ON THE SUPPORTS OF THE WALSH TRANSFORMS OF BOOLEAN FUNCTIONS

CLAUDE CARLET[1,2] AND SIHEM MESNAGER[2]

Abstract. In this paper, we study, in relationship with covering sequences, the structure of those subsets of $\mathbb{F}_2^n$ which can be the Walsh supports of Boolean functions.

1. Introduction

Cryptographic Boolean functions play an important role in the design of hash functions and of stream and block ciphers. Various criteria related to cryptographically desirable Boolean functions have been proposed, such as balancedness, high nonlinearity, high correlation immunity order, high degree of the propagation criterion and inexistence of linear structure. The most important mathematical tool for the study of cryptographic properties of Boolean functions is the Walsh (or Hadamard) transform, the characteristic 2 special case of the discrete Fourier transform. The Walsh transform permits to measure the correlation between a Boolean function and all linear Boolean functions. The knowledge of the Walsh transform of a Boolean function uniquely determines the function and hence it is possible to work entirely with the Walsh transform. In particular, its systematic use leads to uniform, elegants and efficient treatments and statements of the main cryptographic criteria. Resiliency and inexistence of linear structures are directly related to the properties of the support of the Walsh transform of a Boolean function (i.e. its Walsh support). And the existence of covering sequences, which has been shown to have a deep relationship with the cryptographic properties of a function, directly depends on the structure of its Walsh support. Recall that the notion of covering sequence of a Boolean function, related to the derivatives of the function, was introduced in [5]; there is a complete characterization of the balancedness of Boolean functions by means of their covering sequences, and there exists a characterization of those Boolean functions which admit some given covering sequence by means of their Fourier spectra.
The other essential criteria - degree, non-linearity, propagation criterion - are also connected with the Walsh support of a Boolean function.
However, little is known on the possible structure of the Walsh supports of Boolean functions. We know only few generic examples of subsets of $\mathbb{F}_2^n$ which can be the Walsh supports of some Boolean functions on n variables. We know even less examples of subsets of $\mathbb{F}_2^n$ which cannot be such supports.

In this paper, we summerize what is known on this subject and we introduce several new results. In Section 2, we first introduce the notation, the definitions and preliminary results on covering sequences. We study subsequently the Walsh

Date: October 4, 2004.

supports of those balanced Boolean functions whose covering sequences are indicators of flats. We show (Proposition 2.4) that, for any Boolean function f on $\mathbb{F}_2^n$ which admits no derivative equal to the constant function 1 and any flat $a+E$ of $\mathbb{F}_2^n$, there is an equivalence between the fact that f admits the indicator of $a+E$ of $\mathbb{F}_2^n$ as non-trivial covering sequence and the fact that the Walsh support of f is disjoint from the orthogonal space of E. We characterize those Boolean functions on $\mathbb{F}_2^n$ whose Walsh support is disjoint from the orthogonal of a given vector subspace of $\mathbb{F}_2^n$. Next, in Section 3, we study the possible structures of the Walsh supports of Boolean functions. Along the way, we recall what are the Walsh supports of classical Boolean functions : affine, quadratic, bent and partially bent. It is well known that, for every n, many kinds of Boolean functions (including the classical Maiorana-McFarland's functions) can have Walsh support equal to the whole space $\mathbb{F}_2^n$, and that the empty set cannot be such support. Also, any singleton is the support of an affine function. The next natural step is to ask whether the difference $\mathbb{F}_2^n \setminus \{a\}$ (where a denotes any vector of $\mathbb{F}_2^n$) can be or not the Walsh support of a Boolean function. We remark that adding a linear function moves a to 0; this brings us to be interested in finding balanced Boolean functions whose Walsh support is $\mathbb{F}_2^n \setminus \{0\}$. For small values of the number of variables, it is easy to see that every balanced Boolean function f is such that there exists $a \neq 0$ in $\mathbb{F}_2^n$ such that $x \mapsto f(x) \oplus a \cdot x$ is also balanced (in other words, the cardinality of the Walsh support of f cannot equal $2^n - 1$). For $n \geq 10$, we give a construction of a class of balanced Boolean functions whose Walsh support has size $2^n - 1$ (cf. Construction 3.1). Such functions admit only one kind of covering sequences: the sequences which are constant on $\mathbb{F}_2^n \setminus \{0\}$. The question of knowing whether such functions are exceptional arises then (indeed, there are several examples of characteristics of n-variable Boolean functions, which are impossible for small values of n, and which become the common case for high values of n). We prove in Proposition 3.3 that such functions are rare among the balanced Boolean functions.

2. Notation and Preliminaries

We shall have to distinguish in the whole paper between the additions of integers in $\mathbb{Z}$, denoted by $+$ and $\sum_i$, and the additions mod 2, denoted by $\oplus$ and $\bigoplus_i$. For simplicity and because there will be no ambiguity, we shall denote by $+$ the addition of vectors of $\mathbb{F}_2^n$ (words). If x and b are two vectors in $\mathbb{F}_2^n$, we denote by $x \cdot b$ the usual inner product $x \cdot b = \bigoplus_{i=1}^n x_i b_i$ in $\mathbb{F}_2^n$. We recall the basic facts about Boolean functions. A Boolean function f is an $\mathbb{F}_2$-valued function on the vector-space $\mathbb{F}_2^n$ of n-tuples of elements from $\mathbb{F}_2$. Any Boolean function f in n variables admits a unique algebraic normal form (A.N.F.) :

$$f(x_1, \ldots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u \left(\prod_{i=1}^n x_i^{u_i} \right) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u$$

We call the degree of the algebraic normal form of a Boolean function its algebraic degree. The *Hamming weight* $\mathrm{wt}(f)$ of f is the number of vectors x in $\mathbb{F}_2^n$ such that $f(x) = 1$. A function f is *balanced* if $\mathrm{wt}(f) = \mathrm{wt}(f \oplus 1)$, i.e. if $\mathrm{wt}(f) = 2^{n-1}$. The *"sign" function* of f is the integer-valued function $\widehat{\chi_f}(x) = (-1)^{f(x)}$. The Walsh transform of $\widehat{\chi_f}$, whose value at $b \in \mathbb{F}_2^n$ equals by definition $\widehat{\chi_f}(b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x \cdot b}$, is related to the Hamming weight of the function $f \oplus l_b$ (where

