Design-theoretic aspects of vectorial bent functions

Alexandr Polujan
joint work with Alexander Pott

Otto von Guericke University Magdeburg, Germany

KolKom 2019
Paderborn, Germany
November 9, 2019

Boolean and Vectorial Functions

- $\mathbb{F}_2 = \{0, 1\}$: Finite field with 2 elements.
- $\mathbb{F}_2^n$: Vector space over $\mathbb{F}_2$ of dimension n.
- We consider mappings $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$, particularly:
  - Single-output $(m = 1)$ case: Boolean functions.
  - Multi-output $(m \geq 2)$ case: Vectorial functions.
- We identify a vectorial function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ with m coordinate Boolean functions in the following way:

$$F(x_1, \dots, x_n) = \begin{pmatrix} f_1(x_1, \dots, x_n) \\ f_2(x_1, \dots, x_n) \\ \vdots \\ f_m(x_1, \dots, x_n) \end{pmatrix}.$$

- We are interested in bent = perfect nonlinear functions.

Boolean Bent Functions

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

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

has 2^{n-1} solutions for all $a \neq 0$ and any b.

Boolean Bent Functions

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

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

  has 2^{n-1} solutions for all $a \neq 0$ and any b.
- They exist if and only if n is even.

Boolean Bent Functions

- A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called bent if the equation
$$f(x + a) - f(x) = b$$
has 2^{n-1} solutions for all $a \neq 0$ and any b.
- They exist if and only if n is even.

Example 1

A function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2$, given by
$$f(x_1, \ldots, x_n) = x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$$
is bent.

Vectorial Bent Functions

- A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is vectorial bent if

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

has 2^{n-m} solutions for all $a \neq 0$ and all b.

Vectorial Bent Functions

- A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is vectorial bent if

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

  has 2^{n-m} solutions for all $a \neq 0$ and all b.
- They exist if and only if n is even and $m \leq n/2$.

Vectorial Bent Functions

- A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is vectorial bent if

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

has 2^{n-m} solutions for all $a \neq 0$ and all b.
- They exist if and only if n is even and $m \leq n/2$.
- Vectorial bent functions are m-dimensional vector spaces of Boolean bent functions.

Vectorial Bent Functions

- A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is vectorial bent if
$$f(x+a) - f(x) = b$$
has 2^{n-m} solutions for all $a \neq 0$ and all b.
- They exist if and only if n is even and $m \leq n/2$.
- Vectorial bent functions are m-dimensional vector spaces of Boolean bent functions.

Example 2 (The Maiorana-McFarland Construction)

A function $F\colon \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2} \to \mathbb{F}_2^m$, given by
$$F(x, y) := L(x \cdot \pi(y)) + G(y)$$
is vectorial bent if L is any affine function from $\mathbb{F}_2^{n/2}$ onto $\mathbb{F}_2^m$, π is an permutation of $\mathbb{F}_2^{n/2}$ and G is any function on $\mathbb{F}_2^{n/2}$.

Designs and Divisible Designs

- $\mathcal{P}$ is a set of points and $\mathcal{B}$ is a set of blocks.

Designs and Divisible Designs

- $\mathcal{P}$ is a set of points and $\mathcal{B}$ is a set of blocks.
- The pair $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is called a t-(v, k, λ) design, if:
  - $|\mathcal{P}| = v$;
  - $\mathcal{B}$ is a collection of k-subsets of $\mathcal{P}$;
  - Every t-subset of $\mathcal{P}$ is contained in exactly λ blocks of $\mathcal{B}$.

Designs and Divisible Designs

- $\mathcal{P}$ is a set of points and $\mathcal{B}$ is a set of blocks.
- The pair $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is called a t-(v, k, λ) design, if:
  - $|\mathcal{P}| = v$;
  - $\mathcal{B}$ is a collection of k-subsets of $\mathcal{P}$;
  - Every t-subset of $\mathcal{P}$ is contained in exactly λ blocks of $\mathcal{B}$.
- The pair $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is called a (μ, ν, k, λ) divisible design, if:
  - $|\mathcal{P}| = \mu \cdot \nu$, the point set is divided into μ point classes of size ν each;
  - $\mathcal{B}$ is a collection of k-subsets of $\mathcal{P}$;
  - Any two distinct points, which are not equivalent, are contained in exactly λ blocks;
  - Any two distinct points, which are equivalent, are not contained in a block.

