show that a bent function cannot admit \( \frac{n}{2} \)-dimensional affine spaces in its support and in its co-support.

Proposition 7. Let \( n \geq 2 \) be an even integer and let \( f \) be any \( n \)-variable bent Boolean function. Then,

\[
\text{norm}(f) \leq \frac{n}{2}.
\]
and

\[ \text{stab}(f) \leq \text{cons}(f) \leq \frac{n}{2} - 1. \]

**Proof.** The condition \( \sum_{u \in E^\perp} (-1)\hat{f}(u) \cdot a \cdot u = \pm 2^\frac{n}{2} \) implies \( \dim E^\perp \geq \frac{n}{2} \). Hence, \( \text{stab}(f) \leq \text{cons}(f) \leq \text{norm}(f) \leq \frac{n}{2} \). Now let us show that \( \text{cons}(f) \neq \frac{n}{2} \). If \( \hat{f}(0) = 0 \), then for \( a \in \text{supp}(f) \) and \( E \) a vector space of dimension \( \frac{n}{2} \), we cannot have (2), that is, \( \sum_{u \in E^\perp} (-1)\hat{f}(u) \cdot a \cdot u = \sum_{u \in a + E} (-1)\hat{f}(x) = \pm 2^\frac{n}{2} \), because \( E^\perp \) having size \( 2^{n/2} \) and one of the numbers in the left hand side sum evaluating 1, the sum cannot equal \(-2^\frac{n}{2} \), which would be necessary because of the equality with the right hand side sum and since \(|a + E| = 2^\frac{n}{2} \) and \((-1)^{f(a)} = -1 \). If \( \hat{f}(0) = 1 \), then similarly we cannot have (2) with \( a \in \text{cosupp}(f) \) and \( E \) a vector space of dimension \( \frac{n}{2} \). This completes the proof. \( \square \)

The above bounds are tight. Indeed, consider the classical class of \( n \)-variable bent functions named the Maiorana-McFarland original class denoted here by \( M_n \) where \( n \geq 2 \) is even. Recall that the Maiorana-McFarland class \( M_n \) (see [20, 8]) is the set of all the Boolean functions on \( \mathbb{F}_2^n = \{(x, y); x, y \in \mathbb{F}_2^{n/2}\} \) of the form: \( f(x, y) = x \cdot \pi(y) + g(y) \) where \( \pi \) is any permutation on \( \mathbb{F}_2^{n/2} \) and \( g \) any Boolean function \( \mathbb{F}_2^{n/2} \) (“\( n \)” denotes here an inner product on \( \mathbb{F}_2^{n/2} \)). Then, we have:

**Proposition 8.** Let \( n \geq 2 \) be an even integer. Then, for all \( f \in M_n \) we have:

\[ \text{norm}(f) = \frac{n}{2} \]

\[ \text{stab}(f) = \text{cons}(f) = \frac{n}{2} - 1 \]

**Proof.** The first equality is well-known: let \( f(x, y) = x \cdot \pi(y) + g(y) \), then for all \( e \in \mathbb{F}_2^{n/2} \), denoting by \( A_e \) the affine subspace of \( \mathbb{F}_2^n \) of dimension \( n/2 \) defined by \( A_e = \{(x, e); x \in \mathbb{F}_2^{n/2}\} \), and taking \( e_0 = \pi^{-1}(0) \), we have \( f_{|A_{e_0}} = g(e_0) \) which means by Proposition 7 that \( \text{norm}(f) = \dim A_{e_0} = \frac{n}{2} \). Let us prove now that \( \text{stab}(f) = \frac{n}{2} - 1 \). This will complete the proof. The sets \( A_e \), where \( e \in \mathbb{F}_2^{n/2} \), form a partition of \( \mathbb{F}_2^n \). For every \( a \in A_{e_0} \), we have max \{dim \( A \): \( a \in A \) and \( f_{|A} = \text{cst} \)\} \( \geq \frac{n}{2} \) and for every \( a \in A_e \), with \( e \neq e_0 \), we have max \{dim \( A \): \( a \in A \) and \( f_{|A} = \text{cst} \)\} \( \geq \frac{n}{2} - 1 \). The proof is completed by Proposition 7. \( \square \)

**Remark 7.** We know (see [12]) that every cubic bent function \( f \) on 8 variables is normal, that is, \( \text{norm}(f) = 4 \). Moreover, it is proved in [4] that if \( a \in \mathbb{F}_4 \setminus \mathbb{F}_2 \), then the 10-variable Kasami function \( g(x) = tr_{10}(ax^3 - 2^2 + 1) + tr_{10}(bx) \) (where \( tr_n(.) \) is the trace function on \( \mathbb{F}_2^n \)) is a bent non normal function for some \( b \), meaning that we can find some bent function \( g \) such that \( \text{norm}(g) \leq \frac{n}{2} - 1 \). Then, it will be interesting to investigate those bent functions \( f \) such that \( \text{stab}(f) = \text{cons}(f) = \text{norm}(f) \). However, in the case of the Kasami function, it seems difficult to determine mathematically whether this happens for some \( b \).

**The case of plateaued functions**

A class of \( n \)-variable Boolean functions which generalizes bent functions is the class of plateaued functions, whose Walsh transform takes only the values 0 and \( \pm \mu \), where \( \mu \) is necessarily a power of 2, say \( \mu = 2^r \), with \( r \geq \frac{n}{2} \) if \( n \) is even and \( r \geq \frac{n+1}{2} \) if \( n \) is odd (this positive number \( \mu \) is called the amplitude of the plateaued function, see [9]). So let \( f \) be an \( n \)-variable plateaued function of amplitude \( \mu = 2^r \), then if...
$F$ is a vector subspace of $\mathbb{F}_2^n$ and denoting by $K_f$ the Walsh support of $f$ (i.e. the collection of all $u \in \mathbb{F}_2^n$ such that $W_f(u) \neq 0$), there exists a function $\tilde{f} : K_f \rightarrow \{0, 1\}$ such that for all $a \in \mathbb{F}_2^n$, $\sum_{u \in F} (-1)^{u \cdot a}W_f(u) = 2^r \sum_{u \in F \cap K_f} (-1)^{\tilde{f}(u) + a \cdot u}$.

**Proposition 9.** Let $f$ be an $n$-variable plateaued function of amplitude $\mu = 2^r$, then we have

$$\text{norm}(f) \leq r$$

and

$$\text{stab}(f) \leq \text{cons}(f) \leq r - 1.$$ 

Further, if $W_f(0) = 0$, then we have:

$$\text{norm}(f) \leq r - 1.$$

**Proof.** Let $F = E^\perp$ be a vector space and $a \in \mathbb{F}_2^n$. Then, $K_f$ being the Walsh support of $f$, we have $\sum_{u \in F} (-1)^{a \cdot u}W_f(u) = \pm 2^n$ if and only if $\sum_{u \in F \cap K_f} (-1)^{\tilde{f}(u) + a \cdot u} = \pm 2^{n-r}$. Thus, from Relation (1) and any $F$ being a vector space, we have

$$\text{norm}(f) = n - \min \{\text{dim} F, F \in F \text{ such that } \sum_{u \in F \cap K_f} (-1)^{\tilde{f}(u) + a \cdot u} = \pm 2^{n-r}\}.$$

Since the equality $\sum_{u \in F \cap K_f} (-1)^{\tilde{f}(u) + a \cdot u} = \pm 2^{n-r}$ implies $\text{Card}(F \cap K_f) \geq 2^{n-r}$, then $\text{dim} F \geq n - r$ which implies $\text{norm}(f) \leq r$. Further, suppose $W_f(0) = 0$ and let $E$ be a vector space of dimension $r$. Then, $\text{Card}(E^\perp \cap K_f) < 2^{n-r}$ implies that, for all $a \in \mathbb{F}_2^n$, we have $|\sum_{u \in E^\perp \cap K_f} (-1)^{\tilde{f}(u) + a \cdot u}| < 2^{n-r}$ which implies $\text{norm}(f) \leq r - 1$. Now, suppose $W_f(0) \neq 0$. Without loss of generality, we can take $W_f(0) = 2^r$ that is $\tilde{f}(0) = 0$. Suppose then there exist $a \in \text{supp}(f)$ and $E$ a vector space of dimension $r$ such that $A = a + E \subseteq \text{supp}(f)$. Then, we have $\text{Card}(E^\perp \cap K_f) = 2^{n-r}$ which implies $E^\perp \subseteq K_f$ and by the Poisson summation formula we have, $\sum_{u \in E^\perp} (-1)^{a \cdot u}W_f(u) = 2^r \sum_{u \in E^\perp} (-1)^{a \cdot u + \tilde{f}(u)} = 2^{n-r} \sum_{u \in a + E} (-1)^{\tilde{f}(u)}$. Since $0 \in \cosupp(a \cdot u + \tilde{f}(u))$, then $a \in \cosupp(f)$ which is a contradiction. Hence, $\text{cons}(f) \neq r$, that is, $\text{cons}(f) \leq r - 1$ which ends the proof. \hfill $\square$

**Remark 8.** The Maiorana-McFarland plateaued functions (see [24]) show that the above bounds can be reached for some $r$.

### 4. How distinct are the three parameters?

We have seen $\text{norm}(f) \geq \text{cons}(f) \geq \text{stab}(f)$, and in this section, we show that all four situations can happen where each of these two inequalities can be an equality or be strict. For this purpose, the study of the stability in $\text{RM}(2, n)$ and in the class of the K-T functions will be useful.

