On images, preimages and different notions related to APN mappings

Enes Pasalic, René Rodríguez-Aldama, Sadmir Kudin, Ajla Šehović

University of Primorska,
FAMNIT & IAM

June 11, 2026

Table of contents

Notation and basic notions

- $\mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$.

Notation and basic notions

$\mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$.

$\mathbb{F}_{2^n}$ is the finite field with 2^n elements.

Notation and basic notions

$\mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$.

$\longleftrightarrow$

We identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ by fixing a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

$\mathbb{F}_{2^n}$ is the finite field with 2^n elements.

Notation and basic notions

$\mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$.

$\longleftrightarrow$

We identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ by fixing a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

$\mathbb{F}_{2^n}$ is the finite field with 2^n elements.

Hamming weight of $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$: $\quad w_H(x) = |\{1 \leq i \leq n \mid x_i \neq 0\}|$.

Notation and basic notions

$\mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$.

$\longleftrightarrow$

We identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ by fixing a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

$\mathbb{F}_{2^n}$ is the finite field with 2^n elements.

Hamming weight of $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$: $\quad w_H(x) = |\{1 \leq i \leq n \mid x_i \neq 0\}|$.

Hamming distance between $x, x' \in \mathbb{F}_2^n$: $\quad d_H(x, x') = w_H(x + x')$.

Notation and basic notions

$\mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$.

$$\longleftrightarrow$$

We identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ by fixing a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

$\mathbb{F}_{2^n}$ is the finite field with 2^n elements.

Hamming weight of $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$: $\quad w_H(x) = |\{1 \leq i \leq n \mid x_i \neq 0\}|$.

Hamming distance between $x, x' \in \mathbb{F}_2^n$: $\quad d_H(x, x') = w_H(x + x')$.

Vectorial Boolean function: $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $n, m \in \mathbb{N}$ $\qquad$ (n, m)-function.

Notation and basic notions

$\mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$.

$\longleftrightarrow$ We identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ by fixing a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

$\mathbb{F}_{2^n}$ is the finite field with 2^n elements.

Hamming weight of $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$: $\quad w_H(x) = |\{1 \le i \le n \mid x_i \neq 0\}|$.

Hamming distance between $x, x' \in \mathbb{F}_2^n$: $\quad d_H(x, x') = w_H(x + x')$.

Vectorial Boolean function: $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m},\ n, m \in \mathbb{N}$. $\qquad (n, m)$-function.

Notation and basic notions

$\mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$.

$\longleftrightarrow$ We identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ by fixing a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

$\mathbb{F}_{2^n}$ is the finite field with 2^n elements.

Hamming weight of $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$: $\quad w_H(x) = |\{1 \leq i \leq n \mid x_i \neq 0\}|$.

Hamming distance between $x, x' \in \mathbb{F}_2^n$: $\quad d_H(x, x') = w_H(x + x')$.

Vectorial Boolean function: $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m},\ n, m \in \mathbb{N}$. $\qquad (n, m)$-function.

Hamming distance between F, F': $d_H(F, F') = |\{x \in \mathbb{F}_2^n : F(x) \neq F'(x)\}|$.

Notation and basic notions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

Notation and basic notions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

F is k-**to**-1: if $\forall y \in \mathrm{Im}(F),\ |F^{-1}(y)| = |\{x \in \mathbb{F}_{2^n} \mid F(x) = y\}| = k.$

Notation and basic notions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

F is k-**to**-1: if $\forall y \in \mathrm{Im}(F),\ |F^{-1}(y)| = |\{x \in \mathbb{F}_{2^n} \mid F(x) = y\}| = k.$

F is **almost** k-**to**-1: if $\exists!\, y_0 \in \mathrm{Im}(F) : |F^{-1}(y_0)| = 1$ and $\forall y \in \mathrm{Im}(F) \setminus \{y_0\},\ |F^{-1}(y)| = k.$

Notation and basic notions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

F is k-**to**-1: if $\forall y \in \mathrm{Im}(F)$, $|F^{-1}(y)| = |\{x \in \mathbb{F}_{2^n} \mid F(x) = y\}| = k$.

F is **almost** k-**to**-1: if $\exists!\, y_0 \in \mathrm{Im}(F) : |F^{-1}(y_0)| = 1$ and $\forall y \in \mathrm{Im}(F) \setminus \{y_0\}$, $|F^{-1}(y)| = k$.

First-order derivative of F **at** $a \in \mathbb{F}_{2^n}^*$: $D_aF : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, given by $D_aF = F(x) + F(x+a)$.

Notation and basic notions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

F is k-**to**-1: if $\forall y \in \mathrm{Im}(F)$, $|F^{-1}(y)| = |\{x \in \mathbb{F}_{2^n} \mid F(x) = y\}| = k$.

F is **almost** k-**to**-1: if $\exists!\, y_0 \in \mathrm{Im}(F) : |F^{-1}(y_0)| = 1$ and $\forall y \in \mathrm{Im}(F) \setminus \{y_0\}$, $|F^{-1}(y)| = k$.

First-order derivative of F **at** $a \in \mathbb{F}_{2^n}^*$: $D_aF : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, given by $D_aF = F(x) + F(x+a)$.

Differential uniformity of F: $\delta_F = \max\limits_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} |\{x \in \mathbb{F}_{2^n} \mid D_aF(x) = b\}|$.

Notation and basic notions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

F is k-**to**-1: if $\forall y \in \mathrm{Im}(F)$, $|F^{-1}(y)| = |\{x \in \mathbb{F}_{2^n} \mid F(x) = y\}| = k$.

F is **almost** k-**to**-1: if $\exists!\, y_0 \in \mathrm{Im}(F) : |F^{-1}(y_0)| = 1$ and $\forall y \in \mathrm{Im}(F) \setminus \{y_0\}$, $|F^{-1}(y)| = k$.

First-order derivative of F **at** $a \in \mathbb{F}_{2^n}^*$: $D_aF : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, given by $D_aF = F(x) + F(x+a)$.

Differential uniformity of F: $\delta_F = \max\limits_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} |\{x \in \mathbb{F}_{2^n} \mid D_aF(x) = b\}|$.

Definition

Function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *almost perfect nonlinear* (APN), if $\delta_F = 2$, i.e. if equation $F(x) + F(x+a) = b$ has at most 2 solutions, $\forall a, b \in \mathbb{F}_{2^n}$, $a \neq 0$.

Flats

Flats

k-**flat**: a k-dimensional affine subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $2 \leq k \leq n$.

Flats

k-**flat**: a k-dimensional affine subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $2 \leq k \leq n$.

Example: A *2-flat* is a subset $\{x_1, x_2, x_3, x_4\} \subseteq \mathbb{F}_{2^n}$ such that $x_1 + x_2 + x_3 + x_4 = 0$.

Flats

k-**flat**: a *k*-dimensional affine subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $2 \leq k \leq n$.

Example: A *2-flat* is a subset $\{x_1, x_2, x_3, x_4\} \subseteq \mathbb{F}_{2^n}$ such that $x_1 + x_2 + x_3 + x_4 = 0$.
An $(n-1)$-*flat* is the complement $\overline{H_a}$ of a hyperplane H_a, $a \in \mathbb{F}_{2^n}^*$.

Flats

k-**flat**: a k-dimensional affine subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $2 \leq k \leq n$.

Example: A *2-flat* is a subset $\{x_1, x_2, x_3, x_4\} \subseteq \mathbb{F}_{2^n}$ such that $x_1 + x_2 + x_3 + x_4 = 0$.

An $(n-1)$-*flat* is the complement $\overline{H_a}$ of a hyperplane H_a, $a \in \mathbb{F}_{2^n}^*$.

Flats

k-**flat**: a k-dimensional affine subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $2 \leq k \leq n$.

Example: A *2-flat* is a subset $\{x_1, x_2, x_3, x_4\} \subseteq \mathbb{F}_{2^n}$ such that $x_1 + x_2 + x_3 + x_4 = 0$.
An $(n-1)$-*flat* is the complement $\overline{H_a}$ of a hyperplane H_a, $a \in \mathbb{F}_{2^n}^*$.

Set of all 2-**flats in** $\mathbb{F}_{2^n}$: $\mathcal{F}_{2,n} = \{\{x_1, x_2, x_3, x_4\} \subseteq \mathbb{F}_{2^n} \mid \sum_{i=1}^4 x_i = 0\}$.

Flats

k-**flat**: a k-dimensional affine subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $2 \leq k \leq n$.

Example: A *2-flat* is a subset $\{x_1, x_2, x_3, x_4\} \subseteq \mathbb{F}_{2^n}$ such that $x_1 + x_2 + x_3 + x_4 = 0$.

An $(n-1)$-*flat* is the complement $\overline{H_a}$ of a hyperplane H_a, $a \in \mathbb{F}_{2^n}^*$.

Set of all 2-**flats in** $\mathbb{F}_{2^n}$: $\mathcal{F}_{2,n} = \{\{x_1, x_2, x_3, x_4\} \subseteq \mathbb{F}_{2^n} \mid \sum_{i=1}^4 x_i = 0\}$.

Definition

A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if and only if for each $\{x_1, x_2, x_3, x_4\} \in \mathcal{F}_{2,n}$,

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq 0.$$

Flats

k-**flat**: a k-dimensional affine subspace of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, $2 \leq k \leq n$.

Example: A *2-flat* is a subset $\{x_1, x_2, x_3, x_4\} \subseteq \mathbb{F}_{2^n}$ such that $x_1 + x_2 + x_3 + x_4 = 0$.

An $(n-1)$-*flat* is the complement $\overline{H_a}$ of a hyperplane H_a, $a \in \mathbb{F}_{2^n}^*$.

Set of all 2**-flats in** $\mathbb{F}_{2^n}$: $\mathcal{F}_{2,n} = \{\{x_1, x_2, x_3, x_4\} \subseteq \mathbb{F}_{2^n} \mid \sum_{i=1}^{4} x_i = 0\}$.

