A Code-Based Perspective on the Classification of APN Functions

Clémence Bouvier

Université de Lorraine, CNRS, Inria, LORIA

(on-going work with Jules Baudrin and Christophe Levrat)

Journées Au Vert, Saint-Dié-des-Vosges, France
March 12th, 2026

A bit of motivation

Symmetric Cryptography

- ⋆ Vectorial Boolean functions

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$$

classified up to equivalences

- ⋆ preserve cryptographic properties
  - ⋆ differential properties
  - ⋆ linear properties
  - ⋆ ...

A bit of motivation

Symmetric Cryptography

- ⋆ Vectorial Boolean functions

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$$

classified up to equivalences

- ⋆ preserve cryptographic properties
  - ⋆ differential properties
  - ⋆ linear properties
  - ⋆ ...

Coding Theory

- ⋆ Linear binary codes

$$\mathcal{C} \subseteq \mathbb{F}_2^n$$

classified up to equivalences

- ⋆ preserve coding properties
  - ⋆ minimum distance
  - ⋆ dimension
  - ⋆ ...

A bit of motivation

Symmetric Cryptography

- ⋆ Vectorial Boolean functions

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$$

classified up to equivalences

- ⋆ preserve cryptographic properties
  - ⋆ differential properties
  - ⋆ linear properties
  - ⋆ ...

Coding Theory

- ⋆ Linear binary codes

$$\mathcal{C} \subseteq \mathbb{F}_2^n$$

classified up to equivalences

- ⋆ preserve coding properties
  - ⋆ minimum distance
  - ⋆ dimension
  - ⋆ ...

The graph of a function is the fundamental object linking both worlds.

Linearity

Linearity

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function, then

$$\mathcal{W}_F = \max_{u,v \neq 0} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot F(x)} \right|$$

Linearity

Linearity

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function, then

$$\mathcal{W}_F = \max_{u,v \neq 0} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot F(x)} \right|$$

This quantity must be low!

Linearity

Linearity

Let $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function, then

$$\mathcal{W}_{\mathsf{F}} = \max_{u,v \neq 0} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{u \cdot x + v \cdot \mathsf{F}(x)} \right|$$

This quantity must be low!

Examples:

- If $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto Lx + c$, then
$$\mathcal{W}_{\mathsf{F}} = 2^n \ .$$
- If $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto x^{-1}$, with n even, then
$$\mathcal{W}_{\mathsf{F}} = 2^{n/2+1} \ .$$

Differential Uniformity

Differential uniformity

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function, then

$$\delta_F = \max_{a \neq 0, b} \delta_F(a, b) ,$$

where

$$\delta_F(a, b) = |\{x \in \mathbb{F}_2^n, F(x + a) + F(x) = b\}| .$$

Differential Uniformity

Differential uniformity

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function, then

$$\delta_F = \max_{a \neq 0, b} \delta_F(a, b) ,$$

where

$$\delta_F(a, b) = |\{x \in \mathbb{F}_2^n, F(x + a) + F(x) = b\}| .$$

This quantity must be low!

Differential Uniformity

Differential uniformity

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be a function, then

$$\delta_F = \max_{a \neq 0, b} \delta_F(a, b) ,$$

where

$$\delta_F(a, b) = |\{x \in \mathbb{F}_2^n, F(x + a) + F(x) = b\}| .$$

This quantity must be low!

Examples:

- If $F : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto c \cdot x$, then
$$\delta_F = 2^n .$$
- If $F : \mathbb{F}_2^n \to \mathbb{F}_2^n, x \mapsto x^{-1}$, then
$$\delta_F = \begin{cases} 4 & \text{if } n \text{ is even} \\ 2 & \text{if } n \text{ is odd} \end{cases} .$$

APN functions

Note that δ_F is always even:

- $\forall\ a, \exists\ b$ s.t. $\delta_F(a, b) > 0$
- $\forall\ a \neq 0$, x is a solution iff $x + a$ is a solution.

APN functions

Note that δ_F is always even:

- $\star$ $\forall\ a, \exists\ b$ s.t. $\delta_F(a, b) > 0$
- $\star$ $\forall\ a \neq 0$, x is a solution iff $x + a$ is a solution.

APN (Almost Perfect Non-linear) functions

A function F is APN if for all $a \neq 0$ and b, we have $\delta_F = 2$.

APN functions

Note that δ_F is always even:

- $\forall\ a, \exists\ b$ s.t. $\delta_F(a, b) > 0$
- $\forall\ a \neq 0$, x is a solution iff $x + a$ is a solution.

