On rotation-symmetric Boolean bent functions outside the $\mathcal{M}^\#$ class

Alexandr Polujan[1] Sadmir Kudin[2] Enes Pasalic[2]

Otto von Guericke University Magdeburg, Germany[1]

University of Primorska, FAMNIT & IAM, Koper, Slovenia[2]

WCC 2024
The Thirteenth International Workshop on Coding and Cryptography,
18.06.2024

Boolean Functions

- $\mathbb{F}_2 = \{0, 1\}$ is the finite field with 2 elements
- $\mathbb{F}_2^n$ is the vector space of dimension n over $\mathbb{F}_2$
- Mappings $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ are called Boolean functions

- Algebraic Normal Form (ANF) of $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$

$$f(x_0, \ldots, x_{n-1}) = \sum_{v \in \mathbb{F}_2^n} c_v \left(\prod_{i=0}^{n-1} x_i^{v_i} \right),$$

where $c_v \in \mathbb{F}_2$ and $v = (v_0, \ldots, v_{n-1}) \in \mathbb{F}_2^n$

- The algebraic degree of a Boolean function f, denoted by $\deg(f)$, is the degree of its ANF

Equivalence of Boolean Functions

Definition

Functions $f, g \colon \mathbb{F}_2^n \to \mathbb{F}_2$ are equivalent if for all $x \in \mathbb{F}_2^n$

$$f(x) = g(xA + b) + l(x),$$

where $A \in GL(n, 2), b \in \mathbb{F}_2^n$ and l is an affine function on $\mathbb{F}_2^n$

Example

Boolean functions $f, g \colon \mathbb{F}_2^4 \to \mathbb{F}_2$ are equivalent

$f(x_0, x_1, x_2, x_3) = x_0 + x_1 + x_0x_3 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3,$

$g(x_0, x_1, x_2, x_3) = x_0x_1x_2 + x_1x_2x_3,$ since

$$f(x_0, x_1, x_2, x_3) = g((x_1, x_1 + x_2 + x_3, x_0 + x_1, x_1 + x_3) + (1, 0, 0, 1)) + x_0 + x_1$$

Bent Functions

Definition (Rothaus 1976)

A Boolean function f on $\mathbb{F}_2^n$ is called bent if the equation

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

has 2^{n-1} solutions $x \in \mathbb{F}_2^n$ for all $a \in \mathbb{F}_2^n \setminus \{0\}$ and $b \in \mathbb{F}_2$

- The mapping $D_a f(x) = f(x+a)+f(x)$ is called the (first-order) derivative of f at $a \in \mathbb{F}_2^n$

Facts

- Bent functions on $\mathbb{F}_2^n$ exist iff $n = 2m$
- For a bent function f on $\mathbb{F}_2^n$, we have that $2 \leq \deg(f) \leq n/2$

Bent Functions: Applications and the Simplest Example

Applications

- Cryptography and Coding Theory: non-linearity – studied in symmetric cryptography (Carlet 2021)
- Combinatorics: Constructions of designs, (partial) difference sets

Example

For $x = (x_0, \ldots, x_{m-1}), y = (y_0, \ldots, y_{m-1}) \in \mathbb{F}_2^m$, the dot product

$$f(x, y) = \langle x, y \rangle = \sum_{i=0}^{m-1} x_i y_i$$

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

The Completed Maiorana-McFarland Class $\mathcal{M}^\#$

- Maiorana-McFarland bent function on $\mathbb{F}_2^m \times \mathbb{F}_2^m$ is given by

$$f(x, y) = \langle x, \pi(y) \rangle + g(y),$$

where π is a permutation of $\mathbb{F}_2^m$ and $g \colon \mathbb{F}_2^m \to \mathbb{F}_2$

- The completed Maiorana-McFarland class is the set

$$\mathcal{M}^\# = \{f \text{ is bent} : f \text{ is equivalent to } \langle x, \pi(y) \rangle + g(y)\}$$

Facts

- $\mathcal{M}^\#$ contains many bent functions of all possible degrees
- Out of $\approx 2^{106}$ of all bent functions on $\mathbb{F}_2^8$, only $\approx 2^{70}$ are in $\mathcal{M}^\#$ (Langevin and Leander 2011)

