Cubic Boolean Functions With Highest Resiliency

Claude Carlet and Pascale Charpin

***Abstract*—We classify those cubic m-variable Boolean functions which are $(m-4)$-resilient. We prove that there are four types of such functions, depending on the structure of the support of their Walsh spectra. We are able to determine, for each type, the Walsh spectrum and, then, the nonlinearity of the corresponding functions. We also give the dimension of their linear space. This dimension equals $m-k$ where $k=3$ for the first type, $k=4$ for the second type, $k=5$ for the third type, and $5 \leq k \leq 9$ for the fourth type.**

***Index Terms*—Boolean function, cubic function, Hamming weight, Reed–Muller code, resilient function, stream cipher, symmetric cryptography.**

I. Introduction

CONSTRUCTING *good* Boolean functions, with respect to some cryptographic criteria, is still a crucial challenge nowadays in symmetric cryptography. In particular, the Boolean functions used in stream ciphers must have a high order of resiliency (and a high nonlinearity) to resist some divide-and-conquer attacks; see, e.g., [5]. In this context, a lot of works has currently been devoted to the characteristics of resilient functions (see, for instance, [7], [8], [14]).

On the other hand, each Boolean function on m variables can be identified to some binary codeword of length 2^m. This representation of codewords was intensively used by Kasami *et al.* to show the simple structure of codewords of Reed–Muller codes of low weights [9]–[11].

We present here the classification of cubic functions with highest resiliency, i.e., cubic functions on m variables $(m \geq 4)$ which are $(m-4)$-resilient. (Note that quadratic functions with highest resiliency were already classified in [1].) We show that there are four types of such functions, by applying the results of Kasami *et al.* to the supports of the Walsh spectra of the functions (Corollary 2 and Lemma 4). We characterize precisely these four types, describing for each of them the corresponding Walsh spectrum (Section IV). Then we show that the rank of the Walsh spectrum is generally small, and that *for $m > 9$, any $(m-4)$-resilient cubic function has linear structures*. More precisely, these functions can be expressed, up to the addition of affine functions and to the composition by linear isomorphisms, as polynomials of R variables with $R \leq 5$ except for the fourth type where $5 \leq R \leq 9$.

Manuscript received April 13, 2004; revised October 21, 2004. The material in this paper was presented in part at the IEEE International Symposium on Information Theory, Chicago, IL, June/July 2004.

C. Carlet is with the University of Vincennes St Denis, Paris 8, France (e-mail: Claude.Carlet@inria.fr).

P. Charpin is with the INRIA, Domaine de Voluceau, Rocquencourt, BP 105-78153, Le Chesnay Cedex, France (e-mail: Pascale.Charpin@inria.fr).

Communicated by T. Johansson, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2004.840902

We prove also that cubic $(m-4)$-resilient functions have derivatives with weights far from 2^{m-1} (see Lemma 3). Thus, we finally conclude that, cryptographycally speaking, these functions are *bad* unless $m = 5, 6$.

Main notation.

— $\mathrm{wt}(u)$ is the Hamming weight of the vector u;
— $\mathcal{B}_m$ is the set of Boolean functions on m variables;
— $\mathcal{F}(f)$, $f \in \mathcal{B}_m$, is defined by (3);
— $\mathcal{C}_m = \{f \in \mathcal{B}_m \mid deg(f) = 3, f \text{ is } (m-4)\text{-resilient}\}$;
— S_f, S_f^0 are defined by (10) and (17).

II. Preliminaries

Let us denote by $\boldsymbol{F}_2^m$ the binary vector-space of dimension m. Recall that the Hamming weight of any vector $u \in \boldsymbol{F}_2^m$ is $\mathrm{wt}(u) = \sum_{i=1}^m u_i$ (this sum being calculated in $\boldsymbol{Z}$). A Boolean function is usually given by its algebraic normal form (ANF)

$$f(x_1, \ldots, x_m) = \sum_{u \in \boldsymbol{F}_2^m} f^\diamond(u) \left(\prod_{i=1}^m x_i^{u_i} \right) \tag{1}$$

where the sum is calculated $\bmod 2$, $f^\diamond$ is a Boolean function too, and $u = (u_1, \ldots, u_m)$. The *degree* of f, denoted by $\deg(f)$, is the maximal value of $\mathrm{wt}(u)$ such that $f^\diamond(u) \neq 0$. The mapping which carries f to $f^\diamond$ is the binary Möbius transform of f.

Lemma 1: For all $a = (a_1, \ldots, a_m)$ and $b = (b_1, \ldots, b_m)$ in $\boldsymbol{F}_2^m$, define the partial order

$$a \preceq b \Longleftrightarrow a_i \leq b_i, \qquad \forall\, i = 1, \ldots, m.$$

Then, for any f given by (1), we have

$$f^\diamond(u) = \left(\sum_{v \preceq u} f(v) \right) \pmod 2.$$

Then we can express as follows the degree of any Boolean function.

Proposition 1: Let $f \in \mathcal{B}_m$ and let r be an integer in the range $[0, m]$. Then

1) the degree of f is at most r if and only if, for any subspace V_u of $\boldsymbol{F}_2^m$, $\mathrm{wt}(u) \geq r+1$ and V_u of the form
$$V_u = \{v \mid v \preceq u\},$$
the restriction of f to V_u has an even weight;
2) the degree of f is exactly r if and only if f is of degree at most r and there is a subspace V_u, with $\mathrm{wt}(u) = r$ such that the restriction of f to V_u has an odd weight.

So we recall the definition of Reed–Muller codes in this context.

Definition 1: Let us define $\{\boldsymbol{F}_2^m, +\}$ as an ordered vector-space

$$\boldsymbol{F}_2^m = \{\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{2^m-1}\} \tag{2}$$

where $\boldsymbol{v}_i$ is an m-dimensional binary vector. The Reed–Muller code of length 2^m and order $r, 0 \leq r \leq m$, denoted by $R(r,m)$, is the binary code of length 2^m composed of the codewords $(f(\boldsymbol{v}_0), \ldots, f(\boldsymbol{v}_{2^m}))$ where f is a Boolean function on m variables whose degree is less than or equal to r.

For simplicity, and if there is no confusion, we will identify any function $f \in \mathcal{B}_m$ with its corresponding codeword of length 2^m; in particular, the weight of f, denoted $\mathrm{wt}(f)$, is the Hamming weight of this codeword.

A. Basic Terminology and Useful Properties

For any $f \in \mathcal{B}_m$, we denote by $\mathcal{F}(f)$ the character sum

$$\mathcal{F}(f) = \sum_{x \in \boldsymbol{F}_2^m} (-1)^{f(x)}. \tag{3}$$

The function f is said to be *balanced* if $\mathcal{F}(f) = 0$. For any $a \in \boldsymbol{F}_2^m$, define the linear function $\varphi_a : x \mapsto a \cdot x$. The mapping $a \mapsto \mathcal{F}(f + \varphi_a)$ is called the *Walsh transform* of f. The values $\mathcal{F}(f+\varphi_a)$, and the number of times they occur, form the *Walsh spectrum* of f. The *nonlinearity* N_f of f, is related to the Walsh transform via the following expression:

$$N_f = 2^{m-1} - \frac{\mathcal{L}(f)}{2} \quad \text{where} \quad \mathcal{L}(f) = \max_{a \in \boldsymbol{F}_2^m} |\mathcal{F}(f + \varphi_a)|. \tag{4}$$

We shall need the following well-known property.

Proposition 2: Let f be a Boolean function on $\boldsymbol{F}_2^m$ such that, for every $a \in \boldsymbol{F}_2^m$, $\mathcal{F}(f+\varphi_a)$ is divisible by 2^k for some integer k, then the degree of f is upper-bounded by $n - k + 1$.

The derivative of f, with respect to some $a \in \boldsymbol{F}_2^m$, is the function of $\mathcal{B}_m$

$$D_a f : x \mapsto f(x) + f(x + a).$$

When $D_a f$ is constant, a is said to be a *linear structure* of f. The linear space of f is the set of linear structures of f. It is clearly a linear space.

There is a set of classical tools for the study of Boolean functions; we give here, without proof, some formulas which will be used later (see, for instance, [2], [4]). The Parseval's relation is as follows:

$$\sum_{a \in \boldsymbol{F}_2^m} \mathcal{F}^2(f + \varphi_a) = 2^{2m}. \tag{5}$$

We will need this inverse formula

$$\sum_{a \in \boldsymbol{F}_2^m} \mathcal{F}(f + \varphi_a) = 2^m (-1)^{f(0)}. \tag{6}$$

For any subspace U of $\boldsymbol{F}_2^m$ of dimension ℓ, we have

$$\sum_{u \in U} \mathcal{F}^2(f + \varphi_u) = 2^\ell \sum_{v \in U^\perp} \mathcal{F}(D_v f) = 2^\ell \sum_{i=1}^{2^\ell} \mathcal{F}^2(h_i) \tag{7}$$

$$\sum_{u \in U} \mathcal{F}(f + \varphi_u) = 2^\ell \sum_{x \in U^\perp} (-1)^{f(x)} \tag{8}$$

where $U^\perp$ is the dual of U with respect to the scalar product of vectors written in the standard basis, and where the h_i's are the restrictions of f to the cosets of $U^\perp$.