APN (Almost Perfect Non-linear) functions

A function F is APN if for all $a \neq 0$ and b, we have $\delta_F = 2$.

Simple definition but hard to

- find new instances
- classify known instances

Big APN problem

Find a permutation $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ which is APN, for an even n.

Linear and Affine Equivalence

Linear equivalence

Two functions $\mathsf{F}_1, \mathsf{F}_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are linear equivalent if there exist linear permutations A, B s.t.

$$\mathsf{F}_2 = A \circ \mathsf{F}_1 \circ B \ .$$

Linear and Affine Equivalence

Linear equivalence

Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are linear equivalent if there exist linear permutations A, B s.t.

$$F_2 = A \circ F_1 \circ B \ .$$

Example: Let $F_1 : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}, x \mapsto x^3$ and $F_2 : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}, x \mapsto x^5$.

$$F_2(x) = (A \circ F_1 \circ B)(x) \quad \text{where } A(x) = x^2 \text{ and } B(x) = x \ ,$$

implying that $F_1 \sim_{\text{lin}} F_2$.

Linear and Affine Equivalence

Linear equivalence

Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are linear equivalent if there exist linear permutations A, B s.t.

$$F_2 = A \circ F_1 \circ B \ .$$

Example: Let $F_1 : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}, x \mapsto x^3$ and $F_2 : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}, x \mapsto x^5$.

$$F_2(x) = (A \circ F_1 \circ B)(x) \quad \text{where } A(x) = x^2 \text{ and } B(x) = x \ ,$$

implying that $F_1 \sim_{\text{lin}} F_2$.

A and B are not unique!

Linear and Affine Equivalence

Linear equivalence

Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are linear equivalent if there exist linear permutations A, B s.t.

$$F_2 = A \circ F_1 \circ B \ .$$

Example: Let $F_1 : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}, x \mapsto x^3$ and $F_2 : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}, x \mapsto x^5$.

$$F_2(x) = (A \circ F_1 \circ B)(x) \quad \text{where } A(x) = x^2 \text{ and } B(x) = x \ ,$$

implying that $F_1 \sim_{\text{lin}} F_2$.

A and B are not unique!

Affine equivalence

Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are affine equivalent if there exist affine permutations A, B s.t.

$$F_2 = A \circ F_1 \circ B \ .$$

Extended Linear and Affine Equivalence

Extended-Linear equivalence

Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are EL-equivalent if there exist linear permutations A, B and a linear map C s.t.

$$F_2 = A \circ F_1 \circ B + C \ .$$

Extended Linear and Affine Equivalence

Extended-Linear equivalence

Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are EL-equivalent if there exist linear permutations A, B and a linear map C s.t.

$$F_2 = A \circ F_1 \circ B + C \ .$$

Extended-Affine equivalence

Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are EA-equivalent if there exist affine permutations A, B and an affine map C s.t.

$$F_2 = A \circ F_1 \circ B + C \ .$$

Extended Linear and Affine Equivalence

Extended-Linear equivalence

Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are EL-equivalent if there exist linear permutations A, B and a linear map C s.t.

$$F_2 = A \circ F_1 \circ B + C \ .$$

Extended-Affine equivalence

Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are EA-equivalent if there exist affine permutations A, B and an affine map C s.t.

$$F_2 = A \circ F_1 \circ B + C \ .$$

Preserved properties under linear, affine, EL, and EA equivalences:

- ⋆ differential spectrum
- ⋆ Walsh spectrum
- ⋆ algebraic degree
- ⋆ ...

CCZ-equivalence

Inversion

$$\Gamma_F = \{(x, F(x)), x \in \mathbb{F}_2^n\} \quad \text{and} \quad \Gamma_{F^{-1}} = \left\{\left(y, F^{-1}(y)\right), y \in \mathbb{F}_2^n\right\}$$

Noting that

$$\Gamma_F = \left\{\left(F^{-1}(y), y\right), y \in \mathbb{F}_2^n\right\} ,$$

then, we have:

$$\Gamma_F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Gamma_{F^{-1}} .$$

CCZ-equivalence

Inversion

$$\Gamma_F = \{(x, F(x)), x \in \mathbb{F}_2^n\} \quad \text{and} \quad \Gamma_{F^{-1}} = \left\{\left(y, F^{-1}(y)\right), y \in \mathbb{F}_2^n\right\}$$