I. Translation Designs of Bent Functions

- For a subset B of an additive group $(G,+)$ the development of B is an incidence structure $\mathrm{dev}(B) = (\mathcal{P}, \mathcal{B})$ with

$$\mathcal{P} = \{g\colon g \in G\} \quad \text{and} \quad \mathcal{B} = \{B_g\colon B_g = \{b + g : b \in B\}\}.$$

I. Translation Designs of Bent Functions

- For a subset B of an additive group $(G, +)$ the development of B is an incidence structure $\mathrm{dev}(B) = (\mathcal{P}, \mathcal{B})$ with

$$\mathcal{P} = \{g \colon g \in G\} \quad \text{and} \quad \mathcal{B} = \{B_g \colon B_g = \{b + g : b \in B\}\}.$$

- The graph $G_F \subset \mathbb{F}_2^{n+m}$ of a function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$, is the set

$$G_F := \begin{pmatrix} \dots & x & \dots \\ \dots & F(x) & \dots \end{pmatrix}_{x \in \mathbb{F}_2^n}.$$

I. Translation Designs of Bent Functions

- For a subset B of an additive group $(G,+)$ the development of B is an incidence structure $\mathrm{dev}(B)=(\mathcal{P},\mathcal{B})$ with

$$\mathcal{P}=\{g\colon g\in G\} \quad \text{and} \quad \mathcal{B}=\{B_g\colon B_g=\{b+g : b\in B\}\}.$$

- The graph $G_F\subset\mathbb{F}_2^{n+m}$ of a function $F\colon\mathbb{F}_2^n\to\mathbb{F}_2^m$, is the set

$$G_F:=\begin{pmatrix}\dots & x & \dots\\ \dots & F(x) & \dots\end{pmatrix}_{x\in\mathbb{F}_2^n}.$$

- Boolean bent case $f\colon\mathbb{F}_2^n\to\mathbb{F}_2$.
  $\mathrm{dev}(G_f)$ is a $\left(2^n,2^1,2^n,2^{n-1}\right)$ divisible design.

I. Translation Designs of Bent Functions

- For a subset B of an additive group $(G, +)$ the development of B is an incidence structure $\mathrm{dev}(B) = (\mathcal{P}, \mathcal{B})$ with

$$\mathcal{P} = \{g \colon g \in G\} \quad \text{and} \quad \mathcal{B} = \{B_g \colon B_g = \{b + g : b \in B\}\}.$$

- The graph $G_F \subset \mathbb{F}_2^{n+m}$ of a function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$, is the set

$$G_F := \begin{pmatrix} \dots & x & \dots \\ \dots & F(x) & \dots \end{pmatrix}_{x \in \mathbb{F}_2^n}.$$

- Boolean bent case $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$.
  $\mathrm{dev}(G_f)$ is a $\left(2^n, 2^1, 2^n, 2^{n-1}\right)$ divisible design.
- Vectorial bent case $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$.
  $\mathrm{dev}(G_F)$ is a $(2^n, 2^m, 2^n, 2^{n-m})$ divisible design.

II. Addition Designs of Bent Functions

- Consider a linear code $\mathcal{C}(F)$ with generator matrix, given by

$$\begin{pmatrix} 1 & \dots & 1 \\ \dots & x & \dots \\ \dots & F(x) & \dots \end{pmatrix}_{x \in \mathbb{F}_2^n} .$$

II. Addition Designs of Bent Functions

- Consider a linear code $\mathcal{C}(F)$ with generator matrix, given by

$$\begin{pmatrix} 1 & \dots & 1 \\ \dots & x & \dots \\ \dots & F(x) & \dots \end{pmatrix}_{x \in \mathbb{F}_2^n}.$$

- Design $\mathbb{D}(F) = (\mathcal{P}, \mathcal{B})$ is formed by words of minimum weight:

  $\mathcal{P} = \{x \colon x \in \mathbb{F}_2^n\}$ and $\mathcal{B} = \{\mathrm{supp}(f) \colon f \in \mathcal{C}(F), \mathrm{wt}(f) = w_{\min}\}$.