#### 4.1. Stability in $\text{RM}(2, n)$.

For all integer $n$ (with $n \geq 2$) and for every function $f$ in $\text{RM}(2, n)$ non constant, we give the exact values of $\text{stab}(f)$, $\text{cons}(f)$ and $\text{norm}(f)$.

#### 4.1.1. The natural classification of $\text{RM}(2, n)$.

Recall that we write $f \sim g$ when two functions $f$ and $g$ are affinely equivalent. For all $t = 1, \ldots, k = \lceil \frac{n}{2} \rceil$ and $\theta = 0, 1, 2$, let:

$$C_{t, \theta, n} = \{f \in \text{RM}(2, n) : f \sim f_{t, \theta, n} = x_1x_2 + \cdots + x_{2t-1}x_{2t} + \theta\}$$

if $\theta = 0, 1,$
and, if \( n > 2t \):
\[
C_{t,2,n} = \{ f \in RM(2, n) : f \sim f_{t,2,n} = x_1x_2 + \cdots + x_{2t-1}x_{2t} + x_{2t+1} \},
\]
and \( C_{t,2,n} = \emptyset \) otherwise (i.e. when \( n \) is even and \( t = k \)). The Hamming weights in \( C_{t,0,n}, C_{t,1,n} \) and \( C_{t,2,n} \) equal respectively \( 2^{n-1} - 2^{n-t-1}, 2^{n-1} + 2^{n-t-1} \) and \( 2^{n-1} \) (since affinely equivalent functions have the same weight). Furthermore, for all \( t = 1, \ldots, k \), we denote by \( C_{t,n} \) the class defined by:
\[
C_{t,n} = \bigcup_{\theta=0}^{2} C_{t,\theta,n}.
\]
According to Lemma 1, and since the nonlinearity in \( C_{t,n} \) equals \( 2^{n-1} - 2^{n-t-1} \) (equivalent functions having the same nonlinearity), \( (C_{t,n})_{t=1,\ldots,k} \) forms a partition of \( RM(2,n) \setminus RM(1,n) \). Then \( (C_{t,\theta,n})_{t=1,\ldots,k} \) forms with \( RM(1,n) \) a partition of \( RM(2,n) \).

The following result is a direct consequence of Proposition 9 (more precisely of its results on norm), since for all \( t = 1, \ldots, k \) and for all \( f \in \{ f_{t,0,n}, f_{t,1,n}, f_{t,2,n} \} \) it is known that \( W_f(u) \in \{ 0, \pm 2^{n-t} \} \) for all \( u \in \mathbb{F}_2^n \) (see [19, 8]), meaning that \( f \) is plateaued of amplitude \( 2^{n-t} \).

**Lemma 9.** Let \( n \geq 2 \) be an integer, \( k = \left\lfloor \frac{n}{2} \right\rfloor \) and let \( A \) be an affine subspace of \( \mathbb{F}_2^n \). For all \( t = 1, \ldots, k \), we have:
\[
\begin{align*}
(f_{t,0,n})_A = \text{cst} & \text{ or } (f_{t,1,n})_A = \text{cst} \implies \text{codim } A \geq t \\
(f_{t,2,n})_A = \text{cst} & \implies \text{codim } A \geq t + 1
\end{align*}
\]

**Remark 9.** Lemma 9 can also be related to Lemma 3. Indeed, for all \( t = 1, \ldots, k \), \( f_{t,0,n}, f_{t,1,n}, f_{t,2,n} \) are all elements of Class \( K_{n,t,2} \). Thus, by Lemma 3, the equality \((f_{t,\theta,n})_A = \text{cst} \) with \( \theta = 0, 1, 2 \) implies \( \text{codim } A \geq t \). In the case \( \theta = 2 \), observe that \( f_{t,2,n} = f_{t,0,n} + x_{2t+1} + 2t+1 \in V a r(f_{t,0,n}) \); let us show that \((f_{t,2,n})_A \neq \text{cst} \), this will complete an alternate proof of the second property. If the equations defining \( A \) are all independent of \( x_{2t+1} \) (that is, if \( A \) is invariant under translation by the vector of Hamming weight 1 with “1” at position \( 2t+1 \)), then since the ANF of \( f_{t,2,n} \) contains \( x_{2t+1} \), it is not constant on \( A \). If some equations defining \( A \) depend on \( x_{2t+1} \), then there exists a hyperplane \( H \) whose equation involves \( x_{2t+1} \) and such that \( A = H \cap B \) where \( B \) is of codimension \( t-1 \); thus, \((f_{t,2,n})_A = (f_{t,0,n})_B + (x_{2t+1})_H \) and by Corollary 1, \( rk((f_{t,0,n})_B) \geq 2 \) and since \((x_{2t+1})_H \) is affine, \((f_{t,2,n})_A \) is of degree 2 and is not constant.

**4.1.2. Exact values of norm \((f)\), cons \((f)\) and stab \((f)\) for all quadratic functions.**

By the above classification and from Lemma 6, the knowledge of the exact values of the parameters \( \text{norm} (f), \text{cons} (f) \) and \( \text{stab} (f) \) when \( f = f_{t,\theta,n} \) with \( t = 1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor \) and \( \theta = 0, 1, 2 \), provides their knowledge for all quadratic functions.

**Proposition 10.** Let \( n \geq 2 \) be an integer and let \( k = \left\lfloor \frac{n}{2} \right\rfloor \). Then, for all \( t = 1, \ldots, k \) and \( \theta = 0, 1, 2 \) we have:
\[
\begin{align*}
\text{norm} (f_{t,\theta,n}) & = n - t, \text{ for } \theta \in \{ 0, 1 \}, \\
\text{norm} (f_{t,2,n}) & = n - t - 1.
\end{align*}
\]

**Proof.** According to Lemma 9, \( \text{norm} (f_{t,\theta,n}) \leq n-t \) for \( \theta \in \{ 0, 1 \} \) and \( \text{norm} (f_{t,2,n}) \leq n-t-1 \). The equalities \( \text{norm} (f_{t,\theta,n}) = n - t \) for \( \theta \in \{ 0, 1 \} \) and \( \text{norm} (f_{t,2,n}) = n - t - 1 \) come respectively from the fact that for all \( \theta \in \{ 0, 1 \} \), \( f_{t,\theta,n} \) is constant on the affine subspace of codimension \( t \) given by the equations \( x_{2t+1} = 0 \) for
Corollary 2. Let the exact value of these minimums when reaches by the affine functions. Then, for all \( t = 1, \ldots, k \) and for all \( \theta = 0, 1, 2 \) we have:

\[
\text{stab} (f_{t,\theta,n}) = \text{cons} (f_{t,\theta,n}) = n - t - 1
\]

Proposition 11. Let \( n \geq 2 \) be an integer and \( k = \lfloor \frac{n}{2} \rfloor \). Then, for all \( t = 1, \ldots, k \) and for all \( \theta = 0, 1, 2 \) we have:

\[
\text{stab} (f_{t,\theta,n}) = \text{cons} (f_{t,\theta,n}) = n - t - 1
\]

Proof. Note that for all \( t = 1, \ldots, k \) and for all \( \theta = 0, 1, 2 \), the inequality \( \text{cons} (f_{t,\theta,n}) \leq n - t - 1 \) is another direct consequence of Proposition 9. Now, let us show that \( \text{stab} (f_{t,\theta,n}) \geq n - t - 1 \). We have then three cases:

- For \( \theta = 2 \), given \( a \), consider \( B_a \) the affine subspace of codimension \( t \) defined by \( B_a = \{ x : x_1 = a_1; x_3 = a_3; \ldots; x_{2t-1} = a_{2t-1} \} \). Clearly, \( f_{|B_a} \) is affine non constant, which implies the sets \( \text{supp}(f_{|B_a}) \) and \( \text{cosupp}(f_{|B_a}) \) are affine subspaces of dimension \( n - t - 1 \), and \( a \in B_a \). Therefore, \( \text{stab} (f) \geq n - t - 1 \).

- For \( \theta = 0 \), consider the affine subspace \( A_0 = \{ x : x_1 = 0; x_3 = 0; \ldots; x_{2t-1} = 0 \} \) of dimension \( n - t \) on which \( f \) is null. For all \( a \in A_0 \), we have \( \max \{ \dim A : f_{|A} = \text{cst} \} \geq \dim A_0 = n - t \). Now, let \( a \notin A_0 \), There exists \( i \in \{ 1, 3, \ldots, 2k - 1 \} \) such that \( a_i = 1 \). Consider \( B_a \) the affine subspace of codimension \( t \) defined by \( B_a = \{ x : x_1 = a_1; x_3 = a_3; \ldots; x_{2t-1} = a_{2t-1} \} \). Clearly, \( f_{|B_a} \) is affine non constant and \( a \in B_a \) which implies \( \text{stab} (f) \geq n - t - 1 \).

- For \( \theta = 1 \), we can use that \( f_{t,1,n} = f_{t,0,n} + 1 \).

This ends the proof since for all \( f \), \( \text{stab} (f) \leq \text{cons} (f) \).

Hence, for all \( t = 1, \ldots, k = \lfloor \frac{n}{2} \rfloor \), we have:

\[
\begin{cases}
\text{stab} (f) = \text{cons} (f) = \text{norm} (f) & \text{for all } f \in C_{t,2,n} \\
\text{stab} (f) = \text{cons} (f) < \text{norm} (f) & \text{for all } f \in C_{t,0,n} \cup C_{t,1,n}.
\end{cases}
\]

Following Propositions 10 and 11, we can deduce the exact values of \( \text{norm}_{RM(2,n)} \), \( \text{cons}_{RM(2,n)} \) and \( \text{stab}_{RM(2,n)} \) which are respectively the minimal values of \( \text{norm} (f) \), \( \text{cons} (f) \) and \( \text{stab} (f) \) when \( f \) ranges over \( RM(2,n) \). To this aim, we first deduce the exact value of these minimums when \( RM(2,n) \) is replaced by Class \( C_{t,n} \).

