Normality of Boolean bent functions in eight variables, revisited

Alexandr Polujan[a], Luca Mariot[b], Stjepan Picek[c]

[a]Otto von Guericke University Magdeburg, Germany
[b]Semantics, Cybersecurity and Services Group, University of Twente, The Netherlands
[c]Digital Security Group, Radboud University, The Netherlands

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

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
- Let $\mathcal{A}_n$ be the set of all affine functions in n variables

$$\mathcal{A}_n = \{a_0 + a_1x_1 + \cdots + a_nx_n \colon a_i \in \mathbb{F}_2\}$$

- The Hamming distance between $f, g \in \mathcal{B}_n$ is given by

$$d_H(f,g) = |\{x \in \mathbb{F}_2^n \colon f(x) \neq g(x)\}|$$

- The nonlinearity of $f \in \mathcal{B}_n$ is defined by

$$\mathrm{nl}(f) = \min_{l \in \mathcal{A}_n} d_H(f,l)$$

Boolean bent functions, and their normality

- A function $f \in \mathcal{B}_n$ is called bent if $\mathrm{nl}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$
- They exist if $n = 2m$; if $f \in \mathcal{B}_n$ is bent then $\deg(f) \leq n/2$

Boolean bent functions, and their normality

- A function $f \in \mathcal{B}_n$ is called bent if $\mathrm{nl}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$
- They exist if $n = 2m$; if $f \in \mathcal{B}_n$ is bent then $\deg(f) \leq n/2$

Example (Desarguesian partial spread bent functions)

$\mathcal{PS}_{ap}$ class: $f(x, y) = g(xy^{2^m-2})$ for $x, y \in \mathbb{F}_{2^m}$, where $g \in \mathcal{B}_m$ is balanced and $g(0) = 0$

Boolean bent functions, and their normality

- A function $f \in \mathcal{B}_n$ is called bent if $\mathrm{nl}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$
- They exist if $n = 2m$; if $f \in \mathcal{B}_n$ is bent then $\deg(f) \leq n/2$

Example (Desarguesian partial spread bent functions)

$\mathcal{PS}_{ap}$ class: $f(x,y) = g(xy^{2^m-2})$ for $x, y \in \mathbb{F}_{2^m}$, where $g \in \mathcal{B}_m$ is balanced and $g(0) = 0$

Definition (Dobbertin 1995): A bent function $f \in \mathcal{B}_n$ is said to be normal if it is constant on some affine subspace $U \subset \mathbb{F}_2^n$ of dimension $n/2$; otherwise non-normal

Boolean bent functions, and their normality

- A function $f \in \mathcal{B}_n$ is called bent if $\mathrm{nl}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$
- They exist if $n = 2m$; if $f \in \mathcal{B}_n$ is bent then $\deg(f) \leq n/2$

Example (Desarguesian partial spread bent functions)

$\mathcal{PS}_{ap}$ class: $f(x,y) = g(xy^{2^m-2})$ for $x, y \in \mathbb{F}_{2^m}$, where $g \in \mathcal{B}_m$ is balanced and $g(0) = 0$

Definition (Dobbertin 1995): A bent function $f \in \mathcal{B}_n$ is said to be normal if it is constant on some affine subspace $U \subset \mathbb{F}_2^n$ of dimension $n/2$; otherwise non-normal

Definition (Charpin 2004): A bent function $f \in \mathcal{B}_n$ is said to be weakly normal if it is affine on some affine subspace $U \subset \mathbb{F}_2^n$ of dimension $n/2$; otherwise non-weakly-normal

Normality of bent functions: The motivation

Why non-normal bent functions?

Many known constructions are normal. One can consider non-normal bent functions as “new”

Normality of bent functions: The motivation

Why non-normal bent functions?

Many known constructions are normal. One can consider non-normal bent functions as “new”

Example (Desarguesian partial spread bent functions)

$\mathcal{PS}_{ap}$ class: Every $f(x,y) = g(xy^{2^m-2})$ for $x, y \in \mathbb{F}_{2^m}$, where $g \in \mathcal{B}_m$ is balanced and $g(0) = 0$, is normal w.r.t. $\mathbb{F}_{2^m} \times \{0\}$

Normality of bent functions: The motivation

Why non-normal bent functions?

