A method of construction of balanced functions with optimum algebraic immunity

Abstract

Because of the recent algebraic attacks, a high algebraic immunity is now an absolutely necessary (but not sufficient) property for Boolean functions used in stream ciphers. A difference of only 1 between the algebraic immunities of two functions can make a crucial difference with respect to algebraic attacks. Very few examples of (balanced) functions with high algebraic immunity have been found so far. These examples seem to be isolated and no method for obtaining such functions is known. In this paper, we introduce a general method for proving that a given function, in any number of variables, has a prescribed algebraic immunity. We deduce an algorithm for generating balanced functions in any odd number of variables, with optimum algebraic immunity. We also give an algorithm, valid for any even number of variables, for constructing (possibly) balanced functions with optimum (or, if this can be useful, with high but not optimal) algebraic immunity. We also give a new example of an infinite class of such functions. We study their Walsh transforms. To this aim, we completely characterize the Walsh transform of the majority function.

Keywords: Boolean Function, Algebraic attack, Algebraic immunity.

1 Introduction

The two main models of pseudo-random generators using Boolean functions in stream ciphers - the combiner model, in which the outputs to several LFSRs are combined by the nonlinear Boolean function to produce the keystream, and the filter model, in which the content of some of the flip-flops in a single (longer) LFSR constitute the input to the function - have been the objects of a lot of cryptanalyses. This has led to design criteria for these functions, mainly: balancedness, a high algebraic degree, a high nonlinearity and, in the case of the combiner model, a high correlation immunity (the filter model is theoretically equivalent to the combiner model, but the attacks do not work similarly on each system). A recent attack uses the fact that it is possible to obtain a very over-defined system of multivariate nonlinear equations whose unknowns are the bits of the initialization of the LFSR(s). This improvement of an idea due to C. Shannon [29] uses the existence of low degree multiples of the nonlinear function.

It is called *algebraic attack* [5, 14, 17, 18, 15, 25, 27] and has deeply modified the situation with Boolean functions in stream ciphers. Given a Boolean function f on n variables, different kinds of scenarios related to low degree multiples of f have been studied in [18, 27]. The core of the analysis is to find out minimum (or low) degree nonzero annihilators of f or of $1 + f$, that is, functions g such that $f * g = 0$ or $(1 + f) * g = 0$, where "$*$" is the multiplication of functions inheritated from the multiplication in F_2.

Since the introduction of algebraic attacks on stream ciphers [18], the research of Boolean functions that can resist them has not given fully satisfactory results. It has produced only a small number of examples (if we exclude those results of [9] which may be false; see how these results have been modified in [6]) and no method for obtaining such functions. The two main results are:
1. In [19], an iterative construction of a $2k$-variable Boolean function with algebraic immunity provably equal to k (that is, optimal). The produced function has been further studied in [13]. It has very high algebraic degree and there exists an algorithm giving a very fast way (whose complexity is linear in the number of variables) of computing the output to the function, given its input. But the function is not balanced and its nonlinearity is weak.
2. In [20] and [9], examples of symmetric functions (that is, of functions whose outputs depend only on the Hamming weight of their input) achieving optimum algebraic immunities. Being symmetric, they present a risk if attacks using this peculiarity can be found in the future. Moreover, they do not have high nonlinearities either.

Last but not least drawback of all these functions: they do not behave well with respect to fast algebraic attacks [3, 15, 8]: see [2, 21].

In the present paper, we completely change the situation by giving in Section 3 a general way of proving that a given function has algebraic immunity at least k, where k is any integer upper bounded by $\lceil \frac{n}{2} \rceil$, leading to a way of designing Boolean functions, which can be balanced, and whose algebraic immunity is at least k. We deduce that any function, whose value at every vector of weight strictly smaller than $n/2$ (n even) is null (resp. equals 1), and whose value at every vector of weight strictly greater than $n/2$ equals 1 (resp. is null), has algebraic immunity $n/2$. This is the first example of a class of functions with optimal algebraic immunity, which includes many elements for every (even) number of variables[1]. However, these functions are not much different from symmetric functions and we also show that they cannot have good nonlinearity. We then specify our general construction to obtain an algorithm for designing numerous functions in even number of variables n and with optimal algebraic immunity $n/2$, among which exist balanced functions. We also exhibit an infinite class of such functions. We study the Walsh transforms of these functions in Section 6: we completely characterize the Walsh transform of the majority function and we deduce the Walsh transforms of these functions.

[1] It has been independently shown in [4] that some functions of this class have optimum algebraic immunity (in a slightly stronger sense). These functions have a property similar to the existence of a linear structure, which is a potential weakness.

2 Preliminaries

A Boolean function on n variables is a mapping from F_2^n into F_2, the finite field with two elements. We denote by B_n the set of all n-variable Boolean functions. The basic representation of a Boolean function $f(x_1, \ldots, x_n)$ is by the output column of its *truth table*, i.e., a binary string of length 2^n, $f = [f(0,0,\ldots,0), f(1,0,\ldots,0), f(0,1,\ldots,0), f(1,1,\ldots,0), \ldots, f(1,1,\ldots,1)]$.

The *Hamming weight* $wt(f)$ of a Boolean function f on n variables is the weight of this string, that is, the size of the support $supp(f) = \{x \in F_2^n;\ f(x) = 1\}$ of the function. The *Hamming distance* $d(f,g)$ between two Boolean functions f and g is the Hamming weight of their difference $f+g$ (by abuse of notation, we use $+$ to denote the addition in F_2, i.e., the XOR). We say that a Boolean function f is balanced if its truth table contains an equal number of 1's and 0's, that is, if its Hamming weight equals 2^{n-1}.

The truth table does not give an idea of the algebraic complexity of the function. This is why another representation is used. Any Boolean function has a unique representation as a multivariate polynomial over F_2, called the algebraic normal form (ANF),

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

where the a_I's are in F_2. The algebraic degree, $\deg(f)$, is the number of variables in the highest order term with non zero coefficient.
A Boolean function is affine if it has degree at most 1 and the set of all affine functions is denoted by A_n.