$l_b(x) = b \cdot x$) via the relation: $\widehat{\chi_f}(b) = 2^n - 2\mathrm{wt}(f \oplus l_b)$. It satisfies Parseval's relation:

$$\sum_{b\in\mathbb{F}_2^n} \widehat{\chi_f}^2(b) = 2^{2n} \tag{1}$$

and the inverse formula relation:

$$\sum_{b\in\mathbb{F}_2^n} \widehat{\chi_f}(b)(-1)^{b\cdot x} = 2^n \chi_f(x) \tag{2}$$

The *Hamming distance* between two Boolean functions f_1 and f_2 on $\mathbb{F}_2^n$ is equal to the weight of $f_1 \oplus f_2$. The minimum distance between f and the set of all affine functions, called the *nonlinearity* of f, is denoted by N_f and satisfies the relation:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{b\in\mathbb{F}_2^n} |\widehat{\chi_f}(b)| \,. \tag{3}$$

Because of Parseval's relation, it is upper bounded by $2^{n-1} - 2^{n/2-1}$. This bound is tight for n even. The functions which achieve it are called *bent*. But since these functions are never balanced, the maximum nonlinearity of balanced functions is unknown for every $n \geq 8$. Let f be a Boolean function on $\mathbb{F}_2^n$. The autocorrelation function of the real valued function $F(x) = (-1)^{f(x)}$ is defined by $\hat{r}(s) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+f(x+s)}$. If f satisfies ths equality $(2^n - N_{\hat{r}})(2^n - N_{\hat{F}}) = 2^n$, where $N_{\hat{r}}$ and $N_{\hat{F}}$ are the number of zeros of respectively $\hat{r}$ and $\hat{F}$. Then, f is called partially-bent. Throughout this paper, S_f denotes the Walsh support of f, *i.e.* $S_f := \{\omega \in \mathbb{F}_2^n \mid \widehat{\chi_f}(\omega) \neq 0\}$. Let f be a Boolean function on $\mathbb{F}_2^n$ and let $a \in \mathbb{F}_2^n$. The derivative of f with respect to a, denoted by $D_a f$, is defined by : $D_a f(x) = f(x) \oplus f(x + a)$ for every $x \in \mathbb{F}_2^n$. As shown in [5], these derivatives satisfy the identity : $\sum_{a\in\mathbb{F}_2^n} D_a f(x) = \frac{1}{2}\left(2^n - \chi_f(x)\widehat{\chi_f}(0)\right)$.

2.1. **Covering sequences of balanced functions.**

Definition 2.1. A *covering sequence* of a Boolean function f on $\mathbb{F}_2^n$ is any sequence $\lambda = (\lambda_a)_{a\in\mathbb{F}_2^n}$ such that $\sum_{a\in\mathbb{F}_2^n} \lambda_a D_a f$ is a constant function ρ. The value of ρ is called the *level* of this sequence. If $\rho \neq 0$, then we say that the covering sequence is *non-trivial*.

The following characterization of balanced Boolean functions is shown in [5] :

Proposition 2.1. *If a Boolean function on $\mathbb{F}_2^n$ admits a non-trivial covering sequence, then it is balanced. Conversely, any balanced function admits the constant sequence 1 as non-trivial covering sequence (with level 2^{n-1}). Thus, any Boolean function is balanced if and only if it admits a non-trivial covering sequence.*

Any balanced quadratic function, and more generally any balanced partially-bent function (cf. [3]), admits a non-trivial atomic covering sequence (i.e. with one coefficient λ_a equal to 1 and all the others null). Equivalently, it has a derivative equal to 1. For such functions, we can say that balancedness and the existence of covering sequences are clear. *In this paper, we are interested in the functions which admit no derivative $D_a f$ equal to the constant function* 1.

Recall that we denote by $\widehat{\chi_f}(b)$ the value $\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+x\cdot b}$. We denote similarly by $\widehat{\lambda}(b)$ the value $\sum_{a\in\mathbb{F}_2^n}\lambda_a(-1)^{a\cdot b}$, i.e. the value at b of the Fourier transform of the sequence λ. Recall also that the support of λ is $\{a\in\mathbb{F}_2^n \mid \lambda_a\neq 0\}$. The following characterization is shown in [5] :

Theorem 2.2. *Let f be any Boolean function on $\mathbb{F}_2^n$ and $\lambda=(\lambda_a)_{a\in\mathbb{F}_2^n}$ any (real-valued or integer-valued) sequence.*
f admits λ as covering sequence if and only if $\widehat{\lambda}$ takes constant value on the support $S_f=\{b\in\mathbb{F}_2^n \mid \widehat{\chi_f}(b)\neq 0\}$ of $\widehat{\chi_f}$. Let r be this constant value, then the level of this covering sequence is the number $\frac{1}{2}[(\sum_{a\in\mathbb{F}_2^n}\lambda_a)-r]$.

Notice that if $\widehat{\lambda}$ takes value r on the support of $\widehat{\chi_f}$ then, replacing its coefficient λ_0 by λ_0-r, we obtain a covering sequence λ' such that $\widehat{\lambda'}$ takes value 0 on the support of $\widehat{\chi_f}$. Note also that, if the Walsh support of a balanced function equals $\mathbb{F}_2^n\setminus\{0\}$, then, according to Theorem 2.2 and to the bijectivity of the Fourier transform, the only covering sequences of f are constant on $\mathbb{F}_2^n\setminus\{0\}$ (indeed, their Fourier transforms are constant on $\mathbb{F}_2^n\setminus\{0\}$).

2.2. **Walsh support of balanced Boolean functions whose covering sequences are indicators of flats.** Since every balanced function admits the constant covering sequence 1, we focus now on the covering sequences whose coefficients are equal to 0 or 1.In the sequel, we shall always exclude the possibility that a function admits a derivative equal to the constant 1, because it is an extremal case (and it is the simplest case of balancedness for a Boolean function). Moreover, the functions admitting constant derivatives are degenerate (see [8]).
We first make an observation on those Boolean functions which admit a covering sequence which support is included in a vector subspace of $\mathbb{F}_2^n$.

