On bent functions satisfying the dual bent condition[1,2]

Alexandr Polujan[a], Enes Pasalic[b], Sadmir Kudin[b], Fengrong Zhang[c]

[a]Otto von Guericke University Magdeburg, Germany
[b]University of Primorska, FAMNIT & IAM, Koper, Slovenia
[c]Xidian University, Xian, P.R. China

BFA 2023
The 8th International Workshop on
Boolean Functions and their Applications,
05.09.2023

[1]Enes Pasalic, Alexandr Polujan, Sadmir Kudin and Fengrong Zhang. *Design and analysis of bent functions using $\mathcal{M}$-subspaces*. 2023. arXiv: 2304.13432 [cs.IT].

[2]Alexandr Polujan, Enes Pasalic, Sadmir Kudin and Fengrong Zhang. *Bent functions satisfying the dual bent condition and permutations with the $(\mathcal{A}_m)$ property*.

Boolean functions

- Mappings $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ are called Boolean functions
- Let $\mathcal{B}_n$ be the set of all Boolean functions in n variables
- The Walsh-Hadamard transform of $f \in \mathcal{B}_n$ at $a \in \mathbb{F}_2^n$ is defined by

$$\hat{\chi}_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+a\cdot x}$$

- The first-order derivative of $f \in \mathcal{B}_n$ at $a \in \mathbb{F}_2^n$ is defined by is

$$D_a f(x) = f(x+a) + f(x)$$

- The second-order derivative of a function $f \in \mathcal{B}_n$ w.r.t $a, b \in \mathbb{F}_2^n$ is

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

Boolean bent functions

- For $n = 2m$, a function $f \in \mathcal{B}_n$ is called bent if

$$\hat{\chi}_f(a) = \pm 2^{\frac{n}{2}} \quad \text{for all} \quad a \in \mathbb{F}_2^n$$

- For a bent function $f \in \mathcal{B}_n$, a Boolean function $f^* \in \mathcal{B}_n$ defined by

$$\hat{\chi}_f(a) = 2^{\frac{n}{2}}(-1)^{f^*(a)} \quad \text{for all} \quad a \in \mathbb{F}_2^n$$

  is a bent function, called the dual of f

Boolean bent functions

- For $n = 2m$, a function $f \in \mathcal{B}_n$ is called bent if

$$\hat{\chi}_f(a) = \pm 2^{\frac{n}{2}} \quad \text{for all} \quad a \in \mathbb{F}_2^n$$

- For a bent function $f \in \mathcal{B}_n$, a Boolean function $f^* \in \mathcal{B}_n$ defined by

$$\hat{\chi}_f(a) = 2^{\frac{n}{2}} (-1)^{f^*(a)} \quad \text{for all} \quad a \in \mathbb{F}_2^n$$

  is a bent function, called the dual of f

Example (Maiorana-McFarland bent functions)

- Let $\mathbb{F}_2^n \cong \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, π be a permutation of $\mathbb{F}_{2^m}$, and $h \in \mathcal{B}_m$
- For $x, y \in \mathbb{F}_{2^m}$, the function $f(x, y) = Tr(x\pi(y)) + h(y)$ is bent
- Its dual is $f^*(x, y) = Tr(y\pi^{-1}(x)) + h(\pi^{-1}(x))$

Decompositions of Boolean functions

- Let $f \in \mathcal{B}_{n+2}$ and $\langle a, b\rangle \subset \mathbb{F}_2^{n+2}$ be a two-dimensional subspace
- Consider the restrictions of $f \in \mathcal{B}_{n+2}$ w.r.t. affine subspaces

$$\underbrace{f|_{0+\mathbb{F}_2^n}}_{f_1\in\mathcal{B}_n},\ \underbrace{f|_{a+\mathbb{F}_2^n}}_{f_2\in\mathcal{B}_n},\ \underbrace{f|_{b+\mathbb{F}_2^n}}_{f_3\in\mathcal{B}_n},\ \underbrace{f|_{a+b+\mathbb{F}_2^n}}_{f_4\in\mathcal{B}_n}$$

- We call (f_1, f_2, f_3, f_4) a decomposition of $f \in \mathcal{B}_{n+2}$ w.r.t. $\langle a, b\rangle$

