Some Classification Results on Maiorana-McFarland Bent Functions

Philippe Langevin[1] and Alexandr Polujan[2]

philippe.langevin@univ-tln.fr alexandr.polujan@gmail.com

[1] Imath, Université de Toulon, La Garde, France

[2] Otto von Guericke University Magdeburg, Germany

BFA 2024
The 9th International Workshop on
Boolean Functions and their Applications,
09.09.2024

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
- Algebraic Normal Form (ANF) of $f \in \mathcal{B}_n$

$$f(z_1, \ldots, z_n) = \sum_{v \in \mathbb{F}_2^n} c_v \left(\prod_{i=1}^{n} z_i^{v_i} \right),$$

  where $c_v \in \mathbb{F}_2$ and $v = (z_1, \ldots, z_n) \in \mathbb{F}_2^n$
- Algebraic degree $\deg(f)$ is the degree of the ANF of $f \in \mathcal{B}_n$
- Walsh-Hadamard transform of $f \in \mathcal{B}_n$ at $u \in \mathbb{F}_2^n$ is defined by

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

Boolean Bent Functions

Definition

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

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

Example

We identify $\mathbb{F}_2^n$ with $\mathbb{F}_2^m \times \mathbb{F}_2^m$. For $x, y \in \mathbb{F}_2^m$, the dot product

$$f(x, y) = \langle x, y \rangle = \sum_{i=1}^{m} x_i y_i$$

defines a quadratic bent function f on $\mathbb{F}_2^m \times \mathbb{F}_2^m$

Maiorana-McFarland Bent Functions

Definition

The Maiorana-McFarland class is the set of Boolean bent functions on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ of the form

$$\mathcal{M} = \{\ f_{\pi,g}(x,y) = \langle x, \pi(y) \rangle + g(y)\ :\ \pi \text{ permutes } \mathbb{F}_2^m,\ g \in \mathcal{B}_m\ \}$$

Facts

- $\mathcal{M}$ is a fundamental primary class of bent functions (along with the partial spread class $\mathcal{PS}$)
- $\mathcal{M}$ contains many functions on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ of all possible degrees d with $2 \leq d \leq m$

Equivalence of Boolean Functions

- Let $S\left(\mathbb{F}_2^n\right)$ be the group of all permutations of $\mathbb{F}_2^n$
- The general affine group

$$\mathrm{AGL}(n,2)=\left\{\begin{bmatrix} A & b \\ & 1 \end{bmatrix} : A \in \mathrm{GL}(n,2), b \in \mathbb{F}_2^n\right\}$$

- The action of $\mathrm{AGL}(n,2)$ on $\mathbb{F}_2^n$ is given by

$$\begin{bmatrix} A & b \\ & 1 \end{bmatrix}(x) = Ax+b \quad \text{for } x \in \mathbb{F}_2^n$$

Definition (EA-Equivalence)

Functions $f, f' \in \mathcal{B}_n$ are equivalent if $f'(x) = f(A(x)) + a(x)$ holds for all $x \in \mathbb{F}_2^n$, where $A \in \mathrm{AGL}(n,2)$ and $a \in \mathcal{B}_n$ is affine

Classification of Maiorana-McFarland Bent Functions

- Let $f_{\pi,g}(x,y) := \langle x, \pi(y) \rangle + g(y)$ be a Maiorana-McFarland bent function on $\mathcal{B}_{2m}$

Essential Question

How to select permutations $\pi, \pi' \in S(\mathbb{F}_2^m)$ and Boolean functions $g, g' \in \mathcal{B}_m$, s.t. $f_{\pi,g}$ and $f_{\pi',g'}$ are (in)equivalent?

Strategy: Use "Controllable" Invariants

1. Algebraic degree
2. # of $\mathcal{M}$-subspaces of a fixed dimension[1,2] (a vector space $U \subseteq \mathbb{F}_2^n$ is called an $\mathcal{M}$-subspace of $f \in \mathcal{B}_n$ if $D_{a,b}f = 0$, for all $a, b \in U$)

[1] Alexandr Polujan and Alexander Pott. "Cubic bent functions outside the completed Maiorana-McFarland class". In: *Designs, Codes and Cryptography* 88.9 (2020), pp. 1701–1722.

