Vectorial Boolean Functions with the Maximum Number of Bent Components outside the $\mathcal{M}^{\#}$ class

Amar Bapić[1], Enes Pasalic[1], Alexandr Polujan[2], and Alexander Pott[2]

[1] University of Primorska, FAMNIT & IAM, Glagoljaška 8, 6000 Koper, Slovenia
amar.bapic@famnit.upr.si, enes.pasalic6@gmail.com
[2] Otto-von-Guericke-Universität, Universitätsplatz 2, 39106, Magdeburg, Germany
alexandr.polujan@ovgu.de, alexander.pott@ovgu.de

Abstract. Vectorial Boolean functions with the maximum number of bent components, which are called MNBC functions in this article, were introduced recently and attracted a lot of attention from the research community. So far, all the known nontrivial constructions of MNBC functions belong to the completed Maiorana-McFarland class $\mathcal{M}^{\#}$. In this paper, we show for the first time the existence of nontrivial MNBC functions outside the $\mathcal{M}^{\#}$ class. We classify all MNBC functions in six variables and indicate that several equivalence classes can not be described, up to equivalence, by the Maiorana-McFarland construction. Based on the analysis of the obtained examples, we propose several infinite families of MNBC functions outside the $\mathcal{M}^{\#}$ class.

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

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 $m \,|\, n$, the *trace mapping* $Tr_m^n \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is given by $Tr_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{i \cdot m}}$. The mapping $Tr_1^n \colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called the *absolute trace*.

A mapping $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called an (n, m)-*function*. For $m = 1$, a function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ is called a *Boolean function* in n variables. Any (n, m)-function F can be written as $F(x) = (f_1(x), \ldots, f_m(x))$, where the Boolean functions f_i on $\mathbb{F}_2^n$ are called *coordinate functions* of F. The *Walsh transform* $W_f \colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ of a Boolean function $f \colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by $W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\lambda x)}$ for $\lambda \in \mathbb{F}_{2^n}$. A Boolean function $f \colon \mathbb{F}_{2^n} \to \mathbb{F}_2$, where $n = 2k$, is called *bent* if $|W_f(\lambda)| = 2^{n/2}$ for all $\lambda \in \mathbb{F}_{2^n}$. For a Boolean bent function $f \colon \mathbb{F}_{2^n} \to \mathbb{F}_2$, the Boolean function $\tilde{f} \colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined for any $u \in \mathbb{F}_{2^n}$ by $W_f(u) = 2^{\frac{n}{2}}(-1)^{\tilde{f}(u)}$, is also bent and is called the *dual* of f.

For (n, m)-functions, the bent property is introduced with the notion of *component functions* $F_\lambda \colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ 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 $\lambda \in \mathbb{F}_{2^m}^*$ 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 [10]. 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,m)-function, and g is an arbitrary (n,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. in [14] addressed for the first time the question about the maximum number of bent components for (n,n)-functions. 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 [19] for (n,m)-functions, for which the maximum number of bent components equals to $2^n - 2^{m-n/2}$.

Definition 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 $2^n - 2^{m-k}$.*

On the set of (n,m)-functions we define the following equivalence relations preserving the MNBC property [9,14]. Two (n,m)-functions F and F' are called *EA-equivalent*, if there exist two affine permutations $A_1 \colon \mathbb{F}_2^m \to \mathbb{F}_2^m$, $A_2 \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and an affine function $A_3 \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ 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 $\mathcal{G}_F = \{(x, F(x)) \colon x \in \mathbb{F}_{2^n}\}$ 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 [9,14,18], 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 $(x,y) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}} \mapsto (G(x,y), h(y))$, 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 $\mathcal{M}^\#$. By saying that an (n,m)-function F (either bent or MNBC) is *outside the $\mathcal{M}^\#$ class*, we mean that at least one bent component F_λ is EA-inequivalent to a member of $\mathcal{M}^\#$.