Many known constructions are normal. One can consider non-normal bent functions as "new"

Example (Desarguesian partial spread bent functions)

$\mathcal{PS}_{ap}$ class: Every $f(x,y) = g(xy^{2^m-2})$ for $x, y \in \mathbb{F}_{2^m}$, where $g \in \mathcal{B}_m$ is balanced and $g(0) = 0$, is normal w.r.t. $\mathbb{F}_{2^m} \times \{0\}$

Why non-weakly-normal bent functions?

Weak normality is invariant under extended-affine equivalence

Normality of bent functions, theoretical results

- For n small, one can prove normality theoretically, since the structure of bent functions is known

Normality of bent functions, theoretical results

- For n small, one can prove normality theoretically, since the structure of bent functions is known
- $n = 2, 4$: All bent functions are quadratic, hence normal

Normality of bent functions, theoretical results

- For n small, one can prove normality theoretically, since the structure of bent functions is known
- $n = 2, 4$: All bent functions are quadratic, hence normal
- $n = 6$: All bent functions are Maiorana-McFarland, hence normal

Normality of bent functions, theoretical results

- For n small, one can prove normality theoretically, since the structure of bent functions is known
- $n = 2, 4$: All bent functions are quadratic, hence normal
- $n = 6$: All bent functions are Maiorana-McFarland, hence normal
- $n = 8$:
  - All quadratic bent functions are normal
  - All cubic bent functions are normal (Charpin 2004)

Normality of bent functions, computational results

- $n = 10, 12, 14$: A few examples shown to be non-weakly-normal using an algorithm of Canteaut, Daum, Dobbertin and Leander 2006

Normality of bent functions, computational results

- $n = 10, 12, 14$: A few examples shown to be non-weakly-normal using an algorithm of Canteaut, Daum, Dobbertin and Leander 2006

  Example: The restriction of the Kasami–Welch function $x \in \mathbb{F}_{2^{11}} \mapsto Tr(x^{241})$ to the trace 0/1 elements is a non-weakly-normal bent function on $\mathbb{F}_{2^{10}}$ (Leander and McGuire 2009)

Normality of bent functions, computational results

- $n = 10, 12, 14$: A few examples shown to be non-weakly-normal using an algorithm of Canteaut, Daum, Dobbertin and Leander 2006

  Example: The restriction of the Kasami–Welch function $x \in \mathbb{F}_{2^{11}} \mapsto Tr(x^{241})$ to the trace 0/1 elements is a non-weakly-normal bent function on $\mathbb{F}_{2^{10}}$ (Leander and McGuire 2009)

Result (Leander 2005)

Let $f, g \in \mathcal{B}_n$ be bent and g be additionally quadratic. Then $h(x, y) = f(x) + g(y)$ is (weakly) normal on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ iff f is (weakly) normal on $\mathbb{F}_2^n$.

Normality of bent functions, computational results

- $n = 10, 12, 14$: A few examples shown to be non-weakly-normal using an algorithm of Canteaut, Daum, Dobbertin and Leander 2006

  Example: The restriction of the Kasami–Welch function $x \in \mathbb{F}_{2^{11}} \mapsto Tr(x^{241})$ to the trace 0/1 elements is a non-weakly-normal bent function on $\mathbb{F}_{2^{10}}$ (Leander and McGuire 2009)

Result (Leander 2005)

Let $f, g \in \mathcal{B}_n$ be bent and g be additionally quadratic. Then $h(x, y) = f(x) + g(y)$ is (weakly) normal on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ iff f is (weakly) normal on $\mathbb{F}_2^n$.

- $n \geq 10$: There exist non-weakly-normal bent functions on $\mathbb{F}_2^n$

Normality of bent functions, computational results

- $n = 10, 12, 14$: A few examples shown to be non-weakly-normal using an algorithm of Canteaut, Daum, Dobbertin and Leander 2006

  Example: The restriction of the Kasami–Welch function $x \in \mathbb{F}_{2^{11}} \mapsto Tr(x^{241})$ to the trace 0/1 elements is a non-weakly-normal bent function on $\mathbb{F}_{2^{10}}$ (Leander and McGuire 2009)

Result (Leander 2005)

Let $f, g \in \mathcal{B}_n$ be bent and g be additionally quadratic. Then $h(x, y) = f(x) + g(y)$ is (weakly) normal on $\mathbb{F}_2^n \times \mathbb{F}_2^m$ iff f is (weakly) normal on $\mathbb{F}_2^n$.