Definition 2: A function $f \in \mathcal{B}_m$ is said to be *t-resilient* if $\mathcal{F}(f + \varphi_a) = 0$ for all $a \in \boldsymbol{F}_2^m$ satisfying $0 \leq \mathrm{wt}(a) \leq t$, where $\mathrm{wt}(a)$ is the Hamming weight of the vector a.

Recall the well-known Siegenthaler's bound for $f \in \mathcal{B}_m$ [15]

$$\text{For every } t < m-1,\ f \text{ is } t \text{ resilient} \Rightarrow \deg(f) \leq m - t - 1. \tag{9}$$

B. Two Notions of Rank of a Subset of $\boldsymbol{F}_2^m$

In order to classify a class of cubic resilient functions, we will study extensively the set of nonzeros of the spectrum of these functions. Recall that a *flat* of $\boldsymbol{F}_2^m$ is a subspace or an affine subspace of $\boldsymbol{F}_2^m$.

Definition 3: Let $f \in \mathcal{B}_m$. We call support of the spectrum of f, and we denote by S_f, the subset of $\boldsymbol{F}_2^m$

$$S_f = \{a \in \boldsymbol{F}_2^m \mid \mathcal{F}(f + \varphi_a) \neq 0\}. \tag{10}$$

The rank of S_f will determine the dimension of the linear space of f.

Definition 4: Let E be any subset of $\boldsymbol{F}_2^m$. The *rank* of E is the dimension of the subspace of $\boldsymbol{F}_2^m$ generated by E. The *affine rank* of E is the dimension of the smallest flat containing E.

Note that rank and affine rank, say k and $\boldsymbol{k}$, respectively, may be different. However, it is easy to check that $\boldsymbol{k} \in \{k, k-1\}$. For instance, if E is the complement of any linear hyperplane then $k = m$ while $\boldsymbol{k} = m - 1$. On the other hand, if E contains 0 then $\boldsymbol{k} = k$.

Proposition 3: Let $f \in \mathcal{B}_m$; denote by k and $\boldsymbol{k}$ (respectively) the rank and the affine rank of S_f. Assume that $\boldsymbol{k} < m$.

Then the linear space L of f has dimension $m - \boldsymbol{k}$. More precisely, L contains a subspace U of dimension $m - k$ such that $D_b f = 0$ for all $b \in U$. If $\boldsymbol{k} = k - 1$ then $D_b f = 1$ for all $b \in L \setminus U$ and f is balanced.

Proof: We give an original proof of this essentially known result. Consider the subspace V of dimension $\boldsymbol{k}$ the coset of which is the smallest flat containing S_f. Let $b \in V^\perp$, $b \neq 0$, and denote by H the hyperplane $\{0, b\}^\perp$. Clearly, H contains V and we have, applying (7)

$$\sum_{u \in H} \mathcal{F}^2(f + \varphi_u) = 2^{m-1}(\mathcal{F}(D_0 f) + \mathcal{F}(D_b f)) = 2^{m-1}(2^m + \mathcal{F}(D_b f))$$

where either $S_f \subset H$ or $S_f \cap H = \emptyset$. This is equivalent to saying that the sum in the preceding equation on the left-hand

side either equals 2^{2m}, according to Parseval's relation (5), or equals 0. In other words, $\mathcal{F}(D_b f) \in \{2^m, -2^m\}$, i.e., $D_b f \in \{0,1\}$. Conversely, if $D_b f \in \{0,1\}$, then $S_f \subset H$ or $S_f \cap H = \emptyset$. We have proved that the linear space L of f contains $V^\perp$ and $V^\perp$ only. We deduce that $L = V^\perp$ and that the dimension of L is therefore $m - \boldsymbol{k}$.

Now the equality $S_f \cap H = \emptyset$, for some $b \in V^\perp$, does not hold when $S_f \subset V$, i.e., when $\boldsymbol{k} = k$. Otherwise, if $\boldsymbol{k} = k-1$, $D_b f = 1$ for a half of elements b of L. The proof is completed since any function which has a derivative equal to 1 is balanced. □

C. The Maiorana–McFarland Construction of Resilient Functions

A method for constructing resilient functions was first proposed in [1, Proposition 4.2] and later precised in [6].

Proposition 4: Let $t < r \leq m$ and let ρ be a mapping

$$\rho : \boldsymbol{F}_2^{m-r} \mapsto \{a \in \boldsymbol{F}_2^r / \mathrm{wt}(a) \geq t+1\}. \tag{11}$$

Let $g \in \mathcal{B}_{m-r}$. For any $x \in \boldsymbol{F}_2^r$ and any $y \in \boldsymbol{F}_2^{m-r}$, define

$$f(x_1, \ldots, x_r, y_1, \ldots, y_{m-r}) = x \cdot \rho(y) + g(y).$$

Then f is t-resilient. Moreover

1) if, for every a belonging to the image of ρ, the restriction of g to $\rho^{-1}(a)$ is balanced, then f is $(t+1)$-resilient;
2) if ρ is injective (resp., if for every $a \in \boldsymbol{F}_2^r$, $\#\rho^{-1}(a)$ has size 0 or 2—we shall call *two-to-one* such mapping), then f has a three-valued spectrum $\{0, \pm 2^r\}$ (resp. $\{0, \pm 2^{r+1}\}$).

ρ can be chosen quadratic such that f is cubic.

This construction will allow us to give examples of functions belonging to the four types of $(m-4)$-resilient functions. It can be used, in its general setting with $t \geq m-4$, or in the particular setting of Alinea 1 with $t \geq m-5$.

In the first case, we must choose $t = m-4$: otherwise, the function would be $(m-3)$-resilient, and therefore quadratic. Also we shall take $r \geq m-2$, since $r = m-3$ leads to a constant mapping ρ; we obtain in fact

$$f = x_1 + \cdots + x_{m-3} + g(y_1, y_2, y_3).$$

We cannot take $r \geq m-1$ since f would not then have degree 3. So $r = m-2$.

In the second case, we must take $t = m-5$ and $r \in \{m-3, m-2\}$. In this case, we do not take ρ injective, since we want to be in the case of Alinea 1. If we want to choose ρ two-to-one, then our interest is for the case $r = m-3$. Indeed, if $r = m-2$ then f has a three-valued spectrum $\{0, \pm 2^{m-1}\}$. We will see later that this is impossible for cubic $(m-4)$-resilient functions (see Proposition 6).

III. The Class of Cubic Functions With Highest Resiliency Order

We consider, for $m \geq 4$, the class $\mathcal{C}_m$ of those functions on m variables which are cubic and $(m-4)$-resilient.

We first recall some properties on these functions.

- When f is $(m-4)$-resilient then $\deg(f) \leq 3$, according to (9). Note that a cubic function cannot be $(m-3)$-resilient.
- When $f \in \mathcal{C}_m$ then for any $a \in \boldsymbol{F}_2^m$ (see [14])

$$\mathcal{F}(f + \varphi_a) \equiv 0 \,(\mathrm{mod} 2^{m-2}). \tag{12}$$

- When $f \in \mathcal{C}_m$ then the derivatives of f satisfy

$$\mathcal{F}(D_a f) \equiv 0 \,(\mathrm{mod} 2^{m-2}) \text{ for any } a \in \boldsymbol{F}_2^m. \tag{13}$$

This last property is an improvement of [8, Theorem 5], in the case where functions of $\mathcal{C}_m$ are considered. We will prove this divisibility in Lemma 3 later. Note that the derivatives of cubic functions are of degree at most 2. So we know that the values of Walsh coefficients of such a derivative are 0 or of the form $\pm 2^{(m-2)+s}$, for $s \in \{0,1,2\}$.

A. Properties of the Class $\mathcal{C}_m$

The Boolean functions whose Walsh spectra take three values only are called *three-valued functions*. When these three values are 0 and $\pm 2^s$, such a function is also called *plateaued* in cryptography. The following Lemma is known (see [3, Proposition II.2] and [4, Proposition 4]). It comes straightforwardly from (12), (6), and Parseval's relation since, according to (12), we have for any $f \in \mathcal{C}_m$

$$\sum_{a \in \boldsymbol{F}_2^m} \mathcal{F}^2(f + \varphi_a) = K 2^{2m-4} = 2^{2m}.$$

Lemma 2: Let $f \in \mathcal{B}_m$ satisfying (12); let S_f denote the support of the Walsh spectrum of f and $\#S_f$ be the cardinality of S_f. Then $\#S_f \leq 16$ with equality if and only if f is plateaued, its Walsh spectrum taking the three values 0, 2^{m-2}, and -2^{m-2}. These values then occur, respectively, $2^m - 2^4$, $2^3 + 2(-1)^{f(0)}$, and $2^3 - 2(-1)^{f(0)}$ times.

