Classification of Cubic $(n-4)$-resilient Boolean Functions

An Braeken[1], Yuri Borissov[2], Svetla Nikova[1], and Bart Preneel[1]

[1] Department Electrical Engineering - ESAT/SCD/COSIC,
Katholieke Universiteit Leuven, Kasteelpark Arenberg 10,
B-3001 Leuven, Belgium
an.braeken,svetla.nikova,bart.preneel@esat.kuleuven.ac.be
[2] Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences,
8 G.Bonchev, 1113 Sofia, Bulgaria
yborisov@moi.math.bas.bg

Abstract. Carlet and Charpin classified in [5] the set of cubic $(n-4)$-resilient Boolean functions into four different types with respect to the Walsh spectrum and the dimension of the linear space. Based on the classification of $RM(3,6)/RM(1,6)$, we completed the classification of the cubic $(n-4)$-resilient Boolean function by deriving the corresponding ANF and autocorrelation spectrum for each of the four types. In the same time, we solved an open problem of [5] by proving that all plateaued cubic $(n-4)$-resilient Boolean functions have dimension of the linear space equal either to $n-5$ or $n-6$.

1 Introduction

The properties of quadratic Boolean functions (i.e, the second order Reed-Muller code $RM(2,n)$) are well studied, (e.g. the weight distribution [13], the affine equivalence classes [13], the classification of resilient functions [4] and functions satisfying propagation characteristics [16], etc.) However, it is not trivial to extend these results for functions of higher degrees and even for cubic functions. It is important to understand how the properties behave for the different degrees of functions.
In this paper we focus on the study of cubic functions which satisfy the highest order of resiliency. Resiliency is an important property related to (fast) correlation attacks in stream ciphers [19, 15], which we define in the next section. In [5], Charpin and Carlet made the first step in classifying the set of $(n-4)$-resilient cubic Boolean functions by distinguishing four types of functions with respect to their Walsh spectrum and linear space. In this paper, we extend their classification by deriving the ANF and autocorrelation spectrum of each type. Moreover, we solve the open problem presented in the conclusions of [5]. We prove that the linear space of functions of type IV (i.e., the plateaued cubic $(n-4)$-resilient functions) has dimension either equal to $n-5$ or $n-6$. This result implies that any plateaued cubic $(n-4)$-resilient

Boolean function for $n \geq 7$ has a non-trivial linear structure. Our approach is based on the classification of the equivalence classes of $RM(3,6)/RM(1,6)$ [14, 9].
The paper is organized as follows. We present in Sect. 2 some background and definitions on Boolean functions. In Sect. 3, we extend the classification of [5]. Finally we conclude in Sect. 4.

2 Background and Definitions

Let $\mathbb{F}_2^n$ be the set of all n-tuples $\overline{x} = (x_1, \ldots, x_n)$ of elements in the field $\mathbb{F}_2$ (Galois field with two elements), endowed with the natural vector space structure over $\mathbb{F}_2$. For the sake of clarity, we use "$\oplus, \bigoplus$" for the addition in characteristic 2 and "$+, \sum$" for the addition in $\mathbb{C}$ or in the finite field $\mathbb{F}_{2^n}$.
A Boolean function f is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Any Boolean function is uniquely represented by a polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$, which is called the *algebraic normal* form (ANF):

$$f(\overline{x}) = \bigoplus_{(a_1,\ldots,a_n)\in\mathbb{F}_2^n} h(a_1, \ldots, a_n) x_1^{a_1} \ldots x_n^{a_n} \,,$$

with h a function on $\mathbb{F}_2^n$ defined by $h(\overline{a}) = \bigoplus_{\overline{x} \preceq \overline{a}} f(\overline{x})$. The *algebraic degree* of f, denoted by $\deg(f)$ or shortly d, is defined as the number of variables in the longest term $x_1^{a_1} \ldots x_n^{a_n}$ in the ANF of f. The study of properties of Boolean functions is related to the study of the binary *Reed-Muller codes*. Each codeword of the binary Reed-Muller code of order r in $\mathbb{F}_{2^n}$, denoted by $RM(r,n)$, is the truth table of the corresponding Boolean function with degree less or equal to r.
A Boolean function f is also uniquely determined by its Walsh transform, which is a real-valued function over $\mathbb{F}_2^n$ that can be defined for all $\overline{\omega} \in \mathbb{F}_2^n$ as

$$W_f(\overline{\omega}) = \sum_{\overline{x}\in\mathbb{F}_2^n} (-1)^{f(\overline{x})\oplus\overline{x}\cdot\overline{\omega}} = 2^n - 2wt(f \oplus \overline{x} \cdot \overline{\omega}) \,, \qquad (1)$$

Here the *dot product* or scalar product of the vectors $\overline{x} = (x_1, x_2, \ldots, x_n)$ and $\overline{\omega} = (\omega_1, \omega_2, \ldots, \omega_n)$ is defined as $\overline{x} \cdot \overline{\omega} = x_1\omega_1 \oplus x_2\omega_2 \oplus \cdots \oplus x_n\omega_n$. The *weight* of a vector $\overline{x}$ (resp. function f) is equal to the number of nonzero positions in the vector (resp. truth table) and is denoted by $wt(\overline{x})$ (resp. $wt(f)$).
Related to the Walsh spectrum, we have the definitions of plateauedness, balancedness, correlation-immunity, and resiliency.

Plateaued Functions [22] A Boolean function f is said to be a plateaued function if its Walsh transform W_f takes only three values 0 and $\pm 2^\lambda$, where λ is a positive integer, called the amplitude of the plateaued function.

Balancedness A Boolean function is balanced if its output is equally distributed, i.e., its weight is equal to 2^{n-1}. This translates to $W_f(0) = 0$ in the Walsh spectrum.

Correlation-Immunity [18] A function f is said to be correlation-immune of order t, denoted by $CI(t)$, if the output of the function is statistically independent of the combination of any t of its inputs. For the Walsh spectrum, it holds that $W_f(\overline{\omega}) = 0$, for $1 \leq wt(\overline{\omega}) \leq t$ [10].

Resiliency [18] The combination of correlation-immunity of order t and balancedness results in the property of resiliency of order t, denoted by $R(t)$. Or also, $W_f(\overline{\omega}) = 0$, for $0 \leq wt(\overline{\omega}) \leq t$ [10].

