




Vectorial Boolean functions with the maximum number of bent components beyond the Nyberg's bound

Amar Bapić¹ · Enes Pasalic¹ · Alexandr Polujan²  · Alexander Pott²

Received: 12 August 2022 / Revised: 1 December 2022 / Accepted: 23 December 2022 /
Published online: 15 February 2023
© The Author(s) 2023

Abstract

Recently, several interesting constructions of vectorial Boolean functions with the maximum number of bent components (MNBC functions, for short) were proposed. However, many of them have component functions from the completed Maiorana-McFarland class $\mathcal{M}^\#$. Moreover, no examples of MNBC functions containing component functions provably outside $\mathcal{M}^\#$ are known. In this paper, we classify all MNBC functions in six variables. Based on the analysis of the obtained equivalence classes, we propose several infinite families of MNBC functions with component functions outside the $\mathcal{M}^\#$ class. In particular, two of our new constructions are solutions to the open problem [Bapić et al (eds) Proceedings of the twelfth international workshop on coding and cryptography, 2022, Item 1., p. 9].

Keywords Bent function · Maximum number of bent components · Maiorana-McFarland class · EA-equivalence · CCZ-equivalence · Classification

Mathematics Subject Classification 05B10 · 06E30 · 14G50 · 94C30

This is one of several papers published in *Designs, Codes and Cryptography* comprising the “Special Issue: Coding and Cryptography 2022”.

✉ Alexandr Polujan
alexandr.polujan@ovgu.de

Amar Bapić
amar.bapic@famnit.upr.si

Enes Pasalic
enes.pasalic6@gmail.com

Alexander Pott
alexander.pott@ovgu.de

¹ University of Primorska, FAMNIT & IAM, Glagoljaška 8, 6000 Koper, Slovenia

² Otto von Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany

1 Introduction

Let \mathbb{F}_2^n be the vector space of dimension n over $\mathbb{F}_2 = \{0, 1\}$, which will be frequently endowed with the structure of the finite field $(\mathbb{F}_{2^n}, +, \cdot)$. An element $\alpha \in \mathbb{F}_{2^n}$ is said to be a *primitive element*, if it is a generator of the multiplicative group $\mathbb{F}_{2^n}^*$. For $m \mid n$, the *trace mapping* $Tr_m^n : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$ is given by $Tr_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{i \cdot m}}$. The mapping $Tr_1^n : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ is called the *absolute trace*.

A mapping $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ is called an (n, m) -*function*. For $m = 1$, a function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is called a *Boolean function* in n variables. With \mathcal{B}_n , we will denote the set of all Boolean functions in n variables. Any (n, m) -function F can be written as $F(x) = (f_1(x), \dots, f_m(x))$, where the Boolean functions f_i on \mathbb{F}_2^n are called *coordinate functions* of F . The *Walsh transform* $W_f : \mathbb{F}_{2^n} \rightarrow \mathbb{Z}$ of a Boolean function $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined by $W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + Tr_1^n(\lambda x)}$. A Boolean function $f \in \mathcal{B}_n$, where $n = 2k$, is called *bent* if $|W_f(\lambda)| = 2^{n/2}$ for all $\lambda \in \mathbb{F}_{2^n}$. Note that for n odd, such functions do not exist. For a Boolean bent function $f \in \mathcal{B}_n$, the Boolean function $\tilde{f} \in \mathcal{B}_n$ defined for any $u \in \mathbb{F}_{2^n}$ by $W_{\tilde{f}}(u) = 2^{\frac{n}{2}} (-1)^{\tilde{f}(u)}$, is also bent and is called the *dual* of f . The *algebraic normal form* (ANF, for short) of a Boolean function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is a multivariate polynomial in the ring $\mathbb{F}_2[x_1, \dots, x_n]/(x_1 + x_1^2, \dots, x_n + x_n^2)$, given by $f(x) = \sum_{a \in \mathbb{F}_2^n} c_a (\prod_{i=1}^n x_i^{a_i})$, where $x = (x_1, \dots, x_n)$, $a = (a_1, \dots, a_n) \in \mathbb{F}_2^n$. The *algebraic degree* of a Boolean function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, denoted by $\deg(f)$, is the algebraic degree of its ANF as a multivariate polynomial, that is, $\deg(f) = \max_{a \in \mathbb{F}_2^n} \{wt(a) : c_a \neq 0\}$, where $wt(a) = |\{i : a_i \neq 0, 1 \leq i \leq n\}|$. The *algebraic normal form* of a vectorial (n, m) -function F is defined coordinate-wise and its *algebraic degree* is defined as $\deg(F) := \max_{1 \leq i \leq m} \deg(f_i)$. The *first-order derivative* of an (n, m) -function F in direction $a \in \mathbb{F}_2^n$ is an (n, m) -function $D_a F(x) := F(x+a) + F(x)$. For $a, b \in \mathbb{F}_2^n$, the mapping $D_{a,b} F(x) := F(x+a+b) + F(x+a) + F(x+b) + F(x)$ is called the *second-order derivative* of an (n, m) -function F .

For (n, m) -functions, the bent property is introduced with the notion of *component functions* $F_\lambda \in \mathcal{B}_n$ defined by $F_\lambda(x) = Tr_1^m(\lambda F(x))$ for $\lambda \in \mathbb{F}_{2^m}^*$. An (n, m) -function is called (n, m) -*bent* (*vectorial bent* for $m \geq 2$), if for all $\lambda \in \mathbb{F}_{2^m}^*$, its component functions F_λ are Boolean bent. Vectorial (n, m) -bent functions exist only for $m \leq n/2$; this result is also known as the Nyberg’s Bound [16]. The *Maiorana-McFarland construction* of (n, m) -bent functions describes the functions of the form $G(x, y) = L(x\pi(y)) + g(y)$ for $x, y \in \mathbb{F}_{2^{n/2}}$, where π is a permutation on $\mathbb{F}_{2^{n/2}}$, L is a surjective linear $(n/2, m)$ -function, and g is an arbitrary $(n/2, m)$ -function. With the Nyberg’s bound, one can interpret the bent property of a vectorial function as follows. An (n, m) -function F with $m \leq n/2$ is vectorial bent, if it has the maximum number of bent components F_λ , which is equal to $2^m - 1$. Due to the non-existence of (n, m) -bent functions for $m > n/2$, the maximum number of bent components of (n, m) -functions with $m > n/2$ is less than $2^m - 1$.

In 2018, Pott et al. [22] addressed for the first time the question about the maximum number of bent components for vectorial functions beyond the Nyberg’s bound. It was shown that an (n, n) -function F can have at most $2^n - 2^{n-n/2}$ bent components and that this bound is sharp. This result was generalized in [27] for (n, m) -functions, for which the maximum number of bent components equals to $2^m - 2^{m-n/2}$.

Definition 1.1 Let $n = 2k$ and $m > k$. An (n, m) -function F is called an (n, m) -MNBC function, if it has the maximum number of bent components $2^m - 2^{m-k}$.

On the set of (n, m) -functions we define the following equivalence relations preserving the MNBC property [15, 22]. Two (n, m) -functions F and F' are called *EA-equivalent*, if

there exist two affine permutations $A_1: \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m, A_2: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ and an affine function $A_3: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ s.t. $A_1 \circ F \circ A_2 + A_3 = F'$; functions F and F' are called *CCZ-equivalent*, if there exists an affine permutation \mathcal{L} on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ s.t. $\mathcal{L}(\mathcal{G}_F) = \mathcal{G}_{F'}$, where $\mathcal{G}_F = \{(x, F(x)): x \in \mathbb{F}_{2^n}\}$ is the *graph* of F . Note that CCZ-equivalence is a coarser equivalence relation than EA-equivalence.

Since the introduction of MNBC functions, several constructions of these functions have been proposed. Among them, are several constructions in the univariate representation [15, 22, 26], the trivial construction and the Maiorana-McFarland construction. The *trivial construction* describes (n, m) -MNBC functions of the form $x \in \mathbb{F}_2^n \mapsto (b(x), 0)$, where b is a vectorial $(n, n/2)$ -bent function, while the *Maiorana-McFarland construction* describes (n, m) -MNBC functions of the form $(x, y) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{m/2}} \mapsto (G(x, y), h(y))$, where G is a Maiorana-McFarland $(n, n/2)$ -bent function and h is an arbitrary $(n/2, m)$ -function. In this article, we denote by \mathcal{M} both classes of (n, m) -bent and (n, m) -MNBC functions, and the set of (n, m) -functions EA-equivalent to the \mathcal{M} class is called the *completed Maiorana-McFarland class* and denoted by $\mathcal{M}^\#$. We say that an (n, m) -function F (either bent or MNBC) is *outside the $\mathcal{M}^\#$ class* if at least one bent component F_λ is outside $\mathcal{M}^\#$. The following lemma, due to Dillon [8], is of crucial importance for the discussion on inclusion in $\mathcal{M}^\#$.

Lemma 1.2 [8, p. 102] *A bent function f in n variables belongs to $\mathcal{M}^\#$ if and only if there exists an $(n/2)$ -dimensional vector subspace U of \mathbb{F}_2^n such that the second-order derivatives*

$$D_{a,b}f(x) = f(x) + f(x + a) + f(x + b) + f(x + a + b)$$

vanish for any $a, b \in U$.

The construction of (n, m) -MNBC functions outside the $\mathcal{M}^\#$ class is a difficult theoretical problem. As presented in [1], several nontrivial constructions of (n, m) -MNBC functions contain vectorial $(n, n/2)$ -bent functions, and hence many Boolean bent components from $\mathcal{M}^\#$ class. On the other hand, employing a trivial construction, it is also hard to construct (n, m) -MNBC functions outside the $\mathcal{M}^\#$ class, since only few examples of $(n, n/2)$ -bent functions outside $\mathcal{M}^\#$ are known [3, 19, 21]. In this article, we construct several infinite families of nontrivial MNBC functions outside the $\mathcal{M}^\#$ class using the extension approach, considered recently in [14, 19] in the context of vectorial bent functions. The main idea of our approach is to extend vectorial $(n, n/2)$ -bent functions by non-bent coordinates in such a way, that the remaining bent components fall into secondary constructions of Boolean bent functions outside the $\mathcal{M}^\#$ class, what guarantees that the obtained (n, m) -functions are MNBC and outside $\mathcal{M}^\#$.

The rest of the article is organized in the following way. In Sect. 2, we consider in detail the notion of a t -step extension MNBC function, which we use to distinguish inequivalent MNBC functions, and, particularly, to classify all MNBC functions in six variables. Moreover, we show that some of them are nontrivial and do not belong to the $\mathcal{M}^\#$ class. In the sequel, we present several theoretical constructions of such functions based on the analysis of several large classes of Boolean bent functions, namely, $\mathcal{PS}_{ap}, \mathcal{D}_0$ and \mathcal{C} . In Sect. 3, we propose a partial spread construction of 1-step extension MNBC functions based on \mathcal{PS}_{ap} vectorial bent functions. In Sect. 4, by applying similar techniques, we provide constructions of 1-step and 2-step extension MNBC functions outside $\mathcal{M}^\#$ based on the secondary constructions of Boolean bent functions, namely, $\mathcal{D}_0, \mathcal{C}$ and \mathcal{SC} classes. In Sect. 5, we combine several techniques presented in Sect. 4 for the construction of 1-step and 2-step extension MNBC functions and provide a construction of t -step extension (n, n) -MNBC functions outside the $\mathcal{M}^\#$ class, where $3 \leq t \leq n/6$. With these results, we give a solution to the open problem [4,

Item 1., p. 9]. The paper is concluded in Sect. 6 and representatives of equivalence classes of MNBC functions on \mathbb{F}_2^6 are given in Appendix 1.

2 Complete classification of MNBC functions in six variables

For vectorial Boolean functions with the maximum number of bent components below the Nyberg’s bound, i.e., vectorial bent functions, CCZ- and EA-equivalence coincide [6, 9, 12]. Recently, it was proven that for a vectorial function (beyond the Nyberg’s bound), the MNBC property is invariant under CCZ-equivalence [15]. In view of this recent result, it is reasonable to conjecture, that CCZ-equivalence and EA-equivalence coincide for MNBC functions beyond the Nyberg’s bound as well. Now we give an example of two EA-inequivalent, but CCZ-equivalent MNBC functions in six variables.