II. Addition Designs of Bent Functions

- Consider a linear code $\mathcal{C}(F)$ with generator matrix, given by

$$\begin{pmatrix} 1 & \dots & 1 \\ \dots & x & \dots \\ \dots & F(x) & \dots \end{pmatrix}_{x\in\mathbb{F}_2^n}.$$

- Design $\mathbb{D}(F) = (\mathcal{P}, \mathcal{B})$ is formed by words of minimum weight:

  $\mathcal{P} = \{x \colon x \in \mathbb{F}_2^n\}$ and $\mathcal{B} = \{\mathrm{supp}(f) \colon f \in \mathcal{C}(F), \mathrm{wt}(f) = w_{\min}\}$.

- For a bent function $w_{\min} = 2^{n-1} - 2^{n/2-1}$.

II. Addition Designs of Bent Functions

- Consider a linear code $\mathcal{C}(F)$ with generator matrix, given by

$$\begin{pmatrix} 1 & \dots & 1 \\ \dots & x & \dots \\ \dots & F(x) & \dots \end{pmatrix}_{x\in\mathbb{F}_2^n}.$$

- Design $\mathbb{D}(F) = (\mathcal{P}, \mathcal{B})$ is formed by words of minimum weight:

$\mathcal{P} = \{x \colon x \in \mathbb{F}_2^n\}$ and $\mathcal{B} = \{\mathrm{supp}(f) \colon f \in \mathcal{C}(F), \mathrm{wt}(f) = w_{\min}\}$.

- For a bent function $w_{\min} = 2^{n-1} - 2^{n/2-1}$.
- Boolean bent case $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$.
  $\mathbb{D}(f)$ is a 2-$(2^n, 2^{n-1} - 2^{n/2-1}, \lambda = 2^{n-2} - 2^{n/2-1})$ design.

II. Addition Designs of Bent Functions

- Consider a linear code $\mathcal{C}(F)$ with generator matrix, given by

$$\begin{pmatrix} 1 & \dots & 1 \\ \dots & x & \dots \\ \dots & F(x) & \dots \end{pmatrix}_{x \in \mathbb{F}_2^n}.$$

- Design $\mathbb{D}(F) = (\mathcal{P}, \mathcal{B})$ is formed by words of minimum weight:

$\mathcal{P} = \{x \colon x \in \mathbb{F}_2^n\}$ and $\mathcal{B} = \{\mathrm{supp}(f) \colon f \in \mathcal{C}(F), \mathrm{wt}(f) = w_{\min}\}$.

- For a bent function $w_{\min} = 2^{n-1} - 2^{n/2-1}$.
- Boolean bent case $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$.
  $\mathbb{D}(f)$ is a 2-$(2^n, 2^{n-1} - 2^{n/2-1}, \lambda = 2^{n-2} - 2^{n/2-1})$ design.
- Vectorial bent case $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$.
  $\mathbb{D}(F)$ is a 2-$(2^n, 2^{n-1} - 2^{n/2-1}, \lambda \cdot (2^m - 1))$ design.

Equivalence of Functions and Isomorphism of Designs

- Functions $F, F' \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ are EA-equivalent $F \overset{\mathsf{EA}}{\sim} F'$, if $\exists$ affine permutations $\mathcal{L}_1$ of $\mathbb{F}_2^n$ and $\mathcal{L}_2$ of $\mathbb{F}_2^m$, s.t.

$$F = \mathcal{L}_2 \circ F' \circ \mathcal{L}_1.$$

Equivalence of Functions and Isomorphism of Designs

- Functions $F, F' \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ are EA-equivalent $F \overset{\mathsf{EA}}{\sim} F'$, if $\exists$ affine permutations $\mathcal{L}_1$ of $\mathbb{F}_2^n$ and $\mathcal{L}_2$ of $\mathbb{F}_2^m$, s.t.