Decompositions of Boolean functions

- Let $f \in \mathcal{B}_{n+2}$ and $\langle a, b\rangle \subset \mathbb{F}_2^{n+2}$ be a two-dimensional subspace
- Consider the restrictions of $f \in \mathcal{B}_{n+2}$ w.r.t. affine subspaces

$$\underbrace{f|_{0+\mathbb{F}_2^n}}_{f_1\in\mathcal{B}_n},\ \underbrace{f|_{a+\mathbb{F}_2^n}}_{f_2\in\mathcal{B}_n},\ \underbrace{f|_{b+\mathbb{F}_2^n}}_{f_3\in\mathcal{B}_n},\ \underbrace{f|_{a+b+\mathbb{F}_2^n}}_{f_4\in\mathcal{B}_n}$$

- We call (f_1, f_2, f_3, f_4) a decomposition of $f \in \mathcal{B}_{n+2}$ w.r.t. $\langle a, b\rangle$

Theorem (Canteaut and Charpin 2003)

Let $f \in \mathcal{B}_{n+2}$ be bent and (f_1, f_2, f_3, f_4) be its decomposition w.r.t. $\langle a, b\rangle \subset \mathbb{F}_2^{n+2}$. Then the following hold:

1. *All f_i are bent (bent 4-decomposition) iff $D_{a,b}f^* = 1$.*
2. *All f_i are semi-bent.*
3. *All f_i are 5-valued, i.e., $\hat{\chi}_{f_i}(a) \in \{0, \pm 2^{n/2}, \pm 2^{(n+2)/2}\}\ \forall a \in \mathbb{F}_2^n$.*

Concatenation of Boolean functions

- If $a = (0, \ldots, 0, 1), b = (0, \ldots, 1, 0) \in \mathbb{F}_2^{n+2}$, then the function $f \in \mathcal{B}_{n+2}$ can be reconstructed from f_i as follows

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

- The function $f \in \mathcal{B}_{n+2}$ defined as in (1) is called a concatenation of $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$, and denoted by $f = f_1||f_2||f_3||f_4$

Concatenation of Boolean functions

- If $a = (0, \ldots, 0, 1), b = (0, \ldots, 1, 0) \in \mathbb{F}_2^{n+2}$, then the function $f \in \mathcal{B}_{n+2}$ can be reconstructed from f_i as follows

$$\begin{aligned} f(z, z_{n+1}, z_{n+2}) =& f_1(z) + z_{n+1} z_{n+2}(f_1 + f_2 + f_3 + f_4)(z) \\ &+ z_{n+1}(f_1 + f_3)(z) + z_{n+2}(f_1 + f_2)(z) \end{aligned} \tag{1}$$

- The function $f \in \mathcal{B}_{n+2}$ defined as in (1) is called a concatenation of $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$, and denoted by $f = f_1||f_2||f_3||f_4$

Question: Let $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$ be bent. Under which condition is $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ bent again?

The dual bent condition

Theorem (Hodžić, Pasalic and W. Zhang 2019)

Let $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$ be bent. The function $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is bent iff the dual bent condition

$$f_1^* + f_2^* + f_3^* + f_4^* = 1$$

is satisfied.

- This result was also shown by Preneel, Van Leekwijck, Van Linden, Govaerts and Vandewalle 1991
- A recent application[3]: Generic construction methods of bent functions concatenating Maiorana-McFarland bent functions

[3] Enes Pasalic, Alexandr Polujan, Sadmir Kudin and Fengrong Zhang. *Design and analysis of bent functions using $\mathcal{M}$-subspaces*. 2023. arXiv: 2304.13432 [cs.IT].

The main goal

- To provide new explicit constructions of bent functions using the concatenation of four bent functions (the dual bent condition)

The main goal

- To provide new explicit constructions of bent functions using the concatenation of four bent functions (the dual bent condition)

1. New: What you get $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is not what you start with $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$ (up to EA-equivalence).

2. Explicit infinite families

The main goal

- To provide new explicit constructions of bent functions using the concatenation of four bent functions (the dual bent condition)

1. New: What you get $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is not what you start with $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$ (up to EA-equivalence). We start with

   $\mathcal{MM}^{\#} = \{$ All bent functions EA-equivalent to $Tr(x\pi(y)) + h(y)$ $\}$

2. Explicit infinite families

The main goal

- To provide new explicit constructions of bent functions using the concatenation of four bent functions (the dual bent condition)

1. New: What you get $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is not what you start with $f_1, f_2, f_3, f_4 \in \mathcal{B}_n$ (up to EA-equivalence). We start with

   $\mathcal{MM}^{\#} = \{$ All bent functions EA-equivalent to $Tr(x\pi(y)) + h(y)$ $\}$

2. Explicit infinite families

Main research question: How to specify bent functions $f_i \in \mathcal{MM}^{\#}$ s.t. $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is bent and outside $\mathcal{MM}^{\#}$?