Boolean functions used in cryptographic systems must have high nonlinearity to withstand linear and correlation attacks [22, 10]. The *nonlinearity* of an n-variable function f is its distance from the set of all n-variable affine functions, i.e.,

$$nl(f) = \min_{g \in A_n} (d(f,g)).$$

This parameter can be expressed by means of the Walsh transform. Let $x = (x_1, \ldots, x_n)$ and $a = (a_1, \ldots, a_n)$ both belonging to F_2^n and $x \cdot a = x_1 a_1 + \ldots + x_n a_n$. Let $f(x)$ be a Boolean function on n variables. Then the *Walsh transform* of $f(x)$ is an integer valued function over F_2^n which is defined as

$$W_f(a) = \sum_{x \in F_2^n} (-1)^{f(x) + x \cdot a}.$$

A Boolean function f is balanced if and only if $W_f(0) = 0$. The nonlinearity of f is given by $nl(f) = 2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} |W_f(a)|$.

Any Boolean function should have also high algebraic degree to be cryptographically secure [22]. In fact, it must keep high degree even if a few output bits are modified. In other words, it must have high nonlinearity profile [12].

Another notion plays a role for the combiner model. A function is m-resilient (respectively m-th order correlation immune) if and only if its Walsh transform satisfies $W_f(a) = 0$, for $0 \leq wt(a) \leq m$ (respectively $1 \leq wt(a) \leq m$). Any combining function should be highly resilient to withstand correlation attacks [30].

Recently, it has been identified that any combining or filtering function should not have a low degree multiple. More precisely, it is shown in [18] that, given any n-variable Boolean function f, it is always possible to get a Boolean function g with degree at most $\lceil \frac{n}{2} \rceil$ such that $f * g$ has degree at most $\lceil \frac{n}{2} \rceil$. While choosing a function f, the cryptosystem designer should avoid that the degree of $f * g$ falls much below $\lceil \frac{n}{2} \rceil$ with a nonzero function g whose degree is also much below $\lceil \frac{n}{2} \rceil$. Indeed, otherwise, resulting low degree multivariate relations involving key/state bits and output bits of the combining or filtering function f allow a very efficient attack [18]. In fact, as observed in [27], it is enough to check that f and $f+1$ do not admit nonzero annihilators of such low degrees.

Definition 1 *Given $f \in B_n$, define $AN(f) = \{g \in B_n | \ f * g = 0\}$. Any function $g \in AN(f)$ is called an annihilator of f.*

To check that a function has good algebraic immunity, it is necessary and sufficient to check that f and $f+1$ do not admit nonzero annihilators of low degrees. Indeed, if f or $f+1$ has an annihilator g of low degree d, then $f*g$ either is null or equals g and therefore has degree at most d; conversely, if we have $f * g = h$ where $g \neq 0$ and where g and h have degrees at most d, then either $g = h$, and then g is an annihilator of $f + 1$, or $g \neq h$, and we have then $f * g = h * g$ by multiplying both terms of the equality $f * g = h$ by g, which proves that $f * (g + h) = 0$ and shows that $g + h$ is a nonzero annihilator of f of degree at most d.

Definition 2 *Given $f \in B_n$, the algebraic immunity of f is the minimum degree of all nonzero annihilators of f or $f+1$. We denote it by $AI(f)$.*

Note that $AI(f) \leq \deg(f)$, since $f * (1 + f) = 0$. Note also that the algebraic immunity and the degree, as well as the nonlinearity, are affine invariant (i.e. are invariant under composition by an affine automorphism). Because of the observation made in [18] and recalled above, we have $AI(f) \leq \lceil \frac{n}{2} \rceil$.

If a function has optimal algebraic immunity $\lceil n/2 \rceil$ with n odd, then it is balanced. If it has low nonlinearity, then it must have a low value of $AI(f)$, whatever is n (see [13]). This implies that if one chooses a function with good value of $AI(f)$, this will automatically provide a nonlinearity which is not low. However, it does not assure that the nonlinearity is very high. Hence, the algebraic immunity property takes care of three fundamental properties of a Boolean function, balancedness, algebraic degree and nonlinearity (and more generally nonlinearity profile, see [12]), but it does this incompletely in the case of nonlinearity (and also in the case of balancedness when n is even).

As shown in [3, 15, 8, 2], a high algebraic immunity is a necessary but not sufficient condition for robustness against all kinds of algebraic attacks. Indeed, suppose that one can find g of low degree and $h \neq 0$ such that $f * g = h$, then, even if h has not low degree, a fast algebraic attack is feasible if the degree of h is not too high, see [15, 5, 24]. This has been exploited in [16] to present an attack on SFINKS [7]. Since $f * g = h$ implies $f * h = f * f * g = f * g = h$, we see that h is then an annihilator of $f + 1$ and its degree is then at least equal to the algebraic immunity of f. This means that having high algebraic immunity is not a property that allows resisting all kinds of algebraic attacks, but that it is a necessary condition for a resistance to fast algebraic attacks as well.

3 The general method

The idea of our method is simple but efficient. We use the fact that, if a function has degree strictly less than k and if it is null on a flat of dimension at least k, except maybe at one vector of this flat, then it must be null on the whole flat. We can exploit this idea for the annihilators of f and $f + 1$: to show that f has no nonzero annihilator of degree strictly less than k, we can try to exhibit a sequence of flats of dimensions at least k, such that each of them contains at most one vector lying outside the support of f and outside all those flats which come previously in the sequence (if any), and such that with such vectors, we cover all the complement of the support of f. This leads to the following:

Proposition 1 *Let k be any positive integer such that $k \leq \lceil n/2 \rceil$. A sufficient condition for a function f to have no non-zero annihilator of degree strictly less than k is that there exists a sequence of flats (i.e. of affine subspaces of F_2^n) $(A_i)_{1 \leq i \leq r}$ of dimensions at least k, such that:*

$$\forall i \leq r,\ card(A_i \setminus [supp(f) \cup \bigcup_{i' < i} A_{i'}]) \leq 1 \quad (1)$$

$$F_2^n \setminus supp(f) \subseteq \bigcup_{i \leq r} A_i. \quad (2)$$

Proof: Relation (1) allows proving by induction on i that any annihilator g of degree at most $k-1$ of f is null on A_i for every i, since we know that, for every flat A of dimension at least k, we have $\sum_{x \in A} g(x) = 0$. Then (2) shows that g must be null on F_2^n. □

We obtain by applying Proposition 1 to f and to $f+1$ (exhibiting a sequence of flats $(A_i)_{1 \leq i \leq r}$ for f and a sequence of flats $(A'_i)_{1 \leq i \leq r}$ for $f + 1$) a sub-class of the class of functions with algebraic immunity at least k. We do not know if this sub-class is in fact the whole class and we leave it as an *open problem.* Note that both classes are affine invariant.