Example 2.1 Let $x \in \mathbb{F}_2^6$ and $y \in \mathbb{F}_2^4$ be written as column-vectors. Consider the following MNBC functions $F: \mathbb{F}_2^6 \rightarrow \mathbb{F}_2^4$ and $F': \mathbb{F}_2^6 \rightarrow \mathbb{F}_2^4$ given by algebraic normal forms:

$$F(x) = \begin{pmatrix} x_1x_4 + x_2x_5 + x_3x_6 \\ x_1x_5 + x_1x_6 + x_2x_4 + x_2x_5 + x_3x_4 \\ x_1x_4 + x_1x_5 + x_2x_4 + x_2x_5 + x_2x_6 + x_3x_5 \\ x_1x_2 + x_1x_5 + x_1x_6 + x_2x_4 + x_2x_5 + x_3x_4 \end{pmatrix},$$

$$F'(x) = \begin{pmatrix} x_1x_2x_3 + x_1x_4 + x_2x_5 + x_3x_6 \\ x_1x_2x_4 + x_1x_3 + x_1x_5 + x_2x_3 + x_4x_6 \\ x_1x_2x_5 + x_1x_3 + x_2x_4 + x_2x_5 + x_5x_6 \\ x_1x_2x_3 + x_1x_2 + x_1x_4 + x_2x_5 + x_3x_6 \end{pmatrix}.$$

It is easy to see, that $\text{deg}(F) = 2$ and $\text{deg}(F') = 3$, from what follows that F and F' are EA-inequivalent. However, as we show now, the functions F and F' are CCZ-equivalent. Consider the following affine permutation \mathcal{L} on $\mathbb{F}_2^6 \times \mathbb{F}_2^4$, which is given by

$$\mathcal{L}(x, y) = \begin{pmatrix} x_2 \\ 1 + x_1 + x_2 \\ x_1 + x_5 + x_6 \\ 1 + x_3 + x_4 \\ x_2 + x_3 + x_5 \\ 1 + x_2 + x_3 + y_2 + y_4 \\ x_1 + x_2 + x_3 + x_6 + y_1 + y_3 \\ 1 + x_3 + x_4 + x_5 + x_6 + y_2 \\ 1 + x_1 + x_2 + x_4 + y_3 \\ x_1 + x_2 + x_3 + x_6 + y_1 + y_2 + y_3 + y_4 \end{pmatrix}^T,$$

for $x \in \mathbb{F}_2^6$ and $y \in \mathbb{F}_2^4$. With a computer algebra system, one can check that the sets $\{\mathcal{L}(x, F(x)) : x \in \mathbb{F}_2^6\}$ and $\{(x, F'(x)) : x \in \mathbb{F}_2^6\}$ are equal, thus $\mathcal{L}(\mathcal{G}_F) = \mathcal{G}_{F'}$, and hence F and F' are CCZ-equivalent. With the mapping \mathcal{L} , the functions F and F' are related in the following way. As described in [9, Sect. 7], the mapping \mathcal{L} can be represented as $\mathcal{L}(x, y) = (A_{11}x + A_{12}y + a, A_{21}x + A_{22}y + b)$, where $a = (0, 1, 0, 1, 0, 1)^T \in \mathbb{F}_2^6$, $b = (0, 1, 1, 0)^T \in \mathbb{F}_2^4$, and the matrices $A_{11} \in \mathbb{F}_2^{(6,6)}$, $A_{12} \in \mathbb{F}_2^{(6,4)}$, $A_{21} \in \mathbb{F}_2^{(4,6)}$, $A_{22} \in \mathbb{F}_2^{(4,4)}$

are given by

$$A_{11} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}, A_{12} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{pmatrix}, A_{21} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}, A_{22} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

With the defined above vectors and matrices, it is possible to show that the equality

$$F'(A_{11}x + A_{12}F(x) + a) = A_{21}x + A_{22}F(x) + b$$

holds for all $x \in \mathbb{F}_2^6$.

Remark 2.2 With Example 2.1, we conclude that CCZ-equivalence is more general than EA-equivalence for the class of MNBC functions.

Recently, the complete classification of vectorial bent functions in six variables [19, 21], as well as of quadratic vectorial bent functions in eight variables [18] was obtained. With the same approach, we classify all MNBC functions on \mathbb{F}_2^6 and check, which of them belong to the $\mathcal{M}^\#$ class. First, we give the following definition.

Definition 2.3 Let F be an (n, m) -MNBC function, where $n/2 + 1 \leq m \leq n$. Let the linear code C_F over \mathbb{F}_2 be defined as the row space of the $(n + m + 1) \times 2^n$ -matrix over \mathbb{F}_2 with columns $(1, x, F(x))_{x \in \mathbb{F}_2^n}^T$. We call an (n, m) -MNBC function F a t -step extension if $\dim(C_F) = 1 + n + n/2 + t$, where $1 \leq t \leq n/2$.

Remark 2.4 1. Let F be a t -step extension (n, m) -MNBC function. The value t gives a measure of non-triviality of MNBC-functions. With Definition 2.3, an (n, m) -MNBC function is trivial, if it is a 0-step extension.

2. Note that if two MNBC functions F and F' are t -step and t' -step extension with $t \neq t'$, then F and F' are CCZ-inequivalent, since inequivalent linear codes C_F and $C_{F'}$ define CCZ-inequivalent functions [9, Theorem 9].

3. Let $1 \leq t \leq n/2 - 1$. Given a t -step extension (n, m) -MNBC function F , it is easy to obtain a $(t - 1)$ -step extension (n, m) -MNBC function F' , by removing a suitable non-bent component function of F . On the other hand, it seems to be a difficult problem to find a function $f \in \mathcal{B}_n$ such that the function $F'' : x \mapsto (F(x), f(x))$ is a $(t + 1)$ -step extension $(n, m + 1)$ -MNBC function.

In the following proposition, we summarize our computational results about the classification of MNBC functions in six variables.

Proposition 2.5 On \mathbb{F}_2^6 , there exist 40 CCZ-equivalence classes of MNBC functions. Among them, there are:

1. 13 CCZ-equivalence classes of 0-step extension; these are the (6, 3)-bent functions in [21, Table A2(c)].
2. 17 CCZ-equivalence classes of 1-step extension.
3. 7 CCZ-equivalence classes of 2-step extension.
4. 3 CCZ-equivalence classes of 3-step extension.

If an MNBC function F on \mathbb{F}_2^6 is a 2-step or a 3-step extension, then $F \in \mathcal{M}^\#$.

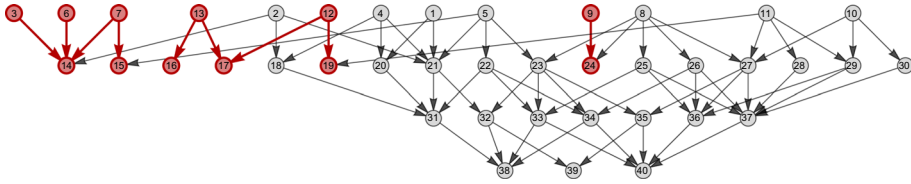


Fig. 1 The structure of CCZ-equivalence classes of $(6, m)$ -MNBC functions. If an equivalence class i is extendable to an equivalence class j , we put a directed edge between them. The equivalence classes denoted by gray are inside $\mathcal{M}^\#$ and by red are outside $\mathcal{M}^\#$ (Color figure online)

Now we briefly discuss the main steps of the used approach. Since any (n, m) -MNBC function F has $2^{m-n/2}$ non-bent components, which form an $(m - n/2)$ -dimensional vector space [22, 27], one can represent F in the form

$$F(x) = (b_1(x), \dots, b_{n/2}(x), n_1(x), \dots, n_{m-n/2}(x)),$$

where all b_i are bent, all n_j are non-bent and $\langle n_1, \dots, n_{m-n/2} \rangle$ is a vector space of non-bent functions of dimension $m - n/2$. Applying a non-degenerate linear transformation to the output of F , we get

$$F'(x) = (b_1(x), \dots, b_{n/2}(x), b_{n/2+1}(x), \dots, b_m(x)),$$

where $b_{n/2+i} := b_i + n_i$ is bent for $1 \leq i \leq m - n/2$, since by [27, Theorem 3.1], all non-bent components of F belong to $\langle n_1, \dots, n_{m-n/2} \rangle$. In this way, we may assume that all coordinate functions of an MNBC function F are bent. Consequently, any (n, m) -MNBC function F can be represented as $F(x) = (\bar{F}(x), f(x))$, where $\bar{F}(x)$ is an $(n, m - 1)$ -MNBC function and f is a Boolean bent function on \mathbb{F}_2^n (for $m = n/2 + 1$ we let \bar{F} be $(n, n/2)$ -bent). In this case, we say that \bar{F} is extendable to F . With this representation of MNBC functions, we start with inequivalent vectorial $(6, 3)$ -bent functions from [21] and extend them recursively to $(6, m)$ -MNBC functions by appending at each step a Boolean bent function without affine terms exhaustively. The extension relation between the obtained CCZ-equivalence classes is given in Fig. 1.

We check CCZ-equivalence of MNBC functions F and F' via equivalence of linear codes C_F and $C_{F'}$ (see [9, Theorem 9]) with the algebra system Magma [5]. With the implementation [20, Algorithm 1] of Lemma 1.2 applied coordinate-wise to all EA-inequivalent MNBC functions contained in a CCZ-equivalence class, we check whether a given CCZ-equivalence class belongs to $\mathcal{M}^\#$. Finally, we list representatives of the obtained CCZ-equivalence classes in the Appendix.

Remark 2.6 1. Alternatively to [20, Algorithm 1], one can use a graph-theoretic approach in order to check, whether a given bent function f on \mathbb{F}_2^n belongs to $\mathcal{M}^\#$. Let $G = (V, E)$ be a graph with the vertex-set $V = \mathbb{F}_2^n$ and the edge-set $E = \{\{a, b\} \in V \times V : D_{a,b}f = 0\}$. Then the existence of a vector space $U \subset \mathbb{F}_2^n$ with $\dim(U) = n/2$ s.t. $D_{a,b}f = 0$ for any $a, b \in U$ is equivalent to the existence of a clique U of size $2^{n/2}$ in G , whose elements form a vector space of dimension $n/2$. For details on the implementation, we refer to [17].

2. On \mathbb{F}_2^6 , there are 17 CCZ-equivalence classes of 1-step extension MNBC functions, and there are 23 EA-equivalence classes of 1-step extension MNBC functions. CCZ-equivalence classes 14 and 21 contain 3 EA-equivalence classes (each), CCZ-equivalence classes 23 and 27 contain 2 EA-equivalence classes (each), and every other CCZ-equivalence class i with $14 \leq i \leq 30$ contains exactly one EA-equivalence class.

Finally, we suggest to work on the following problem in order to shed more light on the phenomenon observed in Example 2.1.

Openproblem 2.7 Find explicit constructions of (n, m) -MNBC functions for all $n \geq 6$ and $n/2 + 1 \leq m \leq n$, which are EA-inequivalent, but CCZ-equivalent.

3 MNBC functions from the \mathcal{PS}_{ap} class

In order to introduce a partial spread construction of MNBC functions, we first give a definition of a partial spread.

Definition 3.1 A partial spread of order s in \mathbb{F}_2^n with $n = 2k$ is a set of s vector subspaces U_1, \dots, U_s of \mathbb{F}_2^n of dimension k each, such that $U_i \cap U_j = \{0\}$ for all $i \neq j$. The partial spread of order $s = 2^k + 1$ in \mathbb{F}_2^n with $n = 2k$ is called a spread.

In the following, we denote by $\mathbb{1}_U : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ the indicator function of $U \subseteq \mathbb{F}_2^n$, i.e., $\mathbb{1}_U(x) = 1$ if $x \in U$, and 0 otherwise. Using the notion of a partial spread, Dillon [8] introduced a partial spread construction of bent functions, which splits the following two classes:

- The \mathcal{PS}^+ class is the set of Boolean bent functions of the form

$$f(x) = \sum_{i=1}^{2^{k-1}+1} \mathbb{1}_{U_i}(x),$$

where the vector spaces $U_1, \dots, U_{2^{k-1}+1}$ of \mathbb{F}_2^n form a partial spread in \mathbb{F}_2^n .

- The \mathcal{PS}^- class is the set of Boolean bent functions of the form

$$f(x) = \sum_{i=1}^{2^{k-1}} \mathbb{1}_{U_i^*}(x),$$

where the vector spaces $U_1, \dots, U_{2^{k-1}}$ of \mathbb{F}_2^n form a partial spread in \mathbb{F}_2^n and $U_i^* := U_i \setminus \{0\}$.

The Desarguesian partial spread class $\mathcal{PS}_{ap} \subset \mathcal{PS}^-$ is the set of Boolean bent functions f on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ of the form $f : (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \mapsto h(x/y)$, where $\frac{x}{0} = 0$, for all $x \in \mathbb{F}_{2^k}$ and $h : \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2$ is a balanced Boolean function with $h(0) = 0$. Similarly to the Boolean case, the Desarguesian partial spread class \mathcal{PS}_{ap} of (n, k) -bent functions with $k = n/2$ is defined as the set of (n, k) -functions F on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ of the form $F : (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \mapsto H(x/y)$, where $x/y = 0$ if $y = 0$ for $x, y \in \mathbb{F}_{2^k}$ and H is a permutation on \mathbb{F}_{2^k} s.t. $H(0) = 0$.

In the following theorem, we give the partial spread construction of MNBC functions.

Theorem 3.2 Let $n = 2k$ and let G be a vectorial (n, k) -bent function from the \mathcal{PS}_{ap} class. Let also U be a spread line of the form $U = \{(0, y) : y \in \mathbb{F}_{2^k}\}$. Then the function $F : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2^{k+1}$ defined as

$$F(x, y) = (G(x, y), \mathbb{1}_U(x, y)) \tag{1}$$

is an $(n, k + 1)$ -MNBC function.

Proof Since $\mathbb{1}_U \in \mathcal{B}_n$ is the indicator of the vector space U of dimension k , we have $\text{wt}(\mathbb{1}_U) = 2^k$ and hence $\mathbb{1}_U$ is not bent. In this way, it is enough to show that for any \mathcal{PS}_{ap} Boolean

bent function g on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, which is a bent component of the function G , the function $g + \mathbb{1}_U$ on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ is bent. For $a, b \in \mathbb{F}_{2^k}$, we compute the Walsh transform $W_{g+\mathbb{1}_U}(a, b)$ of $g + \mathbb{1}_U$ at $a, b \in \mathbb{F}_{2^k}$, by considering the following two cases.

