PAPER Special Section on Multiple-Valued Logic and VLSI Computing

Construction of Multiple-Valued Bent Functions Using Subsets of Coefficients in GF and RMF Domains

Miloš M. RADMANOVIĆ[†a)], *Nonmember and* **Radomir S. STANKOVIĆ**[††b)], *Member*

SUMMARY Multiple-valued bent functions are functions with highest nonlinearity which makes them interesting for multiple-valued cryptography. Since the general structure of bent functions is still unknown, methods for construction of bent functions are often based on some deterministic criteria. For practical applications, it is often necessary to be able to construct a bent function that does not belong to any specific class of functions. Thus, the criteria for constructions are combined with exhaustive search over all possible functions which can be very CPU time consuming. A solution is to restrict the search space by some conditions that should be satisfied by the produced bent functions. In this paper, we proposed the construction method based on spectral subsets of multiple-valued bent functions satisfying certain appropriately formulated restrictions in Galois field (GF) and Reed-Muller-Fourier (RMF) domains. Experimental results show that the proposed method efficiently constructs ternary and quaternary bent functions by using these restrictions.

key words: *multiple-valued functions, cryptography, bent functions, Galois field and Reed-Muller-Fourier domain, construction*

1. Introduction

Bent functions are by the definition the most nonlinear function and at the maximum distance from affine functions. These functions are the core of numerous cryptographic systems thanks to their ability to prevent the system from attacks. They have applications in a variety of such systems, like block chippers, stream chippers and hash functions [1]. Therefore, the study of bent functions for cryptography is fundamental for secure communication in the future [2]. The construction of cryptographically useful bent functions is a difficult task. As the number of variables in a function increases, bent functions become extremely rare in the set of all possible functions. The binary bent functions exist only for the even number of variables. Unlike the binary case, multiple-valued (MV) bent functions may have an odd or an even number of variables. Furthermore, the precise general definition of the structure of bent functions does not exist. Also, there is not a formal method for construction of bent functions.

Thus, during recent years, it has been developed a lot of methods for construction of binary bent functions with some properties using combinatorial, algebraic, and heuristic techniques. Combinatorial techniques for constructing bent functions such as iterative construction methods [2], the Maiorana-McFarland construction method, and the partial spread method [1] are the most popular [1]. The most famous iterative construction was given by Rothaus as early as 1976. Constructions of bent functions can be categorized as primary and secondary [2]. In primary constructions, new bent functions are directly obtained, while in secondary constructions new bent functions are derived from already known bent functions.

Combinatorial techniques are in most cases secondary constructions. Since the algebraic degree of any bent function in polynomial form is restricted, the numbers of researchers have been interested in providing constructions of bent functions using the algebraic technique. The monomial and binomial functions are particular cases of functions in polynomial form. The known monomial bent constructions are methods using exponents of Gold, Dillon, Kasami, Canteaut–Leander and Canteaut–Charpin–Kuyreghyan [1]. The most known binomial bent construction is the method using Niho exponents [1]. In contrast to combinatorial and algebraic constructions, some researches proposed heuristic techniques to obtain bent functions. The methods of gradient descent and the use of a genetic algorithm have proven useful in the random generation of bent functions [3]. These methods can be complex, computationally intensive, difficult to implement, and do not always produce a sufficient variety of bent functions.

Finding the complete set of bent functions for given number of inputs is an open problem and it is known the lower and upper bounds in respect to the number of inputs. Since we are not able to classify the set of bent functions, an important topic in research is to find a subset of bent functions leading to efficient construction of bent functions.

The most common characterization of binary bent functions is the same absolute values of all coefficients of their Walsh spectra. All coefficients have the absolute value $2^{n/2}$, where n is the number of binary function variables. Multiple-valued bent functions can be characterized by the equal value of complex modulus of coefficients of the Vilenkin-Chrestenson (VC) transform. Testing of all VC coefficients of p-valued functions requires computation of all p^n coefficients and related comparisons. This computation, even for small number of variables, requires a lot of processing time [4]. Therefore, techniques for construction of bent functions usually combine construction methods with

Manuscript received September 30, 2020.
Manuscript revised February 17, 2021.
Manuscript publicized April 21, 2021.

[†]The author is with the Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, Niš, 18000, Serbia.
[††]The author is with the Mathematical Institute of SASA, Kneza Mihaila 35, Belgrade, 11000, Serbia.
a) E-mail: milos.radmanovic@elfak.ni.ac.rs
b) E-mail: radomir.stankovic@gmail.com

DOI: 10.1587/transinf.2020LOP0009

the exhaustive search over all possible functions, most often with a small number of variables.

The existing methods are mainly focused on the reduction of the search time [5]. In this paper we propose the reduction of the search time by using restrictions imposed on functions in the GF and RMF domains. The GF and RMF spectral transforms have many applications in signal encoding and processing techniques, synthesis, verification, and testing of circuits, and other areas [6]. For practical applications, it is often necessary to be able to efficiently compute these transforms. With the discovery of a fast algorithm which reduces computational complexity of spectral transform from $O(n^p)$ to $O(nlog_p n)$, the fast spectral transform algorithm is an extremely effective tool. This algorithm is also developed for parallel environments for both shared memory and distributed memory platforms.