The construction of (n,m)-MNBC functions outside the $\mathcal{M}^\#$ class is a difficult theoretical problem. As presented in [1], all known nontrivial constructions of (n,m)-MNBC functions belong to the $\mathcal{M}^\#$ 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 [2,11,13]. In this article, we construct several infinite families of

nontrivial MNBC functions outside the $\mathcal{M}^\#$ class using the extension approach, considered recently in [8,11] 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 Section 2, we classify all MNBC functions in six variables and show that some of them are nontrivial and do not belong to the $\mathcal{M}^\#$ class. In the sequel, we present several constructions explaining the observed phenomenon. In Section 3, we propose a partial spread construction of MNBC functions. In Section 4, we provide constructions of MNBC functions outside $\mathcal{M}^\#$ stemming from several secondary constructions of Boolean bent functions. The paper is concluded in Section 5 and representatives of equivalence classes of MNBC functions on $\mathbb{F}_2^6$ are given in Appendix A.

2 Classification of MNBC functions in six variables

Recently, Polujan and Pott [13] classified all vectorial bent functions in six variables. 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. *Let n be even and let F be an (n, m)-function. Let the linear code $\mathcal{C}_F$ 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 $(1, x, F(x))^T_{x\in\mathbb{F}_{2^n}}$. We call an (n, m)-MNBC function F with $n/2 + 1 \leq m \leq n$ a t-step extension if $\dim(\mathcal{C}_F) = 1 + n + n/2 + t$, where $1 \leq t \leq n/2$.*

With this definition, an (n, m)-MNBC function is trivial, if it is a 0-step extension. More general, if an (n, m)-MNBC function F is a t-step extension, then F is EA-equivalent to an $(n, n/2 + t)$-MNBC function F'. We also note that if two MNBC functions F and F' are t-step and t'-step extensions with $t \neq t'$, then F and F' are CCZ-inequivalent, since inequivalent linear codes $\mathcal{C}_F$ and $\mathcal{C}_{F'}$ define CCZ-inequivalent functions [6, Theorem 9]. In the following proposition, we summarize our computational results about the classification of MNBC functions in six variables.

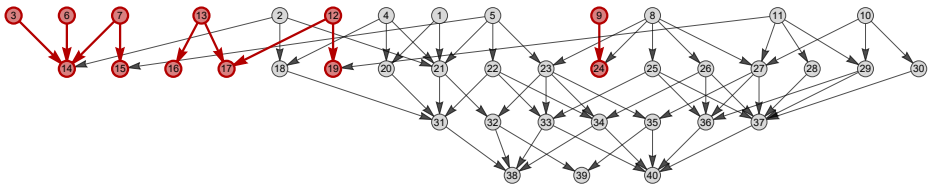
Proposition 1. *On $\mathbb{F}_2^6$, there exist 40 CCZ-equivalence classes of MNBC functions. Among them, there are:*

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

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

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 [14,19], one can represent F in the form $F(x) = (b_1(x), \ldots, b_{n/2}(x), n_1(x), \ldots, n_{m-n/2}(x))$, where all b_i are bent, all n_j are non-bent and $\langle n_1, \ldots, n_{m-n/2} \rangle$ 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 $F'(x) = (b_1(x), \ldots, b_{n/2}(x), b_{n/2+1}(x), \ldots, b_m(x))$, where $b_{n/2+i} := b_i + n_i$ is bent for $1 \leq i \leq m - n/2$, since by definition of an MNBC function all non-bent components of F belong to $\langle n_1, \ldots, n_{m-n/2} \rangle$. 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 [13] and extend them recursively to $(6, m)$-MNBC functions by appending at each step a Boolean bent function without affine terms exhaustively. We check CCZ-equivalence of MNBC functions F and F' via equivalence of linear codes $\mathcal{C}_F$ and $\mathcal{C}_{F'}$ (see [6, Theorem 9]) with the algebra system Magma. With the implementation [12, Algorithm 1] of the second-order derivative criterion [5, Remark 6.3.17] applied coordinate-wise to all EA-equivalence classes of a CCZ-equivalence class, we check whether a CCZ-equivalence class belongs to $\mathcal{M}^{\#}$. Finally, the extension relation between the obtained CCZ-equivalence classes is given in Fig. 1 and look-up tables of representatives are given in the Appendix, see Table 1.

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 $\mathcal{M}^{\#}$.



With these computational results, one can see that even in a small number of variables, nontrivial MNBC functions outside $\mathcal{M}^{\#}$ exist. In the sequel, we provide several theoretical constructions of 1-step extension MNBC functions outside the $\mathcal{M}^{\#}$ class.