The main result

Theorem (Polujan, Pasalic, Kudin and F. Zhang 2023)

Let $m \in \mathbb{N}$ *with* $m \geq 3$ *and* $d^2 \equiv 1 \mod 2^m - 1$. *For* $i = 1, 2, 3$, *define permutations* π_i *of* $\mathbb{F}_{2^m}$ *by* $\pi_i(y) = \alpha_i y^d$, *where* $\alpha_i \in \mathbb{F}_{2^m}^*$ *are pairwise distinct elements s.t.* $\alpha_i^{d+1} = 1$ *and* $\alpha_4^{d+1} = 1$ *with* $\alpha_4 = \alpha_1 + \alpha_2 + \alpha_3$. *Define bent functions* $f_i(x, y) = Tr\left(x\pi_i(y)\right) + h_i(y)$ *for* $x, y \in \mathbb{F}_{2^m}$, *where*

1. $h_i(y) = Tr\left(\frac{\alpha_{i+1}}{\alpha_i^k} y^k\right)$ *for* $i = 1, 2, 3$ *and* $h_4(y) = Tr\left(\frac{\alpha_1}{\alpha_4} y^k\right) + 1$,
2. $\pi_i(y) = \alpha_i y^d$ *satisfy* $D_{a,b}\pi_i \neq 0$ *for all lin. indep.* $a, b \in \mathbb{F}_{2^m}$.

If $wt(d) > 1$, *then* $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{2m+2}$ *is bent and outside* $\mathcal{MM}^\#$.

- For m odd, the APN permutations $\pi_i(y) = \alpha_i y^{-1}$ always work

The key steps of the proof

Consider Maiorana-McFarland bent functions

$$f_i(x, y) = Tr(x\pi_i(y)) + h_i(y)$$

arising from permutations π_i of $\mathbb{F}_{2^m}$ with the $(\mathcal{A}_m)$ property

1. Specify the dual bent condition for such bent functions
2. Find explicit constructions of permutations π_i of $\mathbb{F}_{2^m}$ with the $(\mathcal{A}_m)$ property and suitable $h_i \in \mathcal{B}_m$ s.t. $f = f_1||f_2||f_3||f_4$ is bent
3. Provide conditions for $f_i \in \mathcal{MM}^\#$ s.t. $f = f_1||f_2||f_3||f_4$ is bent and outside $\mathcal{MM}^\#$

Step I: Permutations with the $(\mathcal{A}_m)$ property

Definition (Mesnager 2014)

Let π_1, π_2, π_3 be three permutations of $\mathbb{F}_{2^m}$. We say that π_1, π_2, π_3 have the $(\mathcal{A}_m)$ property if $\pi_4 = \pi_1 + \pi_2 + \pi_3$ is a permutation and $\pi_4^{-1} = \pi_1^{-1} + \pi_2^{-1} + \pi_3^{-1}$.

Step I: Permutations with the $(\mathcal{A}_m)$ property

Definition (Mesnager 2014)

Let π_1, π_2, π_3 be three permutations of $\mathbb{F}_{2^m}$. We say that π_1, π_2, π_3 have the $(\mathcal{A}_m)$ property if $\pi_4 = \pi_1 + \pi_2 + \pi_3$ is a permutation and $\pi_4^{-1} = \pi_1^{-1} + \pi_2^{-1} + \pi_3^{-1}$.