Definition

A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if and only if for each $\{x_1, x_2, x_3, x_4\} \in \mathcal{F}_{2,n}$,

$$F(x_1) + F(x_2) + F(x_3) + F(x_4) \neq 0.$$

$F(x_1)+F(x_3) \neq F(x_2)+F(x_4) \quad \Leftrightarrow \quad F(x_1)+F(x_1+a) \neq F(x_2)+F(x_2+a) \quad \Leftrightarrow \quad F(x)+F(x+a)$ has at most 2 solutions

Table of contents

Flats and their images

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and let $L \subseteq \mathbb{F}_{2^n}$ be a k-flat.

Vanishing

We say that L *vanishes* with respect to F if $\sum_{x \in L} F(x) = 0$.

Flats and their images

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and let $L \subseteq \mathbb{F}_{2^n}$ be a k-flat.

Vanishing

We say that L *vanishes* with respect to F if $\sum_{x \in L} F(x) = 0$.

Breaking

We say that F *breaks* L if $F(L)$ is not a flat.

Flats and their images

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and let $L \subseteq \mathbb{F}_{2^n}$ be a k-flat.

Vanishing

We say that L *vanishes* with respect to F if $\sum_{x \in L} F(x) = 0$.

Breaking

We say that F *breaks* L if $F(L)$ is not a flat.

Strong breaking

We say that F *strongly breaks* L if $\sum_{y \in F(L)} y \neq 0$.

Flats and their images

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and let $L \subseteq \mathbb{F}_{2^n}$ be a k-flat.

Vanishing

We say that L *vanishes* with respect to F if $\sum_{x \in L} F(x) = 0$.

Breaking

We say that F *breaks* L if $F(L)$ is not a flat.

Strong breaking

We say that F *strongly breaks* L if $\sum_{y \in F(L)} y \neq 0$.

Fact: The number of vanishing flats of F can be used as a measure of how close F is to an APN function. [5]

Two generalizations of almost perfect nonlinearity

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

k-strongly non-normal [2]

F is called *k-strongly non-normal* if, for every k-flat $L \subseteq \mathbb{F}_{2^n}$, the restriction $F|_L : L \to \mathbb{F}_{2^m}$ is not affine.

kth-order sum-free [2]

F is called *kth-order sum-free* if, for every k-flat $L \subseteq \mathbb{F}_{2^n}$, $\sum_{x \in L} F(x) \neq 0$.

Two generalizations of almost perfect nonlinearity

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$

k-strongly non-normal [2]

F is called *k-strongly non-normal* if, for every k-flat $L \subseteq \mathbb{F}_{2^n}$, the restriction $F|_L : L \to \mathbb{F}_{2^m}$ is not affine.

kth-order sum-free [2]

F is called *kth-order sum-free* if, for every k-flat $L \subseteq \mathbb{F}_{2^n}$, $\sum_{x \in L} F(x) \neq 0$.

Fact: An APN function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is k-strongly non-normal for every $2 \leq k \leq n$. [2]

How are these notions connected?

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^n}$ a k-flat

How are these notions connected?

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^n}$ a k-flat

$\boxed{F \text{ breaks } L}$: $F(L)$ is not a flat.

$\boxed{F \text{ strongly breaks } L}$: $\sum_{y \in F(L)} y \neq 0$.

$\boxed{F \text{ is } k\text{-strongly non-normal}}$: $F|_L : L \to \mathbb{F}_{2^m}$ is not affine.

$\boxed{F \text{ is } k\text{th-order sum-free}}$: $\sum_{x \in L} F(x) \neq 0$.

How are these notions connected?

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^n}$ a k-flat

$\boxed{F \text{ breaks } L}$: $F(L)$ is not a flat.

$\boxed{F \text{ strongly breaks } L}$: $\sum_{y \in F(L)} y \neq 0$.

$\boxed{F \text{ is } k\text{-strongly non-normal}}$: $F|_L : L \to \mathbb{F}_{2^m}$ is not affine.

$\boxed{F \text{ is } k\text{th-order sum-free}}$: $\sum_{x \in L} F(x) \neq 0$.

$$\boxed{F \text{ strongly breaks } L} \Longrightarrow \boxed{F \text{ breaks } L}$$

How are these notions connected?

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^n}$ a k-flat

$\boxed{F \text{ breaks } L}$: $F(L)$ is not a flat.

$\boxed{F \text{ strongly breaks } L}$: $\sum_{y \in F(L)} y \neq 0$.

$\boxed{F \text{ is } k\text{-strongly non-normal}}$: $F|_L : L \to \mathbb{F}_{2^m}$ is not affine.

$\boxed{F \text{ is } k\text{th-order sum-free}}$: $\sum_{x \in L} F(x) \neq 0$.

$$\boxed{F \text{ strongly breaks } L} \Longrightarrow \boxed{F \text{ breaks } L} \Longrightarrow \boxed{F \text{ is } k\text{-strongly non-normal}}$$

How are these notions connected?

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^n}$ a k-flat

$\boxed{F \text{ breaks } L}$: $F(L)$ is not a flat.

$\boxed{F \text{ strongly breaks } L}$: $\sum_{y \in F(L)} y \neq 0$.

$\boxed{F \text{ is } k\text{-strongly non-normal}}$: $F|_L : L \to \mathbb{F}_{2^m}$ is not affine.

$\boxed{F \text{ is } k\text{th-order sum-free}}$: $\sum_{x \in L} F(x) \neq 0$.

$$\boxed{F \text{ strongly breaks } L} \Longrightarrow \boxed{F \text{ breaks } L} \Longrightarrow \boxed{F \text{ is } k\text{-strongly non-normal}}$$

$$\boxed{F \text{ is } k\text{th-order sum-free}} \Longrightarrow \boxed{F \text{ is } k\text{-strongly non-normal}}$$

Unbroken flats

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^n}$ a k-flat

Unbroken flats

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^n}$ a k-flat

Set of all unbroken 2**-flats w.r.t.** F: $\mathcal{UF}_{n,F} = \{L \in \mathcal{F}_{2,n} \mid F(L) \text{ is a flat}\}$

Unbroken flats

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^n}$ a k-flat

Set of all unbroken 2**-flats w.r.t.** F: $\mathcal{UF}_{n,F} = \{L \in \mathcal{F}_{2,n} \mid F(L) \text{ is a flat}\}$

Theorem

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an APN function, and let $\mathcal{P} := \{F^{-1}(a) \mid a \in \mathbb{F}_{2^n}, |F^{-1}(a)| \geq 3\}$. If $\mathcal{P} \neq \emptyset$, then the number of unbroken 2-dimensional flats is

$$|\mathcal{UF}_{n,F}| = \sum_{P \in \mathcal{P}} \binom{|P|}{3}.$$

Otherwise, $|\mathcal{UF}_{n,F}| = 0$. In particular, if F is almost k-to-1, with $k \geq 3$, then

$$|\mathcal{UF}_{n,F}| = \frac{\binom{k}{3}(2^n - 1)}{k} = \frac{(2^n - 1)(k-1)(k-2)}{6}.$$

Proof sketch :)

Setup and definition: Let $F : \mathbb{F}_{2n} \to \mathbb{F}_{2n}$ be an APN function. Let $L = \{x_1, x_2, x_3, x_4\}$ be a 2-dimensional flat.
Define $\mathcal{P} = \{F^{-1}[a] \mid a \in \mathbb{F}_{2n}, |F^{-1}[a]| \geq 3\}$ (fibers of F with size at least 3).

Proof sketch :)

Setup and definition: Let $F : \mathbb{F}_{2n} \to \mathbb{F}_{2n}$ be an APN function. Let $L = \{x_1, x_2, x_3, x_4\}$ be a 2-dimensional flat.
Define $\mathcal{P} = \{F^{-1}[a] \mid a \in \mathbb{F}_{2n}, |F^{-1}[a]| \geq 3\}$ (fibers of F with size at least 3).

1. What can happen on a 2-dimensional flat $L = \{x_1, x_2, x_3, x_4\}$?

Since F is APN, the restriction $F|_L$ is neither constant nor two-to-one.

Proof sketch :)

Setup and definition: Let $F: \mathbb{F}_{2n} \to \mathbb{F}_{2n}$ be an APN function. Let $L = \{x_1, x_2, x_3, x_4\}$ be a 2-dimensional flat.
Define $\mathcal{P} = \{F^{-1}[a] \mid a \in \mathbb{F}_{2n}, |F^{-1}[a]| \geq 3\}$ (fibers of F with size at least 3).

1. What can happen on a 2-dimensional flat $L = \{x_1, x_2, x_3, x_4\}$?

Since F is APN, the restriction $F|_L$ is neither constant nor two-to-one.

Thus, the only possible sizes for $|F(L)|$ are 2, 3, or 4.

Proof sketch :)

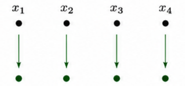
Setup and definition: Let $F : \mathbb{F}_{2n} \to \mathbb{F}_{2n}$ be an APN function. Let $L = \{x_1, x_2, x_3, x_4\}$ be a 2-dimensional flat.
Define $\mathcal{P} = \{F^{-1}[a] \mid a \in \mathbb{F}_{2n}, |F^{-1}[a]| \geq 3\}$ (fibers of F with size at least 3).

1. What can happen on a 2-dimensional flat $L = \{x_1, x_2, x_3, x_4\}$?

Since F is APN, the restriction $F|_L$ is neither constant nor two-to-one.

Thus, the only possible sizes for $|F(L)|$ are 2, 3, or 4.

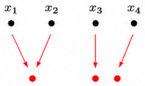
Case A: $|F(L)| = 4$ (one-to-one)



The four images are all distinct.

→ L is broken (APN).

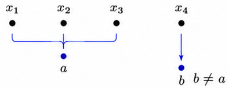
Case B: $|F(L)| = 3$



Exactly three distinct images.