We now present several important relations that will be used throughout the paper. Let f be a Boolean function on $\mathbb{F}_2^n$ and $\overline{\omega}$ be a vector in $\mathbb{F}_2^n$, such that $wt(\overline{\omega}) = r$. By $f_{\overline{\omega}}$ we denote the Boolean function on $\mathbb{F}_2^{n-r}$, defined as follows. Let $i_1, \ldots, i_r$ be such that $\omega_{i_1} = \cdots = \omega_{i_r} = 1$ and $\omega_j = 0$ for $j \notin \{i_1, \ldots, i_r\}$. Then $f_{\overline{\omega}}$ is formed from f by setting the variable x_j to 0 if and only if $j \in \{i_1, \ldots, i_r\}$. This function is also called the subfunction of f with respect to the vector $\overline{w}$ or the restriction defined by $\overline{w}$.

Theorem 1. *[6] Let $f(x_1, \ldots, x_n)$ be a Boolean function and $\overline{\omega} \in \mathbb{F}_2^n$. Then*

$$\sum_{\overline{\theta} \leq \overline{\omega}} W_f(\overline{\theta}) = 2^n - 2^{wt(\overline{\omega})+1} wt(f_{\overline{\omega}}). \tag{2}$$

This theorem leads to the divisibility result on the Walsh coefficients $W_f(\overline{w}) = 0 \mod 2^{t+2+\lceil \frac{n-t-2}{d} \rceil}$ of t-resilient functions of degree d.
Finally, also the autocorrelation function (or spectrum) of f is an important tool in the study of Boolean functions, which is a real-valued function over $\mathbb{F}_2^n$ that can be defined for all $\overline{\omega} \in \mathbb{F}_2^n$ as

$$r_f(\overline{\omega}) = \sum_{\overline{x} \in \mathbb{F}_2^n} (-1)^{f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\omega})} .$$

However, note that the autocorrelation spectrum does not uniquely determine the function in contrast to the previous transformations. Related to the autocorrelation spectrum are the definitions of derivative and linear structure:

Derivative The function $D_{\overline{\omega}} f(\overline{x}) = f(\overline{x}) \oplus f(\overline{x} \oplus \overline{\omega})$ is called the derivative of f with respect to the vector $\overline{\omega}$.

Linear Structure [8, 12] If the derivative $D_{\overline{\omega}} f$ is a constant function, the vector $\overline{\omega}$ is called a linear structure of f. The set of linear structures forms a subspace which is called linear space of the function and is denoted by $\mathcal{LS}_f$.

A particular type of functions that satisfy $|W_f(\overline{w})| = 2^{n/2}$ for all $\overline{w} \in \mathbb{F}_2^n$ are called *bent functions* [7, 17]. It is well known that $D_{\overline{w}}f$ is balanced for all $\overline{w} \in \mathbb{F}_2^n \setminus \{0\}$.
Two Boolean functions f_1 and f_2 on $\mathbb{F}_2^n$ are called *equivalent* with respect to the general affine group $AGL(2,n)$ if and only if

$$f_1(\overline{x}) = f_2(\overline{x}A \oplus \overline{a}) \oplus \overline{x}\overline{B}^t \oplus b, \ \ \forall x \in \mathbb{F}_2^n\,, \tag{3}$$

where A is a nonsingular binary $n \times n$-matrix, b is a binary constant, and $\overline{a}, \overline{B}$ are n-dimensional binary vectors. If $\overline{B}, b$ are zero, the functions f_1 and f_2 are said to be affine equivalent. We shall also say that f_2 is transformable into f_1. If in the above equation also $\overline{a} = \overline{0}$, then f_1 and f_2 are said to be linearly equivalent. Note also that the action of $AGL(2,n)$ on $RM(r,m)/RM(r-1,m)$ is reduced to the action of the general linear group $GL(2,n)$, since translations leave every element of $RM(r,m)/RM(r-1,m)$ fixed.

3 Classification of $(n-4)$-resilient cubic Boolean Functions

Carlet and Charpin have proved in [5] that the set of $(n-4)$-resilient cubic Boolean functions can be divided into four different types based on the Walsh spectrum and the dimension of the linear space.
The set of tuples in which the first element denotes the absolute Walsh value and the second element the number of times it occurs form the absolute Walsh spectrum of f. The four types of $(n-4)$-resilient cubic Boolean functions on $\mathbb{F}_2^n$ have the following absolute Walsh spectra and linear dimensions:

I. Walsh spectrum: $\{(2^{n-2}, 7), (3 \cdot 2^{n-2}, 1), (0, 2^n - 8)\}$, $\dim(\mathcal{LS}_f) = n - 3$.
II. Walsh spectrum: $\{(2^{n-2}, 8), (2^{n-1}, 2), (0, 2^n - 10)\}$, $\dim(\mathcal{LS}_f) = n - 4$.
III. Walsh spectrum: $\{(2^{n-2}, 12), (2^{n-1}, 1), (0, 2^n - 13)\}$, $\dim(\mathcal{LS}_f) = n - 5$.
IV. Walsh spectrum: $\{(2^{n-2}, 16), (0, 2^n - 16)\}$, $n - 9 \leq \dim(\mathcal{LS}_f) \leq n - 5$.

Notice that functions of type IV are plateaued. We now complete this classification by computing the ANF and the autocorrelation spectrum of each type. Moreover, we prove that $\dim(\mathcal{LS}_f) = n - 5$ or $n - 6$ for functions of type IV.
Further on in our investigations we will use the following Lemma, which slightly strengthens Lemma 3 in [5].

Lemma 1. *Any cubic function whose Walsh values are divisible by* 2^{n-2} *has autocorrelation spectrum with values also divisible by* 2^{n-2}.

The proof in [5] exploits only the divisibility property of the Walsh spectrum. That is why it is also valid for functions, with all Walsh values divisible by 2^{n-2}.

3.1 The Dimension of Linear Space of Functions of Type IV

The proofs of the next theorems make use of the representatives of the affine equivalence classes of $RM(3,n)/RM(2,n), n = 6, 7$ and 8 (see Appendix A). Denote the class with representative $f_i \oplus RM(2,n)$ by C_i for $1 \le i \le 6, 12$, and 32 in dimensions $6, 7$, and 8 respectively.

Theorem 2. *Cubic functions of* 7 *variables with Walsh values divisible by* 32 *can only belong to the affine equivalence classes* C_2, C_3 *or* C_5 *of* $RM(3,7)/RM(2,7)$.