Theorem (Cepak, Pasalic and Muratović-Ribić 2019)

Let $f_i(x, y) = Tr(x\pi_i(y)) + h_i(y)$ *for* $i \in \{1, 2, 3\}$ *and* $x, y \in \mathbb{F}_{2^m}$*, where the permutations* π_i *have the* $(\mathcal{A}_m)$ *property and* $f_4 = f_1 + f_2 + f_3$*. If*

$$\sum_{i=1}^{3} h_i(\pi_i^{-1}(y)) + (h_1 + h_2 + h_3)((\pi_1 + \pi_2 + \pi_3)^{-1}(y)) = 1,$$

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

Step I: Generalizing the previous result

Theorem (Polujan, Pasalic, Kudin and F. Zhang 2023)

Let $n = 2m$ *and* $f_i(x,y) = Tr\left(x\pi_i(y)\right) + h_i(y)$ *for* $i \in \{1,2,3\}$ *and* $x, y \in \mathbb{F}_{2^m}$*, where the permutations* π_j *have the* $(\mathcal{A}_m)$ *property, and let* $s \in \mathcal{B}_m$*. Define* $h_4 \in \mathcal{B}_m$ *as* $h_4(y) = h_1(y) + h_2(y) + h_3(y) + s(y)$ *and a bent function* $f_4 \in \mathcal{B}_n$ *as* $f_4(x,y) = f_1(x,y) + f_2(x,y) + f_3(x,y) + s(y)$*. If*

$$\sum_{i=1}^{3} h_i(\pi_i^{-1}(y)) + \underbrace{(h_1 + h_2 + h_3 + s)}_{h_4}((\pi_1 + \pi_2 + \pi_3)^{-1}(y)) = 1,$$

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

Step I: Generalizing the previous result

Theorem (Polujan, Pasalic, Kudin and F. Zhang 2023)

Let $n = 2m$ and $f_i(x, y) = Tr\,(x\pi_i(y)) + h_i(y)$ for $i \in \{1, 2, 3\}$ and $x, y \in \mathbb{F}_{2^m}$, where the permutations π_j have the $(\mathcal{A}_m)$ property, and let $s \in \mathcal{B}_m$. Define $h_4 \in \mathcal{B}_m$ as $h_4(y) = h_1(y) + h_2(y) + h_3(y) + s(y)$ and a bent function $f_4 \in \mathcal{B}_n$ as $f_4(x, y) = f_1(x, y) + f_2(x, y) + f_3(x, y) + s(y)$. If

$$\sum_{i=1}^{3} h_i(\pi_i^{-1}(y)) + \underbrace{(h_1 + h_2 + h_3 + s)}_{h_4}((\pi_1 + \pi_2 + \pi_3)^{-1}(y)) = 1,$$

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

- The case $s = 0$ corresponds to the result of Cepak, Pasalic and Muratović-Ribić 2019
- Advantage: More freedom to choose the function f_4

Step II: Permutations with the $(\mathcal{A}_m)$ property explicitly

Theorem (Mesnager, Cohen and Madore 2015)

Let $m \in \mathbb{N}$ with $m \geq 3$ and $d^2 \equiv 1 \mod 2^m - 1$. For $i = 1, 2, 3$, define permutations π_i of $\mathbb{F}_{2^m}$ by $\pi_i(y) = \alpha_i y^d$, where $\alpha_i \in \mathbb{F}_{2^m}^*$ are pairwise distinct elements s.t. $\alpha_i^{d+1} = 1$ and $\alpha_4^{d+1} = 1$ with $\alpha_4 = \alpha_1 + \alpha_2 + \alpha_3$. Then, the permutations π_i of $\mathbb{F}_{2^m}$ have the $(\mathcal{A}_m)$ property and furthermore π_1, π_2, π_3 and $\pi_4 = \pi_1 + \pi_2 + \pi_3$ are involutions.

Step II: Permutations with the $(\mathcal{A}_m)$ property explicitly

Theorem (Mesnager, Cohen and Madore 2015)

Let $m \in \mathbb{N}$ with $m \geq 3$ and $d^2 \equiv 1 \mod 2^m - 1$. For $i = 1, 2, 3$, define permutations π_i of $\mathbb{F}_{2^m}$ by $\pi_i(y) = \alpha_i y^d$, where $\alpha_i \in \mathbb{F}_{2^m}^*$ are pairwise distinct elements s.t. $\alpha_i^{d+1} = 1$ and $\alpha_4^{d+1} = 1$ with $\alpha_4 = \alpha_1 + \alpha_2 + \alpha_3$. Then, the permutations π_i of $\mathbb{F}_{2^m}$ have the $(\mathcal{A}_m)$ property and furthermore π_1, π_2, π_3 and $\pi_4 = \pi_1 + \pi_2 + \pi_3$ are involutions.

- How to specify h_i, s.t. for $f_i(x, y) = Tr(x\pi_i(y)) + h_i(y)$ the dual bent condition $\sum_{i=1}^{4} h_i(\pi_i^{-1}(y)) = 1$ is satisfied?