→ L is broken.

Case C: $|F(L)| = 2$ (almost 3-to-one)



Three points map to a, one point to $b \neq a$.

→ L is unbroken
(maps to a 1-dimensional flat $\{a, b\}$).

Proof sketch :)

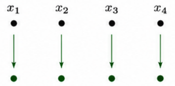
Setup and definition: Let $F : \mathbb{F}_{2n} \to \mathbb{F}_{2n}$ be an APN function. Let $L = \{x_1, x_2, x_3, x_4\}$ be a 2-dimensional flat. Define $\mathcal{P} = \{F^{-1}[a] \mid a \in \mathbb{F}_{2n}, |F^{-1}[a]| \geq 3\}$ (fibers of F with size at least 3).

1. What can happen on a 2-dimensional flat $L = \{x_1, x_2, x_3, x_4\}$?

Since F is APN, the restriction $F|_L$ is neither constant nor two-to-one.

Thus, the only possible sizes for $|F(L)|$ are $2, 3,$ or 4.

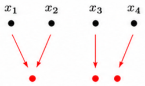
Case A: $|F(L)| = 4$ (one-to-one)



The four images are all distinct.

$\to$ L is broken (APN).

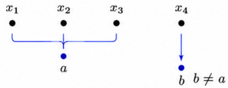
Case B: $|F(L)| = 3$



Exactly three distinct images.

$\to$ L is broken.

Case C: $|F(L)| = 2$ (almost 3-to-one)



Three points map to a, one point to $b \neq a$.

$\to$ L is unbroken
(maps to a 1-dimensional flat $\{a, b\}$).

2. When is L unbroken?

From the cases above:
L is unbroken if and only if $F|_L$ is almost 3-to-one (Case C).
Equivalently, L must contain 3 points from the same fiber $F^{-1}[a]$ and another point $b \neq a$.

Proof sketch :)

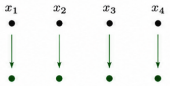
Setup and definition: Let $F : \mathbb{F}_{2n} \to \mathbb{F}_{2n}$ be an APN function. Let $L = \{x_1, x_2, x_3, x_4\}$ be a 2-dimensional flat.
Define $\mathcal{P} = \{F^{-1}[a] \mid a \in \mathbb{F}_{2n}, |F^{-1}[a]| \geq 3\}$ (fibers of F with size at least 3).

1. What can happen on a 2-dimensional flat $L = \{x_1, x_2, x_3, x_4\}$?

Since F is APN, the restriction $F|_L$ is neither constant nor two-to-one.

Thus, the only possible sizes for $|F(L)|$ are 2, 3, or 4.

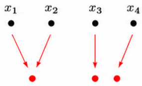
Case A: $|F(L)| = 4$ (one-to-one)



The four images are all distinct.

$\to$ L is broken (APN).

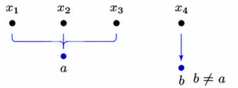
Case B: $|F(L)| = 3$



Exactly three distinct images.

$\to$ L is broken.

Case C: $|F(L)| = 2$ (almost 3-to-one)



Three points map to a, one point to $b \neq a$.

$\to$ L is unbroken
(maps to a 1-dimensional flat $\{a, b\}$).

2. When is L unbroken?

From the cases above:
L is unbroken if and only if $F|_L$ is almost 3-to-one (Case C).
Equivalently, L must contain 3 points from the same fiber $F^{-1}[a]$ and another point $b \neq a$.

3. How many unbroken flats come from a fixed fiber?

Fix $a \in \mathbb{F}_{2n}$ and let $P = F^{-1}[a]$ with $|P| = m \geq 3$.

Any 3 distinct points in P determine a unique 2-dimensional flat.

Proof sketch :)

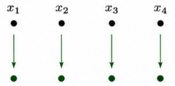
Setup and definition: Let $F : \mathbb{F}_{2n} \to \mathbb{F}_{2n}$ be an APN function. Let $L = \{x_1, x_2, x_3, x_4\}$ be a 2-dimensional flat.
Define $\mathcal{P} = \{F^{-1}[a] \mid a \in \mathbb{F}_{2n}, |F^{-1}[a]| \geq 3\}$ (fibers of F with size at least 3).

1. What can happen on a 2-dimensional flat $L = \{x_1, x_2, x_3, x_4\}$?

Since F is APN, the restriction $F|_L$ is neither constant nor two-to-one.

Thus, the only possible sizes for $|F(L)|$ are 2, 3, or 4.

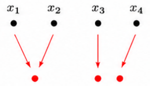
Case A: $|F(L)| = 4$ (one-to-one)



The four images are all distinct.

$\to$ L is broken (APN).

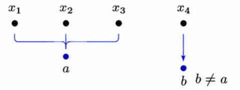
Case B: $|F(L)| = 3$



Exactly three distinct images.

$\to$ L is broken.

Case C: $|F(L)| = 2$ (almost 3-to-one)



Three points map to a, one point to $b \neq a$.

$\to$ L is unbroken
(maps to a 1-dimensional flat $\{a, b\}$).

2. When is L unbroken?

From the cases above:
L is unbroken if and only if $F|_L$ is almost 3-to-one (Case C).
Equivalently, L must contain 3 points from the same fiber $F^{-1}[a]$ and another point $b \neq a$.

3. How many unbroken flats come from a fixed fiber?

Fix $a \in \mathbb{F}_{2n}$ and let $P = F^{-1}[a]$ with $|P| = m \geq 3$.

Any 3 distinct points in P determine a unique 2-dimensional flat.

Number of such flats from P

$$= \binom{m}{3}$$

(choose any 3 points in P)

Proof sketch :)

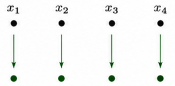
Setup and definition: Let $F : \mathbb{F}_{2n} \to \mathbb{F}_{2n}$ be an APN function. Let $L = \{x_1, x_2, x_3, x_4\}$ be a 2-dimensional flat.
Define $\mathcal{P} = \{F^{-1}[a] \mid a \in \mathbb{F}_{2n}, |F^{-1}[a]| \geq 3\}$ (fibers of F with size at least 3).

1. What can happen on a 2-dimensional flat $L = \{x_1, x_2, x_3, x_4\}$?

Since F is APN, the restriction $F|_L$ is neither constant nor two-to-one.

Thus, the only possible sizes for $|F(L)|$ are 2, 3, or 4.

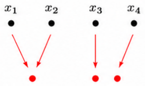
Case A: $|F(L)| = 4$ (one-to-one)



The four images are all distinct.

$\to$ L is broken (APN).

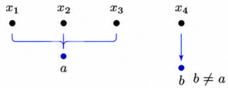
Case B: $|F(L)| = 3$



Exactly three distinct images.

$\to$ L is broken.

Case C: $|F(L)| = 2$ (almost 3-to-one)



Three points map to a, one point to $b \neq a$.

$\to$ L is unbroken (maps to a 1-dimensional flat $\{a, b\}$).

2. When is L unbroken?

From the cases above:
L is unbroken if and only if $F|_L$ is almost 3-to-one (Case C).
Equivalently, L must contain 3 points from the same fiber $F^{-1}[a]$ and another point $b \neq a$.

3. How many unbroken flats come from a fixed fiber?

Fix $a \in \mathbb{F}_{2n}$ and let $P = F^{-1}[a]$ with $|P| = m \geq 3$.

Any 3 distinct points in P determine a unique 2-dimensional flat.

Number of such flats from P

$$= \binom{m}{3}$$

(choose any 3 points in P)

4. Total number of unbroken 2-dimensional flats

- If $\mathcal{P} = \{F^{-1}[a] \mid |F^{-1}[a]| \geq 3\} \neq \emptyset$, then

$$|UB_{n,F}| = \sum_{P \in \mathcal{P}} \binom{|P|}{3}.$$

- If $\mathcal{P} = \emptyset$ (i.e., every fiber has size ≤ 2),

$$|UB_{n,F}| = 0.$$

Proof sketch :)

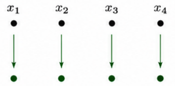
Setup and definition: Let $F : \mathbb{F}_{2n} \to \mathbb{F}_{2n}$ be an APN function. Let $L = \{x_1, x_2, x_3, x_4\}$ be a 2-dimensional flat.
Define $\mathcal{P} = \{F^{-1}[a] \mid a \in \mathbb{F}_{2n}, |F^{-1}[a]| \geq 3\}$ (fibers of F with size at least 3).

1. What can happen on a 2-dimensional flat $L = \{x_1, x_2, x_3, x_4\}$?

Since F is APN, the restriction $F|_L$ is neither constant nor two-to-one.

Thus, the only possible sizes for $|F(L)|$ are 2, 3, or 4.

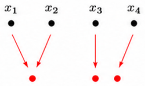
Case A: $|F(L)| = 4$ (one-to-one)



The four images are all distinct.

$\to$ L is broken (APN).

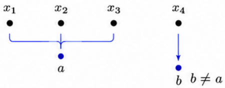
Case B: $|F(L)| = 3$



Exactly three distinct images.

$\to$ L is broken.

Case C: $|F(L)| = 2$ (almost 3-to-one)



Three points map to a, one point to $b \neq a$.

$\to$ L is unbroken (maps to a 1-dimensional flat $\{a, b\}$).

2. When is L unbroken?

From the cases above:
L is unbroken if and only if $F|_L$ is almost 3-to-one (Case C).
Equivalently, L must contain 3 points from the same fiber $F^{-1}[a]$ and another point $b \neq a$.

3. How many unbroken flats come from a fixed fiber?

Fix $a \in \mathbb{F}_{2n}$ and let $P = F^{-1}[a]$ with $|P| = m \geq 3$.

Any 3 distinct points in P determine a unique 2-dimensional flat.