Corollary 2. Let \( n \geq 2 \) be an integer and \( k = \lfloor \frac{n}{2} \rfloor \). Then, for all \( t = 1, \ldots, k \),

\[
\text{cons}_{C_{t,n}} = \text{stab}_{C_{t,n}} = n - t - 1
\]

and

\[
\text{norm}_{C_{t,n}} = \begin{cases} 
n - t - 1 & \text{for all } t = 1, \ldots, k - 1 \\
\frac{n-1}{2} & \text{for } t = \frac{n-1}{2}, \text{ } n \text{ odd} \\
\frac{n}{2} & \text{for } t = \frac{n}{2}, \text{ } n \text{ even}
\end{cases}
\]

This implies in its turn:

Corollary 3. Let \( n \geq 2 \) be an integer. Then we have:

\[
\text{cons}_{RM(2,n)} = \text{stab}_{RM(2,n)} = \begin{cases} 
\frac{n-1}{2} & \text{if } n \text{ is even} \\
\frac{n}{2} & \text{if } n \text{ is odd}
\end{cases}
\]

\[
\text{norm}_{RM(2,n)} = \begin{cases} 
\frac{n-1}{2} & \text{if } n \text{ is even} \\
\frac{n}{2} & \text{if } n \text{ is odd}
\end{cases}
\]

Proof. Clearly, the minimal values of the three parameters in \( RM(2,n) \) are not reached by the affine functions. Then, \( \text{norm}_{RM(2,n)} \), \( \text{cons}_{RM(2,n)} \) and \( \text{stab}_{RM(2,n)} \) are given by functions in the classes \( C_{t,n} \). Further, since for all \( t = 1, \ldots, k - 1 \), \( \text{cons}_{C_{t+1,n}} = \text{stab}_{C_{t+1,n}} = n - t - 2 < n - t - 1 = \text{stab}_{C_{t,n}} = \text{cons}_{C_{t,n}} \) and \( \text{norm}_{C_{t+1,n}} < \text{norm}_{C_{t,n}} \), then \( \text{norm}_{RM(2,n)} \), \( \text{cons}_{RM(2,n)} \) and \( \text{stab}_{RM(2,n)} \) are
Remark 10. According to Proposition 8 and Corollary 3, \( \text{stab}_{RM(2,n)} \), \( \text{cons}_{RM(2,n)} \) and \( \text{norm}_{RM(2,n)} \) are reached by the bent functions.

Classes \( C_{t,2,n} \) and \( C_{t,0,n} \cup C_{t,1,n} \) provide then two of the four examples we are looking for (see the introduction of this section). It seems very difficult to make the same study for \( RM(3,n) \), \( RM(4,n) \) etc. Nevertheless, we can make the study of the stability in Class K-T and the general form of functions in this class will be used to provide the two other examples.

4.2. Values of the three parameters in the class of Kasami-Tokura functions.

In the following, we give the exact values of \( \text{norm}(g) \), \( \text{cons}(g) \) and \( \text{stab}(g) \) when \( g \) ranges over each of the two Kasami-Tokura classes, that we denote by \( KT^1_{\nu,\mu,n} \) and \( KT^2_{\nu,\mu,n} \).

4.2.1. Exact values of \( \text{norm}(f) \), \( \text{cons}(f) \) and \( \text{stab}(f) \) for all \( f \in KT^1_{\nu,\mu,n} \).

Let \( n,\nu \) and \( \mu \) be three integers. Recall that for \( n \geq \nu + \mu \) and \( \nu \geq \mu \geq 2 \), the first class \( KT^1_{\nu,\mu,n} \) contains all functions \( f \) in \( RM(\nu,n) \) such that \( f \sim x_1 x_2 \ldots x_{\nu-\mu} (x_{\nu-\mu+1} \ldots x_{\nu} + x_{\nu+1} \ldots x_{\nu+\mu}) \).

Proposition 12. Let \( n,\nu \) and \( \mu \) be three integers such that \( n \geq \nu + \mu \) and \( \nu \geq \mu \geq 2 \). Then for every function \( g \) in \( KT^1_{\nu,\mu,n} \), we have:

\[
\text{norm}(g) = \begin{cases} 
  n - 2 & \text{if } \nu = \mu \\
  n - 1 & \text{if } \nu \geq \mu + 1.
\end{cases}
\]

Proof. According to Lemma 6, we only have to prove the equality for the representative \( f(x) = x_1 x_2 \ldots x_{\nu-\mu} (x_{\nu-\mu+1} \ldots x_{\nu} + x_{\nu+1} \ldots x_{\nu+\mu}) \) of Class \( KT^1_{\nu,\mu,n} \).

If \( \nu \geq \mu + 1 \), then the monomial \( x_1 x_2 \ldots x_{\nu-\mu} \) has strictly positive degree and \( f \) is null on the hyperplane \( H \) of equation for instance \( x_1 = 0 \), which implies directly \( \text{norm}(f) = n - 1 \) since \( \text{norm}(f) < n \) because \( f \) is not constant.

If \( \nu = \mu \), then the function equals \( f(x) = x_1 \ldots x_\mu + x_{\mu+1} \ldots x_{2\mu} \) and belongs to Class \( K_{n,\mu,2} \) of Definition 6. Since \( \mu \geq 2 \), then Theorem 1 with \( k = 1 \) implies that \( f \) is non-constant on any affine hyperplane of \( \mathbb{F}_2^n \). Thus, \( f_{A} = \text{cst} \) implies \( \text{dim} A \leq n - 2 \) and since \( f \) is null on the affine space \( A = \{ x : x_1 = x_{\mu+1} = 0 \} \) of dimension \( n - 2 \), then we have \( \text{norm}(f) = n - 2 \).
Then for every function \( g \) in \( KT_{n,\mu,n} \) we have:

\[
\text{cons} (g) \leq n - \nu - 1.
\]

**Proof.** Since \( \text{cons} (.) \) is an affine invariant, we need to prove the inequality only for \( f(x) = x_1 x_2 \ldots x_{\nu - \mu} x_{\mu + 1} \ldots x_{\nu + 1} \ldots x_{\nu + \mu} \). Note that \( \text{supp}(f) \) is included in the affine space \( A = \{ x \in F_2^n : x_1 = x_2 = \ldots = x_{\nu - \mu} = 1 \} \) of dimension \( n - \nu + \mu \). Suppose \( \text{supp}(f) \) contains an affine space \( B = a + E \) where \( E \) is a vector space of dimension \( n - \nu \). By applying the Poisson summation formula to \( f_A \) we have

\[
(3) \quad \sum_{u \in E^+} (-1)^{a \cdot u} W_{f_A}(u) = 2^\mu \sum_{u \in a + E^+} (-1)^{f_A(u)} = -2^{n - \nu + \mu}.
\]

Since \( f_A = x_{\nu - \mu + 1} \ldots x_{\nu + \mu} \), we can apply the above observations on \( W_h(u) \) for \( h = f_A \) and with \( n - \nu + \mu \) instead of \( n \). We know then that

\[
W_{f_A}(u) \text{ takes its values in } \{ 0, \pm 2^{n-\nu-\mu+1}, \pm 2^{n-\nu-\mu+2}(2^{\nu-1} - 1), \pm 2^{n-\nu-\mu+2}(2^{\nu-2} - 2^\mu + 1) \}.
\]

Let \( K_1 = \{ u \in E^+ : W_{f_A}(u) = \pm 2^{n-\nu-\mu+2}(2^{\nu-1} - 1) \} \) and \( K_2 = \{ u \in E^+ : W_{f_A}(u) = \pm 2^{n-\nu-\mu+2} \} \) and since \( W_{f_A}(0) = 2^{n-\nu-\mu+2}(2^{\nu-2} - 2^\mu + 1) \) (meaning that the zero vector in \( E^+ \), does not belong to \( K_1 \cup K_2 \)), then \( \text{Card}(K_1) + \text{Card}(K_2) \leq \text{Card}(E^+) - 1 = 2^n - 1 \). So, there exist \( p, q \in \mathbb{Z} \) such that \( 2^{n-\nu-\mu+2}(2^{\nu-1} - 1)p = \sum_{u \in K_1} (-1)^{a \cdot u} W_{f_A}(u) \) and \( 2^{n-\nu-\mu+2}q = \sum_{u \in K_2} (-1)^{a \cdot u} W_{f_A}(u) \) with \( |p| \leq \text{Card}(K_1) \) and \( |q| \leq \text{Card}(K_2) \) and then, Relation (3) becomes

\[
(4) \quad 2^{n-\nu-\mu+2}(2^{\nu-2} - 2^\mu + 1) + 2^{n-\nu-\mu+2}(2^{\nu-1} - 1)p + 2^{n-\nu-\mu+2}q = -2^{n-\nu+\mu}.
\]

Dividing each term in Relation (4) by \( 2^{n-\nu-\mu+2} \) yields

\[
(5) \quad q + (2^{\nu-1} - 1)p = -2^{2\nu-1} + 2^{\mu} - 1,
\]

Relation (5), by using the triangular inequality, implies: \( 2^{2\nu-1} - 2^\mu + 1 \leq |q| + (2^{\nu-1} - 1)|p| \) and since \( |p| + |q| \leq 2^\mu - 1 \), then we have the inequalities

\[
2^{2\nu-1} - 2^\mu + 1 \leq 2^\mu - 1 + (2^{\nu-1} - 2)|p| \leq 2^\mu - 1 + (2^{\nu-1} - 2)(2^\mu - 1)
\]

which yields

\[
2^{2\nu-1} - 2^\mu + 1 \leq 2^{2\nu-1} - 2^\mu - 2^{\nu-1} + 1
\]

and this is not possible. Therefore, we have \( \text{cons}(f) \leq n - \nu - 1 \).