Step II: Permutations with the $(\mathcal{A}_m)$ property explicitly

Theorem (Mesnager, Cohen and Madore 2015)

Let $m \in \mathbb{N}$ *with* $m \geq 3$ *and* $d^2 \equiv 1 \mod 2^m - 1$. *For* $i = 1, 2, 3$, *define permutations* π_i *of* $\mathbb{F}_{2^m}$ *by* $\pi_i(y) = \alpha_i y^d$, *where* $\alpha_i \in \mathbb{F}_{2^m}^*$ *are pairwise distinct elements s.t.* $\alpha_i^{d+1} = 1$ *and* $\alpha_4^{d+1} = 1$ *with* $\alpha_4 = \alpha_1 + \alpha_2 + \alpha_3$. *Then, the permutations* π_i *of* $\mathbb{F}_{2^m}$ *have the* $(\mathcal{A}_m)$ *property and furthermore* π_1, π_2, π_3 *and* $\pi_4 = \pi_1 + \pi_2 + \pi_3$ *are involutions.*

- How to specify h_i, s.t. for $f_i(x, y) = Tr(x\pi_i(y)) + h_i(y)$ the dual bent condition $\sum_{i=1}^{4} h_i(\pi_i^{-1}(y)) = 1$ is satisfied?

Proposition (Polujan, Pasalic, Kudin and F. Zhang 2023)

Additionally, define Boolean functions $h_i \in \mathcal{B}_m$ *as follows*

$$h_i(y) = Tr\left(\frac{\alpha_{i+1}}{\alpha_i^k} y^k\right) \quad \text{for } i = 1, 2, 3 \quad \text{and } h_4(y) = Tr\left(\frac{\alpha_1}{\alpha_4} y^k\right) + 1.$$

Then $f = f_1 || f_2 || f_3 || f_4 \in \mathcal{B}_{2m+2}$ *is bent.*

Step III: $\mathcal{M}$-subspaces of bent functions from $\mathcal{MM}^{\#}$

Theorem (Dillon 1974)

A Boolean bent function $f \in \mathcal{B}_{2m}$ belongs to $\mathcal{MM}^{\#}$ iff there exists an m-dimensional linear subspace U of $\mathbb{F}_2^n$ s.t. $D_a D_b f = 0$ for any $a, b \in U$.

Step III: $\mathcal{M}$-subspaces of bent functions from $\mathcal{MM}^\#$

Theorem (Dillon 1974)

A Boolean bent function $f \in \mathcal{B}_{2m}$ belongs to $\mathcal{MM}^\#$ iff there exists an m-dimensional linear subspace U of $\mathbb{F}_2^n$ s.t. $D_a D_b f = 0$ for any $a, b \in U$.

Definition (Polujan and Pott 2020)

For $f \in \mathcal{B}_n$, we call a linear subspace U of $\mathbb{F}_2^n$ s.t. $D_a D_b f = 0$ for any $a, b \in U$ an $\mathcal{M}$-subspace of f

Step III: $\mathcal{M}$-subspaces of bent functions from $\mathcal{MM}^\#$

Theorem (Dillon 1974)

A Boolean bent function $f \in \mathcal{B}_{2m}$ belongs to $\mathcal{MM}^\#$ iff there exists an m-dimensional linear subspace U of $\mathbb{F}_2^n$ s.t. $D_a D_b f = 0$ for any $a, b \in U$.

Definition (Polujan and Pott 2020)

For $f \in \mathcal{B}_n$, we call a linear subspace U of $\mathbb{F}_2^n$ s.t. $D_a D_b f = 0$ for any $a, b \in U$ an $\mathcal{M}$-subspace of f

- Let $f(x, y) = Tr(x\pi(y)) + h(y)$ be bent on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$

Step III: $\mathcal{M}$-subspaces of bent functions from $\mathcal{MM}^\#$

Theorem (Dillon 1974)

A Boolean bent function $f \in \mathcal{B}_{2m}$ belongs to $\mathcal{MM}^\#$ iff there exists an m-dimensional linear subspace U of $\mathbb{F}_2^n$ s.t. $D_aD_bf = 0$ for any $a, b \in U$.

