Bent functions - five decades later

Enes Pasalic

University of Primorska, Koper, Slovenia
Joint work with S. Kudin, A. Polujan and F. Zhang

IRSEE 2025, September 2025

Summary of the talk

- Bent functions and their applications
- Primary classes of bent functions
- Modifying the $\mathcal{M}$-class
- $\mathcal{M}$-subspaces in the design of bent functions, 4-concatenation
- Bent functions in the $\mathcal{GMM}$ class
- Concluding remarks

Boolean functions

- Boolean mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $\mathbb{F}_2 = \{0, 1\}$. All such f in $\mathfrak{B}_n$.

Definition

The *truth table of f* - evaluation of f for all possible inputs.

x_3	x_2	x_1	$f(x)$	$f(x) \oplus x_1$	$W_f(a)$
0	0	0	0	0	0
0	0	1	0	1	4
0	1	0	0	0	0
0	1	1	1	0	-4
1	0	0	1	1	4
1	0	1	1	0	0
1	1	0	0	0	4
1	1	1	1	0	0

The **truth table** gives $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3$, $\deg(f) = 2$.

Walsh transform and research complexity

- **Walsh (Fourier) transform** for $f : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}; \quad a \in \mathbb{F}_2^n; \quad a \cdot x = a_1 x_1 \oplus \cdots \oplus a_n x_n.$$

- Parseval's equality: $\sum_{a \in \mathbb{F}_2^n} W_f(a)^2 = 2^{2n}$, **for any** $f \in \mathfrak{B}_n$!

- Measures the Hamming distance between f and linear functions $a \cdot x$ (linear cryptanalysis); covering radius of 1st order Reed-Muller code

- **COMPLEXITY:** The space too large 2^{2^n} to search for suitable ones to be used in (symmetric-key) cryptography

- The research complexity comes from different cryptographic requests: nonlinearity, alg. degree, resiliency, higher order nonl. ...

Walsh transform and research complexity

- **Walsh (Fourier) transform** for $f : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}; \quad a \in \mathbb{F}_2^n; \quad a \cdot x = a_1x_1 \oplus \cdots \oplus a_nx_n.$$

- Parseval's equality: $\sum_{a \in \mathbb{F}_2^n} W_f(a)^2 = 2^{2n}$, **for any** $f \in \mathfrak{B}_n$!

- Measures the Hamming distance between f and linear functions $a \cdot x$ (linear cryptanalysis); covering radius of 1st order Reed-Muller code

- **COMPLEXITY:** The space too large 2^{2^n} to search for suitable ones to be used in (symmetric-key) cryptography

- The research complexity comes from different cryptographic requests: nonlinearity, alg. degree, resiliency, higher order nonl. ...

Walsh transform and research complexity

- **Walsh (Fourier) transform** for $f : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}; \quad a \in \mathbb{F}_2^n; \quad a \cdot x = a_1 x_1 \oplus \cdots \oplus a_n x_n.$$

- Parseval's equality: $\sum_{a \in \mathbb{F}_2^n} W_f(a)^2 = 2^{2n}$, **for any** $f \in \mathfrak{B}_n$!

- Measures the Hamming distance between f and linear functions $a \cdot x$ (linear cryptanalysis); covering radius of 1st order Reed-Muller code

- **COMPLEXITY:** The space too large 2^{2^n} to search for suitable ones to be used in (symmetric-key) cryptography

- The research complexity comes from different cryptographic requests: nonlinearity, alg. degree, resiliency, higher order nonl. ...

Bent functions - perfect combinatorial objects

Why perfect ??

- Walsh **spectra is uniform** $W_f \in \{\pm 2^{\frac{n}{2}}\}$ for bent $f \in \mathfrak{B}_n$, for even n only, thus **highest nonlinearity** (distance to affine functions) !!
- Take a **derivative** $D_a f(x) := f(x \oplus a) \oplus f(x)$ for any nonzero a, then $D_a f(x)$ is a **balanced** function ($\#0 = \#1$ in the truth table) !
- Given f, its Cayley graph ($(u, v) \in E_f$ IFF $f(u \oplus v) = 1$) is strongly regular (SRG) !! ...

Applications ??

- cryptography
- spread spectrum communications, sequences
- **coding theory**
- correspondence to (relative) difference sets, design theory

Bent functions - perfect combinatorial objects

Why perfect ??

- Walsh **spectra is uniform** $W_f \in \{\pm 2^{\frac{n}{2}}\}$ for bent $f \in \mathfrak{B}_n$, for even n only, thus **highest nonlinearity** (distance to affine functions) !!
- Take a **derivative** $D_a f(x) := f(x \oplus a) \oplus f(x)$ for any nonzero a, then $D_a f(x)$ is a **balanced** function ($\#0 = \#1$ in the truth table) !
- Given f, its Cayley graph ($(u, v) \in E_f$ IFF $f(u \oplus v) = 1$) is strongly regular (SRG) !! ...

Applications ??

- cryptography
- spread spectrum communications, sequences
- **coding theory**
- correspondence to (relative) difference sets, design theory

Difference sets of 2-abelian group $G = \mathbb{Z}_2^{2m}$

Combinatorial structure of additive 2-abelian group $G = \mathbb{Z}_2^{2m}$, with $n = 2m$.

- In general, a k-**subset** D of a group G is a (v, k, λ) difference set, if the following holds:
  - $|G| = v; \qquad |D| = k$
  - $g = d - d'$ has exactly λ solutions $d, d' \in D$ if $g \neq 0$.

- **FACT:** Only difference sets in $\mathbb{Z}_2^{2m} = \mathbb{F}_2^{2m} = G$ have parameters

$$(2^{2m}, |D| = 2^{2m-1} \pm 2^{m-1}, \lambda = 2^{2m-2} \pm 2^{m-1}).$$

EXAMPLE: For $n = 2m = 4$ difference sets of the form $(16, 6, 2)$ exist.

HOW: Take $D = \{x : f(x) = 1\}$ of a (necessarily) **bent function** as in the next example ! E.g. $0001 = 1010 + 1011$ (and vice versa)

Difference sets of 2-abelian group $G = \mathbb{Z}_2^{2m}$

Combinatorial structure of additive 2-abelian group $G = \mathbb{Z}_2^{2m}$, with $n = 2m$.

- In general, a k-**subset** D of a group G is a (v, k, λ) difference set, if the following holds:
  - $|G| = v; \qquad |D| = k$
  - $g = d - d'$ has exactly λ solutions $d, d' \in D$ if $g \neq 0$.
- **FACT:** Only difference sets in $\mathbb{Z}_2^{2m} = \mathbb{F}_2^{2m} = G$ have parameters

$$(2^{2m}, |D| = 2^{2m-1} \pm 2^{m-1}, \lambda = 2^{2m-2} \pm 2^{m-1}).$$

EXAMPLE: For $n = 2m = 4$ difference sets of the form $(16, 6, 2)$ exist.

HOW: Take $D = \{x : f(x) = 1\}$ of a (necessarily) **bent function** as in the next example ! E.g. $0001 = 1010 + 1011$ (and vice versa)

Difference sets of 2-abelian group $G = \mathbb{Z}_2^{2m}$

Combinatorial structure of additive 2-abelian group $G = \mathbb{Z}_2^{2m}$, with $n = 2m$.

- In general, a k-**subset** D of a group G is a (v, k, λ) difference set, if the following holds:
  - $|G| = v; \qquad |D| = k$
  - $g = d - d'$ has exactly λ solutions $d, d' \in D$ if $g \neq 0$.
- **FACT:** Only difference sets in $\mathbb{Z}_2^{2m} = \mathbb{F}_2^{2m} = G$ have parameters

$$(2^{2m}, |D| = 2^{2m-1} \pm 2^{m-1}, \lambda = 2^{2m-2} \pm 2^{m-1}).$$

EXAMPLE: For $n = 2m = 4$ difference sets of the form $(16, 6, 2)$ exist.

HOW: Take $D = \{x : f(x) = 1\}$ of a (necessarily) **bent function** as in the next example ! E.g. $0001 = 1010 + 1011$ (and vice versa)

Difference set - an example

- Example $f(x,y) = x \cdot y = x_1y_1 \oplus x_2y_2$, for $x = (x_1, x_2)$, $y = (y_1, y_2)$.

y_2	y_1	x_2	x_1	$f(x,y)$
0	0	0	0	0
0	**0**	**0**	**1**	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	1
0	1	1	0	0
0	1	1	1	1
1	0	0	0	0
1	0	0	1	0
1	**0**	**1**	**0**	1
1	**0**	**1**	**1**	1
1	1	0	0	0
1	1	0	1	1
1	1	1	0	1
1	1	1	1	0

Primary classes of bent functions - $\mathcal{M}$ class

- It turns out that for $n \leq 6$, n is even, **all bent functions are in** the (completed) Maiorana-McFarland ($\mathcal{M}$) class given by

$$f(x,y) = x \cdot \pi(y) + g(y) \quad x, y \in \mathbb{F}_2^{n/2},$$

  where π is a **permutation** on $\mathbb{F}_2^{n/2}$ and $g \in \mathfrak{B}_{n/2}$ **arbitrary** Boolean.
- For any fixed $y = a$, $f(x,a) = x \cdot \pi(a) + g(a)$ is affine in x.