[2] Enes Pasalic, Alexandr Polujan, Sadmir Kudin and Fengrong Zhang. "Design and Analysis of Bent Functions Using $\mathcal{M}$-Subspaces". In: *IEEE Transactions on Information Theory* 70.6 (2024), pp. 4464–4477.

The Known Classification Results

- $n = 2, 4$: 1 quadratic class

[3] John F. Dillon. "A survey of bent functions". In: *NSA Technical Journal* Special Issue (1972), pp. 191–215.

[4] An Braeken. "Cryptographic Properties of Boolean Functions and S-Boxes". PhD thesis. Katholieke Universiteit Leuven, Mar. 2006.

[5] Philippe Langevin. *Classification of Bent Cubics in 8 variables*.

[6] Philippe Langevin and Xiang-Dong Hou. "Counting Partial Spread Functions in Eight Variables". In: *IEEE Transactions on Information Theory* 57 (2011), pp. 2263–2269.

[7] Philippe Langevin and Gregor Leander. "Classification of Boolean Quartic Forms in eight variables". In: *Boolean Functions in Cryptology and Information Security*. Vol. 18. 2008, pp. 139–147.

The Known Classification Results

- $n = 2, 4$: 1 quadratic class
- $n = 6$: 4 classes = 1 quadratic + 3 cubic[3]

[3] John F. Dillon. "A survey of bent functions". In: *NSA Technical Journal* Special Issue (1972), pp. 191–215.

[4] An Braeken. "Cryptographic Properties of Boolean Functions and S-Boxes". PhD thesis. Katholieke Universiteit Leuven, Mar. 2006.

[5] Philippe Langevin. *Classification of Bent Cubics in 8 variables*.

[6] Philippe Langevin and Xiang-Dong Hou. "Counting Partial Spread Functions in Eight Variables". In: *IEEE Transactions on Information Theory* 57 (2011), pp. 2263–2269.

[7] Philippe Langevin and Gregor Leander. "Classification of Boolean Quartic Forms in eight variables". In: *Boolean Functions in Cryptology and Information Security*. Vol. 18. 2008, pp. 139–147.

The Known Classification Results

- $n = 2, 4$: 1 quadratic class
- $n = 6$: 4 classes $=$ 1 quadratic $+$ 3 cubic[3]
- $n = 8$: 1 quadratic $+$ 8 cubic[4,5] $+ X$ quartic (looks doable)

[3] John F. Dillon. "A survey of bent functions". In: *NSA Technical Journal* Special Issue (1972), pp. 191–215.

[4] An Braeken. "Cryptographic Properties of Boolean Functions and S-Boxes". PhD thesis. Katholieke Universiteit Leuven, Mar. 2006.

[5] Philippe Langevin. *Classification of Bent Cubics in 8 variables*.

[6] Philippe Langevin and Xiang-Dong Hou. "Counting Partial Spread Functions in Eight Variables". In: *IEEE Transactions on Information Theory* 57 (2011), pp. 2263–2269.

[7] Philippe Langevin and Gregor Leander. "Classification of Boolean Quartic Forms in eight variables". In: *Boolean Functions in Cryptology and Information Security*. Vol. 18. 2008, pp. 139–147.

The Known Classification Results

- $n = 2, 4$: 1 quadratic class
- $n = 6$: 4 classes = 1 quadratic + 3 cubic[3]
- $n = 8$: 1 quadratic + 8 cubic[4,5] + X quartic (looks doable)
  1. "Structurally more complicated" partial spread bent functions are classified and enumerated[6] in dimension 8
  2. The number of bent functions in dimension 8 equivalent to $\mathcal{M}$ up to addition of affine terms[7] is $\leq 2^{72,38}$

[3] John F. Dillon. "A survey of bent functions". In: *NSA Technical Journal* Special Issue (1972), pp. 191–215.

[4] An Braeken. "Cryptographic Properties of Boolean Functions and S-Boxes". PhD thesis. Katholieke Universiteit Leuven, Mar. 2006.