Now we can describe more precisely the ANF of the functions of $\mathcal{C}_m$.

Proposition 5: Let $f \in \mathcal{C}_m$, the ANF of which is expressed by (1). Let $u = (u_1, \ldots, u_m)$ such that $\mathrm{wt}(u) = 3$ and let $\overline{u} = (u_1 + 1, \ldots, u_m + 1)$. Then for any such u

$$f^\diamond(u) = 1 \Longleftrightarrow \mathcal{F}(f + \varphi_{\overline{u}}) = \pm 2^{m-2}\lambda$$

where $\lambda \in \{1,3\}$. Notably, the ANF of f cannot have more than 16 terms of degree 3.

Proof: From Lemma 1, $f^\diamond(u) = 1$ if and only if the integer sum $A = \sum_{v \preceq u} f(v)$ is odd. Since f is $(m-4)$-resilient, applying (8) we obtain for $\mathrm{wt}(u) = 3$

$$\sum_{v \preceq \overline{u}} \mathcal{F}(f + \varphi_v) = \mathcal{F}(f + \varphi_{\overline{u}}) = 2^{m-3} \sum_{v \preceq u} (-1)^{f(v)}.$$

Since $f \in \mathcal{C}_m$ then $\mathcal{F}(f + \varphi_{\overline{u}}) = \pm 2^{m-2}\lambda$ with $\lambda \in [0,4]$, from (12). On the other hand, A is odd if and only if $\sum_{v \preceq u} (-1)^{f(v)}$ is equal either to ± 2 or to ± 6. This is equivalent to $\lambda \in \{1,3\}$. As explained through Lemma 1 and Proposition 1, each term of degree 3 in the ANF of f is determined by A odd for some u such that $\mathrm{wt}(u) = 3$. The proof is completed by using Lemma 2. □

We immediately deduce that if $f \in \mathcal{C}_m$ then there is at least one v such that $\mathcal{F}(f+\varphi_v) = \pm 2^{m-2}\lambda$ with λ odd. Moreover, this v, if it is unique, must be of weight $m-3$, because otherwise, there would be no term of degree 3 in the ANF of f, a contradiction.

Corollary 1: Let $f \in \mathcal{C}_m$. Then there is at least one v in $\boldsymbol{F}_2^m$ satisfying $\mathrm{wt}(v) = m-3$ and such that

$$\mathcal{F}(f+\varphi_v) = \pm 2^{m-2}\lambda, \qquad \lambda \in \{1,3\}.$$

Remark 1: The previous properties hold in a more general context, notably for t-resilient functions of optimized degree $d = m-t-1$. In this general case, Corollary 1 becomes: there is at least one v satisfying $\mathrm{wt}(v) = t+1$ such that $\mathcal{F}(f+\varphi_v) = \pm 2^{t+2}\lambda$, for some odd λ. Note that, according to Proposition 2, it is impossible that all values of Walsh spectrum of f are divisible by 2^{t+3}.

Now we are going to improve upon [8, Theorem 5] for the divisibility properties of the derivatives of $f \in \mathcal{C}_m$.

Lemma 3: Let $f \in \mathcal{C}_m$. Then for any $a \in \boldsymbol{F}_2^m$

$$\mathcal{F}(D_a f) \equiv 0 \ ((\mathrm{mod}) 2^{m-2}).$$

More precisely

$$\mathcal{F}(D_a f) = 2^{m-3}(\lambda_a - 8), \qquad \lambda_a \in \{0,4,6,8,10,12,16\}.$$

Proof: Let $a \in \boldsymbol{F}_2^m$ where $a \neq 0$ and $H = \{0,a\}^\perp$. Then we have, applying (7)

$$\sum_{v \in H} \mathcal{F}^2(f+\varphi_v) = 2^{m-1}(\mathcal{F}(D_0 f) + \mathcal{F}(D_a f))$$

which gives

$$2^{2m-4}\lambda_a = 2^{m-1}(2^m + \mathcal{F}(D_a f)) \tag{14}$$

for some nonnegative integer λ_a. Clearly, λ_a is greater than or equal to $\#(H \cap S_f)$. We get from (14)

$$\mathcal{F}(D_a f) = 2^{m-3}\lambda_a - 2^m = 2^{m-3}(\lambda_a - 8). \tag{15}$$

Moreover, we have from (8)

$$\sum_{v \in H} \mathcal{F}(f+\varphi_v) = 2^{m-1}((-1)^{f(0)} + (-1)^{f(a)})$$

which can be rewritten as

$$2^{m-2}\mu_a = 2^{m-1}((-1)^{f(0)} + (-1)^{f(a)})$$

for some integer μ_a. It appears then that $\mu_a \in \{0, \pm 4\}$. Thus, the number of $v \in H \cap S_f$ such that $\mathcal{F}(f+\varphi_v) = \pm 2^{m-2}\nu$, with ν odd, is an even number. We deduce that λ_a is an even number as well.

Since f is cubic, the degree of $D_a f$ is less than or equal to 2. Thus, either $\mathcal{F}(D_a f) = 0$ or $|\mathcal{F}(D_a f)|$ is equal to a power of 2, implying in (15)

$$\lambda_a = 8 \text{ or } \lambda_a = 8 \pm 2^s, \qquad s \in \{1,2,3\}. \qquad \square$$

B. The Structure of the Support

We begin by stating some notation. Let $f \in \mathcal{C}_m$. Then we can write its Walsh coefficients as follows:

$$\mathcal{F}(f+\varphi_a) = 2^{m-2}\phi(a) \text{ where}$$
$$\phi : a \in \boldsymbol{F}_2^m \longmapsto \{0, \pm 1, \pm 2, \pm 3, \pm 4\}. \tag{16}$$

Note that $\phi(a) = \pm 4$ is in fact impossible, since f would then be affine. Recall that S_f denotes the support of the Walsh spectrum of f (see (10)). Let us define the odd part of this support

$$S_f^o = \{a \mid \phi(a) \equiv 1 \ (\mathrm{mod}) 2\}. \tag{17}$$

We also consider the Boolean function σ defined by

$$\sigma(a) = 1 \Longleftrightarrow \phi(a) \text{ is odd} \tag{18}$$

which is called the *indicator* of S_f^o.

Theorem 1: Let $f \in \mathcal{C}_m$ and let S_f^o be defined by (17). Then the indicator σ of S_f^o is a Boolean function of degree $m-3$ exactly.

Proof: From (8), we have for any subspace V of dimension $m-2$

$$\sum_{v \in V} \mathcal{F}(f+\varphi_v) = 2^{m-2} \sum_{v \in V} \phi(v) = 2^{m-2} \sum_{u \in V^\perp} (-1)^{f(u)}.$$

Thus, we get

$$\sum_{v \in V} \phi(v) = \sum_{u \in V^\perp} (-1)^{f(u)}$$

where the sum of the right-hand side is even. Then

$$\sum_{v \in V} \phi(v) \equiv 0 \ ((\mathrm{mod}) 2).$$

In other words

$$\#(S_f^o \cap V) \equiv 0 \ (\mathrm{mod}) 2.$$

Now we apply Proposition 1. Since the restriction of σ to any vector-space V of dimension $m-2$ is even, the degree of σ is at most $m-3$. On the other hand, we know, from Corollary 1, that there is at least one $v \in \boldsymbol{F}_2^m$ such that $\mathrm{wt}(v) = m-3$ and

$$\sum_{u \preceq v} \phi(u) = \phi(v) = \pm\lambda, \quad \lambda \text{ odd}.$$

Thus, the degree of σ is exactly $m-3$. $\square$

Kasami and Tokura determined in [9] the number of codewords of weight w, where $d \leq w < 2d$, of any Reed–Muller code of minimum weight d. The ANF of those Boolean functions corresponding to these codewords of *low* weights in any Reed–Muller code were characterized. We are here interested in the Reed–Muller codes of length 2^m and order $m-3$, denoted $R(m-3,m)$; its minimum distance equals 8. We proved that the indicator σ of S_f^o, $f \in \mathcal{C}_m$, belongs to $R(m-3,m)$; moreover, since $\#S_f^o \leq 16$ the weight of σ is in the range $[8,16]$. Theorem 1 of [9] can be rewritten for $R(m-3,m)$ as follows.