Since the algebraic degree of bent functions in the GF and RMF domains is restricted, the spectral search space for discovering of bent functions in the GF and RMF domains is discussed in [7]. It is shown that in the GF and RMF domains the discovery is extended to ternary bent functions with 6 variables, and to quaternary bent functions with 4 variables. For construction of these functions with the large number of variables, it can be used various secondary construction techniques applied on discovered bent functions. In the multiple-valued case, the size of spectral search space in the GF and RMF domains increases rapidly in respect to multiple-valued order, as well as the number of variables. Therefore, discovery of bent functions necessarily requires additional reduction of the spectral search space by satisfying restrictions in GF and RMF domains. It was shown that using restrictions of binary functions in the Reed-Muller (RM) domain, the set of functions can be split into the spectral subset with respect to three different criteria related to the properties of RM-spectra of bent functions. The vertical, horizontal, and grid RM subsets are defined [8]. Experimental results showed some interesting properties of different subsets in the spectral RM domain which can be helpful in designing construction methods for obtaining bent functions.

Thus, in this paper, it is presented an efficient method for construction of bent functions using GF and RMF domain subsets. GF and RMF subsets are based on the restrictions of the number and order of spectral coefficients for bent functions. Using properties of bent functions in the GF and RMF domains, there are vertical, horizontal, and grid subsets of MV functions. The aim is to show how to restrict the spectral search space for bent functions in the GF and RMF domains. Experimental results show that the proposed method for construction of bent functions in the GF and RMF domain extends obtaining ternary and quaternary bent functions. This method is investigated using different subsets in the GF as well as in the RMF domain. As the function size increases, the amount of VC coefficients computations extremely increases. For this reason, it is experimented with benchmarks up to 6 variables.

This paper is organized as follows: Sect. 2 shortly introduces the definitions of GF and RMF transforms of MV functions and the appropriate fast computation algorithms. Sections 3 and 5 give an overview of vertical, horizontal and grid subsets of functions in GF and RMF domains. In Sect. 4, it is described the method for construction of bent functions in GF and RMF domains. The features of proposed method for ternary and quaternary functions were experimentally tested in Sect. 6. In Sect. 7, some of the concluding remarks of the proposed method are presented and how the solution can be found in future work.

2. Background Theory

2.1 Galois Field Transform

Binary RM transform, can be generalized to multiple-valued domains as GF transforms, which are defined as representations of p-valued functions over finite fields GF(p).

Each n-variable p-valued function can be represented as a polynomial form [6]:

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=0}^{p^n-1} g_i \phi_i, \tag{1}$$

where $g_i \in \{0, 1, \ldots, p-1\}$ and ϕ_i are the product terms defined in the Hadamard order as elements of the vector $X_{GF}(n)$ defined as:

$$X_{GF}(n) = \bigotimes_{i=1}^{n} X_{GF}(1), \tag{2}$$

where $X_{GF}(1) = [x_i^0 \;\; x_i^1 \;\; x_i^2 \;\; \ldots \;\; x_i^{p-1}]$ and addition and multiplication are carried out in $GF(p)$. In matrix notation, for a function f specified by the function vector $F = [f(0), \ldots, f(p^n - 1)]^T$, the GF sepectrum represented as a vector $S_{f,GF} = [S_f(0), S_f(1), \ldots, S_f(p^n - 1)]^T$ is calculated as [6]:

$$S_{f,GF} = G_{GF}(n)F \tag{3}$$

where,

$$\begin{aligned} G_{GF}(n) &= \bigotimes_{i=1}^{n} G_{GF}(1), \\ G_{GF}(1) &= (X_{GF}(1))^{-1} in GF(p). \end{aligned} \tag{4}$$

For the considerations in this paper, the indices of spectral coefficients are represented as p-ary representation of integers $0, 1, \ldots, p^{n-1}$. For example, in this notation, for $p = 3$ and $n = 2$, the GF-spectrum is $S_{f,GF} = [S_f(00), S_f(01), S_f(02), S_f(10), S_f(11), S_f(12), S_f(20), S_f(21), S_f(22)]^T$. The number of non-zero bits in ternary representation for indices is the order of the spectral coefficient. Accordingly, the algebraic degree is the maximum number of non-zero bits in ternary representation for indices.

For example, the basic Galois field transform matrices, for $GF(3)$ and $GF(4)$ are defined as:

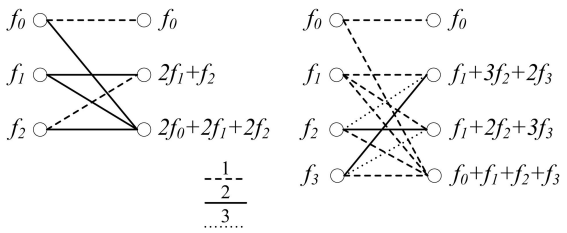

Fig. 1 The elementary butterfly operations for the basic GF transform matrices for ternary and quaternary functions.

$$G_{3GF}(1) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 2 & 2 & 2 \end{bmatrix}. \tag{5}$$

and,

$$G_{4GF}(1) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 2 \\ 0 & 1 & 2 & 3 \\ 1 & 1 & 1 & 1 \end{bmatrix}. \tag{6}$$

The fast computing FFT-like algorithms developed in signal processing can be used to compute the coefficients in GF or RMF functional expressions. Figure 1 shows the elementary butterflies operations (flow-graphs) for the basic GF (Eq. (5) and Eq. (6)) transform matrices, respectively, for ternary and quaternary functions.