Definition (Polujan and Pott 2020)

For $f \in \mathcal{B}_n$, we call a linear subspace U of $\mathbb{F}_2^n$ s.t. $D_aD_bf = 0$ for any $a, b \in U$ an $\mathcal{M}$-subspace of f

- Let $f(x, y) = Tr(x\pi(y)) + h(y)$ be bent on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$
- The max. number of $\mathcal{M}$-subspaces of dim. m is $\prod_{i=1}^{m}(2^i + 1)$, and it is achieved iff f is quadratic (Kolomeec 2017)
- The min. number of $\mathcal{M}$-subspaces of dim. m is 1, since $U = \mathbb{F}_{2^m} \times \{0\}$ always works (Dillon 1974)

Step III: $\mathcal{M}$-subspaces of bent functions from $\mathcal{MM}^\#$

Theorem (Dillon 1974)

A Boolean bent function $f \in \mathcal{B}_{2m}$ belongs to $\mathcal{MM}^\#$ iff there exists an m-dimensional linear subspace U of $\mathbb{F}_2^n$ s.t. $D_aD_bf = 0$ for any $a, b \in U$.

Definition (Polujan and Pott 2020)

For $f \in \mathcal{B}_n$, we call a linear subspace U of $\mathbb{F}_2^n$ s.t. $D_aD_bf = 0$ for any $a, b \in U$ an $\mathcal{M}$-subspace of f

- Let $f(x, y) = Tr(x\pi(y)) + h(y)$ be bent on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$
- The max. number of $\mathcal{M}$-subspaces of dim. m is $\prod_{i=1}^{m}(2^i + 1)$, and it is achieved iff f is quadratic (Kolomeec 2017)
- The min. number of $\mathcal{M}$-subspaces of dim. m is 1, since $U = \mathbb{F}_{2^m} \times \{0\}$ always works (Dillon 1974)
- How to achieve the min. number and why it is important?

Step III: $\mathcal{M}$-subspaces of $f = f_1||f_2||f_3||f_4$

Proposition (Pasalic, Polujan, Kudin and F. Zhang 2023)

Let π *be a permutation of* $\mathbb{F}_{2^m}$. *If* $D_aD_b\pi \neq 0$ *for all linearly independent* $a, b \in \mathbb{F}_{2^m}$, *then for any* $h \in \mathcal{B}_m$ *the Maiorana-McFarland bent function* $f(x,y) = Tr(x\pi(y)) + h(y)$ *has the unique* $\mathcal{M}$*-subspace.*

Step III: $\mathcal{M}$-subspaces of $f = f_1||f_2||f_3||f_4$

Proposition (Pasalic, Polujan, Kudin and F. Zhang 2023)

Let π be a permutation of $\mathbb{F}_{2^m}$. If $D_a D_b \pi \neq 0$ for all linearly independent $a, b \in \mathbb{F}_{2^m}$, then for any $h \in \mathcal{B}_m$ the Maiorana-McFarland bent function $f(x, y) = Tr(x\pi(y)) + h(y)$ has the unique $\mathcal{M}$-subspace.

- E.g., one can take an APN permutation π

Step III: $\mathcal{M}$-subspaces of $f = f_1||f_2||f_3||f_4$

Proposition (Pasalic, Polujan, Kudin and F. Zhang 2023)

Let π be a permutation of $\mathbb{F}_{2^m}$. If $D_a D_b \pi \neq 0$ for all linearly independent $a, b \in \mathbb{F}_{2^m}$, then for any $h \in \mathcal{B}_m$ the Maiorana-McFarland bent function $f(x,y) = Tr(x\pi(y)) + h(y)$ has the unique $\mathcal{M}$-subspace.

- E.g., one can take an APN permutation π

Proposition (Pasalic, Polujan, Kudin and F. Zhang 2023)

Let $f_1, \ldots, f_4 \in \mathcal{B}_n$ be Maiorana-McFarland bent functions, each having the unique $\mathcal{M}$-subspaces $U = \mathbb{F}_{2^m} \times \{0\}$ of dim. $n/2$. Then, the shape of an $\mathcal{M}$-subspace of $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ of dim. $n/2+1$ is determined.

Step III: $\mathcal{M}$-subspaces of $f = f_1||f_2||f_3||f_4$

Proposition (Pasalic, Polujan, Kudin and F. Zhang 2023)

Let π be a permutation of $\mathbb{F}_{2^m}$. If $D_a D_b \pi \neq 0$ for all linearly independent $a, b \in \mathbb{F}_{2^m}$, then for any $h \in \mathcal{B}_m$ the Maiorana-McFarland bent function $f(x, y) = Tr(x\pi(y)) + h(y)$ has the unique $\mathcal{M}$-subspace.