Case 1 Let $a, b \in \mathbb{F}_{2^k}$ with $b \neq 0$. The Walsh transform of $g + \mathbb{1}_U$ is given by

$$\begin{aligned} W_{g+\mathbb{1}_U}(a, b) &= \sum_{x, y \in \mathbb{F}_{2^k}} (-1)^{g(x, y) + \mathbb{1}_U(x, y) + Tr_1^k(ax + by)} \\ &= \sum_{y \in \mathbb{F}_{2^k}} (-1)^{g(0, y) + \mathbb{1}_U(0, y) + Tr_1^k(by)} \\ &\quad + \sum_{x \in \mathbb{F}_{2^k}^*} \sum_{y \in \mathbb{F}_{2^k}} (-1)^{g(x, y) + \mathbb{1}_U(x, y) + Tr_1^k(ax + by)} = W_g(a, b) = \pm 2^k, \end{aligned}$$

since $\sum_{y \in \mathbb{F}_{2^k}} (-1)^{g(0, y) + \mathbb{1}_U(0, y) + Tr_1^k(by)} = -\sum_{y \in \mathbb{F}_{2^k}} (-1)^{Tr_1^k(by)} = 0$ (because $b \neq 0$), and the function g is bent on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

Case 2 Let $a, b \in \mathbb{F}_{2^k}$ with $b = 0$. The Walsh transform of $g + \mathbb{1}_U$ is given by

$$\begin{aligned} W_{g+\mathbb{1}_U}(a, 0) &= \sum_{x, y \in \mathbb{F}_{2^k}} (-1)^{g(x, y) + \mathbb{1}_U(x, y) + Tr_1^k(ax)} \\ &= \sum_{y \in \mathbb{F}_{2^k}} (-1)^{g(0, y) + \mathbb{1}_U(0, y)} + \sum_{x \in \mathbb{F}_{2^k}^*} \sum_{y \in \mathbb{F}_{2^k}} (-1)^{g(x, y) + \mathbb{1}_U(x, y) + Tr_1^k(ax)} \\ &= -2^k + W_g(a, 0) - 2^k. \end{aligned}$$

Since for \mathcal{PS}_{ap} bent function g on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ the Walsh transform $W_g(a, 0) = +2^k$ for any $a \in \mathbb{F}_{2^k}$, we have that $W_{g+\mathbb{1}_U}(a, 0) = -2^k$. This completes the proof. \square

Remark 3.3 1. In the same way, it is possible to show that for the spread line $U = \{(x, 0) : x \in \mathbb{F}_{2^k}\}$ the $(n, k + 1)$ -function F of the form (1) is MNBC. 2. The bent component functions of MNBC functions of the form (1) belong to the \mathcal{PS}_{ap} and \mathcal{PS}^+ classes. Addition of the indicator of the spread line $\mathbb{F}_{2^k} \times \{0\}$ or the indicator of $\{0\} \times \mathbb{F}_{2^k}$ to a \mathcal{PS}_{ap} bent function g on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ gives a bent function in \mathcal{PS}^+ class, because the \mathcal{PS}_{ap} bent function g is constant 0 on the mentioned spread lines. Similarly, one can use other spreads (not necessarily Desarguesian) for the construction of MNBC functions.

3. Weng, Feng and Qiu [24] proved that almost every \mathcal{PS}_{ap} bent function on \mathbb{F}_2^n is outside $\mathcal{M}^\#$. Since $2^{n/2} - 1$ component functions of MNBC functions of the form (1) belong to \mathcal{PS}_{ap} , we have that almost every MNBC function of this form is outside $\mathcal{M}^\#$. Remarkably, with this construction one can extend a vectorial bent function in $\mathcal{PS}_{ap} \cap \mathcal{M}^\#$ to an MNBC function outside $\mathcal{M}^\#$, as the example of equivalence classes 11 and 19 in Fig. 1 shows; this is the only such an example in six variables, since the only equivalence classes of $(6, 3)$ -bent functions inside \mathcal{PS}_{ap} are 11, 12 and 13 (see Fig. 1 and [21, Table IV.2]).

4. Any \mathcal{PS}_{ap} vectorial bent function $(x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \mapsto H(x/y)$ in $n = 2k = 6$ variables can be extended to at least two inequivalent 1-step extension MNBC functions from the \mathcal{PS}_{ap} class. With Magma [5], one can show that for any permutation H on \mathbb{F}_{2^k} , MNBC functions of the form

$$\begin{aligned} F : (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} &\mapsto (H(x/y), \mathbb{1}_U(x, y)), \\ F' : (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} &\mapsto (H(x/y), \mathbb{1}_V(x, y)), \end{aligned} \tag{2}$$

where $U = \{(0, y) : y \in \mathbb{F}_{2^k}\}$ and $V = \{(x, 0) : x \in \mathbb{F}_{2^k}\}$, are CCZ-inequivalent.

Conjecture 1 In view of the last observation in Remark 3.3, we conjecture that MNBC functions F and F' defined by (2) are inequivalent for any permutation H on \mathbb{F}_{2^k} .

4 MNBC functions from secondary constructions of Boolean bent functions

In this section, using secondary constructions of Boolean bent functions, we construct three families of MNBC functions: two families of 1-step extension stemming from \mathcal{D}_0 and \mathcal{C} classes, and one family of 2-step extension stemming from the SC class, which is a superclass of \mathcal{D}_0 and \mathcal{C} .

4.1 MNBC functions stemming from the \mathcal{D}_0 class

In the following, we define $\delta_0 \in \mathcal{B}_k$ to be the indicator of $0 \in \mathbb{F}_{2^k}$, i.e., $\delta_0 = \mathbb{1}_{\{0\}}$. With this notation, Boolean functions $f: \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2$ of the form

$$f(x, y) = Tr_1^k(x\pi(y)) + \delta_0(x) \quad \text{for } x, y \in \mathbb{F}_{2^k}, \tag{3}$$

where π is a permutation on \mathbb{F}_{2^k} , are bent and the set of bent functions of the form (3) is called the \mathcal{D}_0 class of Boolean bent functions [7]. Carlet [7] proved, that bent functions of the form (3), where π is a quadratic permutation such that there is no affine hyperplane of \mathbb{F}_{2^k} on which π is affine, do not belong to the $\mathcal{M}^\#$ class. In a recent work [11], the authors provided a complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^\#$, which we summarize in the following theorem.

Theorem 4.1 [11, Theorems 5,7] *Let k be an integer, $k \geq 4$. Let π be a permutation of \mathbb{F}_{2^k} with one of the following two properties:*

1. *The algebraic degree of π satisfies $\text{deg}(\pi) \geq 3$;*
2. *The permutation π is quadratic and there is no affine hyperplane of \mathbb{F}_{2^k} on which π is affine.*

Then the function $f: \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2$ defined by $f(x, y) = Tr_1^k(x\pi(y)) + \delta_0(x)$ for $x, y \in \mathbb{F}_{2^k}$ is a bent function in \mathcal{D}_0 outside $\mathcal{M}^\#$. Moreover, the second condition is also a necessary one for quadratic permutations.

With the use of bent functions from $\mathcal{D}_0 \setminus \mathcal{M}^\#$ class, we derive the following family of MNBC functions.

Theorem 4.2 *Let $n = 2k \geq 8$ and let $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$. Let π be a permutation on \mathbb{F}_{2^k} satisfying one of conditions of Theorem 4.1. Then the (n, n) -function F defined by*

$$F(x, y) = x\pi(y) + \gamma\delta_0(x) \text{ for } x, y \in \mathbb{F}_{2^k}, \tag{4}$$

is a 1-step extension (n, n) -MNBC function outside the $\mathcal{M}^\#$ class.

Proof First, we show that the function F has the maximum number of bent components and is outside $\mathcal{M}^\#$. Let $\lambda \in \mathbb{F}_{2^n}^*$ be arbitrary. Then

$$F_\lambda(x, y) = Tr_1^k(x\pi(y)Tr_k^n(\lambda)) + \delta_0(x)Tr_1^n(\lambda\gamma)$$

is not bent if and only if $Tr_k^n(\lambda) = 0$. This holds, if $\lambda \in \mathbb{F}_{2^k}^*$. Thus, there are $(2^n - 1) - (2^k - 1) = 2^n - 2^k$ bent components. Since $|\{x \in \mathbb{F}_{2^n} : Tr_1^n(\gamma x) = 1\}| = |\{x \in \mathbb{F}_{2^n} : Tr_1^n(\gamma x) = 0\}| = 2^{n-1}$, there exist at least $2^n - 2^k - 2^{n-1} = 2^k(2^{k-1} - 1)$ many $\lambda \notin \mathbb{F}_{2^k}$ such that $Tr_1^n(\lambda\gamma) = 1$. In this case, we have that $F_\lambda \in \mathcal{D}_0 \setminus \mathcal{M}^\#$. Now we show that F is a 1-step extension. Since $G(x, y) := x\pi(y)$ is an (n, k) -function, we can write $G(x, y) = (g_1(x, y), \dots, g_k(x, y))$, where $g_1, \dots, g_k : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2$. Since $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, we can construct the function F' in the following form

$$F'(x, y) = (g_1(x, y), \dots, g_k(x, y), \delta_0(x)).$$

Thus, F' is an MNBC $(n, k + 1)$ -function, since the non-bent component functions of F' are 0 and δ_0 . Furthermore, we note that the dimension of the linear code $\mathcal{C}_{F'}$ is given by $\dim(\mathcal{C}_{F'}) = 1 + n + k + 1$ which, by definition, means that F' is a nontrivial MNBC $(n, k + 1)$ -function. Consequently, the MNBC (n, n) -function F is a 1-step extension. \square

4.2 MNBC functions stemming from the \mathcal{C} class

In this section, we present several infinite families of MNBC functions provably outside the $\mathcal{M}^\#$ class based on the generic construction of MNBC functions introduced in [2]. This construction is based on the property (P_U) , which was introduced in [23] and has several applications in the construction of vectorial Boolean bent functions [26] and MNBC functions [2].

Definition 4.3 Let $n, \tau \in \mathbb{N}$ with n even and $\tau \leq n/2$ and let $g \in \mathcal{B}_n$. Then g is said to satisfy property (P_U) with the defining set $U = \{u_1, \dots, u_\tau\} \subset \mathbb{F}_{2^n}$ if for all $1 \leq i < j \leq \tau$ the equation $g(x + u_i + u_j) + g(x + u_i) + g(x + u_j) + g(x) = 0$ holds for all $x \in \mathbb{F}_{2^n}$.

In [2], Bapić and Pasalic generalized the results of [26] and provided the following generic method for the construction of MNBC functions. Below we give a slightly reformulated version of [2, Construction 2].

Construction 4.4 Let $n = 2k$ and let $U = \{u_1, \dots, u_\tau\}$ be a set of $\tau \leq k$ linearly independent elements in \mathbb{F}_{2^n} . Let $G : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^k}$ be any vectorial bent function whose dual bent components $\tilde{G}_\lambda, \lambda \in \mathbb{F}_{2^k}^*$ satisfy the property (P_U) with the defining set U . Let $s | k$ and let $\mathbf{h} : \mathbb{F}_2^s \rightarrow \mathbb{F}_{2^s}$ be any (τ, s) -function. Then for any $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, the function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ defined as follows

$$F(x) = G(x) + \gamma \mathbf{h}(Tr_1^n(u_1x), \dots, Tr_1^n(u_\tau x)), \tag{5}$$

has the maximum number of bent components.

In [2], it was shown that several Maiorana-McFarland vectorial bent functions $G : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$ satisfy the conditions of Construction 4.4. Now we show that for these vectorial bent functions $G : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^k}$ one can specify a vectorial function \mathbf{h} , such that MNBC functions, obtained via Construction 4.4, are outside the $\mathcal{M}^\#$ class. The choice of the function \mathbf{h} is strongly related with \mathcal{C} and \mathcal{D}_0 classes of Boolean bent functions, which contain functions provably outside $\mathcal{M}^\#$.

Recall that the \mathcal{C} class of bent functions introduced by Carlet [7] is the set of Boolean functions $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2$ of the form

$$f(x, y) = Tr_1^k(x\pi(y)) + \mathbb{1}_{L^\perp}(x), \tag{6}$$

where L is any vector subspace of \mathbb{F}_{2^k} , $\mathbb{1}_{L^\perp}$ is the indicator function of the *orthogonal complement* $L^\perp = \{x \in \mathbb{F}_{2^k} : Tr_1^k(xy) = 0, \forall y \in L\}$, and π is any permutation on \mathbb{F}_{2^k} such that

$$(C) \quad \pi^{-1}(a + L) \text{ is a flat (affine subspace), for all } a \in \mathbb{F}_{2^k}.$$

The permutation π^{-1} and the subspace L are then said to satisfy the (C) property. For short, we also write (π^{-1}, L) has *property (C)*. Recall that a Boolean function $f \in \mathcal{B}_n$ has a *linear structure* if there exists an element $a \in \mathbb{F}_{2^n}^*$ such that $x \mapsto f(x + a) + f(x)$ is a constant function. In [25], the following set of sufficient conditions for Boolean bent functions in $\mathcal{C} \setminus \mathcal{M}^\#$ class was proposed.

Theorem 4.5 [25, Theorem 1] *Let $n = 2k \geq 8$ be an even integer and let $f(x, y) = Tr_1^k(x\pi(y)) + \mathbb{1}_{L^\perp}(x)$, where $x, y \in \mathbb{F}_{2^k}$, L is any vector subspace of \mathbb{F}_{2^k} and π is a permutation on \mathbb{F}_{2^k} s.t. (π^{-1}, L) has property (C). If $\dim(L) \geq 2$ and for all $\lambda \in \mathbb{F}_{2^k}^*$ the function $x \in \mathbb{F}_{2^k} \mapsto Tr_1^k(\lambda\pi(x))$ has no nonzero linear structure, then $f \notin \mathcal{M}^\#$.*

Using Construction 4.4 and Theorem 4.5, we obtain the following family of MNBC functions outside the $\mathcal{M}^\#$ class.

Theorem 4.6 *Let $U = \{u_1, \dots, u_\tau\}$ be a set of τ linearly independent elements in $\mathbb{F}_{2^k}^*$, where $n = 2k \geq 8$ and $\tau \mid k$. Let π be a permutation on \mathbb{F}_{2^k} and $G(x, y) = x\pi(y)$, where $x, y \in \mathbb{F}_{2^k}$, be an (n, k) -bent function whose dual bent components $\tilde{G}_\lambda, \lambda \in \mathbb{F}_{2^k}^*$, satisfy the property (P_U) with the defining set U . Let $\mathbf{h} \in \mathcal{B}_\tau$ be defined by its ANF as follows*

$$\mathbf{h}(x_1, \dots, x_\tau) = \prod_{i=1}^\tau (x_i + 1). \tag{7}$$

If $((\lambda\pi)^{-1}, \langle U \rangle)$ satisfies the (C) property and the conditions of Theorem 4.5 for all $\lambda \in \mathbb{F}_{2^k}^$, then the (n, n) -function F constructed from G and \mathbf{h} as*

$$F(x, y) = G(x, y) + \gamma \mathbf{h}(Tr_1^k(u_1x), \dots, Tr_1^k(u_\tau x)), \tag{8}$$

where $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, is a 1-step extension (n, n) -MNBC function outside $\mathcal{M}^\#$.

