Radboud University

Properties of χ

Jan Schoone, Joan Daemen

End-of-ESCADA Workshop Radboud University

28 August 2024

ESCADA

Introduction

$$\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}},\ x \mapsto y$$

Introduction

$$\chi \colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}},\ x \mapsto y$$
$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

Introduction

$$\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}},\ x \mapsto y$$
$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

Investigate different forms of χ:

$$\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}},\, x \mapsto y$$
$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

Investigate different forms of χ:

- as a map of n-periodic sequences;

Introduction

$$\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}, x \mapsto y$$
$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

Investigate different forms of χ:

- as a map of n-periodic sequences;
- as a map of bi-infinite sequences;

Introduction

$$\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}},\ x \mapsto y$$
$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

Investigate different forms of χ:

- as a map of n-periodic sequences;
- as a map of bi-infinite sequences;
- as a univariate polynomial;

Introduction

$$\chi \colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}},\ x \mapsto y$$
$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

Investigate different forms of χ:

- as a map of n-periodic sequences;
- as a map of bi-infinite sequences;
- as a univariate polynomial;
- the function rule over other finite fields.

Outline

χ on *n*-periodic sequences

χ on bi-infinite sequences

Univariate forms of χ_n

Bounds on univariate forms of χ_n

Number of univariate representations of χ_n

Polynomial automorphisms

Known properties

- χ is shift-invariant,

Known properties

- χ is shift-invariant, we have $\chi \circ \tau = \tau \circ \chi$, with:

Known properties

- χ is shift-invariant, we have $\chi \circ \tau = \tau \circ \chi$, with:

$$\tau \colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}},\, x \mapsto y$$
$$y_i = x_{i+1}$$

Known properties

- χ is shift-invariant, we have $\chi \circ \tau = \tau \circ \chi$, with:

$$\tau : \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}, x \mapsto y$$
$$y_i = x_{i+1}$$

- Restricting χ to finite sequences of odd length, then it is bijective. [Daemen,1995]

χ on n-periodic sequences

Periodic states

Definition

A state $\sigma \in \mathbb{F}_2^{\mathbb{Z}}$ is called *periodic* when there exists an integer $n \geq 1$ such that $\tau^n(\sigma) = \sigma$.

Periodic states

Definition

A state $\sigma \in \mathbb{F}_2^{\mathbb{Z}}$ is called *periodic* when there exists an integer $n \geq 1$ such that $\tau^n(\sigma) = \sigma$.

- We say that σ is *n-periodic*.

Definition

A state $\sigma \in \mathbb{F}_2^{\mathbb{Z}}$ is called *periodic* when there exists an integer $n \geq 1$ such that $\tau^n(\sigma) = \sigma$.

- We say that σ is *n-periodic*.
- The minimal n for which σ is n-periodic, is called the *period* of σ.

Definition

A state $\sigma \in \mathbb{F}_2^{\mathbb{Z}}$ is called *periodic* when there exists an integer $n \geq 1$ such that $\tau^n(\sigma) = \sigma$.

- We say that σ is *n-periodic*.
- The minimal n for which σ is n-periodic, is called the *period* of σ.
- We write $\widehat{\mathbb{F}_2}$ for the set of all periodic spaces.

Periodic states

Definition

A state $\sigma \in \mathbb{F}_2^{\mathbb{Z}}$ is called *periodic* when there exists an integer $n \geq 1$ such that $\tau^n(\sigma) = \sigma$.

- We say that σ is *n-periodic*.
- The minimal n for which σ is n-periodic, is called the *period* of σ.
- We write $\widehat{\mathbb{F}_2}$ for the set of all periodic spaces.
- We write Σ_n for the set of n-periodic states.

Periodic states

Definition

A state $\sigma \in \mathbb{F}_2^{\mathbb{Z}}$ is called *periodic* when there exists an integer $n \geq 1$ such that $\tau^n(\sigma) = \sigma$.

- We say that σ is *n-periodic*.
- The minimal n for which σ is n-periodic, is called the *period* of σ.
- We write $\widehat{\mathbb{F}_2}$ for the set of all periodic spaces.
- We write Σ_n for the set of n-periodic states.

Example

0^*, 1^*, $(01)^*$, $(10111)^*$.

