On bent functions satisfying the dual bent condition

Alexandr Polujan[1], Enes Pasalic[2], Sadmir Kudin[2], Fengrong Zhang[3,4]

[1] Otto-von-Guericke-Universität, Universitätsplatz 2, 39106, Magdeburg, Germany
alexandr.polujan@gmail.com

[2] University of Primorska, FAMNIT & IAM, Glagoljaška 8, 6000 Koper, Slovenia
{enes.pasalic6@gmail.com, sadmir.kudin@iam.upr.si}

[3] State Key Laboratory of Integrated Services Networks,
Xidian University, Xian 710071, P.R. China

[4] Mine Digitization Engineering Research Center of Ministry of Education,
China University of Mining and Technology, Xuzhou, Jiangsu 221116, China
zhfl203@163.com

Abstract

For a concatenation of four bent functions $f = f_1||f_2||f_3||f_4$, the necessary and sufficient condition that f is bent is that the *dual bent condition* is satisfied [5, Theorem III.1], i.e., $f_1^*+f_2^*+f_3^*+f_4^* = 1$. However, specifying four bent functions satisfying this duality condition is in general quite a difficult task. Commonly, to simplify this problem, certain connections between f_i are assumed such as the one considered originally in [4] and later analyzed in [2]. Among them, is the construction method of bent functions satisfying the dual bent condition using the permutations of $\mathbb{F}_2^m$ with the $(\mathcal{A}_m)$ property [2, Theorem 7]. In this paper, we generalize this result and provide a construction of new permutations with the $(\mathcal{A}_m)$ property from the old ones. Combining these two results, we obtain a recursive construction method of bent functions satisfying the dual bent condition. Consequently, we provide a condition on the functions f_1, f_2, f_3, f_4, such that obtained with our approach bent functions are not equivalent to Maiorana-McFarland ones. Finally, with our construction method, we explain how one can construct homogeneous cubic bent functions, of which constructions only very few are known.

Keywords: Boolean bent function, dual bent condition, Maiorana-McFarland class, bent 4-concatenation, equivalence.

1 Preliminaries

Let $n = 2m$ and let $\mathcal{B}_n$ denote the set of Boolean functions in n variables. A function $f \in \mathcal{B}_n$ is called *bent*, if for all non-zero $a \in \mathbb{F}_2^n$ the first-order derivatives $D_a f(x) = f(x + a) + f(x)$ are balanced. Let $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$ be four bent functions satisfying the dual bent condition. Then the function $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ defined by

$$f(z, z_{n+1}, z_{n+2}) = f_1(z)+z_{n+1}(f_1+f_3)(z)+z_{n+2}(f_1+f_2)(z)+z_{n+1}z_{n+2}(f_1+f_2+f_3+f_4)(z) \quad (1.1)$$

is bent and called the *bent 4-concatenation* of f_1, f_2, f_3, f_4, see [1]. As the following result shows, the dual bent condition could be satisfied [2] by using Maiorana-McFarland bent functions arising from permutations with the $(\mathcal{A}_m)$ property [6], which means that for three permutations π_i of $\mathbb{F}_2^m$, we have that $\pi_1 + \pi_2 + \pi_3 = \pi$ is also a permutation and $\pi^{-1} = \pi_1^{-1} + \pi_2^{-1} + \pi_3^{-1}$.

Theorem 1.1. *[2, Theorem 7] Let $f_j(x, y) = Tr(x\pi_j(y))+h_j(y)$ for $j \in \{1, 2, 3\}$ and $x, y \in \mathbb{F}_{2^m}$, where the permutations π_j satisfy the condition $(\mathcal{A}_m)$. If the functions h_j satisfy*

$$h_1(\pi_1^{-1}(x)) + h_2(\pi_2^{-1}(x)) + h_3(\pi_3^{-1}(x)) + (h_1 + h_2 + h_3)((\pi_1 + \pi_2 + \pi_3)^{-1}(x)) = 1, \quad (1.2)$$

then f_1, f_2, f_3 satisfy $f_1^* + f_2^* + f_3^* + f_4^* = 1$, where $f_1 + f_2 + f_3 = f_4$.

2 Constructing bent functions satisfying the dual bent condition recursively

First, we provide a generalization of Theorem 1.1. We omit the proof of this statement in order to explain in detail those results, which are more technical.