3 Partial spread construction of MNBC functions

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

Definition 3. *A partial spread of order s in $\mathbb{F}_2^n$ with $n = 2k$ is a set of s vector subspaces $U_1, \ldots, U_s$ 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 $\mathbb{1}_U : \mathbb{F}_2^n \to \mathbb{F}_2$ 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 [5] introduced a partial spread construction of bent functions, which includes 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 $U_1, \ldots, U_{2^{k-1}+1}$ 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 $U_1, \ldots, U_{2^{k-1}}$ 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 $f\colon (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \mapsto h\,(x/y)$, where $x/y = 0$ if $y = 0$ for $x, y \in \mathbb{F}_{2^k}$ and $h\colon \mathbb{F}_{2^k} \to \mathbb{F}_2$ 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 $F\colon (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \mapsto H\,(x/y)$, 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 on, whose bent components belong to both $\mathcal{PS}_{ap}$ and $\mathcal{PS}^+$ classes.

Theorem 1. *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 $U = \{(0, y)\colon y \in \mathbb{F}_{2^k}\}$. Then the function $F\colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2^{k+1}$ defined as*

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

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

Proof. Since $\mathbb{1}_U\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is the indicator of the vector space U of dimension k, we have $wt(\mathbb{1}_U) = 2^k$ 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

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

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. □

Remark 1. 1. In the same way, one can show that for the spread line $U = \{(x,0)\colon x \in \mathbb{F}_{2^k}\}$ 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 [16] 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 [13, Table IV.2.]).

4 MNBC functions stemming from $\mathcal{C}$ and $\mathcal{D}_0$ classes

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 [3]. This construction is based on the property (P_U), which was introduced in [15] and has several applications in the construction of vectorial Boolean bent functions [18] and MNBC functions [3].

Definition 4. *Let $n, \tau \in \mathbb{N}$ with $\tau \leq n/2$ and let $g\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$. Then g is said to satisfy property (P_U) with the defining set $U = \{u_1, \ldots, u_\tau\} \subset \mathbb{F}_{2^n}$ 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 [3], Bapić and Pasalic generalized the results of [18] and provided the following generic method for the construction of MNBC functions. Below we give a slightly reformulated version of [3, Construction 2].

Construction 2 *Let $n = 2k$ and let $U = \{u_1, \ldots, u_\tau\}$ be a set of $\tau \leq k$ linearly independent elements in $\mathbb{F}_{2^n}^*$. Let $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$ 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 $\mathbf{h}\colon \mathbb{F}_2^\tau \to \mathbb{F}_{2^s}$ be any (τ, s)-function. Then for any $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, the function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined as follows*

$$F(x) = G(x) + \gamma \mathbf{h}(Tr_1^n(u_1 x), \ldots, Tr_1^n(u_\tau x)), \tag{2}$$

has the maximum number of bent components.

In [3], it was shown that several Maiorana-McFarland vectorial bent functions $G\colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ satisfy the conditions of Construction 2. Now we show that for these vectorial bent functions $G\colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ one can specify a vectorial function $\mathbf{h}$, such that MNBC functions, obtained via Construction 2, 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 [4] is the set of Boolean functions $f\colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ of the form

$$f(x, y) = Tr_1^k(x\pi(y)) + \mathbb{1}_{L^\perp}(x), \tag{3}$$

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 $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ 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 [17], the following set of sufficient conditions for Boolean bent functions in $\mathcal{C} \setminus \mathcal{M}^\#$ class was proposed.

Theorem 3. *[17, 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 2 and Theorem 3, we obtain the following family of MNBC functions outside the $\mathcal{M}^\#$ class.

Theorem 4. *Let $U = \{u_1, \ldots, u_\tau\}$ be a set of τ linearly independent elements in $\mathbb{F}_{2^k}^*$, where $n = 2k \geq 8$ and $\tau \,|\, k$. 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 $\mathbf{h} : \mathbb{F}_2^\tau \to \mathbb{F}_2$ be defined by*

$$\mathbf{h}(X_1, \ldots, X_\tau) = \prod_{i=1}^{\tau}(X_i + 1). \tag{4}$$

If $((\lambda\pi)^{-1}, \langle U\rangle)$ satisfies the (C) property and the conditions of Theorem 3 for all $\lambda \in \mathbb{F}_{2^k}^*$, then the (n,n)-function F constructed from G and $\mathbf{h}$ as

$$F(x,y) = G(x,y) + \gamma \mathbf{h}(Tr_1^k(u_1 x), \ldots, Tr_1^k(u_\tau x)), \tag{5}$$