Periodic states

Definition

A state $\sigma \in \mathbb{F}_2^{\mathbb{Z}}$ is called *periodic* when there exists an integer $n \geq 1$ such that $\tau^n(\sigma) = \sigma$.

- We say that σ is *n-periodic*.
- The minimal n for which σ is n-periodic, is called the *period* of σ.
- We write $\widehat{\mathbb{F}_2}$ for the set of all periodic spaces.
- We write Σ_n for the set of n-periodic states.

Example

0^*, 1^*, $(01)^*$, $(10111)^*$.

The set of n-periodic spaces has 2^n elements and is isomorphic to $\mathbb{F}_2^n$.

Definition

A state $\sigma \in \mathbb{F}_2^{\mathbb{Z}}$ is called *periodic* when there exists an integer $n \geq 1$ such that $\tau^n(\sigma) = \sigma$.

- We say that σ is *n-periodic*.
- The minimal n for which σ is n-periodic, is called the *period* of σ.
- We write $\widehat{\mathbb{F}_2}$ for the set of all periodic spaces.
- We write Σ_n for the set of n-periodic states.

The set of n-periodic spaces has 2^n elements and is isomorphic to $\mathbb{F}_2^n$.

We can define χ on $\widehat{\mathbb{F}_2}$, or as χ_n on $\mathbb{F}_2^n$ (here indices modulo n).

χ_n and invertibility

Theorem (Daemen, 1995)

If n is odd, then χ_n is invertible.

Theorem (Daemen, 1995)

If n is odd, then χ_n is invertible.

The ANF for χ_n^{-1} is given by [Liu, Sarkar, Meier, Isobe, 2022].

Theorem (Daemen, 1995)

If n is odd, then χ_n is invertible.

The ANF for χ_n^{-1} is given by [Liu, Sarkar, Meier, Isobe, 2022].

The map $\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, for odd n, is an element of $(\mathrm{Bij}(\mathbb{F}_2^n), \circ)$.

Theorem (Daemen, 1995)

If n is odd, then χ_n is invertible.

The ANF for χ_n^{-1} is given by [Liu, Sarkar, Meier, Isobe, 2022].

The map $\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, for odd n, is an element of $(\mathrm{Bij}(\mathbb{F}_2^n), \circ)$.

Theorem

If n is odd, then the order of χ_n is $2^{\lceil \lg(n) \rceil}$.

Visualisation

$$
\begin{array}{cccccccccccccccccccccccc|ccccccc}
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & . & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & . & . & . & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & . & 1 & . & 1 & . & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & . & . & . & . & . & . & . & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & . & 1 & . & . & . & . & . & 1 & . & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & . & . & . & 1 & . & . & . & 1 & . & . & . & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & . & . & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 \\
. & . & . & . & . & . & . & . & . & . & . & . & 1 & . & 1 & . & . & . & . & . & . & . & . & . & . & . & . & . & 1 & . & 1 \\
. & . & . & . & . & . & . & . & . & . & 1 & . & . & . & 1 & . & . & . & . & . & . & . & . & . & . & . & 1 & . & . & . & 1 \\
. & . & . & . & . & . & . & . & 1 & . & 1 & . & 1 & . & 1 & . & . & . & . & . & . & . & . & . & 1 & . & 1 & . & 1 & . & 1 \\
. & . & . & . & . & . & 1 & . & . & . & . & . & . & . & 1 & . & . & . & . & . & . & . & 1 & . & . & . & . & . & . & . & 1 \\
. & . & . & . & 1 & . & 1 & . & . & . & . & . & 1 & . & 1 & . & . & . & . & . & 1 & . & 1 & . & . & . & . & . & 1 & . & 1 \\
. & . & 1 & . & . & . & 1 & . & . & . & 1 & . & . & . & 1 & . & . & . & 1 & . & . & . & 1 & . & . & . & 1 & . & . & . & 1 \\
1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1 & . & 1
\end{array}
$$

Example: χ_6

1 time:

Name: 1-cycle

Example: χ_6

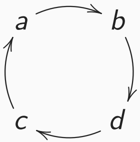
12 times:

$$a \rightleftarrows b$$

Name: 2-cycle

Example: χ_6

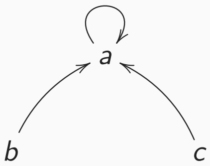
6 times:



Name: 4-cycle

Example: χ_6

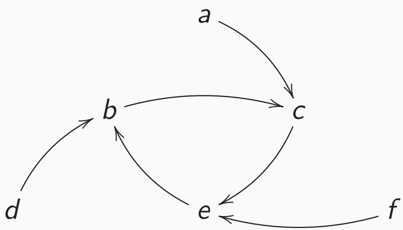
1 time:



Name: prong

Example: χ_6

2 times:



Name: spin

Example: χ_6 summary

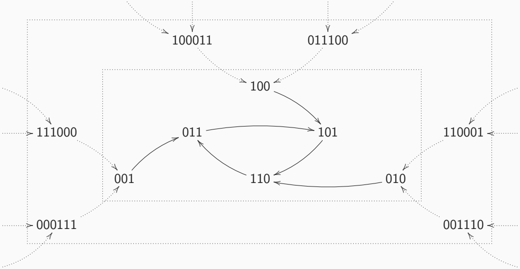
shape	number	number of states
1-cycle	1	1
2-cycle	12	24
4-cycle	6	24
prong	1	3
spin	2	12

Example: χ_6 summary

shape	number	number of states
1-cycle	1	1
2-cycle	12	24
4-cycle	6	24
prong	1	3
spin	2	12
		64

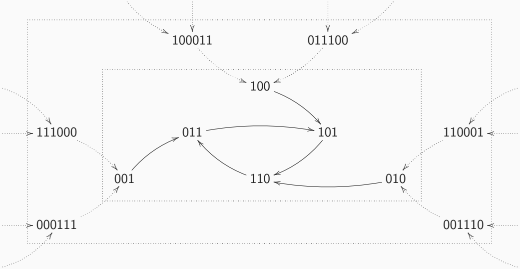
State diagram bigger example

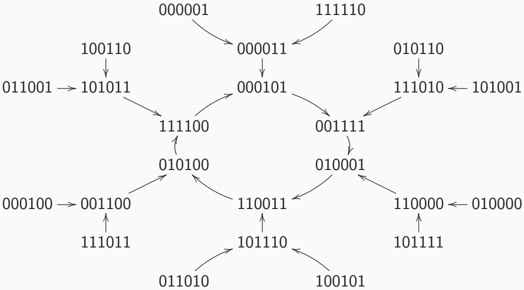
We omit the zeroes in even positions, to obtain:



State diagram bigger example

We omit the zeroes in even positions, to obtain:





Snowflakes

- States that have a 1 in an odd position and a 1 in an even position, occur in cycles;

Snowflakes

- States that have a 1 in an odd position and a 1 in an even position, occur in cycles;
- States that have all odd (or even) positions 0 (name: $S_{n,0}$) occur in snowflake-like components;

Snowflakes

- States that have a 1 in an odd position and a 1 in an even position, occur in cycles;
- States that have all odd (or even) positions 0 (name: $S_{n,0}$) occur in snowflake-like components;
- These states can be represented by polynomials:

Snowflakes

- States that have a 1 in an odd position and a 1 in an even position, occur in cycles;
- States that have all odd (or even) positions 0 (name: $S_{n,0}$) occur in snowflake-like components;
- These states can be represented by polynomials:

$$(x_0, 0, x_1, 0, \ldots, x_{n-1}, 0) \mapsto \sum_{i=0}^{n-1} x_i X^{n-(i+1)}$$

Snowflakes

- States that have a 1 in an odd position and a 1 in an even position, occur in cycles;
- States that have all odd (or even) positions 0 (name: $S_{n,0}$) occur in snowflake-like components;
- These states can be represented by polynomials:

$$(x_0, 0, x_1, 0, \dots, x_{n-1}, 0) \mapsto \sum_{i=0}^{n-1} x_i X^{n-(i+1)}$$

- Then χ_n is just multiplication by $1 + X$ modulo $X^n + 1$.

- States that have a 1 in an odd position and a 1 in an even position, occur in cycles;
- States that have all odd (or even) positions 0 (name: $S_{n,0}$) occur in snowflake-like components;
- These states can be represented by polynomials:

$$(x_0, 0, x_1, 0, \ldots, x_{n-1}, 0) \mapsto \sum_{i=0}^{n-1} x_i X^{n-(i+1)}$$

- Then χ_n is just multiplication by $1 + X$ modulo $X^n + 1$.