Noting that

$$\Gamma_F = \left\{\left(F^{-1}(y), y\right), y \in \mathbb{F}_2^n\right\} ,$$

then, we have:

$$\Gamma_F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Gamma_{F^{-1}} .$$

CCZ equivalence [Carlet, Charpin and Zinoviev, DCC98]

Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are CCZ-equivalent if there exists an affine permutation $\mathcal{A}$ s.t.

$$\Gamma_{F_2} = \mathcal{A}(\Gamma_{F_1}) .$$

CCZ-equivalence

Inversion

$$\Gamma_F = \{(x, F(x)), x \in \mathbb{F}_2^n\} \quad \text{and} \quad \Gamma_{F^{-1}} = \left\{\left(y, F^{-1}(y)\right), y \in \mathbb{F}_2^n\right\}$$

Noting that

$$\Gamma_F = \left\{\left(F^{-1}(y), y\right), y \in \mathbb{F}_2^n\right\} ,$$

then, we have:

$$\Gamma_F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Gamma_{F^{-1}} .$$

CCZ equivalence [Carlet, Charpin and Zinoviev, DCC98]

Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are CCZ-equivalent if there exists an affine permutation $\mathcal{A}$ s.t.

$$\Gamma_{F_2} = \mathcal{A}(\Gamma_{F_1}) .$$

The degree is not preserved!

Summary of Equivalences

Functions equivalence

Let $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be two CCZ equivalent functions i.e. $\mathcal{A}(\Gamma_{F_1}) = \Gamma_{F_2}$.
Let $\mathcal{L}$ be the linear part of $\mathcal{A}$, i.e. $\mathcal{L} : x \mapsto \mathcal{A}(x) + \mathcal{A}(0)$ with:

$$\mathcal{L} = \begin{pmatrix} A & D \\ C & B \end{pmatrix} .$$

The functions F_1 and F_2 are said to be:

- ⋆ EA equivalent if $D = 0$ (and EL equivalent if $\mathcal{A}(0) = 0$).
- ⋆ affine equivalent if $D = C = 0$ (and linear equivalent if $\mathcal{A}(0) = 0$).

Summary of Equivalences

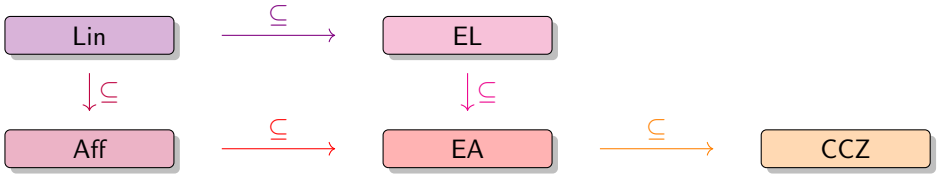
Functions equivalence

Let $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$ be two CCZ equivalent functions i.e. $\mathcal{A}(\Gamma_{F_1}) = \Gamma_{F_2}$.
Let $\mathcal{L}$ be the linear part of $\mathcal{A}$, i.e. $\mathcal{L} : x \mapsto \mathcal{A}(x) + \mathcal{A}(0)$ with:

$$\mathcal{L} = \begin{pmatrix} A & D \\ C & B \end{pmatrix} .$$

The functions F_1 and F_2 are said to be:

- ⋆ EA equivalent if $D = 0$ (and EL equivalent if $\mathcal{A}(0) = 0$).
- ⋆ affine equivalent if $D = C = 0$ (and linear equivalent if $\mathcal{A}(0) = 0$).



Algorithmic PoV

Decisional Problem

- ⋆ **Input:** Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$
- ⋆ **Output:** Are $F_1 \sim_{ccz} F_2$?

How? Search for invariants

- ⋆ differential spectrum
- ⋆ Walsh spectrum
- ⋆ ...

Algorithmic PoV

Decisional Problem

- ⋆ **Input:** Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$
- ⋆ **Output:** Are $F_1 \sim_{ccz} F_2$?

How? Search for invariants

- ⋆ differential spectrum
- ⋆ Walsh spectrum
- ⋆ ...

Necessary but not sufficient...

Computational Problem

- ⋆ **Input:** Two functions $F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^m$
- ⋆ **Output:** If $F_1 \sim_{ccz} F_2$, find $\mathcal{A}$ s.t. $\mathcal{A}(\Gamma_{F_1}) = \Gamma_{F_2}$.