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 2, 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 3 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 $G(x,y) = (g_1(x,y), \ldots, g_k(x,y))$, where $g_i \colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ for all $1 \le i \le k$. Since $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, we can construct the function F' in the following form $F'(x,y) = (g_1(x,y), \ldots, g_k(x,y), g_{k+1}(x,y))$, where $g_{k+1}(x,y) := \mathbf{h}(Tr_1^k(u_1 x), \ldots, Tr_1^k(u_\tau x))$. 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 [2, 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 2. *Let $k \ge 4$ and s be a positive divisor of k such that k/s is odd. Let $U = \{1, \alpha, \ldots, \alpha^{\tau-1}\}$ 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 $wt(d) \ge 3$ 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*

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

where $\mathbf{h}$ is defined by (4), is a 1-step extension (n,n)-MNBC function outside the $\mathcal{M}^{\#}$ class.

Proof. By [3, Proposition 3], the dual bent components $\tilde{G}_\lambda$ 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 2, 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 $F_\lambda(x,y) = Tr_1^k(\lambda x y^d) + \mathbb{1}_{\langle U\rangle^{\perp}}(x)$. 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 [7, Theorem 5.8]. Since $wt(d) \geq 3$, by [17, Proposition 5] it follows that $Tr_1^k(\lambda\pi)$ has no nonzero linear structures. Thus by Theorem 3 it follows that F_λ is in $\mathcal{C}$ outside $\mathcal{M}^\#$. Hence, F is outside $\mathcal{M}^\#$. Finally, from Theorem 4, we conclude that F is a 1-step extension. □

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

$$f(x, y) = Tr_1^k(x\pi(y)) + \delta_0(x) \quad \text{for } x, y \in \mathbb{F}_{2^k}, \tag{6}$$

where π is a permutation on $\mathbb{F}_{2^k}$, whose restriction to any linear hyperplane of $\mathbb{F}_{2^k}$ is not affine, are bent and outside the $\mathcal{M}^\#$ class [4]. The set of the Boolean bent functions of the form (6) is called $\mathcal{D}_0$ *class* of Boolean bent functions. With the use of bent functions from $\mathcal{D}_0$ class, one can derive the following family of MNBC functions following the main steps of the proof of Theorem 4.

Theorem 5. *Let $n = 2k \geq 8$ and let $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$. Let π be a permutation on $\mathbb{F}_{2^k}$ whose restriction to any linear hyperplane of $\mathbb{F}_{2^k}$ is not affine. Then the (n, n)-function F defined by*

$$F(x, y) = x\pi(y) + \gamma\delta_0(x) \text{ for } x, y \in \mathbb{F}_{2^k}, \tag{7}$$

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

5 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. Finally, we would like to mention some open problems.

1. In Sections 3 and 4, we proposed several constructions of 1-step extensions MNBC functions outside the $\mathcal{M}^\#$ class. A further research direction is to construct t-step extensions (n, k)-MNBC functions outside $\mathcal{M}^\#$ for $t \geq 2$.
2. In $n = 6$ variables, all $(n/2 - 1)$-step and $n/2$-step extensions 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 extensions MNBC functions outside $\mathcal{M}^\#$ can in general exist for $n > 6$.

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).