Proof From Construction 4.4, it follows that the function F is an (n, n) -MNBC function. The function \mathbf{h} , defined in such a way, represents the indicator function of the subspace $\langle U \rangle^\perp$ of \mathbb{F}_{2^k} . If $Tr_1^k(\lambda\gamma) = 1$ for $\lambda \in \mathbb{F}_{2^k}^*$, then $F_\lambda(x, y) = Tr_1^k(x\lambda\pi(y)) + \mathbb{1}_{\langle U \rangle^\perp}(x)$. Since $((\lambda\pi)^{-1}, \langle U \rangle)$ satisfies the (C) property and the conditions of Theorem 4.5 for all $\lambda \in \mathbb{F}_{2^k}^*$, it follows that $F_\lambda \in \mathcal{C} \setminus \mathcal{M}^\#$. If $Tr_1^k(\lambda\gamma) = 0$ then $F_\lambda \in \mathcal{M}^\#$, hence F is outside $\mathcal{M}^\#$. Now we show that F is a 1-step extension. Since $G(x, y) := x\pi(y)$ is an (n, k) -function, we can write $G(x, y) = (g_1(x, y), \dots, g_k(x, y))$, where $g_i : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2$ for all $1 \leq i \leq k$. Since $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, we can construct the function F' (see Remark 2.4) in the following form $F'(x, y) = (g_1(x, y), \dots, g_k(x, y), g_{k+1}(x, y))$, where the function g_{k+1} is defined by $g_{k+1}(x, y) := \mathbf{h}(Tr_1^k(u_1x), \dots, Tr_1^k(u_\tau x))$. Thus, F' is an $(n, k + 1)$ -MNBC function, since the non-bent components of F' are 0 and g_{k+1} . Finally, since $\mathcal{C}_F = \mathcal{C}_{F'}$, we have that $\dim(\mathcal{C}_F) = \dim(\mathcal{C}_{F'}) = 1 + n + k + 1$, consequently the (n, n) -MNBC function F is a 1-step extension. □

Following the proof of [3, Proposition 3], we give the following family of 1-step extension (n, n) -MNBC functions outside $\mathcal{M}^\#$ by specifying the permutation π to be a power mapping.

Proposition 4.7 *Let $k \geq 4$ and s be a positive divisor of k such that k/s is odd. Let $U = \{1, \alpha, \dots, \alpha^{\tau-1}\}$ be a set of τ linearly independent elements in $\mathbb{F}_{2^s}^*$, α is a primitive element in \mathbb{F}_{2^s} and $\tau \mid k$. Let $G(x, y) = x\pi(y)$, where $x, y \in \mathbb{F}_{2^k}$, $\pi(y) = y^d$ is a permutation on \mathbb{F}_{2^k} for a positive integer d such that $\text{wt}(d) \geq 3$ and $d(2^s + 1) \equiv 1 \pmod{2^k - 1}$. Then $(\pi^{-1}, \langle U \rangle)$, satisfies the (C) property and for any $\gamma \notin \mathbb{F}_{2^k}$, the function*

$$F(x, y) = xy^d + \gamma \mathbf{h}(Tr_1^k(x), Tr_1^k(\alpha x), \dots, Tr_1^k(\alpha^{\tau-1}x)),$$

where \mathbf{h} is defined by (7), is a 1-step extension (n, n) -MNBC function outside the $\mathcal{M}^\#$ class.

Proof By [2, Proposition 3], the dual bent components \tilde{G}_λ of G satisfy the property (P_U) with the defining set U given above for any $\lambda \in \mathbb{F}_{2^k}^*$. Thus, from Construction 4.4, it follows that the function F is an (n, n) -MNBC function. We will show that F is outside $\mathcal{M}^\#$. Let $\lambda \in \mathbb{F}_{2^k}^*$ be arbitrary. If $Tr_1^k(\lambda\gamma) = 0$, we have that $F_\lambda(x, y) = G_\lambda(x, y) \in \mathcal{M}^\#$. Suppose that $Tr_1^k(\lambda\gamma) = 1$, then $F_\lambda(x, y) = Tr_1^k(\lambda xy^d) + \mathbb{1}_{\langle U \rangle^\perp}(x)$. For any permutation π on \mathbb{F}_{2^k} , let $\sigma_\lambda(y) := \lambda\pi(y)$. Note that $\sigma_\lambda^{-1}(y) = \pi^{-1}(\lambda^{-1}y)$. Let $\pi(y) = y^d$, where d is defined above. Then, $\sigma_\lambda^{-1}(y) = \lambda^{-2^s-1}\pi^{-1}(y)$, where $\pi^{-1}(y) = y^{2^s+1}$. We will show that $(\sigma_\lambda^{-1}, \langle U \rangle)$ satisfies the (C) property. Let $a \in \mathbb{F}_{2^k}$ be arbitrary. Then

$$\sigma_\lambda^{-1}(a + \langle U \rangle) = \lambda^{-2^s-1}(a + \langle U \rangle)^{2^s+1} = \lambda^{-s}\pi^{-1}(a + \langle U \rangle)$$

is a flat as $\pi^{-1}(a + \langle U \rangle)$ is a flat by [13, Theorem 5.8]. Since $\text{wt}(d) \geq 3$, by [25, Proposition 5] it follows that $Tr_1^k(\lambda\pi)$ has no nonzero linear structures. Thus, by Theorem 4.5 it follows that F_λ is in \mathcal{C} outside $\mathcal{M}^\#$. Hence, F is outside $\mathcal{M}^\#$. Finally, from Theorem 4.6, we conclude that F is a 1-step extension. □

4.3 MNBC functions stemming from the SC class

In [3, Sect. 3], the first two authors defined a new superclass of bent functions obtained from the \mathcal{C} and \mathcal{D}_0 class as follows. Let π be a permutation on \mathbb{F}_{2^k} and let $L \subset \mathbb{F}_{2^k}$ be a linear subspace of \mathbb{F}_{2^k} such that (π^{-1}, L) satisfies the (C) property. Then the class of bent functions $f: \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2$ containing all functions of the form

$$f(x, y) = Tr_1^k(x\pi(y)) + a_0\mathbb{1}_{L^\perp}(x) + a_1\delta_0(x), \quad a_i \in \mathbb{F}_2, \tag{9}$$

is called SC and is a superclass of \mathcal{D}_0 and \mathcal{C} .

As the following result shows, under certain conditions, the functions in SC are outside the completed Maiorana-McFarland class $\mathcal{M}^\#$.

Theorem 4.8 [3, Theorem 5] *Let π be a permutation on \mathbb{F}_{2^k} and let $L \subset \mathbb{F}_{2^k}$ be a linear subspace of \mathbb{F}_{2^k} such that (π^{-1}, L) satisfies the (C) property and the conditions of Theorem 4.5. Then the function $f: \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2$ defined by*

$$f(x, y) = Tr_1^k(x\pi(y)) + \mathbb{1}_{L^\perp}(x) + \delta_0(x) \tag{10}$$

is a bent function in SC outside $\mathcal{M}^\#$.

With the notation of Proposition 4.7, we construct the following family of MNBC functions.

Theorem 4.9 *Let $x, y \in \mathbb{F}_{2^k}$. The function $F: \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_{2^n}$ defined by*

$$F(x, y) = xy^d + \gamma_1 \mathbf{h}(Tr_1^k(x), Tr_1^k(\alpha x), \dots, Tr_1^k(\alpha^{\tau-1}x)) + \gamma_2 \delta_0(x), \tag{11}$$

where $t < k$, is a 2-step extension (n, n) -MNBC function outside $\mathcal{M}^\#$, for all $\gamma_1, \gamma_2 \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$.

Proof First, we show that F has the maximum number of bent components and is outside $\mathcal{M}^\#$. Let $\lambda \in \mathbb{F}_{2^n}^*$ be arbitrary. Then

$$F_\lambda(x, y) = Tr_1^k(x\pi(y)Tr_k^n(\lambda)) + \mathbf{h}(Tr_1^k(x), Tr_1^k(\alpha x), \dots, Tr_1^k(\alpha^{t-1}x))Tr_1^n(\lambda\gamma_1) + \delta_0(x)Tr_1^n(\lambda\gamma_2)$$

is not bent if and only if $Tr_k^n(\lambda) = 0$. This holds, if $\lambda \in \mathbb{F}_{2^k}^*$. Thus, there are $(2^n - 1) - (2^k - 1) = 2^n - 2^k$ bent components. Since $|\{x \in \mathbb{F}_{2^n} : Tr_1^n(\gamma_i x) = 1\}| = |\{x \in \mathbb{F}_{2^n} : Tr_1^n(\gamma_i x) = 0\}| = 2^{n-1}$, there exist at least $2^n - 2^k - 2^{n-1} = 2^k(2^{k-1} - 1)$ many $\lambda \notin \mathbb{F}_{2^k}$ such that $Tr_1^n(\lambda\gamma_i) = 1$, for $i = 1, 2$. When $Tr_1^k(\lambda\gamma_1) = Tr_1^k(\lambda\gamma_2) = 1$, the component is in \mathcal{SC} outside $\mathcal{M}^\#$, if $Tr_1^k(\lambda\gamma_1) = 1, Tr_1^k(\lambda\gamma_2) = 0$, the component is in \mathcal{C} outside $\mathcal{M}^\#$, and if $Tr_1^k(\lambda\gamma_1) = 0, Tr_1^k(\lambda\gamma_2) = 1$, the component is in \mathcal{D}_0 outside $\mathcal{M}^\#$. Now we show that F is a 2-step extension. Since $G(x, y) := x\pi(y)$ is an (n, k) -function, we can write $G(x, y) = (g_1(x, y), \dots, g_k(x, y))$, where $g_1, \dots, g_k: \mathbb{F}_{2^n} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2$. Since $\gamma_1, \gamma_2 \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, we can construct the function F' in the following form $F'(x, y) = (g_1(x, y), \dots, g_k(x, y), \mathbf{h}(X), \delta_0(x))$, $X = (Tr_1^k(x), \dots, Tr_1^k(\alpha^{t-1}x))$. Thus, F' is an MNBC $(n, k + 2)$ -function, since the non-bent component functions of F' are 0, δ_0 and \mathbf{h} . Note that if $t = k$, then $\delta_0 = \mathbf{h}$. Thus, we assume that $t < k$. Furthermore, we note that the dimension of the linear code $\mathcal{C}_{F'}$ is given by $\dim(\mathcal{C}_{F'}) = 1 + n + k + 2$ which, by definition, means that F' is a nontrivial MNBC $(n, k + 2)$ -function. Consequently, the MNBC (n, n) -function F is a 2-step extension. □

Example 4.10 Let $n = 12$ and the multiplicative group of $\mathbb{F}_{2^{12}}$ be given by $\mathbb{F}_{2^n}^* = \langle \alpha \rangle$, where the primitive element α satisfies $\alpha^{12} + \alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha + 1 = 0$. Let $\lambda = \alpha^{\frac{2^{12}-1}{3}}$. If we choose $L = \langle 1, \lambda \rangle$ and $\pi(y) = y^{38}$, then (π^{-1}, L) satisfies the (C) property (see [25, Example 1]) and $\text{wt}(38) = 3$, that is, π admits no linear structures. Using a computer algebra system, one can check that the following $(12, 12)$ -MNBC functions

$$F_1(x, y) = xy^{38} + \alpha^{233}(Tr_1^6(x) + 1)(Tr_1^6(\lambda x) + 1) \text{ and} \\ F_2(x, y) = xy^{38} + \alpha^{233}(Tr_1^6(x) + 1)(Tr_1^6(\lambda x) + 1) + \alpha^{121}\delta_0(x)$$

are 1-step and 2-step extension, respectively. That is, the dimensions of the linear codes \mathcal{C}_{F_1} and \mathcal{C}_{F_2} , are equal to $1 + n + n/2 + 1 = 20$ and $1 + n + n/2 + 2 = 21$, respectively.

5 A family of t -step extension MNBC functions

In [3], the authors presented the following secondary construction of vectorial bent functions outside $\mathcal{M}^\#$, which can be used to construct nontrivial (n, n) -MNBC functions outside $\mathcal{M}^\#$.

Theorem 5.1 *Let $n = 2k \geq 8$ and $t \geq 3$ be a positive divisor of k such that k/t is odd. Let $\pi(y) = y^d$ be a permutation on \mathbb{F}_{2^k} such that $d(2^t + 1) \equiv 1 \pmod{2^k - 1}$ and $\text{wt}(d) \geq 3$. Let α be a primitive element of \mathbb{F}_{2^t} . Then the (n, n) -function F defined by*

$$F(x, y) = xy^d + \mathbf{H}(x), \quad x, y \in \mathbb{F}_{2^k}$$

with

$$\mathbf{H}(x) = \left(Tr_1^k(x) + 1 \right) \cdot \left(\sum_{i=1}^{t-1} \gamma_i \alpha^i \left(Tr_1^k(\alpha^i x) + 1 \right) \right) + \mu \delta_0(x),$$

where $\gamma_i, \mu \notin \mathbb{F}_{2^k}, \gamma_i \neq \gamma_j (i \neq j)$, is a t -step extension (n, n) -function outside $\mathcal{M}^\#$.

Proof Similarly as in the proof of Theorems 4.2 and 4.9, we note that F has $(2^n - 1) - (2^k - 1) = 2^n - 2^k$ bent components, some of which are outside $\mathcal{M}^\#$.

Let $Tr_1^k(\lambda) = 1$. When $Tr_1^k(\lambda \gamma_i \alpha^i) = 1$ for at least one $i \in \{1, \dots, t-1\}$ and $Tr_1^k(\lambda \mu) = 0$, the component is in \mathcal{C} outside $\mathcal{M}^\#$ (as shown in [3, Proposition 2]). If $Tr_1^k(\lambda \gamma_i \alpha^i) = 1$ for at least one $i \in \{1, \dots, t-1\}$ and $Tr_1^k(\lambda \mu) = 1$, the component is in \mathcal{SC} outside $\mathcal{M}^\#$ (as shown in [3, Corollary 3]). Lastly, if $Tr_1^k(\lambda \gamma_i \alpha^i) = 0$ for all $i \in \{1, \dots, t-1\}$ and $Tr_1^k(\lambda \mu) = 1$, the component is in \mathcal{D}_0 outside $\mathcal{M}^\#$. For the remaining cases, it is easy to see that the components are in $\mathcal{M}^\#$. Now we show that F is an t -step extension.