Example 1 The simplest known example of a function with optimal algebraic immunity (whatever is n) is the *majority function*, which takes value 1 at all vectors of weights at least $n/2$ (that is, at least $\lceil n/2 \rceil$) and 0 at all the other

vectors[2]. For instance, let us take $n = 5$. The support of the majority function is then the set of vectors of weights at least 3. We consider an annihilator of degree at most 2. By hypothesis, it is null at every vector of weight at least 3. We look for a sequence of flats A_i of dimensions at least 3 and such that, at each step, it contains exactly one new vector of weight at most 2, and which covers the set of all vectors of weights at most 2. We can take the set of all flats of the form $\{x \in F_2^n / supp(a) \subseteq supp(x)\}$ where a has weight at most 2 and where the order on the a's is by decreasing weights (whatever is the order for a fixed weight). By induction we see that the annihilator is also null at every vector of weight at most 2 and therefore is trivial. We look also for a sequence of flats A'_j of dimension at least 3 and such that, at each step, it contains exactly one new vector of weight at least 3, and which covers the set of all vectors of weight at least 3. We can take the set of all vector spaces of the form $\{x \in F_2^n / supp(x) \subseteq supp(a)\}$ where a has weight at least 3 and where the order on the a's is by increasing weights.
In the general case, we can take for the A'_j's the vector spaces $\{x \in F_2^n /\, supp(x) \subseteq supp(a)\}$ where a ranges over the set of vectors of weights at least $k = \lceil n/2 \rceil$, the order being by increasing weights (with any order for vectors of the same weight), and for the A_i's the flats $\{x \in F_2^n /\, supp(a) \subseteq supp(x)\}$ where a ranges over the set of vectors of weights at most $n - k$, the order being by decreasing weights. Then, for every i, the set $A_i \setminus \bigcup_{i'<i} A_{i'}$ being a subset of A_i, the set $A_i \setminus [supp(f) \cup \bigcup_{i'<i} A_{i'}]$ is a singleton if A_i has dimension $n - k$, and otherwise $A_i \setminus \bigcup_{i'<i} A_{i'}$ equals the singleton containing the vector of minimum weight in A_i. Similarly, for every j, the set $A'_j \setminus \bigcup_{j'<j} A'_{j'}$ being a subset of A'_j, the set $A'_j \setminus [supp(f+1) \cup \bigcup_{j'<j} A'_{j'}]$ is a singleton if A'_j has dimension k, and otherwise, $A'_j \setminus \bigcup_{j'<j} A'_{j'}$ equals the singleton containing the vector of maximum weight in A'_j. □

Remark 1 The flats in Example 1 are the simplest possible ones that can be used in Proposition 1: the flats A'_i are the vector spaces of equations $x_j = 0$ (where j ranges over a set depending on i and of size at most $\lfloor n/2 \rfloor$) and the flats A_i are their translates by the vector $(1, \ldots, 1)$. □

Open problems:
1. Find an example of application of Proposition 1 to a function f (resp. to the function $f+1$) in which some flats A_i (resp. A'_i) are vector spaces and some are not, and which leads to a function affinely inequivalent to the majority function.
2. Find an example of application of Proposition 1 in which some of the flats A_i and A'_i have equations of the form $x_j + x_k = \epsilon$ ($\epsilon \in F_2$) and which is not affinely equivalent to functions related through Proposition 1 to flats of equations $x_j = \epsilon$. Note that, more generally, the A_i's can be chosen as the cosets of the kernels of linear mappings $\phi : F_2^n \to F_2^m$ where $m \leq \lfloor n/2 \rfloor$; for instance,

[2]Another possible choice of a majority function, which has been considered in [20], takes value 1 at all vectors of weights strictly greater than $n/2$; when n is even, this gives a function which is different, but which equals $f(x + (1, \ldots, 1)) + 1$ where f is the majority function considered here; this alternate majority function is therefore affine equivalent to $f + 1$.

using the structure of the field F_{2^n}, some of the flats A_i, A'_j could have equations $tr_{n/m}(ax) = b$, where $m \geq 2$ is a divisor of n, $tr_{n/m}(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}$, $a \in F_{2^n}$ and $b \in F_{2^m}$. $\square$

4 Constructing functions with optimum algebraic immunity, in odd numbers of variables

In [1], A. Canteaut has observed that, if a balanced function f in an odd number n of variables admits no non-zero annihilator of degree at most $\frac{n-1}{2}$, then it has optimum algebraic immunity $\frac{n+1}{2}$ (this means that we do not need to check also that $f+1$ has no non-zero annihilator of degree at most $\frac{n-1}{2}$ for showing that f has optimum algebraic immunity). For self-completeness, let us recall the reasons why this is true. Consider the Reed-Muller code of length 2^n and of order $\frac{n-1}{2}$. This code is self-dual (i.e. is its own dual) [26]. Let G be a generator matrix of this code. Each column of G is labeled by a vector of F_2^n. Saying that f has no non-zero annihilator of degree at most $\frac{n-1}{2}$ is equivalent to saying that the matrix obtained by selecting those columns of G corresponding to the elements of the support of f has full rank $\sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i} = 2^{n-1}$. Since f has weight 2^{n-1}, this is also equivalent to saying that the support of the function is an information set, that is (assuming for simplicity that the columns corresponding to the support of f are the 2^{n-1} first ones), that we can take $G = (Id \,|\, M)$. Then the complement of the support of f is also an information set (otherwise there would exist a vector $(z \,|\, 0)$, $z \neq 0$, in the code and this is clearly impossible since G is also a parity-check matrix of the code).

This simplifaction in the research of functions with optimum algebraic immunity leads to the following algorithm:

Algorithm

1. For i from 1 to 2^{n-1}:
   - choose an $\frac{n+1}{2}$-dimensional flat A_i such that the set $A_i \setminus [\bigcup_{i'<i} A_{i'}]$ is non-empty and has minimum size among all $\frac{n+1}{2}$-dimensional flats having this property;
   - choose a vector a_i in $A_i \setminus [\bigcup_{i'<i} A_{i'}]$;
2. Output the function whose support equals $\{a_i,\, 1 \leq i \leq 2^{n-1}\}$.

If, for 2^{n-1} times, we can apply step 1, then we end up with a balanced function with optimum algebraic immunity, according to Proposition 1 and to Canteaut's result. The condition that the set $A_i \setminus [\bigcup_{i'<i} A_{i'}]$ has minimum size optimizes the probability that this can be possible.