Proof. In [2], we have already proved that functions linearly equivalent to functions with cubic part among f_4, f_6, f_8, f_{10}, f_{11}, and f_{12} have a Walsh value that is not divisible by 16 as well as functions linearly equivalent to a function from $f_9 \oplus RM(2,7)$ have a Walsh value non-divisible by 32.
To show that also class C_7 does not contain such functions, we use Lemma 1. Let $g(\overline{x}) = f_7(\overline{x}) \oplus q(\overline{x})$, where $q(\overline{x})$ is quadratic. The derivative of $g(\overline{x})$ with respect to the vector $\overline{\omega} = (0,0,0,0,0,0,1)$ is $D_{\overline{\omega}}f(\overline{x}) = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus l(x_1,x_2,x_3,x_4,x_5,x_6)$ where l is an affine function of the variables $x_1,\dots,x_6$. This derivative represents a bent function of 6 variables and thus $|r_f(\overline{\omega})| = 16$. Since the autocorrelation spectrum of the set of first order derivatives is affine invariant of $RM(r,n)/RM(r-1,n)$ [3, Proposition 2], this holds for all functions linearly equivalent to functions from $f_7 \oplus RM(2,7)$. If C_7 contains a function, satisfying the divisibility condition according to Lemma 1, all the values of its autocorrelation spectrum are divisible by 32, which is a contradiction. $\square$

In order to show that Theorem 2 can be generalized for dimensions $n \ge 7$, we need the following lemma.

Lemma 2. *Let f be a cubic form of n variables, $n \ge 7$ which does not belong to the affine equivalence classes C_2, C_3, C_5 in $RM(3,n)/RM(2,n)$. Then at least one of the following properties is satisfied:*

1. *f is linearly equivalent to a function having a subfunction with respect to a vector of weight $n-6$ which belongs to C_4 or C_6 in $RM(3,6)/RM(2,6)$;*
2. *f is linearly equivalent to a function having a subfunction with respect to a vector of weight $n-7$ which belongs to C_7 or C_9 in $RM(3,7)/RM(2,7)$.*

Proof. The proof goes by induction with respect to n. For $n = 7$, it is easy to check that the functions $f_4, f_6, f_8, f_{10}, f_{11}$, and f_{12} have a subfunction with respect to $x_7 = 0$ which is either f_4 or f_6. We will use Proposition 6 of [3], which shows that the function f is linearly equivalent to a function of the form $f_i \oplus x_n q$, where $f_i \oplus RM(2,n-1)$ is a representative of the class in $RM(3,n-1)/RM(2,n-1)$ and q a nonzero quadratic function of the variables $x_1,\dots,x_{n-1}$. If $i \notin \{1,2,3,5\}$ substituting

$x_n = 0$ and using the inductive assumption we conclude that the theorem holds. So, we only have to show that the theorem also holds when f_i is one of the functions f_1, f_2, f_3, f_5. If $f = f_1 \oplus x_n q = x_n q$ and if f depends in a nonlinear way on all n variables, by Dickson's theorem f is linearly equivalent to a function of the form $x_n(x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{n-2}x_{n-1})$ (for n odd). Therefore there exists a subfunction with respect to a vector of weight $n-7$, which is linearly equivalent to f_7.
Let f be linearly equivalent to $f_i \oplus x_n q$ for $i = \{2, 3, 5\}$. Since f depends in a nonlinear way on n variables, f should contain at least the term $x_n x_{n-1} x_j$ where $j \in \{1, \ldots, n-2\}$. Since, none of the variables x_i for $i \in \{1, \ldots, 6\}$ is contained in each term of f_5, we can obtain a subfunction with respect to the restriction $x_k = 0$ for $k \notin \{j, n, n-1, a, b, c\}$ where $x_a x_b x_c$ is a term in f_5 which does not contain the variable x_j, i.e., the subfunction $x_a x_b x_c \oplus x_n x_{n-1} x_j \oplus x_n q'(x_j, x_n, x_{n-1}, x_a, x_b, x_c)$, with q' a quadratic function in its arguments. This function is linearly equivalent to f_4.
For f_3, the same reasoning as above can be applied, except if $x_j = x_2$. Let $x_j = x_2$. If f depends in a nonlinear way on n variables with $n \geq 8$, then also the term $x_n x_{n-2} x_l$ with $l \in \{1, \ldots, n-1\} \setminus \{2\}$ is contained in the ANF since f_3 depends in a nonlinear way on 5 variables. Taking the restriction with respect to x_{n-1}, we are in the same situation as for f_5.
Finally, for f_2, in order to obtain a function that depends in a nonlinear way on n variables with $n \geq 8$, there exists a term $x_n x_l x_j$ in the ANF of f with $l \in \{4, 5, \ldots, n-1\}$ such that the variable x_j is not equal to $\{x_1, x_2, x_3\}$. Therefore, we can apply the same approach as explained for the function f_5. $\square$

Theorem 3. *Any cubic function of n variables with Walsh values divisible by 2^{n-2} belongs to one of the affine equivalence classes C_2, C_3 or C_5 in $RM(3,n)/RM(2,n)$ for $n \geq 7$.*

Proof. Taking into account Lemma 2 we have to consider the following two cases:

1. When there exists a vector $\overline{w}$ of weight $n-6$ for which the restriction $f_{\overline{w}}$ belongs to the classes C_4 or C_6 in $RM(3,6)/RM(2,6)$;
2. When there exists a vector $\overline{w}$ of weight $n-7$ for which the restriction $f_{\overline{w}}$ belongs to the classes C_7 or C_9 in $RM(3,7)/RM(2,7)$.

In the first case we can even prove that there are no cubic functions with Walsh values divisible by 2^{n-3}. Suppose that f is such a function and let $\widetilde{f}$ be the image of f under the invertible linear transformation, described in Lemma 2. Now applying equation (2) we obtain

$$\sum_{\overline{v} \preceq \overline{w}} W_{\widetilde{f}}(\overline{v}) = 2^n - 2^{n-5} \cdot wt(\widetilde{f}_{\overline{w}}).$$

The Walsh transform values of $\widetilde{f}$ are divisible by 2^{n-3} and thus, 4 is a divisor of $wt(\widetilde{f_{\overline{w}}})$. But from [11, p. 113] we see that there is no weight divisible by 4 in the cosets $f_4 \oplus RM(2,6)$ and $f_6 \oplus RM(2,6)$. Since the weight of a function is linear invariant we reach a contradiction.
Proceeding in a similar way in the second case we obtain that all Walsh values of $\widetilde{f_{\overline{w}}}$ (which belongs to the classes C_7 or C_9) are divisible by 32. This is a contradiction with Theorem 2 and the proof is completed. □

Corollary 1. *Any $(n-4)$-resilient cubic function belongs to one of the affine equivalence classes C_2, C_3 or C_5 of $RM(3,n)/RM(2,n)$ for $n \geq 7$.*

¿From now on we will consider only functions of type IV. Recall that these functions are plateaued.

Theorem 4. *Each of the classes C_2, C_3 and C_5 contains functions of type IV.*

Proof. The functions $f_2 \oplus x_2x_4 \oplus x_1x_5$, $f_3 \oplus x_2x_6 \oplus x_1x_3$, $f_5 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_5$ on $\mathbb{F}_2^n$ are functions of type IV in the classes C_2, C_3 and C_5, respectively.