- E.g., one can take an APN permutation π

Proposition (Pasalic, Polujan, Kudin and F. Zhang 2023)

Let $f_1, \ldots, f_4 \in \mathcal{B}_n$ be Maiorana-McFarland bent functions, each having the unique $\mathcal{M}$-subspaces $U = \mathbb{F}_{2^m} \times \{0\}$ of dim. $n/2$. Then, the shape of an $\mathcal{M}$-subspace of $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ of dim. $n/2 + 1$ is determined.

- If $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is in $\mathcal{MM}^{\#}$, there are a few witnesses

Step III: $\mathcal{M}$-subspaces of $f = f_1||f_2||f_3||f_4$

Proposition (Pasalic, Polujan, Kudin and F. Zhang 2023)

Let π be a permutation of $\mathbb{F}_{2^m}$. If $D_a D_b \pi \neq 0$ for all linearly independent $a, b \in \mathbb{F}_{2^m}$, then for any $h \in \mathcal{B}_m$ the Maiorana-McFarland bent function $f(x,y) = Tr(x\pi(y)) + h(y)$ has the unique $\mathcal{M}$-subspace.

- E.g., one can take an APN permutation π

Proposition (Pasalic, Polujan, Kudin and F. Zhang 2023)

Let $f_1, \ldots, f_4 \in \mathcal{B}_n$ be Maiorana-McFarland bent functions, each having the unique $\mathcal{M}$-subspaces $U = \mathbb{F}_{2^m} \times \{0\}$ of dim. $n/2$. Then, the shape of an $\mathcal{M}$-subspace of $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ of dim. $n/2+1$ is determined.

- If $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$ is in $\mathcal{MM}^\#$, there are a few witnesses
- Hence, easier to check the Dillon's criterion

Back to the main result

Theorem (Polujan, Pasalic, Kudin and F. Zhang 2023)

Let $m \in \mathbb{N}$ with $m \geq 3$ and $d^2 \equiv 1 \mod 2^m - 1$. For $i = 1, 2, 3$, define permutations π_i of $\mathbb{F}_{2^m}$ by $\pi_i(y) = \alpha_i y^d$, where $\alpha_i \in \mathbb{F}_{2^m}^*$ are pairwise distinct elements s.t. $\alpha_i^{d+1} = 1$ and $\alpha_4^{d+1} = 1$ with $\alpha_4 = \alpha_1 + \alpha_2 + \alpha_3$. Define bent functions $f_i(x, y) = Tr\left(x\pi_i(y)\right) + h_i(y)$ for $x, y \in \mathbb{F}_{2^m}$, where

1. $h_i(y) = Tr\left(\frac{\alpha_{i+1}}{\alpha_i^k} y^k\right)$ *for* $i = 1, 2, 3$ *and* $h_4(y) = Tr\left(\frac{\alpha_1}{\alpha_4} y^k\right) + 1$,
2. $\pi_i(y) = \alpha_i y^d$ *satisfy* $D_{a,b}\pi_i \neq 0$ *for all lin. indep.* $a, b \in \mathbb{F}_{2^m}$.

If $wt(d) > 1$, then $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{2m+2}$ is bent and outside $\mathcal{MM}^\#$.

- For m odd, the APN permutations $\pi_i(y) = \alpha_i y^{-1}$ always work

Conclusion and future work

Summary

I. An explicit construction method of bent functions, including the construction from APN permutations

II. More results in the extended abstract:

1. A recursive construction of permutations with the $(\mathcal{A}_m)$ property
2. Further analysis of homogeneous cubic bent functions

Open problems

1. Find further explicit constructions of bent functions of the form $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$.
2. Particularly, if $f_i(x,y) = Tr\left(x\pi_i(y)\right) + h_i(y)$, what are the other choices of π_i and h_i?

On bent functions satisfying the dual bent condition[1,2]

Alexandr Polujan[a], Enes Pasalic[b], Sadmir Kudin[b], Fengrong Zhang[c]

[a]Otto von Guericke University Magdeburg, Germany
[b]University of Primorska, FAMNIT & IAM, Koper, Slovenia
[c]Xidian University, Xian, P.R. China

BFA 2023
The 8th International Workshop on
Boolean Functions and their Applications,
05.09.2023

[1]Enes Pasalic, Alexandr Polujan, Sadmir Kudin and Fengrong Zhang. *Design and analysis of bent functions using $\mathcal{M}$-subspaces*. 2023. arXiv: 2304.13432 [cs.IT].