[5] Philippe Langevin. *Classification of Bent Cubics in 8 variables*.

[6] Philippe Langevin and Xiang-Dong Hou. "Counting Partial Spread Functions in Eight Variables". In: *IEEE Transactions on Information Theory* 57 (2011), pp. 2263–2269.

[7] Philippe Langevin and Gregor Leander. "Classification of Boolean Quartic Forms in eight variables". In: *Boolean Functions in Cryptology and Information Security*. Vol. 18. 2008, pp. 139–147.

Open Problem

Classify and enumerate all bent functions from $\mathcal{M}$ in dimension 8.

Problem and Main Results

Open Problem

Classify and enumerate all bent functions from $\mathcal{M}$ in dimension 8.

Main Result 1 (Langevin and Polujan 2024)

Let $\mathcal{CM}(2m, 2)$ denote the # of equivalence classes of Maiorana-McFarland bent functions on $\mathbb{F}_2^m \times \mathbb{F}_2^m$. Then, $\mathcal{CM}(8, 2) = 325$.

Problem and Main Results

Open Problem

Classify and enumerate all bent functions from $\mathcal{M}$ in dimension 8.

Main Result 1 (Langevin and Polujan 2024)

Let $\mathcal{CM}(2m, 2)$ denote the # of equivalence classes of Maiorana-McFarland bent functions on $\mathbb{F}_2^m \times \mathbb{F}_2^m$. Then, $\mathcal{CM}(8, 2) = 325$.

Main Result 2 (Langevin and Polujan 2024)

The number of bent functions on $\mathbb{F}_2^8$ that are equivalent to the $\mathcal{M}$ class (up to addition of affine terms) is equal to

$$537\,611\,571\,837\,677\,338\,624 \approx 2^{68{,}86}.$$

Methodology

$$\mathcal{M} = \{ \ f_{\pi,g}(x,y) = \langle x, \pi(y) \rangle + g(y) \ : \ \pi \in \mathcal{S}(\mathbb{F}_2^m), \ g \in \mathcal{B}_m \ \}$$

- Brute force works for $n \le 6$, but not for $n = 2m = 8$

$$\frac{(2^m)!}{2^m} \cdot \frac{2^{2^m}}{2^{m+1}} \overset{m=4}{=} 2\,678\,117\,105\,664\,000 \approx 2^{51}$$

Methodology

$$\mathcal{M} = \{\ f_{\pi,g}(x,y) = \langle x, \pi(y)\rangle + g(y)\ :\ \pi \in \mathcal{S}(\mathbb{F}_2^m),\ g \in \mathcal{B}_m\ \}$$

- Brute force works for $n \leq 6$, but not for $n = 2m = 8$

$$\frac{(2^m)!}{2^m} \cdot \frac{2^{2^m}}{2^{m+1}} \overset{m=4}{=} 2\,678\,117\,105\,664\,000 \approx 2^{51}$$

Main Steps

I. Complexity reduction

II. Classification
   - Preclassification (to avoid the need for invariants)
   - Refinement (classify preclasses)

III. Invariants (sanity check)

Step I: Complexity Reduction — The Main Idea

- Let $\pi \in S(\mathbb{F}_2^m)$ and $g \in \mathcal{B}_m$ be arbitrary

Step I: Complexity Reduction — The Main Idea

- Let $\pi \in S(\mathbb{F}_2^m)$ and $g \in \mathcal{B}_m$ be arbitrary

1. The action of (A, R) with $A \in GL(m, 2)$ and $R \in \mathrm{AGL}(m, 2)$ on $f_{\pi,g} \in \mathcal{B}_{2m}$ is given by

$$\begin{aligned} f_{\pi,g}(x, y) \circ (A, R) =& \langle A(x), \pi(R(y)) \rangle + g(R(y)) \\ =& \langle x, A^* \circ \pi \circ R(y) \rangle + g(R(y)), \end{aligned}$$