The proof above does not work if we replace \( \leq n - \nu - 1 \) by \( \leq n - \nu - 2 \) and indeed, the following result shows that the above bound is tight (in a strong sense).

**Proposition 14.** Let \( n, \nu \) and \( \mu \) be three integers such that \( n \geq \nu + \mu \) and \( \nu \geq \mu \geq 2 \). Then for every function \( g \) in \( KT_{n,\mu,n} \) we have:

\[
\text{stab} (g) \geq n - \nu - 1.
\]

**Proof.** Since \( \text{stab} (.) \) is an affine invariant, we need to prove the inequality only for \( f(x) = x_1 x_2 \ldots x_{\nu - \mu} x_{\mu + 1} \ldots x_{\nu + 1} \ldots x_{\nu + \mu} \). Clearly, an element \( a \) belongs to \( \text{supp}(f) \) if and only if \( a \) satisfies one of the two following conditions:

- \( a_i = 1 \) for all \( i \in \{ 1, \ldots, \nu \} \) and there exists \( i_a \in \{ \nu + 1, \ldots, \nu + \mu \} \) such that \( a_{i_a} = 0 \)
- \( a_i = 1 \) for all \( i \in \{ 1, \ldots, \nu - \mu, \nu + 1, \ldots, \nu + \mu \} \) and there exists \( j_a \in \{ \nu - \mu + 1, \ldots, \nu \} \) such that \( a_{j_a} = 0 \). These two above conditions show that \( \text{supp}(f) \) contains two series of affine spaces of dimension \( n - \nu - 1 \), one of which contains \( a \): the affine spaces

\[
A = \{ x : x_i = 1 \forall i \in \{ 1, 2, \ldots, \nu \} \text{ and } x_{i_a} = 0 \}
\]

and the affine spaces

\[
B = \{ x : x_i = 1 \forall i \in \{ \nu + 1, \ldots, \nu + \mu \} \text{ and } x_{j_a} = 0 \}.
\]
Thus, since \(0 \in A\), we have \(\max \{\dim A : f_1 A = 1 \text{ and } a \in A\} \geq n - \nu - 1\).

Now let us consider the co-support. An element \(a\) belongs to \(cosupp(f)\) if and only if it satisfies one of the three following conditions:
- there exists \(i_a \in \{1, \ldots, n + \mu - 1, \ldots, \nu\}\) such that \(a_{i_a} = 0\),
- there exists \((j_a, k_a) \in \{\nu - \mu + 1, \ldots, \nu\} \times \{\nu + 1, \ldots, \nu + \mu\}\) such that \(a_{j_a} = a_{k_a} = 0\),
- for all \(i \in \{\nu - \mu + 1, \ldots, \nu + \mu\}\), \(a_i = 1\). These three above conditions show that \(cosupp(f)\) contains three series of affine spaces of dimensions larger than or equal to \(n - \mu \geq n - \nu\), one of which contains \(a\): \(A = \{x : x_{i_a} = 0\}\) where \(i_a \in \{1, \ldots, n - \mu\}\), \(B = \{x : x_{j_a} = x_{k_a} = 0\}\) where \((j_a, k_a) \in \{\nu - \mu + 1, \ldots, \nu\} \times \{\nu + 1, \ldots, \nu + \mu\}\), and
\[
C = \{x : x_{\nu - \mu + i} = x_{\nu + i} \text{ for all } i \in \{1, \ldots, \mu\}\}
\]
which ends the proof.

To summarize Propositions 12, 13 and 14, let \(n, \nu\) and \(\mu\) be three integers such that \(n \geq \nu + \mu\) and \(\nu \geq \mu \geq 2\), then for every function \(g \in KT_{\nu, \mu, n}^\nu\):
\[
n - \nu - 1 = \text{stab}(g) = \text{cons}(g) < \text{norm}(g) = \begin{cases} n - 2 & \text{if } \nu = \mu \\ n - 1 & \text{if } \nu > 1 \text{ if } \nu + \mu + 1. \end{cases}
\]

4.2.2. Exact values of \(\text{norm}(f), \text{cons}(f)\) and \(\text{stab}(f)\) for all \(f \in KT_{\nu, \mu, n}^\nu\). Let \(n, \nu\) and \(\mu\) be three integers. Recall that for \(\nu, \mu \geq 2\) and \(n \geq \nu + 2\mu - 2\), the second class \(KT_{\nu, \mu, n}^\nu\) contains all functions \(f\) in \(RM(\nu, n)\) such that \(f \sim x_1 x_2 \ldots x_{\nu-2} (x_{\nu-1} x_\nu + x_{\nu+1} x_{\nu+2} + \cdots + x_{\nu+2\mu - 3} x_{\nu+2\mu - 2})\).

Proposition 15. Let \(n, \nu\) and \(\mu\) be three integers such that \(n \geq \nu + \mu\) and \(\nu \geq \mu \geq 2\). Then, for every function \(g \sim x_1 x_2 \ldots x_{\nu-2} (x_{\nu-1} x_\nu + x_{\nu+1} x_{\nu+2} + \cdots + x_{\nu+2\mu - 3} x_{\nu+2\mu - 2})\) in \(KT_{\nu, \mu, n}^\nu\) we have:
\[
\text{norm}(g) = \begin{cases} n - \mu & \text{if } \nu = 2 \\ n - 1 & \text{if } \nu > 2. \end{cases}
\]

Proof. We just prove the equality for the representative \(f(x) = x_1 x_2 \ldots x_{\nu-2} (x_{\nu-1} x_\nu + x_{\nu+1} x_{\nu+2} + \cdots + x_{\nu+2\mu - 3} x_{\nu+2\mu - 2})\) of Class \(KT_{\nu, \mu, n}^\nu\).

If \(\nu > 2\), then we can observe that \(g\) is null on the hyperplane \(H\) of equation \(x_{\nu-2} = 0\) which implies directly \(\text{norm}(f) = n - 1\).

If \(\nu = 2\), then \(f(x) = x_1 x_2 + x_3 x_4 + \cdots + x_{2\mu - 1} x_{2\mu} \in C_{\mu, 0, n}\) and by Proposition 10, we have \(\text{norm}(f) = n - \mu\) which ends the proof.

The following observation will be useful to justify the exact value of \(\text{cons}(f)\) and \(\text{stab}(f)\) in Class \(KT_{\nu, \mu, n}^\nu\).

Remark 11. Let \(n \geq 2\) be an integer and \(k = \left\lfloor \frac{n}{2} \right\rfloor\). For all \(t = 1, \ldots, k\), recall that \(f_{t, 0, n}\) and \(f_{t, 1, n}\) are plateaued of amplitude \(2^{n-t}\) and by setting \(f = f_{t, 0, n}\), suppose \(supp(f)\) contains an affine space \(A\) of dimension \(n - t\). Then, \(A = a + E\) where \(a \in supp(f)\), \(E\) is a vector space of dimension \(n - t\) and by the Poisson summation formula, we have \(\sum_{u \in E} (-1)^{a \cdot u} W_f(u) = -2^n\). Since \(W_f(u) \in \{0, 2^{n-t} (-1)^{f(u)}\}\), consider the set \(F \subseteq E^\perp\) which is the collection of all \(u \in E^\perp\) for which \(W_f(u) = 2^{n-t} (-1)^{f(u)}\). Then, \(\sum_{u \in E} (-1)^{a \cdot u} W_f(u) = 2^{n-t} \sum_{u \in F} (-1)^{a \cdot u + f(u)} = -2^n\) which implies \(card(F) \geq 2^{n-t}\) that is, \(F = E^\perp\) and we have \(a \cdot u + f(u)\) is constant on \(E^\perp\). Thus, since \(0 \in cosupp(a \cdot u + f(u))\), then the relation \(\sum_{u \in E} (-1)^{a \cdot u + f(u)} = 2^n = 2^{n-t} \sum_{u \in E} (-1)^{a \cdot u + f(u)} = 2^n = 2^{n-t} \sum_{u \in E} (-1)^{a \cdot u + f(u)}\) implies \(a \in cosupp(f)\) which is a contradiction. Thus, there is no affine space of dimension \(n - t\) included in
Proof. We just need to show the equality for $\nu$ Proposition 16.

Let $t \supset \text{supp}$ defined by $\nu$ Proposition 13, the Walsh transform of the $n$-variable function $g$ is then valued in $\nu$ Proposition 17.