2.2 Reed-Muller-Fourier Transform

The Reed-Muller-Fourier transform is a generalization of the Reed-Muller transform of Boolean functions considered in the Gibbs algebra [6]. There are two reasons for introducing Gibbs algebra in the context of the RM transform. The transform matrix used in the GF transform does not have a triangular form as it is the case for the RM transform of Boolean functions. Further, the GF transform does not share many common features of Fourier series for real-valued functions of real-valued variables [6].

Denote by G a group of n-ary p-valued sequences $x = (x_1, \ldots, x_n)$ with the group operation componentwise addition modulo p defined as [6]:

$$\begin{aligned} &\forall x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in G \\ &x \oplus y = (x_1, \ldots, x_n) \oplus (y_1, \ldots, y_n) = \\ &\quad = ((x_1 \oplus y_1) \ldots (x_n \oplus y_n)) mod p \end{aligned} \tag{7}$$

Denote by Z_p the set of first p non-negative integers. For each $x \in G$, the p-adic contraction is defined as a mapping $\sigma : G \to Z_p$, given by [6]:

$$\sigma(x) = \sum_{i=1}^{n} x_i p^{n-i} \tag{8}$$

Denote by $P(G)$ the set of all functions $f : G \to Z_p$. In $P(G)$, we define the addition as modulo p addition [6]:

$$(f \oplus g)(x) = f(x) \oplus g(x), \forall x \in G \tag{9}$$

and multiplication as a convolutionwise (Gibbs) multiplication:

$$\begin{aligned} &(fg)(0) = 0, \\ &(fg)(x) = \sum_{s=0}^{\sigma(x)-1} f(\sigma(x) - 1 - s)g(s), \ \forall x \in G, \ x \neq 0. \end{aligned} \tag{10}$$

The following definition allows to consider the RMF-expressions as polynomial expressions representing a generalization of the Reed-Muller expressions for Boolean functions to multiple-valued functions.

Any p-valued n-variable function $x = (x_1, \ldots, x_n)$ can be expanded in powers of variables $x_i, i = 1, \ldots, n$ as [6]:

$$f(x_1, \ldots, x_n) = (-1)^n \sum_{a \in V^n} q(a) x_1^{*a_1} \ldots x_n^{*a_n} \tag{11}$$

where V^n is the set of all p-valued n-tuples, $q(a) \in \{0, 1, 2, \ldots, p-1\}$, and the exponentiation is defined as $x^{*0} = -1 mod p$, and for $i > 0$, x^{*i} is determined in terms of the convolutionwise (Gibbs) multiplication defined above. In matrix notation, a set of p^n product terms appearing in the positive polarity RMF expression is given by [6]:

$$X_{pRMF}(n) = \bigotimes_{i=1}^{n} X_i(1), \tag{12}$$

where $X_i = [x_i^{*0} x_i^{*1} \ldots x_i^{*(p-1)}]$ and with multiplication modulo p and exponentiation defined above applied to the p-valued variables.

In matrix notation, for a function f specified by the function vector $F = [f(0), \ldots, f(p^n - 1)]^T$, the RMF spectrum represented as a vector $S_{f,RMF} = [S_f(0), S_f(1), \ldots, S_f(p^n - 1)]^T$ is calculated as:

$$S_{f,RMF} = R_{pRMF}(n) F \tag{13}$$

where,

$$\begin{aligned} &R_{pRMF}(n) = \bigotimes_{i=1}^{n} R_{pRMF}(1), \\ &R_{pRMF}(1) = (X_{pRMF}(1))^{-1}. \end{aligned} \tag{14}$$

For example, the basic RMF transform matrices, for ternary and quaternary functions are defined as:

$$R_{3RMF}(1) = 2 \begin{bmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{bmatrix}. \tag{15}$$

and,

$$R_{4RMF}(1) = 3 \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 1 & 1 & 3 & 3 \end{bmatrix}. \tag{16}$$

Figure 2 shows the elementary butterflies operations (flow-graphs) for the basic RMF (Eq. (15) and Eq. (16)) transform matrices, respectively, for ternary and quaternary functions.

2.3 Vilenkin-Chrestenson Transform

The Vilenkin-Chrestenson (VC) transform is viewed as a

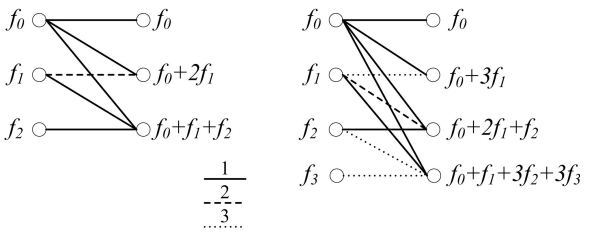

Fig. 2 The elementary butterfly operations for the basic RMF transform matrices for ternary and quaternary functions.