References

1. Anbar, N., Kalaycı, T., Meidl, W.: Analysis of (n, n)-functions obtained from the Maiorana-McFarland class. IEEE Transactions on Information Theory **67**(7), 4891–4901 (2021). (p. 2.)
2. Bapić, A., Pasalic, E.: Constructions of (vectorial) bent functions outside the completed Maiorana-McFarland class. Submitted. (pp. 2 and 8.)
3. Bapić, A., Pasalic, E.: A new method for secondary constructions of vectorial bent functions. Designs, Codes and Cryptography (2021). (pp. 6, 7, and 8.)
4. Carlet, C.: Two new classes of bent functions. vol. 765, pp. 77–101 (1993). (pp. 7 and 9.)
5. Dillon, J.F.: Elementary Hadamard difference sets. Ph.D. thesis, University of Maryland (1974). (pp. 4 and 5.)
6. Edel, Y., Pott, A.: On the equivalence of nonlinear functions. In: Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, pp. 87–103 (2009). (pp. 3 and 4.)
7. Mandal, B., Stănică, P., Gangopadhyay, S., Pasalic, E.: An analysis of the $\mathcal{C}$ class of bent functions. Fundamenta Informaticae **146**, 271–292 (2016). (p. 9.)
8. Meidl, W., Polujan, A.A., Pott, A.: Linear codes and incidence structures of bent functions and their generalizations. ArXiv abs/2012.06866 (2020). (p. 3.)
9. Mesnager, S., Zhang, F., Tang, C., Zhou, Y.: Further study on the maximum number of bent components of vectorial functions. Designs, Codes and Cryptography **87**, 2597–2610 (2019). (p. 2.)
10. Nyberg, K.: Perfect nonlinear S-Boxes. In: Advances in Cryptology - EUROCRYPT '91. Lecture Notes in Computer Science, vol. 547, pp. 378–386. Springer (1991). (p. 2.)
11. Polujan, A.A.: Boolean and vectorial functions: A design-theoretic point of view. Ph.D. thesis, Otto-von-Guericke-Universität Magdeburg (2021). (pp. 2 and 3.)
12. Polujan, A.A., Pott, A.: Cubic bent functions outside the completed Maiorana-McFarland class. Designs, Codes and Cryptography **88**(9), 1701–1722 (2020). (p. 4.)
13. Polujan, A.A., Pott, A.: On design-theoretic aspects of Boolean and vectorial bent functions. IEEE Transactions on Information Theory **67**(2), 1027–1037 (2021). (pp. 2, 3, 4, 6, and 11.)
14. Pott, A., Pasalic, E., Muratović-Ribić, A., Bajrić, S.: On the maximum number of bent components of vectorial functions. IEEE Transactions on Information Theory **64**(1), 403–411 (2018). (pp. 2 and 4.)
15. Tang, C., Zhou, Z., Qi, Y., Zhang, X., Fan, C., Helleseth, T.: Generic construction of bent functions and bent idempotents with any possible algebraic degrees. IEEE Transactions on Information Theory **63**(10), 6149–6157 (2017). (p. 6.)
16. Weng, G., Feng, R., Qiu, W.: On the ranks of bent functions. Finite Fields and Their Applications **13**(4), 1096–1116 (2007). (p. 6.)
17. 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). (pp. 7 and 9.)
18. Zheng, L., Kan, H., Peng, J., Tang, D.: Constructing vectorial bent functions via second-order derivatives. Discrete Mathematics **344**(8), 112473 (2021). (pp. 2 and 6.)
19. Zheng, L., Peng, J., Kan, H., Jun, L., Luo, J.: On constructions and properties of (n, m)-functions with maximal number of bent components. Designs, Codes and Cryptography **88**, 2171–2186 (2020). (pp. 2 and 4.)

A MNBC functions in six variables

In Table 1, we list look-up tables of representatives of CCZ-equivalence classes of MNBC functions in $n = 6$ variables. The representatives f_i of CCZ-equivalence classes $1 \le i \le 13$ have the form $f_i = (F_i^3, 0)$, where F_i^3 is a vectorial $(6, 3)$-bent function in [13, Table A2(c)] and 0 is the null-vector. For convenience, we sort the first 13 CCZ-equivalence classes in Table 1 as in Fig. 1. The look-up table of the representative f_i is given by the list $[f_i(0), f_i(1), \ldots, f_i(j), \ldots, f_i(2^n - 1)]$, where both input $0 \le j \le 2^n - 1$ and output $0 \le f_i(j) \le 2^n - 1$ are integers. For an integer $j = \sum_{i=1}^{n} x_i 2^{n-i}$, its binary representation is given by the vector $(x_1, \ldots, x_n) \in \mathbb{F}_2^n$.