Theorem 2: [9] Let $\sigma \in R(m-3,m)$ such that $8 \leq \mathrm{wt}(\sigma) < 16$. Then, up to an affine nonsingular transformation, the ANF of σ has one of the following forms:

1) $\sigma(y_1,\dots,y_m) = y_1\dots y_{m-6}(y_{m-5}y_{m-4}y_{m-3} + y_{m-2}y_{m-1}y_m)$; in this case $\mathrm{wt}(\sigma)=14$;
2) $\sigma(y_1,\dots,y_m) = y_1\dots y_{m-5}(y_{m-4}y_{m-3} + \epsilon y_{m-2}y_{m-1})$, where $\epsilon \in \{0,1\}$; in this case, if $\epsilon = 0$ then $\mathrm{wt}(\sigma)=8$ else $\mathrm{wt}(\sigma)=12$.

Now, according to Theorem 2, we are able to classify the functions f of $\mathcal{C}_m$ by means of the properties of S_f^o.

Corollary 2: Let $f \in \mathcal{C}_m$ and let S_f^o be defined by (17). Then we have the following.

i) The cardinality of S_f^o is divisible by 4; it is equal at least to 8.
ii) $\#S_f^o = 8$ if and only if S_f^o is a three-dimensional flat.
iii) When $\#S_f^o = 12$, the indicator σ of S_f^o is given by Theorem 2, item 2), with $\epsilon = 1$ and $m \geq 5$. Moreover the affine rank of S_f^o is exactly 5 and the rank of S_f^o is equal to 5 if $m = 5$ and to 6 otherwise.
iv) If $\#S_f^o = 16$, then S_f^o cannot be a four-dimensional flat. In this case, $S_f^o = S_f$ and the affine rank of S_f is at least 5.

Proof: In addition to the definition of Reed–Muller codes (Definition 1), recall that the code $R(r,m)$ has minimum distance 2^{m-r} and that its set of minimum-weight codewords is the set of indicators of flats of dimension $m-r$ (see, for instance, [12, Ch. 13, Sec. 4]). Recall that σ denotes the indicator of S_f^o. Let us denote by k and $\boldsymbol{k}$ the rank and the affine rank of S_f^o.

i) From Theorem 1, $\sigma \in R(m-3,m) \setminus R(m-4,m)$. According to Lemma 2, we then deduce that $8 \leq \#S_f^o \leq 16$. Let us denote by S_f^e the set of a such that $\phi(a)$ is even. Using Parseval's relation, we get

$$\sum_{a\in S_f^o} \phi^2(a) + \sum_{a\in S_f^e} \phi^2(a) = 16.$$

This indicates that the cardinality of S_f^o is divisible by 4.

ii) We have $\#S_f^o = 8$ if and only if σ is the indicator of some minimum-weight codeword of $R(m-3,m)$, some three-dimensional flat. In this case $\boldsymbol{k}=3$.

iii) If $\#S_f^o = 12$ then, from Theorem 2, we have, up to affine equivalence

$$\sigma(y_1,\dots,y_m) = y_1\dots y_{m-5}(y_{m-4}y_{m-3} + y_{m-2}y_{m-1}).$$

Set $V = \{y \in \boldsymbol{F}_2^m \mid y_1 = \cdots = y_{m-5} = 1\}$ and let U_1, U_2 be the two subsets of V defined, respectively, by $y_{m-4} = y_{m-3} = 1$ and $y_{m-2} = y_{m-1} = 1$. We have

$$S_f^o = (U_1 \cup U_2) \setminus (U_1 \cap U_2)$$

where U_1 and U_2 are two three-dimensional flats whose intersection has cardinality 2. Thus, $\boldsymbol{k} = 5$. Indeed, let $U_1 = u + U_1'$, where U_1' is the vector-space $\langle a,b,c\rangle$ generated by three linearly independent vectors a, b, and c. Assume, without loss of generality, that $U_1 \cap U_2 = \{u, u+a\}$, then $U_2 = u + \langle a,d,e\rangle$, where a, d, and e are linearly independent. It is a simple matter to check that the smallest flat containing S_f^o is $u + \langle a,b,c,d,e\rangle$. Hence, $k \leq 6$. If $m = 5$ then $k = 5$ is obviously the maximum possible value for k (and we shall show below that this case actually occurs). Otherwise, the $(m-5)$ first coordinates of u being equal to 1 and the $(m-5)$ first coordinates of a, of b, of c, of d, and of e being null, u is linearly independent of a, b, c, d, and e, and we have $k = 6$.

iv) If $\#S_f^o = 16$ then when $\phi(a) \neq 0$ we get $\phi(a) = \pm 1$, according to Lemma 2, implying $S_f^o = S_f$. In this case, σ cannot be the indicator of a minimum-weight codeword of $R(m-4,m)$, that is, of a four-dimensional flat. Thus, the affine rank of S_f is at least 5, completing the proof. □

Remark 2: Theorem 1 could be written in a more general context for any Boolean function f as soon as the coefficients of the Walsh spectrum of f satisfy good divisibility properties. It is of most interest in our context, since the degree of f is small and the divisibility is high.

IV. To Classify the Class $\mathcal{C}_m$

Now we are looking at the different types of functions of $\mathcal{C}_m$; first, we distinguish the suitable values of Walsh coefficients for $f \in \mathcal{C}_m$. According to (12), we have $\mathcal{F}(f+\varphi_a) = 2^{m-2}\phi(a)$ for any a, where $\phi(a)$ is defined by (16). The following nonzero values of $\phi(a)$ can appear:

$\mathcal{F}(f+\varphi_a)$	$\phi(a)$	$\mathrm{wt}(f+\varphi_a)$
2^{m-2}	1	$2^{m-1}-2^{m-3}$
-2^{m-2}	-1	$2^{m-1}+2^{m-3}$
2^{m-1}	2	2^{m-2}
-2^{m-1}	-2	$2^{m-1}+2^{m-2}$
$3\times 2^{m-2}$	3	2^{m-3}
$-3\times 2^{m-2}$	-3	$7*2^{m-3}$

According to Corollary 1, we have first the following proposition.

Proposition 6: Let f be in $\mathcal{C}_m$. Then the values of the Walsh spectrum of f cannot be $\{0, \pm 2^{m-1}\}$.

We are going to classify the functions of $\mathcal{C}_m$ by means of their spectrum. We differentiate four main cases which appear by using Parseval's relation. The possible values of $a \mapsto \phi(a)$ are in $\{0, \pm 1, \pm 2, \pm 3\}$. Parseval's relation gives here

$$\sum_{a\in\boldsymbol{F}_2^m} \phi^2(a) = A_1 + 4A_2 + 9A_3 = 16$$

where, for $i \in \{1,2,3\}$

$$A_i = \#\{a \mid \phi(a) = \pm i\}.$$

Thus, $A_1 + A_2 + A_3 = \#S_f$ and $A_1 + A_3 = \#S_f^o$.

We fully apply Corollary 2. It appears first that $A_3 \in \{0,1\}$. If $A_3 = 1$ the only possibility is $A_1 = 7$, since $\#S_f^o \geq 8$, and $A_2 = 0$; this will be our first type. Now we assume that $A_3 = 0$. Note that $A_1 \neq 0$, from Proposition 6. Hence, $A_1 = 4r$ with $r \geq 2$, that is, $A_1 \in \{8, 12, 16\}$.

This results in four cases only.

Lemma 4: With the previous notation, there are four types of functions of $\mathcal{C}_m$, characterized by the A_i:

I) $A_1=7$, $A_2=0$, and $A_3=1$ implying $\#S_f=\#S_f^o=8$;
II) $A_1=8$, $A_2=2$, and $A_3=0$ implying $\#S_f=10$;
III) $A_1=12$, $A_2=1$, and $A_3=0$ implying $\#S_f=13$;
IV) $A_1=16$ and $A_2=A_3=0$ implying $\#S_f=\#S_f^o=16$.

These cases will be called, respectively, *type* **I**, **II**, **III**, and **IV** and will be studied in Sections IV-A–C. Note that the two first cases are strongly related; they correspond to the case where S_f^o is a flat of dimension 3. So they will be treated together in Section IV-A.

A. Cases I and II

In accordance with Corollary 2, we first examine the two cases where S_f contains a flat of dimension 3. This happens when $\#S_f^o = 8$ and, from Lemma 4, there are two such cases, namely, type **I** and type **II**. Assume that S_f^o is a three-dimensional flat; since f is $m-4$-resilient, we must have

$$a \in S_f^o \Longrightarrow \mathrm{wt}(a) \geq m-3.$$

According to Corollary 1, at least one $a \in S_f^o$, say b, is such that $\mathrm{wt}(b) = m-3$. For clarity we suppose that $b = (0,0,0,1,\ldots,1)$ (this does not restrict the generality, up to permutation of the variables). Thus, $S_f^o = b + C$ where C is some subspace of $\boldsymbol{F}_2^m$ of dimension 3. Let G be the generator matrix of C. We can assume that

$$G = \left[\begin{array}{ccc|c} 1 & 0 & 0 & \\ 0 & 1 & 0 & M \\ 0 & 0 & 1 & \end{array}\right] \tag{19}$$

where M is a $3 \times (m-3)$ binary matrix. Indeed, assume that G cannot be arranged in such a manner. Thus, modulo some linear combination of rows, G could have one row of the form $a = (0,0,0,a_1\ldots,a_{m-3})$, where a is some nonzero vector. This would imply $\mathrm{wt}(b+a) \leq m-4$, a contradiction.