generalization of the Walsh transaform. The VC spectrum, represented as the vector $S_{f,VC} = [S_f(0), S_f(1), \ldots, S_f(p^n - 1)]^T$, is computed using the VC transform matrix [6]:

$$S_{f,VC} = VC_p(n)F \tag{17}$$

where,

$$VC_p(n) = \bigotimes_{i=1}^{n} VC_p(1), \tag{18}$$

For example, the basic VC transform matrices for $p = 3$ and $p = 4$ are defined as:

$$VC_3(1) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & e_2 & e_1 \\ 1 & e_1 & e_2 \end{bmatrix}, \quad \begin{matrix} e_1 = -0.5(1 + i\sqrt{3}) \\ e_2 = -0.5(1 - i\sqrt{3}) \end{matrix} \tag{19}$$

and,

$$VC_4(1) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & i & -1 & -i \end{bmatrix}. \tag{20}$$

An n-variable p-valued function is called bent if all VC coefficients in the vector $S_{f,VC}$ have the same complex modulus (magnitude) of value $p^{n/2}$ [2]. In computing the VC transform of p-valued functions it is usually used the encoding $(0, 1, 2) \rightarrow (1, e_1, e_2)$ and $(0, 1, 2, 3) \rightarrow (1, -1, i, -i)$ for $p = 3$ and $p = 4$, respectively.

3. Subsets of Bent Functions in GF and RMF Domains

Since the algebraic degree of n-variable p-valued bent functions in the polynomial form is at most $\lceil n/2 \rceil$ for $n > 2$, the possible positions of the non-zero coefficients in the spectrum of bent functions are restricted. By using the same feature in the case of binary bent functions, we proposed in [8] splitting the set of all Boolean bent functions with respect to three different criteria related to the properties of their RM spectra. In this paper, the approach is generalized to ternary and quaternary functions. We consider the number and the order of non-zero coefficients for bent functions of different degree. Depending on that, as in the binary case, [8], [9], we define three different subsets: vertical, horizontal, and grid, for multiple-valued functions. Another difference is that we are using coefficients of two different transforms, the GF and RMF spectra.

3.1 Vertical GF and RMF Subsets

The possible number of non-zero coefficients in GF and RMF spectra of bent functions is limited as well as their position in the spectrum, since the order of coefficients has an upper bound. For example, the ternary bent functions with 4 variables can have non-zero GF or RMF coeffcients of order 0, 1, or 2. Thus, the number of non-zero values in the 3-valued representation of their coefficient index of GF or RMF spectrum is less or equal 2.

If a bent function has k non-zero GF coefficients in the spectrum, then this function belongs to the Vertical GF k-subset denoted by $V_{GF}(k)$. The number of possible V_{GF} subsets depends of the number of variables. The value of k needs to be less or equal to the possible number of non-zero coefficients in the GF spectrum of a bent function. For example, two ternary bent functions of 2 variables with GF spectra $S_{f_1,GF} = [1, 0, 2, 0, 0, 0, 2, 0, 0]^T$ and $S_{f_2,GF} = [2, 0, 1, 0, 0, 0, 1, 0, 0]^T$ have 3 non-zero GF-coefficients and belong to the subset $V_{GF}(3)$.

The same definition applied to the RMF spectra of bent functions. If a bent function has k non-zero RMF-coefficients in the spectrum, then this function belongs to the Vertical RMF k-subset denoted by $V_{RMF}(k)$. Also, the number of possible V_{RMF} subsets depends on the number of variables. For example, two ternary bent functions of 2 variables with RMF spectra $S_{f_1,RMF} = [0, 0, 2, 1, 0, 0, 1, 0, 0]^T$ and $S_{f_2,RMF} = [0, 0, 1, 1, 0, 0, 1, 0, 0]^T$ have 3 non-zero RMF-coefficients and belong to the subset $V_{RMF}(3)$.

3.2 Horizontal GF and RMF Subsets

The possible order of non-zero coefficients in GF and RMF spectra of bent functions is also specified, since the algebraic degree of their polynomial representations has an upper bound. For example, the ternary functions with 4 variables can have coefficients of orders: 0,1, or 2.

If a bent function has the minimum k_{min} and the maximum k_{max} order of GF-coefficients in the spectrum, then this function belongs to the Horizontal GF (k_{min}, k_{max})-subset denoted by $H_{GF}(k_{min}, k_{max})$. The number of possible H_{GF} subsets depends of the number of variables. For example, for the ternary functions with 4 variables, there are 6 possible H_{GF} subsets: $H_{GF}(0, 0)$, $H_{GF}(0, 1)$, $H_{GF}(0, 2)$, $H_{GF}(1, 1)$, $H_{GF}(1, 2)$, and, $H_{GF}(2, 2)$. Note that, it can happen that some possible subset does not contain a bent function. For example, two ternary bent functions of 2 variables with GF spectra $S_{f_1,GF} = [0, 1, 1, 0, 0, 0, 2, 0, 0]^T$ and $S_{f_2,GF} = [0, 1, 2, 0, 0, 0, 2, 0, 0]^T$ have coefficients of order 1. It means that they belong to the subset $H_{GF}(1, 1)$. The corresponding polynomial forms are:

$$\begin{aligned} f_1(x_1, x_2) &= x_2^1 \oplus x_2^2 \oplus 2x_1^2 \\ f_2(x_1, x_2) &= x_2^1 \oplus 2x_2^2 \oplus 2x_1^2 \end{aligned} \tag{21}$$