Number of such flats from P

$$= \binom{m}{3}$$

(choose any 3 points in P)

4. Total number of unbroken 2-dimensional flats

- If $\mathcal{P} = \{F^{-1}[a] \mid |F^{-1}[a]| \geq 3\} \neq \emptyset$, then

$$|UB_{n,F}| = \sum_{P \in \mathcal{P}} \binom{|P|}{3}.$$

- If $\mathcal{P} = \emptyset$ (i.e., every fiber has size ≤ 2),

$$|UB_{n,F}| = 0.$$

5. Almost k-to-one case

If F is almost k-to-one (every fiber has size $k \geq 3$), then there are $\dfrac{2^n - 1}{k}$ fibers (since $k \mid (2^n - 1)$).

$$|UB_{n,F}| = \frac{2^n - 1}{k} \cdot \binom{k}{3} = \frac{(2^n - 1)(k-1)(k-2)}{6}$$

Example

Gold function: $F : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$, $F(x) = x^3$.

Example

Gold function: $F : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$, $F(x) = x^3$.

$F^{-1}(a)$	$a \in \mathrm{Im}(F)$
$\{(0,0,0,0,0,0)\}$	$(0,0,0,0,0,0)$
$\{(0,0,0,0,0,1),(0,0,1,1,1,0),(0,0,1,1,1,1)\}$	$(0,0,0,0,0,1)$
$\{(0,0,0,0,1,0),(0,1,1,1,0,0),(0,1,1,1,1,0)\}$	$(0,0,1,0,0,0)$
$\{(0,0,0,0,1,1),(0,1,0,0,0,1),(0,1,0,0,1,0)\}$	$(0,0,1,1,1,1)$
$\{(0,0,0,1,0,0),(1,1,1,0,0,0),(1,1,1,1,0,0)\}$	$(0,1,1,0,1,1)$
$\{(0,0,0,1,0,1),(1,1,0,0,1,1),(1,1,0,1,1,0)\}$	$(0,0,1,1,1,0)$
$\{(0,0,0,1,1,0),(1,0,0,0,1,0),(1,0,0,1,0,0)\}$	$(1,0,0,0,1,1)$
$\{(0,0,0,1,1,1),(1,0,1,0,1,0),(1,0,1,1,0,1)\}$	$(1,1,0,0,0,0)$
$\{(0,0,1,0,0,0),(1,0,0,0,1,1),(1,0,1,0,1,1)\}$	$(1,1,0,1,0,1)$
$\{(0,0,1,0,0,1),(1,0,0,1,0,1),(1,0,1,1,0,0)\}$	$(1,0,0,1,1,1)$
$\{(0,0,1,0,1,0),(1,1,0,1,1,1),(1,1,1,1,0,1)\}$	$(1,0,1,0,1,1)$
$\{(0,0,1,0,1,1),(1,1,0,0,1,0),(1,1,1,0,0,1)\}$	$(1,1,1,1,1,1)$
$\{(0,0,1,1,0,0),(0,1,0,0,1,1),(0,1,1,1,1,1)\}$	$(1,0,1,1,1,1)$
$\{(0,0,1,1,0,1),(0,1,0,0,0,0),(0,1,1,1,0,1)\}$	$(1,0,1,0,0,1)$
$\{(0,1,0,1,0,0),(1,0,0,0,0,1),(1,1,0,1,0,1)\}$	$(1,1,0,1,0,0)$
$\{(0,1,0,1,0,1),(1,0,1,1,1,0),(1,1,1,0,1,1)\}$	$(0,0,0,1,1,0)$
$\{(0,1,0,1,1,0),(1,0,1,0,0,1),(1,1,1,1,1,1)\}$	$(1,0,0,0,1,0)$
$\{(0,1,0,1,1,1),(1,0,0,1,1,1),(1,1,0,0,0,0)\}$	$(0,1,0,1,1,0)$
$\{(0,1,1,0,0,0),(1,0,0,1,1,0),(1,1,1,1,1,0)\}$	$(0,1,0,1,0,0)$
$\{(0,1,1,0,0,1),(1,0,1,0,0,0),(1,1,0,0,0,1)\}$	$(1,0,0,0,0,1)$
$\{(0,1,1,0,1,0),(1,0,0,0,0,0),(1,1,1,0,1,0)\}$	$(1,0,0,1,0,0)$
$\{(0,1,1,0,1,1),(1,0,1,1,1,1),(1,1,0,1,0,0)\}$	$(0,1,0,1,1,1)$

Example

Gold function: $F : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$, $F(x) = x^3$.

$F^{-1}(a)$	$a \in \mathrm{Im}(F)$
$\{(0,0,0,0,0,0)\}$	$(0,0,0,0,0,0)$
$\{(0,0,0,0,0,1),(0,0,1,1,1,0),(0,0,1,1,1,1)\}$	$(0,0,0,0,0,1)$
$\{(0,0,0,0,1,0),(0,1,1,1,0,0),(0,1,1,1,1,0)\}$	$(0,0,1,0,0,0)$
$\{(0,0,0,0,1,1),(0,1,0,0,0,1),(0,1,0,0,1,0)\}$	$(0,0,1,1,1,1)$
$\{(0,0,0,1,0,0),(1,1,1,0,0,0),(1,1,1,1,0,0)\}$	$(0,1,1,0,1,1)$
$\{(0,0,0,1,0,1),(1,1,0,0,1,1),(1,1,0,1,1,0)\}$	$(0,0,1,1,1,0)$
$\{(0,0,0,1,1,0),(1,0,0,0,1,0),(1,0,0,1,0,0)\}$	$(1,0,0,0,1,1)$
$\{(0,0,0,1,1,1),(1,0,1,0,1,0),(1,0,1,1,0,1)\}$	$(1,1,0,0,0,0)$
$\{(0,0,1,0,0,0),(1,0,0,0,1,1),(1,0,1,0,1,1)\}$	$(1,1,0,1,0,1)$
$\{(0,0,1,0,0,1),(1,0,0,1,0,1),(1,0,1,1,0,0)\}$	$(1,0,0,1,1,1)$
$\{(0,0,1,0,1,0),(1,1,0,1,1,1),(1,1,1,1,0,1)\}$	$(1,0,1,0,1,1)$
$\{(0,0,1,0,1,1),(1,1,0,0,1,0),(1,1,1,0,0,1)\}$	$(1,1,1,1,1,1)$
$\{(0,0,1,1,0,0),(0,1,0,0,1,1),(0,1,1,1,1,1)\}$	$(1,0,1,1,1,1)$
$\{(0,0,1,1,0,1),(0,1,0,0,0,0),(0,1,1,1,0,1)\}$	$(1,0,1,0,0,1)$
$\{(0,1,0,1,0,0),(1,0,0,0,0,1),(1,1,0,1,0,1)\}$	$(1,1,0,1,0,0)$
$\{(0,1,0,1,0,1),(1,0,1,1,1,0),(1,1,1,0,1,1)\}$	$(0,0,0,1,1,0)$
$\{(0,1,0,1,1,0),(1,0,1,0,0,1),(1,1,1,1,1,1)\}$	$(1,0,0,0,1,0)$
$\{(0,1,0,1,1,1),(1,0,0,1,1,1),(1,1,0,0,0,0)\}$	$(0,1,0,1,1,0)$
$\{(0,1,1,0,0,0),(1,0,0,1,1,0),(1,1,1,1,1,0)\}$	$(0,1,0,1,0,0)$
$\{(0,1,1,0,0,1),(1,0,1,0,0,0),(1,1,0,0,0,1)\}$	$(1,0,0,0,0,1)$
$\{(0,1,1,0,1,0),(1,0,0,0,0,0),(1,1,1,0,1,0)\}$	$(1,0,0,1,0,0)$
$\{(0,1,1,0,1,1),(1,0,1,1,1,1),(1,1,0,1,0,0)\}$	$(0,1,0,1,1,1)$

F is almost 3-to-1

$$|\mathcal{UF}_{6,F}| = \frac{\binom{3}{3}(2^6-1)}{3} = 21.$$

Example

Gold function: $F : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$, $F(x) = x^3$.

$F^{-1}(a)$	$a \in \mathrm{Im}(F)$
$\{(0,0,0,0,0,0)\}$	$(0,0,0,0,0,0)$
$\{(0,0,0,0,0,1),(0,0,1,1,1,0),(0,0,1,1,1,1)\}$	$(0,0,0,0,0,1)$
$\{(0,0,0,0,1,0),(0,1,1,1,0,0),(0,1,1,1,1,0)\}$	$(0,0,1,0,0,0)$
$\{(0,0,0,0,1,1),(0,1,0,0,0,1),(0,1,0,0,1,0)\}$	$(0,0,1,1,1,1)$
$\{(0,0,0,1,0,0),(1,1,1,0,0,0),(1,1,1,1,0,0)\}$	$(0,1,1,0,1,1)$
$\{(0,0,0,1,0,1),(1,1,0,0,1,1),(1,1,0,1,1,0)\}$	$(0,0,1,1,1,0)$
$\{(0,0,0,1,1,0),(1,0,0,0,1,0),(1,0,0,1,0,0)\}$	$(1,0,0,0,1,1)$
$\{(0,0,0,1,1,1),(1,0,1,0,1,0),(1,0,1,1,0,1)\}$	$(1,1,0,0,0,0)$
$\{(0,0,1,0,0,0),(1,0,0,0,1,1),(1,0,1,0,1,1)\}$	$(1,1,0,1,0,1)$
$\{(0,0,1,0,0,1),(1,0,0,1,0,1),(1,0,1,1,0,0)\}$	$(1,0,0,1,1,1)$
$\{(0,0,1,0,1,0),(1,1,0,1,1,1),(1,1,1,1,0,1)\}$	$(1,0,1,0,1,1)$
$\{(0,0,1,0,1,1),(1,1,0,0,1,0),(1,1,1,0,0,1)\}$	$(1,1,1,1,1,1)$
$\{(0,0,1,1,0,0),(0,1,0,0,1,1),(0,1,1,1,1,1)\}$	$(1,0,1,1,1,1)$
$\{(0,0,1,1,0,1),(0,1,0,0,0,0),(0,1,1,1,0,1)\}$	$(1,0,1,0,0,1)$
$\{(0,1,0,1,0,0),(1,0,0,0,0,1),(1,1,0,1,0,1)\}$	$(1,1,0,1,0,0)$
$\{(0,1,0,1,0,1),(1,0,1,1,1,0),(1,1,1,0,1,1)\}$	$(0,0,0,1,1,0)$
$\{(0,1,0,1,1,0),(1,0,1,0,0,1),(1,1,1,1,1,1)\}$	$(1,0,0,0,1,0)$
$\{(0,1,0,1,1,1),(1,0,0,1,1,1),(1,1,0,0,0,0)\}$	$(0,1,0,1,1,0)$
$\{(0,1,1,0,0,0),(1,0,0,1,1,0),(1,1,1,1,1,0)\}$	$(0,1,0,1,0,0)$
$\{(0,1,1,0,0,1),(1,0,1,0,0,0),(1,1,0,0,0,1)\}$	$(1,0,0,0,0,1)$
$\{(0,1,1,0,1,0),(1,0,0,0,0,0),(1,1,1,0,1,0)\}$	$(1,0,0,1,0,0)$
$\{(0,1,1,0,1,1),(1,0,1,1,1,1),(1,1,0,1,0,0)\}$	$(0,1,0,1,1,1)$