where A^* is the adjoint of A

Step I: Complexity Reduction — The Main Idea

- Let $\pi \in S(\mathbb{F}_2^m)$ and $g \in \mathcal{B}_m$ be arbitrary

1. The action of (A, R) with $A \in GL(m, 2)$ and $R \in \mathrm{AGL}(m, 2)$ on $f_{\pi,g} \in \mathcal{B}_{2m}$ is given by

$$\begin{aligned} f_{\pi,g}(x,y) \circ (A,R) =& \langle A(x), \pi(R(y)) \rangle + g(R(y)) \\ =& \langle x, A^* \circ \pi \circ R(y) \rangle + g(R(y)), \end{aligned}$$

where A^* is the adjoint of A

2. Addition of $\langle x, v \rangle$ to $f_{\pi,g}(x,y)$ does not change equivalence class:

$$f_{\pi,g}(x,y) \equiv \langle x, L \circ \pi \circ R(y) \rangle + g \circ R(y) = f_{\pi',g'}(x,y),$$

where $\pi' := L \circ \pi \circ R$, $g' := g \circ R$, L is the composition of A^* by the translation $x \mapsto x + v$, for $v \in \mathbb{F}_2^m$

$$f_{\pi,g}(x,y) \equiv \langle x, \underbrace{L \circ \pi \circ R}_{\pi'}(y)\rangle + \underbrace{g \circ R}_{g'}(y) = f_{\pi',g'}(x,y)$$

$\Rightarrow$ $L \circ \pi \circ R$ is the action of $(L,R) \in \mathrm{AGL}(m,2)^2$ on $\pi \in S\left(\mathbb{F}_2^m\right)$

$\Rightarrow$ Orbits are $(\mathrm{AGL}(m,2), \mathrm{AGL}(m,2))$-double cosets in $S\left(\mathbb{F}_2^m\right)$

Step I: Complexity Reduction — Double Cosets in $S\left(\mathbb{F}_2^m\right)$

$$f_{\pi,g}(x,y) \equiv \langle x, \underbrace{L \circ \pi \circ R}_{\pi'}(y)\rangle + \underbrace{g \circ R}_{g'}(y) = f_{\pi',g'}(x,y)$$

$\Rightarrow$ $L \circ \pi \circ R$ is the action of $(L,R) \in \mathrm{AGL}(m,2)^2$ on $\pi \in S\left(\mathbb{F}_2^m\right)$

$\Rightarrow$ Orbits are $(\mathrm{AGL}(m,2), \mathrm{AGL}(m,2))$-double cosets in $S\left(\mathbb{F}_2^m\right)$

Conclusion

1. π' runs through the representatives double cosets in $S\left(\mathbb{F}_2^m\right)$
2. g' runs through the orbit determined by the action of $\mathrm{stab}(\pi')$ on the set of Boolean functions $\mathcal{B}_m$ without affine terms $B(2,m,m)$

Step I: Complexity Reduction — Double Cosets in $S(\mathbb{F}_2^m)$

$$f_{\pi,g}(x,y) \equiv \langle x, \underbrace{L \circ \pi \circ R}_{\pi'}(y)\rangle + \underbrace{g \circ R}_{g'}(y) = f_{\pi',g'}(x,y)$$

$\Rightarrow$ $L \circ \pi \circ R$ is the action of $(L,R) \in \mathrm{AGL}(m,2)^2$ on $\pi \in S(\mathbb{F}_2^m)$

$\Rightarrow$ Orbits are $(\mathrm{AGL}(m,2), \mathrm{AGL}(m,2))$-double cosets in $S(\mathbb{F}_2^m)$

Conclusion

1. π' runs through the representatives double cosets in $S(\mathbb{F}_2^m)$
2. g' runs through the orbit determined by the action of $\mathrm{stab}(\pi')$ on the set of Boolean functions $\mathcal{B}_m$ without affine terms $B(2,m,m)$

- Classification of permutations of $\mathbb{F}_2^m$ is a well-studied topic, especially for $m = 4$!