If a bent function has the minimum and the maximum order of RMF-coefficients in the spectrum then

this function belongs to the Horizontal RMF (k_{min}, k_{max})-subset denoted by $H_{RMF}(k_{min}, k_{max})$. For example, two ternary bent functions of 2 variables with RMF spectra $S_{f_1,RMF} = [0,0,2,0,0,0,1,0,0]^T$ and $S_{f_2,RMF} = [0,0,1,0,0,0,2,0,0]^T$ have all the coefficients of order 1. It means that they belong to the subset $H_{RMF}(1,1)$. The corresponding polynomial forms are:

$$\begin{aligned} f_1(x_1,x_2) &= 2x_2^{*2} \oplus x_1^{*2} \\ f_2(x_1,x_2) &= x_2^{*2} \oplus 2x_1^{*2} \end{aligned} \tag{22}$$

3.3 Grid GF and RMF Subsets

In definition of this subset, we take into account both, the orders and the number of non-zero coefficients. If a bent function has k non-zero GF coefficients and the minimum k_{min} and the maximum k_{max} order of GF-coefficients in the spectrum then this function belongs to the Grid GF (k, k_{min}, k_{max})-subset denoted by $G_{GF}(k, k_{min}, k_{max})$. The number of possible G_{GF} subsets depends of the number of variables. For example, for the ternary functions with 2 variables, some possible G_{GF} subsets are: $G_{GF}(1,0,1)$, $G_{GF}(2,0,1)$, and, $G_{GF}(3,0,1)$. For example, two ternary bent functions of 2 variables with GF spectra $S_{f_1,GF} = [0,1,1,0,0,0,2,0,0]^T$ and $S_{f_2,GF} = [0,1,2,0,0,0,2,0,0]^T$ belong to the subset $G_{GF}(3,1,1)$.

If a bent function has k non-zero RMF coefficients and the minimum k_{min} and the maximum k_{max} order of RMF coefficients in the spectrum then this function belongs to the Grid RMF (k, k_{min}, k_{max})-subset denoted by $G_{RMF}(k, k_{min}, k_{max})$. For example, two ternary bent functions of 2 variables with RMF spectra $S_{f_1,RMF} = [0,0,2,0,0,0,1,0,0]^T$ and $S_{f_2,RMF} = [0,0,1,0,0,0,2,0,0]^T$ belong to the subset $G_{RMF}(2,1,1)$.

4. Constructions of Bent Functions in GF and RMF Domains

The algorithm for the construction of bent functions using GF and RMF subsets is given as Algorithm 1.

Algorithm 1

1: Set the number of function variables n.
2: Set the domain: GF or RMF.
3: Set the type of subsets: vertical, horizontal, or grid.
4: Set the selected subsets parameters (the number of the non-zero coefficients for the vertical, min and max order of the non-zero coefficients, for the horizontal, and all three parameters for the greed).
5: Random create functions within the selected subset.
6: Compute the VC spectrum and test bentness for created function, if failed, go to the step 2, else return bent function found.

The algorithm for the construction of bent functions using GF or RMF subsets takes as its input the number of function variables. In any of three types of subsets it takes as its input parameter the number of non-zero GF or RMF coefficients. This parameter should be less then the maximal number of non-zero coefficients that is allowed for bent functions. Depending on the selected type of the subset, it also takes the min and max parameters as the range for the order of the non-zero coefficients. This max parameter should be less then maximal order of coefficients that is allowed for bent functions. The orders of GF or RMF coefficients restrict their positions in the spectrum. These restrictions ensure construction possibility and consequently reduce the possible search space in the GF or RMF domain for bent function random construction.

For example, for the ternary functions with 4 variables, there are 1 zero order, 8 first order, and 24 second order coefficients. The set of possible coefficients of the GF-spectrum for bent functions is $[S_f(0000), S_f(0001), S_f(0002), S_f(0010), S_f(0020),$ $S_f(0100), S_f(0200), S_f(1000), S_f(2000), S_f(0011),$ $S_f(0012), S_f(0021), S_f(0022), S_f(0101), S_f(0102),$ $S_f(0201), S_f(0202), S_f(0110), S_f(0120), S_f(0210),$ $S_f(0220), S_f(1001), S_f(1002), S_f(2001), S_f(2002),$ $S_f(1010), S_f(1020), S_f(2010), S_f(2020), S_f(1100),$ $S_f(1200), S_f(2100), S_f(2200)]^T$.

Thus, the search space size of random construction in GF or RMF domains is $3^{1+8+24} - 1 = 3^{33} - 1$. If the order is restricted, for example, to the $H_{GF}(1,1)$-subset, then the search space size of random construction using subset in GF or RMF domains is only $3^8 - 1$.

The bent testing of VC coefficients includes checking if all the coefficients have the complex modulus (magnitude) equal to $p^{n/2}$. Computation of VC coefficients in this algorithm is performed by the Fast VC spectral transform.