- $n \geq 10$: There exist non-weakly-normal bent functions on $\mathbb{F}_2^n$
- The only missing case: $n = 8$ degree 4

Normality of bent functions in $n = 8$ variables

Research Questions:

1. Do non-normal bent functions of 8 variables and degree 4 exist? (Charpin 2004, Open problem 5)

Normality of bent functions in $n = 8$ variables

Research Questions:

1. Do non-normal bent functions of 8 variables and degree 4 exist? (Charpin 2004, Open problem 5)
2. Do non-normal partial spread bent functions in the $\mathcal{PS}^- \setminus \mathcal{PS}_{ap}$ class exist? (Leander 2005, p.17)

Normality of bent functions in $n = 8$ variables

Research Questions:

1. Do non-normal bent functions of 8 variables and degree 4 exist? (Charpin 2004, Open problem 5)
2. Do non-normal partial spread bent functions in the $\mathcal{PS}^- \setminus \mathcal{PS}_{ap}$ class exist? (Leander 2005, p.17)
3. What's about weak normality?

Normality of bent functions in $n = 8$ variables

Research Questions:

1. Do non-normal bent functions of 8 variables and degree 4 exist? (Charpin 2004, Open problem 5)
2. Do non-normal partial spread bent functions in the $\mathcal{PS}^- \setminus \mathcal{PS}_{ap}$ class exist? (Leander 2005, p.17)
3. What's about weak normality?

Main Results:

I. Non-normal bent functions on $\mathbb{F}_2^8$ in the $\mathcal{PS}^- \setminus \mathcal{PS}_{ap}$ exist

II. Partial spread bent functions on $\mathbb{F}_2^8$ are normal or weakly normal

III. Generation of non-(weakly) normal bent functions using genetic programming: A designer's perspective

Partial spread bent functions: The $\mathcal{PS}^-$ class

Definition: A partial spread of order s in $\mathbb{F}_2^n$ with $n = 2m$ is a set of s vector subspaces $U_1, \ldots, U_s$ of $\mathbb{F}_2^n$ of dimension m each, such that $U_i \cap U_j = \{0\}$ for all $i \neq j$.

Partial spread bent functions: The $\mathcal{PS}^-$ class

Definition: A partial spread of order s in $\mathbb{F}_2^n$ with $n = 2m$ is a set of s vector subspaces $U_1, \ldots, U_s$ of $\mathbb{F}_2^n$ of dimension m each, such that $U_i \cap U_j = \{0\}$ for all $i \neq j$.

- The partial spread class $\mathcal{PS}^-$ (Dillon 1974):

$$f(x) = \sum_{i=1}^{2^{m-1}} \mathbb{1}_{U_i^*}(x) \quad \text{where } U_i^* := U_i \setminus \{0\}$$

and vector subspaces $U_1, \ldots, U_{2^{m-1}}$ of $\mathbb{F}_2^n$ form a partial spread

Partial spread bent functions: The $\mathcal{PS}^-$ class

Definition: A partial spread of order s in $\mathbb{F}_2^n$ with $n = 2m$ is a set of s vector subspaces $U_1, \ldots, U_s$ of $\mathbb{F}_2^n$ of dimension m each, such that $U_i \cap U_j = \{0\}$ for all $i \neq j$.

- The partial spread class $\mathcal{PS}^-$ (Dillon 1974):

$$f(x) = \sum_{i=1}^{2^{m-1}} \mathbb{1}_{U_i^*}(x) \quad \text{where } U_i^* := U_i \setminus \{0\}$$

and vector subspaces $U_1, \ldots, U_{2^{m-1}}$ of $\mathbb{F}_2^n$ form a partial spread

- The only known explicit subclass of $\mathcal{PS}^-$ is $\mathcal{PS}_{ap}$
- All members of $\mathcal{PS}_{ap} \subset \mathcal{PS}^-$ are normal

$\mathcal{PS}^-$ bent functions in $n = 8$ variables

- Up to equivalence, all $\mathcal{PS}^-$ bent functions in $n = 8$ variables are known (Langevin and Hou 2011)