Table 1. Look-up tables of CCZ-inequivalent MNBC functions in six variables.

i	Look-up table of a representative f_i of the CCZ-equivalence class i
	0-step extensions
3	[0,0,0,0,0,0,1,1,0,4,0,4,2,6,3,7,0,1,6,7,2,3,5,4,0,5,6,3,0,5,7,2,0,2,2,0,5,7,6,4,1,7,3,5,6,0,5,3,0,3,4,7,7,4,2,1,1,6,5,2,4,3,1,6]
6	[0,0,0,1,0,3,0,2,0,4,0,5,1,6,1,7,0,0,4,5,0,2,4,7,2,6,6,3,3,5,7,0,0,1,2,2,5,7,7,4,2,6,0,5,6,1,4,2,1,1,7,6,6,4,0,3,5,0,3,7,3,4,5,3]
7	[0,0,0,1,0,2,1,2,0,4,1,4,0,6,1,6,0,0,5,4,1,3,5,6,2,6,6,3,3,5,7,0,0,0,2,3,4,6,7,4,3,7,0,5,7,1,4,3,1,1,7,6,6,4,1,2,4,0,3,6,3,5,4,3]
13	[0,0,0,1,0,7,4,3,0,5,7,2,5,3,6,1,0,4,0,4,1,2,3,1,0,3,4,6,4,4,2,2,0,0,0,1,5,3,0,6,1,4,6,3,3,4,1,7,2,6,3,7,4,6,6,5,6,5,3,1,7,6,1,0]
2	[0,0,0,0,0,0,0,0,0,4,1,5,2,6,3,7,0,1,7,6,3,2,4,5,0,5,6,3,1,4,7,2,0,2,3,1,5,7,6,4,0,6,2,4,7,1,5,3,1,2,5,6,7,4,3,0,1,6,4,3,5,2,0,7]
12	[0,0,0,1,0,6,4,3,0,4,7,2,4,2,6,1,0,5,0,4,0,2,2,1,1,3,4,7,5,4,3,3,0,1,1,0,5,2,1,6,0,4,6,2,3,5,1,7,2,7,2,7,4,6,7,5,7,4,2,1,7,7,0,0]
4	[0,0,0,0,0,0,0,0,0,4,1,5,2,6,3,7,0,1,7,6,3,2,4,5,0,5,6,3,1,4,7,2,0,2,3,1,5,7,6,4,0,6,2,4,7,1,5,3,0,3,4,7,6,5,2,1,1,6,4,3,5,2,0,7]
1	[0,0,0,0,0,0,0,0,0,4,1,5,2,6,3,7,0,1,7,6,3,2,4,5,0,5,6,3,1,4,7,2,0,2,3,1,5,7,6,4,0,6,2,4,7,1,5,3,0,3,4,7,6,5,2,1,0,7,5,2,4,3,1,6]
5	[0,0,0,1,0,2,0,3,0,4,0,5,0,6,0,7,0,0,5,4,1,3,4,7,2,6,7,2,3,5,6,1,0,0,2,3,4,6,6,5,3,7,1,4,7,1,5,2,0,0,6,7,7,5,1,2,5,1,3,6,2,4,4,3]
9	[0,0,0,3,0,0,5,6,0,1,7,5,0,0,2,1,0,5,1,6,2,7,2,5,2,6,6,0,1,4,4,3,0,1,0,2,4,5,1,3,2,2,5,6,6,7,4,6,4,2,5,1,3,5,3,7,1,6,5,0,7,1,2,6]
8	[0,0,3,0,0,5,6,0,0,7,4,0,0,2,1,0,5,0,7,2,7,3,4,3,6,6,1,1,4,5,2,0,1,0,2,4,5,1,3,2,3,5,7,6,7,4,6,4,2,4,0,3,5,2,6,0,6,5,1,7,1,3,7]
11	[0,0,0,0,0,6,5,3,0,5,7,2,5,2,6,1,0,4,1,5,1,2,3,0,0,2,4,6,4,5,2,3,0,0,0,0,4,2,1,7,1,4,6,3,3,4,0,7,3,7,2,6,4,7,6,5,7,5,3,1,6,7,0,1]
10	[0,0,0,0,0,6,5,3,0,5,7,2,4,3,7,0,0,4,1,5,0,3,2,1,0,2,4,6,4,5,2,3,0,0,0,0,4,2,1,7,1,4,6,3,2,5,1,6,3,7,2,6,5,6,7,4,7,5,3,1,6,7,0,1]
	1-step extensions
14	[0,0,0,0,0,0,1,1,0,8,2,10,4,12,7,15,0,2,15,13,6,4,8,10,1,11,12,6,3,9,15,5,0,5,6,3,11,14,12,9,1,12,5,8,14,3,11,6,2,5,11,12,15,8,7,0,2,13,9,6,11,4,1,14]