- **Introduced in 1973**, and Dillon showed in 1976 that $f \in \mathcal{M}^{\#}$ IFF $\exists$ lin. subspace V with $\dim(V) = n/2$ s. t. **for all** $a, b \in V$:

$$D_a D_b f(x) = f(x) + f(x+a) + f(x+b) + f(x+a+b) = 0, \quad \forall x \in \mathbb{F}_2^n.$$

- EA-equivalence provides **completed class** $\mathcal{M}^{\#}$:

$$\mathcal{M}^{\#} = \{f(Ax+b)+c\cdot x+d : f \in \mathcal{M}, A \in GL(n,\mathbb{F}_2), b,c \in \mathbb{F}_2^n, d \in \mathbb{F}_2\}.$$

Primary classes of bent functions - $\mathcal{M}$ class

- It turns out that for $n \leq 6$, n is even, **all bent functions are in** the (completed) Maiorana-McFarland ($\mathcal{M}$) class given by

$$f(x,y) = x \cdot \pi(y) + g(y) \quad x, y \in \mathbb{F}_2^{n/2},$$

where π is a **permutation** on $\mathbb{F}_2^{n/2}$ and $g \in \mathfrak{B}_{n/2}$ **arbitrary** Boolean.

- For any fixed $y = a$, $f(x,a) = x \cdot \pi(a) + g(a)$ is affine in x.

- **Introduced in 1973**, and Dillon showed in 1976 that $f \in \mathcal{M}^{\#}$ IFF $\exists$ lin. subspace V with $\dim(V) = n/2$ s. t. **for all** $a, b \in V$:

$$D_aD_bf(x) = f(x) + f(x+a) + f(x+b) + f(x+a+b) = 0, \quad \forall x \in \mathbb{F}_2^n.$$

- EA-equivalence provides **completed class** $\mathcal{M}^{\#}$:

$$\mathcal{M}^{\#} = \{f(Ax+b)+c\cdot x+d : f \in \mathcal{M}, A \in GL(n,\mathbb{F}_2), b, c \in \mathbb{F}_2^n, d \in \mathbb{F}_2\}.$$

- It turns out that for $n \leq 6$, n is even, **all bent functions are in** the (completed) Maiorana-McFarland ($\mathcal{M}$) class given by

$$f(x,y) = x \cdot \pi(y) + g(y) \quad x, y \in \mathbb{F}_2^{n/2},$$

where π is a **permutation** on $\mathbb{F}_2^{n/2}$ and $g \in \mathfrak{B}_{n/2}$ **arbitrary** Boolean.

- For any fixed $y = a$, $f(x,a) = x \cdot \pi(a) + g(a)$ is affine in x.

- **Introduced in 1973**, and Dillon showed in 1976 that $f \in \mathcal{M}^{\#}$ IFF $\exists$ lin. subspace V with $\dim(V) = n/2$ s. t. **for all** $a, b \in V$:

$$D_a D_b f(x) = f(x) + f(x+a) + f(x+b) + f(x+a+b) = 0, \;\; \forall x \in \mathbb{F}_2^n.$$

- EA-equivalence provides **completed class** $\mathcal{M}^{\#}$:

$$\mathcal{M}^{\#} = \{ f(Ax+b) + c \cdot x + d : f \in \mathcal{M}, A \in GL(n, \mathbb{F}_2), b, c \in \mathbb{F}_2^n, d \in \mathbb{F}_2 \}.$$

Showing that $V = \mathbb{F}_2^{n/2} \times \{0_{n/2}\}$ is an $\mathcal{M}$-subspace

- Any V s.t. $D_a D_b f = 0$ for all $a, b \in V$ is called an $\mathcal{M}$-subspace.
- For $f \in \mathcal{M}$ the **canonical $\mathcal{M}$-subspace** is $V = \mathbb{F}_2^{n/2} \times \{0_{n/2}\}$ (might be many more but for any V we have $\dim(V) \leq n/2$)
- **Proof:** Consider $f(x, y) = x \cdot \pi(y)$ (since $g(y)$ does not matter) and
- Let $a = (a_1, 0_{n/2}), b = (b_1, 0_{n/2}) \in \mathbb{F}_2^{n/2} \times \{0_{n/2}\}$. Then,

$$\begin{aligned} f(x + a_1, y) &= (x + a_1) \cdot \pi(y) \\ f(x + b_1, y) &= (x + b_1) \cdot \pi(y) \\ f(x + a_1 + b_1, y) &= (x + a_1 + b_1) \cdot \pi(y) \end{aligned}$$

- We get $f(x, y) + f(x + a_1, y) + f(x + b_1, y) + f(x + a_1 + b_1, y) = 0$, for all $x, y \in \mathbb{F}_2^{n/2}$.

Showing that $V = \mathbb{F}_2^{n/2} \times \{0_{n/2}\}$ is an $\mathcal{M}$-subspace

- Any V s.t. $D_a D_b f = 0$ for all $a, b \in V$ is called an $\mathcal{M}$-subspace.
- For $f \in \mathcal{M}$ the **canonical $\mathcal{M}$-subspace** is $V = \mathbb{F}_2^{n/2} \times \{0_{n/2}\}$ (might be many more but for any V we have $\dim(V) \leq n/2$)
- **Proof:** Consider $f(x, y) = x \cdot \pi(y)$ (since $g(y)$ does not matter) and
- Let $a = (a_1, 0_{n/2}), b = (b_1, 0_{n/2}) \in \mathbb{F}_2^{n/2} \times \{0_{n/2}\}$. Then,

$$\begin{aligned} f(x + a_1, y) &= (x + a_1) \cdot \pi(y) \\ f(x + b_1, y) &= (x + b_1) \cdot \pi(y) \\ f(x + a_1 + b_1, y) &= (x + a_1 + b_1) \cdot \pi(y) \end{aligned}$$

- We get $f(x, y) + f(x + a_1, y) + f(x + b_1, y) + f(x + a_1 + b_1, y) = 0$, for all $x, y \in \mathbb{F}_2^{n/2}$.

Showing that $V = \mathbb{F}_2^{n/2} \times \{0_{n/2}\}$ is an $\mathcal{M}$-subspace

- Any V s.t. $D_a D_b f = 0$ for all $a, b \in V$ is called an $\mathcal{M}$-subspace.

- For $f \in \mathcal{M}$ the **canonical $\mathcal{M}$-subspace** is $V = \mathbb{F}_2^{n/2} \times \{0_{n/2}\}$ (might be many more but for any V we have $\dim(V) \leq n/2$)

- **Proof:** Consider $f(x, y) = x \cdot \pi(y)$ (since $g(y)$ does not matter) and

- Let $a = (a_1, 0_{n/2}), b = (b_1, 0_{n/2}) \in \mathbb{F}_2^{n/2} \times \{0_{n/2}\}$. Then,

$$\begin{aligned} f(x + a_1, y) &= (x + a_1) \cdot \pi(y) \\ f(x + b_1, y) &= (x + b_1) \cdot \pi(y) \\ f(x + a_1 + b_1, y) &= (x + a_1 + b_1) \cdot \pi(y) \end{aligned}$$

- We get $f(x, y) + f(x + a_1, y) + f(x + b_1, y) + f(x + a_1 + b_1, y) = 0$, for all $x, y \in \mathbb{F}_2^{n/2}$.

Primary classes of bent functions - $\mathcal{PS}$ class

- Also, Partial Spread ($\mathcal{PS}$) class of Dillon 1976 (indicator of a union of $2^{n/2-1}$ (or $2^{n/2-1}+1$) of **disjoint lin. subspaces of dim.** $n/2$).

- **PROBLEM (Classification/Enumeration):** Both $\mathcal{M}$ and $\mathcal{PS}$ class only a **tiny portion** of all bent functions - find other classes !!

- For $n = 8$, both $\mathcal{M}^{\#}$ and $\mathcal{PS}^{\#}$ give only 2^{77} out of 2^{106} bent functions

Primary classes of bent functions - $\mathcal{PS}$ class

- Also, Partial Spread ($\mathcal{PS}$) class of Dillon 1976 (indicator of a union of $2^{n/2-1}$ (or $2^{n/2-1}+1$) of **disjoint lin. subspaces of dim.** $n/2$).

- **PROBLEM (Classification/Enumeration):** Both $\mathcal{M}$ and $\mathcal{PS}$ class only a **tiny portion** of all bent functions - find other classes !!