- The *number of* $(\mathrm{AGL}(m,2), \mathrm{AGL}(m,2))$*-double cosets in* $S(\mathbb{F}_2^m)$ is denoted by $\mathfrak{N}(m,2)$
- For $m=4$, it is well-known[8] that $\mathfrak{N}(4,2)=302$
- All 302 representatives π_i are known[9]

[8] Xiang-Dong Hou. "Affinity of permutations of $\mathbb{F}_2^n$". In: *Discrete Applied Mathematics* 154.2 (2006), pp. 313–325.

[9] Christophe De Cannière. "Analysis And Design of Symmetric Encryption Algorithms". PhD thesis. Katholieke Universiteit Leuven, May 2007.

Step I: Complexity Reduction — The Result

- The *number of* $(\mathrm{AGL}(m,2),\mathrm{AGL}(m,2))$*-double cosets in* $S(\mathbb{F}_2^m)$ is denoted by $\mathfrak{N}(m,2)$
- For $m=4$, it is well-known[8] that $\mathfrak{N}(4,2)=302$
- All 302 representatives π_i are known[9]
- Computing the action of $\mathrm{stab}(\pi_i)$ on the space $B(2,2,4)$, we get

$$\frac{(2^m)!}{2^m}\cdot\frac{2^{2^m}}{2^{m+1}} \quad\longrightarrow\quad \sum_{i=1}^{\mathfrak{N}(m,2)} |O(\mathrm{stab}(\pi_i),B(2,m,m))|$$

$$2\,678\,117\,105\,664\,000\approx 2^{51} \quad\xrightarrow{m=4}\quad 417\,914\approx 2^{18}$$

[8] Xiang-Dong Hou. "Affinity of permutations of $\mathbb{F}_2^n$". In: *Discrete Applied Mathematics* 154.2 (2006), pp. 313–325.

[9] Christophe De Cannière. "Analysis And Design of Symmetric Encryption Algorithms". PhD thesis. Katholieke Universiteit Leuven, May 2007.

Step II: Classification — Intuition

- We have a set S containing $417\,914$ bent functions in $\mathcal{M}$
- How to write $S = S_1 \sqcup \cdots \sqcup S_k$ s.t. classification in each S_i is easy?
- Use the observations from the $n = 2m = 6$ case

Step II: Classification — Intuition

- We have a set S containing $417\,914$ bent functions in $\mathcal{M}$
- How to write $S = S_1 \sqcup \cdots \sqcup S_k$ s.t. classification in each S_i is easy?
- Use the observations from the $n = 2m = 6$ case

1. There are $\mathfrak{N}(3, 2) = 4$ equivalence classes of bent functions
2. A possible system of representatives is given by the functions

$$f_{\pi_i,0}(x, y) = \langle x, \pi_i(y) \rangle,$$

   $\pi_i \in \mathcal{S}\left(\mathbb{F}_2^3\right)$ runs through the representatives of the double cosets

3. The functions $f_{\pi_i,g}$ and $f_{\pi_j,g'}$ might be equivalent

Step II: Classification — Intuition

- We have a set S containing $417\,914$ bent functions in $\mathcal{M}$
- How to write $S = S_1 \sqcup \cdots \sqcup S_k$ s.t. classification in each S_i is easy?
- Use the observations from the $n = 2m = 6$ case

  1. There are $\mathfrak{N}(3,2) = 4$ equivalence classes of bent functions
  2. A possible system of representatives is given by the functions

     $$f_{\pi_i,0}(x,y) = \langle x, \pi_i(y) \rangle,$$

     $\pi_i \in \mathcal{S}\left(\mathbb{F}_2^3\right)$ runs through the representatives of the double cosets
  3. The functions $f_{\pi_i,g}$ and $f_{\pi_j,g'}$ might be equivalent

$\Rightarrow$ $S_i = \{ f_{\pi_i,g} \colon g \in O(\mathrm{stab}(\pi_i), B(2,4,4)) \}$, for $1 \le i \le 302$