15	[0,0,0,2,0,4,1,7,0,9,1,10,1,12,0,15,0,0,11,9,2,6,8,14,4,13,14,5,7,10,13,2,0,0,4,6,9,13,12,10,6,15,3,8,14,3,11,4,0,0,13,15,15,11,3,5,11,2,7,12,5,8,9,6]
16	[0,0,0,2,0,15,8,7,0,10,15,5,11,6,12,3,0,8,0,8,2,5,7,2,1,6,9,12,9,9,4,4,0,0,0,2,10,7,0,13,2,8,13,7,6,9,3,14,5,13,7,15,8,13,13,10,12,11,6,3,14,12,3,1]
17	[0,0,0,2,0,13,9,7,0,8,14,5,8,5,13,2,0,10,1,8,0,5,5,2,2,7,8,15,10,8,6,7,0,3,3,1,11,4,3,12,1,9,12,4,7,11,3,14,4,14,4,14,8,12,14,11,15,9,4,3,14,14,1,1]
18	[0,0,0,0,0,0,0,0,0,8,2,10,5,13,7,15,0,2,15,13,7,5,8,10,0,10,13,7,2,8,15,5,0,5,7,2,10,15,13,8,0,13,5,8,15,2,10,7,2,5,10,13,15,8,7,0,3,12,9,6,11,4,1,14]
19	[0,0,0,1,0,13,11,7,0,11,15,5,11,5,13,2,0,9,3,11,3,5,6,1,1,4,8,12,9,11,4,7,0,1,1,0,9,5,2,14,3,8,13,6,7,9,1,15,6,15,5,12,8,14,12,10,15,11,6,2,12,15,0,3]
20	[0,0,0,0,0,0,0,0,0,8,2,10,5,13,7,15,0,2,15,13,7,5,8,10,0,10,13,7,2,8,15,5,0,5,7,2,10,15,13,8,0,13,5,8,15,2,10,7,0,7,8,15,13,10,5,2,1,14,11,4,9,6,3,12]
21	[0,0,0,0,0,0,0,0,0,8,2,10,5,13,7,15,0,2,15,13,7,5,8,10,0,10,13,7,2,8,15,5,0,5,7,2,10,15,13,8,0,13,5,8,15,2,10,7,1,6,9,14,12,11,4,3,1,14,11,4,9,6,3,12]
22	[0,0,0,2,0,4,0,6,0,9,0,11,0,13,0,15,0,0,11,9,2,6,9,15,4,13,15,4,6,11,13,2,0,0,4,6,9,13,13,11,6,15,2,9,15,2,11,4,0,1,13,14,15,10,2,5,11,3,6,12,4,8,9,7]
23	[0,0,0,2,0,4,0,6,0,9,0,11,0,13,0,15,0,0,11,9,2,6,9,15,4,13,15,4,6,11,13,2,0,1,4,7,9,12,13,10,6,14,2,8,15,3,11,5,0,1,13,14,15,10,2,5,11,3,6,12,4,8,9,7]
24	[0,0,0,7,0,1,10,12,0,0,15,8,0,0,5,2,0,10,0,15,5,15,7,8,7,13,13,2,2,9,10,4,0,2,0,5,8,11,2,6,5,7,10,15,13,15,8,13,8,5,8,0,7,10,5,13,0,13,10,2,15,3,7,14]
25	[0,0,0,7,0,0,10,13,0,0,15,8,0,0,5,2,0,10,0,15,5,15,7,8,7,13,13,2,2,8,10,5,0,2,0,5,8,10,2,7,5,7,10,15,13,15,8,13,8,5,9,1,7,10,4,12,0,13,11,3,15,2,6,14]
26	[0,0,0,7,0,0,10,13,0,0,15,8,0,0,5,2,0,10,0,15,5,15,7,8,7,13,13,2,2,8,10,5,0,2,1,4,8,10,3,6,5,7,11,14,13,15,9,12,8,5,8,0,7,10,5,13,0,13,10,2,15,2,7,15]
27	[0,0,0,7,0,0,10,13,0,0,15,8,0,0,5,2,0,10,0,15,5,15,7,8,7,13,13,2,2,8,10,5,0,2,1,4,8,10,3,6,5,7,11,14,13,15,9,12,8,5,9,1,7,10,4,12,0,13,11,3,15,2,6,14]
28	[0,0,0,0,0,13,10,7,0,10,15,5,11,4,12,3,0,8,2,10,2,5,7,0,1,4,9,12,9,11,4,6,0,0,0,0,8,5,2,15,2,8,13,7,6,9,1,14,7,15,5,13,8,15,13,10,14,11,6,3,12,14,1,3]