F is almost 3-to-1

$$|\mathcal{UF}_{6,F}| = \frac{\binom{3}{3}(2^6-1)}{3} = 21.$$

$$\begin{aligned}\mathcal{UF}_{6,F} = \{&\{38,0,24,62\},\{21,46,0,59\},\{29,0,16,13\},\\ &\{40,0,49,25\},\{51,0,54,5\},\{27,47,0,52\},\\ &\{19,0,31,12\},\{55,0,61,10\},\{35,8,0,43\},\\ &\{23,0,39,48\},\{22,41,63,0\},\{50,57,0,11\},\\ &\{14,15,0,1\},\{30,0,2,28\},\{3,0,18,17\},\\ &\{37,0,9,44\},\{56,60,0,4\},\{0,33,53,20\},\\ &\{0,32,58,26\},\{7,0,42,45\},\{36,0,6,34\}\}.\end{aligned}$$

Flat $\{x_1, x_2, x_3, x_4\}$ is represented by the integer labels of its elements in $\mathbb{F}_{2^6}$.

Example

Gold function: $F : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$, $F(x) = x^3$

$F^{-1}(a)$	$a \in \mathrm{Im}(F)$
$\{(0,0,0,0,0,0)\}$	$(0,0,0,0,0,0)$
$\{(0,0,0,0,0,1),(0,0,1,1,1,0),(0,0,1,1,1,1)\}$	$(0,0,0,0,0,1)$
$\{(0,0,0,0,1,0),(0,1,1,1,0,0),(0,1,1,1,1,0)\}$	$(0,0,1,0,0,0)$
$\{(0,0,0,0,1,1),(0,1,0,0,0,1),(0,1,0,0,1,0)\}$	$(0,0,1,1,1,1)$
$\{(0,0,0,1,0,0),(1,1,1,0,0,0),(1,1,1,1,0,0)\}$	$(0,1,1,0,1,1)$
$\{(0,0,0,1,0,1),(1,1,0,0,1,1),(1,1,0,1,1,0)\}$	$(0,0,1,1,1,0)$
$\{(0,0,0,1,1,0),(1,0,0,0,1,0),(1,0,0,1,0,0)\}$	$(1,0,0,0,1,1)$
$\{(0,0,0,1,1,1),(1,0,1,0,1,0),(1,0,1,1,0,1)\}$	$(1,1,0,0,0,0)$
$\{(0,0,1,0,0,0),(1,0,0,0,1,1),(1,0,1,0,1,1)\}$	$(1,1,0,1,0,1)$
$\{(0,0,1,0,0,1),(1,0,0,1,0,1),(1,0,1,1,0,0)\}$	$(1,0,0,1,1,1)$
$\{(0,0,1,0,1,0),(1,1,0,1,1,1),(1,1,1,1,0,1)\}$	$(1,0,1,0,1,1)$
$\{(0,0,1,0,1,1),(1,1,0,0,1,0),(1,1,1,0,0,1)\}$	$(1,1,1,1,1,1)$
$\{(0,0,1,1,0,0),(0,1,0,0,1,1),(0,1,1,1,1,1)\}$	$(1,0,1,1,1,1)$
$\{(0,0,1,1,0,1),(0,1,0,0,0,0),(0,1,1,1,0,1)\}$	$(1,0,1,0,0,1)$
$\{(0,1,0,1,0,0),(1,0,0,0,0,1),(1,1,0,1,0,1)\}$	$(1,1,0,1,0,0)$
$\{(0,1,0,1,0,1),(1,0,1,1,1,0),(1,1,1,0,1,1)\}$	$(0,0,0,1,1,0)$
$\{(0,1,0,1,1,0),(1,0,1,0,0,1),(1,1,1,1,1,1)\}$	$(1,0,0,0,1,0)$
$\{(0,1,0,1,1,1),(1,0,0,1,1,1),(1,1,0,0,0,0)\}$	$(0,1,0,1,1,0)$
$\{(0,1,1,0,0,0),(1,0,0,1,1,0),(1,1,1,1,1,0)\}$	$(0,1,0,1,0,0)$
$\{(0,1,1,0,0,1),(1,0,1,0,0,0),(1,1,0,0,0,1)\}$	$(1,0,0,0,0,1)$
$\{(0,1,1,0,1,0),(1,0,0,0,0,0),(1,1,1,0,1,0)\}$	$(1,0,0,1,0,0)$
$\{(0,1,1,0,1,1),(1,0,1,1,1,1),(1,1,0,1,0,0)\}$	$(0,1,0,1,1,1)$

F is almost 3-to-1

$$|\mathcal{UF}_{6,F}| = \frac{\binom{3}{3}(2^6-1)}{3} = 21.$$

$$\begin{aligned}\mathcal{UF}_{6,F} = \{&\{38,0,24,62\},\{21,46,0,59\},\{29,0,16,13\},\\ &\{40,0,49,25\},\{51,0,54,5\},\{27,47,0,52\},\\ &\{19,0,31,12\},\{55,0,61,10\},\{35,8,0,43\},\\ &\{23,0,39,48\},\{22,41,63,0\},\{50,57,0,11\},\\ &\{14,15,0,1\},\{30,0,2,28\},\{3,0,18,17\},\\ &\{37,0,9,44\},\{56,60,0,4\},\{0,33,53,20\},\\ &\{0,32,58,26\},\{7,0,42,45\},\{36,0,6,34\}\}.\end{aligned}$$

Flat $\{x_1,x_2,x_3,x_4\}$ is represented by the integer labels of its elements in $\mathbb{F}_{2^6}$.

Question

What is the maximal dimension of an unbroken flat, given an APN function?

Some computational observations

Table: Representatives of CCZ classes of APN functions for $n = 6$ with $\deg(F) \leq 3$. α is a root of the primitive polynomial $x^6 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$.

F	Univariate representation of F
D_1	x^3
D_2	$x^3 + \alpha^{11}x^6 + \alpha x^9$
D_3	$\alpha x^5 + x^9 + \alpha^4 x^{17} + \alpha x^{18} + \alpha^4 x^{20} + \alpha x^{24} + \alpha^4 x^{34} + \alpha x^{40}$
D_4	$\alpha^7 x^3 + x^5 + \alpha^3 x^9 + \alpha^4 x^{10} + x^{17} + \alpha^6 x^{18}$
D_5	$x^3 + \alpha x^{24} + x^{10}$
D_6	$x^3 + \alpha^{17}(x^{17} + x^{18} + x^{20} + x^{24})$
D_7	$x^3 + \alpha^{11}x^5 + \alpha^{13}x^9 + x^{17} + \alpha^{11}x^{33} + x^{48}$
D_8	$\alpha^{25}x^5 + x^9 + \alpha^{38}x^{12} + \alpha^{25}x^{18} + \alpha^{25}x^{36}$
D_9	$\alpha^{40}x^5 + \alpha^{10}x^6 + \alpha^{62}x^{20} + \alpha^{35}x^{33} + \alpha^{15}x^{34} + \alpha^{29}x^{48}$
D_{10}	$\alpha^{34}x^6 + \alpha^{52}x^9 + \alpha^{48}x^{12} + \alpha^6 x^{20} + \alpha^9 x^{33} + \alpha^{23}x^{34} + \alpha^{25}x^{40}$
D_{11}	$x^9 + \alpha^4(x^{10} + x^{18}) + \alpha^9(x^{12} + x^{20} + x^{40})$
D_{12}	$\alpha^{52}x^3 + \alpha^{47}x^5 + \alpha x^6 + \alpha^9 x^9 + \alpha^{44}x^{12} + \alpha^{47}x^{33} + \alpha^{10}x^{34} + \alpha^{33}x^{40}$
D_{13}	$\alpha(x^6 + x^{10} + x^{24} + x^{33}) + x^9 + \alpha^4 x^{17}$
D. APN Perm.	long univariate representation
EP	$x^3 + \alpha^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + \alpha^{14}(\alpha^{18}x^9 + \alpha^{36}x^{18} + \alpha^9 x^{36}$ $+x^{21} + x^{42} + \mathrm{Tr}(\alpha^{27}x + \alpha^{52}x^3 + \alpha^6 x^5 + \alpha^{19}x^7 + \alpha^{28}x^{11} + \alpha^2 x^{13}))$

Unbroken 2-flats

Table: Number of unbroken and strongly unbroken 2-flats of APN functions in 6 variables.