Let $n \geq 2$ and $n \geq \nu + 2\mu - 2$. Then, for every function $g$ in $KT_{\nu,\mu,n}^2$ we have:

$$\text{stab}(g) = \text{cons}(g) = n - \nu - \mu + 1.$$  

Proof. We just need to show the equality for $f(x) = x_1 x_2 \ldots x_{\nu - 2} (x_{\nu - 1} x_\nu + x_{\nu + 1} x_{\nu + 2} + \cdots + x_{\nu + 2\mu - 3} x_{\nu + 2\mu - 2})$. Let $A$ be the affine space of dimension $n - \nu + 2$

$$\nu$$

defined by $A = \{x \in \mathbb{F}_2^n : x_1 = x_2 = \cdots = x_{\nu - 2} = 1\}$. Clearly, $\text{supp}(f) = \text{supp}(f|_A)$ and since $f|_A = x_{\nu - 1} x_\nu + x_{\nu + 1} x_{\nu + 2} + \cdots + x_{\nu + 2\mu - 3} x_{\nu + 2\mu - 2} \sim \nu f_{\mu,0,n-\nu+2}$, then according to Remark 11, the greatest affine space included in $\text{supp}(f_{\mu,0,n-\nu+2})$ is of dimension $n - \nu - \mu + 1$ which implies $\text{cons}(f) \leq n - \nu - \mu + 1$. Let us show now that $\text{stab}(f) \geq n - \nu - \mu + 1$.

Let $a \in \text{supp}(f) = \text{supp}(f|_A)$. From Proposition 11, we have $\text{stab}(f|_A) = n - \nu - \mu + 1$ and by Remark 1, there exists an affine space of dimension at least $n - \nu - \mu + 1$ containing $a$ and on which $f$ is constant. Now let $a \in \text{cosupp}(f)$. Then either $a_1 = a_2 = \cdots = a_{\nu - 2} = 1$ and $f(a) = 0$ or there exists $i_0 \in \{1, 2, \ldots, \nu - 2\}$ such that $a_{i_0} = 0$. Thus, if $a_1 = a_2 = \cdots = a_{\nu - 2} = 1$ and $f(a) = 0$ that is, $a \in \text{cosupp}(f|_A)$, then since $\text{stab}(f|_A) = n - \nu - \mu + 1$, by Remark 1 there exists an affine space of dimension at least $n - \nu - \mu + 1$ containing $a$ and on which $f$ is null. However, if there exists $i_0 \in \{1, 2, \ldots, \nu - 2\}$ such that $a_{i_0} = 0$, then $\text{cosupp}(f)$ contains the hyperplane $H$ of equation $x_{i_0} = 0$ which contains $a$. Therefore for all $a \in \text{supp}(f) \cup \text{cosupp}(f)$ there exists an affine space of dimension at least $n - \nu - \mu + 1$ containing $a$ and on which $f$ is constant that is, $\text{stab}(f) \geq n - \nu - \mu + 1$ which ends the proof.

Hence, for every function $g$ in Class $K_{\nu,\mu,n} = KT_{\nu,\mu,n}^1 \cup KT_{\nu,\mu,n}^2$ we have: $\text{stab}(g) = \text{cons}(g) < \text{norm}(g)$ meaning that we can not find the two other examples we are looking for in this class. Nevertheless, we use the general form of functions in this class to construct in what follows the two other examples.

4.2.3. An infinite class of functions $g$ such that $\text{stab}(g) < \text{cons}(g) < \text{norm}(g)$. Let $n, \nu$ and $\mu \geq 0$ be three integers such that $\nu \geq \mu + 1$, and $n \geq \nu + \mu$. We denote by $M_{\nu,\mu,n}$, the class of all functions belonging to $RM(\nu, n)$ which are affinely equivalent to $g(x) = x_1 x_2 \ldots x_{\nu - \mu - 1} (x_{\nu - \mu} x_{\nu - \mu + 1} \ldots x_{\nu} + x_{\nu + 1} \ldots x_{\nu + \mu})$. Class $M_{\nu,\mu,n}$ is similar to Class $KT_{\nu,\mu,n}^1$ of Kasami-Tokura function but there are disjoint since functions in this new class are all a sum of two functions of distinct degree.

The proof of the following proposition is similar to the proof of Proposition 12.

Proposition 17. Let $n, \nu$ and $\mu \geq 0$ be three integers such that $\nu \geq \mu + 1$, and $n \geq \nu + \mu$. Then for every function $f$ in $M_{\nu,\mu,n}$ we have:

$$\text{norm}(f) = \begin{cases} n - 2 & \text{if } \nu = \mu + 1 \\ n - 1 & \text{if } \nu \geq \mu + 2 \end{cases}.$$  

In order to determine the exact value of $\text{cons}(f)$ when $f \in M_{\nu,\mu,n}$, we shall need in the next proposition, as in Subsection 4.2.1 all the Walsh values of function $g(x) = x_1 x_2 \ldots x_{\mu - 1} + x_{\mu + 2} \ldots x_{2\mu + 1}$ when $\mu \geq 2$ and from the observation before Proposition 13, the Walsh transform of the $n$-variable function $g$ is then valued in $\{0, 2^{\nu - 2\mu + 1}, 2\mu - 3 \times 2^{\mu - 1} + 1, 2 \times 2^{\mu - 2\mu + 1}, 2^{\mu - 1} - 1, 2^{2\mu - 2\mu + 1} (2\mu - 1), 2^{2\mu - 2\mu + 1} (2^{\mu - 1} - 1), 2^{2\mu - 2\mu + 1} (2^{\mu - 1} - 1), 2^{2\mu - 2\mu + 1} (2^{\mu - 1} - 1)\}$.  

Advances in Mathematics of Communications Volume XX, No. X (2019), XXX–XXX
Proposition 18. Let $n, \nu$ and $\mu \geq 2$ be three integers such that $\nu \geq \mu + 1$, and $n \geq \nu + \mu$. Then, for every function $f$ in $M_{\nu, \mu, n}$ we have:

$$
\text{cons}(f) = n - \nu.
$$

Proof. Let us show first that there is no affine space of codimension $\nu - 1$ contained in $\text{supp}(f)$ where $f(x) = x_1x_2 \ldots x_{\nu-1}(x_\nu - \mu x_{\nu-\mu + 1} \ldots x_\nu + x_{\nu+1} \ldots x_{\nu+\mu})$.

Note that $\text{supp}(f)$ is contained in the affine space $U = \{x : x_i = 1 \forall i \in \{1, \ldots, \nu - \mu - 1\}$ of dimension $\gamma = n - \nu + \mu + 1$. Suppose $\text{supp}(f)$ contains an affine space $A = a + E$ where $E$ is a vector space of dimension $n - \nu + 1$. By applying the Poisson summation formula to $f|_U$ we have

$$
(6) \quad \sum_{u \in E^\perp} (-1)^{a \cdot u} W_{f|_U}(u) = 2^\mu \sum_{u \in a + E} (-1)^{f|_U(u)} = -2^\gamma.
$$

Since $f|_U(x) = x_{\nu-\mu}x_{\nu-\mu+2} \ldots x_\nu + x_{\nu+1} \ldots x_{\nu+\mu}$, we can apply the above observations on $W_g(u)$ for $g = f|_U$ and with $\gamma$ instead of $n$. We know then that $W_{f|_U}$ takes its values in $\{0, 2\gamma-2\mu+1(2\mu-1-3 \times 2\nu-1+1), \pm 2\gamma-2\mu+1(2\nu-1-1), \pm 2\gamma-2\mu+1(2\nu-1), \pm 2\gamma-2\mu+1\}$. We set $K_1 = \{u \in E^\perp : W_{f|_U}(u) = \pm 2\gamma-2\nu+1(2\nu-1-1)\}$, $K_2 = \{u \in E^\perp : W_{f|_U}(u) = \pm 2\gamma-2\mu+1(2\mu-1)\}$ and $K_3 = \{u \in E^\perp : W_{f|_U}(u) = \pm 2\gamma-2\mu+1\}$ and since $W_{f|_U}(0) = 2\gamma-2\mu+1(2\mu-1-3 \times 2\nu-1+1)$ (meaning that the zero vector in $E^\perp$, does not belong to $K_1 \cup K_2 \cup K_3$, then $\text{Card}(K_1) + \text{Card}(K_2) + \text{Card}(K_3) \leq \text{Card}(E^\perp) - 1 = 2\gamma - 1$. So, there exist $p, q, r \in \mathbb{Z}$ such that

$$
2\gamma-2\mu+1(2\mu-1-3 \times 2\nu-1+1) p = \sum_{u \in K_1} (-1)^{a \cdot u} W_{f|_U}(u), \quad 2\gamma-2\mu+1(2\mu-1) q = \sum_{u \in K_2} (-1)^{a \cdot u} W_{f|_U}(u) \quad \text{and} \quad 2\gamma-2\mu+1 r = \sum_{u \in K_3} (-1)^{a \cdot u} W_{f|_U}(u) \quad \text{with} \quad |p| \leq \text{Card}(K_1), \quad |q| \leq \text{Card}(K_2) \quad \text{and} \quad |r| \leq \text{Card}(K_3) \quad \text{and then, Relation (6) becomes 2\gamma-2\mu+1(2\mu-1-3 \times 2\nu-1+1)+ 2\gamma-2\mu+1(2\mu-1) p + 2\gamma-2\mu+1(2\mu-1) q + 2\gamma-2\mu+1 r = -2^\gamma. Devising each member of this last equality by 2\gamma-2\mu+1 yields}
$$