- For $n=8$, both $\mathcal{M}^{\#}$ and $\mathcal{PS}^{\#}$ give only 2^{77} out of 2^{106} bent functions

Modifying the $\mathcal{M}$ class - the $\mathcal{C}$ class

- Originally suggested by Dillon in his PhD thesis, developed by C. Carlet in 1993

- The class $\mathcal{C}$ is the set of all (bent) Boolean functions of the form

$$f(x,y) = x \cdot \pi(y) + \mathbb{1}_{L^\perp}(x), \quad x, y \in \mathbb{F}_2^m$$

  where L is any linear subspace of $\mathbb{F}_2^m$, $\mathbb{1}_{L^\perp}$ is the indicator function of the space $L^\perp$, and π is any permutation of $\mathbb{F}_2^m$ such that:

$$(C) \qquad \phi(a+L) \text{ is an affine subspace, for all } a \in \mathbb{F}_2^m, \text{ with } \phi := \pi^{-1}.$$

- Modification performed for any $(x,y) \in L^\perp \times \mathbb{F}_2^m$!

Some sufficient conditions for $\mathcal{C}$ class

Theorem (F. Zhang, EP, N. Cepak, Y. Wei 2016)

Let $n = 2m \geq 8$ *and*

$$f(x,y) = x \cdot \pi(y) \oplus 1_{L^\perp}(x), \quad x, y \in \mathbb{F}_2^m$$

so that (π, L) *has property* (C). *If* (π, L) *satisfies:*

1. $\dim(L) \geq 2$;
2. $u \cdot \pi$ *has no nonzero linear structure for all* $u \in \mathbb{F}_2^m \setminus \{0_n\}$,

then f **does not belong to** $\mathcal{M}^\#$.

- **NOTE**: Linear structure means that $u \cdot \pi(y) + u \cdot \pi(y + a) = 0/1$!
- Using $\pi(y) = (\pi_1(y), \ldots, \pi_m(y))$ we want to avoid $u_1\pi_1(y) + \cdots + u_m\pi_m(y) + u_1\pi_1(y + a) + \cdots + u_m\pi_m(y + a) = 0/1.$

Some sufficient conditions for $\mathcal{C}$ class

Theorem (F. Zhang, EP, N. Cepak, Y. Wei 2016)

Let $n = 2m \geq 8$ and

$$f(x,y) = x \cdot \pi(y) \oplus 1_{L^\perp}(x), \quad x, y \in \mathbb{F}_2^m$$

so that (π, L) has property (C). If (π, L) satisfies:

1. $\dim(L) \geq 2$;
2. *$u \cdot \pi$ has no nonzero linear structure for all $u \in \mathbb{F}_2^m \setminus \{0_n\}$,*

then f **does not belong to $\mathcal{M}^\#$**.

- **NOTE**: Linear structure means that $u \cdot \pi(y) + u \cdot \pi(y+a) = 0/1$!
- Using $\pi(y) = (\pi_1(y), \ldots, \pi_m(y))$ we want to avoid $u_1\pi_1(y) + \cdots + u_m\pi_m(y) + u_1\pi_1(y+a) + \cdots + u_m\pi_m(y+a) = 0/1.$

An explicit family in $\mathcal{C}$ outside $\mathcal{M}$

A few articles on this topic "bent functions in $\mathcal{C}/\mathcal{D}$ outside $\mathcal{M}^{\#}$", for instance one result (for large $n = 2m$) is:

Theorem ([3]- S. Kudin, EP)

- *Let m, k and t be three integers such that and $m \geq k \geq t + 3 \geq 4$.*
- *Let S be an* **arbitrary subset** *of $E_t = \langle \mathbb{e}_1, \mathbb{e}_2, \ldots, \mathbb{e}_t \rangle \subset \mathbb{F}_2^m$.*
- *Let $\sigma_S(y)$ be an* **arbitrary non-identity permutation** *of $\mathbb{F}_2^m$ which fixes elements in $\mathbb{F}_2^m \setminus S$, (hence $|S| \geq 2$).*
- *Define $f(x, y) = x \cdot \sigma_S(y) + 1_{E_k^{\perp}}(x)$, with $x, y \in \mathbb{F}_2^m$, where $E_k = \langle \mathbb{e}_1, \mathbb{e}_2, \ldots, \mathbb{e}_k \rangle \subseteq \mathbb{F}_2^m$.*
- *Then, f is a* **bent function in $\mathcal{C}$ outside $\mathcal{M}^{\#}$**.

An explicit family in $\mathcal{C}$ outside $\mathcal{M}$

A few articles on this topic "bent functions in $\mathcal{C}/\mathcal{D}$ outside $\mathcal{M}^{\#}$", for instance one result (for large $n = 2m$) is:

Theorem ([3]- S. Kudin, EP)

- *Let* m, k *and* t *be three integers such that and* $m \geq k \geq t + 3 \geq 4$.
- *Let* S *be an* **arbitrary subset** *of* $E_t = \langle \mathbb{e}_1, \mathbb{e}_2, \ldots, \mathbb{e}_t \rangle \subset \mathbb{F}_2^m$.
- *Let* $\sigma_S(y)$ *be an* **arbitrary non-identity permutation** *of* $\mathbb{F}_2^m$ *which fixes elements in* $\mathbb{F}_2^m \setminus S$, *(hence* $|S| \geq 2$*).*
- *Define* $f(x, y) = x \cdot \sigma_S(y) + 1_{E_k^{\perp}}(x)$, *with* $x, y \in \mathbb{F}_2^m$, *where* $E_k = \langle \mathbb{e}_1, \mathbb{e}_2, \ldots, \mathbb{e}_k \rangle \subseteq \mathbb{F}_2^m$.
- *Then,* f *is a* **bent function in** $\mathcal{C}$ **outside** $\mathcal{M}^{\#}$.

Modifying the $\mathcal{M}$ class - the $\mathcal{D}$ class

- The class $\mathcal{D}$, defined similarly as $\mathcal{C}$ by C. Carlet in 1993, is the set of all Boolean **(bent)** functions of the form

$$f(x,y) = x \cdot \pi(y) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y), \quad x, y \in \mathbb{F}_2^m,$$

(D) E_1, E_2 two linear subspaces of $\mathbb{F}_2^m$ such that $\pi(E_2) = E_1^{\perp}$, and $\dim(E_1) + \dim(E_2) = m$ (min. distance between bent functions 2^m).

- Special case when $E_1 = 0_m$ and $E_2 = \mathbb{F}_2^m$ (**called $\mathcal{D}_0$ class**), then

$$\mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) = \delta_0(x) = \prod_{i=1}^{m}(x_i \oplus 1).$$

- Carlet proved that $\mathcal{D}_0 \not\subset \mathcal{M}^{\#}$ and $\mathcal{D}_0 \not\subset \mathcal{PS}^{\#}$; in the former case **enough that a restriction of π to any hyperplane is not affine !**

Modifying the $\mathcal{M}$ class - the $\mathcal{D}$ class

- The class $\mathcal{D}$, defined similarly as $\mathcal{C}$ by C. Carlet in 1993, is the set of all Boolean **(bent)** functions of the form

$$f(x,y) = x \cdot \pi(y) + 1\!\!1_{E_1}(x) 1\!\!1_{E_2}(y), \;\; x, y \in \mathbb{F}_2^m,$$

(D) E_1, E_2 two linear subspaces of $\mathbb{F}_2^m$ such that $\pi(E_2) = E_1^{\perp}$, and $\dim(E_1) + \dim(E_2) = m$ (min. distance between bent functions 2^m).

- Special case when $E_1 = 0_m$ and $E_2 = \mathbb{F}_2^m$ (**called $\mathcal{D}_0$ class**), then

$$1\!\!1_{E_1}(x) 1\!\!1_{E_2}(y) = \delta_0(x) = \prod_{i=1}^{m} (x_i \oplus 1).$$

- Carlet proved that $\mathcal{D}_0 \not\subset \mathcal{M}^{\#}$ and $\mathcal{D}_0 \not\subset \mathcal{PS}^{\#}$; in the former case **enough that a restriction of π to any hyperplane is not affine !**

Modifying the $\mathcal{M}$ class - the $\mathcal{D}$ class

- The class $\mathcal{D}$, defined similarly as $\mathcal{C}$ by C. Carlet in 1993, is the set of all Boolean **(bent)** functions of the form

$$f(x,y) = x \cdot \pi(y) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y), \;\; x, y \in \mathbb{F}_2^m,$$

(D) E_1, E_2 two linear subspaces of $\mathbb{F}_2^m$ such that $\pi(E_2) = E_1^{\perp}$, and $\dim(E_1) + \dim(E_2) = m$ (min. distance between bent functions 2^m).

- Special case when $E_1 = 0_m$ and $E_2 = \mathbb{F}_2^m$ (**called $\mathcal{D}_0$ class**), then

$$\mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) = \delta_0(x) = \prod_{i=1}^{m}(x_i \oplus 1).$$

- Carlet proved that $\mathcal{D}_0 \not\subset \mathcal{M}^{\#}$ and $\mathcal{D}_0 \not\subset \mathcal{PS}^{\#}$; in the former case **enough that a restriction of π to any hyperplane is not affine** !