F	# unbroken 2-flats	# strongly unbroken 2-flats
D_1	21	0
D_2	21	0
D_3	9	13
D_4	8	13
D_5	7	21
D_6	18	9
D_7	18	15
D_8	4	9
D_9	15	17
D_{10}	8	13
D_{11}	6	13
D_{12}	7	14
D_{13}	8	11
D. APN Perm.	0	0
EP	25	21

Unbroken 3-flats

Table: Number of unbroken and strongly unbroken 3-flats of APN functions in 6 variables.

F	# unbroken 3-flats	# strongly unbroken 3-flats
D_1	9	3285
D_2	0	3285
D_3	0	7779
D_4	1	7721
D_5	23	6561
D_6	1	7332
D_7	1	7073
D_8	0	7617
D_9	10	6640
D_{10}	1	7711
D_{11}	1	7809
D_{12}	1	7586
D_{13}	0	7502
D. APN Perm.	0	184
EP	0	4336

Unbroken 4-flats

Table: Number of unbroken and strongly unbroken 4-flats of APN functions in 6 variables.

F	# unbroken 4-flats	# strongly unbroken 4-flats
D_1	0	714
D_2	0	714
D_3	0	546
D_4	0	549
D_5	0	203
D_6	0	497
D_7	0	454
D_8	0	473
D_9	0	329
D_{10}	0	531
D_{11}	0	559
D_{12}	0	494
D_{13}	0	499
D. APN Perm.	0	812
EP	0	391

Unbroken 4-flats - there's none :)

Table: Number of unbroken and strongly unbroken 4-flats of APN functions in 6 variables.

F	# unbroken 4-flats	# strongly unbroken 4-flats
D_1	0	714
D_2	0	714
D_3	0	546
D_4	0	549
D_5	0	203
D_6	0	497
D_7	0	454
D_8	0	473
D_9	0	329
D_{10}	0	531
D_{11}	0	559
D_{12}	0	494
D_{13}	0	499
D. APN Perm.	0	812
EP	0	391

Table of contents

More notation and basic notions

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

More notation and basic notions

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

Set of affine (n, m)**-functions:** $\mathcal{A}_{n,m}$

More notation and basic notions

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

Set of affine (n, m)**-functions:** $\mathcal{A}_{n,m}$

Vectorial nonlinearity: $\mathcal{NL}_V(F) = \min_{\Phi \in \mathcal{A}_{n,m}} d_H(F, \Phi)$

More notation and basic notions

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

Set of affine (n, m)-functions: $\mathcal{A}_{n,m}$

Vectorial nonlinearity: $\mathcal{NL}_V(F) = \min_{\Phi \in \mathcal{A}_{n,m}} d_H(F, \Phi)$

Problem: Computing $\mathcal{NL}_V(F)$ is difficult.

More notation and basic notions

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

Set of affine (n, m)-functions: $\mathcal{A}_{n,m}$

Vectorial nonlinearity: $\mathcal{NL}_V(F) = \min_{\Phi \in \mathcal{A}_{n,m}} d_H(F, \Phi)$

Problem: Computing $\mathcal{NL}_V(F)$ is difficult.

Cool observation: Flats provide a lower bound on $\mathcal{NL}_V(F)$.

More notation and basic notions

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

Set of affine (n, m)-functions: $\mathcal{A}_{n,m}$

Vectorial nonlinearity: $\mathcal{NL}_V(F) = \min_{\Phi \in \mathcal{A}_{n,m}} d_H(F, \Phi)$

Problem: Computing $\mathcal{NL}_V(F)$ is difficult.

Cool observation: Flats provide a lower bound on $\mathcal{NL}_V(F)$.

Idea: Estimate the number of broken and unbroken 2-flats.

Lower bound on vectorial nonlinearity

Unbroken 2-flats: $\mathcal{UF}_{n,F} = \{L \in \mathcal{F}_{2,n} : F(L) \text{ is a flat}\}$.

Theorem

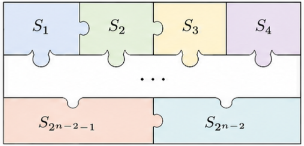
Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and let $|\mathcal{UF}_{n,F}| = w$. Then

$$\mathcal{NL}_V(F) \geq 2^{n-2} - w.$$

Proof sketch :)

Idea: Decompose $\mathbb{F}_2^n$ into 2-dimensional flats S_i

$\mathbb{F}_2^n =$

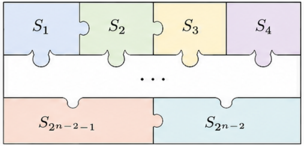


- Partition $\mathbb{F}_2^n$ into 2^{n-2} disjoint 2-dimensional affine subspaces (flats) $S_1, S_2, \ldots, S_{2n-2}$.

Think of F as a puzzle made of small pieces: its restrictions $F_{|S_i}$.

Proof sketch :)

Idea: Decompose $\mathbb{F}_2^n$ into 2-dimensional flats S_i

$\mathbb{F}_2^n =$ 

- Partition $\mathbb{F}_2^n$ into 2^{n-2} disjoint 2-dimensional affine subspaces (flats) $S_1, S_2, \ldots, S_{2n-2}$.

Think of F as a puzzle made of small pieces: its restrictions $F_{|S_i}$.

Vectorial nonlinearity

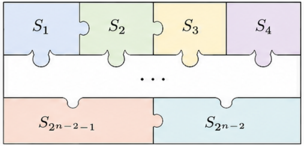
$$\mathcal{NL}_V(F) = \min_{\Phi \in \mathcal{A}_{n,n}} d_H(F, \Phi)$$

Distance from F to the set of affine functions is measured by the Hamming distance.

Proof sketch :)

Idea: Decompose $\mathbb{F}_2^n$ into 2-dimensional flats S_i

$\mathbb{F}_2^n =$



- Partition $\mathbb{F}_2^n$ into 2^{n-2} disjoint 2-dimensional affine subspaces (flats) $S_1, S_2, \dots, S_{2^{n-2}}$.

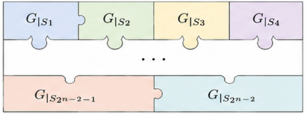
Think of F as a puzzle made of small pieces: its restrictions $F_{|S_i}$.

Vectorial nonlinearity

$$\mathcal{NL}_V(F) = \min_{\Phi \in \mathcal{A}_{n,n}} d_H(F, \Phi)$$

Distance from F to the set of affine functions is measured by the Hamming distance.

Any affine function $G \in \mathcal{A}_{n,n}$



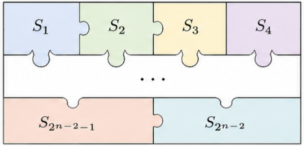
The restriction of G to each flat S_i is also affine.

Thus, choosing G is equivalent to choosing affine functions $G_{|S_i}$ on each S_i.

Proof sketch :)

Idea: Decompose $\mathbb{F}_2^n$ into 2-dimensional flats S_i

$\mathbb{F}_2^n =$



- Partition $\mathbb{F}_2^n$ into 2^{n-2} disjoint 2-dimensional affine subspaces (flats) $S_1, S_2, \dots, S_{2^{n-2}}$.

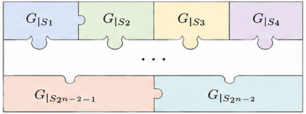
Think of F as a puzzle made of small pieces: its restrictions $F_{|S_i}$.

Vectorial nonlinearity

$$\mathcal{NL}_V(F) = \min_{\Phi \in \mathcal{A}_{n,n}} d_H(F, \Phi)$$

Distance from F to the set of affine functions is measured by the Hamming distance.

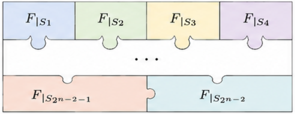
Any affine function $G \in \mathcal{A}_{n,n}$



The restriction of G to each flat S_i is also affine.

Thus, choosing G is equivalent to choosing affine functions $G_{|S_i}$ on each S_i.

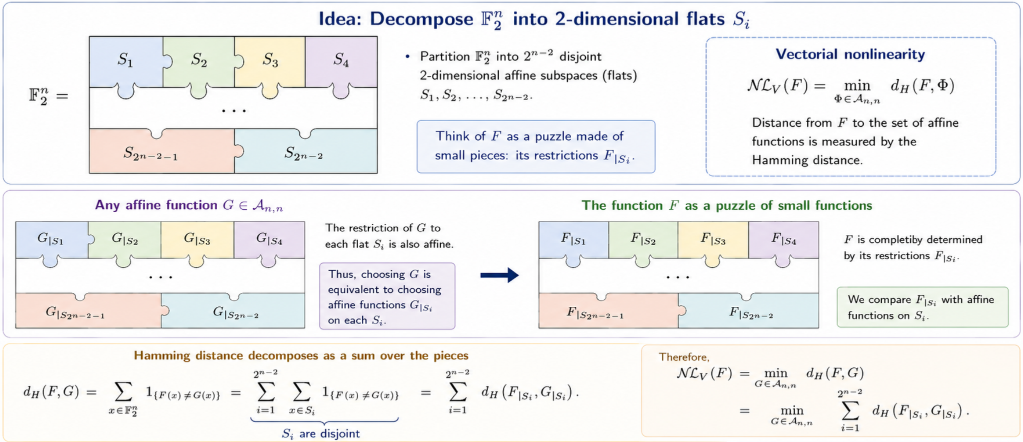
The function F as a puzzle of small functions



F is completiby determined by its restrictions $F_{|S_i}$.

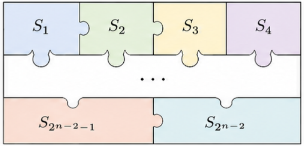
We compare $F_{|S_i}$ with affine functions on S_i.

Proof sketch :)



Proof sketch :)

Idea: Decompose $\mathbb{F}_2^n$ into 2-dimensional flats S_i

$\mathbb{F}_2^n =$ 

- Partition $\mathbb{F}_2^n$ into 2^{n-2} disjoint 2-dimensional affine subspaces (flats) $S_1, S_2, \dots, S_{2^{n-2}}$.