We will now prove the linear dimension of functions of the class C_2. Let us first investigate the functions which belong to the class C_2.

Lemma 3. *Any function from $x_1x_2x_3 \oplus RM(2,n)/RM(1,n)$ for $n \geq 6$ is transformable into direct sum $f_1(\overline{x}) \oplus f_2(\overline{y})$, where the function $f_1(\overline{x})$ belongs to the set $\{x_1x_2x_3, x_1x_2x_3 \oplus x_1x_4, x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5, x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6\}$ and $f_2(\overline{y})$ belongs to the set $\{0, y_1y_2, \ldots, y_1y_2 \oplus \ldots \oplus y_{k-1}y_k\}$.*

Proof. Any function g, which belongs to the coset $f_2 \oplus RM(2,n)$ can be decomposed as $g_3 \oplus g_c \oplus g_{n-3}$, where the function g_3 contains the term $x_1x_2x_3$ together with a quadratic function g_3' of the variables $\{x_1, x_2, x_3\}$, the function g_{n-3} is a quadratic function of the variables $\{x_4, \ldots, x_n\}$ with rank $2k$ for $k \geq 0$, and the function g_c contains cross terms from both sets of variables.
First, the function g_3' can be absorbed in the cubic term $x_1x_2x_3$. Then, there exists a linear transformation that maps g_{n-3} onto $0, x_nx_{n-1}, \ldots, x_nx_{n-1} \oplus \cdots \oplus x_5x_4$ and maps the variables x_1, x_2, x_3 onto itself. Suppose g_{n-3} is equal to $x_nx_{n-1} \oplus \cdots \oplus x_lx_{l-1}$ for $5 \leq l \leq n$. The terms in g_c that contain the variables $x_{l-1}, \ldots, x_n$ can be absorbed in g_{n-3}. Consequently, g_c is of the form $x_1l_1 \oplus x_2l_2 \oplus x_3l_3$ where l_1, l_2, l_3 are linear functions in the variables $x_4, \ldots, x_{l-2}$. Thus, after applying a suitable linear transformation, the functions l_1, l_2, l_3 can be mapped onto

$$\begin{array}{llll} l_1 = 0 & l_2 = 0 & l_3 = 0 & \\ l_1 = x_4 & l_2 = 0 & l_3 = 0 & \text{if } l-1 > 4; \\ l_1 = x_4 & l_2 = x_5 & l_3 = 0 & \text{if } l-1 > 5; \\ l_1 = x_4 & l_2 = x_5 & l_3 = x_6 & \text{if } l-1 > 6. \end{array}$$

This will lead to the form as stated in the theorem. □

Theorem 5. *The dimension of the linear space of the functions on $\mathbb{F}_2^n$ from type IV in class C_2 is equal to $n-5$.*

Proof. From Lemma 3, we derive the form of the functions from the coset $x_1x_2x_3 \oplus RM(2,n)$ for $n \geq 6$. The Walsh spectrum of $f_1(\overline{x}) \oplus f_2(\overline{y})$ is equal to the product of the Walsh spectra of $f_1(\overline{x})$ and $f_2(\overline{y})$. Consequently, the only plateaued functions with amplitude 2^{n-2} which belongs to C_2 are the functions equivalent to the function $x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5$. Therefore, the dimension of the linear space of these functions is equal to $n-5$. □

¿From now on we will denote by $\overline{e}_i$ the binary vector of weight 1, which $i-$th coordinate is "1". In order to derive the dimension of the linear space for plateaued functions of classes C_3 and C_5, we make use of the following three basic lemmas.

Lemma 4. *Let g be a function of type IV on $\mathbb{F}_2^n$ and $W_g(\overline{0}) = 2^{n-2}$. Then the weight of g is equal to $2^{n-1} - 2^{n-3}$ and there are three possible weights for the subfunctions of g:*

- *if $W_g(\overline{e}_i) = 2^{n-2}$, then $wt(g(\overline{x}|x_i = 0)) = 2^{n-3}$;*
- *if $W_g(\overline{e}_i) = -2^{n-2}$, then $wt(g(\overline{x}|x_i = 0)) = 2^{n-2}$;*
- *if $W_g(\overline{e}_i) = 0$, then $wt(g(\overline{x}|x_i = 0)) = 3 \cdot 2^{n-4}$.*

Proof. The proof follows from equation (2). □

Lemma 5. *(Kasami et al., van Tilborg [20, 21]) Let us denote by $P_{3,1}$ the functions which are transformable to a function of degree 3 with ANF in which each term involves the same variable. If $f \in RM(3,n)$ and $wt(f) = 2^{n-2}$ then either $f \in P_{3,1}$ or f is transformable into one of the following forms:*

1. $x_2(x_1x_3 \oplus x_4x_5) \oplus x_1x_3$;
2. $x_2(x_1x_3 \oplus x_4x_5) \oplus x_3x_4x_6$;
3. $x_2(x_1x_3 \oplus x_4x_5) \oplus x_4x_6x_7$.

Lemma 6. *[21, Th.1.3.2] If $f(x_1,\ldots,x_m) = x_1x_2 \oplus \cdots \oplus x_{2k-1}x_{2k} \oplus (a_0 \oplus \sum_{i=1}^m a_ix_i)(b_0 \oplus \sum_{i=1}^m b_ix_i)$, $(2k \leq m)$, then f is transformable into one of the following forms:*

$x_1x_2 \oplus \cdots \oplus x_{2k-3}x_{2k-2}$,	$wt(f) = 2^{m-1} - 2^{m-k}$
$x_1x_2 \oplus \cdots \oplus x_{2k-3}x_{2k-2} \oplus 1$,	$wt(f) = 2^{m-1} + 2^{m-k}$
$x_1x_2 \oplus \cdots \oplus x_{2k-3}x_{2k-2} \oplus x_{2k-1}$,	$wt(f) = 2^{m-1}$
$x_1x_2 \oplus \cdots \oplus x_{2k-3}x_{2k-2} \oplus x_{2k-1}x_{2k}$,	$wt(f) = 2^{m-1} - 2^{m-k-1}$
$x_1x_2 \oplus \cdots \oplus x_{2k-1}x_{2k} \oplus 1$,	$wt(f) = 2^{m-1} + 2^{m-k-1}$
$x_1x_2 \oplus \cdots \oplus x_{2k-1}x_{2k} \oplus x_{2k+1}$,	$wt(f) = 2^{m-1}$
$x_1x_2 \oplus \cdots \oplus x_{2k-1}x_{2k} \oplus x_{2k+1}x_{2k+2}$,	$wt(f) = 2^{m-1} - 2^{m-k-2}$