29	[0,0,0,0,0,13,10,7,0,10,15,5,8,7,15,0,0,8,2,10,0,7,5,2,0,5,8,13,9,11,4,6,0,0,0,0,8,5,2,15,2,8,13,7,5,10,2,13,7,15,5,13,10,13,15,8,15,10,7,2,12,14,1,3]
30	[0,0,0,0,0,13,10,7,0,10,15,5,9,6,14,1,0,8,2,10,0,7,5,2,1,4,9,12,9,11,4,6,0,0,0,0,8,5,2,15,2,8,13,7,4,11,3,12,7,15,5,13,10,13,15,8,14,11,6,3,12,14,1,3]
	2-step extensions
31	[0,0,0,0,0,0,0,0,0,16,4,20,11,27,15,31,0,4,31,27,15,11,16,20,0,20,27,15,4,16,31,11,0,11,15,4,20,31,27,16,0,27,11,16,31,4,20,15,2,13,18,29,25,22,9,6,3,28,23,8,19,12,7,24]
32	[0,0,0,0,0,0,0,0,0,16,4,20,11,27,15,31,0,4,31,27,15,11,16,20,0,20,27,15,4,16,31,11,0,11,15,4,20,31,27,16,1,26,10,17,30,5,21,14,2,13,18,29,25,22,9,6,3,28,23,8,19,12,7,24]
33	[0,0,0,4,0,8,0,12,0,19,0,23,0,27,0,31,0,0,23,19,4,12,19,31,8,27,31,8,12,23,27,4,0,2,8,14,19,25,27,21,12,29,4,17,31,6,23,10,0,3,27,28,31,20,4,11,23,7,12,24,8,16,19,15]
34	[0,0,0,4,0,8,0,12,0,19,0,23,0,27,0,31,0,1,23,18,4,13,19,30,8,26,31,9,12,22,27,5,0,2,8,14,19,25,27,21,12,29,4,17,31,6,23,10,0,2,27,29,31,21,4,10,23,6,12,25,8,17,19,14]
35	[0,0,0,4,0,8,0,12,0,19,0,23,0,27,0,31,0,1,23,18,4,13,19,30,8,26,31,9,12,22,27,5,0,2,8,14,19,25,27,21,12,29,4,17,31,6,23,10,0,3,27,28,31,20,4,11,23,7,12,24,8,16,19,15]
36	[0,0,0,15,0,0,20,27,0,0,31,16,0,0,11,4,0,20,0,31,11,31,15,16,15,27,27,4,4,16,20,11,0,4,2,9,16,20,6,13,11,15,22,29,27,31,18,25,16,11,19,3,15,20,8,24,0,27,23,7,31,4,12,28]
37	[0,0,0,15,0,0,20,27,0,0,31,16,0,0,11,4,0,20,1,30,11,31,14,17,15,27,26,5,4,16,21,10,0,4,2,9,16,20,6,13,11,15,22,29,27,31,18,25,16,11,18,2,15,20,9,25,0,27,22,6,31,4,13,29]
	3-step extensions
38	[0,0,0,0,0,0,0,0,0,32,8,40,23,55,31,63,0,8,63,55,31,23,32,40,0,40,55,31,8,32,63,23,0,23,31,8,40,63,55,32,2,53,21,34,61,10,42,29,4,27,36,59,51,44,19,12,7,56,47,16,39,24,15,48]
39	[0,0,0,0,0,0,0,0,0,32,8,40,23,55,31,63,0,8,63,55,31,23,32,40,1,41,54,30,9,33,62,22,0,23,31,8,40,63,55,32,2,53,21,34,61,10,42,29,4,27,36,59,51,44,19,12,7,56,47,16,39,24,15,48]
40	[0,0,0,8,0,16,0,24,0,39,0,47,0,55,0,63,0,2,47,37,8,26,39,61,16,53,63,18,24,45,55,10,0,4,16,28,39,51,55,43,24,59,8,35,63,12,47,20,0,7,55,56,63,40,8,23,47,15,24,48,16,32,39,31]