Since $G(x, y) := x\pi(y)$ is an (n, k) -function, we can write

$$G(x, y) = (g_1(x, y), \dots, g_k(x, y)),$$

where $g_i: \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2$, for $i = 1, \dots, k$. For $\mu, \gamma_1, \dots, \gamma_{t-1} \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$ and $1, \alpha, \dots, \alpha^{t-1} \in \mathbb{F}_{2^t}$, we have that $\{\mu, \gamma_1 \alpha, \dots, \gamma_{t-1} \alpha^{t-1}\}$ is a linearly independent set over \mathbb{F}_2 (since α is a primitive element of \mathbb{F}_{2^t}). Furthermore, because $\gamma_i, \mu \notin \mathbb{F}_{2^k}$ we have that $\gamma_i \alpha^i, \mu \notin \mathbb{F}_{2^k}$ for $i = 1, \dots, t-1$, and thus the set

$$\{1, \omega, \dots, \omega^{k-1}, \mu, \gamma_1 \alpha, \dots, \gamma_{t-1} \alpha^{t-1}\}$$

is linearly independent over \mathbb{F}_2 , where ω is a primitive element of \mathbb{F}_{2^k} satisfying $\omega^{(2^k-1)/(2^t-1)} = \alpha$. Let us show that the functions $h_t = \delta_0, h_i = \mathbb{1}_{\langle 1, \alpha^i \rangle^\perp}, i = 1, \dots, t-1$, are linearly independent. Let us consider their linear combination $\lambda_1 h_1 + \dots + \lambda_{t-1} h_{t-1} + \lambda_t h_t$. Suppose that for some $i \in \{1, \dots, t\}$ we have $\lambda_i = 1$.

If $\lambda_t = 1$, then

$$\delta_0 = \sum_{j=1}^{t-1} \lambda_j h_j = \sum_{j \in J} h_j,$$

where $J = \{j : 1 \leq j \leq t-1, \lambda_j = 1\}$. We have that

$$\begin{aligned} \mathbb{1}_{\langle 1, \alpha, \dots, \alpha^{k-1} \rangle^\perp} &= \delta_0 = \sum_{j \in J} h_j \\ &= (Tr_1^k(x) + 1) \left(Tr_1^k \left(\sum_{j \in J} \alpha^{jx} \right) + \sum_{j \in J} \lambda_j \right) \\ &= \begin{cases} \mathbb{1}_{\langle 1, \sum_{j \in J} \alpha^j \rangle^\perp}, & \text{if } \sum_{j \in J} \lambda_j = 1 \\ \mathbb{1}_{\langle 1, \sum_{j \in J} \alpha^j \rangle^\perp} + l, & \text{otherwise} \end{cases}, \end{aligned}$$

where $l(x) = Tr_1^k(x) + 1$. It is easy to note that the left- and right-hand side cannot be equal, no matter what the choice of $\lambda_i \in \mathbb{F}_2$ is.

Hence, without loss of generality, we may assume that $\lambda_t = 0$. Suppose that for some $i \in \{1, \dots, t-1\}$ we have $\lambda_i = 1$. Then

$$h_i = \sum_{j \neq i, j=1}^{t-1} \lambda_j h_j = \sum_{j \in J} h_j,$$

where $J = \{j : 1 \leq j \leq t - 1, j \neq i, \lambda_j = 1\}$. Let $\xi = \sum_{j \in J} \alpha^j$. It is easy to compute that

$$\mathbb{1}_{\langle 1, \alpha^i \rangle^\perp} = h_i = (Tr_1^k(x) + 1)(Tr_1^k(\xi x) + \varepsilon), \quad \varepsilon = \sum_{j \in J} \lambda_j.$$

If $\varepsilon = 1$, it follows that $\langle 1, \xi \rangle = \langle 1, \alpha^i \rangle$, which implies that $\xi \in \langle 1, \alpha^i \rangle$. This is not possible because ξ is a linear combination of $\{\alpha, \dots, \alpha^{t-1}\} \setminus \{\alpha^i\}$ and α is a primitive element of \mathbb{F}_{2^t} . If $\varepsilon = 0$, we have that

$$1 = h_i(0) = (Tr_1^k(0) + 1)(Tr_1^k(\xi 0)) = 0,$$

which is not true. Thus, we must have that $\lambda_i = 0$ for all $i = 1, \dots, t$. In other words, h_1, \dots, h_t are linearly independent over \mathbb{F}_2 . Furthermore, we have that the functions $g_1, \dots, g_k, h_1, \dots, h_t$ are also linearly independent. Hence we can construct the function F' in the following form

$$F'(x, y) = (g_1(x, y), \dots, g_k(x, y), h_1(x), \dots, h_t(x)).$$

Thus, F' is an $(n, k + t)$ -MNBC function, since the non-bent component functions of F' are 0 and $v \cdot (h_1, \dots, h_t)$ for $v \in \mathbb{F}_2^*$. Furthermore, as the coordinates $g_1, \dots, g_k, h_1, \dots, h_t$ are linearly independent, we note that the dimension of the linear code $C_{F'}$ is given by $\dim(C_{F'}) = 1 + n + k + t$ which, by definition, means that F' is a nontrivial $(n, k + t)$ -MNBC function. Consequently, the (n, n) -MNBC function F is an t -step extension. \square

Example 5.2 Let $k = 9$ and $t = 3$. Suppose that α is a primitive element of \mathbb{F}_{2^3} . Since $284 \cdot (2^3 + 1) \pmod{2^9 - 1} = 1$, let $\pi(y) = y^{284}$ be a permutation on \mathbb{F}_{2^9} . Let $\gamma_1, \gamma_2, \gamma_3$ be distinct elements in $\mathbb{F}_{2^{18}} \setminus \mathbb{F}_{2^9}$. Then

$$F(x, y) = xy^{284} + (Tr_1^9(x) + 1)(\gamma_1 \alpha (Tr_1^9(\alpha x) + 1) + \gamma_2 \alpha^2 (Tr_1^9(\alpha^2 x) + 1)) + \gamma_3 \delta_0(x)$$

is a 3-step $(18, 18)$ -MNBC function outside $\mathcal{M}^\#$.

Additionally, we specify the bounds for the value of t in Theorem 5.1, thus determining a measure of non-triviality of the constructed MNBC-functions.

Remark 5.3 Let $n = 2k$ and k/t be odd, i.e., $k = mt, m$ odd. Note that $m > 1$ as for $m = 1$ we obtain that $d(2^t + 1) \pmod{2^t - 1} = 1$ holds for $d = 2^{t-1}$ and $\text{wt}(d) = 1$ which implies that the function is in $\mathcal{M}^\#$. Hence, without loss of generality, we may assume that $m \geq 3$, then $t = \frac{n}{2m} \leq \frac{n}{6}$, i.e., we have that $3 \leq t \leq n/6$. Furthermore, since t is a positive divisor of k and $k/\text{gcd}(k, t) = k/t$ is odd it follows that $\text{gcd}(2^t + 1, 2^k - 1) = 1$. From [10, Theorem 4.1.-(i)], there exists a unique solution of the linear congruence $d(2^t + 1) \equiv 1 \pmod{2^k - 1}$.

Finally, we give a precise expression of d for $t = 3$, and hence, show that Example 5.2 is a particular instance of an explicit infinite family of MNBC functions.

Proposition 5.4 Let $k = 3m$, where $m = 3 + 2l$ for some $l \in \mathbb{N}_0$. Let also

$$d = 2^{k-1} + \sum_{i=1}^{l+1} \left(2^{k-6i+1} + 2^{k-6i} + 2^{k-6i-1} \right).$$

Then we have that $\text{wt}(d) \geq 3$ and $d(2^3 + 1) \equiv 1 \pmod{2^k - 1}$.

Proof The fact that $\text{wt}(d) \geq 3$ follows from the definition of d . Denote by θ the number $(2^3 + 1)d - 1$ and compute it in the following way:

$$\begin{aligned} \theta &= 2^{k+2} + 2^{k-1} \\ &\quad + \sum_{i=1}^{l+1} \left(2^{k-6i+4} + 2^{k-6i+3} + 2^{k-6i+2} + 2^{k-6i+1} + 2^{k-6i} + 2^{k-6i-1} \right) - 1 \\ &= 2^{k+2} + 2^{k-1} + \left(2^{k-2} + 2^{k-3} + 2^{k-4} + 2^{k-5} + 2^{k-6} + 2^{k-7} \right) \\ &\quad + \left(2^{k-8} + 2^{k-9} + 2^{k-10} + 2^{k-11} + 2^{k-12} + 2^{k-13} \right) + \dots \\ &\quad + \left(2^{k-6l-2} + 2^{k-6l-3} + 2^{k-6l-4} + 2^{k-6l-5} + 2^{k-6l-6} + 2^{k-6l-7} \right) \\ &\quad + 2 + 1 - 2 - 1 - 1 \\ &= 2^{k+2} + 2^k - 1 - 4 = 2^2(2^k - 1) + (2^k - 1) = (2^k - 1)(2^2 + 1), \end{aligned}$$

because $k - 6l = 9$ and $2^k - 1 = \sum_{i=0}^{k-1} 2^i$. Since $(2^k - 1)\theta$, the result follows. □

6 Conclusion and open problems

In this paper, we classified all MNBC functions in six variables and proposed several constructions of MNBC functions outside the $\mathcal{M}^\#$ class. In addition to the questions raised in Sects. 2 and 3, we would like to mention the following open problems.

1. In $n = 6$ variables, all $(n/2 - 1)$ -step and $n/2$ -step extension MNBC functions belong to the $\mathcal{M}^\#$ class. In view of this observation, it is interesting to ask whether $(n/2 - 1)$ -step and $n/2$ -step extension MNBC functions outside $\mathcal{M}^\#$ can in general exist for $n > 6$.
2. To the best of our knowledge, for a t -step extension (n, n) -MNBC function outside the $\mathcal{M}^\#$ class, the largest known value of t is equal to $n/6$ and achieved by the construction in Theorem 5.1. In view of this result, we suggest to find constructions of t -step extension (n, n) -MNBC functions outside the $\mathcal{M}^\#$ class with $t > n/6$.

Acknowledgements Amar Bapić and Enes Pasalic are partly supported by bilateral project BI-DE/19-20-005 (Funkcije nad končnimi polji/Functions on Finite Fields). Alexandr Polujan and Alexander Pott are partly supported by DAAD Project 57450927 (Functions on Finite Fields, PPP Slovenia). The authors would like to thank the anonymous reviewers for their valuable comments, which helped to improve the presentation of the results.

Funding Open Access funding enabled and organized by Projekt DEAL.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

Appendix: CCZ-inequivalent MNBC functions in six variables

Below we list representatives of CCZ-equivalence classes of MNBC functions in $n = 6$ variables as polynomials $f_i : \mathbb{F}_{2^6} \rightarrow \mathbb{F}_{2^6}$, where $\mathbb{F}_{2^6}^* = \langle a \rangle$ with $a^6 + a^4 + a^3 + a + 1 = 0$. Note that the representatives f_i of CCZ-equivalence classes $1 \leq i \leq 13$ are univariate representations of the mappings $z \in \mathbb{F}_2^6 \rightarrow (F_i^3(z), 0)$, where F_i^3 is a vectorial $(6, 3)$ -bent function in [21, Table A2(c)] and 0 is the null-vector. For convenience, we sort the representatives of the first 13 CCZ-equivalence classes as in Fig. 1.

0-step extensions:

- $f_3. a^8x^{48} + a^{57}x^{40} + a^{13}x^{36} + a^{20}x^{34} + a^3x^{33} + a^{60}x^{32} + a^{47}x^{24} + a^{10}x^{20} + a^{45}x^{18} + a^{59}x^{17} + a^{35}x^{16} + a^{10}x^{12} + a^2x^{10} + a^{48}x^9 + a^{47}x^8 + a^{50}x^6 + a^{55}x^5 + a^{18}x^4 + a^{47}x^3 + a^{25}x$
- $f_6. a^{35}x^{56} + a^{21}x^{52} + a^{10}x^{50} + a^{55}x^{49} + a^{41}x^{48} + a^3x^{44} + a^{18}x^{42} + a^{50}x^{41} + a^{22}x^{40} + a^9x^{38} + a^{20}x^{37} + a^{16}x^{36} + a^{34}x^{35} + a^{48}x^{34} + a^{62}x^{33} + a^{12}x^{32} + a^{26}x^{28} + a^{59}x^{26} + a^{11}x^{24} + a^{51}x^{22} + a^{51}x^{21} + a^{40}x^{20} + a^{46}x^{19} + a^{32}x^{18} + a^{26}x^{17} + a^{50}x^{16} + a^{62}x^{14} + a^{32}x^{13} + a^7x^{12} + a^{12}x^{11} + a^{43}x^{10} + a^{30}x^9 + a^{16}x^8 + a^{62}x^7 + a^2x^6 + a^{34}x^5 + a^{42}x^3 + a^{23}x^2 + a^3x$
- $f_7. a^{58}x^{56} + a^{38}x^{52} + a^{27}x^{50} + a^{59}x^{49} + a^{58}x^{48} + a^{28}x^{44} + a^{16}x^{42} + a^{17}x^{41} + a^{36}x^{40} + a^{23}x^{38} + a^{23}x^{37} + a^{51}x^{36} + a^{25}x^{35} + a^{52}x^{34} + a^{37}x^{33} + a^{21}x^{32} + a^{10}x^{28} + a^{26}x^{26} + a^{57}x^{25} + a^{16}x^{24} + a^{40}x^{22} + a^4x^{21} + a^{14}x^{20} + a^{38}x^{19} + a^{53}x^{18} + a^{45}x^{17} + a^{36}x^{16} + a^{15}x^{14} + a^{46}x^{13} + a^{29}x^{12} + a^{24}x^{11} + a^{39}x^{10} + a^{37}x^9 + a^{39}x^8 + a^{50}x^7 + a^{22}x^6 + a^6x^5 + a^{46}x^4 + a^{36}x^3 + a^{16}x^2 + x$
- $f_{13}. a^{52}x^{56} + a^{42}x^{52} + a^{22}x^{50} + a^{28}x^{49} + a^{21}x^{48} + a^4x^{44} + a^{58}x^{42} + a^{57}x^{41} + a^{13}x^{40} + a^{26}x^{38} + a^6x^{37} + a^{53}x^{36} + a^{20}x^{35} + a^{51}x^{34} + a^{12}x^{33} + a^{37}x^{32} + a^{53}x^{28} + a^{61}x^{26} + a^{53}x^{25} + a^{50}x^{24} + a^{29}x^{22} + a^{25}x^{21} + a^{14}x^{20} + a^{42}x^{19} + a^{22}x^{18} + a^{24}x^{17} + a^{39}x^{16} + a^{48}x^{14} + a^{30}x^{13} + a^{41}x^{12} + a^{17}x^{11} + a^{41}x^{10} + a^{16}x^9 + a^{59}x^8 + a^{23}x^7 + a^8x^6 + a^{53}x^5 + a^{15}x^4 + a^{28}x^3 + a^6x^2 + a^{46}x$
- $f_2. a^{34}x^{48} + a^{58}x^{40} + a^{28}x^{36} + a^{39}x^{34} + a^{14}x^{33} + a^{36}x^{32} + a^{25}x^{24} + a^{24}x^{20} + a^5x^{18} + a^{13}x^{17} + a^{17}x^{16} + a^{35}x^{12} + a^{54}x^{10} + a^{14}x^9 + a^{26}x^8 + a^6x^6 + a^6x^5 + a^{57}x^4 + a^{60}x^3 + a^{50}x^2 + a^{18}x$
- $f_{12}. a^{48}x^{56} + a^9x^{52} + a^{41}x^{50} + a^{25}x^{49} + a^{37}x^{48} + a^{38}x^{44} + a^{58}x^{42} + a^{61}x^{41} + a^5x^{40} + a^5x^{38} + a^{32}x^{37} + a^{58}x^{36} + a^{38}x^{35} + a^6x^{34} + a^{13}x^{33} + a^{61}x^{32} + a^{32}x^{28} + a^{23}x^{26} + a^{12}x^{25} + a^{32}x^{22} + a^{25}x^{21} + a^{15}x^{20} + a^{58}x^{19} + a^{34}x^{18} + a^8x^{17} + a^{32}x^{16} + a^{35}x^{14} + a^{22}x^{13} + a^{60}x^{12} + a^{47}x^{11} + a^3x^{10} + a^{62}x^9 + a^{54}x^8 + a^{33}x^7 + a^{34}x^6 + a^{34}x^5 + a^{47}x^4 + a^2x^3 + a^{25}x^2 + a^{19}x$
- $f_4. a^{19}x^{56} + a^3x^{52} + a^{40}x^{50} + a^{36}x^{49} + a^{55}x^{48} + a^{43}x^{44} + a^{44}x^{42} + a^4x^{41} + a^{32}x^{40} + a^{10}x^{38} + a^{15}x^{37} + a^{25}x^{36} + a^7x^{35} + a^5x^{34} + a^{11}x^{33} + a^{21}x^{32} + a^{42}x^{28} + a^{34}x^{26} + a^{21}x^{25} + a^{41}x^{24} + a^{54}x^{22} + a^{23}x^{21} + a^{55}x^{20} + a^6x^{19} + a^{39}x^{18} + a^{60}x^{17} + a^{54}x^{16} + a^{22}x^{14} + a^{18}x^{13} + a^{11}x^{12} + a^{28}x^{11} + a^{48}x^{10} + a^{24}x^9 + a^{56}x^8 + a^{12}x^7 + a^{48}x^6 + a^{34}x^5 + a^{12}x^4 + a^{62}x^3 + a^{20}x^2 + a^{27}x$
- $f_1. a^{42}x^{48} + a^{23}x^{40} + a^{21}x^{36} + a^{27}x^{33} + a^{22}x^{32} + a^{57}x^{24} + a^7x^{20} + a^{26}x^{18} + a^{30}x^{17} + a^{30}x^{16} + a^{13}x^{12} + a^{29}x^{10} + a^{35}x^9 + a^{45}x^8 + a^7x^6 + a^{14}x^5 + a^{23}x^4 + ax^3 + a^{25}x^2 + a^{19}x$
- $f_5. a^{13}x^{56} + a^{56}x^{52} + a^{28}x^{50} + a^{39}x^{49} + a^{53}x^{48} + a^{25}x^{44} + a^{24}x^{42} + a^{34}x^{41} + a^{27}x^{40} + a^{49}x^{38} + a^{57}x^{37} + a^{16}x^{36} + a^{42}x^{35} + a^{17}x^{34} + a^{30}x^{33} + a^{32}x^{32} + a^8x^{28} + a^{61}x^{26} + a^{33}x^{25} + a^{41}x^{24} + a^{14}x^{22} + a^{55}x^{21} + a^{30}x^{20} + a^2x^{19} + a^{32}x^{18} + a^{29}x^{17} + a^{26}x^{16} + a^{37}x^{14} + a^{43}x^{13} + a^{56}x^{12} + a^{14}x^{11} + a^{56}x^{10} + a^{30}x^9 + a^6x^8 + a^{53}x^7 + a^6x^6 + a^{21}x^5 + a^{34}x^4 + a^6x^3 + a^{48}x^2 + a^{11}x$

$$\begin{aligned}
f_9. & a^{56}x^{56} + a^4x^{52} + a^{42}x^{50} + a^{49}x^{49} + a^{22}x^{48} + a^{55}x^{44} + a^{60}x^{42} + a^3x^{41} + a^{20}x^{40} \\
& + a^{55}x^{38} + a^{61}x^{37} + a^9x^{36} + a^{57}x^{35} + a^{39}x^{34} + a^{11}x^{33} + a^{31}x^{32} + a^7x^{28} + a^{52}x^{26} + a^{51}x^{24} \\
& + a^{56}x^{22} + a^9x^{21} + a^{24}x^{20} + a^{41}x^{19} + a^{36}x^{18} + a^{35}x^{17} + a^{56}x^{16} + a^{22}x^{14} + a^8x^{13} + a^{15} \\
& x^{12} + a^{37}x^{11} + a^{60}x^{10} + a^{18}x^9 + a^{29}x^8 + a^{52}x^7 + a^{13}x^6 + a^{12}x^5 + a^{28}x^4 + a^{26} \\
& x^3 + a^{53}x^2 + a^{59}x \\
f_{10}. & a^{16}x^{52} + a^9x^{50} + a^{33}x^{49} + a^{57}x^{48} + a^{35}x^{44} + a^{27}x^{42} + a^{32}x^{41} + a^9x^{40} + a^{48}x^{38} \\
& + a^{57}x^{37} + a^{42}x^{36} + a^{61}x^{35} + a^{33}x^{34} + a^{28}x^{33} + a^{35}x^{32} + a^{53}x^{28} + a^{40}x^{26} + a^{56}x^{25} + a^{57} \\
& x^{24} + a^{11}x^{22} + a^{10}x^{21} + a^{25}x^{20} + a^{18}x^{19} + a^{30}x^{18} + a^{44}x^{17} + a^{17}x^{16} + a^{17}x^{14} + a^{25}x^{13} \\
& + a^{16}x^{12} + a^{22}x^{11} + a^{26}x^{10} + a^{41}x^9 + a^{41}x^8 + a^{24}x^7 + a^{12}x^6 + a^{36}x^5 + ax^4 + a^{53}x^3 + \\
& a^4x^2 + a^3x \\
f_{11}. & a^{55}x^{56} + a^{39}x^{50} + a^8x^{49} + a^{14}x^{48} + a^{14}x^{44} + a^{27}x^{42} + a^{52}x^{41} + a^{18}x^{40} + a^{55}x^{38} \\
& + a^{46}x^{37} + a^{53}x^{36} + a^{56}x^{35} + x^{34} + a^{17}x^{33} + a^{35}x^{32} + a^{42}x^{28} + a^{39}x^{26} + a^{50}x^{25} + a^{45}x^{24} \\
& + ax^{22} + a^{10}x^{21} + a^2x^{20} + a^{62}x^{19} + a^{22}x^{18} + a^{34}x^{17} + a^{11}x^{16} + a^{24}x^{14} + a^3x^{13} + a^{22}x^{12} \\
& + a^{45}x^{11} + a^{31}x^{10} + a^{16}x^9 + a^{21}x^8 + a^{44}x^7 + a^{40}x^6 + a^{48}x^5 + a^{18}x^4 + a^{46}x^3 + a^{33}x^2 + a^3x \\
f_{10}. & a^{55}x^{56} + a^{39}x^{50} + a^8x^{49} + a^{57}x^{48} + a^{14}x^{44} + a^{27}x^{42} + a^{52}x^{41} + a^{42}x^{40} + a^{55}x^{38} \\
& + a^{46}x^{37} + a^{32}x^{36} + a^{56}x^{35} + a^{24}x^{34} + a^{11}x^{33} + a^8x^{32} + a^{42}x^{28} + a^{39}x^{26} + a^{50}x^{25} + a^{48} \\
& x^{24} + ax^{22} + a^{10}x^{21} + a^{12}x^{20} + a^{62}x^{19} + a^{36}x^{18} + a^{19}x^{17} + a^{16}x^{16} + a^{24}x^{14} + a^3x^{13} + a^{29} \\
& x^{12} + a^{45}x^{11} + a^{24}x^{10} + a^{51}x^9 + a^{49}x^8 + a^{44}x^7 + a^{57}x^6 + a^{13}x^5 + a^{42}x^4 + a^{52}x^3 + \\
& a^{14}x^2 + a^{47}x
\end{aligned}$$

1-step extensions

$$\begin{aligned}
f_{14}. & a^{62}x^{48} + a^{17}x^{40} + a^{29}x^{36} + a^{26}x^{34} + a^{26}x^{33} + a^{48}x^{32} + a^{49}x^{24} + a^8x^{20} + a^{13}x^{18} + \\
& a^{26}x^{17} + a^{27}x^{16} + a^{31}x^{12} + a^{41}x^{10} + a^9x^9 + a^{42}x^8 + a^{16}x^6 + a^8x^5 + a^{25}x^4 + a^{23}x^3 \\
& + a^{11}x^2 + a^{62}x \\
f_{15}. & a^2x^{56} + a^{32}x^{52} + a^{18}x^{50} + a^{46}x^{49} + a^{52}x^{48} + a^{54}x^{44} + a^{45}x^{42} + a^{56}x^{41} + a^7x^{40} \\
& + a^{46}x^{38} + a^{32}x^{37} + a^6x^{36} + a^{44}x^{35} + a^{41}x^{34} + a^{50}x^{33} + a^{21}x^{32} + a^{34}x^{28} + a^{49}x^{26} + \\
& a^{50}x^{25} + x^{24} + a^{60}x^{22} + a^{15}x^{21} + a^{34}x^{20} + a^{46}x^{19} + a^{47}x^{18} + a^4x^{17} + a^7x^{16} + a^{50}x^{14} + \\
& a^7x^{13} + a^5x^{12} + a^{57}x^{11} + a^{17}x^{10} + a^{12}x^9 + a^{17}x^8 + a^{60}x^6 + a^2x^5 + a^7x^4 + a^{23}x^3 + \\
& a^{49}x^2 + a^{34}x \\
f_{16}. & a^{52}x^{56} + a^{43}x^{52} + a^{34}x^{50} + a^{28}x^{49} + a^{31}x^{48} + a^{60}x^{44} + a^{58}x^{42} + a^{54}x^{41} + a^{46}x^{40} \\
& + a^{55}x^{38} + a^9x^{37} + a^{15}x^{36} + a^{20}x^{35} + a^{42}x^{34} + a^{54}x^{33} + a^{38}x^{32} + a^{53}x^{28} + a^{40}x^{26} + \\
& a^{29}x^{25} + a^{49}x^{24} + a^{62}x^{22} + a^{25}x^{21} + a^{17}x^{20} + a^{48}x^{19} + a^{26}x^{18} + a^{13}x^{17} + a^3x^{16} + a^{48}x^{14} \\
& + a^{59}x^{13} + a^{44}x^{12} + a^8x^{11} + a^{21}x^{10} + a^{32}x^9 + a^{43}x^8 + a^{23}x^7 + a^{20}x^6 + a^{38}x^5 + a^{49}x^4 \\
& + a^{32}x^3 + a^{27}x^2 + a^6x \\
f_{17}. & a^{27}x^{56} + a^{27}x^{52} + a^{17}x^{50} + a^{23}x^{49} + a^{31}x^{48} + a^{44}x^{44} + a^2x^{42} + a^{53}x^{41} + a^{29}x^{40} \\
& + a^{48}x^{38} + a^{23}x^{37} + a^{24}x^{36} + a^{26}x^{35} + a^{43}x^{34} + a^{17}x^{33} + a^8x^{32} + a^4x^{28} + a^{20}x^{26} \\
& + a^2x^{25} + a^{30}x^{24} + a^7x^{22} + a^{49}x^{21} + a^{39}x^{20} + a^{26}x^{19} + a^{24}x^{18} + a^{62}x^{17} + a^{37}x^{16} + \\
& a^{49}x^{14} + a^{53}x^{13} + a^{37}x^{12} + a^{37}x^{11} + a^{28}x^{10} + a^2x^9 + a^{51}x^8 + a^{53}x^7 + a^{45}x^6 + a^{18}x^5 \\
& + a^{38}x^4 + a^{34}x^3 + a^{52}x^2 + a^{15}x \\
f_{18}. & a^{20}x^{56} + a^4x^{52} + a^{41}x^{50} + a^{37}x^{49} + a^8x^{48} + a^{44}x^{44} + a^{45}x^{42} + a^5x^{41} + a^{12}x^{40} \\
& + a^{11}x^{38} + a^{16}x^{37} + a^{61}x^{36} + a^8x^{35} + a^{34}x^{34} + a^{37}x^{33} + a^{35}x^{32} + a^{43}x^{28} + a^{35}x^{26} + a^{22}x^{25} \\
& + a^{59}x^{24} + a^{55}x^{22} + a^{24}x^{21} + a^{30}x^{20} + a^7x^{19} + a^{52}x^{18} + a^{25}x^{17} + a^{22}x^{16} + a^{23}x^{14} + a^{19} \\
& x^{13} + a^{26}x^{12} + a^{29}x^{11} + a^{26}x^{10} + a^{26}x^9 + a^{18}x^8 + a^{13}x^7 + a^{52}x^6 + a^7x^5 + a^{51}x^4 \\
& + a^{50}x^3 + a^{37}x^2 + a^{22}x \\
f_{19}. & a^{15}x^{56} + a^{25}x^{52} + a^{33}x^{49} + a^{14}x^{48} + a^{61}x^{44} + a^{18}x^{42} + a^{14}x^{41} + a^2x^{40} + a^{39}x^{38} + \\
& a^{27}x^{37} + a^{55}x^{36} + a^{53}x^{35} + a^{62}x^{34} + a^{17}x^{33} + a^{22}x^{32} + a^{20}x^{28} + a^9x^{26} + a^2x^{25} \\
& + a^{45}x^{24} + a^{34}x^{22} + a^{26}x^{21} + a^{19}x^{20} + a^{43}x^{19} + a^{14}x^{18} + a^{59}x^{17} + a^{24}x^{16} + a^{45}x^{14} + a^{46} \\
& x^{13} + a^{22}x^{12} + a^{62}x^{11} + a^{49}x^{10} + a^{47}x^9 + a^6x^8 + a^{27}x^7 + a^{40}x^6 + a^{16}x^5 + a^{22}x^4 \\
& + a^{46}x^3 + a^{58}x^2 + a^{32}x
\end{aligned}$$