$$F = \mathcal{L}_2 \circ F' \circ \mathcal{L}_1.$$

- Designs $\mathcal{D}$ and $\mathcal{D}'$ with incidence matrices M and M' are isomorphic $\mathcal{D} \cong \mathcal{D}'$, if $\exists$ permutation matrices P_1 and P_2, s.t.

$$M = P_2 \ M' \ P_1.$$

Equivalence of Functions and Isomorphism of Designs

- Functions $F, F' \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ are EA-equivalent $F \overset{\text{EA}}{\sim} F'$, if $\exists$ affine permutations $\mathcal{L}_1$ of $\mathbb{F}_2^n$ and $\mathcal{L}_2$ of $\mathbb{F}_2^m$, s.t.

$$F = \mathcal{L}_2 \circ F' \circ \mathcal{L}_1.$$

- Designs $\mathcal{D}$ and $\mathcal{D}'$ with incidence matrices M and M' are isomorphic $\mathcal{D} \cong \mathcal{D}'$, if $\exists$ permutation matrices P_1 and P_2, s.t.

$$M = P_2 \; M' \; P_1.$$

- Main Question: Does isomorphism of translation and addition designs coincide with EA-equivalence of bent functions?

EA-Equivalence and Isomorphism of Designs

Result 1 (Folklore)

Let $F, F' \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be bent. $F \overset{\mathsf{EA}}{\sim} F' \Rightarrow \operatorname{dev}(G_F) \cong \operatorname{dev}(G_{F'})$.

EA-Equivalence and Isomorphism of Designs

Result 1 (Folklore)

Let $F, F' \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be bent. $F \overset{\mathsf{EA}}{\sim} F' \Rightarrow \operatorname{dev}(G_F) \cong \operatorname{dev}(G_{F'})$.

- Boolean bent case: $f \overset{\mathsf{EA}}{\sim} f' \not\Leftarrow \operatorname{dev}(G_f) \cong \operatorname{dev}(G_{f'})$.
- Vectorial bent case: $F \overset{\mathsf{EA}}{\sim} F' \overset{?}{\Leftarrow} \operatorname{dev}(G_F) \cong \operatorname{dev}(G_{F'})$.

EA-Equivalence and Isomorphism of Designs

Result 1 (Folklore)

Let $F, F' \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be bent. $F \overset{\text{EA}}{\sim} F' \Rightarrow \operatorname{dev}(G_F) \cong \operatorname{dev}(G_{F'})$.

- Boolean bent case: $f \overset{\text{EA}}{\sim} f' \not\Leftarrow \operatorname{dev}(G_f) \cong \operatorname{dev}(G_{f'})$.
- Vectorial bent case: $F \overset{\text{EA}}{\sim} F' \overset{?}{\Leftarrow} \operatorname{dev}(G_F) \cong \operatorname{dev}(G_{F'})$.

Result 2 (Kantor 1983; Dillon and Schatz 1987; Bending 1993)

Let $f, f' \colon \mathbb{F}_2^n \to \mathbb{F}_2$ be Boolean bent. $f \overset{\text{EA}}{\sim} f' \iff \mathbb{D}(f) \cong \mathbb{D}(f')$.

EA-Equivalence and Isomorphism of Designs

Result 1 (Folklore)

Let $F, F' \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be bent. $F \overset{\mathsf{EA}}{\sim} F' \Rightarrow \mathrm{dev}(G_F) \cong \mathrm{dev}(G_{F'})$.

- Boolean bent case: $f \overset{\mathsf{EA}}{\sim} f' \not\Leftarrow \mathrm{dev}(G_f) \cong \mathrm{dev}(G_{f'})$.
- Vectorial bent case: $F \overset{\mathsf{EA}}{\sim} F' \overset{?}{\Leftarrow} \mathrm{dev}(G_F) \cong \mathrm{dev}(G_{F'})$.

Result 2 (Kantor 1983; Dillon and Schatz 1987; Bending 1993)

Let $f, f' \colon \mathbb{F}_2^n \to \mathbb{F}_2$ be Boolean bent. $f \overset{\mathsf{EA}}{\sim} f' \iff \mathbb{D}(f) \cong \mathbb{D}(f')$.