Theorem 2.1. *Let $f_j(x,y) = Tr\left(x\pi_j(y)\right) + h_j(y)$ for $j \in \{1,2,3\}$ and $x, y \in \mathbb{F}_{2^m}$ with $n = 2m$, where the permutations π_j satisfy the condition $(\mathcal{A}_m)$, and let $s \in \mathcal{B}_m$. Define a function $h_4 \in \mathcal{B}_m$ as $h_4 = h_1 + h_2 + h_3 + s$ and a bent function $f_4 \in \mathcal{B}_n$ as $f_4 = f_1 + f_2 + f_3 + s$. If the functions h_j satisfy*

$$h_1\left(\pi_1^{-1}(x)\right) + h_2\left(\pi_2^{-1}(x)\right) + h_3\left(\pi_3^{-1}(x)\right) + h_4\left(\left(\pi_1 + \pi_2 + \pi_3\right)^{-1}(x)\right) = 1, \tag{2.1}$$

then $f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is bent.

In the following example, we show the existence of permutations π_i and functions h_i with $h_4 \neq h_1 + h_2 + h_3$ satisfying the conditions of Theorem 2.1.

Example 2.2. Define the permutations π_i on $\mathbb{F}_2^4$ as follows:

$$\pi_1(y) = \begin{pmatrix} y_1 + y_2 + y_1y_4 + y_2y_4 + y_3y_4 \\ y_1 + y_1y_2 + y_3 + y_2y_3 + y_2y_4 \\ y_1y_2 + y_3 + y_1y_3 + y_2y_4 + y_3y_4 \\ y_1 + y_3 + y_1y_3 + y_2y_3 + y_4 + y_1y_4 + y_2y_4 \end{pmatrix}, \pi_2(y) = \pi_1(y) + \begin{pmatrix} y_2 + y_3 + y_4 \\ 1 + y_2 + y_3 + y_4 \\ y_1 + y_3 \\ y_1 + y_3 \end{pmatrix},$$

$$\pi_3(y) = \pi_1(y) + \begin{pmatrix} y_1 + y_4 \\ y_1 + y_2 \\ 1 + y_1 + y_2 \\ 1 + y_1 + y_4 \end{pmatrix}, \pi_4(y) = (\pi_1 + \pi_2 + \pi_3)(y).$$

The algebraic normal forms of the functions h_i are given as follows:

$$\begin{aligned} &h_1(y) = y_1y_3y_4, \quad h_2(y) = y_2y_3 + y_1y_4 + y_2y_4 + y_3y_4 + y_1y_3y_4, \\ &h_3(y) = y_1y_3 + y_2y_3 + y_3y_4 + y_1y_3y_4, \quad h_4(y) = (h_1 + h_2 + h_3)(y) + s(y), \end{aligned}$$

where $s(y) = y_1 + y_2 + y_4$. One can check that the defined above permutations π_i of $\mathbb{F}_2^4$, satisfy the $(\mathcal{A}_4)$ property. Moreover, the condition (2.1) is satisfied as well, and thus by Theorem 2.1, we have that $f_1||f_2||f_3||f_4 \in \mathcal{B}_{10}$ is bent for bent functions $f_i(x,y) = x \cdot \pi_i(y) + h_i(y)$, where $x, y \in \mathbb{F}_2^4$.

Now, we show that as soon as a single example of such permutations π_i on $\mathbb{F}_2^m$ and Boolean functions h_i on $\mathbb{F}_2^m$ is found (here m is a fixed integer), then one can always construct many such examples on $\mathbb{F}_2^k$, where $k > m$ is an arbitrary integer.

Lemma 2.3. *Let σ_1, σ_2 be permutations of $\mathbb{F}_2^m$. Define the function $\pi\colon \mathbb{F}_2^{m+1} \to \mathbb{F}_2^{m+1}$ by*

$$\pi(y, y_{m+1}) = \left(y_{m+1}\sigma_1(y) + (1 + y_{m+1})\sigma_2(y), y_{m+1}\right), \text{ for all } y \in \mathbb{F}_2^m, y_{m+1} \in \mathbb{F}_2.$$

Then, π is a permutation, and its inverse on $\mathbb{F}_2^{m+1}$ is given by the permutation ρ on $\mathbb{F}_2^{m+1}$, defined by

$$\rho(y, y_{m+1}) = \left(y_{m+1}\sigma_1^{-1}(y) + (1 + y_{m+1})\sigma_2^{-1}(y), y_{m+1}\right), \text{ for all } y \in \mathbb{F}_2^m, y_{m+1} \in \mathbb{F}_2.$$

Now we are ready to provide a recursive construction of Maiorana-McFarland bent functions $f_1', f_2', f_3', f_4' \in \mathcal{B}_{n+2}$ satisfying the condition $(f_1')^* + (f_2')^* + (f_3')^* + (f_4')^* = 1$ from bent functions $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$ satisfying the condition $f_1^* + f_2^* + f_3^* + f_4^* = 1$ using Theorem 2.1.