Rotation-Symmetric (RotS) Boolean Functions

Definition (Pieprzyk and Qu 1998)

A Boolean function f on $\mathbb{F}_2^n$ is called rotation-symmetric (RotS) if it is invariant under circular translation of indices, i.e.,

$$\begin{aligned} & f(x_0, x_1, x_2, \ldots, x_{n-2}, x_{n-1}) \\ =& f(x_{n-1}, x_0, x_1, \ldots, x_{n-3}, x_{n-2}) \\ & \vdots \\ =& f(x_1, x_2, x_3, \ldots, x_{n-1}, x_0) \end{aligned}$$

holds for all $x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n$

Motivation (efficient evaluation)

RotS property is important for components in the rounds of hashing algorithms, since evaluations from previous iterations can be reused

Rotation-Symmetric (RotS) Bent Functions

Definition (Stănică and Maitra 2008)

A Boolean function f on $\mathbb{F}_2^n$ is called RotS bent if it is rotation-symmetric and bent

Example

The following function f on $\mathbb{F}_2^4$ is RotS bent

$$
\begin{aligned}
&f(x_0, x_1, x_2, x_3) = x_0x_2 + x_1x_3 \\
=&f(x_3, x_0, x_1, x_2) = x_3x_1 + x_0x_2 \\
=&f(x_2, x_3, x_0, x_1) = x_2x_0 + x_3x_1 \\
=&f(x_1, x_2, x_3, x_0) = x_1x_3 + x_2x_0
\end{aligned}
$$

- Finding infinite families is a non-trivial problem!

Quadratic RotS Bent Functions

Some quadratic bent Functions (Folklore)

$f(x) = \sum_{i=0}^{m-1} x_i x_{i+m}$ and $f(x) = \sum_{0 \le i < j \le n-1} x_i x_j$ are RotS bent on $\mathbb{F}_2^n$

Quadratic RotS Bent Functions

Some quadratic bent Functions (Folklore)

$f(x) = \sum_{i=0}^{m-1} x_i x_{i+m}$ and $f(x) = \sum_{0 \le i < j \le n-1} x_i x_j$ are RotS bent on $\mathbb{F}_2^n$

General case (Gao, Zhang, Liu, Carlet 2012)

Quadratic RotS function

$$f_c(x) = c_m \left(\sum_{i=0}^{m-1} x_i x_{m+i} \right) + \sum_{i=1}^{m-1} c_i \left(\sum_{j=0}^{n-1} x_j x_{i+j} \right)$$

is bent on $\mathbb{F}_2^n$ iff $F_c(X) = \sum_{i=1}^{m-1} c_i \left(X^{2^i} + X^{2^{n-i}} \right) + c_m X^{2^m}$ is a permutation polynomial

Non-quadratic RotS Bent Functions

Cubic functions (Gao, Zhang, Liu, Carlet 2012)

For $n = 2m$, $m \geq 2$ and $0 < t < m$, RotS cubic function

$$f_t(x) = \sum_{i=0}^{m-1} x_i x_{m+i} + \sum_{i=0}^{n-1} (x_i x_{t+i} x_{m+i} + x_i x_{t+i})$$

is bent on $\mathbb{F}_2^n$ iff $r = m/\gcd(m,t)$ is odd

Non-quadratic RotS Bent Functions

Cubic functions (Gao, Zhang, Liu, Carlet 2012)

For $n = 2m$, $m \geq 2$ and $0 < t < m$, RotS cubic function

$$f_t(x) = \sum_{i=0}^{m-1} x_i x_{m+i} + \sum_{i=0}^{n-1} (x_i x_{t+i} x_{m+i} + x_i x_{t+i})$$

is bent on $\mathbb{F}_2^n$ iff $r = m/\gcd(m,t)$ is odd

Higher (maximum) degree functions (Tang, Qi, Zhou, Fan 2018)

$$f_c(x) + h(x_0 + x_m, \ldots, x_{m-1} + x_{n-1}) \quad \text{and}$$
$$f_t(x) + h(x_0 + x_m, \ldots, x_{m-1} + x_{n-1}),$$

where h is any RotS function on $\mathbb{F}_2^m$

- More constructions: (Su, Tang 2017) and (Zhao, Zheng, Zhang 2018)

Problem and the Main Result

Fact

All known until 2018 RotS bent functions belong to $\mathcal{M}^{\#}$

Open Problem (Zhao, Zheng, Zhang 2018)

How to construct RotS bent functions outside $\mathcal{M}^{\#}$?