Theorem 6. *The dimension of the linear space of the functions on $\mathbb{F}_2^n$ from type IV in class C_3 is either equal to $n-5$ or $n-6$.*

Proof. Let g be a function of type IV, which belongs to the coset $f_3 \oplus RM(2,n)$, i.e. $g(\overline{x}) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus q(\overline{x})$, where $q(\overline{x})$ is a quadratic function. We can assume without loss of generality that $W_g(\overline{0}) = 2^{n-2}$. It is well known that if all the Walsh values of a given function are divisible by 2^l then all the Walsh values of its subfunctions with respect to a vector of weight w are divisible by 2^{l-w}. Let ν be the following vector: $\nu = (0,0,0,0,0,1,1,\dots,1)$. Consequently, since all the Walsh values of g are divisible by 2^{n-2}, we obtain that $g_\nu(\overline{x}) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus q_\nu(\overline{x})$ is such that all its Walsh values are divisible by 8.
¿From the classification of Berlekamp and Welch [1] for Boolean functions of 5 variables we see that the only possible cosets of $RM(1,n)$ for g_ν are the cosets with representatives $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_3$ and $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_3 \oplus x_1x_4 \oplus x_3x_5$. Therefore we have to consider the following two cases for g:

1. $g(\overline{x}) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_3 \oplus q_1(\overline{x})$,
2. $g(\overline{x}) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_3 \oplus x_1x_4 \oplus x_3x_5 \oplus q_2(\overline{x})$,

where each quadratic term of $q_i(\overline{x})$, $i = 1,2$ contains a variable x_j, for $j \geq 6$.
Let us consider the *first case*. By Lemma 4 there are three possibilities for the weights of the subfunctions of $g(\overline{x})$ with respect to the variable x_2. If $wt(g(\overline{x}|x_2 = 0)) = 2^{n-3} = d_{min}(RM(2,n-1))$, we substitute $x_2 = 0$ and get $g(\overline{x}|x_2 = 0) = x_1x_3 \oplus q_1(\overline{x}|x_2 = 0)$. By Lemma 6 the function $g(\overline{x})$ must be equal to let say $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_3 \oplus x_1y_1 \oplus x_2y_2$, where y_1, y_2 are some affine functions of x_j, for $j \geq 6$. If y_1 or/and y_2 vanish then $\dim(\mathcal{LS})_g \leq n-6$. If both y_1 and y_2 are non-zero, since by Lemma 4 $g(\overline{x}|x_2 = 1)$ is balanced they will be linearly independent. Then $g(\overline{x})$ cannot be a plateaued function since the Walsh spectrum of the function $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_2x_6 \oplus x_1x_7$ on $\mathbb{F}_2^7$ is not three-valued. Therefore $\dim(\mathcal{LS})_g \leq n-6$. Proceeding in a similar way, if $wt(g(\overline{x}|x_2 = 0)) = 2^{n-2}$ we arrive at the same conclusion, i.e. $\dim(\mathcal{LS})_g \leq n-6$. Finally, by using Lemma 6 and consecutively substituting $x_2 = 0$ and $x_2 = 1$ we conclude that a function $g(\overline{x})$, with $wt(g(\overline{x}|x_2 = 0)) = wt(g(\overline{x}|x_2 = 1)) = 3 \cdot 2^{n-4} = 1.5d_{min}(RM(2,n-1))$ cannot be plateaued.
Consider now the *second case*, when $g(\overline{x}) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_3 \oplus x_1x_4 \oplus x_3x_5 \oplus q_2(\overline{x})$. The subfunction $g(\overline{x}|x_2 = 0) = x_1x_3 \oplus x_1x_4 \oplus x_3x_5 \oplus q_2(\overline{x}|x_2 = 0)$ has weight 1.5 $d_{min}(RM(2,n-1))$. Then using Lemma 6 the function $g(\overline{x})$ is equal for example to $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1(x_3 \oplus x_4 \oplus y_1) \oplus x_3x_5 \oplus x_2y_2$, where y_1 and y_2 are some affine functions of x_j, for $j \geq 6$. By substituting $x_2 = 1$ we get that $g(\overline{x}|x_2 = 1) = x_5(x_3 \oplus x_4) \oplus x_1x_4 \oplus x_1y_1 \oplus y_2$ and by Lemma 6 we can conclude that $y_2 = 0$, and if $y_1 \neq 0$ the function $g(\overline{x})$ is not plateaued. Hence the dimension of the linear space is $n-5$. □

Theorem 7. *The dimension of the linear space of the functions from type IV in class C_5 on $\mathbb{F}_2^n$ is equal to $n-6$.*

Proof. Let g be a function of type IV, which belongs to the coset $f_5 \oplus RM(2,n)$, i.e. $g(\overline{x}) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus q(\overline{x})$, where $q(\overline{x})$ is a quadratic function. Similarly as in the proof above, we assume that $W_g(\overline{0}) = 2^{n-2}$. We consider the vector $\nu = (0,0,0,0,0,0,1,1,\dots,1)$ and obtain that $g_\nu(\overline{x}) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus q_\nu(\overline{x})$ satisfies the property that all its Walsh values are divisible by 16.
¿From the classification of cubic functions of 6 variables, we conclude that only the following function has to be investigated: $g(\overline{x}) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_5 \oplus q(\overline{x})$, where each quadratic term of $q(\overline{x})$ contains a variable x_j for $j \geq 7$.
Let us first consider the subfunctions with respect to the variable x_3. We have that $g(\overline{x}|x_3 = 0) = x_2x_4x_5 \oplus x_2(x_1 \oplus x_5) \oplus q(\overline{x}|x_3 = 0)$. Suppose that $W_g(\overline{e}_3) = 2^{n-2}$ (the case $W_g(\overline{e}_3) = -2^{n-2}$ is treated in a similar way, substituting $x_3 = 1$) then $wt(g(\overline{x}|x_3 = 0)) = 2^{n-3} = 2d_{min}RM(3,n-1)$. Then by Lemma 5 the function $g(\overline{x}) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_5 \oplus x_2y_1 \oplus x_3y_2$, where y_1, y_2 are affine functions of x_j, $j \geq 7$. If one of y_1 or y_2 is not equal to zero then by computing the Walsh spectra we see that $g(\overline{x})$ cannot be a plateaued function.
It remains the case, when $W_g(\overline{e}_3) = 0$. We will show that this is impossible. Consider the subfunctions with respect to the variable x_4. We obtain that $g(\overline{x}|x_4 = 0) = x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_5 \oplus q(\overline{x}|x_4 = 0)$. By Lemma 5 we see that $wt(g(\overline{x}|x_4 = 0))$ cannot be $2d_{min}RM(3,n-1)$. If this weight is equal to 2^{n-2}, then $wt(g(\overline{x}|x_4 = 1)) = 2d_{min}RM(3,n-1)$, but since $g(\overline{x}|x_4 = 1) = x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_3x_6 \oplus q(\overline{x}|x_4 = 1)$ we arrive at a contradiction with Lemma 5. Therefore $wt(g(\overline{x}|x_4 = 0)) = wt(g(\overline{x}|x_4 = 1)) = 3 \cdot 2^{n-4}$ and the Walsh value $W_g(\overline{e}_4) = 0$.
Now by using (2) for the vector $\overline{\omega} = (0,0,1,1,0,\dots,0)$ we obtain $W_g(\overline{0}) + W_g(\overline{e}_3) + W_g(\overline{e}_4) + W_g(\overline{\omega}) = 2^n - 8wt(g_{\overline{\omega}})$. Then

$$wt(g_{\overline{\omega}}) = 3 \cdot 2^{n-5} - \frac{W_g(\overline{\omega})}{8}.$$