Proposition 2.4. *Let π_j for $j \in \{1,2,3\}$ be three permutations on $\mathbb{F}_2^m$ which satisfy the condition $(\mathcal{A}_m)$. Let σ be a permutation of $\mathbb{F}_2^m$. Denote by $\pi_4 = \pi_1 + \pi_2 + \pi_3$ and let Boolean functions h_j on $\mathbb{F}_2^m$ $j \in \{1,2,3,4\}$ satisfy*

$$h_1\left(\pi_1^{-1}(y)\right) + h_2\left(\pi_2^{-1}(y)\right) + h_3\left(\pi_3^{-1}(y)\right) + h_4\left(\pi_4^{-1}(y)\right) = 1.$$

Define four permutations ϕ_i on $\mathbb{F}_2^{m+1}$ as

$$\phi_i(y, y_{m+1}) = \begin{cases} (\pi_i(y), 1) & \text{if } y_{m+1} = 1 \\ (\sigma(y), 0) & \text{if } y_{m+1} = 0 \end{cases}, \quad \text{for all } y \in \mathbb{F}_2^m, y_{m+1} \in \mathbb{F}_2,$$

and four Boolean functions h_i' on $\mathbb{F}_2^{m+1}$ as follows

$$\begin{aligned} h_i'(y, y_{m+1}) &= y_{m+1} h_i(y) \text{ for } i \in \{1,2,3\}, \\ h_4'(y, y_{m+1}) &= y_{m+1} h_4(y) + y_{m+1} + 1. \end{aligned}$$

Then, the following hold.

1. *Permutations ϕ_1, ϕ_2, ϕ_3 satisfy the condition $(\mathcal{A}_m)$.*
2. *Functions h_j' satisfy*

   $$h_1'\left(\phi_1^{-1}(y, y_{m+1})\right) + h_2'\left(\phi_2^{-1}(y, y_{m+1})\right) + h_3'\left(\phi_3^{-1}(y, y_{m+1})\right) + h_4'\left(\phi_4^{-1}(y, y_{m+1})\right) = 1,$$

   for all $y \in \mathbb{F}_2^m, y_{m+1} \in \mathbb{F}_2$, where $\phi_4 = \phi_1 + \phi_2 + \phi_3$.
3. *Boolean functions $f_j'(x', y') = Tr\left(x'\phi_j(y')\right) + h_j'(y')$ for $j \in \{1,2,3,4\}$ and $x', y' \in \mathbb{F}_2^{m+1}$ are bent, moreover, $f_1'||f_2'||f_3'||f_4' \in \mathcal{B}_{n+2}$ is bent as well.*

Proof. 1. The property $(\mathcal{A}_m)$ means that for three permutations ϕ_i on $\mathbb{F}_2^{m+1}$, we have that $\phi_1 + \phi_2 + \phi_3 = \phi_4$ is also a permutation and $\phi_4^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$. First, we show that ϕ_4 is a permutation. By definition of ϕ_4, we get that for all $y \in \mathbb{F}_2^m$, $y_{m+1} \in \mathbb{F}_2$ holds

$$\phi_4(y, y_{m+1}) = \begin{cases} ((\pi_1 + \pi_2 + \pi_3)(y), 1) & \text{if } y_{m+1} = 1 \\ (\sigma(y), 0) & \text{if } y_{m+1} = 0 \end{cases}.$$