Problem and the Main Result

Fact

All known until 2018 RotS bent functions belong to $\mathcal{M}^{\#}$

Open Problem (Zhao, Zheng, Zhang 2018)

How to construct RotS bent functions outside $\mathcal{M}^{\#}$?

Theorem (Polujan, Kudin, Pasalic 2024)

Let $n = 2m$. Consider the following RotS bent function f on $\mathbb{F}_2^n$ of (Su, 2019) defined by

$$S(x_0, x_1 \cdots, x_{n-1}) = \sum_{i=0}^{m-1} (x_i x_{m+i}) + \sum_{i=0}^{n-1} (x_i x_{i+1} \cdots x_{i+m-2} \overline{x_{i+m}}),$$

where $\overline{x_{i+m}} = x_{i+m} + 1$. For all $n \geq 8$, S is outside the $\mathcal{M}^{\#}$ class.

Why this Construction?

- For a Boolean function f on $\mathbb{F}_2^n$ with $\deg(f) \geq 2$,

$$2\text{-rank}(f) := \mathrm{rank}_{\mathbb{F}_2} \left(f(x+y)\right)_{x,y \in \mathbb{F}_2^n}$$

is an invariant under EA-equivalence (Weng, Feng, Qiu 2007)

Theorem (Weng, Feng, Qiu 2007)

Let f on $\mathbb{F}_2^n$ be bent s.t. $f \in \mathcal{M}^\#$. Then, 2-rank$(f) \leq 2^{n/2+1} - 2$.

- For the RotS bent function S on $\mathbb{F}_2^n$, we have

n	8	10	12
$\mathcal{M}^\#$-Bound	30	62	126
2-rank(S)	42	112	286

Main Tool for the Analysis

Theorem (Dillon 1974)

A Boolean bent function f on $\mathbb{F}_2^n$ belongs to $\mathcal{M}^\#$ iff there exists an $n/2$-dimensional linear subspace U of $\mathbb{F}_2^n$ s.t. the second-order derivative

$$D_a D_b f(x) = f(x + a + b) + f(x + a) + f(x + b) + f(x) = 0,$$

for any $a, b \in U$.

Main Tool for the Analysis

Theorem (Dillon 1974)

A Boolean bent function f on $\mathbb{F}_2^n$ belongs to $\mathcal{M}^\#$ iff there exists an $n/2$-dimensional linear subspace U of $\mathbb{F}_2^n$ s.t. the second-order derivative

$$D_aD_bf(x) = f(x+a+b) + f(x+a) + f(x+b) + f(x) = 0,$$

for any $a, b \in U$.

To Do

For every subspace $U \subset \mathbb{F}_2^n$ of dim $n/2$, find $a, b \in U$ s.t. $D_aD_bf \neq 0$

- Use the techniques developed in (Pasalic, Polujan, Kudin, Zhang 2024)

Sketch of the Proof

$$S\left(x_0, x_1 \cdots, x_{n-1}\right) = \sum_{i=0}^{m-1} \left(x_i x_{m+i}\right) + \sum_{i=0}^{n-1} \left(x_i x_{i+1} \cdots x_{i+m-2} \overline{x_{i+m}}\right)$$

1. Observe that the term $x_0 x_1 \cdots x_{m-2} \overline{x_m}$ is an indicator of $v = (1, 1, \ldots, 1, 0) \in \mathbb{F}_2^m$, i.e., $\delta_v(x) = \delta_0(x + v)$
2. Show, that $\deg(D_a D_b \delta_0) = m - 2$, for all distinct $a, b \in \mathbb{F}_2^m$
3. For an arbitrary m-dimensional subspace U of $\mathbb{F}_2^n$, consider the subspace W of U with $\dim(W) \geq m - 4$ of the form $w = (w_0, \ldots, w_{n-1}) \in W$ with $w_0 = w_{m-1} = w_m = w_{n-1} = 0$
4. Define $L : W \to \mathbb{F}_2^{m-2}$ by $L(w_0, \ldots, w_{n-1}) = (w_1, \ldots, w_{m-2})$, for all $(w_0, \ldots, w_{n-1}) \in W$. By the rank-nullity theorem, we have:

$$\dim(W) = \dim(Ker(L)) + \dim(Im(L)).$$

Sketch of the Proof

$$S\left(x_0, x_1 \cdots, x_{n-1}\right) = \sum_{i=0}^{m-1} \left(x_i x_{m+i}\right) + \sum_{i=0}^{n-1} \left(x_i x_{i+1} \cdots x_{i+m-2} \overline{x_{i+m}}\right)$$