Proposition 2.3. *Let E be any vector subspace of $\mathbb{F}_2^n$. Let f be any Boolean function on $\mathbb{F}_2^n$. Then f admits a covering sequence λ with support $S\subseteq E$ if and only if the restriction of f to any coset of E (viewed as a function on E) admits the same covering sequence λ.*

Proof. The condition is clearly necessary and sufficient since the integer-valued function $\sum_{a\in E}\lambda_a D_a f$ is equal to a constant function ρ if and only if its restriction to any coset of E equals ρ. □

Proposition 2.4. *Let E be any vector subspace of $\mathbb{F}_2^n$ and $u+E$ any of its cosets. Let f be any Boolean function on $\mathbb{F}_2^n$. Assume it admits no derivative $D_a f$ equal to the constant function 1. Then f admits the indicator of $u+E$ as non-trivial covering sequence if and only if the support of $\widehat{\chi_f}$ is disjoint from $E^\perp=\{x\in\mathbb{F}_2^n \mid x\cdot v=0,\ \forall v\in E\}$. This is equivalent to the fact that the restriction of f to any coset of E is balanced. The level of this covering sequence is then equal to $|E|/2$ and the indicator of every coset of E is also a covering sequence of f with the same level. More generally, any sequence λ such that for every $a\in E$ and every $u\in\mathbb{F}_2^n$, $\lambda_{a+u}=\lambda_u$ is also a covering sequence of f.*

Proof. Denote by λ the indicator of $u+E$. For every $b\in\mathbb{F}_2^n$, $\widehat{\lambda}(b)=\sum_{a\in E}(-1)^{(u+a)\cdot b}$ equals $(-1)^{u\cdot b}\ |E|$ if $b\in E^\perp$ and 0 otherwise. Thus, according to Theorem 2.2, alinea 2, λ is a covering sequence of f if and only if the support of $\widehat{\chi_f}$ is either included in $E^\perp\cap u^\perp$ (but in such case, the covering sequence is trivial, since we

have then $r = \sum_{a\in\mathbb{F}_2^n} \lambda_a = |E|$ in Theorem 2.2; this is excluded by the hypothesis) or included in $E^\perp \setminus u^\perp$ (but in such case, for every element a of $u+E$, the function $D_a f$ is equal to the constant function 1, since we have then $r = -|E|$ in Theorem 2.2; this is also excluded by the hypothesis), or disjoint from $E^\perp$ (in which case the level of the sequence is equal to $|E|/2$). This last case is the only one satisfying the hypothesis. Its equivalence with the fact that the restriction of f to any coset of E is balanced is a consequence of Proposition 2.3 applied to the sequence equal to the indicator of E and of Proposition 2.1.
The indicator of every coset of E is then clearly also a covering sequence of such function f with the same level.
Any sequence λ such that $\lambda_{a+u} = \lambda_u$ for every $a \in E$ and every $u \in \mathbb{F}_2^n$ is the linear combination of the indicators of cosets of E. Therefore, it is also a covering sequence of f. □

Remark. If a balanced functions f is such that $\widehat{\chi_f}^{-1}(0)$ contains a non-zero vector b, then we can apply Propositions 2.4 and 2.3 to the vector-subspace $E^\perp = \{0, b\}$. Hence, a balanced function admits a non-trivial non-constant covering sequence if and only if its Walsh support is different from $\mathbb{F}_2^n \setminus \{0\}$.

Remark. Let f be any Boolean function on $\mathbb{F}_2^n$ and $\lambda = (\lambda_a)_{a\in\mathbb{F}_2^n}$ a covering sequence of f. Let r be the constant value of $\widehat{\lambda}$ on the support of $\widehat{\chi_f}$. Then the nonlinearity of f satisfies:

$$N_f \leq 2^{n-1} - \frac{2^{n-1}}{\sqrt{|\widehat{\lambda}^{-1}(r)|}}.$$

Indeed, according to Parseval's relation (1) and since the support of $\widehat{\lambda}$ is included in $\widehat{\lambda}^{-1}(r)$, we have

$$\sum_{b\in\widehat{\lambda}^{-1}(r)} \widehat{\chi_f}^2(b) = 2^{2n}.$$

Thus, we have

$$\max_{b\in\mathbb{F}_2^n} \left(\widehat{\chi_f}^2(b)\right) = \max_{b\in\widehat{\lambda}^{-1}(r)} \left(\widehat{\chi_f}^2(b)\right) \geq \frac{2^{2n}}{|\widehat{\lambda}^{-1}(r)|}$$

and the result follows from relation (3).

3. The Walsh supports of Boolean functions

We denote by $\mathcal{S}_n$ the set of all the Walsh supports of Boolean functions on $\mathbb{F}_2^n$. We begin with some general elementary remarks on $\mathcal{S}_n$. We subsequently study the possible structures of Walsh supports.

3.1. **Generalities.** For every n, $\mathcal{S}_n$ is globally invariant under any affine automorphism of $\mathbb{F}_2^n$. Indeed, it is clearly invariant under translations since if $g(x) = f(x) \oplus a \cdot x$ then $S_g = a + S_f$, and it is also invariant under linear isomorphisms: let f be any Boolean function on $\mathbb{F}_2^n$, and L any linear automorphism of $\mathbb{F}_2^n$; let $L^\star$ be the unique linear automorphism of $\mathbb{F}_2^n$ such that, for every x and y in $\mathbb{F}_2^n$, we have: $y \cdot L^\star(x) = L(y) \cdot x$ (the matrices of these two automorphisms are transposed one of each other and we have $(L^\star)^{-1} = (L^{-1})^\star$). Then for every b in $\mathbb{F}_2^n$, we have $\widehat{\chi_{f\circ L^\star}}(b) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f\circ L^\star(x)+x\cdot b} = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+L^{\star\,-1}(x)\cdot b} =$

$\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+x\cdot L^{-1}(b)} = \widehat{\chi_f}(L^{-1}(b))$. Thus, the Walsh support of $f\circ L^\star$ is equal to $L(S_f)$.