Since $\pi_4 = \pi_1 + \pi_2 + \pi_3$ is a permutation, we get that ϕ_4 is a permutation as well. Now, we show that $\phi_4^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$. By Lemma 2.3, we have that for all $y \in \mathbb{F}_2^m$, $y_{m+1} \in \mathbb{F}_2$ holds

$$\phi_4^{-1}(y, y_{m+1}) = (\phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1})(y, y_{m+1}),$$

from what follows that permutations ϕ_1, ϕ_2, ϕ_3 satisfy the condition $(\mathcal{A}_m)$.
2. Observe that for $j \in \{1,2,3\}$, we have that for all $y \in \mathbb{F}_2^m, y_{m+1} \in \mathbb{F}_2$ holds

$$h_i'(\phi_i^{-1}(y, y_{m+1})) = \begin{cases} h_i'(\phi_i^{-1}(y, 1)) & \text{if } y_{m+1} = 1 \\ h_i'(\phi_i^{-1}(y, 0)) & \text{if } y_{m+1} = 0 \end{cases} = \begin{cases} h_i(\pi_i^{-1}(y)) & \text{if } y_{m+1} = 1 \\ 0 & \text{if } y_{m+1} = 0 \end{cases}$$

Similarly, one can show that for all $y \in \mathbb{F}_2^m, y_{m+1} \in \mathbb{F}_2$ holds

$$h_4'(\phi_i^{-1}(y, y_{m+1})) = \begin{cases} h_4'(\phi_4^{-1}(y, 1)) & \text{if } y_{m+1} = 1 \\ h_4'(\phi_4^{-1}(y, 0)) & \text{if } y_{m+1} = 0 \end{cases} = \begin{cases} h_4((\pi_1 + \pi_2 + \pi_3)^{-1}(y)) & \text{if } y_{m+1} = 1 \\ 1 & \text{if } y_{m+1} = 0 \end{cases}.$$

Finally, for all $y \in \mathbb{F}_2^m, y_{m+1} \in \mathbb{F}_2$, we consider the sum

$$\sum_{i=1}^{4} h_i'\left(\phi_i^{-1}(y, y_{m+1})\right) = \begin{cases} \sum_{i=1}^{3} h_i\left(\phi_i^{-1}(y)\right) + h_4((\pi_1 + \pi_2 + \pi_3)^{-1}(y)) & \text{if } y_{m+1} = 1 \\ 1 & \text{if } y_{m+1} = 0 \end{cases} = 1,$$

since $h_1\left(\pi_1^{-1}(y)\right) + h_2\left(\pi_2^{-1}(y)\right) + h_3\left(\pi_3^{-1}(y)\right) + h_4((\pi_1 + \pi_2 + \pi_3)^{-1}(y)) = 1$ holds for all $y \in \mathbb{F}_2^m$.
3. The statement follows immediately from Theorem 2.1. □

3 Analysis of the obtained construction method

Recall that the set of all bent functions, which are extended-affine equivalent to functions of the form $f(x,y) = x \cdot \pi(y) + h(y)$ for $x, y \in \mathbb{F}_2^m$, where π is a permutation of $\mathbb{F}_2^m$, and $h \in \mathcal{B}_m$ is an arbitrary Boolean function is called the *completed Maiorana-McFarland class* and denoted by $\mathcal{M}^{\#}$. It is well-known [3] that a bent function $f \in \mathcal{B}_n$ belongs to the $\mathcal{M}^{\#}$ iff there exists a vector space U of dimension m, such that $D_a D_b f = 0$ for all $a, b \in U$; such a vector space is called [10] an *$\mathcal{M}$-subspace* of a bent function $f \in \mathcal{M}^{\#}$. Note that if $f \in \mathcal{M}$, then at least one $\mathcal{M}$-subspace of f has the form $U = \mathbb{F}_2^m \times \{0_m\}$, which we call the *canonical $\mathcal{M}$-subspace* of f.

Since in the bent 4-concatenation we consider bent functions $f_i \in \mathcal{B}_n$ in $\mathcal{M}^{\#}$, it is essential to specify the conditions on these functions such that the resulting function $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is outside $\mathcal{M}^{\#}$. Otherwise one just gets a complicated construction method of bent functions in $\mathcal{M}^{\#}$. For this purpose, we will use the following description of $\mathcal{M}$-subspaces of $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$.