$\mathcal{D}_0$ outside $\mathcal{M}^\#$ - large degree

Lemma ([3])

Let $g \in \mathfrak{B}_n$. If there exists an $(n-k)$-dimensional $\mathcal{M}$-subspace H of $\mathbb{F}_2^n$, such that $D_aD_bg = 0$ for all $a, b \in H$, then $\deg(g) \leq k+1$.

Theorem ([3])

Let m be an integer, $m \geq 4$. Let π be a permutation of $\mathbb{F}_2^m$ with $\deg(\pi) \geq 3$. Then,

$$f(x,y) = x \cdot \pi(y) + \delta_0(x) \in \mathcal{D}_0, \quad x, y \in \mathbb{F}_2^m,$$

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

- The algebraic degree of π over $\mathbb{F}_2^m$ is $\deg(\pi) = \max_{1 \leq i \leq m} \deg(\pi_i)$.

$\mathcal{D}_0$ outside $\mathcal{M}^{\#}$ - large degree

Lemma ([3])

Let $g \in \mathfrak{B}_n$. If there exists an $(n-k)$-dimensional $\mathcal{M}$-subspace H of $\mathbb{F}_2^n$, such that $D_a D_b g = 0$ for all $a, b \in H$, then $\deg(g) \le k+1$.

Theorem ([3])

Let m be an integer, $m \ge 4$. Let π be a permutation of $\mathbb{F}_2^m$ with $\deg(\pi) \ge 3$. Then,

$$f(x,y) = x \cdot \pi(y) + \delta_0(x) \in \mathcal{D}_0, \quad x, y \in \mathbb{F}_2^m,$$

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

- The algebraic degree of π over $\mathbb{F}_2^m$ is $\deg(\pi) = \max_{1 \le i \le m} \deg(\pi_i)$.

$\mathcal{D}_0$ outside $\mathcal{M}^{\#}$ - quadratic case

Theorem ([3]- complete characterization)

Let π be a **quadratic permutation** *of $\mathbb{F}_2^m$, $m \geq 4$. Then,*

$$f(x, y) = x \cdot \pi(y) + \delta_0(x) \in \mathcal{M}^{\#}$$

IFF there is a linear hyperplane of $\mathbb{F}_2^m$ on which π is affine.

- The presented results give some explicit families of bent functions outside $\mathcal{M}^{\#}$ but we are **far away from** 2^{106} (e.g. $\#\mathcal{D}_0^{\#} < \#\mathcal{M}^{\#}$).
- To handle this, we have taken **two different approaches**:
  - concatenation/decomposition method (in terms of $\mathcal{M}$-subspaces)
  - and the generalized M-M class ($\mathcal{GMM}$)

$\mathcal{D}_0$ outside $\mathcal{M}^\#$ - quadratic case

Theorem ([3]- complete characterization)

Let π *be a* **quadratic permutation** *of* $\mathbb{F}_2^m$, $m \geq 4$. *Then,*

$$f(x, y) = x \cdot \pi(y) + \delta_0(x) \in \mathcal{M}^\#$$

IFF there is a linear hyperplane of $\mathbb{F}_2^m$ *on which* π *is affine.*

- The presented results give some explicit families of bent functions outside $\mathcal{M}^\#$ but we are **far away from** 2^{106} (e.g. $\#\mathcal{D}_0^\# < \#\mathcal{M}^\#$).
- To handle this, we have taken **two different approaches**:
  - concatenation/decomposition method (in terms of $\mathcal{M}$-subspaces)
  - and the generalized M-M class ($\mathcal{GMM}$)

$\mathcal{M}$-subspaces of Boolean (bent) functions

- Recall, for $f \in \mathfrak{B}_n$ a vector subspace V of $\mathbb{F}_2^n$ is called an $\mathcal{M}$-subspace of f, if $D_a D_b f = 0$, for all $a, b \in V$.

- **The maximum dimension of any $\mathcal{M}$-subspace V is** $n/2$, for any bent function f ($\dim(V) = n/2 \Leftrightarrow f \in \mathcal{M}^{\#}$).

- Useful to distinguish bent functions $\{f\}$ w.r.t. the **maximal dimension of $\mathcal{M}$-subspaces, called linearity index of** f, $\mathrm{ind}(f)$.

- Important, $\mathcal{M}$-subspaces are invariant under EA-equivalence - meaning that the number of $\mathcal{M}$-subspaces of any fixed dimension is the same! (A. Polujan, PhD thesis)

- **IDEA:** Much easier to construct $f = f_1||f_2||f_3||f_4 \notin \mathcal{M}^{\#}$ when $f_i \in \mathcal{M}^{\#}$ has a **unique $\mathcal{M}$-subspace** of dimension $n/2$.

$\mathcal{M}$-subspaces of Boolean (bent) functions

- Recall, for $f \in \mathfrak{B}_n$ a vector subspace V of $\mathbb{F}_2^n$ is called an $\mathcal{M}$-subspace of f, if $D_aD_bf = 0$, for all $a, b \in V$.

- **The maximum dimension of any $\mathcal{M}$-subspace V is** $n/2$, for any bent function f ($\dim(V) = n/2 \Leftrightarrow f \in \mathcal{M}^\#$).

- Useful to distinguish bent functions $\{f\}$ w.r.t. the **maximal dimension of $\mathcal{M}$-subspaces, called linearity index of** f, $\mathrm{ind}(f)$.

- Important, $\mathcal{M}$-subspaces are invariant under EA-equivalence - meaning that the number of $\mathcal{M}$-subspaces of any fixed dimension is the same! (A. Polujan, PhD thesis)

- **IDEA:** Much easier to construct $f = f_1||f_2||f_3||f_4 \notin \mathcal{M}^\#$ when $f_i \in \mathcal{M}^\#$ has a **unique $\mathcal{M}$-subspace** of dimension $n/2$.

Non-unique $\mathcal{M}$-subspace of maximal dimension

Proposition ([5])

Let π *be a* **permutation** *of* $\mathbb{F}_2^m$ **having a non-zero linear structure** $s \in \mathbb{F}_2^m$, *i.e., for some* $v \in \mathbb{F}_2^m$, *i.e.*

$$D_s\pi(y) = \pi(y) + \pi(y+s) = v, \quad \text{for all } y \in \mathbb{F}_2^m.$$

Then, the bent function $f \in \mathcal{M}$

$$f(x,y) = x \cdot \pi(y) + h(y), \quad x, y \in \mathbb{F}_2^m,$$

has **at least two** m**-dimensional** $\mathcal{M}$**-subspaces**.

P_1 induces uniqueness

Theorem ([5])

Let π be a permutation of $\mathbb{F}_2^m$ which has the following (P_1) property:

$$D_v D_w \pi \neq 0_m \quad \text{for all linearly independent } v, w \in \mathbb{F}_2^m. \qquad (P_1)$$

(thus $\pi(y) + \pi(y+v) + \pi(y+w) + \pi(y+v+w) \neq 0_m$)

Letting $f(x, y) = x \cdot \pi(y) + h(y)$, for all $x, y \in \mathbb{F}_2^m$, then:

1) *Permutation π has no linear structures.*

2) *The vector space $V = \mathbb{F}_2^m \times \{0_m\}$ is the* **unique** *m-dimensional $\mathcal{M}$-subspace of f.*

P_1 induces uniqueness

Theorem ([5])

Let π be a permutation of $\mathbb{F}_2^m$ which has the following (P_1) property:

$$D_v D_w \pi \neq 0_m \quad \text{for all linearly independent } v, w \in \mathbb{F}_2^m. \qquad (P_1)$$

(thus $\pi(y) + \pi(y+v) + \pi(y+w) + \pi(y+v+w) \neq 0_m$)

Letting $f(x,y) = x \cdot \pi(y) + h(y)$, for all $x, y \in \mathbb{F}_2^m$, then:

1) *Permutation π has no linear structures.*

2) *The vector space $V = \mathbb{F}_2^m \times \{0_m\}$ is the **unique** m-dimensional $\mathcal{M}$-subspace of f.*

P_2 characterizes uniqueness

Definition

Let π be a permutation of $\mathbb{F}_2^m$. Let $S \subset \mathbb{F}_2^m$ with $\dim(S) = m - k$, with $1 \leq k \leq m-1$, such that $D_a D_b \pi = 0_m$ for all $a, b \in S$. Then, π satisfies the property (P_2) w.r.t. S if $\nexists V \subset \mathbb{F}_2^m$, with $\dim(V) = k$, such that

$$v \cdot D_a\pi(y) = 0; \text{ for all } a \in S, \text{ all } y \in \mathbb{F}_2^m, \text{ and for all } v \in V. \tag{P_2}$$

If π satisfies this property w.r.t. any linear subspace S of $\mathbb{F}_2^m$ of arbitrary dimension $1 \leq \dim(S) \leq m-1$, then we simply say that π satisfies (P_2).