Moreover, for any vector c generated by G, we must have $\mathrm{wt}(b+c) \geq m-3$. Obviously this is possible if and only if each row of M is a vector with Hamming weight at most 1. Thus, we have proved the following.

Lemma 5: Let $f \in \mathcal{C}_m$ such that S_f^o is a three-dimensional flat. Then, up to a permutation of the coordinates

$$S_f^o = b + C, \qquad \text{where } b = (0,0,0,1,\ldots,1)$$

and C is a linear binary code of length m and dimension 3. The generator matrix G of C is defined by (19) where M is a $3 \times (m-3)$ binary matrix whose rows have weight at most 1.

1) Functions of $\mathcal{C}_m$ of Type I: Recall that case **I** is the only one for which $A_3 \neq 0$; that is, there exists $v \in S_f$ such that $\mathcal{F}(f+\varphi_v) = \pm 3 \times 2^{m-2}$. Then, the function g, equal to $f+\varphi_v$ if $\mathcal{F}(f+\varphi_v) = 3\times 2^{m-2}$ and to $f+\varphi_v+1$ if $\mathcal{F}(f+\varphi_v) = -3\times 2^{m-2}$, satisfies $\mathcal{F}(g) = 3 \times 2^{m-2}$, and therefore corresponds to an element of (minimum) weight $2^{m-1} - 3 * 2^{m-3} = 2^{m-3}$ in the Reed–Muller code of order 3. Hence, this function is the indicator of an $(m-3)$-dimensional flat. Replacing $g(x)$ by $g(x+u)$ where $g(u) = 1$ permits to ensure that $g(0) = 1$ and $\mathcal{F}(g) = 3 \times 2^{m-2}$ in the same time. So, we shall be able to move case **I** to the following situation.

Proposition 7: Let g be a function on m variables of degree 3 such that $g(0) = 1$ and $\mathcal{F}(g) = 3 * 2^{m-2}$. Then we have the following.

i) Function g is the indicator (i.e., the characteristic function) of a vector-subspace E of $\boldsymbol{F}_2^m$ of codimension 3. So the ANF of g has the form

$$g = (\varphi_a + 1)(\varphi_b + 1)(\varphi_c + 1) \tag{20}$$

where a, b, and c are linearly independent, and are such that $\langle a,b,c\rangle^\perp$ equals E (whatever is the choice of a, b, and c satisfying these two conditions); the linear space of g equals E.

ii) The function $g + \varphi_v$ is balanced if and only if the four vectors (a,b,c,v) are linearly independent, and S_g equals the vector-space $E^\perp$ (generated by a, b, and c).

iii) The values of the Walsh coefficients are

values	0	$3 * 2^{m-2}$	-2^{m-2}
number	$2^m - 8$	1	7

In particular $\mathcal{L}(g) = 3 * 2^{m-2}$.

Proof: As recalled earlier, the minimum codewords of the Reed–Muller code of order 3 are those codewords which support is an affine subspace (a flat) of dimension $m-3$; then the statement **i)** is obvious, since this flat E containing 0, it is a vector-space and, hence, it equals the intersection of three independent linear hyperplanes containing E.

ii), iii): Consider the functions $g + \varphi_v$, $v \in \boldsymbol{F}_2^{m*}$, where g is defined by (20). Since g is the indicator of E, a vector-space of codimension 3, there are two possible weigths for $g + \varphi_v$:

— either the kernel H of φ_v contains E, that is $v \in E^\perp$, providing

$$\begin{aligned}\mathcal{F}(g+\varphi_v) &= \sum_{x\in H}(-1)^{g(x)} + \sum_{x\notin H}(-1)^{\varphi_v(x)} \\ &= 2^{m-2} - 2^{m-1} = -2^{m-2};\end{aligned}$$

— or H contains a half of E implying that $g+\varphi_v$ is balanced. □

Corollary 3: Let $f \in \mathcal{C}_m$ be a function of type **I**. Let v be the unique vector such that $\mathcal{F}(f+\varphi_v) = \pm 3 * 2^{m-2}$. Let g be the function $f+\varphi_v$ or $f+\varphi_v+1$, composed with some translation, so that $\mathcal{F}(g) = 3 * 2^{m-2}$ and $g(0) = 1$. Then g satisfies **i)**, **ii)**, and **iii)** of Proposition 7, and $S_f^o = S_f$ is a three-dimensional flat. The rank and the affine rank of S_f are, respectively, 4 and 3. Denoting $f(0) = \epsilon$ and $\mathcal{F}(f+\varphi_v) = 3 * 2^{m-2}(-1)^\eta$, the values of the Walsh coefficients of f are

values	0	$3 * 2^{m-2}(-1)^\eta$
number	$2^m - 8$	1
values	$2^{m-2}(-1)^\eta$	$-2^{m-2}(-1)^\eta$
number	$2 + 2(-1)^{\epsilon+\eta}$	$5 - 2(-1)^{\epsilon+\eta}$

In particular, $\mathcal{L}(f) = 3 * 2^{m-2}$; so $N_f = 2^{m-3}$. Moreover, up to a permutation of the variables, the ANF of f has the form

$$\begin{aligned}f = (x_1 + \lambda_1 x_{i_1} + \epsilon_1)(x_2 + \lambda_2 x_{i_2} + \epsilon_2)(x_3 + \lambda_3 x_{i_3} + \epsilon_3) \\ + \varphi_v(x) + \epsilon\end{aligned} \tag{21}$$

where $\{i_1,i_2,i_3\} \subseteq \{4,\ldots,m\}$, $\lambda_i \in \{0,1\}$, $\epsilon_1,\epsilon_2,\epsilon_3,\epsilon \in \{0,1\}$, and where, denoting by e_i the ith vector of the canonical basis of $\boldsymbol{F}_2^m$, the vector $v + (0,0,0,1,\ldots,1)$ is any element of

the vector-space generated by $a = e_1 + \lambda_1 e_{i_1}$, $b = e_2 + \lambda_2 e_{i_2}$, and $c = e_3 + \lambda_3 e_{i_3}$.

Proof: The first part of the proof is directly deduced from Lemma 4 and from Proposition 7, applied to the function g, equal to $f + \varphi_v$ if $\mathcal{F}(f + \varphi_v) = 3 \times 2^{m-2}$ and to $f + \varphi_v + 1$ if $\mathcal{F}(f + \varphi_v) = -3 \times 2^{m-2}$, and composed with some translation. The Walsh coefficient at a of a function $g(x+u)$ being equal to $(-1)^{\varphi_a(u)}$ times the Walsh coefficient at a of g, the values of the Walsh coefficients of f are equal to $0, \pm 3 * 2^{m-2}$, and $\pm 2^{m-2}$, according to Proposition 7; Relation (6) gives the enumeration.

We are going to study now the ANF of f. Suppose that the ANF of f is as in (21), which can be expressed

$$f = (\varphi_a + \epsilon_1)(\varphi_b + \epsilon_2)(\varphi_c + \epsilon_3) + \varphi_v + \epsilon. \qquad (22)$$

It is easy to check that, for any $u \in \boldsymbol{F}_2^m$, $0 \leq \mathrm{wt}(u) \leq m - 4$, the vectors a, b, c, and $u + v$ are linearly independent, implying that $f + \varphi_u$ is balanced, according to Proposition 7.

Conversely, we consider $f \in \mathcal{C}_m$ of type **I**. We can assume that $f(0) = 1$ and $\mathcal{F}(f + \varphi_v) = 3 * 2^{m-2}$, replacing f by $x \mapsto f(x + u) + \epsilon$ for some $u \in \boldsymbol{F}_2^m$ and $\epsilon \in \boldsymbol{F}_2$. This proves, according to Proposition 7, that f has the form (22), where a, b, and c are any linearly independent vectors of the vector-space C such that $S_f = v + C$. According to Lemma 5, C has, up to permutation of the coordinates, the generator matrix G defined by (19), where each row of M has weight at most 1. Hence, we can take $a = e_1 + \lambda_1 e_{i_1}$, $b = e_2 + \lambda_2 e_{i_2}$, and $c = e_3 + \lambda_3 e_{i_3}$. According to Lemma 5 again, $v + (0, 0, 0, 1, \ldots, 1)$ is any element of the vector-space generated by a, b, and c. □

2) Functions of $\mathcal{C}_m$ of Type II: The functions of type **II** differ from the previous type by the fact that their support is the union of a three-dimensional flat, which is S_f^o, with two other elements.