If f is a Boolean function on $\mathbb{F}_2^n$ and g a Boolean function on $\mathbb{F}_2^m$, then $S_f\times S_g$ is the Walsh support of the function $h(x,y)=f(x)\oplus g(y)$ on $\mathbb{F}_2^{n+m}$. In particular, taking g affine, S_g is then a singleton and $S_h = S_f\times\{a\}$.

We do not know any other example of an operation on sets, under which $\mathcal{S}_n$ would be globally invariant. In particular, $\mathcal{S}_n$ is not invariant under intersection; indeed, it contains all singletons (it is well-known that if f is affine, say $f(x)=a\cdot x\oplus\epsilon$, then S_f equals the singleton $\{a\}$, and the converse is true according to Parseval's relation and to Relation (2)) and it does not contain the empty set. It is not invariant under union or symmetric difference either; indeed, it does not contain pairs: let us suppose that a pair $\{a,b\}$, $a\neq b$, is the Walsh support of a Boolean function f; let us denote by λ_a and λ_b the values of the Walsh transform of f at a and b; then, we have $|\lambda_a|<2^n$ and $|\lambda_b|<2^n$ according to Parseval's relation; and according to Relation (2), we have $\lambda_a+\lambda_b=\pm 2^n$ and $\lambda_a-\lambda_b=\pm 2^n$, which is clearly impossible. Many secondary constructions of Boolean functions permit to express the Walsh transform of the constructed function f by means of those of the functions taken in input; but the Walsh support of f depends on the values of the these Walsh transforms - not only on their supports. This is the case, for instance, of Siegenthaler's construction $f(x,x_{n+1})=(x_{n+1}\oplus 1)f_1(x)\oplus x_{n+1}f_2(x)$, for which we have $\widehat{\chi_f}(a,a_{n+1})=\widehat{\chi_{f_1}}(a)+(-1)^{a_{n+1}}\widehat{\chi_{f_2}}(a)$.

3.2. **The whole space $\mathbb{F}_2^n$ as a Walsh support.** For every n, $\mathcal{S}_n$ contains $\mathbb{F}_2^n$ as an element, i.e. there exist functions f whose Walsh support is equal to $\mathbb{F}_2^n$. These functions, which are such that no function $f(x)\oplus b\cdot x\oplus\epsilon$ (where $b\in\mathbb{F}_2^n$, $\epsilon\in\mathbb{F}_2$) is balanced, can be constructed in many different ways. A first class of examples of such functions is that of Boolean functions of odd weights. A second class, valid for every even n, is that of *bent* functions, which are characterized by the fact that, for every $b\in\mathbb{F}_2^n$, the number $\widehat{\chi_f}(b)$ has magnitude $2^{n/2}$. A third example can be found in the general class of Maiorana-McFarland functions. The following proposition is well-known (see for instance [2, 4]).

Proposition 3.1. *Let s and t be any positive integers, g any Boolean function on $\mathbb{F}_2^t$ and ϕ any mapping from $\mathbb{F}_2^t$ to $\mathbb{F}_2^s$. Define for every $x\in\mathbb{F}_2^s$ and every $y\in\mathbb{F}_2^t$: $f(x,y)=x\cdot\phi(y)\oplus g(y)$. Then*

$$\widehat{\chi_f}(a,b)=2^s\sum_{y\in\phi^{-1}(a)}(-1)^{g(y)\oplus b\cdot y},\forall a\in\mathbb{F}_2^s,\ b\in\mathbb{F}_2^t.$$

Thus, if for every $a\in\mathbb{F}_2^s$ the set $\phi^{-1}(a)$ has odd size (such ϕ exists if and only if $s\leq t$) then the support of $\widehat{\chi_f}$ is equal to $\mathbb{F}_2^{s+t}$.

3.3. **The other flats of $\mathbb{F}_2^n$ as Walsh supports.**

3.3.1. *Even-dimensional flats.* For every n, the Walsh support of any quadratic function on $\mathbb{F}_2^n$ is a flat of $\mathbb{F}_2^n$ of even dimension. Conversely any flat of $\mathbb{F}_2^n$ of even dimension is the Walsh support of a quadratic function.

Indeed, any quadratic function f on $\mathbb{F}_2^n$ may be written (see [10]) as $f=q^{(t)}\circ A\oplus\ell_a\oplus\epsilon$, where $q^{(t)}$ denotes the canonical quadratic function: $q^{(t)}(x_1,...,x_n)=$

$\bigoplus_{i=1}^{t} x_i x_{t+i}$, $\epsilon \in \mathbb{F}_2$, A is a linear automorphism of $\mathbb{F}_2^n$ and ℓ_a, $a \in \mathbb{F}_2^n$, is the linear Boolean function $\ell_a(x) := a \cdot x$. According to Subsection 3.1, we have $S_f = a + A^\star(S_{q^{(t)}})$. It is well known that $S_{q^{(t)}} = \mathbb{F}_2^{2t} \times \{0\}$ and so S_f is a flat of $\mathbb{F}_2^n$ of even dimension. Conversely, let $a + V$ be any flat of $\mathbb{F}_2^n$ of even dimension (V being a vector subspace of $\mathbb{F}_2^n$); there exists a linear automorphism A of $\mathbb{F}_2^n$ such that $A(V) = \mathbb{F}_2^{2t} \times \{0\}$. Set $f := q^{(t)} \circ A^{\star -1} \oplus \ell_a$. Hence $S_f = a + A^{-1}(\mathbb{F}_2^{2t} \times \{0\}) = a + V$.

More generally, the Walsh support of any partially-bent function on $\mathbb{F}_2^n$, that is, of any function $f = g \circ A \oplus \ell_a \oplus \epsilon$, where g is a bent function on $2t$ variables and A is a linear mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{2t}$, is a flat of $\mathbb{F}_2^n$ of even dimension. Conversely any flat of $\mathbb{F}_2^n$ of even dimension is the Walsh support of a partially-bent function, in which the choice of the bent function g is arbitrary.