5 Constructing functions with optimum algebraic immunity, in even numbers of variables

Note that, if the support S of a function (in any number of variables) satisfying the hypotheses of Proposition 1 contains a k-dimensional flat A (resp. is disjoint of a k-dimensional flat A), then if we take off one vector belonging to A from S (resp. if we include such vector in S), we obtain a function which still satisfies the hypotheses of Proposition 1: we can consider this flat as being the first item of the sequence of the A_i's (resp. the A'_i's) and shift all the other flats in the same sequence (r, resp. s, being increased by 1). This can be applied iteratively. In the case that n is even, this implies that the method of Proposition 1 illustrated in Example 1 works more generally for any function taking value 0 at all vectors of weights strictly smaller than $n/2$ and value 1 at all vectors of weights strictly greater than $n/2$, whatever are its values at the vectors of weight $n/2$.

Corollary 1 *Let f be any function in an even number of variables n, such that $f(x) = 0$ if $wt(x) < n/2$ and $f(x) = 1$ if $wt(x) > n/2$ (or conversely). Then f has optimum algebraic immunity $n/2$.*

Remark 2 A similar result has been independently obtained in [4] and is complementary of ours. The functions obtained there are those of Corollary 1 above, such that the set of vectors of weight $n/2$ in their support is stable under translation by $(1, \ldots, 1)$. They satisfy then a somewhat stronger condition and are potentially more robust against algebraic attacks. Note that they all have the property that $f(x + (1, \ldots, 1)) = f(x) + 1$ if $wt(x) \neq n/2$ and $f(x + (1, \ldots, 1)) = f(x)$ if $wt(x) = n/2$. This looks like a linear structure (a function f has the linear structure a if $f(x + a)$ equals $f(x)$ plus a constant, see [23, 11]) though it is different; it may however be a weakness. □

Some of the functions of Corollary 1 are balanced. We show in Section 6 that these functions cannot have good nonlinearities.
These functions are not symmetric, but they are almost symmetric in the sense that their outputs vary, for a given fixed weight, only when this weight is $n/2$. This may be a weakness (see [2]). We shall give below further examples which do not present such almost symmetry.

In the case that n is even, it has been observed in [9] that the function equal to the majority function for input vectors of weights at most $n - 1$ and null at the vector of weight n has optimum algebraic immunity. This is quite obvious with Proposition 1: we can take the same flats A_i and A'_j as for the majority function, since A_1 contains the vector of weight n and vectors of weights between $n/2$ and $n - 1$, that is, belonging to the support of the function.
In fact, a much more general result can be stated.

Corollary 2 *Let n be even and let $a^1, \ldots, a^{\binom{n}{n/2}}$ be an ordering of the set of all vectors of weight $n/2$ in F_2^n. For every $i \in \left\{1, \ldots, \binom{n}{n/2}\right\}$, let us denote by A_i the flat $\{x \in F_2^n / \, supp(a^i) \subseteq supp(x)\}$ and by A'_i the vector space*

$\{x \in F_2^n / \, supp(x) \subseteq supp(a^i)\}$. Let I, J and K be three disjoint subsets of $\left\{1, \ldots, \binom{n}{n/2}\right\}$. Assume that, for every $i \in I$, there exists a vector $b^i \neq a^i$ such that $b^i \in A_i \setminus \bigcup_{i' \in I; i' < i} A_{i'}$. Assume that, for every $i \in J$, there exists a vector $c^i \neq a^i$ such that $c^i \in A'_i \setminus \bigcup_{i' \in J; i' < i} A'_{i'}$. Then the function whose support equals:

$$\{x \in F_2^n / \, wt(x) > n/2\} \cup \{c^i, \, i \in J\} \cup \{a^i, \, i \in I \cup K\} \setminus \{b^i, \, i \in I\}$$

has algebraic immunity $n/2$.

Proof: Let the sequence of the flats A_i of Proposition 1 begin with the flats A_i described above for $i \in I$ and be completed by all the other flats $\{x \in F_2^n / \, supp(a) \subseteq supp(x)\}$, ordered by decreasing weights of the vectors a of weights at most $n/2$. Let the sequence of the flats A'_i begin with the vector spaces A'_i described above for $i \in J$ and be completed by all the other vector spaces $\{x \in F_2^n / \, supp(x) \subseteq supp(a)$ ordered by increasing weights of the vectors a of weights at least $n/2$. Then, as for Example 1, the hypotheses of Proposition 1 are satisfied. The only differences with Example 1 are that, for any $i \in I$, the set $A_i \setminus [supp(f) \cup \bigcup_{i' < i} A_{i'}]$ equals $\{b_i\}$ and for any $i \in J$, the set $A'_i \setminus [supp(f+1) \cup \bigcup_{i' < i} A'_{i'}]$ equals $\{c_i\}$. □

An alternate way of presenting the construction of Corollary 2 is, after choosing an ordering of the set of vectors of weight $n/2$ in F_2^n and two disjoint subsets I, J of $\left\{1, \ldots, \binom{n}{n/2}\right\}$, allow $b^i \in A_i$, $i \in I$ (resp. $c^i \in A'_i$, $i \in J$) to have also weight $n/2$ (that is, to be equal to a^i). The support of the constructed function equals then the union of $\{x \in F_2^n / \, wt(x) > n/2\} \cup \{c^i, \, i \in J\} \setminus \{b^i, \, i \in I\}$ and of a set of vectors of weight $n/2$, including all the vectors a^i such that b^i has not weight $n/2$ and excluding all those such that c^i has not weight $n/2$. Note that, whatever is the ordering of the set of vectors of weight $n/2$ in F_2^n, there is then, at each step, a possible choice of the vectors b^i and c^i since in any case choosing $b^i = a^i$ and $c^i = a^i$ satisfies the condition that $b^i \in A_i \setminus \bigcup_{i' \in I; i' < i} A_{i'}$ (resp. $c^i \in A'_i \setminus \bigcup_{i' \in J; i' < i} A'_{i'}$). Hence, this viewpoint leads to an algorithm for constructing (possibly balanced) functions in even number n of variables with algebraic immunity $n/2$:

Algorithm

- Choose two positive integers $k \leq l \leq \binom{n}{n/2}$;
- For i ranging from 1 to k, choose a vector a^i of weight $n/2$, different from $a^1, \ldots, a^{i-1}$, and a vector b^i such that $supp(a^i) \subseteq supp(b^i)$ and $\forall i' < i$, $supp(a'^i) \not\subseteq supp(b^i)$;
- For i ranging from $k+1$ to l, choose a vector a^i of weight $n/2$, different from $a^1, \ldots, a^{i-1}$, and a vector c^i such that $supp(c^i) \subseteq supp(a^i)$ and $\forall k+1 \leq i' < i$, $supp(c^i) \not\subseteq supp(a'^i)$;

- Output the function whose support equals $\{x \in F_2^n / \, wt(x) > n/2\} \setminus \{b^i, \, i = 1, \ldots, k\} \cup \{a^i, \, i = 1, \ldots, k\} \cup \{c^i, \, i = k+1, \ldots, l\}$.