- Boolean bent case: Were introduced by Kantor in 1975.
- Vectorial bent case: Were introduced by Ding, Munemasa and Tonchev in 2019.

EA-Equivalence and Isomorphism of Designs

Result 1 (Folklore)

Let $F, F' \colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be bent. $F \overset{\text{EA}}{\sim} F' \Rightarrow \operatorname{dev}(G_F) \cong \operatorname{dev}(G_{F'})$.

- Boolean bent case: $f \overset{\text{EA}}{\sim} f' \not\Leftarrow \operatorname{dev}(G_f) \cong \operatorname{dev}(G_{f'})$.
- Vectorial bent case: $F \overset{\text{EA}}{\sim} F' \overset{?}{\Leftarrow} \operatorname{dev}(G_F) \cong \operatorname{dev}(G_{F'})$.

Result 2 (Kantor 1983; Dillon and Schatz 1987; Bending 1993)

Let $f, f' \colon \mathbb{F}_2^n \to \mathbb{F}_2$ be Boolean bent. $f \overset{\text{EA}}{\sim} f' \iff \mathbb{D}(f) \cong \mathbb{D}(f')$.

- Boolean bent case: Were introduced by Kantor in 1975.
- Vectorial bent case: Were introduced by Ding, Munemasa and Tonchev in 2019.
- Vectorial bent case: $F \overset{\text{EA}}{\sim} F' \overset{?}{\iff} \mathbb{D}(F) \cong \mathbb{D}(F')$.

Two Problems: Boolean vs. Vectorial Case

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	?

Two Problems: Boolean vs. Vectorial Case

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Conjecture Yes, for all even n

1. The conjecture of Ding, Munemasa and Tonchev 2019.
   Addition designs of Boolean and vectorial bent functions behave in the same way.

Two Problems: Boolean vs. Vectorial Case

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Conjecture Yes, for all even n

1. The conjecture of Ding, Munemasa and Tonchev 2019.
   Addition designs of Boolean and vectorial bent functions behave in the same way.
2. Translation designs of vectorial bent functions.
   Nothing is known for $n \geq 6$.

Two Problems: Boolean vs. Vectorial Case

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Yes, for all even n

1. The conjecture of Ding, Munemasa and Tonchev 2019.
   Addition designs of Boolean and vectorial bent functions behave in the same way. ✓
2. Translation designs of vectorial bent functions.
   Nothing is known for $n \geq 6$.

Two Problems: Boolean vs. Vectorial Case

<table>
<tr><th>Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?</th><th>Translation Designs $\mathrm{dev}(G_F)$</th><th>Addition Designs $\mathbb{D}(F)$</th></tr>
<tr><td>$m = 1$: Boolean case</td><td>No, isomorphism is more general for all $n \geq 6$</td><td rowspan="2">Yes, for all even n</td></tr>
<tr><td>$m \geq 2$: Vectorial case</td><td>?</td></tr>
</table>

1. The conjecture of Ding, Munemasa and Tonchev 2019.
   Addition designs of Boolean and vectorial bent functions behave in the same way. ✓
2. Translation designs of vectorial bent functions.
   Nothing is known for $n \geq 6$.

Two Problems: Boolean vs. Vectorial Case

<table>
<tr><th>Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?</th><th>Translation Designs $\mathrm{dev}(G_F)$</th><th>Addition Designs $\mathbb{D}(F)$</th></tr>
<tr><td>$m = 1$: Boolean case</td><td>No, isomorphism is more general for all $n \geq 6$</td><td rowspan="2">Yes, for all even n</td></tr>
<tr><td>$m \geq 2$: Vectorial case</td><td>Yes, for $n = 6$</td></tr>
</table>

1. The conjecture of Ding, Munemasa and Tonchev 2019.
   Addition designs of Boolean and vectorial bent functions behave in the same way. ✓
2. Translation designs of vectorial bent functions.
   Nothing is known for $n \geq 6$. ✓

1. The Conjecture of Ding, Munemasa and Tonchev 2019

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Conjecture Yes, for all even n

1. The Conjecture of Ding, Munemasa and Tonchev 2019

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Conjecture Yes, for all even n

- Functions $F, F'\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ are called CCZ-equivalent, if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ s.t. $\mathcal{L}(G_F) = G_{F'}$.