Step II: Classification — Results

Preclassification

1. Classify with Magma each set S_i with $1 \leq i \leq 302$
2. With this approach, we get 335 “preclasses”

Step II: Classification — Results

Preclassification

1. Classify with Magma each set S_i with $1 \leq i \leq 302$
2. With this approach, we get 335 “preclasses”

Refinment

Classify the “preclasses”. We get 325 equivalence classes

Step II: Classification — Results

Preclassification

1. Classify with Magma each set S_i with $1 \leq i \leq 302$
2. With this approach, we get 335 “preclasses”

Refinment

Classify the “preclasses”. We get 325 equivalence classes

Main Tool

Functions $f, f' \in \mathcal{B}_n$ are equivalent iff the codes $\mathcal{C}_f$ and $\mathcal{C}_{f'}$ (defined by generator matrices $\mathbf{G}_f$ and $\mathbf{G}_{f'}$) are equivalent

$$\mathbf{G}_f = \begin{array}{cl} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ x_1 & x_2 & x_3 & \cdots & x_{2^n} \\ f(x_1) & f(x_2) & f(x_3) & \cdots & f(x_{2^n}) \end{pmatrix} & \begin{array}{l} 1 \text{ row} \\ n \text{ rows} \\ 1 \text{ row} \end{array} \end{array}$$

Step III: Invariants

- Find a set of invariants that uniquely labels each equivalence class
- In this case, we need 3 "neighborhood invariants" to distinguish all 325 classes

[10] Alexandr Polujan and Alexander Pott. "Towards the classification of quadratic vectorial bent functions in 8 variables". In: *The 7th international workshop on Boolean functions and their applications*. 2022.

[11] Philippe Langevin and Gregor Leander. "Classification of Boolean Quartic Forms in eight variables". In: *Boolean Functions in Cryptology and Information Security*. Vol. 18. 2008, pp. 139–147.

Step III: Invariants

- Find a set of invariants that uniquely labels each equivalence class
- In this case, we need 3 "neighborhood invariants" to distinguish all 325 classes

1. $J_k(f) = \{ *WS(f+g)\colon \deg(g) = 2 \text{ of rank } k * \}$
   a is generalization[10] of the invariant $\Theta(f)$ (takes 313 values)

[10] Alexandr Polujan and Alexander Pott. "Towards the classification of quadratic vectorial bent functions in 8 variables". In: *The 7th international workshop on Boolean functions and their applications*. 2022.

[11] Philippe Langevin and Gregor Leander. "Classification of Boolean Quartic Forms in eight variables". In: *Boolean Functions in Cryptology and Information Security*. Vol. 18. 2008, pp. 139–147.

Step III: Invariants

- Find a set of invariants that uniquely labels each equivalence class
- In this case, we need 3 "neighborhood invariants" to distinguish all 325 classes

1. $J_k(f) = \{*WS(f+g)\colon \deg(g) = 2$ of rank $k*\}$
   a is generalization[10] of the invariant $\Theta(f)$ (takes 313 values)
2. $M(f)$ is a multiplicative version of J_2
3. $K(f)$ is the dimension of the kernel of the map[11] from $RM(2,8)$ into $B(4,6,8)$ that maps $g \mapsto gf \mod RM(3,8)$

[10] Alexandr Polujan and Alexander Pott. "Towards the classification of quadratic vectorial bent functions in 8 variables". In: *The 7th international workshop on Boolean functions and their applications*. 2022.

[11] Philippe Langevin and Gregor Leander. "Classification of Boolean Quartic Forms in eight variables". In: *Boolean Functions in Cryptology and Information Security*. Vol. 18. 2008, pp. 139–147.

Main Results

Main Result 1 (Langevin and Polujan 2024)

Let $\mathcal{CM}(2m,2)$ denote the $\#$ of equivalence classes of Maiorana-McFarland bent functions on $\mathbb{F}_2^m \times \mathbb{F}_2^m$. Then, $\mathcal{CM}(8,2) = 325$.

Main Results

Main Result 1 (Langevin and Polujan 2024)

Let $\mathcal{CM}(2m,2)$ denote the # of equivalence classes of Maiorana-McFarland bent functions on $\mathbb{F}_2^m \times \mathbb{F}_2^m$. Then, $\mathcal{CM}(8,2) = 325$.