The weight of the function equals $2^{n-1} - \frac{1}{2}\binom{n}{n/2}$, plus the number of b^i of weight $n/2$, plus $l - k$.
The number of functions with optimal algebraic immunity that we can obtain this way is difficult to evaluate, but it seems large. It is upper bounded by $\left(2^{1+n/2}\right)^{\binom{n}{n/2}}$, but this upper bound is approximately in $\Omega\left(2^{\frac{\sqrt{n}}{\sqrt{2\pi}}2^{n/2}}\right)$, and is therefore asymptotically huge. Note that it is easy to produce balanced functions with this method.

In [9] is asserted that the function whose support equals the union of the set of vectors of weight $n/2 - 4$ and of the set of vectors of weights at least $n/2$ except those of weight $n/2 + 4$ has optimum algebraic immunity. This result is probably false (see a correct version in [6]), but it is true up to some (even) value of n which has to be determined. We give now an example of an infinite class of functions, among which some differ slightly from the function just mentioned, and for which we can prove that the algebraic immunity equals $n/2$, thanks to Corollary 2. In this example, the ordering on the set of vectors of weight $n/2$ plays no role.

Corollary 3 *Let n be even and let u be any nonzero vector of weight less than $n/2$ in F_2^n. Let f be any function whose support contains:*
1. all vectors of weights strictly greater than $n/2$, except those of weight $wt(u) + n/2$ and whose supports contain the support of u,
2. all vectors of weight $n/2 - wt(u)$ and whose supports are disjoint of the support of u,
3. all vectors of weight $n/2$ and whose supports are disjoint of the support of u,
4. any additional vectors of weight $n/2$ and whose supports neither are disjoint of the support of u nor contain it.
Then f has algebraic immunity $n/2$.

Proof: For every vector a of weight $n/2$ and whose support is disjoint of the support of u, let $b_a = a \vee u$ be the vector whose support equals the union of those of a and u. Obviously, b_a has weight $wt(u) + n/2$ and its support contains the support of u. For every vector a of weight $n/2$ and whose support contains the support of u, let $c_a = a \setminus u$ be the vector whose support equals the difference between those of a and u. Obviously, c_a has weight $n/2 - wt(u)$ and its support is disjoint of the support of u. For two distinct vectors a and a' of weight $n/2$ and whose supports are disjoint of the support of u, we have $supp(a') \not\subseteq supp(b_a)$, and for two distinct vectors a and a' of weight $n/2$ and whose supports contain the support of u, we have $supp(c_a) \not\subseteq supp(a')$. Corollary 2, applied with $A_i = \{x \in F_2^n / \, supp(a^i) \subseteq supp(x)\}$, where a^i is the i-th vector of weight $n/2$ in some predetermined order (any order will work), $A'_i = \{x \in F_2^n / \, supp(x) \subseteq supp(a^i)\}$, $b^i = a^i \vee u$, $c^i = a^i \setminus u$, and taking for I the indices of those vectors a^i whose supports are disjoint of the support of u, for J the indices of those vectors a^i whose supports contain the support of u, and for K the indices of some extra vectors a^i, proves then that f has algebraic immunity $n/2$. □

Notation: We shall denote by f_L the function described in Corollary 1, where L is the set of those vectors of weight $n/2$ at which f_L takes value 1, and by $f_{u,L}$ the function described in Corollary 3, where L is the set of those vectors of weight $n/2$, whose supports neither are disjoint of the support of u nor contain it, and at which $f_{u,L}$ takes value 1.

Note that $f_{u,L}$ is not symmetric (it is "less" symmetric than f_L, in the sense that its distance to symmetric functions is greater). It can be balanced too:

Lemma 1 *For every nonzero vector u of weight less than $n/2$ and every subset L of the set of those vectors of weight $n/2$, whose supports neither are disjoint of the support of u nor contain it, the weight of function $f_{u,L}$ equals $2^{n-1}-\frac{1}{2}\binom{n}{n/2}+\binom{n-wt(u)}{n/2}+|L|$. Hence, $f_{u,L}$ is balanced if and only if $|L|=\frac{1}{2}\binom{n}{n/2}-\binom{n-wt(u)}{n/2}$. Given $u\neq 0$, there always exists such L.*

Proof: The number of those vectors corresponding to case 1 in Corollary 3 equals $\sum_{i=1+n/2}^{n}\binom{n}{i}-\binom{n-wt(u)}{n/2}=2^{n-1}-\frac{1}{2}\binom{n}{i}-\binom{n-wt(u)}{n/2}$; the number of those corresponding to case 2 equals $\binom{n-wt(u)}{n/2-wt(u)}=\binom{n-wt(u)}{n/2}$ and the number of those corresponding to case 3 equals this same number. Hence, the number of those corresponding to cases 1-3 equals $2^{n-1}-\frac{1}{2}\binom{n}{n/2}+\binom{n-wt(u)}{n/2}$. The number $|L|$ of those vectors corresponding to case 4 in Corollary 3 can be any non-negative number upper bounded by $\binom{n}{n/2}-\binom{n-wt(u)}{n/2}-\binom{n-wt(u)}{n/2-wt(u)}=\binom{n}{n/2}-2\binom{n-wt(u)}{n/2}$. Hence, a necessary and sufficient condition for the existence of a balanced function $f_{u,L}$ is that $\frac{1}{2}\binom{n}{n/2}-\binom{n-wt(u)}{n/2}\geq 0$ since we have then $\frac{1}{2}\binom{n}{n/2}-\binom{n-wt(u)}{n/2}\leq\binom{n}{n/2}-2\binom{n-wt(u)}{n/2}$. And this condition is satisfied since $\frac{1}{2}\binom{n}{n/2}=\binom{n-1}{n/2}$. □

6 Study of the Walsh transforms of the constructed functions

We study now the Walsh spectra of the functions f_L and $f_{u,L}$. In Appendix, we determine the Walsh spectrum of the majority function f (only its nonlinearity was investigated in [20]). The following lemma is obvious.