Proposition 3.1. *[9] Let $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$ be four Boolean functions (not necessarily bent), such that $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is a bent function in $\mathcal{M}^{\#}$. Let $W \subset \mathbb{F}_2^{n+2}$ be an $\mathcal{M}$-subspace of f. Then, there exists an $(\frac{n}{2}-1)$-dimensional subspace V of $\mathbb{F}_2^n$ such that $V \times \{(0,0)\}$ is a subspace of W, and such that for all $i = 1, \ldots, 4$ the equality $D_a D_b f_i = 0$ holds for all $a, b \in V$.*

For the main result of this section, we will also need to define the (P_1) property, which was recently introduced in [9] for specifying Maiorana-McFarland bent functions with the unique canonical $\mathcal{M}$-subspace. We say that the mapping $\pi\colon \mathbb{F}_2^m \to \mathbb{F}_2^m$ has the property (P_1) if $D_v D_w \pi \neq 0_m$ for all linearly independent $v, w \in \mathbb{F}_2^m$.

Theorem 3.2. *Let $n = 2m$ for $m > 3$ and define three bent functions $f_i(x,y) = x \cdot \pi_i(y) + h_i(y)$, with $x, y \in \mathbb{F}_2^m$, for $i = 1, \ldots, 3$, where π_i satisfies the property (P_1) and additionally $\pi_1 + \pi_2$ satisfies the property (P_1), and furthermore we assume that the components of $\pi_1 + \pi_2$ do not admit linear structures. Define $f = f_1||f_2||f_3||f_4$ where $f_4(x,y) = f_1(x,y) + f_2(x,y) + f_3(x,y) + s(y)$ (consequently $h_4 = h_1 + h_2 + h_3 + s$) using suitable h_i so that the dual bent condition in (2.1) is satisfied. Then, the functions f_i share the unique canonical $\mathcal{M}$-subspace $U = \mathbb{F}_2^m \times \{0_m\}$ and furthermore bent function $f \in \mathcal{B}_{n+2}$ is outside $\mathcal{M}^{\#}$. In particular, the same conclusion is valid when $s(y) = 0$.*

Proof. Denoting $a = (a', a^{(1)}, a^{(2)})$ and $b = (b', b^{(1)}, b^{(2)})$ and $a', b' \in \mathbb{F}_2^n$ and $a^{(i)}, b^{(i)} \in \mathbb{F}_2$, the second-order derivative of f is given by $D_a D_b f(x, y_1, y_2) =$

$$\begin{aligned}
&= D_{a'} D_{b'} f_1(x) + y_1 D_{a'} D_{b'} f_{13}(x) + y_2 D_{a'} D_{b'} f_{12}(x) + y_1 y_2 D_{a'} D_{b'} f_{1234}(x) \\
&+ a^{(1)} D_{b'} f_{13}(x + a') + b^{(1)} D_{a'} f_{13}(x + b') + a^{(2)} D_{b'} f_{12}(x + a') + b^{(2)} D_{a'} f_{12}(x + b') \\
&+ (a^{(1)} y_2 + a^{(2)} y_1 + a^{(1)} a^{(2)}) D_{b'} f_{1234}(x + a') + (b^{(1)} y_2 + b^{(2)} y_1 + b^{(1)} b^{(2)}) \\
&\times D_{a'} f_{1234}(x + b') + (a^{(1)} b^{(2)} + b^{(1)} a^{(2)}) f_{1234}(x + a' + b'),
\end{aligned} \tag{3.1}$$

where $f_{i_1 \ldots i_k} := f_{i_1} + \cdots + f_{i_k}$. Since $D_u D_v \pi_i(y) \neq 0$ for any nonzero $u \neq v \in \mathbb{F}_2^m$ (as π_i satisfies the property (P_1), the functions f_i share the unique canonical $\mathcal{M}$-subspace $U = \mathbb{F}_2^m \times \{0_m\}$. For convenience, we denote $a' = (a_1, a_2)$ and $b' = (b_1, b_2)$, where $a_i, b_i \in \mathbb{F}_2^m$. W.l.o.g. we assume that $D_{a_2} D_{b_2}(\pi_1(y) + \pi_2(y)) \neq 0$ for any $a_2, b_2 \in \mathbb{F}_2^m$ ($a_2, b_2 \neq 0$ and distinct), and the term $y_2 D_{a'} D_{b'} f_{12}(x,y)$ in (3.1) cannot be canceled unless $a_2 = 0$ or $b_2 = 0$ or $a_2 = b_2$, which is due to the fact that (same can be deduced for $D_{(a_1,a_2)} D_{(b_1,b_2)} f_{13}(x,y)$)

$$\begin{aligned}
D_{(a_1,a_2)} D_{(b_1,b_2)} f_{12}(x,y) =& x \cdot (D_{a_2} D_{b_2}(\pi_1(y) + \pi_2(y))) + a_1 \cdot D_{b_2}(\pi_1 + \pi_2)(y + a_2) \\
&+ b_1 \cdot D_{a_2}(\pi_1 + \pi_2)(y + b_2) + D_{a_2} D_{b_2} h_{12}(y).
\end{aligned} \tag{3.2}$$