5. Consider the following two cases

5.1 If $\dim(Im(L)) \geq 2$, there exist $a, b \in W$ s.t. $(a_1, \ldots, a_{m-2})$ and $(b_1, \ldots, b_{m-2})$ are linearly independent. Show that $m-2$ degree terms of $D_a D_b(x_0 x_1 \cdots x_{m-2} \overline{x_m})$ can not be canceled by $m-2$ degree terms of $D_a D_b(x_m x_{m+1} \cdots x_{2m-2} \overline{x_0})$.

5.2 If $\dim(Im(L)) \leq 1$, then $\dim(Ker(L)) \geq m-4-1 = m-5 \geq 2$, assuming $m \geq 7$. Take linearly independent $a, b \in W \cap Ker(L)$. Show that $m-2$ degree terms of $D_a D_b(x_m x_{m+1} \cdots x_{2m-2} \overline{x_0})$ can not be canceled by $m-2$ degree terms of $D_a D_b(x_0 x_1 \cdots x_{m-2} \overline{x_m})$.

6. Thus, $\exists\, a, b \in W \subseteq U$, s.t. $\deg(D_a D_b S) = m-2 \Rightarrow S \notin \mathcal{M}^{\#}$.

7. For $4 \leq m \leq 6$, use 2-rank. □

More Results in the Paper

1. Analysis of higher-order derivatives of indicator functions
2. The dual bent function $\tilde{S}$ on $\mathbb{F}_2^n$ is outside $\mathcal{M}^\#$ too
3. Classification of RotS cubic bent on $\mathbb{F}_2^{10}$ computationally

$f_i \in C_i$	SANF of a representative $f_i \in C_i$	$\|C_i\|$
f_1	$x_0x_5 + x_0x_1x_4 + x_0x_1x_6 + x_0x_1x_7$	384
f_2	$x_0x_5 + x_0x_1x_3 + x_0x_1x_4 + x_0x_1x_5 + x_0x_1x_6 + x_0x_1x_7 + x_0x_1x_8$	24
f_3	$x_0x_5 + x_0x_1x_2 + x_0x_1x_3 + x_0x_1x_5 + x_0x_1x_6 + x_0x_1x_8 + x_0x_2x_6$	72
f_4	$x_0x_1 + x_0x_5 + x_0x_1x_3 + x_0x_1x_6 + x_0x_1x_8$	384
f_5	$x_0x_1 + x_0x_5 + x_0x_1x_3 + x_0x_1x_5 + x_0x_1x_6 + x_0x_1x_8 + x_0x_2x_7$	384
f_6	$x_0x_5 + x_0x_1x_2 + x_0x_1x_4 + x_0x_1x_6 + x_0x_1x_8 + x_0x_2x_4$	192
f_7	$x_0x_5 + x_0x_1x_2 + x_0x_1x_4 + x_0x_1x_7 + x_0x_2x_6$	36
f_8	$x_0x_5 + x_0x_1x_4 + x_0x_1x_8 + x_0x_2x_4 + x_0x_2x_7$	96
Total	—	1572

- The function f_8 is RotS cubic bent outside $\mathcal{M}^\#$

Conclusion and Future Work

Results

1. The first proof showing that an infinite family of RotS bent functions (of max. degree) is outside $\mathcal{M}^{\#}$
2. The first examples of RotS bent functions of low degree outside $\mathcal{M}^{\#}$

Open Problems

1. Find "rich" infinite families of RotS bent functions outside $\mathcal{M}^{\#}$
2. Provide an alternative proof using 2-rank
3. Further analysis of the new cubic function outside $\mathcal{M}^{\#}$

On rotation-symmetric Boolean bent functions outside the $\mathcal{M}^\#$ class

Alexandr Polujan[1] Sadmir Kudin[2] Enes Pasalic[2]

Otto von Guericke University Magdeburg, Germany[1]

University of Primorska, FAMNIT & IAM, Koper, Slovenia[2]

WCC 2024
The Thirteenth International Workshop on Coding and Cryptography,
18.06.2024

Further Reading I

[Car21] Claude Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021. DOI: https://doi.org/10.1017/9781108606806 (cit. on p. 5).