Lemma 2 *Let L be any set of vectors of weight $n/2$. Let f_L be the function in an even number of variables n whose support equals the union of the set $\{x\in F_2^n \,/\, wt(x)>n/2\}$ and of L (see Corollary 1). Let a be any vector and let $i=wt(a)$. Then*

$$W_{f_L}(a)=(-1)^{i+1}W_f(a)-2\sum_{x\in L}(-1)^{a\cdot x}$$

where f is the majority function (whose support equals $\{x \in F_2^n \,/\, wt(x) \geq n/2\}$).

We can see now that all functions f_L have bad nonlinearities. Indeed, according to [20], we know that the maximum of $|W_f(a)|$ is achieved when a has weight 1, that is, $nl(f) = 2^{n-1} - \frac{1}{2}|W_f(a)|$ with $wt(a) = 1$. We have, for every vector a of weight 1: $W_f(a) = -(n/2+1)\left(\binom{n-1}{n/2+1} - \binom{n-1}{n/2}\right) = 2\binom{n-1}{n/2}$, according to [20] or to Lemma 4 (see Appendix). We also have $\sum_{wt(a)=1}\sum_{x\in L}(-1)^{a\cdot x} = \sum_{x\in L}(n - 2w_H(x)) = 0$. Hence, there exists at least one vector a of weight 1 such that $\sum_{x\in L}(-1)^{a\cdot x} < 0$ and the nonlinearity of f_L is worse than the nonlinearity of f.

Lemma 3 *Let u be any nonzero vector of weight less than $n/2$ and L any set of vectors of weight $n/2$ whose supports neither are disjoint of the support of u nor contain it. Let $f_{u,L}$ be the function described in Corollary 3. Let a be any vector and let $i = wt(a)$. Then:*
- if i is even, then $W_{f_{u,L}}(a)$ equals

$$(-1)^{i+1}W_f(a) - 2\sum_{\substack{x\in F_2^n/wt(x)=n/2\\ supp(u)\cap supp(x)=\emptyset}}(-1)^{a\cdot x} - 2\sum_{x\in L}(-1)^{a\cdot x},$$

- if $i = wt(a)$ is odd and $a\cdot u = 0$, then it equals

$$(-1)^{i+1}W_f(a) + 2\sum_{\substack{x\in F_2^n/wt(x)=n/2\\ supp(u)\cap supp(x)=\emptyset}}(-1)^{a\cdot x} - 2\sum_{x\in L}(-1)^{a\cdot x},$$

- if $i = wt(a)$ is odd and $a\cdot u = 1$, then it equals

$$(-1)^{i+1}W_f(a) - 6\sum_{\substack{x\in F_2^n/wt(x)=n/2\\ supp(u)\cap supp(x)=\emptyset}}(-1)^{a\cdot x} - 2\sum_{x\in L}(-1)^{a\cdot x}.$$

Proof: The value at $a \in F_2^n$ of the Walsh transform of the indicator of vectors of weights strictly greater than $n/2$ being equal to $(-1)^{i+1}W_f(a)$, where $i = wt(a)$, the Walsh transform of $f_{u,L}$ equals

$$\begin{aligned}
& (-1)^{i+1}W_f(a) + 2\sum_{\substack{x\in F_2^n/wt(x)=n/2+wt(u)\\ supp(u)\subseteq supp(x)}}(-1)^{a\cdot x}\\
& -2\sum_{\substack{x\in F_2^n/wt(x)=n/2-wt(u)\\ supp(u)\cap supp(x)=\emptyset}}(-1)^{a\cdot x} - 2\sum_{\substack{x\in F_2^n/wt(x)=n/2\\ supp(u)\cap supp(x)=\emptyset}}(-1)^{a\cdot x} - 2\sum_{x\in L}(-1)^{a\cdot x}\\
= \; & (-1)^{i+1}W_f(a) + 2\sum_{\substack{x\in F_2^n/wt(x)=n/2\\ supp(u)\cap supp(x)=\emptyset}}\left[(-1)^{a\cdot(x+u)} - (-1)^{a\cdot(\overline{x}+u)} - (-1)^{a\cdot x}\right]\\
& -2\sum_{x\in L}(-1)^{a\cdot x},
\end{aligned}$$

where $\overline{x} = x + (1, \ldots, 1)$. Indeed, for every vector $x \in F_2^n$, the condition ($wt(x) = n/2 + wt(u)$ and $supp(u) \subseteq supp(x)$) is equivalent to ($wt(x+u) = n/2$ and $supp(u) \cap supp(x+u) = \emptyset$) and the condition ($wt(x) = n/2 - wt(u)$ and $supp(u) \cap supp(x) = \emptyset$) is equivalent to ($wt(\overline{x}) = n/2 + wt(u)$ and $supp(u) \subseteq supp(\overline{x})$).
If $wt(a)$ is even, then we have $(-1)^{a\cdot(x+u)} - (-1)^{a\cdot(\overline{x}+u)} - (-1)^{a\cdot x} = -(-1)^{a\cdot x}$. If $wt(a)$ is odd, then we have $(-1)^{a\cdot(x+u)} - (-1)^{a\cdot(\overline{x}+u)} - (-1)^{a\cdot x} = 2(-1)^{a\cdot(x+u)} - (-1)^{a\cdot x}$. And if $a \cdot u = 0$, then we have $2(-1)^{a\cdot(x+u)} - (-1)^{a\cdot x} = (-1)^{a\cdot x}$; if $a \cdot u = 1$, then we have $2(-1)^{a\cdot(x+u)} - (-1)^{a\cdot x} = -3(-1)^{a\cdot x}$. This completes the proof. □

Note that the argument used for proving that the functions f_L have bad nonlinearities does not show that the functions $f_{u,L}$ cannot have good nonlinearities either: for every reals λ and μ, we have

$$\sum_{i=0}^{n}\left[\lambda \sum_{\substack{x\in F_2^n/wt(x)=n/2\\ supp(u)\cap supp(x)=\emptyset}} (-1)^{a\cdot x} + \mu \sum_{x\in L}(-1)^{a\cdot x}\right] =$$

$$\lambda \sum_{\substack{x\in F_2^n/wt(x)=n/2\\ supp(u)\cap supp(x)=\emptyset}} (n - 2w_H(x)) + \mu \sum_{x\in L}(n - 2w_H(x)) = 0.$$

Hence, there exists at least one vector a of weight 1 such that the number $\lambda \sum_{\substack{x\in F_2^n/wt(x)=n/2\\ supp(u)\cap supp(x)=\emptyset}} (-1)^{a\cdot x} + \mu \sum_{x\in L}(-1)^{a\cdot x}$ is negative. But in the formulae of Lemma 3, the values of λ and μ differ according to whether $a \cdot u$ is null or not.