1. The Conjecture of Ding, Munemasa and Tonchev 2019

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Conjecture Yes, for all even n

- Functions $F, F'\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ are called CCZ-equivalent, if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ s.t. $\mathcal{L}(G_F) = G_{F'}$.
- CCZ-equivalence is code equivalence.

1. The Conjecture of Ding, Munemasa and Tonchev 2019

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Conjecture Yes, for all even n

- Functions $F, F'\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ are called CCZ-equivalent, if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ s.t. $\mathcal{L}(G_F) = G_{F'}$.
- CCZ-equivalence is code equivalence.

$F \overset{\text{CCZ}}{\sim} F' \quad \Longleftrightarrow \quad \mathcal{C}(F) \overset{\text{code}}{\sim} \mathcal{C}(F')$ Dillon, B., K., M. 2009

1. The Conjecture of Ding, Munemasa and Tonchev 2019

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Conjecture Yes, for all even n

- Functions $F, F'\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ are called CCZ-equivalent, if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ s.t. $\mathcal{L}(G_F) = G_{F'}$.
- CCZ-equivalence is code equivalence.

$$F \overset{\text{CCZ}}{\sim} F' \iff \mathcal{C}(F) \overset{\text{code}}{\sim} \mathcal{C}(F') \quad \text{Dillon, B., K., M. 2009}$$

$$\underset{F,F' \text{ are bent}}{\iff} \mathbb{D}(F) \cong \mathbb{D}(F') \quad \text{Ding, M., T. 2019}$$

1. The Conjecture of Ding, Munemasa and Tonchev 2019

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Conjecture Yes, for all even n

- Functions $F, F'\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ are called CCZ-equivalent, if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_2^n \times \mathbb{F}_2^m$ s.t. $\mathcal{L}(G_F) = G_{F'}$.
- CCZ-equivalence is code equivalence.

$$F \overset{\text{CCZ}}{\sim} F' \iff \mathcal{C}(F) \overset{\text{code}}{\sim} \mathcal{C}(F')$$ Dillon, B., K., M. 2009

$$\overset{F,F'\text{ are bent}}{\iff} \mathbb{D}(F) \cong \mathbb{D}(F')$$ Ding, M., T. 2019

$$F \overset{\text{CCZ}}{\sim} F' \overset{F,F'\text{ are bent}}{\iff} F \overset{\text{EA}}{\sim} F'$$ Budaghyan, Carlet 2009

The Conjecture is True

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Yes, for all even n

The Conjecture is True

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Yes, for all even n

Theorem 1

Let $F, F'\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be vectorial bent. Then $F \overset{\mathsf{EA}}{\sim} F'$ iff their addition designs $\mathbb{D}(F) \cong \mathbb{D}(F')$.

The Conjecture is True

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	

Theorem 1

Let $F, F'\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be vectorial bent. Then $F \overset{\mathsf{EA}}{\sim} F'$ iff their addition designs $\mathbb{D}(F) \cong \mathbb{D}(F')$.

The Conjecture is True

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	

Theorem 1

Let $F, F'\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ be vectorial bent. Then $F \overset{\mathsf{EA}}{\sim} F'$ iff their addition designs $\mathbb{D}(F) \cong \mathbb{D}(F')$.

- A technical proof: see the thesis of Bending 1993.

2. Translation Designs of Vectorial Bent Functions

<table>
<tr><th>Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?</th><th>Translation Designs $\mathrm{dev}(G_F)$</th><th>Addition Designs $\mathbb{D}(F)$</th></tr>
<tr><td>$m = 1$: Boolean case</td><td>No, isomorphism is more general for all $n \geq 6$</td><td rowspan="2">Yes, for all even n</td></tr>
<tr><td>$m \geq 2$: Vectorial case</td><td>?</td></tr>
</table>

2. Translation Designs of Vectorial Bent Functions

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	

- All Boolean bent functions in 6 variables form:

2. Translation Designs of Vectorial Bent Functions

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	

- All Boolean bent functions in 6 variables form:
  - 4 EA-equivalence classes;
  - 3 Non-isomorphic designs $\mathrm{dev}(G_f)$.