We have to consider 3 cases according to the values of $W_g(\overline{\omega})$. The corresponding weights for $g_{\overline{\omega}}$ are: $3 \cdot 2^{n-5}$, 2^{n-4}, 2^{n-3}. Since $(g(\overline{x}|x_3 = 1, x_4 = 1)) = x_1 \oplus x_6$, the weight 2^{n-3} for $g_{\overline{\omega}}$ will not appear. Consider the most complex case, when $wt(g_{\overline{\omega}}) = 3 \cdot 2^{n-5}$. It easy to verify that also the weights of $g(\overline{x}|x_3 = 0, x_4 = 1)$, $(g(\overline{x}|x_3 = 1, x_4 = 0))$ and $(g(\overline{x}|x_3 = 1, x_4 = 1))$ are equal to $3 \cdot 2^{n-5}$. By using Lemma 6 we have $g(\overline{x}) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_5 \oplus x_3y_1 \oplus x_4y_2 \oplus y_3y_4$, where y_1, y_2 are affine functions of x_j, $j \geq 7$ and y_3, y_4 are affine functions independent from x_2 and $x_1 \oplus x_5$.
Since the weights of the restrictions of $g(\overline{x})$ over the hyperplanes $a_3x_3 \oplus a_4x_4 = 1$, $(a_3, a_4) \in \mathbb{F}_2^2 \setminus \overline{0}$ are equal to $3 \cdot 2^{n-4}$ and by using the randomization Lemma from

[13, pp. 372] we obtain that y_1, y_2 are linearly dependent on y_3, y_4. Considering all the possible linear combinations of y_3 and y_4 we see that $g(\overline{x})$ cannot be a plateaued function. The other possible weight of $g_{\overline{\omega}}$ leads to the same conclusion and hence $W_g(\overline{e}_3) = 0$ is impossible. So, $g(\overline{x})$ is plateaued only if $q(\overline{x}) \equiv 0$ and therefore the dimension of the linear space is $n-6$. □

Corollary 2. *Plateaued cubic functions with amplitude $n-2$ without linear structure for $n \geq 7$ do not exist.*

3.2 ANF

Theorem 8. *The 4 types of $(n-4)$-resilient cubic Boolean functions on $\mathbb{F}_2^n$ belong (up to linear transformations) to the following cosets of $RM(1,n)$:*

I. $x_1x_2x_3 \oplus RM(1,n)$
II. $x_1x_2x_3 \oplus x_1x_4 \oplus RM(1,n)$
III. $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_3 \oplus RM(1,n)$
IV. *If* $\dim(\mathcal{LS}_f) = n-5$*:*
  (i) $x_1x_2x_3 \oplus x_2x_4 \oplus x_1x_5 \oplus RM(1,n)$
  (ii) $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4 \oplus x_1x_3 \oplus x_1x_5 \oplus RM(1,n)$
  If $\dim(\mathcal{LS}_f) = n-6$*:*
  (i) $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_2x_6 \oplus x_1x_3 \oplus RM(1,n)$
  (ii) $x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_5 \oplus RM(1,n)$

Proof. It is well-known (see for instance [8],[12]) that any function with linear space of dimension k can be transformed by an affine transformation in the sum of two functions f_1 and f_2 where f_1 is a nonlinear function that nonlinearly depends on $n-k$ variables and f_2 a linear function. As a consequence, up to an affine transformation, the nonlinear part of the functions of type I, II, and III depends on 3, 4, resp. 5 variables, while the nonlinear part of the functions of type IV depends on 5 or 6 variables. From Table 1 in Appendix B, we derive the corresponding ANF. □

3.3 Autocorrelation Spectrum

The set of tuples in which the first element denotes the absolute value in the autocorrelation spectrum and the second element the number of times it occurs form the absolute autocorrelation spectrum of f. Since all the functions in a fixed coset of $RM(1,n)$ have the same absolute autocorrelation spectrum, we immediately obtain:

Theorem 9. *The 4 types of $(n-4)$-resilient cubic Boolean functions on $\mathbb{F}_2^n$ have the following absolute autocorrelation spectrum*

I. $\{(2^n, 2^{n-3}), (2^{n-1}, 2^n - 2^{n-3})\}$

II. $\{(2^n, 2^{n-4}), (2^{n-1}, 2^{n-1} - 2^{n-3}), (0, 2^{n-1} + 2^{n-4})\}$

III. $\{(2^n, 2^{n-5}), (2^{n-1}, 2^{n-2} - 2^{n-4}), (2^{n-2}, 2^{n-1}), (0, 2^{n-2} + 2^{n-5})\}$

IV. *If* $\dim(\mathcal{LS}_f) = n - 5$*:*

(i) $\{(2^n, 2^{n-5}), (2^{n-1}, 2^{n-3}), (0, 2^n - 2^{n-5} - 2^{n-3})\}$

(ii) $\{(2^n, 2^{n-5}), (2^{n-2}, 2^{n-1}), (0, 2^n - 2^{n-5} - 2^{n-1})\}$

If $\dim(\mathcal{LS}_f) = n - 6$*:*

(i) $\{(2^n, 2^{n-6}), (2^{n-1}, 2^{n-2} - 2^{n-4}), (0, 2^n - 2^{n-3} - 2^{n-4} - 2^{n-6})\}$

(ii) $\{(2^n, 2^{n-6}), (2^{n-1}, 2^{n-4}), (2^{n-2}, 2^{n-1}), (0, 2^{n-1} - 2^{n-4} - 2^{n-6})\}$

For classes I and II, we note that the autocorrelation values are all divisible by 2^{n-1}. This can be proven similarly as in [5, Lemma 3], but by taking into account that the 8 vectors which yield non-zero value in the Walsh spectrum of a function of type I, and the 8 vectors with value 2^{n-2} in the Walsh spectrum of a function of type II belong to a flat of dimension 3, also proven in [5].