Proposition ([5])

Let π be a non-affine permutation of $\mathbb{F}_2^m$ and $f(x,y) = x \cdot \pi(y)$ be bent Then, π has (P_2) IFF the only m-dim. $\mathcal{M}$-subspace of f is $\mathbb{F}_2^m \times \{0_m\}$.

P_2 characterizes uniqueness

Definition

Let π be a permutation of $\mathbb{F}_2^m$. Let $S \subset \mathbb{F}_2^m$ with $\dim(S) = m - k$, with $1 \leq k \leq m-1$, such that $D_a D_b \pi = 0_m$ for all $a, b \in S$. Then, π satisfies the property (P_2) w.r.t. S if $\nexists V \subset \mathbb{F}_2^m$, with $\dim(V) = k$, such that

$$v \cdot D_a\pi(y) = 0; \text{ for all } a \in S, \text{ all } y \in \mathbb{F}_2^m, \text{ and for all } v \in V. \qquad (P_2)$$

If π satisfies this property w.r.t. any linear subspace S of $\mathbb{F}_2^m$ of arbitrary dimension $1 \leq \dim(S) \leq m-1$, then we simply say that π satisfies (P_2).

Proposition ([5])

Let π be a non-affine permutation of $\mathbb{F}_2^m$ and $f(x,y) = x \cdot \pi(y)$ be bent Then, π has (P_2) IFF the only m-dim. $\mathcal{M}$-subspace of f is $\mathbb{F}_2^m \times \{0_m\}$.

P_1 and P_2 properties - constructions on larger spaces

Proposition ([5])

Let σ_1 and σ_2 be two permutations of $\mathbb{F}_2^m$ such that $D_u D_v \sigma_1 \neq D_u D_v \sigma_2$ for any distinct elements $u, v \in \mathbb{F}_2^{m*}$. Define $\pi : \mathbb{F}_2^{m+1} \to \mathbb{F}_2^{m+1}$ by

$$\pi(y, y_{m+1}) = (\sigma_1(y) + y_{m+1}(\sigma_1(y) + \sigma_2(y)), y_{m+1}), \forall y \in \mathbb{F}_2^m, y_{m+1} \in \mathbb{F}_2.$$

Then, π is a permutation of $\mathbb{F}_2^{m+1}$ satisfying (P_1).

Theorem ([8])

Let σ_1 and σ_2 be two permutations of $\mathbb{F}_2^m$ and assume that $\sigma_1 + \sigma_2$ satisfies (P_2). Then, π above satisfies (P_2).

Proposition ([8])

Let π be a permutation of $\mathbb{F}_2^m$. If π satisfies (P_1), then it satisfies (P_2).

P_1 and P_2 properties - constructions on larger spaces

Proposition ([5])

Let σ_1 and σ_2 be two permutations of $\mathbb{F}_2^m$ such that $D_uD_v\sigma_1 \neq D_uD_v\sigma_2$ for any distinct elements $u, v \in \mathbb{F}_2^{m*}$. Define $\pi : \mathbb{F}_2^{m+1} \to \mathbb{F}_2^{m+1}$ by

$$\pi(y, y_{m+1}) = (\sigma_1(y) + y_{m+1}(\sigma_1(y) + \sigma_2(y)), y_{m+1}), \forall y \in \mathbb{F}_2^m, y_{m+1} \in \mathbb{F}_2.$$

Then, π is a permutation of $\mathbb{F}_2^{m+1}$ satisfying (P_1).

Theorem ([8])

Let σ_1 and σ_2 be two permutations of $\mathbb{F}_2^m$ and assume that $\sigma_1 + \sigma_2$ satisfies (P_2). Then, π above satisfies (P_2).

Proposition ([8])

Let π be a permutation of $\mathbb{F}_2^m$. If π satisfies (P_1), then it satisfies (P_2).

P_1 and P_2 properties - constructions on larger spaces

Proposition ([5])

Let σ_1 and σ_2 be two permutations of $\mathbb{F}_2^m$ such that $D_u D_v \sigma_1 \neq D_u D_v \sigma_2$ for any distinct elements $u, v \in \mathbb{F}_2^{m*}$. Define $\pi \colon \mathbb{F}_2^{m+1} \to \mathbb{F}_2^{m+1}$ by

$$\pi(y, y_{m+1}) = (\sigma_1(y) + y_{m+1}(\sigma_1(y) + \sigma_2(y)), y_{m+1}), \forall y \in \mathbb{F}_2^m, y_{m+1} \in \mathbb{F}_2.$$

Then, π is a permutation of $\mathbb{F}_2^{m+1}$ satisfying (P_1).

Theorem ([8])

Let σ_1 and σ_2 be two permutations of $\mathbb{F}_2^m$ and assume that $\sigma_1 + \sigma_2$ satisfies (P_2). Then, π above satisfies (P_2).

Proposition ([8])

Let π be a permutation of $\mathbb{F}_2^m$. If π satisfies (P_1), then it satisfies (P_2).

ℓ-optimality - minimal dimension of $\mathcal{M}$-subspaces

Definition

Let $f \in \mathcal{B}_n$ be bent. If $\mathrm{ind}(f) = 1$, we say that f is ℓ-optimal, i.e., $D_a D_b f \neq 0$, for any lin. indep. $a, b \in \mathbb{F}_2^n$.

Theorem ([8])

Let π be a permutation of $\mathbb{F}_2^m$, $m \geq 4$, satisfying (P_1). Define

$$f(x, y) = x \cdot \pi(y) + \delta_0(x), \quad x, y \in \mathbb{F}_2^m.$$

Then, $\mathrm{ind}(f) \leq 2$ (thus $f \notin \mathcal{M}^{\#}$). Furthermore, $\mathrm{ind}(f) = 1$, if and only if π has no components with linear structures (i.e. $u \cdot D_a\pi \neq 0/1$).

Bent revelation - simple reasoning works

- Kept myself asking, **how to get closer to** 2^{106} **?!**, for $n = 8$.
- One lovely morning (or evening) the revelation came:
  - **FACT**: All bent functions in $n = 6$ variables are in the $\mathcal{M}$ class
  - **FACT**: A bent function f in $n + 2 = 8$ variables can be viewed as a concatenation of 4 functions f_i in 6 variables, so that $f = f_1||f_2||f_3||f_4$
  - **FACT -Canteaut-Charpin 2000**: These f_i can be bent, semi-bent ($W_{f_i} \in \{0, \pm 2^{n/2+1}\}$) or 5-valued spectra ($W_{f_i} \in \{0, \pm 2^{n/2}, \pm 2^{n/2+1}\}$)
  - Does it mean that we can concatenate $f_i \in \mathcal{M}$ and get f outside $\mathcal{M}$?
  - YES !!

Bent revelation - simple reasoning works

- Kept myself asking, **how to get closer to 2^{106} ?!**, for $n = 8$.
- One lovely morning (or evening) the revelation came:
  - **FACT**: All bent functions in $n = 6$ variables are in the $\mathcal{M}$ class
  - **FACT**: A bent function f in $n + 2 = 8$ variables can be viewed as a concatenation of 4 functions f_i in 6 variables, so that $f = f_1||f_2||f_3||f_4$
  - **FACT -Canteaut-Charpin 2000**: These f_i can be bent, semi-bent ($W_{f_i} \in \{0, \pm 2^{n/2+1}$) or 5-valued spectra ($W_{f_i} \in \{0, \pm 2^{n/2}, \pm 2^{n/2+1}$)
  - Does it mean that we can concatenate $f_i \in \mathcal{M}$ and get f outside $\mathcal{M}$?
  - YES !!

Bent revelation - simple reasoning works

- Kept myself asking, **how to get closer to** 2^{106} **?!**, for $n = 8$.
- One lovely morning (or evening) the revelation came:
  - **FACT**: All bent functions in $n = 6$ variables are in the $\mathcal{M}$ class
  - **FACT**: A bent function f in $n + 2 = 8$ variables can be viewed as a concatenation of 4 functions f_i in 6 variables, so that $f = f_1||f_2||f_3||f_4$
  - **FACT -Canteaut-Charpin 2000**: These f_i can be bent, semi-bent ($W_{f_i} \in \{0, \pm 2^{n/2+1}$) or 5-valued spectra ($W_{f_i} \in \{0, \pm 2^{n/2}, \pm 2^{n/2+1}$)
  - Does it mean that we can concatenate $f_i \in \mathcal{M}$ and get f outside $\mathcal{M}$?
  - YES !!

4-concatenation

- Let $f = f_1||f_2||f_3||f_4 \in \mathfrak{B}_{n+2}$, whose ANF is given by

  $$f(x, y_1, y_2) = f_1(x)+y_1(f_1+f_3)(x)+y_2(f_1+f_2)(x)+y_1y_2(f_1+f_2+f_3+f_4)(x),$$

  where $x \in \mathbb{F}_2^n$ and $y_1, y_2 \in \mathbb{F}_2$.

- **Subfunctions:** $f_1(x) = f(x, 0, 0)$, $f_2(x) = f(x, 0, 1)$, $f_3(x) = f(x, 1, 0)$ and $f_4(x) = f(x, 1, 1)$.