Thus, for any $a = (a_1, a_2, a^{(1)}, a^{(2)})$ and $b = (b_1, b_2, b^{(1)}, b^{(2)})$ in some $(m+1)$-dimensional subspace W of $\mathbb{F}_2^{2m+2}$, we necessarily have that either $a_2 = 0$ or $b_2 = 0$, alternatively $a_2 = b_2$.

Since the functions f_i share the unique canonical $\mathcal{M}$-subspace $U = \mathbb{F}_2^m \times \{0_m\}$, any other subspace V of $\mathbb{F}_2^m \times \mathbb{F}_2^m$ for which $D_{a'}D_{b'}f_i(x,y) = 0$ for all $a', b' \in V$ must have dimension less than m. By Proposition 3.1, if f defined on $\mathbb{F}_2^{2m+2}$ belongs to $\mathcal{M}^\#$ then for any $\mathcal{M}$-subspace W of f of dimension $m+1$ there must exist $V \subset \mathbb{F}_2^{2m}$ of dimension $m-1$ such that $D_aD_bf_i = 0$ for all $i = 1, \ldots, 4$ and any $a, b \in V$. Furthermore, $V \times (0,0)$ is a subspace of W. There are only two possibilities for V, i.e., either $V \subset U = \mathbb{F}_2^m \times \{0_m\}$ or $V \not\subset U$.

We first consider the case that $V \subset U = \mathbb{F}_2^m \times \{0_m\}$, where $\dim(V) = m-1$. Then, $V \times (0,0) \subset W$ and to extend this subspace to W, we need to adjoin two elements of $\mathbb{F}_2^{2m+2}$, say $u = (u_1, u_2, u^{(1)}, u^{(2)}), v = (v_1, v_2, v^{(1)}, v^{(2)}) \in \mathbb{F}_2^m \times \mathbb{F}_2^m \times \mathbb{F}_2 \times \mathbb{F}_2$, and $u' = (u_1, u_2)$, $v' = (v_1, v_2)$. Then, we cannot have the case that $u_2 = v_2 = 0_m$ since this would imply that f_{12} on $\mathbb{F}_2^n$ has an $\mathcal{M}$-subspace of dimension $n/2+1$ which is impossible (see for instance [8]). On the other hand, if $u_2 \neq v_2 \neq 0$ then again $y_1 D_{u'}D_{v'}f_{12}(x,y)$ cannot be canceled in (3.1). W.l.o.g. we assume that $u_2 = 0$ and $v_2 \neq 0$, which implies that $U \times (0,0) \subset W$. Hence, $W = \langle U \times (0,0), v\rangle$, where $v_2 \neq 0$. Notice that the case $u_2 = v_2$, which also might lead to $D_{u'}D_{v'}f_{12}(x,y) = 0$, reduces to this case since $u_2 + v_2 = 0$ and then $u' + v' \in U$. Now, we note that in $W = \langle U \times (0,0), v\rangle$ there must exist an element $z = (z', 0, 0)$ such that $z_1 = v_1$ and consequently $z' + v' = (0_m, v_2)$. Considering (3.2), and replacing $a' \to z' = (v_1, 0_m)$ and $b' \to (0_m, v_2)$, we have that only the term $v_1 \cdot D_{b_2}(\pi_1 + \pi_2)(y)$ remains, which cannot be zero due to our assumption that the components of $\pi_1 + \pi_2(y)$ do not admit linear structures.

The second case arises when $V \not\subset U$, where $\dim(V) = m-1$. Hence, V contains at least one element $a' = (a_1, a_2) \notin U$, so that $a_2 \neq 0$. If V contains one more element not in U, say b', then $D_{a'}D_{b'}f_{12}(x,y) \neq 0$ and consequently $D_aD_bf(x,y,y_1,y_2) \neq 0$. If V does not contain one more element which is not in U, then it can be extended to U (by replacing a' with some $(u_1, 0_m)$) and the above arguments apply. □

Monomial permutations satisfying the $(\mathcal{A}_m)$ property were specified in [7]. We show that in a small number of variables, it is possible to find suitable functions h_i, such that the conditions of Theorem 3.2 are satisfied.