Proposition 8: Let $f \in \mathcal{C}_m$ of *type* **II**. Then
- $\mathcal{L}(f) = 2^{m-1}$; so $N_f = 2^{m-2}$;
- $\#S_f = 10$, $\#S_f^o = 8$ and $\#S_f^e = 2$ (i.e., the value $\pm 2^{m-1}$ appears two times in the spectrum of f); S_f^o is a three-dimensional flat and S_f^e is a line which is parallel to S_f^o.

Assuming that $f(0) = 0$, the spectrum of f has one of these two forms:

	form 1
values	$0,\ 2^{m-2},\ -2^{m-2},\ 2^{m-1}$
number	$2^m - 10,\ 4,\ 4,\ 2$
	form 2
values	$0, 2^{m-2}, -2^{m-2}, 2^{m-1}, -2^{m-1}$
number	$2^m - 10,\ 6,\ 2,\ 1,\ 1$

The affine rank $\boldsymbol{k}$ of S_f is equal to 4. The rank k of S_f is equal to 4 or 5. For $m \geq 5$, f has a linear space of dimension $m - 4$.

Moreover, let H and H^c be the two complementary hyperplanes, the directions of which are orthogonal to the direction of the line S_f^e, then one of the restrictions of f to H and H^c is affine and the other one is quadratic.

Proof: In accordance with Lemma 4, we know that the Walsh spectrum of f is contained in the set $\{0, \pm 2^{m-2}, \pm 2^{m-1}\}$ where $\pm 2^{m-2}$ appears eight times and $\pm 2^{m-1}$ appears two times. Recall that the Walsh coefficients have the form $2^{m-2}\phi(a)$, $a \in \boldsymbol{F}_2^m$, where $\phi(a)$ is defined by (16). Now, since $f(0) = 0$, we deduce from (6)

$$4 = \sum_{a \in \boldsymbol{F}_2^m} \phi(a) = 2 \times \epsilon + \lambda - \mu$$

where $\lambda + \mu = 8$ and $\epsilon \in \{0, \pm 2\}$. First, let us show that it is impossible to have $\epsilon = -2$: in this case, we have $8 = \lambda - \mu$ implying $\lambda = 8$ and $\mu = 0$; let V be the direction of S_f^o, which is a three-dimensional flat; set $S_f^o = a + V$; then we get, applying (8) to the function $f + \varphi_a$

$$\sum_{v \in V} \mathcal{F}(f + \varphi_{a+v}) = 8 \sum_{x \in V^\perp} (-1)^{f(x) + a \cdot x} = 8 * 2^{m-2};$$

this is impossible since $V^\perp$ has size 2^{m-3}. If $\epsilon = 2$ then $4 = 4 + 2\lambda - 8$ implies $(\lambda, \mu) = (4, 4)$. If $\epsilon = 0$ then $4 = 2\lambda - 8$ implies $(\lambda, \mu) = (6, 2)$. Then we get the forms 1 and 2 of the Walsh spectrum.

The affine rank $\boldsymbol{k}$ of S_f equals at most the affine rank of S_f^o plus 2, that is at most 5. Assume that $\boldsymbol{k} = 5$. Then $m \geq 5$ and we can define a hyperplane H such that its coset $a + H$ contains S_f^o and only one $e \in S_f$ such that $\phi(e) = \pm 2$. Thus, applying (8) again

$$\sum_{u \in H} \mathcal{F}(f + \varphi_{a+u}) = 2^{m-2}(\lambda - \mu) + \tau 2^{m-1} = 2^{m-1} \sum_{x \in H^\perp} (-1)^{f(x) + x \cdot a}$$

where $\tau = \pm 1$. Since $\lambda - \mu$ equals either 4 or 0 and the sum on $H^\perp$ equals either 0 or ± 2, this is impossible. Thus, $\boldsymbol{k} = 4$ and the rank k is equal to 4 or 5, since the rank of S_f^o equals 4. From Proposition 3, f has a linear space of dimension $m - 4$.

Let us denote by a and $b = a + c$ the two elements of S_f^e. According to (7) applied to $U = \{0, c\}$ and to the function $f + \varphi_a$, we get

$$\mathcal{F}^2(f + \varphi_a) + \mathcal{F}^2(f + \varphi_b) = 2(\mathcal{F}^2(h_1) + \mathcal{F}^2(h_2))$$

where h_1 and h_2 are the restrictions of $f + \varphi_a$ to the hyperplane $U^\perp$ and to its coset. On the other hand, the sum above is equal to 2^{2m-1}. It is well known that the only possibility is then $\mathcal{F}^2(h_1) = 2^{2m-2}$ and $\mathcal{F}^2(h_2) = 0$ (or *vice versa*) (see the Annex of [3]).

Thus, assuming that h_1 is constant, we claim that f is affine on $U^\perp$. Now we look at h_2, the restriction of f to the coset of $U^\perp$. For any $u \in \boldsymbol{F}_2^m$, we have $f + \varphi_u = (h_1 + \kappa_u, h_2 + \ell_u)$ where (κ_u, ℓ_u) denote the restrictions of φ_u and $h_1 + \kappa_u$ is balanced unless $u = a$ or $u = a + c$; in this case, it is constant. Thus, we get
- if $f + \varphi_u$ is balanced then $h_2 + \ell_u$ is balanced;
- if $\mathcal{F}(f + \varphi_u) = \pm 2^{m-1}$ then $u = a$ or $u = a + c$ implying $h_2 + \ell_u$ balanced;
- if $\mathcal{F}(f + \varphi_u) = \pm 2^{m-2}$ then $\mathcal{F}(h_2 + \ell_u) = \pm 2^{m-2}$.

Finally, assuming that f is of degree 3, it appears that the Walsh spectrum of h_2 is divisible by 2^{m-2}. Hence, according to Proposition 2, the $(m-1)$-variable function h_2 is quadratic. □

We have proved that the functions of type **II** are of interest for $m = 4$ only; indeed, they have a nonzero linear structure for $m > 4$. For $m = 4$ we get cubic balanced functions.

Example 1: For $m = 4$, the following functions are of form 1 and of form 2, respectively (according to the previous proposition)

$$\begin{aligned} f_1(x) &= x_1x_2x_3 + x_1x_4 + x_2 \\ f_2(x) &= x_1x_3x_4 + x_2x_3x_4 + x_1x_2 \\ &\quad + x_1x_3 + x_3 + x_1 + x_4 + x_2. \end{aligned}$$

Note that $f_1 = x_2(x_1x_3 + 1) + x_4x_1$. So f_1 can be obtained by Maiorana–McFarland construction (11), with $\rho(x_1, x_3) = (x_1x_3 + 1, x_1)$ and $g = 0$.

Now consider $h = x_5(f_1 + 1) + (x_5 + 1)f_1$ for $m = 5$. That is,

$$h = x_1x_2x_3 + x_1x_4 + x_2 + x_5.$$

Then h is in $\mathcal{C}_5$ of type **II**; it is cubic, 1-resilient and of form 1. Moreover, h has a linear structure $a = (0, 0, 0, 0, 1)$ with $D_ah = 1$.

B. Functions of $\mathcal{C}_m$ of Type III

Considering functions of type **III**, a number of properties are easily stated.

Proposition 9: Let $f \in \mathcal{C}_m$ of *type* **III**. Then

— $\mathcal{L}(f) = 2^{m-1}$, so $N_f = 2^{m-2}$;
— $\#S_f = 13$, $\#S_f^o = 12$, and $\#S_f^e = 1$ (i.e., the value $\pm 2^{m-1}$ appears only one time in the spectrum of f).

Assuming that $f(0) = 0$, the spectrum of f has one of these two forms

	form 1
values	$0,\ 2^{m-2},\ -2^{m-2},\ 2^{m-1}$
number	$2^m - 13,\ 7,\ 5,\ 1$
	form 2
values	$0,\ 2^{m-2},\ -2^{m-2},\ -2^{m-1}$
number	$2^m - 13,\ 9,\ 3,\ 1$

The affine rank $\boldsymbol{k}$ of S_f is equal to 5. The rank k of S_f is equal to 5 if $m = 5$ and to 6 otherwise. For $m \geq 6$, f has a linear space of dimension $m - 5$.