3.3.2. *Odd-dimensional flats.* For every n, there also exist functions whose Walsh supports are odd-dimensional flats $a + E$ of $\mathbb{F}_2^n$ of dimensions greater than 3 (E being a vector subspace of $\mathbb{F}_2^n$) : take for instance $f := \delta_{E^\perp} \oplus \ell_a$ where ℓ_a denotes the linear Boolean function $\ell_a(x) := a \cdot x$ and $\delta_{E^\perp}$ denotes the indicator of $E^\perp := \{x \in \mathbb{F}_2^n \mid \forall y \in E,\, x \cdot y = 0\}$; according to Subsection 3.1, $S_f = a + S_{\delta_{E^\perp}}$; now, straightforward calculation yields

$$\widehat{\chi_{\delta_{E^\perp}}}(\omega) = \begin{cases} 2^n - 2\left|E^\perp\right| & \text{if } \omega = 0 \\ -2\left|E^\perp\right| & \text{if } \omega \in E \setminus \{0\} \\ 0 & \text{otherwise} \end{cases}$$

Therefore $S_{\delta_{E^\perp}} = E$.

Remark. We have excluded the case of 1-dimensional flats in the construction above. Actually, this case is peculiar, since we have seen that a pair (that is, a 1-dimensional flat) cannot be the Walsh support of a Boolean function..

3.4. **Complements of singletons.** As seen in the introduction, if a Boolean function f is such that there exists a balanced function $f(x) \oplus b \cdot x \oplus \epsilon$ in the coset of the Reed-Muller code of order 1 which contains f, then changing $f(x)$ into $f(x) \oplus b \cdot x \oplus \epsilon$ permits to assume that f itself is balanced. Thus we are brought to study the Walsh supports of balanced functions. We show now that there exist balanced functions f such that $\widehat{\chi_f}^{-1}(0)$ contains no non-zero vector, by giving a construction of a new class of a Boolean function whose Walsh support is $\mathbb{F}_2^n \setminus \{0\}$ in any dimension $n \geq 10$. This has never been settled in the literature.

Construction 3.1. Let k and m be two positive integers such that $m \geq k + 2$ and $2^{k-1} \geq m + 1$ (this is possible only with $m \geq 6$ and $k \geq 4$). Then there exists a mapping ϕ from $\mathbb{F}_2^m$ to $\mathbb{F}_2^k$ such that the size of $\phi^{-1}(0)$ is equal to 1 and, for any nonzero vector $a \in \mathbb{F}_2^k$, the size of $\phi^{-1}(a)$ is an odd integer greater than or equal to 3. There also exists a subset E of $\mathbb{F}_2^k \times \mathbb{F}_2^m$ such that $E \subseteq \{(x, y) \in \mathbb{F}_2^k \times \mathbb{F}_2^m / \, x \cdot \phi(y) = 0\}$, such that $|E| = 2^{k-1}$ and which contains an element $(0, v)$ of even Hamming weight as well as all the elements of the form $(0, u^i)$, where the vector u^i ($1 \leq i \leq m$) is defined as $u^i_j = 1$ if $j = i$ and $u^i_j = 0$ otherwise. We denote by δ_E the indicator of E: $\delta_E(x, y) = 1$ if $(x, y) \in E$ and $\delta_E(x, y) = 0$ otherwise. Define then the following Boolean function f on $\mathbb{F}_2^{k+m}$:

$$\forall (x, y) \in \mathbb{F}_2^k \times \mathbb{F}_2^m, \quad f(x, y) := \phi(y) \cdot x \oplus \delta_E(x, y).$$

Proposition 3.2. *Let f be defined as in construction 3.1. Then f is balanced and the Walsh support S_f of f equals $\mathbb{F}_2^n \setminus \{0\}$.*

Proof. A straightforward calculation yields

$$\forall (a,b) \in \mathbb{F}_2^k \times \mathbb{F}_2^m, \quad \widehat{\chi_f}(a,b) = 2^k \sum_{y \in \phi^{-1}(a)} (-1)^{b \cdot y} - 2 \sum_{(x,y) \in E} (-1)^{a \cdot x \oplus b \cdot y}.$$

In particular, when $(a,b) = (0,0)$, we have :

$$\widehat{\chi_f}(0,0) = 2^k |\phi^{-1}(0)| - 2|E| = 0$$

which ensures that f is balanced. Let $(a,b) \in \mathbb{F}_2^k \times \mathbb{F}_2^m$ be a non zero word i.e. $(a,b) \neq (0,0)$. If $b = 0$ then

$$\widehat{\chi_f}(a,0) \geq 2^k |\phi^{-1}(a)| - 2^k > 0$$

since $|\phi^{-1}(a)| > 1$. Assume now that $b \neq 0$. We have :

$$\forall y \in \phi^{-1}(a), \quad (-1)^{b \cdot y} \equiv 1 \pmod 2$$

Since $|\phi^{-1}(a)|$ is odd, it holds

$$\sum_{y \in \phi^{-1}(a)} (-1)^{b \cdot y} \equiv |\phi^{-1}(a)| \equiv 1 \pmod 2$$

which implies that

$$2^k \left| \sum_{y \in \phi^{-1}(a)} (-1)^{b \cdot y} \right| \geq 2^k.$$

Therefore it suffices to show that

$$\left| \sum_{(x,y) \in E} (-1)^{a \cdot x \oplus b \cdot y} \right| < 2^{k-1} = |E|$$

to ensure that $\widehat{\chi_f}(a,b) \neq 0$. To this end, we show that we can find two elements z_1 and z_2 in E such that $(a,b) \cdot z_1 = 0$ and $(a,b) \cdot z_2 = 1$. Suppose that b is not the all-one vector. There exists then at least two indices i and j such that $b_i = 0$ and $b_j = 1$, and it suffices to take $z_1 = (0, u^i)$ and $z_2 = (0, u^j)$. If b is the all-one vector, it suffices to take $z_1 = (0, v)$ and $z_2 = (0, u^1)$. □

Concerning the values of n smaller than 10, we know that for $n = 1$, the Boolean function $f : x \in \mathbb{F}_2 \mapsto x$ is such that $S_f = \mathbb{F}_2 \setminus \{0\}$. By computer search, we know that there is no Boolean function f such that $S_f = \mathbb{F}_2^n \setminus \{0\}$ when $n \in \{2,3,4\}$. We classify in appendix B all the Walsh supports of Boolean function in 5 variables using a computer and observe that there does not exists Boolean function in 5 variables whose Walsh support is equal to $\mathbb{F}_2^5 \setminus \{0\}$.