- $f_{20}. a^{20}x^{56} + a^4x^{52} + a^{41}x^{50} + a^{37}x^{49} + a^{46}x^{48} + a^{44}x^{44} + a^{45}x^{42} + a^5x^{41} + a^{46}x^{40} + a^{11}x^{38} + a^{16}x^{37} + a^{57}x^{36} + a^8x^{35} + ax^{34} + a^{11}x^{33} + a^{48}x^{32} + a^{43}x^{28} + a^{35}x^{26} + a^{22}x^{25} + a^{16}x^{24} + a^{55}x^{22} + a^{24}x^{21} + a^{44}x^{20} + a^7x^{19} + a^{14}x^{18} + a^{34}x^{17} + a^6x^{16} + a^{23}x^{14} + a^{19}x^{13} + ax^{12} + a^{29}x^{11} + a^{10}x^{10} + a^{31}x^9 + a^{19}x^8 + a^{13}x^7 + a^{49}x^6 + a^{33}x^5 + a^{41}x^4 + a^{23}x^3 + a^{59}x^2 + a^{34}x$
- $f_{21}. a^{42}x^{48} + a^{47}x^{40} + a^{30}x^{36} + a^{58}x^{34} + a^{27}x^{33} + a^{55}x^{32} + a^{57}x^{24} + a^{32}x^{20} + a^{22}x^{18} + a^{58}x^{17} + a^5x^{16} + a^{13}x^{12} + a^{59}x^{10} + a^{60}x^9 + a^{22}x^8 + a^7x^6 + a^{59}x^5 + a^{48}x^4 + ax^3 + ax^2 + a^{23}x$
- $f_{22}. a^{20}x^{56} + a^4x^{52} + a^{41}x^{50} + x^{48} + a^{44}x^{44} + a^{45}x^{42} + a^{59}x^{41} + a^{31}x^{40} + a^{11}x^{38} + a^{43}x^{37} + a^6x^{36} + a^{17}x^{35} + a^{55}x^{34} + a^2x^{33} + a^{58}x^{32} + a^{43}x^{28} + a^{35}x^{26} + a^{31}x^{25} + a^{17}x^{24} + a^{55}x^{22} + a^{15}x^{21} + a^{45}x^{20} + a^{52}x^{19} + a^{47}x^{18} + a^{10}x^{17} + a^{32}x^{16} + a^{23}x^{14} + ax^{13} + a^{19}x^{12} + a^{47}x^{11} + a^{20}x^{10} + a^{12}x^9 + a^{56}x^8 + a^{49}x^7 + a^{31}x^6 + a^{24}x^5 + a^{44}x^4 + a^{37}x^3 + a^{13}x^2 + a^3x$
- $f_{23}. a^{21}x^{56} + a^{16}x^{52} + a^{31}x^{50} + a^{23}x^{49} + a^{62}x^{48} + a^{10}x^{44} + a^3x^{42} + a^{49}x^{41} + a^{23}x^{40} + a^{44}x^{38} + a^{40}x^{37} + a^{32}x^{36} + a^{23}x^{35} + a^{56}x^{34} + a^{23}x^{33} + a^{22}x^{32} + a^{12}x^{28} + a^{41}x^{26} + a^{45}x^{25} + a^6x^{24} + a^{38}x^{22} + a^{20}x^{21} + a^{58}x^{20} + a^{32}x^{19} + a^{46}x^{18} + a^8x^{17} + a^{45}x^{16} + a^{39}x^{14} + a^{60}x^{13} + a^{29}x^{12} + a^{48}x^{11} + x^{10} + a^{39}x^9 + a^{62}x^8 + ax^7 + a^{28}x^6 + a^{50}x^5 + a^{49}x^4 + a^{56}x^3 + a^{33}x^2 + a^{52}x$
- $f_{24}. a^{30}x^{56} + a^{53}x^{52} + a^{53}x^{50} + a^{11}x^{49} + a^{48}x^{48} + a^{13}x^{44} + a^{18}x^{42} + a^{26}x^{41} + a^{55}x^{40} + a^{43}x^{38} + a^8x^{37} + a^{52}x^{36} + a^{51}x^{35} + a^{18}x^{34} + a^{29}x^{33} + a^{62}x^{32} + a^{15}x^{28} + a^{58}x^{26} + a^{24}x^{25} + a^{30}x^{24} + a^5x^{22} + a^{26}x^{21} + a^{24}x^{20} + a^{12}x^{19} + a^{48}x^{18} + a^{15}x^{17} + a^{50}x^{16} + a^5x^{14} + a^{24}x^{13} + a^{46}x^{12} + a^{47}x^{11} + a^{24}x^{10} + a^{56}x^9 + a^{18}x^8 + a^{50}x^7 + a^{22}x^5 + a^{35}x^4 + a^{55}x^3 + a^{47}x^2 + a^{51}x$
- $f_{25}. a^9x^{56} + a^{55}x^{52} + a^{42}x^{50} + a^6x^{49} + a^{24}x^{48} + a^{56}x^{44} + a^{18}x^{42} + a^{28}x^{41} + a^8x^{40} + a^{11}x^{38} + a^9x^{37} + a^{19}x^{36} + a^{42}x^{35} + a^{28}x^{34} + a^{33}x^{33} + a^{23}x^{32} + a^4x^{28} + ax^{26} + a^{21}x^{25} + a^2x^{24} + a^{55}x^{22} + a^{26}x^{21} + a^{13}x^{20} + a^{39}x^{19} + a^{21}x^{18} + a^{35}x^{17} + x^{16} + a^2x^{14} + ax^{13} + a^{18}x^{12} + a^{18}x^{11} + a^{33}x^{10} + a^{55}x^9 + a^{15}x^8 + a^{33}x^7 + a^{58}x^6 + a^{52}x^5 + a^{24}x^4 + x^3 + a^8x^2 + a^{57}x$
- $f_{26}. a^9x^{56} + a^{55}x^{52} + a^{42}x^{50} + a^6x^{49} + a^{62}x^{48} + a^{56}x^{44} + a^{18}x^{42} + a^{28}x^{41} + a^{30}x^{40} + a^{11}x^{38} + a^9x^{37} + a^{13}x^{36} + a^{42}x^{35} + a^{15}x^{34} + a^4x^{33} + a^{13}x^{32} + a^4x^{28} + ax^{26} + a^{21}x^{25} + a^{34}x^{24} + a^{55}x^{22} + a^{26}x^{21} + a^{11}x^{20} + a^{39}x^{19} + a^{43}x^{17} + a^{33}x^{16} + a^2x^{14} + ax^{13} + a^{23}x^{12} + a^{18}x^{11} + a^{38}x^{10} + a^{49}x^9 + a^{58}x^8 + a^{33}x^7 + a^{50}x^6 + a^{18}x^5 + a^{28}x^4 + a^5x^3 + a^{19}x^2 + a^5x$
- $f_{27}. a^{34}x^{56} + a^{15}x^{52} + a^{36}x^{50} + a^{61}x^{49} + a^9x^{48} + a^{20}x^{44} + a^{44}x^{42} + a^{61}x^{41} + a^{10}x^{40} + a^{10}x^{38} + a^{11}x^{37} + a^{52}x^{36} + a^{11}x^{35} + a^{14}x^{34} + a^{23}x^{33} + a^{16}x^{32} + x^{28} + a^{50}x^{26} + a^{58}x^{25} + a^{44}x^{24} + a^{13}x^{22} + a^{11}x^{21} + a^{52}x^{20} + a^{48}x^{19} + a^{48}x^{18} + a^{38}x^{17} + a^{36}x^{16} + a^{41}x^{14} + a^{50}x^{13} + a^{43}x^{12} + a^{46}x^{11} + a^4x^{10} + a^{56}x^9 + a^{42}x^8 + a^{57}x^7 + a^{61}x^6 + a^{19}x^5 + a^3x^4 + a^{43}x^3 + a^{22}x^2 + a^{34}x$
- $f_{28}. a^{55}x^{56} + a^{35}x^{52} + a^{43}x^{50} + a^8x^{49} + a^{49}x^{48} + a^{32}x^{44} + a^{27}x^{42} + a^{23}x^{41} + a^{56}x^{40} + a^{26}x^{38} + a^{28}x^{37} + a^{15}x^{36} + a^{56}x^{35} + a^{26}x^{34} + a^{31}x^{33} + a^{60}x^{32} + a^{42}x^{28} + a^{13}x^{26} + a^{44}x^{25} + a^{55}x^{24} + a^{14}x^{22} + a^{10}x^{21} + a^{60}x^{20} + a^{25}x^{19} + a^{26}x^{18} + a^{20}x^{17} + a^{54}x^{16} + a^{24}x^{14} + a^{10}x^{13} + a^{50}x^{12} + a^{32}x^{11} + a^{29}x^{10} + a^{32}x^9 + a^3x^8 + a^{44}x^7 + a^{34}x^6 + a^{26}x^5 + a^7x^4 + a^{22}x^3 + a^4x^2 + a^{21}x$
- $f_{29}. a^{55}x^{56} + a^{35}x^{52} + a^{43}x^{50} + a^8x^{49} + a^{56}x^{48} + a^{32}x^{44} + a^{27}x^{42} + a^{23}x^{41} + a^{14}x^{40} + a^{26}x^{38} + a^{28}x^{37} + a^{40}x^{36} + a^{56}x^{35} + a^{19}x^{34} + a^{53}x^{33} + a^3x^{32} + a^{42}x^{28} + a^{13}x^{26} + a^{44}x^{25} + a^9x^{24} + a^{14}x^{22} + a^{10}x^{21} + a^{41}x^{20} + a^{25}x^{19} + a^{55}x^{18} + a^{27}x^{17} + a^2x^{16} + a^{24}x^{14} + a^{10}x^{13} + a^5x^{12} + a^{32}x^{11} + a^4x^{10} + a^{29}x^9 + a^{50}x^8 + a^{44}x^7 + a^{49}x^6 + a^{61}x^5 + a^{31}x^4 + a^{16}x^3 + a^{36}x^2 + a^{61}x$
- $f_{30}. a^{55}x^{56} + a^{35}x^{52} + a^{43}x^{50} + a^8x^{49} + a^{35}x^{48} + a^{32}x^{44} + a^{27}x^{42} + a^{23}x^{41} + a^6x^{40} + a^{26}x^{38} + a^{28}x^{37} + a^{46}x^{36} + a^{56}x^{35} + a^{60}x^{34} + a^{57}x^{33} + a^{54}x^{32} + a^{42}x^{28} + a^{13}x^{26} + a^{44}x^{25} + a^5x^{24} + a^{14}x^{22} + a^{10}x^{21} + a^{46}x^{20} + a^{25}x^{19} + a^{15}x^{18} + a^{58}x^{17} + a^{44}x^{16} + a^{24}x^{14}$

$$+a^{10}x^{13}+a^{24}x^{12}+a^{32}x^{11}+a^{42}x^{10}+a^9x^9+a^{56}x^8+a^{44}x^7+a^7x^6+a^{44}x^5+a^{19}x^4+a^{12}x^3+a^{29}x^2+a^{44}x$$