Theorem 3.3. *[7] Let $m \geq 3$ be an integer and $d^2 \equiv 1 \mod 2^m - 1$. Let π_i be three permutations of $\mathbb{F}_2^m$ defined by $\pi_i(y) = \alpha_i y^d$, for $i = 1, 2, 3$, where $\alpha_i \in \mathbb{F}_{2^m}^*$ are pairwise distinct elements such that $\alpha_i^{d+1} = 1$ and $\alpha_4^{d+1} = 1$ where $\alpha_4 = \alpha_1 + \alpha_2 + \alpha_3$. Then, the permutations π_i satisfy the property $(\mathcal{A}_m)$ and furthermore π_i are involutions as well as $\pi_4 = \pi_1 + \pi_2 + \pi_3$.*

Example 3.4. Let $m = 4$ and the multiplicative group of $\mathbb{F}_{2^4}$ be given by $\mathbb{F}_{2^4}^* = \langle a\rangle$, where the primitive element a satisfies $a^4 + a + 1 = 0$. Let $d = 14$, which satisfies $d^2 \equiv 1 \mod 15$. Define $\alpha_1 = a, \alpha_2 = a^2, \alpha_3 = a^4$ and $\alpha_4 = \alpha_1 + \alpha_2 + \alpha_3 = a^8$. It is possible to check that for $i = 1, \ldots, 3$, the defined permutations π_i as well as $\pi_1 + \pi_2$ satisfy the property (P_1) and additionally the components of $\pi_1 + \pi_2$ do not admit linear structures. Define the following four Boolean functions $h_1(y) = 0, h_2(y) = Tr(y), h_3(y) = Tr(ay), h_4(y) = Tr(a^{13}y) + 1$, as well as four bent Maiorana-McFarland bent functions $f_i(x,y) = Tr(x\pi_i(y)) + h_i(y)$ for $i = 1, 2, 3, 4$, where $x, y \in \mathbb{F}_{2^3}$. Note that $h_1(y) + h_2(y) + h_3(y) + h_4(y) = s(y) = Tr(a^{11}y) + 1$, and hence, $f_4 = f_1 + f_2 + f_3 + s$. Since the functions h_i satisfy the condition (2.1) of Theorem 2.1, we have that $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_8$. By Theorem 3.2, the function f is outside $\mathcal{M}^\#$.

Open Problem 3.5. 1. Find explicit infinite families of permutations π_i and Boolean functions h_i satisfying the conditions of Theorem 2.1. 2. Relax the conditions of Theorem 2.1. The latter question is motivated by the fact that even in $n = 6$ variables we were able to find permutations π_i and Boolean functions h_i in $m = 3$ variables, such that the concatenation of corresponding bent functions f_i is bent and outside $\mathcal{M}^\#$. These examples, however, cannot be covered by Theorem 2.1, since all permutations in 3 variables are quadratic, and hence, their components have linear structures.

4 An application to the design of homogeneous bent functions

A Boolean function is called *homogeneous* if all the monomials in its ANF have the same algebraic degree. Now, we show how bent functions satisfying the dual bent condition and permutations with the $(\mathcal{A}_m)$ property can be used for the construction of homogeneous bent functions.

Proposition 4.1. *Let $f_1 \in \mathcal{B}_n$ be a homogeneous cubic bent function. Let $q_1, q_2 \in \mathcal{B}_n$ be two homogeneous quadratic functions, such that $f_2 = f_1 + q_2$ and $f_3 = f_1 + q_3$ are bent, and additionally $f_1 + f_2 + f_3$ is also bent. Defining $f_4 = f_1 + f_2 + f_3 + s$ for $s \in \mathcal{B}_n$, the function $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is homogeneous cubic bent iff $f_1^* + f_2^* + f_3^* = (f_1 + f_2 + f_3 + s)^* + 1$, where $s \in \mathcal{B}_n$ is a linear function.*