[2]Alexandr Polujan, Enes Pasalic, Sadmir Kudin and Fengrong Zhang. *Bent functions satisfying the dual bent condition and permutations with the $(\mathcal{A}_m)$ property*.

Further Reading I

[CC03] A. Canteaut and P. Charpin. "Decomposing bent functions". In: *IEEE Transactions on Information Theory* 49.8 (2003), pp. 2004–2019. DOI: https://doi.org/10.1109/TIT.2003.814476 (cit. on pp. 5, 6).

[CPM19] Nastja Cepak, Enes Pasalic and Amela Muratović-Ribić. "Frobenius linear translators giving rise to new infinite classes of permutations and bent functions". In: *Cryptography and Communications* 11.6 (Nov. 2019), pp. 1275–1295. DOI: https://doi.org/10.1007/s12095-019-00395-1 (cit. on pp. 16–19).

Further Reading II

[Dil74] J. F. Dillon. "Elementary Hadamard Difference Sets". PhD thesis. University of Maryland, 1974. DOI: https://doi.org/10.13016/M2MS3K194 (cit. on pp. 23–27).

[HPZ19] Samir Hodžić, Enes Pasalic and Weiguo Zhang. "Generic Constructions of Five-Valued Spectra Boolean Functions". In: *IEEE Transactions on Information Theory* 65.11 (2019), pp. 7554–7565. DOI: https://doi.org/10.1109/TIT.2019.2910808 (cit. on p. 9).

Further Reading III

[Kol17] Nikolay Kolomeec. “The graph of minimal distances of bent functions and its properties”. In: *Designs, Codes and Cryptography* 85.3 (Dec. 2017), pp. 395–410. ISSN: 1573-7586. DOI: https://doi.org/10.1007/s10623-016-0306-4 (cit. on pp. 23–27).

[MCM15] Sihem Mesnager, Gérard Cohen and David Madore. “On Existence (Based on an Arithmetical Problem) and Constructions of Bent Functions”. In: *Cryptography and Coding*. Ed. by Jens Groth. Cham: Springer International Publishing, 2015, pp. 3–19. ISBN: 978-3-319-27239-9. DOI: https://doi.org/10.1007/978-3-319-27239-9_1 (cit. on pp. 20–22).

Further Reading IV

[Mes14] Sihem Mesnager. "Several New Infinite Families of Bent Functions and Their Duals". In: *IEEE Transactions on Information Theory* 60.7 (2014), pp. 4397–4407. DOI: https://doi.org/10.1109/TIT.2014.2320974 (cit. on pp. 16, 17).

[Pas+23] Enes Pasalic, Alexandr Polujan, Sadmir Kudin and Fengrong Zhang. *Design and analysis of bent functions using $\mathcal{M}$-subspaces*. 2023. DOI: https://doi.org/10.48550/arXiv.2304.13432. arXiv: 2304.13432 [cs.IT] (cit. on pp. 1, 9, 28–30, 33).

[Pol+23] Alexandr Polujan, Enes Pasalic, Sadmir Kudin and Fengrong Zhang. *Bent functions satisfying the dual bent condition and permutations with the $(\mathcal{A}_m)$ property*. 2023 (cit. on pp. 1, 14, 18–22, 31, 33).

Further Reading V

[PP20] Alexandr Polujan and Alexander Pott. "Cubic bent functions outside the completed Maiorana-McFarland class". In: *Designs, Codes and Cryptography* 88.9 (Sept. 2020), pp. 1701–1722. DOI: https://doi.org/10.1007/s10623-019-00712-y (cit. on pp. 23–27).

[Pre+91] Bart Preneel, Werner Van Leekwijck, Luc Van Linden, René Govaerts and Joos Vandewalle. "Propagation Characteristics of Boolean Functions". In: *Advances in Cryptology — EUROCRYPT '90*. Ed. by Ivan Bjerre Damgård. Berlin, Heidelberg: Springer Berlin Heidelberg, 1991, pp. 161–173. ISBN: 978-3-540-46877-6. DOI: https://doi.org/10.1007/3-540-46877-3_14 (cit. on p. 9).