  Reason:

$$\chi(x_0, 0, x_1, 0, \ldots, x_{n-1}, 0) = (x_0 + x_1, 0, x_1 + x_2, 0, \ldots, x_{n-1} + x_0, 0)$$

△

Proposition

Let $n = 2m$ with $m > 1$ an odd integer. Then the length of the cycle in a snowflake is a divisor of $2^o - 1$, where $o = \mathrm{ord}_{\mathbb{Z}/m\mathbb{Z}}(2)$.

Proposition

Let $n = 2m$ with $m > 1$ an odd integer. Then the length of the cycle in a snowflake is a divisor of $2^o - 1$, where $o = \mathrm{ord}_{\mathbb{Z}/m\mathbb{Z}}(2)$.

Proposition

The length of the cycle in snowflakes of period n with $\frac{n}{2} = 2^k \cdot m$ with $m > 1$ odd, is 2^k times the length of the cycle in the snowflakes of period n with $\frac{n}{2} = m$.

Proposition

Let $n = 2m$ with $m > 1$ an odd integer. Then the length of the cycle in a snowflake is a divisor of $2^o - 1$, where $o = \operatorname{ord}_{\mathbb{Z}/m\mathbb{Z}}(2)$.

Proposition

The length of the cycle in snowflakes of period n with $\frac{n}{2} = 2^k \cdot m$ with $m > 1$ odd, is 2^k times the length of the cycle in the snowflakes of period n with $\frac{n}{2} = m$.

Theorem

Let $\sigma = (\sigma_0, \ldots, \sigma_{n-1})^*$ be a state in $S_{n,0}$. We have that σ is in the cycle if and only if $f_\sigma(X)$ has exactly 2^{k-1} divisors $X + 1$.

Snowflakes: Statements

Proposition

Let $n = 2m$ with $m > 1$ an odd integer. Then the length of the cycle in a snowflake is a divisor of $2^o - 1$, where $o = \mathrm{ord}_{\mathbb{Z}/m\mathbb{Z}}(2)$.

Proposition

The length of the cycle in snowflakes of period n with $\frac{n}{2} = 2^k \cdot m$ with $m > 1$ odd, is 2^k times the length of the cycle in the snowflakes of period n with $\frac{n}{2} = m$.

Theorem

Let $\sigma = (\sigma_0, \ldots, \sigma_{n-1})^*$ be a state in $S_{n,0}$. We have that σ is in the cycle if and only if $f_\sigma(X)$ has exactly 2^{k-1} divisors $X + 1$.

Furthermore, if $f_\sigma(X)$ has $2^{k-1} - \ell$ divisors $X + 1$, then $\chi^\ell(\sigma)$ is in the cycle.

χ is surjective on periodic states

- For even n, χ_n is not surjective, as 0^n, $(10)^{n/2}$ and $(01)^{n/2}$ all map to 0^n.

χ is surjective on periodic states

- For even n, χ_n is not surjective, as 0^n, $(10)^{n/2}$ and $(01)^{n/2}$ all map to 0^n.
- Thus, there exists some $y \in \mathbb{F}_2^n$ such that $\chi_n(x) \neq y$ for all $x \in \mathbb{F}_2^n$.

χ is surjective on periodic states

- For even n, χ_n is not surjective, as 0^n, $(10)^{n/2}$ and $(01)^{n/2}$ all map to 0^n.
- Thus, there exists some $y \in \mathbb{F}_2^n$ such that $\chi_n(x) \neq y$ for all $x \in \mathbb{F}_2^n$.
- However, there exists a $z \in \mathbb{F}_2^{2n}$ such that $\chi_{2n}(z) = y \| y$.

χ is surjective on periodic states

- For even n, χ_n is not surjective, as 0^n, $(10)^{n/2}$ and $(01)^{n/2}$ all map to 0^n.
- Thus, there exists some $y \in \mathbb{F}_2^n$ such that $\chi_n(x) \neq y$ for all $x \in \mathbb{F}_2^n$.
- However, there exists a $z \in \mathbb{F}_2^{2n}$ such that $\chi_{2n}(z) = y \| y$.
- We see that every element in Σ_n has a preimage in Σ_{2n}.