2. Translation Designs of Vectorial Bent Functions

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	

- All Boolean bent functions in 6 variables form:
  - 4 EA-equivalence classes;
  - 3 Non-isomorphic designs $\mathrm{dev}(G_f)$.
- Example (Kholosha and Pott 2013)

$$x_1x_4 + x_2x_5 + x_3x_6 \quad \text{and} \quad x_1x_4 + x_2x_5 + x_3x_6 + x_4x_5x_6.$$

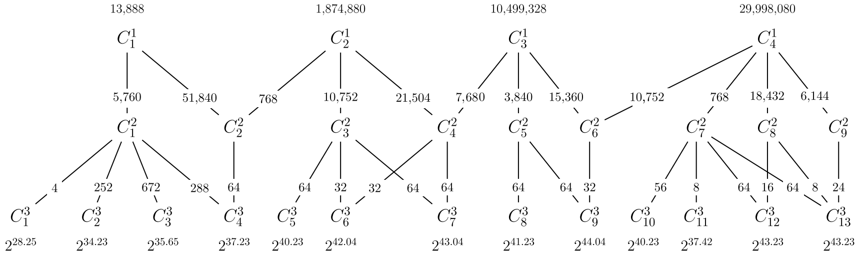
2. Translation Designs of Vectorial Bent Functions

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	

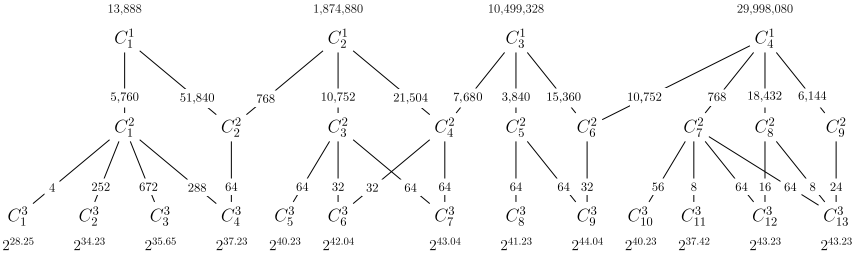
- All Boolean bent functions in 6 variables form:
  - 4 EA-equivalence classes;
  - 3 Non-isomorphic designs $\mathrm{dev}(G_f)$.
- Example (Kholosha and Pott 2013)

  $x_1x_4 + x_2x_5 + x_3x_6$ and $x_1x_4 + x_2x_5 + x_3x_6 + x_4x_5x_6$.
- Problem: The classification of vectorial bent functions in 6 variables is not known.

Classification and Count of Vectorial Bent Functions on $\mathbb{F}_2^6$

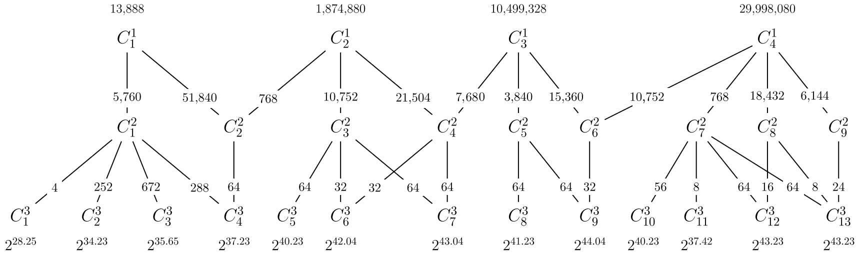


Classification and Count of Vectorial Bent Functions on $\mathbb{F}_2^6$



(n, m)	# of Bent Functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$	# of EA-eq. Classes	# of Isom. Classes
$(6,1)$	$5{,}425{,}430{,}528 \approx 2^{32.33}$	4	3
$(6,2)$	$23{,}392{,}233{,}361{,}244{,}160 \approx 2^{54.37}$	9	9
$(6,3)$	$121{,}282{,}113{,}886{,}947{,}901{,}440 \approx 2^{66.71}$	13	13