Proof: In accordance with Lemma 4, we know that the Walsh spectrum of f is contained in the set $\{0, \pm 2^{m-2}, \pm 2^{m-1}\}$ where $\pm 2^{m-2}$ appears 12 times and $\pm 2^{m-1}$ (say $2^{m-1}(-1)^\epsilon$) only once. Recall that the Walsh coefficients have the form $2^{m-2}\phi(a)$, $a \in \boldsymbol{F}_2^m$, where $\phi(a)$ is defined by (16). Now, denoting $\lambda = \#\{a \in \boldsymbol{F}_2^m / \phi(a) = 1\}$ and $\mu = \#\{a \in \boldsymbol{F}_2^m / \phi(a) = -1\}$, we have from (6) and since $f(0) = 0$

$$4 = \sum_{a \in \boldsymbol{F}_2^m} \phi(a) = 2(-1)^\epsilon + \lambda - \mu, \qquad \text{with } \lambda + \mu = 12.$$

Then $4 = 2(-1)^\epsilon + 2\lambda - 12$ which implies

$$\lambda = 8 - (-1)^\epsilon, \qquad \text{and } \mu = 4 + (-1)^\epsilon.$$

In accordance with Corollary 2, **iii**, we know that $\boldsymbol{k} \geq 5$ where 5 is exactly the affine rank of S_f^o; moreover, the rank of S_f^o is 6 when $m \geq 6$. Since S_f contains only one element, say e which is not in S_f^o, then $\boldsymbol{k} \leq 6$. So we have only to treat the case $\boldsymbol{k} = 6$ (with $m \geq 6$) where e is not in the five-dimensional flat containing S_f^o. We can define an hyperplane H such that its coset $a + H$, $a \notin H$, contains S_f^o and does not contain e. We have then, applying (8)

$$\begin{aligned} \sum_{u \in a+H} \mathcal{F}(f + \varphi_u) &= 2^{m-2}(\lambda - \mu) \\ &= \sum_{u \in H} \mathcal{F}(f + \varphi_{a+u}) \\ &= 2^{m-1} \sum_{x \in H^\perp} (-1)^{f(x)+x\cdot a}. \end{aligned}$$

Hence, since $H^\perp$ has two elements, $\lambda - \mu$ belongs to the set $\{-4, 0, 4\}$. But we have proved that $\lambda - \mu$ equals either 6 or 2, a contradiction. This completes the proof. □

Remark: Let us denote again by e the element of S_f^e. Let $a = e + c$ be any element of S_f^o. According to (7) applied to $U = \{0, c\}$ and to the function $f + \varphi_e$, we have

$$\mathcal{F}^2(f + \varphi_e) + \mathcal{F}^2(f + \varphi_a) = 2(\mathcal{F}^2(h_1) + \mathcal{F}^2(h_2))$$

where h_1 and h_2 are the restrictions of $f + \varphi_e$ to the two cosets of $U^\perp$. Since

$$\mathcal{F}^2(f + \varphi_e) + \mathcal{F}^2(f + \varphi_a) = 5 * 2^{2m-4}$$

and since the only possibility for $5 * 2^{2m-5} = 10 * 2^{2m-6}$ being equal to the sum of two squares is

$$10 * 2^{2m-6} = (3 * 2^{m-3})^2 + (2^{m-3})^2$$

(this can easily be shown, by methods similar to those of the appendix in [3]), we deduce that h_1 or h_2 (say h_1) is such that $\mathcal{F}(h_1) = \pm 3 * 2^{m-3}$. By replacing f by $f + 1$ if $\mathcal{F}(h_1) = -3 * 2^{m-3}$, we may assume that $\mathcal{F}(h_1) = 3 * 2^{m-3}$. Since the $(m-1)$-variable function h_1 has degree at most 3, this implies that it is the indicator of a flat of codimension 3.

Since the affine rank of their support is always 5, the functions of $\mathcal{C}_m$ of type **III** are of most interest when $m = 5$. They are cubic functions of five variables which are 1-resilient and have no linear structure. Note that for $m \leq 5$ it is very easy to produce all the functions of $\mathcal{C}_m$ by using a computer. As an illustration, we give one example for each form of functions of type **III**.

Example 2: Let $m = 5$ and $h = x_1x_2x_3 + x_3x_4x_5$. The function

$$h + x_2x_3 + x_2x_4 + x_3x_5 + x_4x_5 + x_1 + x_2$$

is 1-resilient and has spectrum of the first form, i.e., $(\lambda, \mu) = (7, 5)$ with previous notation. The function

$$h + x_3x_4 + x_3x_5 + x_4x_5 + x_1 + x_2$$

is of the second form—$(\lambda, \mu) = (9, 3)$.

Actually, these two functions can be obtained by Maiorana–McFarland construction. Let us denote by f the first one. We have

$$f = x_2(x_1x_3 + x_3 + x_4 + 1) + x_5(x_3x_4 + x_3 + x_4) + x_1$$

providing

$$\rho(x_1, x_3, x_4) = (x_1x_3 + x_3 + x_4 + 1, x_3x_4 + x_3 + x_4)$$

and $g(x_1, x_3, x_4) = x_1$; f is 1-resilient thanks to Alinea 1 of Proposition 4, since g is balanced on each of the sets

$$\rho^{-1}(1,0) = \{(0,0,0), (1,0,0)\},$$
$$\rho^{-1}(0,1) = \{(0,0,1), (0,1,0), (1,0,1), (1,1,1)\}$$
$$\rho^{-1}(1,1) = \{(0,1,1), (1,1,0)\}.$$

We obtain a similar construction for the second function.

C. Functions of $\mathcal{C}_m$ of Type IV

In this section we treat the functions of type **IV** as defined by Lemma 4. We first summarize some properties, according to our previous results.

Proposition 10: Let $f \in \mathcal{C}_m$ of *type* **IV**. Then
— $\mathcal{L}(f) = 2^{m-2}$ and $N_f = 2^{m-1} - 2^{m-3}$;
— $\#S_f = 16$ and $\#S_f^o = S_f$.
The spectrum of f contains three values only (f is said to be three-valued, or more precisely plateaued). Assuming that $f(0) = 0$, this spectrum is as follows:

value	number it occurs
0	$2^m - 16$
2^{m-2}	10
-2^{m-2}	6

Let us denote, respectively, by $\boldsymbol{k}$ and k the affine rank and the rank of S_f, then $5 \leq \boldsymbol{k} \leq k \leq 9$.

Proof: The first part of the proof is deduced from Lemma 4. Particularly, the values of the Walsh coefficients of f are 0 and $\pm 2^{m-2}$. As we recalled at the beginning of Section III-A, the Walsh spectrum of f is well known.

From Corollary 2, **iv**), we know that $5 \leq \boldsymbol{k}$ (with $\boldsymbol{k} \leq k$). Recall the notation $\mathcal{F}(f + \varphi_a) = 2^{m-2}\phi(a)$. Since $f(0) = 0$, there are ten values $\phi(a) = 1$ and six values $\phi(a) = -1$. Let $T^+ = \{a | \phi(a) > 0\}$ and denote by k' the rank of T^+. Set $T^- = \{a | \phi(a) < 0\}$. Let W be the k'-dimensional flat generated by T^+. Then we have

$$\sum_{a \in W} \mathcal{F}(f + \varphi_a) = (10 - D)2^{m-2}$$

where D is equal to the number of $a \in T^-$ which are in W (we have $D \leq 6$). The sum above (on the left-hand side) is less than or equal to 2^m, since it is equal to $2^{k'}\lambda$ where $|\lambda| \leq 2^{m-k'}$ (see (8)). Thus, we must have $D = 6$, implying $T^- \subset W$ and then $S_f \subset W$. So $k' = k$ and we have proved that $5 \leq k \leq 10$.

We now use the proof of Lemma 3 with the same notation. Suppose that $k = 10$. Let us choose an element of T^+. Since this element is linearly independent of the nine others, there exists $a \in \boldsymbol{F}_2^m$ such that the dual of $\{0, a\}$, say the hyperplane H, contains these nine linearly independent elements and not all ten. Thus, we obtain

$$\mu_a = \sum_{v \in H} \phi(v) = 9 - \ell$$

where ℓ is the number of those elements of T^- which are in H. Since $\ell \leq 6$ then $\mu_a > 0$ and we have seen that in this case $\mu_a = 4$ implying $\ell = 5$. On the other hand, $\lambda_a = \#(H \cap S_f)$; so $\lambda_a = 9 + 5 = 14$. From Lemma 3, this value is impossible. So $k = 10$ is impossible; since $\boldsymbol{k} \leq k$, we get $\boldsymbol{k} \leq k \leq 9$ completing the proof. □

Therefore, we have proved the next corollary.

Corollary 4: There are no functions of type **IV** for $m < 5$. For every $m \geq 5$, these functions have optimal nonlinearity $2^{m-1} - 2^{m-3}$. For $m = 5$, such a function f has no linear structure; it is such that the affine rank of S_f is equal to 5.