5. Illustrative Examples

In this section, we enumerate bent functions in some vertical, horizontal and grid subsets, in the GF and RMF domains, for ternary and quaternary functions. The aim is to provide specifications how to restrict the search space in GF and RMF domains for bent functions according to the probability of finding them in selected subsets.

Table 1 shows the number of ternary bent functions in the vertical subsets $V_{GF}(k)$ and $V_{RMF}(k)$ for functions of one variable. Table 2 shows the number of ternary bent functions in the subsets $V_{GF}(k)$ and $V_{RMF}(k)$ for two variables. For ternary functions, number of bent functions is equal for all vertical subsets between GF and RMF domains.

Table 3 shows the number of quaternary bent functions in the subsets $V_{GF}(k)$ and $V_{RMF}(k)$ for one variable. Table 4 shows the number of quaternary bent functions in the sub-

Table 1 The number of ternary bent functions in $V_{GF}(k)$ and $V_{RMF}(k)$ for one variable

k	$\#f$ of $V_{GF}(k)$	$\#f$ of $V_{RMF}(k)$
1	3	2
2	8	8
3	8	8

Table 2 The number of ternary bent functions in $V_{GF}(k)$ and $V_{RMF}(k)$ for two variables

k	$\#f$ of $V_{GF}(k)$	$\#f$ of $V_{RMF}(k)$
1	2	2
2	24	24
3	100	100
4	184	184
5	144	144
6	32	32

Table 3 The number of quaternary bent functions in $V_{GF}(k)$ and $V_{RMF}(k)$ for one variable

k	$\#f$ of $V_{GF}(k)$	$\#f$ of $V_{RMF}(k)$
1	1	1
2	5	4
3	11	15
4	15	12

Table 4 The number of quaternary bent functions in $V_{GF}(k)$ and $V_{RMF}(k)$ for two variables

k	$\#f$ **of** $V_{GF}(k)$	$\#f$ **of** $V_{RMF}(k)$
1	0	2
2	3	48
3	33	404
4	184	1754
5	792	4774
6	3190	9646
7	9554	16404
8	20128	24504
9	34328	32090
10	41983	35180
11	37101	31440
12	27744	21506
13	15640	12350
14	7888	7686
15	2136	2376
16	0	540

sets $V_{GF}(k)$ and $V_{RMF}(k)$ for two variables. For quaternary functions, number of bent functions is not equal for all vertical subsets between GF and RMF domains. For example, vertical subset $V_{GF}(4)$ has about 9.5 times more bent functions than $V_{RMF}(4)$. It means that in this case, construction of bent functions in RMF domain will be about 9.5 times faster than in the GF domain.

Table 5 shows the number of ternary bent functions in the subsets $H_{GF}(k_{min}, k_{max})$ and $H_{RMF}(k_{min}, k_{max})$ for two variables where $(k_{min}, k_{max}) \in \{(0,1),(1,1),(1,2),(2,2)\}$. Table 6 shows the number of quaternary bent functions in the subsets $H_{GF}(k_{min}, k_{max})$ and $H_{RMF}(k_{min}, k_{max})$ for two variables where $(k_{min}, k_{max}) \in \{(0,1),(1,1),(1,2),(2,2)\}$. Note that for ternary and quaternary functions, number of bent functions is equal for all horizontal subsets between GF and RMF domains.

Table 7 shows the number of ternary bent functions in the subsets $G_{GF}(k, k_{min}, k_{max})$ and $G_{RMF}(k, k_{min}, k_{max})$ for two variables where $(k, k_{min}, k_{max}) \in \{(1,2,2),(2,0,1),(2,1,1),(2,1,2),(3,0,1),(3,1,1),(3,1,2))\}$. Again, for ternary functions, number of bent functions is equal for all grid subsets between GF and RMF domains. Table 8

Table 5 The number of ternary bent functions in $H_{GF}(k_{min}, k_{max})$ and $H_{RMF}(k_{min}, k_{max})$ for two variables

(k_{min}, k_{max})	$\#f$ of $H_{GF}(k_{min}, k_{max})$	$\#f$ of $H_{RMF}(k_{min}, k_{max})$
0,1	108	108
1,1	36	36
1,2	162	162
2,2	2	2

Table 6 The number of quaternary bent functions in $H_{GF}(k_{min}, k_{max})$ and $H_{RMF}(k_{min}, k_{max})$ for two variables

k	$\#f$ of $V_{GF}(k)$	$\#f$ of $V_{RMF}(k)$
0,1	256	256
1,1	64	64
1,2	50176	50176
2,2	12	12

Table 7 The number of ternary bent functions in $G_{GF}(k, k_{min}, k_{max})$ and $G_{RMF}(k, k_{min}, k_{max})$ for two variables

(k, k_{min}, k_{max})	$\#f$ of $G_{GF}(k, k_{min}, k_{max})$	$\#f$ of $G_{RMF}(k, k_{min}, k_{max})$
1,2,2	2	2
2,0,1	4	4
2,1,1	4	4
2,1,2	20	20
3,0,1	24	24
3,1,1	16	16
3,1,2	60	60

Table 8 The number of quaternary bent functions in $G_{GF}(k, k_{min}, k_{max})$ and $G_{RMF}(k, k_{min}, k_{max})$ for two variables

(k, k_{min}, k_{max})	$\#f$ of $G_{GF}(k, k_{min}, k_{max})$	$\#f$ of $G_{RMF}(k, k_{min}, k_{max})$
2,0,1	1	1
2,1,1	1	1
2,1,2	3	42
2,2,2	2	5
3,0,1	7	11
3,1,1	4	8
3,1,2	24	278
3,2,2	0	5

shows the number of quaternary bent functions in the subsets $G_{GF}(k, k_{min}, k_{max})$ and $G_{RMF}(k, k_{min}, k_{max})$ for two variables. For quaternary functions, as it was the case with the vertical subsets, the number of bent functions is different between the GF and RMF domain.