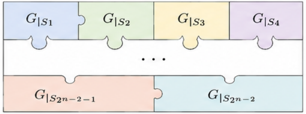
Think of F as a puzzle made of small pieces: its restrictions $F_{|S_i}$.

Vectorial nonlinearity

$$\mathcal{NL}_V(F) = \min_{\Phi \in \mathcal{A}_{n,n}} d_H(F, \Phi)$$

Distance from F to the set of affine functions is measured by the Hamming distance.

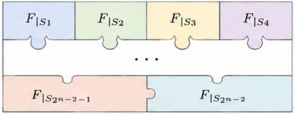
Any affine function $G \in \mathcal{A}_{n,n}$



The restriction of G to each flat S_i is also affine.

Thus, choosing G is equivalent to choosing affine functions $G_{|S_i}$ on each S_i.

The function F as a puzzle of small functions



F is completiby determined by its restrictions $F_{|S_i}$.

We compare $F_{|S_i}$ with affine functions on S_i.

Hamming distance decomposes as a sum over the pieces

$$d_H(F,G) = \sum_{x \in \mathbb{F}_2^n} 1_{\{F(x) \neq G(x)\}} = \underbrace{\sum_{i=1}^{2^{n-2}} \sum_{x \in S_i} 1_{\{F(x) \neq G(x)\}}}_{S_i \text{ are disjoint}} = \sum_{i=1}^{2^{n-2}} d_H\left(F_{|S_i}, G_{|S_i}\right).$$

Therefore,

$$\mathcal{NL}_V(F) = \min_{G \in \mathcal{A}_{n,n}} d_H(F,G) = \min_{G \in \mathcal{A}_{n,n}} \sum_{i=1}^{2^{n-2}} d_H\left(F_{|S_i}, G_{|S_i}\right).$$

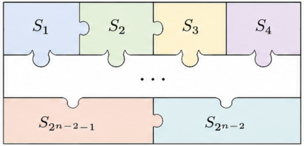
→ If $F_{|S_i}$ is affine, we can choose $G_{|S_i} = F_{|S_i}$ and get $d_H(F_{|S_i}, G_{|S_i}) = 0$.

→ If $F_{|S_i}$ is not affine (i.e., S_i is broken), then for any affine $G_{|S_i}$, $d_H(F_{|S_i}, G_{|S_i}) \geq 1$.

Proof sketch :)

Idea: Decompose $\mathbb{F}_2^n$ into 2-dimensional flats S_i

$\mathbb{F}_2^n =$



- Partition $\mathbb{F}_2^n$ into 2^{n-2} disjoint 2-dimensional affine subspaces (flats) $S_1, S_2, \dots, S_{2^{n-2}}$.

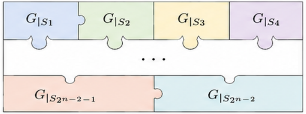
Think of F as a puzzle made of small pieces: its restrictions $F_{|S_i}$.

Vectorial nonlinearity

$$\mathcal{NL}_V(F) = \min_{\Phi \in \mathcal{A}_{n,n}} d_H(F, \Phi)$$

Distance from F to the set of affine functions is measured by the Hamming distance.

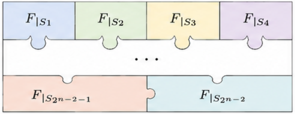
Any affine function $G \in \mathcal{A}_{n,n}$



The restriction of G to each flat S_i is also affine.

Thus, choosing G is equivalent to choosing affine functions $G_{|S_i}$ on each S_i.

The function F as a puzzle of small functions



F is completiby determined by its restrictions $F_{|S_i}$.

We compare $F_{|S_i}$ with affine functions on S_i.

Hamming distance decomposes as a sum over the pieces

$$d_H(F,G) = \sum_{x \in \mathbb{F}_2^n} 1_{\{F(x) \neq G(x)\}} = \underbrace{\sum_{i=1}^{2^{n-2}} \sum_{x \in S_i} 1_{\{F(x) \neq G(x)\}}}_{S_i \text{ are disjoint}} = \sum_{i=1}^{2^{n-2}} d_H\left(F_{|S_i}, G_{|S_i}\right).$$

Therefore,

$$\mathcal{NL}_V(F) = \min_{G \in \mathcal{A}_{n,n}} d_H(F,G) = \min_{G \in \mathcal{A}_{n,n}} \sum_{i=1}^{2^{n-2}} d_H\left(F_{|S_i}, G_{|S_i}\right).$$

→ If $F_{|S_i}$ is affine, we can choose $G_{|S_i} = F_{|S_i}$ and get $d_H(F_{|S_i}, G_{|S_i}) = 0$.

→ If $F_{|S_i}$ is not affine (i.e., S_i is broken), then for any affine $G_{|S_i}$, $d_H(F_{|S_i}, G_{|S_i}) \geq 1$.

Conclusion

If $|\mathcal{U}_{2,F}| = w$ (i.e., w unbroken flats), then at least $2^{n-2} - w$ flats are broken, so $\mathcal{NL}_V(F) \geq 2^{n-2} - w$.

Lower bound on vectorial nonlinearity

Unbroken 2**-flats:** $\mathcal{UF}_{n,F} = \{L \in \mathcal{F}_{2,n} : F(L) \text{ is a flat}\}$.

Theorem

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *and let* $|\mathcal{UF}_{n,F}| = w$. *Then*

$$\mathcal{NL}_V(F) \geq 2^{n-2} - w.$$

Lower bound on vectorial nonlinearity

Unbroken 2-flats: $\mathcal{UF}_{n,F} = \{L \in \mathcal{F}_{2,n} : F(L) \text{ is a flat}\}$.

Theorem

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *and let* $|\mathcal{UF}_{n,F}| = w$. *Then*

$$\mathcal{NL}_V(F) \geq 2^{n-2} - w.$$

Corollary

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be the inverse function defined by* $F(x) = x^{-1}$, *where* n *is odd. Then* F *breaks all 2-flats [3]. Hence*

$$\mathcal{NL}_V(F) \geq 2^{n-2}.$$

Table of contents

Preimage investigation

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and let $L \subseteq \mathbb{F}_{2^n}$ be a k-flat.

Preimage investigation

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and let $L \subseteq \mathbb{F}_{2^n}$ be a k-flat.

Question: If $F(L)$ is an r-flat, what can be said about the relation between k and r?

Preimage investigation

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and let $L \subseteq \mathbb{F}_{2^n}$ be a k-flat.

Question: If $F(L)$ is an r-flat, what can be said about the relation between k and r?

To study this, define

$$\lambda_{L,i} = \left|\{\, b \in \mathbb{F}_{2^m} : |F^{-1}(b) \cap L| = i\}\right|, \qquad \text{for } 0 \leq i \leq 2^k.$$

Preimage investigation

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and let $L \subseteq \mathbb{F}_{2^n}$ be a k-flat.

Question: If $F(L)$ is an r-flat, what can be said about the relation between k and r?

To study this, define

$$\lambda_{L,i} = \left| \{ b \in \mathbb{F}_{2^m} : |F^{-1}(b) \cap L| = i \} \right|, \qquad \text{for } 0 \leq i \leq 2^k.$$

$(\lambda_{L,i} = \#\{\text{points in } \mathrm{Im}(F) \text{ with exactly } i \text{ preimages in } L\})$

Preimage investigation

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and let $L \subseteq \mathbb{F}_{2^n}$ be a k-flat.

Question: If $F(L)$ is an r-flat, what can be said about the relation between k and r?

To study this, define

$$\lambda_{L,i} = \left|\{\, b \in \mathbb{F}_{2^m} : |F^{-1}(b) \cap L| = i\}\right|, \qquad \text{for } 0 \leq i \leq 2^k.$$

$$(\lambda_{L,i} = \#\{\text{points in } \mathrm{Im}(F) \text{ with exactly } i \text{ preimages in } L\})$$

These numbers satisfy

$$\sum_{i=1}^{2^k} i\,\lambda_{L,i} = 2^k, \qquad \text{and} \qquad \sum_{i=1}^{2^k} \lambda_{L,i} = 2^r.$$

Preimage investigation

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ and let $L \subseteq \mathbb{F}_{2^n}$ be a k-flat.

Question: If $F(L)$ is an r-flat, what can be said about the relation between k and r?

To study this, define

$$\lambda_{L,i} = \left|\{\, b \in \mathbb{F}_{2^m} : |F^{-1}(b) \cap L| = i\}\right|, \qquad \text{for } 0 \leq i \leq 2^k.$$

$(\lambda_{L,i} = \#\{\text{points in } \mathrm{Im}(F) \text{ with exactly } i \text{ preimages in } L\})$

These numbers satisfy

$$\sum_{i=1}^{2^k} i\,\lambda_{L,i} = 2^k \qquad \text{and} \qquad \sum_{i=1}^{2^k} \lambda_{L,i} = 2^r.$$

(counts points of L) (counts points of $F(L)$)

Restrictions on preimages

Proposition

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ satisfy $|F^{-1}(y)| \leq 3$ for all $y \in \mathbb{F}_{2^n}$. If L is a k-flat and $F(L)$ is an r-flat with $r \geq 2$, then

$$(\lambda_{L,1}, \lambda_{L,2}, \lambda_{L,3}) \equiv (0,0,0),\ (2,0,2),\ (1,2,1),\ (-1,2,-1) \pmod 4.$$

Restrictions on preimages

Proposition

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *satisfy* $|F^{-1}(y)| \leq 3$ *for all* $y \in \mathbb{F}_{2^n}$*. If* L *is a* k*-flat and* $F(L)$ *is an* r*-flat with* $r \geq 2$*, then*

$$(\lambda_{L,1}, \lambda_{L,2}, \lambda_{L,3}) \equiv (0,0,0),\ (2,0,2),\ (1,2,1),\ (-1,2,-1) \pmod 4.$$