4 Conclusion

Based on the classification of $RM(3,6)/RM(1,6)$, we have solved the open problem from [5] concerning the dimension of the linear space of cubic plateaued $(n-4)$-resilient Boolean functions. Moreover, we have extended the classification of the cubic $(n-4)$-resilient functions with the ANF representation and autocorrelation spectrum.

References

1. E.R. Berlekamp and L.R. Welch. Weight distribution of the cosets of the $(32, 6)$ Reed-Muller code. *IEEE Transactions on Information Theory*, IT-18(1):203–207, 1972.
2. Y. Borissov, A. Braeken, S. Nikova, and B. Preneel. On the covering radii of binary Reed-Muller codes in the set of resilient Boolean functions. *IEEE Transactions on Information Theory*, 51(3):1182–1189, March 2005.
3. E. Brier and P. Langevin. Classification of Boolean cubic forms of nine variables. *IEEE Information Theory Workshop 2003*, pages 179–182, 2003.
4. P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation immune functions. In *Advances in Cryptology — CRYPTO 1991*, volume 576 of *Lecture Notes in Computer Science*, pages 86–100. Joan Feigenbaum, editor, Springer, 1991.
5. C. Carlet and P. Charpin. Cubic Boolean functions with highest resiliency. *IEEE Transactions on Information Theory*, 2005.
6. C. Carlet and P. Sarkar. Spectral domain analysis of correlation immune and resilient Boolean functions. *Finite fields and Applications*, 8:120–130, 2002.
7. J. Dillon. *Elementary Hadamard Difference Sets.* PhD thesis, University of Maryland, 1974.
8. J.H. Evertse. Linear structures in block ciphers. In *Advances in Cryptology — EUROCRYPT 1987*, volume 304 of *Lecture Notes in Computer Science*, pages 249–266. David Chaum, Wyn L. Price, editors, Springer, 1987.
9. J. Fuller. Affine equivallence classes. http://www.isrc.qut.edu.au/people/fuller/.

10. X. Guo-Zhen and J. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory*, IT-34(3):596–571, 1988.
11. X.D. Hou. $GL(m,2)$ acting on $R(r,m)/R(r-1,m)$. *Discrete Mathematics*, 149:99–122, 1996.
12. X. Lai. Additive and linear structures of cryptographic functions. In *Fast Software Encryption — FSE 1994*, volume 1008 of *Lecture Notes in Computer Science*, pages 75–85. Bart Preneel, editor, Springer, 1994.
13. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier Science Publisher, 1991. ISBN 0-444-85193-3.
14. J.A. Maiorana. A classification of the cosets of the Reed-Muller code $r(1,6)$. *Mathematics of Computation*, 57(195):403–414, 1991.
15. W. Meier and O. Staffelbach. Fast correlation attacks on certain stream ciphers. *Journal of Cryptology*, 1(3):67–86, 1992.
16. B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology — EUROCRYPT 1990*, volume 473 of *Lecture Notes in Computer Science*, pages 161–173. I.B. Damgård, editor, Springer, 1990.
17. O.S. Rothaus. On bent functions. *Journal of Combinatorial Theory (A)*, 20:300–305, 1976.
18. T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, 1984.
19. T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Transactions on Computers*, C-34(1):81–85, January 1985.
20. S. Azumi T. Kasami, N. Tokura. On the weight enumerators on weights less than $2.5d$ of Reed-Muller codes. *Information and Control*, 30:380–395, 1976.
21. Henk van Tilborg. On weight in codes. Master's thesis, TU Eindhoven, 1971.
22. Y. Zheng and X.M. Zhang. Strong linear dependence of unbiased distribution on non-propagative vectors. In *Selected Areas in Cryptography — SAC 1999*, volume 1758 of *Lecture Notes in Computer Science*, pages 92–105. H. Heys and C. Adams, editors, Springer, 2000.

A Representatives of the $GL(n,2)$ orbits in $RM(3,n)/RM(2,n)$ with $n \leq 8$

Theorem 10. *[11] Let $s(r,n)$ denote the number of $GL(n,2)$-orbits in $RM(3,n)/RM(2,n)$. Then*

1. *$s(3,6) = 6$ and $f_i \oplus RM(2,6)$ for $1 \leq i \leq 6$ are the representatives of the $GL(6,2)$-orbits in $RM(3,6)/RM(2,6)$,*
2. *$s(3,7) = 12$ and $f_i \oplus RM(2,7)$ for $1 \leq i \leq 12$ are the representatives of the $GL(7,2)$-orbits in $RM(3,7)/RM(2,7)$,*
3. *$s(3,8) = 32$ and $f_i \oplus RM(2,8)$ for $1 \leq i \leq 32$ are the representatives of the $GL(8,2)$-orbits in $RM(3,8)/RM(2,8)$, where the Boolean functions f_i are given by*