$\mathcal{PS}^-$ bent functions in $n = 8$ variables

- Up to equivalence, all $\mathcal{PS}^-$ bent functions in $n = 8$ variables are known (Langevin and Hou 2011)
- The representatives are available online (Langevin 2012)

	extension			classification		stabilization	
n	time	size	time	time	class	time	psf
4	1	5	1	0	3	1	64374841666437120
5	15	233	55	10	22	10	202670571231809372 16
6	69	4893	1162	385	341	6	133998981239236932 4032
7	415	29691	7038	7246	3726	62	1783333713266206153 1136
8	1076	60943	14449	33501	9316	229	4605609666146707341 3120
9	681	31715	7516	8594	5442	19529	2452065057612704097 8944
10	219	8871	2109	698	1336	23	473149704582291102 1056
11	75	2759	654	148	303	6	713809537614313684 992
12	20	675	160	30	42	10	38019657690425327616
13	3	96	23	4	6	2	129740065512357888
14	0	11	3	0	1	59	44213490155520
15	0	3	1	0	1	11186	6579388416
16	0	2	0	0	1	0	200787
17	0	1	0	0	1	0	1

$\mathcal{PS}^-$ bent functions in $n = 8$ variables

- Up to equivalence, all $\mathcal{PS}^-$ bent functions in $n = 8$ variables are known (Langevin and Hou 2011)
- The representatives are available online (Langevin 2012)

	extension			classification			stabilization
n	time	size	time	time	class	time	psf
4	1	5	1	0	3	1	64374841666437120
5	15	233	55	10	22	10	20267057123180937216
6	69	4893	1162	385	341	6	1339989812392369324032
7	415	29691	7038	7246	3726	62	17833337132662061531136
8	1076	60943	14449	33501	9316	229	46056096661467073413120
9	681	31715	7516	8594	5442	19529	24520650576127040978944
10	219	8871	2109	698	1336	23	4731497045822911021056
11	75	2759	654	148	303	6	713809537614313684992
12	20	675	160	30	42	10	38019657690425327616
13	3	96	23	4	6	2	129740065512357888
14	0	11	3	0	1	59	44213490155520
15	0	3	1	0	1	11186	6579388416
16	0	2	0	0	1	0	200787
17	0	1	0	0	1	0	1

- How to check normality of $9\,316$ bent functions in a reasonable time?

Checking Normality for $n = 8$ variables

- One can use the following result (Charpin 2004, Theorem 1)

Algorithm. Checking normality

Require: Bent function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$.

for all subspaces V of dimension $n/2$ **do**

  Check the following condition: f is constant on $b + V$ iff

$$(-1)^{b \cdot v} \hat{\chi}_f(v) = \varepsilon 2^{n/2}, \text{ for all } v \in V^{\perp}$$

  where ε is constant, equal either to $+1$ or -1.

  Output affine subspaces $b + V$, on which f is constant.

end for

Checking Normality for $n = 8$ variables

- One can use the following result (Charpin 2004, Theorem 1)

Algorithm. Checking normality

Require: Bent function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$.

1: **for all** subspaces V of dimension $n/2$ **do**

2: **Check** the following condition: f is constant on $b + V$ iff

$$(-1)^{b\cdot v}\hat{\chi}_f(v) = \varepsilon 2^{n/2}, \text{ for all } v \in V^{\perp}$$

where ε is constant, equal either to $+1$ or -1.

3: **Output** affine subspaces $b + V$, on which f is constant.

4: **end for**

- There are $200\,787$ vector spaces of dim 4 in $\mathbb{F}_2^8$ and $9\,316$ $\mathcal{PS}^-$ bent functions to check

Checking Normality for $n = 8$ variables

- One can use the following result (Charpin 2004, Theorem 1)

Algorithm. Checking normality

Require: Bent function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$.
1: **for all** subspaces V of dimension $n/2$ **do**
2: **Check** the following condition: f is constant on $b + V$ iff

$$(-1)^{b\cdot v}\hat{\chi}_f(v) = \varepsilon 2^{n/2}, \text{ for all } v \in V^{\perp}$$

where ε is constant, equal either to $+1$ or -1.
3: **Output** affine subspaces $b + V$, on which f is constant.
4: **end for**