$$
(7) \quad r + (2\mu-1) p + (2\mu-1) q = -2^\mu + 3 \times 2\mu-1 - 1 \quad \text{Note that if} \quad r = p = 0, \text{then Relation (7) becomes (2\mu-1) q = -2^\mu + 3 \times 2\mu-1 - 1 \quad \text{which is not possible. Indeed, since the inequality -2^\mu + 1 \leq q \leq -2^\mu - 1 \text{ holds}, then multiplying each member of it by (2\mu-1) yields -2^{2\mu}+3.2\mu-1-1 < -2^{2\mu}+2.2\mu-1-1 \leq (2\mu-1) q \leq -2^{2\mu}+2.2\mu-1+1 \text{ meaning that (2\mu-1) q \neq -2^{2\mu}+3.2\mu-1-1. So, we have r \neq 0 or p \neq 0 which then implies |q| \leq 2^\mu - 2. Moreover, Relation (7), by using the triangular inequality, implies 2^\mu - 3 \times 2\mu-1 + 1 \leq |r| + (2\mu-1) |p| + (2\mu-1) |q| \quad \text{and since |r| \leq (2\mu-1) - |p| - |q|, then we have the inequalities}
$$

$$
2^{2\mu} - 3 \times 2\mu-1 + 1 \leq |r| + (2\mu-1) |p| + (2\mu-1) |q| \leq 2^{2\mu} - 1 + (2\mu-1) - 2|p| + (2\mu-2)|q|. \quad \text{Since the inequalities |p| \leq (2\mu-1) - |q| \quad \text{and |q| \leq (2\mu-2) hold, then we have}
$$

$$
2^{\mu-1} + (2\mu-2)|p| + (2\mu-2)|q| \leq 2^{\mu-1} + (2\mu-2)\mu + 2\mu-1|q| \leq 2^{\mu-1} + (2\mu-2)|p| + (2\mu-2)|q| = 2^{\mu-1} - 2(2\mu-1) + 2\mu-1(2\mu-2) = 2^{\mu-1} - 5 \times 2\mu-1 + 1 \quad \text{and this is not possible because for all \mu \geq 2, 2^{\mu-1} - 5 \times 2\mu-1 + 1 < 2^{\mu-1} - 3 \times 2\mu-1 + 1. Therefore, supp(f) contains no affine space of codimension \nu - 1 (that is, cons(f) \leq n - \nu) and the proof is completed by observing that supp(f) contains the affine space A = \{x : x_{\nu - \mu} = 0 and x_i = 1 for all i \in \{1, \ldots, \nu - \mu - 1, \nu + 1, \ldots, \nu + \mu\} of dimension n - \nu. \}
$$

Let us show now that for every function $f$ in $M_{\nu, \mu, n}$ we have $\text{stab}(f) < n - \nu$. \hfill \Box
Proposition 19. Let $n, \nu$ and $\mu \geq 2$ be three integers such that $\nu \geq \mu + 1$, and $n \geq \nu + \mu$. Then, for every function $f$ in $M_{\nu, \mu, n}$ we have:

$$\text{stab}(f) < n - \nu.$$ 

Proof. It suffices to show that no affine space of codimension $\nu$ included in $\text{supp}(g)$ where $g = x_1 x_2 \ldots x_{\nu - \mu - 1} (x_{\nu - \mu} x_{\nu - \mu + 1} \ldots x_{\nu + x_{\nu + 1} \ldots x_{\nu + \mu}})$, contains the element $a$ of $\text{supp}(g)$ such that $a_i = 1$ if and only if $i \in \{1, 2, \ldots, \nu\}$.

Let $A$ be an affine space of codimension $\nu$, we have then to prove that either $A \not\subseteq \text{supp}(g)$ or $a \notin A$. Since $\text{supp}(g) = \text{supp}(g|_U)$ where $U$ is the affine space of $\mathbb{F}_2^n$ of dimension $n - \nu + \mu + 1$ defined by $U = \{x : x_i = 1 \forall i \in \{1, \ldots, \nu - \mu - 1\}\}$, then $A \not\subseteq U$ implies $A \not\subseteq \text{supp}(g)$. So, we suppose in the following that $A \subseteq U$. Note that $g|_U(x) = x_{\nu - \mu} x_{\nu - \mu + 1} \ldots x_{\nu} + x_{\nu + 1} \ldots x_{\nu + \mu}$ and by setting $g|_U(x) = h(x) = m_{\nu, \mu} + m_{\nu, \mu}'$ where $m_{\nu, \mu} = x_{\nu - \mu} x_{\nu - \mu + 1} \ldots x_{\nu}$ and $m_{\nu, \mu}' = x_{\nu + 1} \ldots x_{\nu + \mu}$, we have to show now that either $A \not\subseteq \text{supp}(h)$ or $a \notin A$. Then, $A$ being characterized by a system of $\mu + 1$ linearly independent equations and this system being equivalent to a system which expresses $\mu + 1$ distinct variables $x_{i_1}, x_{i_2}, \ldots, x_{i_{\mu + 1}}$ by means of the other variables, we denote by $s$ with $s \leq \mu + 1$, the number of distinct variables among the $\mu + 1$ variables $x_{i_1}, x_{i_2}, \ldots, x_{i_{\mu + 1}}$, which appear in $m_{\nu, \mu}$. We have all the possible following cases:

- if $s = 0$, then $(m_{\nu, \mu})|_{A}$ is of degree $\mu + 1$ and since $(m_{\nu, \mu}')|_{A}$ is of degree at most $\mu$, then $h|_{A} \neq 1$ that is, $A \not\subseteq \text{supp}(h)$
- if $s = 1$, then either $(m_{\nu, \mu})|_{A}$ contains a sum of monomials of degree $\mu + 1$ which can not be canceled in $h|_{A}$ and implying $h|_{A} \neq 1$ that is, $A \not\subseteq \text{supp}(h)$.

Either $(m_{\nu, \mu})|_{A}$ is null or is a sum of monomials of degree $\mu$ and we have:

- suppose $(m_{\nu, \mu})|_{A}$ is null. If $(m_{\nu, \mu}')|_{A} = 1$, then $A$ is characterized by at least $\mu$ equations of the form $x_{j_i} = 1$ for all $j_i \in \{\nu + 1 \ldots \nu + \mu + 1\}$ and in this case $a \notin A$. But if $(m_{\nu, \mu}')|_{A} \neq 1$, then $h|_{A} \neq 1$ that is, $A \not\subseteq \text{supp}(h)$.

- if $(m_{\nu, \mu})|_{A}$ is of degree $\mu$, then $(m_{\nu, \mu}')|_{A}$ can not be of the form $1 + a(x)$ where $a$ is a sum of monomials of degree $\mu$ meaning that $h|_{A} \neq 1$ that is, $A \not\subseteq \text{supp}(h)$. Indeed, for any monomial $l(x) = x_{j_1} \ldots x_{j_p}$ and for any affine space $A$, the constant $1$ appears in $(l(x))|_{A}$ implies $(l(x))|_{A} = 1$ (when $A$ is characterized by at least $p$ equations of the form $x_{j_i} = 1$ for $i = 1, \ldots, p$) or $(l(x))|_{A}$ always contains at least one monomial of degree $1$ (when $A$ is characterized by at least $p$ equations of the form $x_{j_i} = 1 + a_i(x)$ for $i = 1, \ldots, p$, where any $a_i$ is linear, $x_{j_i}$ does not appear in $a_i(x)$ and at least one $a_i \neq 0$).

- if $1 \leq s < \mu + 1$ (which implies $\mu + 1 - s < \mu$), then $(m_{\nu, \mu})|_{A}$ (resp. $(m_{\nu, \mu}')|_{A}$) is either null or a sum of monomials of degree at least $1$ which implies $h|_{A} \neq 1$ that is, $A \not\subseteq \text{supp}(h)$.

- if $s = \mu + 1$, then all the $\mu + 1$ distinct variables in $m_{\nu, \mu}$ are substituted and we have $(m_{\nu, \mu}')|_{A} = m_{\nu, \mu}'$ which is of degree $\mu$. Since $(m_{\nu, \mu})|_{A}$ can not be of the form $1 + a$ where $a$ is a monomial of degree $\mu \geq 2$ then we have $h|_{A} \neq 1$ that is, $A \not\subseteq \text{supp}(h)$.

This ends the proof.

Let $n, \nu$ and $\mu \geq 2$ be three integers such that $\nu \geq \mu + 1$, and $n \geq \nu + \mu$. Then for every function $f$ in $M_{\nu, \mu, n}$ Proposition 17, 18 and 19 imply

$$\text{stab}(g) < n - \nu = \text{cons}(g) < \text{norm}(g) = \begin{cases} 
 n - 2 & \text{if } \nu = \mu + 1 \\
 n - 1 & \text{if } \nu \geq \mu + 2
\end{cases}.$$
4.2.4. An infinite class of functions $g$ such that $\text{stab}(g) < \text{cons}(g) = \text{norm}(g)$. We give a class of functions for which we have $\text{stab}(g) < \text{cons}(g) = \text{norm}(g)$ for all $g$. Let $n$, $\mu$ and $\nu$ be three integers such that $2 \leq \nu < \mu \leq n$. We denote by $N_{\nu, \mu, n}$, the class of all functions $f$ in $\text{RM}(\nu, n)$ such that $f \sim x_1 x_2 \ldots x_\nu + x_\mu$.