Proposition

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *satisfy* $|F^{-1}(y)| \leq 3$ *for all* $y \in \mathbb{F}_{2^n}$*. Then for every unbroken* 3*-flat* L *satisfies*

$$(\lambda_{L,1}, \lambda_{L,2}, \lambda_{L,3}) \in \{(8,0,0),\ (0,4,0),\ (2,0,2),\ (1,2,1)\}.$$

Application to 2-to-1 functions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is 2-to-1, $L \subseteq \mathbb{F}_{2^n}$ is a k-flat, $F(L)$ is an r-flat

Application to 2-to-1 functions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is 2-to-1, $L \subseteq \mathbb{F}_{2^n}$ is a k-flat, $F(L)$ is an r-flat

$$\sum_{i=1}^{2^k} i\,\lambda_{L,i} = 2^k \qquad \text{and} \qquad \sum_{i=1}^{2^k} \lambda_{L,i} = 2^r$$

Application to 2-to-1 functions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is 2-to-1, $L \subseteq \mathbb{F}_{2^n}$ is a k-flat, $F(L)$ is an r-flat

$$\lambda_{L,1} + 2\lambda_{L,2} = 2^k \qquad \text{and} \qquad \lambda_{L,1} + \lambda_{L,2} = 2^r$$

Application to 2-to-1 functions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is 2-to-1, $L \subseteq \mathbb{F}_{2^n}$ is a k-flat, $F(L)$ is an r-flat

$$\lambda_{L,1} + 2\lambda_{L,2} = 2^k \qquad \text{and} \qquad \lambda_{L,1} + \lambda_{L,2} = 2^r$$

$$\downarrow$$

$$\lambda_{L,1} = 2^{r+1} - 2^k \qquad \lambda_{L,2} = 2^k - 2^r.$$

Application to 2-to-1 functions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is 2-to-1, $L \subseteq \mathbb{F}_{2^n}$ is a k-flat, $F(L)$ is an r-flat

$$\lambda_{L,1} + 2\lambda_{L,2} = 2^k \qquad \text{and} \qquad \lambda_{L,1} + \lambda_{L,2} = 2^r$$

$$\downarrow$$

$$\lambda_{L,1} = 2^{r+1} - 2^k \qquad \lambda_{L,2} = 2^k - 2^r.$$

$$\downarrow$$

$$2^{r+1} \geq 2^k$$

Application to 2-to-1 functions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is 2-to-1, $L \subseteq \mathbb{F}_{2^n}$ is a k-flat, $F(L)$ is an r-flat

$$\lambda_{L,1} + 2\lambda_{L,2} = 2^k \qquad \text{and} \qquad \lambda_{L,1} + \lambda_{L,2} = 2^r$$

$$\downarrow$$

$$\lambda_{L,1} = 2^{r+1} - 2^k \qquad \lambda_{L,2} = 2^k - 2^r.$$

$$\downarrow$$

$$2^{r+1} \geq 2^k$$

$$\downarrow$$

$$r \geq k - 1.$$

Application to 2-to-1 functions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is 2-to-1, $L \subseteq \mathbb{F}_{2^n}$ is a k-flat, $F(L)$ is an r-flat

$$\lambda_{L,1} + 2\lambda_{L,2} = 2^k \qquad \text{and} \qquad \lambda_{L,1} + \lambda_{L,2} = 2^r$$

$$\downarrow$$

$$\lambda_{L,1} = 2^{r+1} - 2^k \qquad \lambda_{L,2} = 2^k - 2^r.$$

$$\downarrow$$

$$2^{r+1} \geq 2^k$$

$$\downarrow$$

$$r \geq k - 1.$$

Conclusion: An unbroken k-flat can only have as its image a $(k-1)$-flat or a k-flat.

Currently working on...

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN permutation

Observation from the airport: $\phi_F : \mathcal{F}_{2,n} \to \mathbb{F}_{2^n}$, $\phi_F(\{x_1, x_2, x_3, x_4\}) = \sum_{i=1}^{4} F(x_i)$

Currently working on...

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN permutation

Observation from the airport: $\phi_F : \mathcal{F}_{2,n} \to \mathbb{F}_{2^n}$, $\phi_F(\{x_1, x_2, x_3, x_4\}) = \sum_{i=1}^{4} F(x_i)$

n **odd**: ϕ_F seems to be balanced

Currently working on...

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN permutation

Observation from the airport: $\phi_F : \mathcal{F}_{2,n} \to \mathbb{F}_{2^n}$, $\phi_F(\{x_1, x_2, x_3, x_4\}) = \sum_{i=1}^{4} F(x_i)$

n **odd**: ϕ_F seems to be balanced $\;\to\;$ true for $x^d : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

Currently working on...

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN permutation

Observation from the airport: $\phi_F : \mathcal{F}_{2,n} \to \mathbb{F}_{2^n}$, $\phi_F(\{x_1, x_2, x_3, x_4\}) = \sum_{i=1}^{4} F(x_i)$

n **odd**: ϕ_F seems to be balanced $\rightarrow$ true for $x^d : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$
$\rightarrow$ true for the two sporadic examples over $\mathbb{F}_{2^9}$

Currently working on...

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN permutation

Observation from the airport: $\phi_F : \mathcal{F}_{2,n} \to \mathbb{F}_{2^n}$, $\phi_F(\{x_1, x_2, x_3, x_4\}) = \sum_{i=1}^{4} F(x_i)$

n **odd**: ϕ_F seems to be balanced $\;\to\;$ true for $x^d : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

$\to\;$ true for the two sporadic examples over $\mathbb{F}_{2^9}$

$$\forall c \in \mathbb{F}_{2^n}^* : \quad |\phi_F^{-1}(c)| = \frac{2^{n-2}(2^{n-1}-1)}{3}$$

Currently working on...

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN permutation

Observation from the airport: $\phi_F : \mathcal{F}_{2,n} \to \mathbb{F}_{2^n}$, $\phi_F(\{x_1, x_2, x_3, x_4\}) = \sum_{i=1}^{4} F(x_i)$

n **odd**: ϕ_F seems to be balanced $\rightarrow$ true for $x^d : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$
$\rightarrow$ true for the two sporadic examples over $\mathbb{F}_{2^9}$

$$\forall c \in \mathbb{F}_{2^n}^* : \quad |\phi_F^{-1}(c)| = \frac{2^{n-2}(2^{n-1}-1)}{3}$$

n **even**: ϕ_F seems to be balanced-like

Currently working on...

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN permutation

Observation from the airport: $\phi_F : \mathcal{F}_{2,n} \to \mathbb{F}_{2^n}$, $\phi_F(\{x_1, x_2, x_3, x_4\}) = \sum_{i=1}^{4} F(x_i)$

n **odd**: ϕ_F seems to be balanced $\to$ true for $x^d : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$
$\to$ true for the two sporadic examples over $\mathbb{F}_{2^9}$

$$\forall c \in \mathbb{F}_{2^n}^* : \quad |\phi_F^{-1}(c)| = \frac{2^{n-2}(2^{n-1}-1)}{3}$$

n **even**: ϕ_F seems to be balanced-like $\to$ true for Dillon's permutation

Currently working on...

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN permutation

Observation from the airport: $\phi_F : \mathcal{F}_{2,n} \to \mathbb{F}_{2^n}$, $\phi_F(\{x_1, x_2, x_3, x_4\}) = \sum_{i=1}^{4} F(x_i)$

n **odd**: ϕ_F seems to be balanced $\to$ true for $x^d : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$
$\to$ true for the two sporadic examples over $\mathbb{F}_{2^9}$

$$\forall c \in \mathbb{F}_{2^n}^* : \quad |\phi_F^{-1}(c)| = \frac{2^{n-2}(2^{n-1}-1)}{3}$$

n **even**: ϕ_F seems to be balanced-like $\to$ true for Dillon's permutation

$$\mathbb{F}_{2^n}^* = V_{56} \cup V_7, \quad \forall c \in V_{56} : |\phi_F^{-1}(c)| = 160 \text{ and } \forall c \in V_7 : |\phi_F^{-1}(c)| = 208$$

Current and future directions

Current and future directions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN function

- What is the maximal dimension of an unbroken flat for F?

Current and future directions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN function

- What is the maximal dimension of an unbroken flat for F?
- For F quadratic, can we provide a tight lower bound on the vectorial nonlinearity?

Current and future directions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN function

- What is the maximal dimension of an unbroken flat for F?
- For F quadratic, can we provide a tight lower bound on the vectorial nonlinearity?
- Analysis of image sets of F (see [4], [1])

Current and future directions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN function

- What is the maximal dimension of an unbroken flat for F?
- For F quadratic, can we provide a tight lower bound on the vectorial nonlinearity?
- Analysis of image sets of F (see [4], [1]) : flats contained in the image set.

Current and future directions

$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ an APN function

- What is the maximal dimension of an unbroken flat for F?
- For F quadratic, can we provide a tight lower bound on the vectorial nonlinearity?
- Analysis of image sets of F (see [4], [1]) : flats contained in the image set.
- Develop observations from the airport.

Thank you! :)
Questions?

References I

L. Budaghyan, I. Ivkovic, and N. Kaleyski.
Triplicate functions.
Cryptography and Communications, 15:35–83, 2023.

C. Carlet.
Two generalizations of almost perfect nonlinearity.
Journal of Cryptology, 38(20), 2025.

N. Kolomeec and D. Bykov.
On the image of an affine subspace under the inverse function within a finite field.
Designs, Codes and Cryptography, 92(2):467–476, 2024.

L. Kölsch, B. Kriepke, and G. M. Kyureghyan.
Image sets of perfectly nonlinear maps.
Designs, Codes and Cryptography, 91:1–27, 2023.

S. Li, W. Meidl, A. Polujan, A. Pott, C. Riera, and P. Stanica.
Vanishing flats: a combinatorial viewpoint on the planarity of functions and their application.
IEEE Transactions on Information Theory, 66(11):7101–7112, 2020.