$$
\begin{aligned}
f_1 &= 0\\
f_2 &= x_1x_2x_3\\
f_3 &= x_1x_2x_3 \oplus x_2x_4x_5\\
f_4 &= x_1x_2x_3 \oplus x_4x_5x_6\\
f_5 &= x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6\\
f_6 &= x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6\\
f_7 &= x_1x_2x_7 \oplus x_3x_4x_7 \oplus x_5x_6x_7\\
f_8 &= x_1x_2x_3 \oplus x_4x_5x_6 \oplus x_1x_4x_7\\
f_9 &= x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4x_7\\
f_{10} &= x_1x_2x_3 \oplus x_4x_5x_6 \oplus x_1x_4x_7 \oplus x_2x_5x_7\\
f_{11} &= x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_1x_6x_7\\
f_{12} &= x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_1x_6x_7 \oplus x_2x_4x_7\\
f_{13} &= x_1x_2x_3 \oplus x_4x_5x_6 \oplus x_1x_7x_8\\
f_{14} &= x_1x_2x_3 \oplus x_4x_5x_6 \oplus x_1x_7x_8 \oplus x_4x_7x_8\\
f_{15} &= x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_6x_7x_8 \oplus x_1x_4x_7\\
f_{16} &= x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_7x_8\\
f_{17} &= x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_1x_7x_8\\
f_{18} &= x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_1x_6x_7 \oplus x_2x_3x_8\\
f_{19} &= x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_1x_5x_8 \oplus x_2x_3x_7 \oplus x_6x_7x_8\\
f_{20} &= x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_2x_7x_8 \oplus x_2x_4x_7 \oplus x_1x_6x_8\\
f_{21} &= x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_2x_7x_8 \oplus x_3x_4x_7 \oplus x_1x_6x_8 \oplus x_2x_3x_7 \oplus x_1x_4x_7\\
f_{22} &= x_1x_2x_3 \oplus x_2x_3x_4 \oplus x_3x_4x_5 \oplus x_4x_5x_6 \oplus x_5x_6x_7 \oplus x_6x_7x_8 \oplus x_1x_2x_8 \oplus x_2x_3x_8\\
&\quad \oplus x_3x_4x_8 \oplus x_4x_5x_8 \oplus x_5x_6x_8 \oplus x_1x_7x_8\\
f_{23} &= x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_1x_6x_7 \oplus x_5x_7x_8\\
f_{24} &= x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_1x_6x_7 \oplus x_5x_6x_8\\
f_{25} &= x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \oplus x_1x_6x7 \oplus x_2x_4x_8\\
f_{26} &= x_1x_2x_3 \oplus x_4x_5x_6 \oplus x_1x_4x_7 \oplus x_2x_5x_7 \oplus x_2x_6x_8 \oplus x_2x_7x_8 \oplus x_3x_4x_8\\
f_{27} &= x_1x_2x_3 \oplus x_4x_5x_6 \oplus x_1x_4x_7 \oplus x_2x_5x_7 \oplus x_1x_6x_8 \oplus x_1x_7x_8 \oplus x_2x_4x_8 \oplus x_3x_5x_8\\
f_{28} &= x_1x_2x_7 \oplus x_3x_4x_7 \oplus x_5x_6x_7 \oplus x_2x_5x_8 \oplus x_3x_6x_8\\
f_{29} &= x_1x_2x_3 \oplus x_4x_5x_6 \oplus x_1x_4x_7 \oplus x_3x_6x_8\\
f_{30} &= x_1x_2x_3 \oplus x_4x_5x_6 \oplus x_1x_4x_7 \oplus x_3x_6x_8 \oplus x_5x_7x_8\\
f_{31} &= x_1x_2x_3 \oplus x_4x_5x_6 \oplus x_1x_4x_7 \oplus x_3x_6x_8 \oplus x_4x_7x_8 \oplus x_5x_6x_8\\
f_{32} &= x_1x_2x_3 \oplus x_4x_5x_6 \oplus x_1x_4x_7 \oplus x_1x_6x_8 \oplus x_2x_5x_8 \oplus x_3x_4x_8
\end{aligned}
$$

B Classification of $RM(3,6)/RM(1,6)$ under the action of $AGL(2,6)$

Table 1. The number of cosets, weight distribution and autocorrelation spectra of affine equivalent classes of $RM(3,6)/RM(1,6)$. The functions are represented in abbreviated notation (only the number of the variables) and the sum should be considered modulo 2.

	Representative	Number of Cosets	Walsh transform	Autocorrelation Transform
f_1	0	1	(0,63),(64,1)	(0,63),(64,1)
	12	651	(0,60),(32,4)	(0,48),(64,16)
	14+23	18 228	(0,48),(16,16)	(0,60),(64,16)
	16+25+34	13 888	(8,64)	(0,63),(64,1)
f_2	0	$1\,395 \times 8$	(0,56),(16,7),(48,1)	(32,56),(64,8)
	14	$1\,395 \times 392$	(0,54),(16,8),(32,2)	(0,36),(32,24),(64,4)
	24+15	$1\,395 \times 2\,352$	(0,48),(16,16)	(0,54),(32,8),(64,2)
	16+25+34	$1\,395 \times 1\,344$	(64,8)	(0,63),(64,1)
	45	$1\,395 \times 3\,584$	(0,32),(8,28),(24,2)	(0,48),(32,14),(64,2)
	16+45	$1\,395 \times 25\,088$	(0,24),(8,32),(16,8)	(0,57),(32,6),(64,1)
f_3	0	$54\,684 \times 32$	(0,32),(8,30),(24,1),(40,1)	(16,32),(32,30),(64,2)
	13	$54\,684 \times 320$	(0,51),(16,12),(32,1)	(0,18),(16,32),(32,12),(64,2)
	14	$54\,684 \times 480$	(0,32),(8,28),(24,4)	(0,24),(16,32),(32,6),(64,2)
	16	$54\,684 \times 7\,680$	(0,28),(8,30),(16,4),(24,2)	(0,39),(16,16),(32,8),(64,1)
	26	$54\,684 \times 32$	(0,30),(8,32),(32,2)	(0,32),(32,30),(64,2)
	26+13	$54\,684 \times 320$	(0,48),(16,16)	(0,51),(32,12),(64,1)
	26+14	$54\,684 \times 480$	(0,24),(8,32),(16,8)	(0,57),(32,6),(64,1)
	13+15+26+34	$54\,684 \times 192$	(8,64)	(0,63),(64,1)
	34+13+15	$54\,684 \times 23\,040$	(0,48),(16,16)	(0,30),(16,32),(64,2)
	34+16	$54\,684 \times 192$	(0,24),(8,32),(16,8)	(0,45),(16,16),(64,1)
f_4	0	$357\,120 \times 64$	(4,49),(12,14),(36,1)	(16,49),(32,14),(64,1)
	14	$357\,120 \times 3\,136$	(4,49),(12,12),(28,1),(20,2)	(0,24),(16,33),(32,6),(64,1)
	15+24	$357\,120 \times 64$	(4,46),(20,3),(12,15)	(0,36),(16,25),(32,2),(64,1)
	34+25+16	$357\,120 \times 64$	(4,42),(12,21),(20,1)	(0,42),(16,21),(64,1)
f_5	0	$468\,720 \times 448$	(0,27),(8,32),(16,4),(32,1)	(0,9),(16,48),(32,6),(64,1)
	12+13	$468\,720 \times 18$	(0,28),(8,30),(16,4),(24,2)	(0,27),(16,32),(32,4),(64,1)
	15	$468\,720 \times 14\,336$	(0,26),(8,31),(24,1),(16,6)	(0,30),(16,32),(32,1),(64,1)
	12+13+25	$468\,720 \times 2\,222$	(0,48),(16,16)	(0,27),(16,32),(32,4),(64,1)
	14+25	$468\,720 \times 1\,344$	(0,24),(8,32),(16,8)	(0,45),(16,16),(64,1)
	35+26+25+12+13+14	$468\,720 \times 14\,336$	(8,64)	(0,63),(64,1)
	25+15+16	$468\,720 \times 64$	(0,24),(8,32),(16,8)	(0,39),(16,24),(64,1)
f_6	0	$166\,656 \times 3\,584$	(4,45),(12,18),(28,1)	(0,18),(16,45),(64,1)
	12+13	$166\,656 \times 21\,504$	(4,46),(12,15),(20,3)	(0,30),(16,33),(64,1)
	23+15+14	$166\,656 \times 7\,680$	(4,42),(12,21),(20,1)	(0,42),(16,21),(64,1)