Let us set $g(x) = x_1 x_2 \ldots x_\nu + x_\mu$. We can easily check (by using the general form of the equation of a hyperplane) that there is no affine hyperplane on which $g$ is constant and since $\text{supp}(g)$ and $\text{cosupp}(g)$ contains respectively the affine spaces $A = \{ x : x_1 = 0; x_\mu = 1 \}$ and $B = \{ x : x_1 = 0; x_\mu = 0 \}$ of codimension 2 then, $\text{cons}(\cdot)$ and $\text{norm}(\cdot)$ being affinely invariant, we have:

**Proposition 20.** Let $n$, $\mu$ and $\nu$ be three integers such that $2 \leq \nu < \mu \leq n$. Then, for every $f$ in $N_{\nu, \mu, n}$ we have:

$$\text{norm}(f) = \text{cons}(f) = n - 2.$$ 

Moreover, we have

**Proposition 21.** Let $n$, $\mu$ and $\nu$ be three integers such that $3 \leq \nu < \mu \leq n$. Then, for every $f$ in $N_{\nu, \mu, n}$ we have:

$$\text{stab}(f) < n - 2.$$ 

**Proof.** It suffices to show that no affine space of codimension 2 included in $\text{supp}(g)$ where $g = x_1 x_2 \ldots x_\nu + x_\mu$, contains the element $b$ of $\text{supp}(g)$ such that $b_i = 1$ if and only if $i \in \{1, 2, \ldots, \nu\}$. Let $A$ be an affine space of codimension 2, we have then to prove that either $A \notin \text{supp}(g)$ or $b \notin A$. Then, let $x_{i_1}, x_{i_2}$ be the two distinct variables expressed by means of the other variables in the equations of $A$ since $\nu \geq 3$, then $(x_1 x_2 \ldots x_\nu)_{\mid A}$ is either null or is of degree at least $\nu - 2 \geq 1$ and we have three cases:

1. $(x_1 x_2 \ldots x_\nu)_{\mid A}$ contains a monomial of degree $d > \nu - 2$. Then, this monomial is not canceled by the elements of $(x_\mu)_{\mid A}$ which are of degree 1 and we have $g_{\mid A} \neq \text{cst}$ that is, $A \notin \text{supp}(g)$.

2. $(x_1 x_2 \ldots x_\nu)_{\mid A}$ is null. Then if $(x_\mu)_{\mid A} = 1$ (meaning that an equation of $A$ is given by $x_\mu = 1$) then we have $b \notin A$. But if $(x_\mu)_{\mid A} \neq 1$, then $g_{\mid A} \neq 1$ that is, $A \notin \text{supp}(g)$.

3. $(x_1 x_2 \ldots x_\nu)_{\mid A}$ is of degree $\nu - 2 \geq 1$ (this is possible only when $x_{i_1}$ and $x_{i_2}$ are replaced in $x_1 x_2 \ldots x_\nu$). Since $\nu \geq 3$, then $(x_1 x_2 \ldots x_\nu)_{\mid A}$ contains a variable which does not appear in $(x_\mu)_{\mid A} = x_\mu$ which implies $g_{\mid A} \neq 1$ that is, $A \notin \text{supp}(g)$.

This ends the proof. \[\Box\]

Let $n$, $\mu$ and $\nu$ be three integers such that $3 \leq \nu < \mu \leq n$. Then, for every $f$ in $N_{\nu, \mu, n}$, Proposition 20 and 21 directly imply:

$$\text{stab}(g) < \text{cons}(g) = \text{norm}(g).$$

5. Minimal values of the parameters in Reed-Muller codes

In this section, we consider the minimal values of $\text{stab}(f)$, $\text{cons}(f)$ and $\text{norm}(f)$ when $f$ ranges over some particular sets of functions.

**Definition 8.** Let $\mathcal{F}$ be a set of Boolean functions. Then:

$$\text{norm}_{\mathcal{F}} = \min \{ \text{norm}(f) : f \in \mathcal{F} \text{ and } f \text{ is non constant} \},$$

$$\text{cons}_{\mathcal{F}} = \min \{ \text{cons}(f) : f \in \mathcal{F} \text{ and } f \text{ is non constant} \},$$

$$\text{stab}_{\mathcal{F}} = \min \{ \text{stab}(f) : f \in \mathcal{F} \text{ and } f \text{ is non constant} \},$$
Example 1. Taking for $\mathcal{F}$ the Maiorana-McFarland Class $\mathcal{M}_n$ of bent functions ($n$ even) and $\mathcal{F}$ is the whole set of bent functions (which seems elusive) or when $\mathcal{F} = \mathcal{PS} = \mathcal{PS}^- \cup \mathcal{PS}^+$ the Partial Spreads class (introduced in [14] by J. Dillon) whose elements are bent and are the sum (modulo 2) of the indicators of $2^{n/2}-1$ or $2^{n/2}-1 + 1$ disjoint $n/2$–dimensional subspaces of $\mathbb{F}_2^n$.

We consider in particular the case where $\mathcal{F}$ is the Reed-Muller code $RM(r,n)$ of length $2^n$ and order $r$. We give upper bounds for each of the three values $\text{stab}_{RM(r,n)}$, $\text{cons}_{RM(r,n)}$ and $\text{norm}_{RM(r,n)}$, and we determine the exact values of $\text{stab}_{RM(r,n)}$ and $\text{cons}_{RM(r,n)}$ for $r \in \{1, 2, n - 2, n - 1, n\}$ and of $\text{norm}_{RM(r,n)}$ for $r = 1, 2$.

Remark 12. For all $r, n$ with $1 \leq r \leq n$, we have $\text{stab}_{RM(r,n)} \leq \text{cons}_{RM(r,n)} \leq \text{norm}_{RM(r,n)}$. Moreover, for $r \leq n-1$, since $RM(r,n) \subseteq RM(r+1,n)$, then we have $\text{norm}_{RM(r+1,n)} \leq \text{norm}_{RM(r,n)}$; $\text{cons}_{RM(r+1,n)} \leq \text{cons}_{RM(r,n)}$ and $\text{stab}_{RM(r+1,n)} \leq \text{stab}_{RM(r,n)}$.

We have the following upper bounds.

Proposition 22. Let $n, r$ be two integers such that $2 \leq r \leq n$, then we have:

$$\text{norm}_{RM(r,n)} \leq \left\lceil \frac{n}{2} \right\rceil,$$

and

$$\text{stab}_{RM(r,n)} \leq \text{cons}_{RM(r,n)} \leq \min \left\{ \left\lceil \frac{n}{2} \right\rceil, n - r \right\}.$$ 

Proof. Let $n$ be an integer and let us consider the class $K_n, \lfloor \frac{n}{2} \rfloor, 2 \subseteq RM(2,n)$ defined in Definition 6. Let $p = \left\lfloor \frac{n}{2} \right\rfloor$ and $A$ be an affine space. Then according to Lemma 3, for all $f \in K_n, p, 2$, if $f|_A$ is constant then $\dim A \leq n - p$. We have then $\text{norm}(f) \leq n - p = \left\lfloor \frac{n}{2} \right\rfloor$ which implies by Definition 8 that $\text{norm}_{RM(2,n)} \leq \left\lfloor \frac{n}{2} \right\rfloor$ and from Remark 12 we have $\text{stab}_{RM(r,n)} \leq \text{cons}_{RM(r,n)} \leq \text{norm}_{RM(r,n)} \leq \text{norm}_{RM(2,n)} \leq \left\lfloor \frac{n}{2} \right\rfloor$ for all $r \geq 2$. Moreover, let us consider the function $g(x) = x_1 \ldots x_r \in RM(r,n)$ which is an indicator of an $(n-r)$-dimensional affine space. We have $\text{cons}(g) \leq n-r$ and by the definition of $\text{cons}_{RM(r,n)}$, we have $\text{cons}_{RM(r,n)} \leq n - r$ which completes the proof. \hfill \Box

5.1. Exact values of $\text{norm}_{RM(1,n)}$ and of $\text{cons}_{RM(r,n)}$ and $\text{stab}_{RM(r,n)}$ for all $r \in \{1, n - 1, n\}$. The values of $\text{norm}_{RM(r,n)}$, $\text{cons}_{RM(r,n)}$ and $\text{stab}_{RM(r,n)}$ are easily determined for $r = 1$, but for $r \in \{n - 1, n\}$, only the two latter are easily determined.

Proposition 23. Let $n \geq 2$ be an integer. For all $r \in \{1, n - 1, n\}$, we have:

$$\text{stab}_{RM(r,n)} = \text{cons}_{RM(r,n)} = n - r,$$

and

$$\text{norm}_{RM(1,n)} = n - 1.$$

Proof. The result is obvious for $r = 1$. Let $r = n$. All Boolean functions of Hamming weight 1 satisfy $\text{stab}(f) = 0 = \text{cons}(f)$ and then $\text{stab}_{RM(n,n)} = \text{cons}_{RM(n,n)} = 0$. Let now $r = n - 1$. All Boolean functions of Hamming weight 2 belong to $RM(n - 1, n)$ (see e.g. [19]) and satisfy $\text{stab}(f) = \text{cons}(f) = 1$. Hence, according to Lemma 5, we have $\text{stab}_{RM(n-1,n)} = \text{cons}_{RM(n-1,n)} = 1$. \hfill \Box
We leave open the determination of $\text{norm}_{RM(r,n)}$ for $r \in \{n-1,n\}$ (which are not larger than \(\lceil \frac{n}{2} \rceil\), according to Proposition 22); it seems indeed difficult to determine them, even though for $r = n$ the support can be any subset of $\mathbb{F}_2^n$, because minimizing the maximum dimension of affine spaces included in the support (resp. in the co-support) tends to increase the maximum dimension of affine spaces included in the co-support (resp. in the support); finding functions minimizing $\text{norm}_{RM(n,n)}$ corresponds then to finding the best possible trade-off between these two maximal dimensions, and we know that optimizing trade-offs is difficult.