- **(IMPORTANT)** If f_i are bent then $f = f_1||f_2||f_3||f_4$ is bent **IFF** $f_1^* \oplus f_2^* \oplus f_3^* \oplus f_4^* = 1$ [1], with the dual bent functions f_i^* given as:

  $$f_i^*(a) = \begin{cases} 0 & \text{if } W_{f_i}(a) = +2^{n/2} \\ 1 & \text{if } W_{f_i}(a) = -2^{n/2} \end{cases}$$

- Notation f^a means $f(x + a)$ (used on next 2 slides) !!

4-concatenation

- Let $f = f_1||f_2||f_3||f_4 \in \mathfrak{B}_{n+2}$, whose ANF is given by

  $$f(x, y_1, y_2) = f_1(x)+y_1(f_1+f_3)(x)+y_2(f_1+f_2)(x)+y_1y_2(f_1+f_2+f_3+f_4)(x),$$

  where $x \in \mathbb{F}_2^n$ and $y_1, y_2 \in \mathbb{F}_2$.

- **Subfunctions:** $f_1(x) = f(x, 0, 0)$, $f_2(x) = f(x, 0, 1)$, $f_3(x) = f(x, 1, 0)$ and $f_4(x) = f(x, 1, 1)$.

- **(IMPORTANT)** If f_i are bent then $f = f_1||f_2||f_3||f_4$ is bent **IFF** $f_1^* \oplus f_2^* \oplus f_3^* \oplus f_4^* = 1$ [1], with the dual bent functions f_i^* given as:

  $$f_i^*(a) = \begin{cases} 0 & \text{if } W_{f_i}(a) = +2^{n/2} \\ 1 & \text{if } W_{f_i}(a) = -2^{n/2} \end{cases}$$

- Notation f^a means $f(x + a)$ (used on next 2 slides) !!

$\mathcal{M}$-subspaces of 4-concatenation

Theorem ([7])

Let $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$, where $f_1, \ldots, f_4 \in \mathcal{B}_n$ are arbitrary. Let W **be a** $(k+2)$**-dim. subspace of** $\mathbb{F}_2^{n+2}$, *for $k \in \{0, \ldots, n\}$. Then, W is an $\mathcal{M}$-subspace of f* **IFF** *W has one of the following forms:*

a) $W = V \times \{(0,0)\}$, *where $V \subset \mathbb{F}_2^n$ is a* **common** *$(k+2)$-dimensional $\mathcal{M}$-subspace of $f_1, \ldots, f_4$.*

b) $W = \langle V \times \{(0,0)\}, (a,1,0) \rangle$, *where V is a* **common** *$(k+1)$-dimensional $\mathcal{M}$-subspace of $f_1, \ldots, f_4$, and $a \in \mathbb{F}_2^n$ is such that*

$$D_v f_1 + D_v f_2^a = D_v f_3 + D_v f_4^a = 0, \text{ for all } v \in V.$$

c) $W = \langle V \times \{(0,0)\}, (a,0,1) \rangle$, *where V is a* **common** *$(k+1)$-dimensional $\mathcal{M}$-subspace of $f_1, \ldots, f_4$, and $a \in \mathbb{F}_2^n$ is such that*

$$D_v f_1 + D_v f_3^a = D_v f_2 + D_v f_4^a = 0, \text{ for all } v \in V.$$

$\mathcal{M}$-subspaces of 4-concatenation

Theorem ([7])

Let $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$, where $f_1, \ldots, f_4 \in \mathcal{B}_n$ are arbitrary. Let W **be a** $(k+2)$**-dim. subspace of** $\mathbb{F}_2^{n+2}$, *for $k \in \{0, \ldots, n\}$. Then, W is an $\mathcal{M}$-subspace of f* **IFF** *W has one of the following forms:*

a) $W = V \times \{(0,0)\}$, *where $V \subset \mathbb{F}_2^n$ is a* **common** *$(k+2)$-dimensional $\mathcal{M}$-subspace of $f_1, \ldots, f_4$.*

b) $W = \langle V \times \{(0,0)\}, (a,1,0)\rangle$, *where V is a* **common** *$(k+1)$-dimensional $\mathcal{M}$-subspace of $f_1, \ldots, f_4$, and $a \in \mathbb{F}_2^n$ is such that*

$$D_v f_1 + D_v f_2^a = D_v f_3 + D_v f_4^a = 0, \text{ for all } v \in V.$$

c) $W = \langle V \times \{(0,0)\}, (a,0,1)\rangle$, *where V is a* **common** *$(k+1)$-dimensional $\mathcal{M}$-subspace of $f_1, \ldots, f_4$, and $a \in \mathbb{F}_2^n$ is such that*

$$D_v f_1 + D_v f_3^a = D_v f_2 + D_v f_4^a = 0, \text{ for all } v \in V.$$

Corollary ([7]- bent case)

Let $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$, where $f_1, \ldots, f_4 \in \mathcal{B}_n$ and assume that f is bent. Then, f is outside $\mathcal{M}^{\#}$ if and only if

a) *The functions $f_1, \ldots, f_4$ do not share a common $(n/2+1)$-dim. $\mathcal{M}$-subspace (impossible if f_i are bent);*

b) *There are no common $(n/2)$-dim. $\mathcal{M}$-subspaces $V \subset \mathbb{F}_2^n$ of $f_1, \ldots, f_4$ s. t. $\exists a \in \mathbb{F}_2^n$ for which*

$$D_v f_1 + D_v f_2^a = D_v f_3 + D_v f_4^a = 0, \text{ for all } v \in V, \text{ or}$$
$$D_v f_1 + D_v f_3^a = D_v f_2 + D_v f_4^a = 0, \text{ for all } v \in V, \text{ or}$$
$$D_v f_1 + D_v f_4^a = D_v f_2 + D_v f_3^a = 0, \text{ for all } v \in V.$$

c) *There are no common $(n/2-1)$-dim. $\mathcal{M}$-subspaces $V \subset \mathbb{F}_2^n$ of $f_1, \ldots, f_4$ s. t. $\exists a, b \in \mathbb{F}_2^n$ (including $a = b$), for which*

$$D_v f_1 + D_v f_3^a = D_v f_2 + D_v f_4^a = D_v f_1 + D_v f_2^b = D_v f_3 + D_v f_4^b = 0, \text{ and}$$
$$f_1(x) + f_2(x+b) + f_3(x+a) + f_4(x+a+b) = 0, \text{ for all } x \in \mathbb{F}_2^n.$$

Corollary ([7]- bent case)

Let $f = f_1||f_2||f_3||f_4 \in \mathcal{B}_{n+2}$*, where* $f_1, \ldots, f_4 \in \mathcal{B}_n$ *and assume that* f *is bent. Then,* f *is outside* $\mathcal{M}^{\#}$ *if and only if*

- a) *The functions* $f_1, \ldots, f_4$ *do not share a common* $(n/2+1)$*-dim.* $\mathcal{M}$*-subspace (impossible if* f_i *are bent);*
- b) *There are no common* $(n/2)$*-dim.* $\mathcal{M}$*-subspaces* $V \subset \mathbb{F}_2^n$ *of* $f_1, \ldots, f_4$ *s. t.* $\exists a \in \mathbb{F}_2^n$ *for which*

$$D_v f_1 + D_v f_2^a = D_v f_3 + D_v f_4^a = 0, \text{ for all } v \in V, \text{ or}$$
$$D_v f_1 + D_v f_3^a = D_v f_2 + D_v f_4^a = 0, \text{ for all } v \in V, \text{ or}$$
$$D_v f_1 + D_v f_4^a = D_v f_2 + D_v f_3^a = 0, \text{ for all } v \in V.$$

- c) *There are no common* $(n/2-1)$*-dim.* $\mathcal{M}$*-subspaces* $V \subset \mathbb{F}_2^n$ *of* $f_1, \ldots, f_4$ *s. t.* $\exists a, b \in \mathbb{F}_2^n$ *(including* $a = b$*), for which*

$$D_v f_1 + D_v f_3^a = D_v f_2 + D_v f_4^a = D_v f_1 + D_v f_2^b = D_v f_3 + D_v f_4^b = 0, \text{ and}$$
$$f_1(x) + f_2(x+b) + f_3(x+a) + f_4(x+a+b) = 0, \text{ for all } x \in \mathbb{F}_2^n.$$

Satisfying the conditions

Corollary ([7])

- *Let $h, g \in \mathcal{B}_n$ be* **arbitrary bent** *functions.*
- *Define $f_1 = f_3 = g$ and $f_2 = f_4 + 1 = h$*
- *Then, $f = f_1||f_2||f_3||f_4 = g||h||g||h + 1 \in \mathcal{B}_{n+2}$ (or $g||g||h||h + 1$ if you want) is* **bent** *and $f \in \mathcal{M}^\#$* **IFF** *g and h have a* **common** *$(n/2)$-dim. $\mathcal{M}$-subspace; so $g, h \in \mathcal{M}^\#$.*

- How to avoid sharing an $\mathcal{M}^\#$-subspace of dimension $n/2$?
- E.g. take g or h outside $\mathcal{M}^\#$! **We want** $g, h \in \mathcal{M}^\#$ and $f \notin \mathcal{M}^\#$
- **Solution:** $g(x, y) = x \cdot \pi(y)$ and (swap variables) $h(x, y) = y \cdot \pi(x)$. For instance, if π satisfies (P_1) (or (P_2)) then the unique $\mathcal{M}^\#$-subspace of dim. $n/2$ for g and h are $\mathbb{F}_2^{n/2} \times \{0_{n/2}\}$ and $\{0_{n/2}\} \times \mathbb{F}_2^{n/2}$, respectively !