χ on bi-infinite sequences

Surjective on periodic states

Proposition

$\chi\colon \widehat{\mathbb{F}_2} \to \widehat{\mathbb{F}_2}$ *is surjective.*

Reason: Every element $x \in \widehat{\mathbb{F}_2}$ has a period n, so is in Σ_n. Then either it has a preimage in Σ_n, or it has a preimage in $\Sigma_{2n} \subset \widehat{\mathbb{F}_2}$. △

Can we give a concrete explanation whether $\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective?

Intermezzo: Non-periodic state

Define a sequence $(\Delta^{(n)})_{n=0}^{\infty}$ by

Intermezzo: Non-periodic state

Define a sequence $(\Delta^{(n)})_{n=0}^{\infty}$ by

$$\Delta^{(0)} = 1 \text{ and } \Delta^{(n+1)} = \Delta^{(n)} \| 0^n 1$$

Define a sequence $(\Delta^{(n)})_{n=0}^{\infty}$ by

$$\Delta^{(0)} = 1 \text{ and } \Delta^{(n+1)} = \Delta^{(n)} \| 0^n 1$$

Let $\Delta = \lim_{n \to \infty} \Delta^{(n)}$.

Intermezzo: Non-periodic state

Define a sequence $(\Delta^{(n)})_{n=0}^{\infty}$ by

$$\Delta^{(0)} = 1 \text{ and } \Delta^{(n+1)} = \Delta^{(n)} \| 0^n 1$$

Let $\Delta = \lim_{n\to\infty} \Delta^{(n)}$.

For every $n < 0$, we set $\Delta_n = \Delta_{-n}$.

Intermezzo: Non-periodic state

Define a sequence $(\Delta^{(n)})_{n=0}^{\infty}$ by

$$\Delta^{(0)} = 1 \text{ and } \Delta^{(n+1)} = \Delta^{(n)} \| 0^n 1$$

Let $\Delta = \lim_{n \to \infty} \Delta^{(n)}$.

For every $n < 0$, we set $\Delta_n = \Delta_{-n}$.

$$\Delta = \cdots 000100101110100100010000100000100000010000000100000000100000000 \cdots$$

Surjectivity

Non-constructive proof that $\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective.

Surjectivity

Non-constructive proof that $\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective.

Take $\mathbb{F}_2$ with the discrete topology and extend it to the product topology on $\mathbb{F}_2^{\mathbb{Z}}$.

Surjectivity

Non-constructive proof that $\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective.

Take $\mathbb{F}_2$ with the discrete topology and extend it to the product topology on $\mathbb{F}_2^{\mathbb{Z}}$. Then $\widehat{\mathbb{F}_2} \subset \mathbb{F}_2^{\mathbb{Z}}$ is dense and $\mathbb{F}_2^{\mathbb{Z}}$ is a compact Hausdorff space, by Tychonoff's Theorem.

Surjectivity

Non-constructive proof that $\chi \colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective.

Take $\mathbb{F}_2$ with the discrete topology and extend it to the product topology on $\mathbb{F}_2^{\mathbb{Z}}$. Then $\widehat{\mathbb{F}_2} \subset \mathbb{F}_2^{\mathbb{Z}}$ is dense and $\mathbb{F}_2^{\mathbb{Z}}$ is a compact Hausdorff space, by Tychonoff's Theorem.

Theorem (Tikhonov, 1935)

Let $(X, \mathcal{T})$ be a compact Hausdorff space and let $A \subset X$ be dense. Let $f : X \to X$ be a continuous map such that $f_{|A} \colon A \to A$ is surjective.

Surjectivity

Non-constructive proof that $\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective.

Take $\mathbb{F}_2$ with the discrete topology and extend it to the product topology on $\mathbb{F}_2^{\mathbb{Z}}$. Then $\widehat{\mathbb{F}_2} \subset \mathbb{F}_2^{\mathbb{Z}}$ is dense and $\mathbb{F}_2^{\mathbb{Z}}$ is a compact Hausdorff space, by Tychonoff's Theorem.

Theorem (Tikhonov, 1935)

Let $(X, \mathcal{T})$ be a compact Hausdorff space and let $A \subset X$ be dense. Let $f : X \to X$ be a continuous map such that $f_{|A}\colon A \to A$ is surjective. Then f is surjective.

Non-constructive proof that $\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective.