Functions of $\mathcal{C}_m$ of type **IV** exist. The main example is given by the Maiorana–McFarland functions (see Proposition 4), in which the mapping ρ is injective: for $m \geq 5$, such

$$\rho : \boldsymbol{F}_2^2 \mapsto \left\{ a \in \boldsymbol{F}_2^{m-2} / \mathrm{wt}(a) \geq m - 3 \right\}$$

exists, since $\{a \in \boldsymbol{F}_2^{m-2} / \mathrm{wt}(a) \geq m - 3\}$ has at least four elements. Let $g \in \mathcal{B}_2$. For any $x \in \boldsymbol{F}_2^{m-2}$ and any $y \in \boldsymbol{F}_2^2$, define

$$f(x_1, \ldots, x_{m-2}, y_1, y_2) = x \cdot \rho(y) + g(y).$$

Then f is $(m-4)$-resilient; ρ can be chosen quadratic such that f is cubic. Moreover, f is three-valued with spectrum $\{0, \pm 2^{m-2}\}$. Such a function f is the concatenation of the four affine $(m-4)$-resilient functions $x \mapsto x \cdot \rho(y) + g(y)$ (y ranging over $\boldsymbol{F}_2^2$). We are then able to construct functions of $\mathcal{C}_m$ of type **IV**, as we show for $m = 5$ in the next example.

Example 3: Let $m = 5$; thus, $\boldsymbol{k} = k = 5$ (from Proposition 10). The next function of $\mathcal{C}_5$ is of type **IV**

$$\begin{aligned} f(x,y) &= (y_1y_2 + 1)x_1 + (y_1y_2 + y_1 + 1)x_2 + (y_1y_2 + y_1)x_3 \\ &= (y_1 + 1)(y_2 + 1)(x_1 + x_2) + y_1(y_2 + 1)(x_1 + x_3) \\ &\quad + (y_1 + 1)y_2(x_2 + x_3) + y_1y_2(x_1 + x_2 + x_3). \end{aligned} \tag{23}$$

Indeed, the four linear functions which appear in the expression of f, are $x \mapsto \beta_i \cdot x$, $1 \leq i \leq 4$, where

$$\beta_1 = (1,1,0), \quad \beta_2 = (1,0,1)$$
$$\beta_3 = (0,1,1), \quad \beta_4 = (1,1,1);$$

and all of these vectors have weight at least 2. We have

$$\mathcal{F}(f + \varphi_{u,v}) = \pm 2^3 \Leftrightarrow \varphi_{u,v}(x,y) = \beta_i \cdot x + v \cdot y, \quad \text{for some } i.$$

As expected, we obtain 16 nonzero values; moreover, it appears clearly that

$$S_f = \{(u,v) \mid v \in \boldsymbol{F}_2^2 \text{ and } u = \beta_i \text{ for some } i\}.$$

Thus, the rank of S_f is equal to 2 plus the rank of $\{\beta_i, 1 \leq i \leq 4\}$. We get $2+3$ and obviously the rank is here equal to the affine rank, providing $\boldsymbol{k} = 5$.

Clearly, by using the previous construction, we will always obtain $\boldsymbol{k} = 5$ when m increases. We obtained easily functions of type **IV** with $\boldsymbol{k} = m$ for $m = 6$ with a computer; it seems that they are generally coming from Maiorana–McFarland construction where ρ is two-to-one (see the next example). Using the same construction, we obtained $\boldsymbol{k} = 6$ for $m = 7$; for $m > 6$ other constructions have to be found.

Example 4: The next function of $\mathcal{C}_6$ is of type **IV**. It is three-valued, with values $\{0, \pm 2^4\}$, 2-resilient with nonlinearity $2^5 - 2^3$. This function has no linear structure

$$f(x) = x_2(x_1x_3 + 1) + x_5(x_3x_4 + x_4 + 1) + x_6(x_1x_4 + x_1 + x_4) + x_1x_4 + x_3.$$

With Alinea 1 of Proposition 4, we have

$$\rho(x_1, x_3, x_4) = (x_1x_3 + 1, x_3x_4 + x_4 + 1, x_1x_4 + x_1 + x_4)$$

and $g(x_1, x_3, x_4) = x_1x_4 + x_3$, where g is balanced on the sets

$$\begin{aligned}
\rho^{-1}(1,1,0) &= \{(0,0,0), (0,1,0)\} \\
\rho^{-1}(1,0,1) &= \{(0,0,1), (1,0,1)\} \\
\rho^{-1}(1,1,1) &= \{(0,1,1), (1,0,0)\} \\
\rho^{-1}(0,1,1) &= \{(1,1,0), (1,1,1)\}.
\end{aligned}$$

V. Conclusion

Any Boolean function on m variables which is $(m-4)$-resilient has degree at most 3 and nonlinearity less than or equal to $2^{m-1} - 2^{m-3}$. We classified here such functions which are of degree exactly 3. We mainly proved that these functions have generally poor cryptographic properties. First, they have small nonlinearity, except for type **IV**. They have derivatives of weights very far from 2^{m-1} as soon as $m \geq 8$. Moreover, they have linear structures, for $m \geq 10$. We distinguish four types of such functions and, to be precise, the types **I** to **III** correspond to functions which have linear structures for $m \geq 5$. The fourth type is more interesting; for $m = 5$ and $m = 6$, the corresponding functions have no linear structure and a good nonlinearity. Moreover, even if there exist such functions without linear structure for $m = 7$, 8, and 9 their nonlinearity is decreasing. The problem of studying such functions has to be replaced in the general study of three-valued functions (see [2], [3]). More precisely, we face the following research problem and an open problem.

Research problem. Classify cubic Boolean functions which are three-valued, with values of Walsh spectrum $\{0, \pm 2^s\}$, $s \geq m/2$. Characterize those functions which have no linear structure. Determine their order of resiliency.

Open problem. Does there exist functions of $\mathcal{C}_m$ of type **IV** which have no linear structure for $m = 7$, 8, and 9?

We used here the work of Kasami *et al.* [9] for the description of S_f when $f \in \mathcal{C}_m$ belongs to the three first types. When $\#S_f = 16$, the form of the indicator of S_f is studied in [11] and, hopefully, some properties can be exploited for more constructions.

References

[1] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation-immune functions," in *Advances in Cryptology—CRYPTO'91 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, vol. 576, pp. 86–100.

[2] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions," in *Advances in Cryptology—EUROCRYPT 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1807, pp. 507–522.

[3] ——, "On cryptographic properties of the cosets of $R(1,m)$," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1494–1513, May 2001.

[4] A. Canteaut and P. Charpin, "Decomposing bent functions," *IEEE Trans. Inf. Theory*, vol. 49, no. 8, pp. 2004–19, Aug. 2003.

[5] A. Canteaut and M. Trabbia, "Improved fast correlation attacks using parity-check equations of weight 4 and 5," in *Advances in Cryptology—EUROCRYPT 2000 (Lecture Notes in Computer-Science)*. Berlin, Germany: Springer-Verlag, vol. 1807, pp. 573–588.

[6] C. Carlet, "A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction," in *Advances in Cryptology—CRYPT0 2002 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2002, vol. 2442, pp. 549–564.

[7] C. Carlet and P. Sarkar, "Spectral domain analysis of correlation immune and resilient Boolean functions," *Finite Fields Applic.*, no. 8, pp. 120–130, 2002.

[8] P. Charpin and E. Pasalic, "On propagation characteristics of resilient functions," in *Selected Areas in Cryptography, SAC 2003 (lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2003, vol. 2595, pp. 356–365.

[9] T. Kasami and N. Tokura, "On the weight structure of Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. IT-16, no. 6, pp. 752–825, Nov. 1970.

[10] T. Kasami, N. Tokura, and S. Azumi, "On the weight enumeration of weights less than 2.5d of Reed–Muller codes," *Inf. Contr.*, vol. 30, pp. 380–95, 1976.

[11] ——, "On the weight enumeration of weights less than 2.5d of Reed-Muller codes," Osaka Univ., Osaka, Japan, Rep. Faculty of Eng. Sci.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[13] V. S. Pless, W. C. Huffman, and R. A. Brualdi, "An introduction to algebraic codes," in *Handbook of Coding Theory, Part 1: Algebraic Coding*. Amsterdam, The Netherlands: Elsevier, 1998, ch. 1.

[14] P. Sarkar and S. Maitra, "Nonlinearity bounds and constructions of resilient Boolean functions," in *Advances in Cryptology—CRYPTO 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1880, pp. 515–532.

[15] T. Siegenthaler, "Correlation-immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 5, pp. 776–780, Sep. 1984.

[16] Y. Tarannikov and D. Kirienko, "Spectral analysis of high order correlation immune functions," in *Proc. IEEE Int. Symp. Information Theory, ISIT2001*, Washigton, DC, Jun. 2001, p. 69. Full version available online at http://eprint.iacr.org/, Report 2000/050.