Main Result 2 (Langevin and Polujan 2024)

The number of bent functions on $\mathbb{F}_2^8$ that are equivalent to the $\mathcal{M}$ class (up to addition of affine terms) is equal to

$$537\,611\,571\,837\,677\,338\,624 \approx 2^{68,86}.$$

Main Results

Main Result 1 (Langevin and Polujan 2024)

Let $\mathcal{CM}(2m, 2)$ denote the # of equivalence classes of Maiorana-McFarland bent functions on $\mathbb{F}_2^m \times \mathbb{F}_2^m$. Then, $\mathcal{CM}(8, 2) = 325$.

Main Result 2 (Langevin and Polujan 2024)

The number of bent functions on $\mathbb{F}_2^8$ that are equivalent to the $\mathcal{M}$ class (up to addition of affine terms) is equal to

$$537\,611\,571\,837\,677\,338\,624 \approx 2^{68,86}.$$

Proof

Use the orbit-stabilizer theorem

$$\sum_{f_{\pi,g}} \frac{|\,\mathrm{AGL}(2m, 2)|}{|\,\mathrm{stab}(f_{\pi,g})|} = \frac{1\,369\,104\,324\,918\,194\,995\,200}{12\,130\,107\,857\,920} \qquad \square$$

Conclusion and Future Work

Take-Home Message

1. A complete picture of $\mathcal{M}$ class (along with $\mathcal{PS}$) in dimension 8
2. To decide equivalence of $f_{\pi,g}$ and $f_{\pi',g'}$ is non-trivial
3. Find good invariants distinguishing $f_{\pi,g}$ and $f_{\pi',g'}$
4. For the functions $f_{\pi,0}$ and $f_{\pi',0}$, there is a hope for classification

Conclusion and Future Work

Take-Home Message

1. A complete picture of $\mathcal{M}$ class (along with $\mathcal{PS}$) in dimension 8
2. To decide equivalence of $f_{\pi,g}$ and $f_{\pi',g'}$ is non-trivial
3. Find good invariants distinguishing $f_{\pi,g}$ and $f_{\pi',g'}$
4. For the functions $f_{\pi,0}$ and $f_{\pi',0}$, there is a hope for classification

Conjecture

Bent functions $f_{\pi,0}, f_{\pi',0}$ on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ are equivalent $\iff$ π and π' are from the same $(\mathrm{AGL}(m,2), \mathrm{AGL}(m,2))$-double coset in $S\left(\mathbb{F}_2^m\right)$.

Conclusion and Future Work

Take-Home Message

1. A complete picture of $\mathcal{M}$ class (along with $\mathcal{PS}$) in dimension 8
2. To decide equivalence of $f_{\pi,g}$ and $f_{\pi',g'}$ is non-trivial
3. Find good invariants distinguishing $f_{\pi,g}$ and $f_{\pi',g'}$
4. For the functions $f_{\pi,0}$ and $f_{\pi',0}$, there is a hope for classification

Conjecture

Bent functions $f_{\pi,0}, f_{\pi',0}$ on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ are equivalent $\iff$ π and π' are from the same $(\mathrm{AGL}(m,2), \mathrm{AGL}(m,2))$-double coset in $S(\mathbb{F}_2^m)$.

$\Rightarrow$ A lower bound on the # of eq. classes of $\mathcal{M}$ on $\mathbb{F}_2^m \times \mathbb{F}_2^m$

Conclusion and Future Work

Take-Home Message

1. A complete picture of $\mathcal{M}$ class (along with $\mathcal{PS}$) in dimension 8
2. To decide equivalence of $f_{\pi,g}$ and $f_{\pi',g'}$ is non-trivial
3. Find good invariants distinguishing $f_{\pi,g}$ and $f_{\pi',g'}$
4. For the functions $f_{\pi,0}$ and $f_{\pi',0}$, there is a hope for classification

Conjecture

Bent functions $f_{\pi,0}, f_{\pi',0}$ on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ are equivalent $\iff$ π and π' are from the same $(\mathrm{AGL}(m,2), \mathrm{AGL}(m,2))$-double coset in $S(\mathbb{F}_2^m)$.