Concerning the case $n = 6$. Assume there exists a Boolean function f in 6 variables such that $S_f = \mathbb{F}_2^6 \setminus \{0\}$. Let d be the algebraic degree of f (we assume $d \geq 2$ since the Walsh support of affine functions are singletons).

This is known that the values of a balanced Boolean function f in n variables of algebraic degree d are divisible by $2^{2+\lfloor \frac{n-2}{d} \rfloor}$. Therefore, for $d \in \{2,3,4\}$, the Walsh spectra of f is of the form $\{\pm 8k,\, k = 0 \dots 7\}$. Let n_k be the number of words $\omega \in \mathbb{F}_2^6$ such that $\widehat{\chi_f}(\omega) = \pm 8k$. Clearly $n_0 = 1$. Parseval's relation requires that $(\star)$ $\sum_{k=1}^7 k^2 n_k = 64$. Moreover the condition $S_f = \mathbb{F}_2^6 \setminus \{0\}$ implies that $(\star\star)$ $\sum_{k=1}^7 n_k = 63$. One easily note that there is no solutions for the diophantine system

formed with $(\star)$ and $(\star\star)$. This shows that d must be equal to 6. Unfortunately, we are no able to tell more.

Concerning the other values $n \in \{7, 8, 9\}$, the question remains completely open since all the arguments exposed above fail for these values of n.

The question then arises of knowing if there are few or many balanced Boolean functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that $S_f = \mathbb{F}_2^n \setminus \{0\}$. We answer in the proposition below that only a small number of balanced Boolean functions are such that $S_f = \mathbb{F}_2^n \setminus \{0\}$. We denote below by $\mathcal{E}_n$ the set of all balanced Boolean functions on $\mathbb{F}_2^n$.

Proposition 3.3. *For every positive integer $n \geq 10$, the density in $\mathcal{E}_n$ of the set $\{f \in \mathcal{E}_n \mid S_f = \mathbb{F}_2^n \setminus \{0\}\}$ is less than $\sqrt{\frac{\pi}{2}}\, e^{\frac{3}{2^{n+3}}}\, 2^{-\frac{n}{2}}$.*

Proof. Let us introduce the following family of subsets of the set $\mathcal{B}_n$ of all Boolean functions on $\mathbb{F}_2^n$:

$$F_a \,=\, \{f : \mathbb{F}_2^n \to \mathbb{F}_2 \mid S_f = \mathbb{F}_2^n \setminus \{a\}\},$$

where $a \in \mathbb{F}_2^n$.

It is easily shown that all the subsets F_a have the same cardinality: fix $a \in \mathbb{F}_2^n \setminus \{0\}$ and define the mapping φ_a from $\mathcal{B}_n$ to $\mathcal{B}_n$ which maps $f \in \mathcal{B}_n$ to $f \oplus \ell_a$ (where ℓ_a denotes the linear mapping on $\mathbb{F}_2^n$ defined as $\ell_a(x) := a \cdot x$ for every $x \in \mathbb{F}_2^n$). Given $f \in F_a$, one has $S_{\varphi_a(f)} = a + S_f = \mathbb{F}_2^n \setminus \{0\}$ (see Subsection 3.1). Hence φ_a is a bijection between F_a and F_0.
We deduce from the inclusion $\bigcup_{a \in \mathbb{F}_2^n} F_a \subseteq \mathcal{B}_n$ and from the fact that the sets F_a are pairwise disjoint that $|\mathcal{B}_n| \geq 2^n |F_0|$. Hence $|F_0| \leq 2^{2^n - n}$.

Finally, the density in $\mathcal{E}_n$ of F_0 is equal to $\frac{|F_0|}{|\mathcal{E}_n|}$. It is well-known that $|\mathcal{E}_n| = \binom{2^n}{2^{n-1}}$. Moreover Lemma A.2 provides the following lower bound on $|\mathcal{E}_n| : \binom{2^n}{2^{n-1}} \geq \sqrt{\frac{2}{\pi}}\, 2^{2^n - \frac{n}{2}}\, e^{-\frac{3}{2^{n+3}}}$. This lower bound together with the upper bound $|F_0| \leq 2^{2^n - n}$ yields to the result. □

Appendix A. Lower bounds on binomial coefficients

Lemma A.1 (Robbins, [11])**.** *For $n \geq 1$,*

$$n! \,=\, \sqrt{2\pi n}\, \left(\frac{n}{e}\right)^n\, e^{r(n)}$$

where $r(n)$ satisfies $\frac{1}{12n+1} < r(n) < \frac{1}{12n}$.

Lemma A.2. *For $n \geq 1$,*

$$\binom{2^n}{2^{n-1}} \,\geq\, \sqrt{\frac{2}{\pi}}\, 2^{2^n - \frac{n}{2}}\, e^{-\frac{3}{2^{n+3}}}$$

Proof. By definition , $\binom{2^n}{2^{n-1}} = \frac{2^n!}{\left(2^{n-1}!\right)^2}$. If we use Lemma A.1, then we get

$$\binom{2^n}{2^{n-1}} \geq \frac{\sqrt{\pi 2^{n+1}}\, \left(\frac{2^n}{e}\right)^{2^n}\, e^{r(2^n)}}{\pi 2^n \left(\frac{2^{n-1}}{e}\right)^{2^n}\, e^{2r(2^{n-1})}} = \sqrt{\frac{2}{\pi}} 2^{2^n - \frac{n}{2}} e^{r(2^n) - 2r(2^{n-1})}$$