- There are $200\,787$ vector spaces of dim 4 in $\mathbb{F}_2^8$ and $9\,316$ $\mathcal{PS}^-$ bent functions to check
- It took a few hours to check (on a laptop) that all but one $\mathcal{PS}^-$ bent functions are normal

Non-normal $\mathcal{PS}^-$ bent function in $n = 8$ variables

- The following bent function $f \in \mathcal{PS}^- \setminus \mathcal{PS}_{ap}$ class (psf=970 in the list of Langevin 2012) is non-normal

$$
\begin{aligned}
f(x) = {} & x_1 + x_2 + x_1x_2 + x_3 + x_1x_3 + x_2x_3 + x_1x_2x_3 + x_4 + x_1x_4 + x_2x_4 + x_1x_2x_4 + x_3x_4 \\
& + x_1x_3x_4 + x_2x_3x_4 + x_1x_2x_3x_4 + x_5 + x_1x_5 + x_1x_2x_5 + x_1x_3x_5 + x_2x_3x_5 + x_4x_5 + x_1x_4x_5 \\
& + x_2x_4x_5 + x_1x_2x_4x_5 + x_2x_3x_4x_5 + x_6 + x_1x_6 + x_2x_6 + x_3x_6 + x_1x_3x_6 + x_2x_3x_6 \\
& + x_1x_2x_3x_6 + x_1x_4x_6 + x_1x_2x_4x_6 + x_3x_4x_6 + x_1x_3x_4x_6 + x_5x_6 + x_2x_5x_6 + x_3x_5x_6 \\
& + x_2x_3x_5x_6 + x_4x_5x_6 + x_7 + x_2x_7 + x_1x_2x_7 + x_3x_7 + x_2x_3x_7 + x_2x_4x_7 + x_1x_2x_4x_7 \\
& + x_1x_3x_4x_7 + x_2x_3x_4x_7 + x_5x_7 + x_2x_5x_7 + x_1x_2x_5x_7 + x_3x_5x_7 + x_1x_3x_5x_7 + x_4x_5x_7 \\
& + x_1x_4x_5x_7 + x_2x_4x_5x_7 + x_6x_7 + x_1x_6x_7 + x_2x_6x_7 + x_3x_6x_7 + x_2x_3x_6x_7 + x_1x_4x_6x_7 \\
& + x_5x_6x_7 + x_1x_5x_6x_7 + x_2x_5x_6x_7 + x_4x_5x_6x_7 + x_8 + x_1x_8 + x_1x_2x_8 + x_4x_8 + x_1x_4x_8 \\
& + x_2x_4x_8 + x_3x_4x_8 + x_1x_3x_4x_8 + x_2x_3x_4x_8 + x_5x_8 + x_1x_2x_5x_8 + x_4x_5x_8 + x_2x_4x_5x_8 \\
& + x_6x_8 + x_1x_6x_8 + x_2x_6x_8 + x_1x_3x_6x_8 + x_4x_6x_8 + x_5x_6x_8 + x_1x_5x_6x_8 + x_4x_5x_6x_8 \\
& + x_7x_8 + x_1x_7x_8 + x_2x_7x_8 + x_1x_2x_7x_8 + x_3x_7x_8 + x_2x_3x_7x_8 + x_4x_7x_8 + x_5x_7x_8 \\
& + x_1x_5x_7x_8 + x_3x_5x_7x_8 + x_6x_7x_8 + x_1x_6x_7x_8 + x_3x_6x_7x_8 + x_5x_6x_7x_8
\end{aligned}
$$

- It has a trivial automorphism group
- It is weakly-normal

Is there a "nice" description of this function?

Theorem (Gadouleau, Mariot and Picek 2023)

Let $m, l, d \in \mathbb{N}$ such that $m = ld$. If there are $t = 2^{ld-1}$ coprime polynomials of degree $d \geq 1$ over $\mathbb{F}_{2^l}$, possibly including the constant polynomial 1 of degree 0. Then, there exists a partial spread P over $\mathbb{F}_2^n, n = 2m$, whose union of its subspaces with the null vector discarded defines a bent function in the class $\mathcal{PS}^-$.

Is there a "nice" description of this function?