We leave as an *open problem* the difficult question of determining whether some of the balanced functions $f_{u,L}$ can achieve high nonlinearities and be robust against fast algebraic attacks.

References

[1] A. Canteaut. Open problems related to algebraic attacks on stream ciphers. Workshop on Coding and Cryptography 2005. Lecture Notes in Computer Science 3969 (to appear). Paper available on the web http://www-rocq.inria.fr/codes/Anne.Canteaut/Publications/canteaut06a.pdf

[2] F. Armknecht, C. Carlet, P. Gaborit, S. Kuenzli, W. Meier and O. Ruatta. Efficient computation of algebraic immunity for algebraic and fast algebraic attacks. To appear in the Proceedings of EUROCRYPT 2006, published by LNCS.

[3] F. Armknecht and M. Krause. Algebraic Attacks on combiners with memory. In *Advances in Cryptology - CRYPTO 2003*, number 2729 in Lecture Notes in Computer Science, pp. 162–175. Springer Verlag, 2003.

[4] F. Armknecht and M. Krause. Constructing single- and multi-output boolean functions with maximal immunity. To appear in the Proceedings of *ICALP 2006*, Lecture Notes of Computer Science, Springer.

[5] F. Armknecht. Improving Fast Algebraic Attacks. In *FSE 2004*, number 3017 in Lecture Notes in Computer Science, pp. 65–82. Springer Verlag, 2004.

[6] A. Braeken. Cryptographic properties of Boolean functions and S-boxes. PhD thesis available at URL http://homes.esat.kuleuven.be/ abraeken/thesisAn.pdf.

[7] A. Braeken, J. Lano, N. Mentens, B. Preneel and I. Verbauwhede. SFINKS: A Synchronous stream cipher for restricted hardware environments. SKEW - Symmetric Key Encryption Workshop, 2005.

[8] A. Braeken, J. Lano and B. Preneel. Evaluating the Resistance of Filters and Combiners Against Fast Algebraic Attacks. Eprint on ECRYPT, 2005.

[9] A. Braeken and B. Preneel. On the Algebraic Immunity of Symmetric Boolean Functions. In *Indocrypt 2005*, number 3797 in LNCS, pp. 35–48. Springer Verlag, 2005. Also available at Cryptology ePrint Archive, http://eprint.iacr.org/, No. 2005/245, 26 July, 2005.

[10] A. Canteaut and M. Trabbia. Improved fast correlation attacks using parity-check equations of weight 4 and 5. In *EUROCRYPT 2000*, number 1807 in Lecture Notes in Computer Science, pp. 573–588. Springer Verlag, 2000.

[11] C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, to appear in 2006. Prelimnary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html

[12] C. Carlet. On the higher order nonlinearities of algebraic immune functions. To appear in the proceedings of CRYPTO 2006.

[13] C. Carlet, D. Dalai, K. Gupta and S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. To appear in IEEE Transactions on Information Theory.

[14] J. Y. Cho and J. Pieprzyk. Algebraic Attacks on SOBER-t32 and SOBER-128. In *FSE 2004*, number 3017 in Lecture Notes in Computer Science, pp. 49–64. Springer Verlag, 2004.

[15] N. Courtois. Fast algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology - CRYPTO 2003*, number 2729 in Lecture Notes in Computer Science, pp. 176–194. Springer Verlag, 2003.

[16] N. Courtois. Cryptanalysis of SFINKS. In *ICISC 2005*. Also available at Cryptology ePrint Archive, http://eprint.iacr.org/, Report 2005/243, 2005.

[17] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In *Advances in Cryptology - ASIACRYPT 2002*, number 2501 in Lecture Notes in Computer Science, pp. 267–287. Springer Verlag, 2002.

[18] N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. In *Advances in Cryptology - EUROCRYPT 2003*, number 2656 in Lecture Notes in Computer Science, pp. 345–359. Springer Verlag, 2003.

[19] D. K. Dalai, K. C. Gupta and S. Maitra. Cryptographically Significant Boolean functions: Construction and Analysis in terms of Algebraic Immunity. In *Workshop on Fast Software Encryption, FSE 2005*, pp. 98–111, number 3557, Lecture Notes in Computer Science, Springer-Verlag.

[20] D. K. Dalai, S. Maitra and S. Sarkar. Basic Theory in Construction of Boolean Functions with Maximum Possible Annihilator Immunity. Cryptology ePrint Archive, http://eprint.iacr.org/, No. 2005/229, 15 July, 2005. To be published in Designs, Codes and Cryptography.

[21] D. K. Dalai, K. C. Gupta and S. Maitra. Notion of Algebraic Immunity and Its evaluation Related to Fast Algebraic Attacks. In *2nd International Workshop on Boolean Functions: Cryptography and Applications, BFCA 2006*, University of Rouen, France, March 13-15, 2006. Cryptology ePrint Archive, eprint.iacr.org, Report 2006/018, January 2006.

[22] C. Ding, G. Xiao, and W. Shan. *The Stability Theory of Stream Ciphers*. Number 561 in Lecture Notes in Computer Science. Springer-Verlag, 1991.

[23] J. H. Evertse. Linear structures in block ciphers. In *Advances in Cryptology - EUROCRYPT' 87*, no. 304 in Lecture Notes in Computer Science, Springer Verlag, pp. 249-266, 1988.

[24] P. Hawkes and G. G. Rose. Rewriting Variables: The Complexity of Fast Algebraic Attacks on Stream Ciphers. In M. K. Franklin, editor, *Advances in Cryptology - CRYPTO 2004, LNCS 3152*, pp. 390–406. Springer Verlag, 2004.

[25] D. H. Lee, J. Kim, J. Hong, J. W. Han and D. Moon. Algebraic Attacks on Summation Generators. In *FSE 2004*, number 3017 in Lecture Notes in Computer Science, pp. 34–48. Springer Verlag, 2004.

[26] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*, Elsevier, North-Holland, 1977.

[27] W. Meier, E. Pasalic and C. Carlet. Algebraic attacks and decomposition of Boolean functions. In *Advances in Cryptology - EUROCRYPT 2004*, number 3027 in Lecture Notes in Computer Science, pp. 474–491. Springer Verlag, 2004.