Take $\mathbb{F}_2$ with the discrete topology and extend it to the product topology on $\mathbb{F}_2^{\mathbb{Z}}$. Then $\widehat{\mathbb{F}_2} \subset \mathbb{F}_2^{\mathbb{Z}}$ is dense and $\mathbb{F}_2^{\mathbb{Z}}$ is a compact Hausdorff space, by Tychonoff's Theorem.

Theorem (Tikhonov, 1935)

Let $(X, \mathcal{T})$ be a compact Hausdorff space and let $A \subset X$ be dense. Let $f : X \to X$ be a continuous map such that $f_{|A}\colon A \to A$ is surjective. Then f is surjective.

Since, with $\chi(x) = y$, each y_i depends on only three bits of x,

Surjectivity

Non-constructive proof that $\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective.

Take $\mathbb{F}_2$ with the discrete topology and extend it to the product topology on $\mathbb{F}_2^{\mathbb{Z}}$. Then $\widehat{\mathbb{F}_2} \subset \mathbb{F}_2^{\mathbb{Z}}$ is dense and $\mathbb{F}_2^{\mathbb{Z}}$ is a compact Hausdorff space, by Tychonoff's Theorem.

Theorem (Tikhonov, 1935)

Let $(X, \mathcal{T})$ be a compact Hausdorff space and let $A \subset X$ be dense. Let $f : X \to X$ be a continuous map such that $f_{|A}\colon A \to A$ is surjective. Then f is surjective.

Since, with $\chi(x) = y$, each y_i depends on only three bits of x, χ is continuous in the product topology,

Surjectivity

Non-constructive proof that $\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective.

Take $\mathbb{F}_2$ with the discrete topology and extend it to the product topology on $\mathbb{F}_2^{\mathbb{Z}}$. Then $\widehat{\mathbb{F}_2} \subset \mathbb{F}_2^{\mathbb{Z}}$ is dense and $\mathbb{F}_2^{\mathbb{Z}}$ is a compact Hausdorff space, by Tychonoff's Theorem.

Theorem (Tikhonov, 1935)

Let $(X, \mathcal{T})$ be a compact Hausdorff space and let $A \subset X$ be dense. Let $f : X \to X$ be a continuous map such that $f_{|A}\colon A \to A$ is surjective. Then f is surjective.

Since, with $\chi(x) = y$, each y_i depends on only three bits of x, χ is continuous in the product topology, and thus χ is surjective.

Univariate forms of χ_n

Univariate expressions

- Choosing an isomorphism (of vector spaces) from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$:

Univariate expressions

- Choosing an isomorphism (of vector spaces) from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$: χ_n as a univariate polynomial function

Univariate expressions

- Choosing an isomorphism (of vector spaces) from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$: χ_n as a univariate polynomial function: $\chi_n^u(t)$.

- Choosing an isomorphism (of vector spaces) from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$: χ_n as a univariate polynomial function: $\chi_n^u(t)$.
- In practice: interpolation on the inputs and outputs for χ_n to obtain $\chi_n^u(t)$.

Univariate expressions

- Choosing an isomorphism (of vector spaces) from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$: χ_n as a univariate polynomial function: $\chi_n^u(t)$.
- In practice: interpolation on the inputs and outputs for χ_n to obtain $\chi_n^u(t)$.
- Different outcomes for $\chi_n^u(X)$ possible.

Univariate expressions

- Choosing an isomorphism (of vector spaces) from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$: χ_n as a univariate polynomial function: $\chi_n^u(t)$.
- In practice: interpolation on the inputs and outputs for χ_n to obtain $\chi_n^u(t)$.
- Different outcomes for $\chi_n^u(X)$ possible.
- Example: $\chi_3^u(t) = t^6$.

- Choosing an isomorphism (of vector spaces) from $\mathbb{F}_2^n$ to $\mathbb{F}_{2^n}$: χ_n as a univariate polynomial function: $\chi_n^u(t)$.
- In practice: interpolation on the inputs and outputs for χ_n to obtain $\chi_n^u(t)$.
- Different outcomes for $\chi_n^u(X)$ possible.
- Example: $\chi_3^u(t) = t^6$. (With specific choice of basis $\{\alpha^3, \alpha^6, \alpha^5\}$ and $\mathbb{F}_2^3 \to \mathbb{F}_8,\ (a, b, c) \mapsto a\alpha^3 + b\alpha^6 + c\alpha^5$.)