Theorem (Gadouleau, Mariot and Picek 2023)

Let $m, l, d \in \mathbb{N}$ such that $m = ld$. If there are $t = 2^{ld-1}$ coprime polynomials of degree $d \geq 1$ over $\mathbb{F}_{2^l}$, possibly including the constant polynomial 1 of degree 0. Then, there exists a partial spread P over $\mathbb{F}_2^n, n = 2m$, whose union of its subspaces with the null vector discarded defines a bent function in the class $\mathcal{PS}^-$.

- Using coprime polynomials of degree $d = 2$ over $\mathbb{F}_4$, one can construct 273 $\mathcal{PS}^-$ bent functions
- However, all of them are normal

Is there a “nice” description of this function?

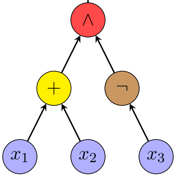
Theorem (Gadouleau, Mariot and Picek 2023)

Let $m, l, d \in \mathbb{N}$ such that $m = ld$. If there are $t = 2^{ld-1}$ coprime polynomials of degree $d \geq 1$ over $\mathbb{F}_{2^l}$, possibly including the constant polynomial 1 of degree 0. Then, there exists a partial spread P over $\mathbb{F}_2^n, n = 2m$, whose union of its subspaces with the null vector discarded defines a bent function in the class $\mathcal{PS}^-$.

- Using coprime polynomials of degree $d = 2$ over $\mathbb{F}_4$, one can construct 273 $\mathcal{PS}^-$ bent functions
- However, all of them are normal
- Other ways to construct non-normal or non-weakly-normal bent functions?

Evolving Boolean functions with Genetic Programming

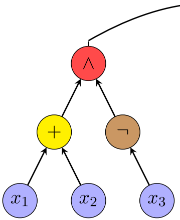
- GP Encoding: An individual is represented by a tree



x_1	x_2	x_3	$f(x)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

Evolving Boolean functions with Genetic Programming

- GP Encoding: An individual is represented by a tree

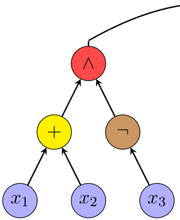


x_1	x_2	x_3	$f(x)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

- Create a random initial population of X individuals
- Repeat Y times

Evolving Boolean functions with Genetic Programming

- GP Encoding: An individual is represented by a tree



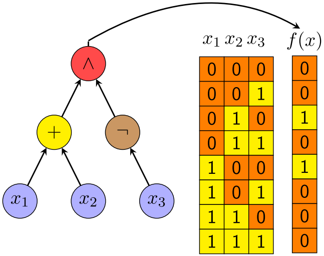
x_1	x_2	x_3	$f(x)$
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

- Create a random initial population of X individuals
- Repeat Y times

1. Evaluation with a fitness function
2. Selection of parents and reproduction
3. Replace the last population

Evolving Boolean functions with Genetic Programming

- GP Encoding: An individual is represented by a tree



- Create a random initial population of 50 individuals
- Repeat $500\,000$ times

1. Evaluation with a fitness function (highest nonlinearity)
2. Selection of parents and reproduction
3. Replace the last population

Evolving bent functions with GP: The results

- After $10\,000$ runs, we got $7\,478$ different bent functions, including

degree, d	# of bent functions with degree d
2	$4\,690$
3	$2\,367$
4	421

Evolving bent functions with GP: The results

- After $10\,000$ runs, we got $7\,478$ different bent functions, including

degree, d	# of bent functions with degree d
2	$4\,690$
3	$2\,367$
4	421

- All bent functions we got are normal

Evolving bent functions with GP: The results

- After $10\,000$ runs, we got $7\,478$ different bent functions, including

degree, d	# of bent functions with degree d
2	$4\,690$
3	$2\,367$
4	421

- All bent functions we got are normal
- The "most complicated" ANF looks as follows

$$g(x) = 1 + x_2 + x_5 + x_6 + x_8 + x_1x_5 + x_1x_7 + x_1x_8 + x_2x_6 + x_2x_7 + x_3x_8 + x_4x_7 + x_2x_5x_8 + x_1x_3x_6x_7 + x_2x_5x_7x_8$$

Conclusion and future work

Summary

I. Non-normal degree 4 bent functions on $\mathbb{F}_2^8$ exist, thus

Corollary: Let f be a non-normal bent function on $\mathbb{F}_2^n$. Then, $n \geq 8$.