[28] A. F. Nikiforov and V. B. Uvarov and S. S. Suskov. Classic Orthogonal Polynomials of a Discrete Variable. New-York, Springer-Verlag, 1992.

[29] C.E. Shannon. Communication theory of secrecy systems. *Bell system technical journal*, 28, pp. 656-715, 1949.

[30] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, September 1984.

Appendix:

Lemma 4 *Let n be even. Set $\omega = e^{4\pi\sqrt{-1}/n}$ and $\omega' = e^{4\pi\sqrt{-1}/(n+2)}$. The Walsh transform of the majority function f equals, if $wt(a)$ is even:*

$$\begin{aligned} W_f(a) &= -\sum_{j=0}^{\min(wt(a),n/2)} (-1)^j \binom{wt(a)}{j}\binom{n-wt(a)}{n/2-j} \\ &= 2-\frac{2}{n}\sum_{j=0}^{n/2-1}(1-\omega^j)^{wt(a)}(1+\omega^j)^{n-wt(a)}; \end{aligned}$$

and if $wt(a)$ is odd:

$$\begin{aligned} W_f(a) &= -\frac{n/2+1}{wt(a)}\sum_{j=0}^{\min(wt(a),n/2+1)} (-1)^j \binom{wt(a)}{j}\binom{n-wt(a)}{n/2+1-j} \\ &= \frac{n/2+1}{wt(a)}-\frac{1}{wt(a)}\sum_{j=0}^{n/2}(1-\omega'^j)^{wt(a)}(1+\omega'^j)^{n-wt(a)}. \end{aligned}$$

Proof: We know that, for every vector a of weight $i \neq 0$, we have

$$W_f(a) = -2\sum_{k=n/2}^{n} K_k(i,n) \tag{3}$$

where K_k is the so-called Krawtchouk polynomial (see [26, Page 151]) defined by

$$K_k(X,n) = \sum_{j=0}^{n}(-1)^j\binom{X}{j}\binom{n-X}{k-j}, \quad k=0,1,\dots n, \tag{4}$$

since it is known that

$$\sum_{wt(x)=k}(-1)^{a\cdot x} = K_k(i,n).$$

The Krawtchouk polynomials can also be defined by means of their generating function [28]: for all integer $i \in \{0,\dots,n\}$ and $z \in \mathbb{C}$,

$$\sum_{k=0}^{n} K_k(i,n)z^k = (1-z)^i(1+z)^{n-i}. \tag{5}$$

• If i is even, then we have $K_{n-k}(i,n) = K_k(i,n)$. Hence we have $W_f(a) = -\sum_{k=0}^{n} K_k(i,n) - K_{n/2}(i,n) = -K_{n/2}(i,n)$ (if $i > 0$), according to Relation (5) applied with $z = 1$. Note that this had been already observed in [20] (the sign was opposite since the majority function considered there was different from the one considered here).
We deduce now an expression which can be easier to use, in some cases. We have $\sum_{j=0}^{n/2-1} \sum_{k=0}^{n} K_k(i,n)\omega^{jk} = \sum_{k=0}^{n} K_k(i,n)(\sum_{j=0}^{n/2-1} \omega^{jk}) = \frac{n}{2}K_0(i,n) + \frac{n}{2}K_n(i,n) + \frac{n}{2}K_{n/2}(i,n) = \frac{n}{2}(2 + K_{n/2}(i,n))$. We deduce, using Relation (5), that $W_f(a) = 2 - \frac{2}{n}\sum_{j=0}^{n/2-1}(1-\omega^j)^i(1+\omega^j)^{n-i}$.

• If i is odd, then the method (that we shall present whatever is the evenness of i) is slightly more complex: we know (see [26, Page 152]) that, for every $k = 0, \ldots, n-2$ and every $i = 0, \ldots, n$ we have:

$$(k+2)K_{k+2}(i,n) - kK_k(i,n) = n[K_{k+1}(i,n) - K_k(i,n)] - 2iK_{k+1}(i,n). \quad (6)$$

Summing up Relation (6) with k ranging from $n/2$ to $n-2$ gives:

$$nK_n(i,n) + (n-1)K_{n-1}(i,n) - (\frac{n}{2}+1)K_{n/2+1}(i,n) - \frac{n}{2}K_{n/2}(i,n) =$$

$$n\left[K_{n-1}(i,n) - K_{n/2}(i,n)\right] - 2i\left[\sum_{k=n/2}^{n} K_k(i,n) - K_n(i,n) - K_{n/2}(i,n)\right].$$

We deduce:

$$\sum_{k=n/2}^{n} K_k(i,n) =$$

$$\frac{n/2+1}{2i}K_{n/2+1}(i,n) + \frac{2i-n/2}{2i}K_{n/2}(i,n) + \frac{2i-n}{2i}K_n(i,n) + \frac{1}{2i}K_{n-1}(i,n) =$$

$$\frac{n/2+1}{2i}K_{n/2+1}(i,n) + \frac{2i-n/2}{2i}K_{n/2}(i,n),$$

using that, for all i, we have $K_0(i,n) = 1, K_1(i,n) = n-2i$ and $K_{n-k}(i,n) = (-1)^i K_k(i,n)$, and therefore $K_n(i,n) = (-1)^i$, $K_{n-1}(i,n) = (-1)^i(n-2i)$. In the case i is even, we checked that we obtain this way the same result as above. Let us consider now the i odd case. We have $K_{n/2}(i,n) = 0$ and we deduce:

$$W_f(a) = -2\sum_{k=n/2}^{n} K_k(i,n) = -\frac{n/2+1}{i}K_{n/2+1}(i,n).$$

We have:
$\sum_{j=0}^{n/2} \sum_{k=0}^{n} K_k(i,n)\omega'^{jk} = \sum_{k=0}^{n} K_k(i,n)(\sum_{j=0}^{n/2} \omega'^{jk}) = (n/2+1)K_0(i,n) + (n/2+1)K_{n/2+1}(i,n) = (n/2+1)(1 + K_{n/2+1}(i,n))$.
We deduce, using Relation (5):
$W_f(a) = \frac{n/2+1}{i} - \frac{1}{i}\sum_{j=0}^{n/2}(1-\omega'^j)^i(1+\omega'^j)^{n-i}$. □

Note that the Walsh spectrum of the function (considered in [20]) which takes value 1 at all vectors of weights strictly greater than $n/2$ equals the opposite of that of f when $wt(a)$ is even and equals that of f when $wt(a)$ is odd.