Experimental results from Table 1–8 showed some interesting properties of different subsets in GF and RMF domain. It is shown that some vertical, horizontal, and grid subsets contain large, but some other a small number of bent functions. There is no difference in the number of ternary bent functions between subsets in the GF and RMF domain. But, for quaternary functions there is the difference. This information can be helpful in designing search method for construction of bent functions.

6. Experimental Results

For an experimental analysis, it is developed an implemen-

tation using C++ programming language of the proposed method for the random construction of bent functions in the GF and RMF domains. Also, it is developed an implementation of the construction of bent functions using GF and RMF subsets. These experiments are performed on a standard PC platform (CPU: 3.6 GHZ, RAM: 12 GB).

Table 9 shows computation performance of the Algorithm 1 for construction of bent function using the random construction in the GF domain and GF subsets. The computational times are given in seconds. It is compared the computation time needed for random construction of one bent function, in respect to the construction of one bent function from the defined subset. Comparison of these numbers is motivated by decreasing computation time when discovery uses GF or RMF subsets. When the number of non-zero coefficients is relatively small, construction of bent functions is faster. The proposed algorithm is implemented and experimentally tested for construction of ternary bent function of 4, 5, and 6 variables and quaternary bent functions of 3, and 4 variables in the GF and RMF domain.

In order to estimate applicability of the proposed algorithm in practice, we point out the following. In the binary case, the keys in block chippers are often constructed by using bent functions. Typically, the length of the key is at least as long as the block length and there are recommendations that the key length should be longer than the block length. For example, in block ciphers with DES algorithm, the keys are composed from four Boolean functions which can be constructed using bent function of 6 variables. The AES algorithm uses a bent function of 8 variables [1]. The keys with a larger number of bits can be obtained by concatenating two or more bent functions. Since a quaternary bent function in n variables can be viewed as an encoding of two binary bent functions in $2n$ variables [10], [11], the proposed method can be used in such applications.

The presented algorithm is compared with our previous algorithm with exhaustive search for random discovering of bent functions in both domains [7]. The proposed algorithm using GF or RMF subsets reduces the number of possible positions of non-zero coefficients in the spectrum. By using vertical subsets for different values of the parameter k all bent functions can be constructed, since bent functions in these subsets are disjoint. This is however not the case with horizontal and grid subsets. The only case when these subsets cover all bent functions is when k_{min} takes the minimum value and k_{max} takes the maximum possible value for the order of the coefficients. The bent functions in these subsets are not disjoint. Very often some functions in one subset of constructed functions are contained in another subset. We do not present the experimental results with these values of parameters, because on the used hardware the computation time limit of 30 minutes is exceeded for both algorithms.

Table 9 Computation time of algorithm for construction of bent functions using GF and RMF subsets

parameters	computation time [s]			
p / n / domain	exhaustive	$V(8)$	$H(3,4)$	$G(8,3,4)$
3 / 4 / GF	0.018	0.003	0.001	0.002
3 / 5 / GF	0.031	0.024	0.014	0.019
3 / 6 / GF	2.743	2.415	1.115	2.112
4 / 3 / GF	0.004	0.001	0.001	0.001
4 / 4 / GF	0.041	0.032	0.025	0.028
3 / 4 / RMF	0.009	0.001	0.001	0.001
3 / 5 / RMF	0.022	0.018	0.011	0.016
3 / 6 / RMF	3.145	2.845	1.458	2.459
4 / 3 / RMF	0.008	0.001	0.001	0.001
4 / 4 / RMF	0.039	0.009	0.022	0.014

Note that in the proposed method, the parameters of subsets can be selected arbitrarily. These parameters directly determine the size of the search space. For different choices of the parameters, the search space ranges from the small size to the entire search space in the GF/RMF domain. For example, for ternary functions of 7 variables, the subset $H(2,2)$ results in a relatively small search space, because it contains only quadratic bent functions. In contrast, for the subset $H(1,4)$ the search space is huge, since the order of the coefficients can take a lot of different values, and therefore the number of different combinations increases exponentially.

It should be noticed that the computation times for construction of bent functions using GF and RMF subsets for all tests are always smaller than using the exhaustive search construction. This was expected since the search space using GF and RMF was reduced. Difference between GF and RMF domain is only obvious between quaternary functions for the vertical and grid subsets. This is due to the large number of functions in the vertical and grid RMF subsets where k is low. Note that for the larger k, the difference will be reversed.