Corollary ([7])

- *Let $h, g \in \mathcal{B}_n$ be* **arbitrary bent** *functions.*
- *Define $f_1 = f_3 = g$ and $f_2 = f_4 + 1 = h$*
- *Then, $f = f_1||f_2||f_3||f_4 = g||h||g||h + 1 \in \mathcal{B}_{n+2}$ (or $g||g||h||h + 1$ if you want) is* **bent** *and $f \in \mathcal{M}^\#$* **IFF** *g and h have a* **common** *$(n/2)$-dim. $\mathcal{M}$-subspace; so $g, h \in \mathcal{M}^\#$.*

- How to avoid sharing an $\mathcal{M}^\#$-subspace of dimension $n/2$?
- E.g. take g or h outside $\mathcal{M}^\#$! **We want** $g, h \in \mathcal{M}^\#$ and $f \notin \mathcal{M}^\#$
- **Solution:** $g(x, y) = x \cdot \pi(y)$ and (swap variables) $h(x, y) = y \cdot \pi(x)$. For instance, if π satisfies (P_1) (or (P_2)) then the unique $\mathcal{M}^\#$-subspace of dim. $n/2$ for g and h are $\mathbb{F}_2^{n/2} \times \{0_{n/2}\}$ and $\{0_{n/2}\} \times \mathbb{F}_2^{n/2}$, respectively !

Satisfying the conditions

Corollary ([7])

- *Let* $h, g \in \mathcal{B}_n$ *be* **arbitrary bent** *functions.*
- *Define* $f_1 = f_3 = g$ *and* $f_2 = f_4 + 1 = h$
- *Then,* $f = f_1||f_2||f_3||f_4 = g||h||g||h + 1 \in \mathcal{B}_{n+2}$ *(or* $g||g||h||h + 1$ *if you want) is* **bent** *and* $f \in \mathcal{M}^{\#}$ **IFF** g *and* h *have a* **common** $(n/2)$*-dim.* $\mathcal{M}$*-subspace; so* $g, h \in \mathcal{M}^{\#}$*.*

- How to avoid sharing an $\mathcal{M}^{\#}$-subspace of dimension $n/2$?
- E.g. take g or h outside $\mathcal{M}^{\#}$! **We want** $g, h \in \mathcal{M}^{\#}$ and $f \notin \mathcal{M}^{\#}$
- **Solution:** $g(x, y) = x \cdot \pi(y)$ and (swap variables) $h(x, y) = y \cdot \pi(x)$. For instance, if π satisfies (P_1) (or (P_2)) then the unique $\mathcal{M}^{\#}$-subspace of dim. $n/2$ for g and h are $\mathbb{F}_2^{n/2} \times \{0_{n/2}\}$ and $\{0_{n/2}\} \times \mathbb{F}_2^{n/2}$, respectively !

Corollary ([7])

Let $g \in \mathcal{B}_n$ be an **arbitrary bent** *function $n \geq 6$. Then, there exists a bent function $f \in \mathcal{B}_{n+2}$ outside $\mathcal{M}^\#$ such that $g(x) = f(x, 0, 0)$, for all $x \in \mathbb{F}_2^n$.*

Theorem ([7])

For $n \geq 6$, the number of bent functions outside $\mathcal{M}^\#$ in $n + 2$ variables is always strictly greater than the number of all bent functions in n variables.

- Many other results in [2]- [7] and quite large families of bent functions outside $\mathcal{M}^\#$, still not close to 2^{106}.

The $\mathcal{GMM}$ class

Definition

Let $n = 2m$ *be an even positive integer and* $0 \leq k \leq m - 1$. *The set*

$$f(x,y) = x \cdot \phi(y) + h(y), \quad x \in \mathbb{F}_2^{m-k}, y \in \mathbb{F}_2^{m+k},$$

is called the strict $\mathcal{GMM}_{m+k}$ *class, with* $\phi\colon \mathbb{F}_2^{m+k} \to \mathbb{F}_2^{m-k}$ *and* $h \in \mathcal{B}_{\frac{n}{2}+k}$

- For $k = 0$, this class corresponds to $\mathcal{M}$ when ϕ permutes $\mathbb{F}_2^m$.
- For $k = m - 1$, any Boolean function is in $\mathcal{GMM}_{n-1}$!
- Indeed, $x \in \mathbb{F}_2$ and $y \in \mathbb{F}_2^{n-1}$, and for fixed y^* we have $f(x, y^*) = x_1 \cdot \phi(y^*) + h(y^*)$ which can be made 0 or 1 via ϕ and h.

The $\mathcal{GMM}$ class

Definition

Let $n = 2m$ *be an even positive integer and* $0 \leq k \leq m-1$. *The set*

$$f(x,y) = x \cdot \phi(y) + h(y), \;\; x \in \mathbb{F}_2^{m-k}, y \in \mathbb{F}_2^{m+k},$$

is called the strict $\mathcal{GMM}_{m+k}$ *class, with* $\phi \colon \mathbb{F}_2^{m+k} \to \mathbb{F}_2^{m-k}$ *and* $h \in \mathcal{B}_{\frac{n}{2}+k}$

- For $k = 0$, this class corresponds to $\mathcal{M}$ when ϕ permutes $\mathbb{F}_2^m$.
- For $k = m-1$, any Boolean function is in $\mathcal{GMM}_{n-1}$!
- Indeed, $x \in \mathbb{F}_2$ and $y \in \mathbb{F}_2^{n-1}$, and for fixed y^* we have $f(x, y^*) = x_1 \cdot \phi(y^*) + h(y^*)$ which can be made 0 or 1 via ϕ and h.

The $\mathcal{GMM}$ class

Definition

Let $n = 2m$ be an even positive integer and $0 \leq k \leq m-1$. The set

$$f(x,y) = x \cdot \phi(y) + h(y), \;\; x \in \mathbb{F}_2^{m-k}, y \in \mathbb{F}_2^{m+k},$$

is called the strict $\mathcal{GMM}_{m+k}$ class, with $\phi\colon \mathbb{F}_2^{m+k} \to \mathbb{F}_2^{m-k}$ and $h \in \mathcal{B}_{\frac{n}{2}+k}$

- For $k = 0$, this class corresponds to $\mathcal{M}$ when ϕ permutes $\mathbb{F}_2^m$.
- For $k = m-1$, any Boolean function is in $\mathcal{GMM}_{n-1}$!
- Indeed, $x \in \mathbb{F}_2$ and $y \in \mathbb{F}_2^{n-1}$, and for fixed y^* we have $f(x, y^*) = x_1 \cdot \phi(y^*) + h(y^*)$ which can be made 0 or 1 via ϕ and h.

The $\mathcal{GMM}_{m+1}$ class

Theorem (X- [2])

Let $n = 2m$ and let $f \in \mathcal{GMM}_{m+1}$ (thus $k = 1$) so that

$$f(x, y) = x \cdot \phi(y) + h(y), \quad x \in \mathbb{F}_2^{m-1}, y \in \mathbb{F}_2^{m+1}, \tag{1}$$

where $\phi \colon \mathbb{F}_2^{m+1} \to \mathbb{F}_2^{m-1}$ and $h \colon \mathbb{F}_2^{m+1} \to \mathbb{F}_2$. Then, f is bent IFF

- *the collection $\{\phi^{-1}(a) \mid a \in \mathbb{F}_2^{m-1}\}$ is a partition of $\mathbb{F}_2^{m+1}$ into 2-***dim. affine subspaces** *(where $\phi^{-1}(a) = \{y \in \mathbb{F}_2^{m+1} \mid \phi(y) = a\}$), and*
- *for every $a \in \mathbb{F}_2^{m-1}$, the restriction of h on $\phi^{-1}(a)$ has odd weight.*

The $\mathcal{GMM}_{m+1}$ class

Theorem (X- [2])

Let $n = 2m$ and let $f \in \mathcal{GMM}_{m+1}$ (thus $k = 1$) so that

$$f(x, y) = x \cdot \phi(y) + h(y), \quad x \in \mathbb{F}_2^{m-1}, y \in \mathbb{F}_2^{m+1}, \tag{1}$$

where $\phi \colon \mathbb{F}_2^{m+1} \to \mathbb{F}_2^{m-1}$ and $h \colon \mathbb{F}_2^{m+1} \to \mathbb{F}_2$. Then, f is bent IFF

- *the collection $\{\phi^{-1}(a) \mid a \in \mathbb{F}_2^{m-1}\}$ is a partition of $\mathbb{F}_2^{m+1}$ into 2-***dim. affine subspaces** *(where $\phi^{-1}(a) = \{y \in \mathbb{F}_2^{m+1} \mid \phi(y) = a\}$), and*
- *for every $a \in \mathbb{F}_2^{m-1}$, the restriction of h on $\phi^{-1}(a)$ has odd weight.*

The $\mathcal{GMM}_{m+1}$ class

Corollary ([2])

Let f be a bent function defined by Eq. (1). Then, the Hamming weight of h satisfies $2^{m-1} \leq \mathrm{wt}(h) \leq 3 \cdot 2^{m-1}$.