[Dil74] J. F. Dillon. "Elementary Hadamard Difference Sets". PhD thesis. University of Maryland, 1974. DOI: https://doi.org/10.13016/M2MS3K194 (cit. on pp. 16, 17).

[Gao+12] Guangpu Gao, Xiyong Zhang, Wenfen Liu and Claude Carlet. "Constructions of Quadratic and Cubic Rotation Symmetric Bent Functions". In: *IEEE Transactions on Information Theory* 58.7 (2012), pp. 4908–4913. DOI: https://doi.org/10.1109/TIT.2012.2193377 (cit. on pp. 9–12).

Further Reading II

[LL11] Philippe Langevin and Gregor Leander. "Counting all bent functions in dimension eight 99270589265934370305785861242880". In: *Des. Codes Cryptography* 59.1-3 (2011), pp. 193–205. DOI: https://doi.org/10.1007/s10623-010-9455-z (cit. on p. 6).

[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: https://doi.org/10.1109/TIT.2024.3352824 (cit. on pp. 16, 17).

Further Reading III

[PKP24] Alexandr Polujan, Sadmir Kudin and Enes Pasalic. "On rotation-symmetric Boolean bent functions outside the $\mathcal{M}^{\#}$ class". In: *Proceedings of the Thirteens International Workshop on Coding and Cryptography*. 2024, pp. 319–330 (cit. on pp. 13, 14).

[PQ98] Josef Pieprzyk and Cheng Xin Qu. "Rotation-symmetric functions and fast hashing". In: *Information Security and Privacy*. Ed. by Colin Boyd and Ed Dawson. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 169–180. DOI: https://doi.org/10.1007/BFb0053731 (cit. on p. 7).

Further Reading IV

[Rot76] O.S Rothaus. "On "bent" functions". In: *Journal of Combinatorial Theory, Series A* 20.3 (1976), pp. 300–305. DOI: https://doi.org/10.1016/0097-3165(76)90024-8 (cit. on p. 4).

[SM08] Pantelimon Stănică and Subhamoy Maitra. "Rotation symmetric Boolean functions—Count and cryptographic properties". In: *Discrete Applied Mathematics* 156.10 (2008), pp. 1567–1580. ISSN: 0166-218X. DOI: https://doi.org/10.1016/j.dam.2007.04.029 (cit. on p. 8).

[ST17] Sihong Su and Xiaohu Tang. "Systematic Constructions of Rotation Symmetric Bent Functions, 2-Rotation Symmetric Bent Functions, and Bent Idempotent Functions". In: *IEEE Transactions on Information Theory* 63.7 (2017), pp. 4658–4667. DOI: 10.1109/TIT.2016.2621751 (cit. on pp. 11, 12).

[Tan+18] Chunming Tang, Yanfeng Qi, Zhengchun Zhou and Cuiling Fan. "Two infinite classes of rotation symmetric bent functions with simple representation". In: *Applicable Algebra in Engineering, Communication and Computing* 29.3 (June 2018), pp. 197–208. DOI: https://doi.org/10.1007/s00200-017-0337-8 (cit. on pp. 11, 12).

Further Reading VI

[WFQ07] Guobiao Weng, Rongquan Feng and Weisheng Qiu. "On the ranks of bent functions". In: *Finite Fields and Their Applications* 13.4 (2007), pp. 1096–1116. DOI: https://doi.org/10.1016/j.ffa.2007.03.001 (cit. on p. 15).

[ZZZ18] Qinglan Zhao, Dong Zheng and Weiguo Zhang. "Constructions of rotation symmetric bent functions with high algebraic degree". In: *Discrete Applied Mathematics* 251 (2018), pp. 15–29. DOI: https://doi.org/10.1016/j.dam.2018.05.048 (cit. on pp. 11–14).