Classification and Count of Vectorial Bent Functions on $\mathbb{F}_2^6$



(n, m)	# of Bent Functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$	# of EA-eq. Classes	# of Isom. Classes
$(6,1)$	$5{,}425{,}430{,}528 \approx 2^{32.33}$	4	3
$(6,2)$	$23{,}392{,}233{,}361{,}244{,}160 \approx 2^{54.37}$	9	9
$(6,3)$	$121{,}282{,}113{,}886{,}947{,}901{,}440 \approx 2^{66.71}$	13	13

Theorem 2

Let F, F' be vectorial bent functions in 6 variables. Then $F \overset{\text{EA}}{\sim} F'$ iff $\operatorname{dev}(G_F) \cong \operatorname{dev}(G_{F'})$.

Conclusion and Future Work

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	?	Yes, for all even n

Conclusion and Future Work

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	Yes, for $n = 6$	

Conclusion and Future Work

Does isomorphism of designs coincide with EA-equivalence for bent functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$?	Translation Designs $\mathrm{dev}(G_F)$	Addition Designs $\mathbb{D}(F)$
$m = 1$: Boolean case	No, isomorphism is more general for all $n \geq 6$	Yes, for all even n
$m \geq 2$: Vectorial case	Conjecture Yes, for all even $n \geq 6$	

Open Problem 1

Attack the conjecture!

Design-theoretic aspects of vectorial bent functions

Alexandr Polujan
joint work with Alexander Pott

Otto von Guericke University Magdeburg, Germany

KolKom 2019
Paderborn, Germany
November 9, 2019

Further Reading I

[BC09] Lilya Budaghyan and Claude Carlet. "CCZ-equivalence and Boolean functions". In: 2009 (Jan. 2009), p. 63 (cit. on pp. 36–41).

[Ben93] Th. D. Bending. "Bent Functions, SDP Designs and their Automorphism Groups". PhD thesis. Queen Mary and Westfield College, Nov. 1993 (cit. on pp. 25–29, 42–45).

[Bro+09] K. A. Browning, J. F. Dillon, R. E. Kibler and M. T. McQuistan. "APN polynomials and related codes". In: *Special volume of Journal of Combinatorics, Information and System Sciences* 34 (2009), pp. 135–159 (cit. on pp. 36–41).

Further Reading II

[DMT19] C. Ding, A. Munemasa and V. D. Tonchev. "Bent Vectorial Functions, Codes and Designs". In: *IEEE Transactions on Information Theory* (2019). DOI: 10.1109/TIT.2019.2922401 (cit. on pp. 25–41).

[JJ87] J.F.Dillon and J.R.Schatz. "Block designs with the symmetric difference property". In: *R.L. Ward (Ed.), Proc. NSA Mathematical Sciences Meetings, U.S. Government Printing Office, Washington, DC* (1987), pp. 159–164 (cit. on pp. 25–29).

[Kan75] William M Kantor. "Symplectic groups, symmetric designs, and line ovals". In: *Journal of Algebra* 33.1 (1975), pp. 43–58. ISSN: 0021-8693. DOI: http://dx.doi.org/10.1016/0021-8693(75)90130-1 (cit. on pp. 25–29).

Further Reading III

[Kan83] William M. Kantor. "Exponential Numbers of Two-weight Codes, Difference Sets and Symmetric Designs". In: *Discrete Math.* 46.1 (Jan. 1983), pp. 95–98. DOI: http://dx.doi.org/10.1016/0012-365X(83)90276-5 (cit. on pp. 25–29).

[KP13] Alexander Kholosha and Alexander Pott. "Bent and related functions". In: *Handbook of Finite Fields.* Ed. by Gary L. Mullen and Daniel Panario. 1st. Chapman & Hall/CRC, 2013, pp. 262–273. DOI: https://doi.org/10.1201/b15006 (cit. on pp. 46–50).