Codes

Code

A $[n, k]$ binary linear code $\mathcal{C}$ is a vector subspace of $\mathbb{F}_2^n$, where

- $\star$ n is the length, i.e. the number of bits of a code word
- $\star$ k is the dimension, i.e. $|\mathcal{C}| = 2^k$

Codes

Code

A $[n, k]$ binary linear code $\mathcal{C}$ is a vector subspace of $\mathbb{F}_2^n$, where

- $\star$ n is the length, i.e. the number of bits of a code word
- $\star$ k is the dimension, i.e. $|\mathcal{C}| = 2^k$

Generating matrix

A generating matrix of $\mathcal{C}$ is a $k \times n$-dimensional matrix whose rows form a basis of $\mathcal{C}$.

Example:

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

G is a generating matrix for $\mathcal{C} = \{000, 011, 101, 110\}$.
The code is of length $n = 3$ and dimension $k = 2$.

Weights and distances

Weight

Let $c \in \mathcal{C} \subseteq \mathbb{F}_2^n$. The weight of c is

$$\mathrm{wt}(c) = |\{c_i \neq 0, c = (c_1, \ldots, c_n)\}| \ .$$

Minimum distance

The minimum distance of a code $\mathcal{C}$ is:

$$d = \min_{c \neq 0 \in \mathcal{C}} \mathrm{wt}(c)$$

Weights and distances

Weight

Let $c \in \mathcal{C} \subseteq \mathbb{F}_2^n$. The weight of c is

$$\mathrm{wt}(c) = |\{c_i \neq 0, c = (c_1, \ldots, c_n)\}| \ .$$

Minimum distance

The minimum distance of a code $\mathcal{C}$ is:

$$d = \min_{c \neq 0 \in \mathcal{C}} \mathrm{wt}(c)$$

We want d to be large...

Singleton Bound

Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ be a $[n, k]$ linear code. Then

$$d \leq n - k + 1 \ .$$

Equivalence of Codes

Code equivalence

Let $\mathcal{C}_1, \mathcal{C}_2$ be two $[n, k]$ binary linear codes.
$\mathcal{C}_1 \sim \mathcal{C}_2$ if there exists a permutation π of $\{1, \dots, n\}$ s.t.

$$\forall\ (c_1, \dots, c_n) \in \mathbb{F}_2^n, \quad (c_1, \dots, c_n) \in \mathcal{C}_1 \iff (c_{\pi(1)}, \dots, c_{\pi(n)}) \in \mathcal{C}_2\ .$$

Equivalence of Codes

Code equivalence

Let $\mathcal{C}_1, \mathcal{C}_2$ be two $[n, k]$ binary linear codes.
$\mathcal{C}_1 \sim \mathcal{C}_2$ if there exists a permutation π of $\{1, \dots, n\}$ s.t.

$$\forall\ (c_1, \dots, c_n) \in \mathbb{F}_2^n, \quad (c_1, \dots, c_n) \in \mathcal{C}_1 \iff (c_{\pi(1)}, \dots, c_{\pi(n)}) \in \mathcal{C}_2\ .$$

Code equivalence

Let $G_1, G_2 \in \mathbb{F}_2^{k \times n}$ be generating matrices of $\mathcal{C}_1, \mathcal{C}_2$.
$\mathcal{C}_1 \sim \mathcal{C}_2$ if there exists an invertible matrix M and a permutation matrix P s.t.

$$M \cdot G_1 \cdot P = G_2\ .$$

Equivalence of Codes

Code equivalence

Let $\mathcal{C}_1, \mathcal{C}_2$ be two $[n, k]$ binary linear codes.
$\mathcal{C}_1 \sim \mathcal{C}_2$ if there exists a permutation π of $\{1, \dots, n\}$ s.t.

$$\forall\ (c_1, \dots, c_n) \in \mathbb{F}_2^n, \quad (c_1, \dots, c_n) \in \mathcal{C}_1 \iff (c_{\pi(1)}, \dots, c_{\pi(n)}) \in \mathcal{C}_2\ .$$

Code equivalence

Let $G_1, G_2 \in \mathbb{F}_2^{k \times n}$ be generating matrices of $\mathcal{C}_1, \mathcal{C}_2$.
$\mathcal{C}_1 \sim \mathcal{C}_2$ if there exists an invertible matrix M and a permutation matrix P s.t.

$$M \cdot G_1 \cdot P = G_2\ .$$

Preserved properties under code equivalence:

- ⋆ weight distribution
- ⋆ minimum distance
- ⋆ ...

Link

Idea: to a function F, associate a code $\mathcal{C}_F$ constructed from its graph Γ_F.

Link

Idea: to a function F, associate a code $\mathcal{C}_{\mathsf{F}}$ constructed from its graph Γ_{F}.