Corollary ([2])

Let $\phi\colon \mathbb{F}_2^{m+1} \to \mathbb{F}_2^{m-1}$ be a 4-to-1 mapping s. t. $\{\phi^{-1}(a) \mid a \in \mathbb{F}_2^{m-1}\}$ is a partition of $\mathbb{F}_2^{m+1}$ into 2-dim. flats. Then, **there are exactly** $2^{3 \cdot 2^{m-1}}$ **functions** *$h\colon \mathbb{F}_2^{m+1} \to \mathbb{F}_2$ s.t. f defined by*

$$f(x,y) = x \cdot \phi(y) + h(y), \;\; x \in \mathbb{F}_2^{m-1}, y \in \mathbb{F}_2^{m+1},$$

is bent.

A counterintuitive result

Before, we were interested in going outside $\mathcal{M}^{\#}$ using $f_1, \ldots, f_4 \in \mathcal{M}^{\#}$. However, we can end up in $\mathcal{M}^{\#}$ using $f_i \notin \mathcal{M}^{\#}$!

Corollary ([2])

For every even $n \geq 8$, there exist bent functions on $\mathbb{F}_2^{n+2}$ that belong to $\mathcal{M}^{\#}$, whose restrictions to $\mathbb{F}_2^n \times \{(0,0)\}$ are bent functions outside $\mathcal{M}^{\#}$.

Bent functions in $\mathcal{GMM}_{m+1}$ that belong to $\mathcal{M}^{\#}$

Proposition ([2])

Let $n = 2m$ and let $f \in \mathcal{B}_n$ be a bent function in $\mathcal{GMM}_{m+1}$, thus satisfying Theorem X, defined by

$$f(x, y) = x \cdot \phi(y) + h(y), \quad x \in \mathbb{F}_2^{m-1}, y \in \mathbb{F}_2^{m+1}.$$

Assume there is $v \in \mathbb{F}_2^{m+1*}$, such that, for all $z \in \mathbb{F}_2^{m-1}$, we have

$$v \in w_z + \phi^{-1}(z), \text{ for some } w_z \in \phi^{-1}(z).$$

Then, f is in $\mathcal{M}^{\#}$.

- For instance, splitting $\mathbb{F}_2^{m+1} = \cup_{i=1}^{2^{m-1}} (w_i + A)$ is not good as $f \in \mathcal{M}^{\#}$.

Proper partitions

- A proper partitioning of $\mathbb{F}_2^{m+1}$ is needed!

- However, even a **simple algorithm given below works**:

1. Select $A_1 = \{0_{m+1}, a_0, b_0, a_0 + b_0\}$, a linear subspace of $\mathbb{F}_2^{m+1}$.
2. Select $a_1, b_1, c_1 \in \mathbb{F}_2^n \setminus A_1$; define

$$A_2 = a_1 + \{0_{m+1}, b_1 + a_1, c_1 + a_1, b_1 + c_1\}$$

   which is an affine 2-dim. subspace of $\mathbb{F}_2^{m+1}$.
3. Continue with selecting a_i, b_i, c_i from $\mathbb{F}_2^{m+1} \setminus \cup_{j=1}^{i} A_j$ and defining $A_{i+1} = \{a_i, b_i, c_i, a_i + b_i + c_i\}$

- For $n = 2m = 8$, we found 4 960 different decompositions of $\mathbb{F}_2^5$ out of which 3 785 were "proper". These **proper** partitions (up to permutations of 2-dim. blocks) along with different h resulted in $\mathbf{2^{79}}$ different bent functions outside $\mathcal{M}^\#$ (larger than $\#\mathcal{M}^\# \cup \mathcal{PS}^\#$) !

Proper partitions

- A proper partitioning of $\mathbb{F}_2^{m+1}$ is needed!

- However, even a **simple algorithm given below works**:

1. Select $A_1 = \{0_{m+1}, a_0, b_0, a_0 + b_0\}$, a linear subspace of $\mathbb{F}_2^{m+1}$.
2. Select $a_1, b_1, c_1 \in \mathbb{F}_2^n \setminus A_1$; define
$$A_2 = a_1 + \{0_{m+1}, b_1 + a_1, c_1 + a_1, b_1 + c_1\}$$
which is an affine 2-dim. subspace of $\mathbb{F}_2^{m+1}$.
3. Continue with selecting a_i, b_i, c_i from $\mathbb{F}_2^{m+1} \setminus \cup_{j=1}^{i} A_j$ and defining $A_{i+1} = \{a_i, b_i, c_i, a_i + b_i + c_i\}$

- For $n = 2m = 8$, we found 4 960 different decompositions of $\mathbb{F}_2^5$ out of which 3 785 were "proper". These **proper** partitions (up to permutations of 2-dim. blocks) along with different h resulted in $\mathbf{2^{79}}$ different bent functions outside $\mathcal{M}^\#$ (larger than $\#\mathcal{M}^\# \cup \mathcal{PS}^\#$) !

Concluding remarks

- Currently, we are investigating $\mathcal{GMM}_{m+2}$, more difficult when ϕ is a 16-to-1 mapping (a proper partition ????).
- Notice that $\mathcal{GMM}_{m+k_1} \subset \mathcal{GMM}_{m+k_2}$ if $k_1 < k_2$, therefore we need to find bent functions in $\mathcal{GMM}_{m+2}$ that are not in $\mathcal{GMM}_{m+1}$.
- Finally, more clarity is required about:
  - How do we distinguish classes of difference sets corresponding to e.g. 2^{106} bent functions for $n = 8$?
  - Even more important is the question about vectorial bent functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^r$ (with $r \leq n/2$) and their classification (partial difference sets).

Concluding remarks

- Currently, we are investigating $\mathcal{GMM}_{m+2}$, more difficult when ϕ is a 16-to-1 mapping (a proper partition ????).

- Notice that $\mathcal{GMM}_{m+k_1} \subset \mathcal{GMM}_{m+k_2}$ if $k_1 < k_2$, therefore we need to find bent functions in $\mathcal{GMM}_{m+2}$ that are not in $\mathcal{GMM}_{m+1}$.

- Finally, more clarity is required about:
  - How do we distinguish classes of difference sets corresponding to e.g. 2^{106} bent functions for $n = 8$?

  - Even more important is the question about vectorial bent functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^r$ (with $r \leq n/2$) and their classification (partial difference sets).

- S. Hodzic, E. Pasalic, Y. Wei. A general framework for secondary constructions of bent and plateaued functions. *Des. Codes Cryptogr.* vol. 88(10): 2007–2035 (2020)
- S. Kudin, E. Pasalic, A. Polujan, F. Zhang and H. Zhao. Almost Maiorana-McFarland bent functions. url=https://arxiv.org/abs/2508.14265, 2025
- S. Kudin, E. Pasalic. A complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^{\#}$ and a general framework for specifying bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$. *Des. Codes Cryptogr.*, vol. 90(8), pp. 1783–1796, (2022).
- S. Kudin, E. Pasalic, N. Cepak, F. Zhang. Permutations without linear structures inducing bent functions outside the completed Maiorana-McFarland class. *Cryptogr. Commun.*, vol. 14(1), pp. 101–116, (2022).
- E. Pasalic, A. Polujan, S. Kudin, and F. Zhang. Design and analysis of bent functions using $\mathcal{M}$-subspaces. *IEEE Trans. Inf. Theory*, vol. 70(6), pp. 4464–4477, 2024.
- A. Polujan, E. Pasalic, S. Kudin, and F. Zhang. Bent functions satisfying the dual bent condition and permutations with the $(\mathcal{A}_m)$ property. *Cryptogr. Commun.*, vol. 16, pp. 1235–1256, 2024.
- S. Kudin, E. Pasalic, A. Polujan, and F. Zhang. The algebraic characterization of $\mathcal{M}$-subspaces of bent concatenations and its application. *IEEE Trans. Inf. Theory*, vol. 71, no. 5, pp. 3999–4011, May 2025.
- S. Kudin, E. Pasalic, A. Polujan, and F. Zhang. Permutations satisfying (P_1) and (P_2) properties and ℓ-optimal bent functions. *submitted*, 2025.