Now

$$r(2^n) - 2r(2^{n-1}) \geq \frac{1}{12\, 2^n + 1} - \frac{2}{12\, 2^{n-1}} \geq -\frac{3}{2^{n+3}}$$

□

Appendix B. Classification of the Walsh supports of Boolean functions in five variables

Berlekamp and Welsh [1] shown that the set of all Boolean functions in 5 variables may be reduced to 48 equivalence classes where the Boolean functions are equivalent if and only if there exists a linear automorphism L on $\mathbb{F}_2^5$, two 5-dimensional binary vectors a and b and a binary scalar c such that

$$\forall x \in \mathbb{F}_2^n, \quad g(x) = f(L(x)+a) \oplus b \cdot x \oplus c \tag{4}$$

For the sake of simplicity, we suppose in the sequel that it holds $b = c = 0$ in (4) when we say that two Boolean functions are equivalent (because if two Boolean functions f and g are such that $g = f \oplus l$ where $l(x) := b \cdot x \oplus c$ then it holds : $S_g = b + S_f$). Berlekamp and Welsh got 29 equivalence classes of even Hamming weight and 19 equivalence classes of odd Hamming weight. In subsection 3.2, we have signalled that the Walsh support of Boolean functions of odd Hamming weight is necessarily equal to the whole space $\mathbb{F}_2^5$. Hence, the Walsh support of any Boolean function which is equivalent with one of the below Boolean function is equal to $\mathbb{F}_2^5$

$$\begin{gathered}
x_1x_2x_3x_4x_5 \\
x_1x_2 \oplus x_1x_2x_3x_4x_5 \\
x_1x_2 \oplus x_3x_4 \oplus x_1x_2x_3x_4x_5 \\
x_1x_2x_3 \oplus x_1x_2x_3x_4x_5 \\
x_1x_2 \oplus x_1x_2x_3 \oplus x_1x_2x_3x_4x_5 \\
x_1x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_3x_4x_5 \\
x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_3x_4x_5 \\
x_1x_4 \oplus x_2x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_3x_4x_5 \\
x_1x_2 \oplus x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_2x_3x_4x_5 \\
x_1x_2 \oplus x_3x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_3x_4x_5 \\
x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_1x_2x_3x_4x_5 \\
x_1x_2 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_1x_2x_3x_4x_5 \\
x_2x_3 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_1x_2x_3x_4x_5 \\
x_2x_3 \oplus x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_1x_2x_3x_4x_5 \\
x_2x_4 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_1x_2x_3x_4x_5 \\
x_2x_3 \oplus x_2x_4 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_1x_2x_3x_4x_5 \\
x_2x_4 \oplus x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_1x_2x_3x_4x_5 \\
x_2x_3 \oplus x_2x_4 \oplus x_3x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_1x_2x_3x_4x_5 \\
x_2x_3 \oplus x_2x_4 \oplus x_3x_5 \oplus x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_1x_2x_3x_4x_5
\end{gathered}$$

Table 1. Equivalence class of odd Hamming weight

It remains therefore to classify the Walsh supports of Boolean functions of the 29 equivalence classes of even Hamming weight. We base our study on the fact that the Walsh supports of two Boolean functions f and g lying in the same equivalent class are linked by the relation : $S_g = L^\star(S_f)$ (Here we take again the notation of (4)). Based on this remark, we obtain for each equivalence class the generic type of Walsh support of the elements. We adopt the following convention to write the Boolean functions and Walsh supports. The Boolean functions are written in abbreviated notation. For example, for $x_1x_2 \oplus x_2x_3x_4x_5$ we simply write $12 + 2345$. We do not write in the table the equivalence class of 0 because the equivalence class of 0 is

simply formed by affine functions on $\mathbb{F}_2^5$ which Walsh supports are the singletons of $\mathbb{F}_2^5$. Moreover, at each line of the below table, we give an element of each equivalence class in the first column and the type of Walsh supports in the second column. The Walsh support are also written in abbreviated notation. More precisely, given a basis $\{v_1, v_2, v_3, v_4, v_5\}$ of $\mathbb{F}_2^5$, we write $\{i\}$ for the singleton $\{v_i\}$, $(i_1 \dots i_p)$ for the vector subspace $\mathrm{span}(v_{i_1}, \dots, v_{i_p})$, $j + (i_1 \dots i_p)$ for the flat $v_j + \mathrm{span}(v_{i_1}, \dots, v_{i_p})$ and $i + j$ for the sum $v_i + v_j$ ($\mathrm{span}(\mathcal{F})$ denotes the vector subspace of $\mathbb{F}_2^5$ generated by the family $\mathcal{F}$ of vectors). For example, $1 + (2345) \cup 4 + (23) \cup (2)$ stands for $v_1 + \mathrm{span}(v_2, v_3, v_4, v_5) \cup v_4 + \mathrm{span}(v_2, v_3) \cup \mathrm{span}(v_2)$ and $(2345) \cup 1 + 4 + (23) \cup \{1\}$ stands for $\mathrm{span}(v_2, v_3, v_4, v_5) \cup v_4 + \mathrm{span}(v_2, v_3) \cup \{v_1\}$. To help the reader, we now explain the meaning of a line of the below table. For example, the second line means that the Walsh support of a Boolean function lying in the equivalence class of $x_1x_2 \oplus x_2x_3x_4x_5$ is of the form $v_1 + \mathrm{span}(v_2, v_3, v_4, v_5) \cup \mathrm{span}(v_2)$ where $\{v_1, v_2, v_3, v_4, v_5\}$ of $\mathbb{F}_2^5$ denotes a basis of $\mathbb{F}_2^5$ and, conversely, given a basis $\{v_1, v_2, v_3, v_4, v_5\}$ of $\mathbb{F}_2^5$, we can find an element in the equivalent class of $x_1x_2 \oplus x_2x_3x_4x_5$ whose Walsh support is equal to $v_1 + \mathrm{span}(v_2, v_3, v_4, v_5) \cup \mathrm{span}(v_2)$.