Link equivalence codes and functions

For any $\mathsf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$, let

$$G_{\mathsf{ccz}}(\mathsf{F}) = \begin{pmatrix} 1 \\ x \\ \mathsf{F}(x) \end{pmatrix}_{x \in \mathbb{F}_2^n}, G_{\mathsf{ea}}(\mathsf{F}) = \begin{pmatrix} 1 & 0 \\ x & 0 \\ \mathsf{F}(x) & y \end{pmatrix}_{\substack{x \in \mathbb{F}_2^n \\ y \in \mathbb{F}_2^m \setminus \{0\}}}, G_{\mathsf{aff}}(\mathsf{F}) = \begin{pmatrix} 1 & 0 & 0 \\ x & 0 & z \\ \mathsf{F}(x) & y & 0 \end{pmatrix}_{\substack{x \in \mathbb{F}_2^n \\ y \in \mathbb{F}_2^m \setminus \{0\} \\ z \in \mathbb{F}_2^n \setminus \{0\}}}$$

be the **generating matrices** of $\mathcal{C}_{\mathsf{ccz}}(\mathsf{F}), \mathcal{C}_{\mathsf{aff}}(\mathsf{F}), \mathcal{C}_{\mathsf{ea}}(\mathsf{F})$ resp. (binary codes of length $n+m+1$).

Link

Idea: to a function F, associate a code $\mathcal{C}_F$ constructed from its graph Γ_F.

Link equivalence codes and functions

For any $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, let

$$G_{ccz}(F) = \begin{pmatrix} 1 \\ x \\ F(x) \end{pmatrix}_{x \in \mathbb{F}_2^n}, G_{ea}(F) = \begin{pmatrix} 1 & 0 \\ x & 0 \\ F(x) & y \end{pmatrix}_{\substack{x \in \mathbb{F}_2^n \\ y \in \mathbb{F}_2^m \setminus \{0\}}}, G_{aff}(F) = \begin{pmatrix} 1 & 0 & 0 \\ x & 0 & z \\ F(x) & y & 0 \end{pmatrix}_{\substack{x \in \mathbb{F}_2^n \\ y \in \mathbb{F}_2^m \setminus \{0\} \\ z \in \mathbb{F}_2^n \setminus \{0\}}}$$

be the **generating matrices** of $\mathcal{C}_{ccz}(F), \mathcal{C}_{aff}(F), \mathcal{C}_{ea}(F)$ resp. (binary codes of length $n+m+1$).

Then :

- $\mathcal{C}_{ccz}(F_1) \sim \mathcal{C}_{ccz}(F_2)$ iff $F_1 \sim_{ccz} F_2$.

Link

Idea: to a function F, associate a code $\mathcal{C}_F$ constructed from its graph Γ_F.

Link equivalence codes and functions

For any $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, let

$$G_{ccz}(F) = \begin{pmatrix} 1 \\ x \\ F(x) \end{pmatrix}_{x \in \mathbb{F}_2^n}, G_{ea}(F) = \begin{pmatrix} 1 & 0 \\ x & 0 \\ F(x) & y \end{pmatrix}_{\substack{x \in \mathbb{F}_2^n \\ y \in \mathbb{F}_2^m \setminus \{0\}}}, G_{aff}(F) = \begin{pmatrix} 1 & 0 & 0 \\ x & 0 & z \\ F(x) & y & 0 \end{pmatrix}_{\substack{x \in \mathbb{F}_2^n \\ y \in \mathbb{F}_2^m \setminus \{0\} \\ z \in \mathbb{F}_2^n \setminus \{0\}}}$$

be the **generating matrices** of $\mathcal{C}_{ccz}(F), \mathcal{C}_{aff}(F), \mathcal{C}_{ea}(F)$ resp. (binary codes of length $n+m+1$).

Then :

- $\mathcal{C}_{ccz}(F_1) \sim \mathcal{C}_{ccz}(F_2)$ iff $F_1 \sim_{ccz} F_2$.
- $\mathcal{C}_{ea}(F_1) \sim \mathcal{C}_{ea}(F_2)$ iff $F_1 \sim_{ea} F_2$.

Link

Idea: to a function F, associate a code $\mathcal{C}_F$ constructed from its graph Γ_F.