7. Conclusion

This paper proposes a technique for efficient construction of multiple-valued bent functions in the GF and RMF domains. The algorithm is based on the random discovery of GF or RMF spectrum of bent function by using GF or RMF subsets. The technique is mainly focused on the reduction of the discovery search time. The GF and RMF subsets are based on the restrictions of the number and/or order of GF or RMF coefficients for bent functions. Using these restrictions, there are vertical, horizontal, and grid subsets of functions.

The proposed algorithm is implemented and experimentally tested for construction ternary and quaternary bent function with up to 6 variables. Experimental results confirm that the time required for construction of bent function when using GF or RMF subsets is smaller than when using random construction. It can be also seen that the proposed algorithm in the GF and RMF domains significantly reduces search space for bent function discovery.

Therefore, in practical application there is a need for using various GF or RMF subsets. Difference between construction of p-valued bent function in the GF and RMF domain is obviously large when p is non prime. It should be noticed that for same number of non-zero coefficients in the

spectrum, there are more bent functions in the RMF domain than in the GF domain. This is true only when the number of non-zero coefficients is small. Thus, when number of non-zero coefficients is small it is more efficient to use construction in the RMF domain. In other cases, the using of GF and RMF domain is equal.

Future work will be on extension of the proposed algorithm to various other spectral domains, like Haar, or Kronecker domains.

Acknowledgments

The work presented in this paper is part of the research of project III44006 for the period 2011-2020, funded by the Ministry of Education and Science of the Republic of Serbia.

References

[1] N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, 2015.
[2] S. Mesnager, Bent Functions, Fundamentals and Results, Springer International Publishing, 2016.
[3] S.W. Schneider, Finding Bent Functions using Genetic Algorithms, Master's thesis, Naval Postgraduate School, Monterey, USA, 2009.
[4] A. Grocholewska-Czurylo and J. Stoklosa, "Generating bent functions," Proc. Advanced Computer Systems Eighth International Conference, ACS2001, pp.361–370, Springer US, Mielno, Poland, 2002.
[5] J. Climent, F. Garcia, and V. Requena, "On the iterative construction of bent functions," ed. N. Mastorakis, A. Cecchi, Proc. 5th WSEAS Int. Conf. Inf. Security and Privacy, pp.15–18. Stevens Point, Wisconsin, United States, Nov. 2006.
[6] R.S. Stanković, J. Astola, and C. Moraga, Representation of Multiple-Valued Logic Functions, Synthesis Lectures on Digital Circuits and Systems, Morgan & Claypool Publishers, 2012.
[7] M. Radmanović and R.S. Stanković, "Discovery of Multiple-Valued Bent Functions in Galois Field and Reed-Muller-Fourier Domains," Proc. 47th IEEE Int. Symp. Multiple-Valued Logic (ISMVL2017), Novi Sad, Serbia, pp.143–148, 2017.
[8] M.M. Radmanović and R.S. Stanković, "Construction of Subsets of Bent Functions Satisfying Restrictions in the Reed–Muller Domain," Facta Universitatis – Series: Electronics and Energetics, vol.31, no.2, pp.207–222, 2018.
[9] M. Radmanović and R. Stanković, "Random generation of bent functions on multicore CPU platform," Proc. 51st Int. Sci. Conf. on Information, Communication and Energy Systems and Technologies (ICEST 2016), Ohrid, Macedonia, pp.239–242, 2016.
[10] P. Sole and N. Tokareva, "On quaternary and binary bent functions," Prikl. Diskr. Mat., supplement no.1, pp.16–18, 2009.
[11] P. Solé and N. Tokareva, "Connections between quaternary and binary bent functions," 2011 IEEE Int. Symp. Information Theory Proceedings, ISIT 2011, St. Petersburg, Russia, 2011.

Miloš M. Radmanović received the B.S., M.S. and Ph.D. degrees in Electronic engineering from the Faculty of Electronic Engineering, University of Niš, Serbia, in 2001, 2006, and 2015, respectively. Currently, he is an assistant professor in the Department of Computer Science, Faculty of Electronic Engineering, University of Niš, Serbia. His research interests include spectral techniques, switching theory and multiple-valued logic, and signal processing.

Radomir S. Stanković received the B.Sc. degree in electronic engineering from the Faculty of Electronics, University of Niš, Serbia, in 1976, and M.Sc. and Ph.D. degrees in applied mathematics from the Faculty of Electrical Engineering, University of Belgrade, Serbia, in 1984 and 1986, respectively. He was a Professor at the Department of Computer Science, Faculty of Electronics, University of Niš, Serbia, until 2017, and a Full research professor at the Mathematical Institute of SASA in Belgrade, Serbia, From 2017 until his retirement in 2019. In 1997, he was awarded by the Kyushu Institute of Technology Fellowship and worked as a visiting researcher at the Department of Computer Science and Electronics, Kyushu Institute of Technology, Iizuka, Fukuoka, Japan. In 2000 he was awarded by the Nokia Professorship by Nokia, Finland. From 1999 until 2017, he worked in part at the Tampere International Center for Signal Processing, Department of Signal Processing Faculty of Computing and Electrical Engineering, Tampere University of Technology, Tampere, Finland, first as a visiting researcher and from 2007 as an adjunct professor. His research interests include switching theory, multiple-valued logic, spectral techniques, and signal processing. A special field of his interest is history of computing.