5.2. A BOUND ON $\text{cons}_{RM(n-i,n)}$ AND $\text{stab}_{RM(n-i,n)}$ WHERE $n \geq i + 2$ AND EXACT VALUE OF $\text{cons}_{RM(n-2,n)}$ AND $\text{stab}_{RM(n-2,n)}$. Proposition 16 yields the following information on $\text{cons}_{RM(n-i,n)}$ and $\text{stab}_{RM(n-i,n)}$ where $n \geq i + 2$.

Lemma 10. Let $n$ and $i$ be two positive integers such that $n \geq i + 2$. Then we have:

$$\text{stab}_{RM(n-i,n)} \leq \text{cons}_{RM(n-i,n)} \leq i - 1$$

Proof. Let $g \in K \mathbb{T}^n_{\mu,n}$ defined by $g(x) = x_1x_2\ldots x_{n-i-2}(x_{n-i-1}x_n + x_{n-i+1}) \in RM(n-i,n)$ of parameters $\nu = n-i$ and $\mu = 2$, then from Proposition 16 we have $\text{cons}(g) = \text{stab}(g) = n-(n-i)-1 = i-1$ which implies $\text{cons}_{RM(n-i,n)} \leq i-1$.

For $i = 2$ or $3$ in Lemma 10 we have:

Corollary 4. Let $n$ be a positive integer. Then, we have

$$\begin{align*}
\text{cons}_{RM(n-2,n)} = \text{stab}_{RM(n-2,n)} &= 1 \text{ for } i = 2 \text{ and } n \geq 4 \\
\text{cons}_{RM(n-3,n)} = \text{stab}_{RM(n-3,n)} &\leq 2 \text{ for } i = 3 \text{ and } n \geq 5.
\end{align*}$$

We have (from all the previous results) the following tabular for all $n \geq 3$:

| $r$ | 1 | 2 | 3 | $n - 3$ |
|-----|---|---|---|---------|
| $\text{stab}_{RM(r,n)}$ | $n-1$ | $\frac{n-1}{2}$, $n$ even | $\frac{n-1}{2}$, $n$ odd | $\leq \min\{n-3, \text{stab}_{RM(2,n)}\}$ | $\leq 2$ |
| $\text{cons}_{RM(r,n)}$ | $n-1$ | $\frac{n-1}{2}$, $n$ even | $\frac{n-1}{2}$, $n$ odd | $\leq \min\{n-3, \text{stab}_{RM(2,n)}\}$ | $\leq 2$ |
| $\text{norm}_{RM(r,n)}$ | $n-1$ | $\frac{n-1}{2}$, $n$ even | $\frac{n-1}{2}$, $n$ odd | $\leq \text{norm}_{RM(2,n)}$ | $\leq \text{norm}_{RM(2,n)}$ |

Our study allows to provide a bound on the universal constants $c_1$ and $c_2$ in [13]. Indeed, from [13, Theorem 1], there exists an universal constant $c_1 \in (0,1)$ such that for all $n$, $q$, $r$ it holds that $k_q(n,r) \geq c_1 \cdot n^{1/(r-1)}$. In particular for $q = 2 = r$, we have $c_1 \cdot n \leq k_2(n,2) = \text{norm}_{RM(2,n)}$ which implies asymptotically that $c_1 \leq \frac{1}{2}$.

From [13, Theorem 2] again, there exists an universal constant $c_2 > 0$ such that for all $q$ (a prime power) and $f : \mathbb{F}_q^n \to \mathbb{F}_q$ a degree $r$ polynomial, there exists a partition of $\mathbb{F}_q^n$ into affine subspaces, each of dimension $c_2 \cdot n^{1/(r-1)}$, $f$ being constant on each part. This implies for $q = 2$ that the support and the co-support of $f$ are recovered by affine space of dimension $c_2 \cdot n^{1/(r-1)}$, meaning that $c_2 \cdot n^{1/(r-1)} \leq \text{stab}(f)$. By taking the minimum over $RM(r,n)$ with $r \geq 2$, we have $c_2 \leq \frac{\text{stab}_{RM(r,n)}}{2n^{1/(r-1)}} \leq \frac{\text{stab}_{RM(2,n)}}{2n^{1/(r-1)}}$ and since $\frac{\text{stab}_{RM(2,n)}}{2n^{1/(r-1)}}$ is minimal for $r = 2$, then we have $c_2 \leq \frac{\text{stab}_{RM(2,n)}}{2n}$ and asymptotically, we have $c_2 \leq 1/4$. 
Conclusion

After studying the general properties of the three parameters \( \text{stab}(\cdot) \), \( \text{cons}(\cdot) \) and \( \text{norm}(\cdot) \), we determined the exact values of each of them in Classes \( RM(1,n) \), \( RM(2,n) \) and in the class of Kasami-Tokura which allowed us to exhibit four examples of infinite classes of Boolean functions showing how distinct our three parameters are. We also gave the exact values of the minimum \( \text{norm}_{RM}(r,n) \) for \( r \in \{1,2\} \) and the exact values of the minima \( \text{stab}_{RM}(r,n) \) and \( \text{cons}_{RM}(r,n) \) for \( r \in \{1,2,n-2,n-1,n\} \). But it seems difficult to determine the exact values of \( \text{stab}_{RM}(r,n) \), \( \text{cons}_{RM}(r,n) \) for \( r \) with \( 3 \leq r \leq n-3 \) and the exact value of \( \text{norm}_{RM}(r,n) \) for \( r \geq 3 \). We leave open the study of these minima and of \( \text{stab}_F \), \( \text{cons}_F \) and \( \text{norm}_F \) when \( F \) is the whole set of bent functions (note in this case that determining \( \text{norm}_F \) is equivalent to find the minimal order \( r \) such that a bent function is \( r \)-normal but not \( (r+1) \)-normal).

References

[1] E. F. Assmus Jr., On the Reed-Muller codes, Discrete Math., 106-107 (1992), 25–33.
[2] J. Boyar and M. G. Find, Constructive relationships between algebraic thickness and normality, in Fundamentals of Computation Theory, Lecture Notes in Comput. Sci., 9210, Springer, Cham, 2015, 106–117.
[3] A. Canteaut, C. Carlet, P. Charpin and C. Fontaine, On cryptographic properties of the cosets of \( R(1,m) \), IEEE Trans. Inform. Theory, 47 (2001), 1494–1513.
[4] A. Canteaut, M. Daum, H. Dobbertin and G. Leander, Normal and non-normal bent functions, Proceedings of the Workshop on Coding and Cryptography, 2003, 91–100.
[5] C. Carlet, Two new classes of bent functions, in Advances in Cryptology, Lecture Notes in Comput. Sci., 765, Springer, Berlin, 1994, 77–101.
[6] C. Carlet, On cryptographic complexity of Boolean functions, Finite Fields with Applications to Coding Theory, Cryptography and Related Areas, Springer, Berlin, 2002, 53–69.
[7] C. Carlet, Recursive lower bounds on the nonlinearity profile of Boolean functions and their applications, IEEE Trans. Inform. Theory, 54 (2008), 1262–1272.
[8] C. Carlet, Boolean functions for cryptography and error-correcting codes, in Monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge University Press, 2010, 257–397. Preliminary version available at: http://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf.
[9] C. Carlet, Boolean and vectorial plateaued functions, and APN functions, IEEE Trans. Inform. Theory, 61 (2015), 6272–6289.
[10] C. Carlet and S. Feukoua, Three basic questions on Booleans functions, Adv. Math. Commun., 11 (2017), 837–855.
[11] C. Carlet and S. Mesnager, Four decades of research on bent functions, Des. Codes Cryptogr., 78 (2016), 5–50.
[12] P. Charpin, Normal Boolean functions, J. Complexity, 20 (2004), 245–265.
[13] G. Cohen and A. Tal, Two structural results for low degree polynomials and applications, in Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, Leibniz Int. Proc. Inform., 40, Schloss Dagstuhl, Leibniz-Zent. Inform., Wadern, 2015, 680–709.
[14] J. F. Dillon, Elementary Hadamard Difference Sets, Ph.D thesis, University of Maryland in College Park, 1974.
[15] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, in Fast Software Encryption, Lecture Notes in Comput. Sci., 1008, Springer, Berlin, 1995, 61–74.
[16] R. E. Jamison, Covering finite field with cosets of subspaces, J. Combinatorial Theory Ser. A, 22 (1977), 253–266.
[17] T. Kasami and N. Tokura, On the weight structure of Reed-Muller codes, IEEE Trans. Information Theory, 16 (1970), 752–759.
[18] A. Logachev, V. Yashchenko and M. Denisenko, Local affinity of Boolean mappings, in Boolean Functions in Cryptology and Information Security, NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur., 18, IOS, Amsterdam, 2008, 148–172.
[19] F. J. MacWilliams and N. J. Sloane, The Theory of Error-Correcting Codes, North-Holland Mathematical Library, 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.
[20] R. L. McFarland, A family of difference sets in non-cyclic groups, J. Combinatorial Theory Ser. A, 15 (1973), 1–10.
[21] J. C. C. McKinsey, On Boolean Functions of Many Variables, Ph.D thesis, University of California in Berkeley, 1936.
[22] S. Mesnager, Bent Functions: Fundamentals and Results, Springer, Cham, 2016.
[23] O. S. Rothaus, On “bent” functions, J. Combinatorial Theory Ser. A, 20 (1976), 300–305.
[24] Zheng and Zhang, Maiorana-McFarland construction of plateaued functions, IEEE Trans. Inform. Theory, 47 (2001), 1215–1223.

Received November 2018; 1st revision November 2018; 2nd revision July 2019.

E-mail address: claude.carlet@univ-paris8.fr
E-mail address: feukouaf@yahoo.fr