2-step extensions:

$$f_{31}. a^{21}x^{56}+a^5x^{52}+a^{42}x^{50}+a^{38}x^{49}+a^{24}x^{48}+a^{45}x^{44}+a^{46}x^{42}+a^6x^{41}+a^{24}x^{40}+a^{12}x^{38}+a^{17}x^{37}+a^{10}x^{36}+a^9x^{35}+a^3x^{34}+a^{19}x^{33}+a^{35}x^{32}+a^{44}x^{28}+a^{36}x^{26}+a^{23}x^{25}+a^{55}x^{24}+a^{56}x^{22}+a^{25}x^{21}+a^{17}x^{20}+a^8x^{19}+a^{58}x^{18}+a^2x^{17}+a^{42}x^{16}+a^{24}x^{14}+a^{20}x^{13}+a^{37}x^{12}+a^{30}x^{11}+a^5x^9+a^{57}x^8+a^{14}x^7+a^{53}x^6+a^{31}x^5+a^{53}x^4+a^{62}x^3+a^{52}x^2+a^{19}x$$

$$f_{32}. ax^{48}+a^{29}x^{36}+a^{57}x^{34}+a^{12}x^{33}+a^{12}x^{32}+a^6x^{24}+a^{27}x^{20}+a^{40}x^{18}+a^{23}x^{17}+a^{55}x^{16}+a^2x^{12}+a^9x^{10}+a^{34}x^9+a^{49}x^8+a^{24}x^6+a^{39}x^5+a^{41}x^4+a^{42}x^3+a^{21}x^2+a^{30}x$$

$$f_{33}. a^{14}x^{56}+a^9x^{52}+a^{24}x^{50}+a^{62}x^{49}+a^{11}x^{48}+a^3x^{44}+a^{59}x^{42}+a^{15}x^{41}+a^{11}x^{40}+a^{37}x^{38}+a^{34}x^{37}+a^{36}x^{36}+a^{10}x^{35}+a^{18}x^{34}+a^{12}x^{33}+a^{61}x^{32}+a^{5}x^{28}+a^{34}x^{26}+a^{27}x^{25}+a^{56}x^{24}+a^{31}x^{22}+a^{18}x^{21}+a^3x^{20}+a^{10}x^{19}+a^{25}x^{18}+a^{48}x^{17}+a^{52}x^{16}+a^{32}x^{14}+a^3x^{13}+a^{44}x^{12}+a^{15}x^{11}+a^{13}x^{10}+a^8x^9+a^{46}x^8+a^{43}x^7+a^8x^6+a^6x^5+a^8x^4+a^{53}x^3+a^{52}x^2+a^{35}x$$

$$f_{34}. a^{14}x^{56}+a^9x^{52}+a^{24}x^{50}+a^{62}x^{49}+a^{61}x^{48}+a^3x^{44}+a^{59}x^{42}+a^{15}x^{41}+a^{57}x^{40}+a^{37}x^{38}+a^{34}x^{37}+a^{36}x^{36}+a^{10}x^{35}+a^{35}x^{34}+a^{14}x^{33}+a^{23}x^{32}+a^5x^{28}+a^{34}x^{26}+a^{27}x^{25}+a^{17}x^{24}+a^{31}x^{22}+a^{18}x^{21}+ax^{20}+a^{10}x^{19}+a^{25}x^{18}+ax^{17}+a^{13}x^{16}+a^{32}x^{14}+a^3x^{13}+a^{14}x^{12}+a^{15}x^{11}+a^{29}x^{10}+a^8x^9+a^{61}x^8+a^{43}x^7+a^{12}x^6+a^{30}x^5+a^{23}x^4+a^{39}x^3+a^4x^2+a^{32}x$$

$$f_{35}. a^{28}x^{52}+a^{54}x^{50}+a^{57}x^{49}+a^{53}x^{48}+a^{14}x^{44}+a^{40}x^{42}+a^{43}x^{41}+a^2x^{40}+a^{40}x^{38}+a^{28}x^{37}+a^{61}x^{36}+a^{25}x^{35}+a^{29}x^{34}+a^{31}x^{33}+a^{51}x^{32}+a^{40}x^{28}+a^3x^{26}+a^6x^{25}+a^{51}x^{24}+a^{29}x^{22}+a^{50}x^{21}+a^{39}x^{20}+a^{49}x^{19}+a^3x^{18}+a^{11}x^{17}+a^{32}x^{16}+a^{58}x^{14}+a^8x^{13}+a^4x^{12}+a^{21}x^{11}+a^{16}x^{10}+a^{61}x^9+a^{11}x^8+a^4x^7+a^4x^6+a^{33}x^5+a^{46}x^4+a^{38}x^2+a^{55}x$$

$$f_{36}. a^{51}x^{56}+x^{52}+a^{25}x^{50}+a^{52}x^{49}+a^{27}x^{48}+a^{45}x^{44}+a^{30}x^{42}+a^{11}x^{41}+a^9x^{40}+a^{46}x^{38}+a^2x^{37}+a^{10}x^{36}+a^{50}x^{35}+a^{50}x^{34}+a^5x^{33}+a^{26}x^{32}+a^8x^{28}+a^{15}x^{26}+a^{54}x^{25}+a^{23}x^{24}+a^{45}x^{22}+a^{27}x^{21}+a^5x^{20}+a^{51}x^{19}+a^{41}x^{18}+a^{33}x^{17}+a^8x^{16}+a^9x^{14}+a^{51}x^{13}+a^{54}x^{12}+a^{53}x^{11}+x^{10}+a^{42}x^9+a^{16}x^8+a^{19}x^7+a^{41}x^6+a^{47}x^5+x^4+a^{50}x^3+a^{13}x^2+a^{11}x$$

$$f_{37}. a^{51}x^{56}+x^{52}+a^{25}x^{50}+a^{52}x^{49}+a^{43}x^{48}+a^{45}x^{44}+a^{30}x^{42}+a^{11}x^{41}+a^{46}x^{38}+a^2x^{37}+a^{30}x^{36}+a^{50}x^{35}+a^{30}x^{34}+a^2x^{33}+a^{48}x^{32}+a^8x^{28}+a^{15}x^{26}+a^{54}x^{25}+a^{19}x^{24}+a^{45}x^{22}+a^{27}x^{21}+a^{43}x^{20}+a^{51}x^{19}+a^{47}x^{18}+a^{62}x^{17}+a^{13}x^{16}+a^9x^{14}+a^{51}x^{13}+a^{24}x^{12}+a^{53}x^{11}+a^{42}x^{10}+a^{37}x^9+a^{46}x^8+a^{19}x^7+a^{49}x^6+a^{57}x^5+a^{29}x^4+a^4x^3+a^{36}x^2+a^{24}x$$

3-step extensions:

$$f_{38}. a^{22}x^{56}+a^6x^{52}+a^{43}x^{50}+a^{39}x^{49}+a^{35}x^{48}+a^{46}x^{44}+a^{47}x^{42}+a^7x^{41}+a^{36}x^{40}+a^{13}x^{38}+a^{18}x^{37}+a^{46}x^{36}+a^{10}x^{35}+a^{21}x^{34}+a^{46}x^{33}+a^3x^{32}+a^{45}x^{28}+a^{37}x^{26}+a^{24}x^{25}+a^{51}x^{24}+a^{57}x^{22}+a^{26}x^{21}+a^{22}x^{20}+a^9x^{19}+a^9x^{18}+a^{52}x^{17}+a^{12}x^{16}+a^{25}x^{14}+a^{21}x^{13}+a^{52}x^{12}+a^{31}x^{11}+a^{49}x^{10}+a^{49}x^9+a^{10}x^8+a^{15}x^7+a^{50}x^6+a^{34}x^5+a^{11}x^4+a^{50}x^3+x^2+a^{25}x$$

$$f_{39}. a^{15}x^{40}+a^{46}x^{36}+a^{34}x^{34}+a^{31}x^{33}+a^{54}x^{32}+a^{16}x^{24}+a^{49}x^{20}+a^9x^{18}+a^9x^{17}+ax^{16}+a^{51}x^{12}+a^{14}x^{10}+a^{49}x^9+a^{55}x^8+a^{13}x^6+a^{61}x^5+a^{33}x^4+a^{39}x^3+a^{59}x^2+a^{26}x$$

$$f_{40}. a^{23}x^{56}+a^{15}x^{52}+a^{12}x^{50}+a^{55}x^{49}+a^{45}x^{48}+a^{61}x^{44}+a^9x^{42}+a^{20}x^{41}+a^{57}x^{40}+a^3x^{38}+a^3x^{37}+a^6x^{36}+a^{37}x^{35}+a^{40}x^{34}+a^{61}x^{33}+x^{32}+a^{20}x^{28}+a^{54}x^{26}+a^9x^{25}+a^{15}x^{24}+a^{52}x^{22}+a^{41}x^{21}+a^{48}x^{20}+a^{56}x^{19}+a^{52}x^{18}+a^{13}x^{17}+a^{15}x^{16}+a^{17}x^{14}+a^{22}x^{13}+a^{20}x^{12}+a^{59}x^{11}+a^{56}x^{10}+a^6x^9+ax^8+a^{52}x^7+a^{59}x^6+a^{46}x^5+a^{36}x^4+a^4x^3+a^4x^2+a^{49}x$$

References

- Anbar N., Kalaycı T., Meidl W.: Analysis of (n, n) -functions obtained from the Maiorana-McFarland class. *IEEE Trans. Inf. Theory* **67**(7), 4891–4901 (2021). <https://doi.org/10.1109/TIT.2021.3079223>.
- Bapić A., Pasalic E.: A new method for secondary constructions of vectorial bent functions. *Des. Codes Cryptogr.* **89**(11), 2463–2475 (2021). <https://doi.org/10.1007/s10623-021-00930-3>.
- Bapić A., Pasalic E.: Constructions of (vectorial) bent functions outside the completed Maiorana-McFarland class. *Discret. Appl. Math.* **314**, 197–212 (2022). <https://doi.org/10.1016/j.dam.2022.02.010>.
- Bapić A., Pasalic E., Polujan A., Pott A.: Vectorial Boolean functions with the maximum number of bent components outside the $\mathcal{M}^\#$ class. In: Proceedings of the twelfth international workshop on coding and cryptography (2022). https://www.wcc2022.uni-rostock.de/storages/uni-rostock/Tagungen/WCC2022/Papers/WCC_2022_paper_9.pdf
- Bosma W., Cannon J., Playoust C.: The Magma algebra system. I. The user language. *J. Symb. Comput.* **24**(3–4), 235–265 (1997). <https://doi.org/10.1006/jsc.1996.0125>. Computational algebra and number theory (London, 1993)
- Budaghyan L., Carlet C.: On CCZ-equivalence and its use in secondary constructions of bent functions. In: Preproceedings of the international workshop on coding and cryptography, WCC 2009, pp. 19–36. Ullensvang, Norway (2009). <https://eprint.iacr.org/2009/042.pdf>
- Carlet C.: Two new classes of bent functions. In: T. Helleseht (ed.) *Advances in Cryptology—EUROCRYPT '93*. Lecture Notes in Computer Science, vol. 765, pp. 77–101. Springer, Berlin, Heidelberg (1993). https://doi.org/10.1007/3-540-48285-7_8
- Dillon J.F.: Elementary Hadamard difference sets. Ph.D. thesis, University of Maryland (1974). <https://doi.org/10.13016/M2MS3K194>
- Edel Y., Pott A.: On the equivalence of nonlinear functions. In: *Enhancing cryptographic primitives with techniques from error correcting codes*, pp. 87–103 (2009). <http://hdl.handle.net/1854/LU-710528>
- Effinger G., Mullen G.: *Elementary number theory* (2021). <https://doi.org/10.1201/9781003193111>.
- Kudin, S., Pasalic, E.: A complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^\#$ and a general framework for specifying bent functions in \mathcal{C} outside $\mathcal{M}^\#$. *Des. Codes Cryptogr.* **90**, 1783–1796 (2022). <https://doi.org/10.1007/s10623-022-01079-3>
- Kyureghyan G.M., Pott A.: Some theorems on planar mappings. In: J. von zur Gathen, J.L. Imaña, Ç.K. Koç (eds.) *Arithmetic of finite fields*, pp. 117–122. Springer, Berlin (2008). https://doi.org/10.1007/978-3-540-69499-1_10
- Mandal B., Stănică P., Gangopadhyay S., Pasalic E.: An analysis of the \mathcal{C} class of bent functions. *Fundam. Inform.* **146**, 271–292 (2016). <https://doi.org/10.3233/FI-2016-1386>.
- Meidl W., Polujan A.A., Pott A.: Linear codes and incidence structures of bent functions and their generalizations. *Discret. Math.* **346**(1), 113157 (2023). <https://doi.org/10.1016/j.disc.2022.113157>.
- Mesnager S., Zhang F., Tang C., Zhou Y.: Further study on the maximum number of bent components of vectorial functions. *Des. Codes Cryptogr.* **87**, 2597–2610 (2019). <https://doi.org/10.1007/s10623-019-00639-4>.
- Nyberg K.: Perfect nonlinear S-Boxes. In: *Advances in cryptography—EUROCRYPT '91*, workshop on the theory and application of cryptographic techniques, Brighton, UK, April 8–11, 1991, Proceedings, Lecture Notes in Computer Science, vol. 547, pp. 378–386. Springer (1991). https://doi.org/10.1007/3-540-46416-6_32
- Pasalic E., Bapić A., Zhang F., Wei Y.: Explicit infinite families of bent functions outside $\mathcal{M}^\#$. *Des. Codes Cryptogr.*
- Polujan A., Pott A.: Towards the classification of quadratic vectorial bent functions in 8 variables. In: *The 7th international workshop on Boolean functions and their applications* (2022)
- Polujan A.A.: Boolean and vectorial functions: A design-theoretic point of view. Ph.D. thesis, Otto-von-Guericke-Universität Magdeburg (2021). <https://doi.org/10.25673/37956>
- Polujan A.A., Pott A.: Cubic bent functions outside the completed Maiorana-McFarland class. *Des. Codes Cryptogr.* **88**(9), 1701–1722 (2020). <https://doi.org/10.1007/s10623-019-00712-y>.
- Polujan A.A., Pott A.: On design-theoretic aspects of Boolean and vectorial bent functions. *IEEE Trans. Inf. Theory* **67**(2), 1027–1037 (2021). <https://doi.org/10.1109/TIT.2020.3040754>.
- Pott A., Pasalic E., Muratović-Ribić A., Bajrić S.: On the maximum number of bent components of vectorial functions. *IEEE Trans. Inf. Theory* **64**(1), 403–411 (2018). <https://doi.org/10.1109/TIT.2017.2749421>.
- Tang C., Zhou Z., Qi Y., Zhang X., Fan C., Helleseht T.: Generic construction of bent functions and bent idempotents with any possible algebraic degrees. *IEEE Trans. Inf. Theory* **63**(10), 6149–6157 (2017). <https://doi.org/10.1109/TIT.2017.2717966>.

24. Weng G., Feng R., Qiu W.: On the ranks of bent functions. *Finite Fields Their Appl.* **13**(4), 1096–1116 (2007). <https://doi.org/10.1016/j.ffa.2007.03.001>.
25. Zhang F., Cepak N., Pasalic E., Wei Y.: Further analysis of bent functions from \mathcal{C} and \mathcal{D} which are provably outside or inside $\mathcal{M}^\#$. *Discret. Appl. Math.* **285**, 458–472 (2020). <https://doi.org/10.1016/j.dam.2020.06.012>.
26. Zheng L., Kan H., Peng J., Tang D.: Constructing vectorial bent functions via second-order derivatives. *Discret. Math.* **344**(8), 112473 (2021). <https://doi.org/10.1016/j.disc.2021.112473>.
27. Zheng L., Peng J., Kan H., Jun L., Luo J.: On constructions and properties of (n, m) -functions with maximal number of bent components. *Des. Codes Cryptogr.* **88**, 2171–2186 (2020). <https://doi.org/10.1007/s10623-020-00770-7>.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.