Equivalence class	Type of Walsh support
2345	(2345)
$12 + 2345$	$1 + (2345) \cup (2)$
$23 + 2345$	(2345)
$23 + 45 + 2345$	(2345)
$12 + 34 + 2345$	$1 + (2345) \cup (234)$
$123 + 2345$	$1 + (2345) \cup (23)$
$12 + 123 + 2345$	$(2345) \cup 1 + (23)$
$24 + 123 + 2345$	$1 + (2345) \cup 4 + (23) \cup (2)$
$14 + 123 + 2345$	$(2345) \cup 1 + 4 + (23) \cup \{1\}$
$45 + 123 + 2345$	$(2345) \cup 1 + (23)$
$12 + 34 + 123 + 2345$	$(2345) \cup 1 + (23)$
$14 + 35 + 123 + 2345$	$(2345) \cup 1 + (3) \cup 1 + 4 + (3) \cup 1 + 5 + (3) \cup 1 + 2 + 4 + 5 + (3)$
$12 + 45 + 123 + 2345$	$1 + (2345) \cup (45) \cup 2 + 5 + (4) \cup 3 + (2) \cup \{2 + 4\}$
$24 + 35 + 123 + 2345$	$1 + (2345) \cup (234) \cup 5 + (23)$
$123 + 145 + 2345$	$1 + (2345) \cup (23) \cup 5 + (4) \cup \{4\}$
$45 + 123 + 145 + 2345$	$(2345) \cup 1 + 3 + (2) \cup 1 + 5 + (4) \cup \{1 + 4\} \cup \{1 + 2\}$
$24 + 45 + 123 + 145 + 2345$	$(2345) \cup 1 + 4 + (3) \cup 1 + 2 + 5 + (4) \cup \{1 + 2 + 3 + 4\} \cup \{1 + 2\}$
$24 + 35 + 123 + 145 + 2345$	$1 + (2345) \cup (2) \cup 4 + (2) \cup 5 + (2) \cup 3 + (4) \cup \{2 + 3 + 4 + 5\} \cup \{3 + 5\}$
123	(123)
$45 + 123$	$\mathbb{F}_2^5$
$14 + 123$	$4 + (123) \cup (1)$
$14 + 25 + 123$	$(12) \cup 4 + (12) \cup 5 + (12) \cup 3 + 4 + 5 + (12)$
$123 + 145$	$\mathbb{F}_2^5$
$23 + 123 + 145$	$3 + (12) \cup (45) \cup 1 + 5 + (4) \cup 2 + (1) \cup \{1 + 4\}$
$24 + 123 + 145$	$\mathbb{F}_2^5$
$23 + 24 + 35 + 123 + 145$	$(2) \cup 4 + (2) \cup 1 + 2 + 3 + (5) \cup 3 + (4) \cup 5 + (2) \cup 1 + 4 + 5 + (2) \cup \{2 + 3 + 4 + 5\} \cup \{1 + 3 + 4 + 5\} \cup \{3 + 5\} \cup \{1 + 2 + 3 + 4\}$
12	(12)
$12 + 34$	(1234)

TABLE 2. Equivalence class of even Hamming weight

References

[1] E. R. Berlekamp, L. R. Welch. Weight Distributions of the Cosets of the $(32, 6)$ Reed-Muller Code. *IEEE Transactions on Information Theory* **18**, 1972.

[2] P. Camion, C. Carlet, P. Charpin, N. Sendrier, On correlation-immune functions, Advances in Cryptology: Crypto '91, Proceedings, Lecture Notes in Computer Science, V. 576, 1991, pp. 86–100.

[3] C. Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, **3**:135–145, 1993.

[4] C. Carlet. More correlation-immune and resilient functions over Galois fields and Galois rings. *Advances in Cryptology, EUROCRYPT' 97, Lecture Notes in Computer Science* 1233, pp. 422-433, Springer Verlag (1997)

[5] C. Carlet and Y. Tarranikov. Covering sequences of Boolean functions and their cryptographic significance. *Designs, Codes and Cryptography*, **25**:263–279, 2002.

[6] Seongtaek Chee, Sangjin Lee, Daiki Lee and Soo Hak Sung, On the Correlation Immune Functions and their Nonlinearity, Advances in Cryptology - Asiacrypt '96, Lecture Notes in Computer Science, V. 1163, 1996, pp. 232–243.

[7] B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, R. Smolensky, The bit extraction problem or t-resilient functions, IEEE Symposium on Foundations of Computer Science, V. 26, 1985, pp. 396–407.

[8] S. Dubuc. Characterization of linear structures. *Designs, Codes and Cryptography* vol. 22, pp. 33-45, 2001.

[9] E. Filiol, C. Fontaine, Highly Nonlinear Balanced Boolean Functions with a Good Correlation Immunity, Advanced in Cryptology, Eurocrypt '98, Helsinki, Finland, Lecture Notes in Computer Sciences, Vol. 1403, 1998, pp. 475–488.

[10] F. J. MacWilliams and N. J. A. Sloane, The theory of error-correcting codes, North–Holland, Amsterdam, 1977.

[11] H. Robbins. A Remark on Stirling Formula. *Amer. Math. Monthly*, 62:26–29, 1955.

[12] P. Sarkar. Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions.

[13] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Transactions on Information theory, V. IT-30, No 5, 1984, pp. 776–780.

[14] T. Siegenthaler, Decrypting a Class of Stream Ciphers Using Ciphertext Only, IEEE Transactions on Computer, V. C-34, No 1, Jan. 1985, pp. 81–85.

[15] H.-U. Simon, A tight $\Omega(\log \log n)$-bound on the time for parallel RAM's to compute nondegenerated boolean functions, FCT'83, Lecture Notes in Computer Science, V. 158, 1984, p. 439–444.

[16] Xiao Guo-Zhen and J. L. Massey. A Spectral Characterization of Correlation-Immune Combining Functions. *IEEE Trans. Inf. Theory*, Vol IT 34, n° 3, pp. 569-571 (1988).

[1]INRIA - Projet CODES, Bâtiment 25, Domaine de Voluceau - Rocquencourt, B.P. 105, 78153 Le Chesnay Cedex - France

[2]MAATICAH, Université de Paris VIII, Département de Mathématiques, 2, rue de la Liberté, 93526 Saint-Denis Cédex - France