$\Rightarrow$ A lower bound on the # of eq. classes of $\mathcal{M}$ on $\mathbb{F}_2^m \times \mathbb{F}_2^m$

m	1	2	3	4	5
$\mathfrak{N}(m,2)$	1	1	4	302	$2\,569\,966\,041\,123\,963\,092$
$\mathcal{CM}(2m,2)$	1	1	4	302+23	$\geq \mathfrak{N}(5,2)$?

Some Classification Results on Maiorana-McFarland Bent Functions

Philippe Langevin[1] and Alexandr Polujan[2]

philippe.langevin@univ-tln.fr alexandr.polujan@gmail.com

[1] Imath, Université de Toulon, La Garde, France

[2] Otto von Guericke University Magdeburg, Germany

BFA 2024
The 9th International Workshop on
Boolean Functions and their Applications,
09.09.2024

Further Reading I

[Bra06] An Braeken. "Cryptographic Properties of Boolean Functions and S-Boxes". PhD thesis. Katholieke Universiteit Leuven, Mar. 2006. URL: https://www.esat.kuleuven.be/cosic/publications/thesis-129.pdf (cit. on pp. 7–10).

[Can07] Christophe De Cannière. "Analysis And Design of Symmetric Encryption Algorithms". PhD thesis. Katholieke Universiteit Leuven, May 2007. URL: http://image.sciencenet.cn/olddata/kexue.com.cn/upload/blog/file/2009/3/200933205219387772.pdf (cit. on pp. 22, 23).

Further Reading II

[Dil72] John F. Dillon. "A survey of bent functions". In: *NSA Technical Journal* Special Issue (1972), pp. 191–215. URL: https://cryptome.org/2015/11/nsa-survey-of-bent-functions.pdf (cit. on pp. 7–10).

[Hou06] Xiang-Dong Hou. "Affinity of permutations of $\mathbb{F}_2^n$". In: *Discrete Applied Mathematics* 154.2 (2006), pp. 313–325. DOI: https://doi.org/10.1016/j.dam.2005.03.022 (cit. on pp. 22, 23).

[Lan] Philippe Langevin. *Classification of Bent Cubics in 8 variables*. URL: https://langevin.univ-tln.fr/project/bent/bent.html (cit. on pp. 7–10).

Further Reading III

[LH11] Philippe Langevin and Xiang-Dong Hou. "Counting Partial Spread Functions in Eight Variables". In: *IEEE Transactions on Information Theory* 57 (2011), pp. 2263–2269. DOI: https://doi.org/10.1109/tit.2011.2112230 (cit. on pp. 7–10).

[LL08] Philippe Langevin and Gregor Leander. "Classification of Boolean Quartic Forms in eight variables". In: *Boolean Functions in Cryptology and Information Security*. Vol. 18. 2008, pp. 139–147. DOI: https://doi.org/10.3233/978-1-58603-878-6-139 (cit. on pp. 7–10, 30–32).

Further Reading IV

[LP24] Philippe Langevin and Alexandr Polujan. “Some classification results on Maiorana-McFarland bent functions”. In: *Proceedings of the 9th International Workshop on Boolean Functions and their Applications*. 2024, To Appear (cit. on pp. 11–13, 33–35).

[Pas+24] Enes Pasalic, Alexandr Polujan, Sadmir Kudin and Fengrong Zhang. “Design and Analysis of Bent Functions Using $\mathcal{M}$-Subspaces”. In: *IEEE Transactions on Information Theory* 70.6 (2024), pp. 4464–4477. DOI: 10.1109/TIT.2024.3352824 (cit. on p. 6).

[PP20] Alexandr Polujan and Alexander Pott. "Cubic bent functions outside the completed Maiorana-McFarland class". In: *Designs, Codes and Cryptography* 88.9 (2020), pp. 1701–1722. DOI: 10.1007/s10623-019-00712-y (cit. on p. 6).

[PP22] Alexandr Polujan and Alexander Pott. "Towards the classification of quadratic vectorial bent functions in 8 variables". In: *The 7th international workshop on Boolean functions and their applications*. 2022. URL: https://boolean.w.uib.no/bfa-2022/ (cit. on pp. 30–32).