Link equivalence codes and functions

For any $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, let

$$G_{ccz}(F) = \begin{pmatrix} 1 \\ x \\ F(x) \end{pmatrix}_{x \in \mathbb{F}_2^n}, G_{ea}(F) = \begin{pmatrix} 1 & 0 \\ x & 0 \\ F(x) & y \end{pmatrix}_{\substack{x \in \mathbb{F}_2^n \\ y \in \mathbb{F}_2^m \setminus \{0\}}}, G_{aff}(F) = \begin{pmatrix} 1 & 0 & 0 \\ x & 0 & z \\ F(x) & y & 0 \end{pmatrix}_{\substack{x \in \mathbb{F}_2^n \\ y \in \mathbb{F}_2^m \setminus \{0\} \\ z \in \mathbb{F}_2^n \setminus \{0\}}}$$

be the **generating matrices** of $\mathcal{C}_{ccz}(F), \mathcal{C}_{aff}(F), \mathcal{C}_{ea}(F)$ resp. (binary codes of length $n+m+1$).

Then :

- $\mathcal{C}_{ccz}(F_1) \sim \mathcal{C}_{ccz}(F_2)$ iff $F_1 \sim_{ccz} F_2$.
- $\mathcal{C}_{ea}(F_1) \sim \mathcal{C}_{ea}(F_2)$ iff $F_1 \sim_{ea} F_2$.
- If F_1 is **not bijective**, $\mathcal{C}_{aff}(F_1) \sim \mathcal{C}_{aff}(F_2)$ iff $F_1 \sim_{aff} F_2$.
  If F_1 is **bijective**, $\mathcal{C}_{aff}(F_1) \sim C_{aff}(F_2)$ iff $F_1 \sim_{aff} F_2$ or $F_1{}^{-1} \sim_{aff} F_2$.

Reed-Muller code

What does the generating matrix of such a code look like?

$$G(\mathrm{F}) = \begin{pmatrix} 1 \\ x \\ \mathrm{F}(x) \end{pmatrix}_{x \in \mathbb{F}_2^n}$$

Reed-Muller code

What does the generating matrix of such a code look like?

$$G(\mathrm{F}) = \begin{pmatrix} 1 \\ x \\ \mathrm{F}(x) \end{pmatrix}_{x \in \mathbb{F}_2^n}$$

Example:

Let $\mathrm{F} : \mathbb{F}_2^3 \to \mathbb{F}_2^2, (x_1, x_2, x_3) \mapsto (x_1, x_2 \oplus x_3)$

$$G(\mathrm{F}) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Reed-Muller code

What does the generating matrix of such a code look like?

$$G(\mathsf{F}) = \begin{pmatrix} 1 \\ x \\ \mathsf{F}(x) \end{pmatrix}_{x \in \mathbb{F}_2^n}$$

Example:

Let $\mathsf{F} : \mathbb{F}_2^3 \to \mathbb{F}_2^2, (x_1, x_2, x_3) \mapsto (x_1, x_2 \oplus x_3)$

$$G(\mathsf{F}) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{matrix} 1 \\ x \in \mathbb{F}_2^3 \\ \\ \mathsf{F}(x), x \in \mathbb{F}_2^3 \\ \\ \end{matrix}$$

Reed-Muller code

What does the generating matrix of such a code look like?

$$G(\mathrm{F}) = \begin{pmatrix} 1 \\ x \\ \mathrm{F}(x) \end{pmatrix}_{x \in \mathbb{F}_2^n}$$

Example:

Let $\mathrm{F} : \mathbb{F}_2^3 \to \mathbb{F}_2^2, (x_1, x_2, x_3) \mapsto (x_1, x_2 \oplus x_3)$

$$G(\mathrm{F}) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \quad \mathcal{R}(1, n)$$

On-going work

Needs

Classify boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, with $n \approx 6, 8$.

On-going work

Needs

Classify boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, with $n \approx 6, 8$.

Tools

Algorithms for codes $\mathcal{C} \subseteq \mathbb{F}_2^n$, with $n \approx 40, 50$.

On-going work

Needs

Classify boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, with $n \approx 6, 8$.

Tools

Algorithms for codes $\mathcal{C} \subseteq \mathbb{F}_2^n$, with $n \approx 40, 50$.

Need to adapt tools or find more appropriate ones

(on-going work with Jules Baudrin and Christophe Levrat)

On-going work

Needs

Classify boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, with $n \approx 6, 8$.

Tools

Algorithms for codes $\mathcal{C} \subseteq \mathbb{F}_2^n$, with $n \approx 40, 50$.

Need to adapt tools or find more appropriate ones

(on-going work with Jules Baudrin and Christophe Levrat)

Thank you!