II. Partial spread bent functions on $\mathbb{F}_2^8$ are normal or weakly normal.

III. Non-normal bent functions in the $\mathcal{PS}^-$ class exist.

Conclusion and future work

Summary

I. Non-normal degree 4 bent functions on $\mathbb{F}_2^8$ exist, thus

Corollary: Let f be a non-normal bent function on $\mathbb{F}_2^n$. Then, $n \geq 8$.

II. Partial spread bent functions on $\mathbb{F}_2^8$ are normal or weakly normal.

III. Non-normal bent functions in the $\mathcal{PS}^-$ class exist.

Open problems

1. Understand the non-normal example, e.g., what is so special in the corresponding partial spread?
2. Do non-weakly-normal bent functions on $\mathbb{F}_2^8$ exist?
3. How to tune GP to produce many "interesting" (e.g., non-normal, non-weakly-normal, with trivial automorphism groups, inequivalent to $\mathcal{MM} \cup \mathcal{PS}$ classes) bent functions?

Normality of Boolean bent functions in eight variables, revisited

Alexandr Polujan[a], Luca Mariot[b], Stjepan Picek[c]

[a]Otto von Guericke University Magdeburg, Germany
[b]Semantics, Cybersecurity and Services Group, University of Twente, The Netherlands
[c]Digital Security Group, Radboud University, The Netherlands

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

Further Reading I

[Can+06] Anne Canteaut, Magnus Daum, Hans Dobbertin and Gregor Leander. "Finding nonnormal bent functions". In: *Discrete Applied Mathematics* 154.2 (2006). Coding and Cryptography, pp. 202–218. DOI: https://doi.org/10.1016/j.dam.2005.03.027 (cit. on pp. 14–18).

[Cha04] Pascale Charpin. "Normal Boolean functions". In: *Journal of Complexity* 20.2 (2004). Festschrift for Harald Niederreiter, Special Issue on Coding and Cryptography, pp. 245–265. DOI: https://doi.org/10.1016/j.jco.2003.08.010 (cit. on pp. 3–6, 10–13, 19–22, 29–31).

Further Reading II

[Dil74] J. F. Dillon. "Elementary Hadamard Difference Sets". PhD thesis. University of Maryland, 1974. DOI: https://doi.org/10.13016/M2MS3K194 (cit. on pp. 23–25).

[Dob95] Hans Dobbertin. "Construction of bent functions and balanced Boolean functions with high nonlinearity". In: *Fast Software Encryption*. Ed. by Bart Preneel. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 61–74. DOI: https://doi.org/10.1007/3-540-60590-8_5 (cit. on pp. 3–6).

Further Reading III

[GMP23] Maximilien Gadouleau, Luca Mariot and Stjepan Picek. "Bent functions in the partial spread class generated by linear recurring sequences". In: *Designs, Codes and Cryptography* 91.1 (Jan. 2023), pp. 63–82. DOI: https://doi.org/10.1007/s10623-022-01097-1 (cit. on pp. 33–35).

[Lan12] Philippe Langevin. "Classification of partial spread functions in eight variables". In: *Philippe Langevin's numerical project page*. 2012. URL: https://langevin.univ-tln.fr/project/spread/psp.html (cit. on pp. 26–28, 32).

Further Reading IV

[Lea05] Gregor Leander. "Normality of bent bunctions monomial- and binomial-bent functions". doctoralthesis. Ruhr-Universität Bochum, Universitätsbibliothek, 2005. URL: https://hss-opus.ub.ruhr-uni-bochum.de/opus4/frontdoor/index/index/year/2018/docId/413 (cit. on pp. 14–22).

[LH11] Philippe Langevin and Xiang-Dong Hou. "Counting Partial Spread Functions in Eight Variables". In: *IEEE Transactions on Information Theory* 57.4 (2011), pp. 2263–2269. DOI: https://doi.org10.1109/TIT.2011.2112230 (cit. on pp. 26–28).

Further Reading V

[LM09] Gregor Leander and Gary McGuire. "Construction of bent functions from near-bent functions". In: *Journal of Combinatorial Theory, Series A* 116.4 (2009), pp. 960–970. DOI: https://doi.org/10.1016/j.jcta.2008.12.004 (cit. on pp. 14–18).