Example 4.2. Consider the following homogeneous functions $f_1, q_2, q_3, s \in \mathcal{B}_8$, which are given by their algebraic normal forms as follows:

$$\begin{aligned}
f_1(z) =& z_1z_2z_5 + z_1z_2z_8 + z_1z_3z_4 + z_1z_3z_5 + z_1z_3z_6 + z_1z_3z_7 + z_1z_4z_5 + z_1z_4z_7 + z_1z_4z_8 \\
&+ z_1z_5z_8 + z_1z_6z_8 + z_2z_3z_4 + z_2z_3z_5 + z_2z_4z_5 + z_2z_4z_6 + z_2z_4z_8 + z_2z_5z_6 + z_2z_6z_7 \\
&+ z_2z_6z_8 + z_2z_7z_8 + z_3z_4z_6 + z_3z_4z_8 + z_3z_5z_6 + z_3z_5z_7 + z_3z_6z_8 + z_4z_7z_8 + z_5z_6z_7 \\
&+ z_5z_6z_8, \\
q_2(z) =& z_1z_4 + z_1z_5 + z_1z_7 + z_5z_7 + z_1z_8 + z_4z_8 + z_6z_7 + z_6z_8 + z_7z_8, \\
q_3(z) =& z_1z_3 + z_1z_4 + z_1z_7 + z_1z_8 + z_2z_3 + z_2z_8 + z_3z_5 + z_3z_8 + z_4z_7 + z_5z_6 + z_6z_7 + z_7z_8, \\
s(z) =& z_1 + z_4 + z_6 + z_8.
\end{aligned}$$

One can check that the functions $f_1, q_2, q_3, s \in \mathcal{B}_8$ satisfy the conditions of Proposition 4.1, and hence $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{10}$ constructed as in Proposition 4.1 is homogeneous cubic bent. Notably, there exists a linear non-degenerate transformation $z \mapsto zA$ such that $f_i(zA) = x \cdot \pi_i(y) + h_i(y)$, where permutations π_i and Boolean functions h_i are defined in Example 2.2, and hence, permutations π_i have the $(\mathcal{A}_4)$ property. Finally, we note that the function $f \notin \mathcal{M}^\#$ since the functions f_i satisfy the conditions of [9, Theorem 5.11].

Open Problem 4.3. Find explicit infinite families of homogeneous bent functions using the dual bent condition and permutations with the $(\mathcal{A}_m)$ property.

References

[1] A. Canteaut, P. Charpin. "Decomposing bent functions". *IEEE Transactions on Information Theory*, vol. 49, no. 8, pp. 2004–2019 (2003). p. 1.

[2] N. Cepak, E. Pasalic, A. Muratović-Ribić. "Frobenius linear translators giving rise to new infinite classes of permutations and bent functions". *Cryptogr. Commun.* 11(6): 1275–1295 (2019). p. 1.

[3] J. F. Dillon. "Elementary Hadamard difference sets". Ph.D. dissertation. *University of Maryland, USA* (1974). p. 4.

[4] S. Hodžić, E. Pasalic, Y. Wei. "A general framework for secondary constructions of bent and plateaued functions". *Des. Codes Cryptogr.* 88(10): 2007–2035 (2020). p. 1.

[5] S. Hodžić, E. Pasalic, W. G. Zhang. "Generic constructions of five-valued spectra Boolean functions". *IEEE Trans. Inf. Theory* 65(11): 7554–7565 (2019). p. 1.

[6] S. Mesnager. "Further constructions of infinite families of bent functions from new permutations and their duals". *Cryptogr. Commun.* 8, 229–246 (2016). p. 1.

[7] S. Mesnager, G. D. Cohen, and D. Madore. "On existence (based on an arithmetical problem) and constructions of bent functions". In: Groth, J. (eds) Cryptography and Coding. IMACC 2015. Lecture Notes in Computer Science, vol 9496. Springer, Cham., (2015). p. 5.

[8] E. Pasalic, A. Bapic, F. Zhang, Y. Wei. "Explicit infinite families of bent functions outside the completed Maiorana-McFarland class". *Des. Codes Cryptogr.* (2023). p. 5.

[9] E. Pasalic, A. Polujan, S. Kudin, F. Zhang. "Design and analysis of bent functions using $\mathcal{M}$-subspaces". arXiv preprint arXiv:2304.13432 (2023) pp. 4 and 6.

[10] A. Polujan, A. Pott. "Cubic bent functions outside the completed Maiorana-McFarland class". *Des. Codes Cryptogr.* 88, 1701–1722 (2020). p. 4.