Power functions

- A *power function* is a function $(-)^e \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ t \mapsto t^e$.

Power functions

- A *power function* is a function $(-)^e \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ t \mapsto t^e$.
- Invertible iff $\gcd(e, 2^n - 1) = 1$.

Power functions

- A *power function* is a function $(-)^e \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ t \mapsto t^e$.
- Invertible iff $\gcd(e, 2^n - 1) = 1$.
- $\mathrm{ord}((-)^e) = \mathrm{ord}_{2^n-1}(e)$.

Power functions

- A *power function* is a function $(-)^e \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ t \mapsto t^e$.
- Invertible iff $\gcd(e, 2^n - 1) = 1$.
- $\operatorname{ord}((-)^e) = \operatorname{ord}_{2^n-1}(e)$.
- Easy: χ_n is not a power function when n even.

Power functions

- A *power function* is a function $(-)^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ t \mapsto t^e$.
- Invertible iff $\gcd(e, 2^n - 1) = 1$.
- $\mathrm{ord}((-)^e) = \mathrm{ord}_{2^n-1}(e)$.
- Easy: χ_n is not a power function when n even.
  $\chi_n((01)^{n/2}) = 0^n \implies \alpha^e = 0$ for some non-zero $\alpha \in \mathbb{F}_{2^n}$. $\triangle$

- A *power function* is a function $(-)^e \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ t \mapsto t^e$.
- Invertible iff $\gcd(e, 2^n - 1) = 1$.
- $\mathrm{ord}((-)^e) = \mathrm{ord}_{2^n-1}(e)$.
- Easy: χ_n is not a power function when n even.
- Less easy: χ_n is not a power function when $n > 3$.

Power functions

- A *power function* is a function $(-)^e \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ t \mapsto t^e$.
- Invertible iff $\gcd(e, 2^n - 1) = 1$.
- $\mathrm{ord}((-)^e) = \mathrm{ord}_{2^n-1}(e)$.
- Easy: χ_n is not a power function when n even.
- Less easy: χ_n is not a power function when $n > 3$.
  If $n > 3$ is such that $2^n - 1$ is a prime number, then easy:

Power functions

- A *power function* is a function $(-)^e \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ t \mapsto t^e$.
- Invertible iff $\gcd(e, 2^n - 1) = 1$.
- $\mathrm{ord}((-)^e) = \mathrm{ord}_{2^n-1}(e)$.
- Easy: χ_n is not a power function when n even.
- Less easy: χ_n is not a power function when $n > 3$.
  If $n > 3$ is such that $2^n - 1$ is a prime number, then easy:
  $\mathrm{ord}(\chi_n) \geq 4$, but $\varphi(2^n - 1) = 2^n - 2$ has only one factor 2. $\triangle$

Power functions

- A *power function* is a function $(-)^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n},\ t \mapsto t^e$.
- Invertible iff $\gcd(e, 2^n - 1) = 1$.
- $\operatorname{ord}((-)^e) = \operatorname{ord}_{2^n-1}(e)$.
- Easy: χ_n is not a power function when n even.
- Less easy: χ_n is not a power function when $n > 3$.
  Done by investigating the differential probabilities for χ_n and power functions.

Definition (Differential probability [Biham, Shamir, 2009])

Let $f\colon G \to H$ be a map between finite groups G and H. Let $g \in G$ and $h \in H$ be arbitrary. Then we define the *differential probability of f at* (g, h) as

$$\mathrm{DP}_f(g, h) = \#\{x \in G \mid f(x) - f(x - g) = h\}/|G|.$$

Differential distributions

Definition (Differential probability [Biham, Shamir, 2009])

Let $f\colon G \to H$ be a map between finite groups G and H. Let $g \in G$ and $h \in H$ be arbitrary. Then we define the *differential probability of f at* (g,h) as

$$\mathrm{DP}_f(g,h) = \#\{x \in G \mid f(x) - f(x-g) = h\}/|G|.$$

input difference (columns); output difference (rows)

χ_3	000	001	010	011	100	101	110	111
000	1	-	-	-	-	-	-	-
001	-	1/4	-	1/4	-	1/4	-	1/4
010	-	-	1/4	1/4	-	-	1/4	1/4
011	-	1/4	1/4	-	-	1/4	1/4	-
100	-	-	-	-	1/4	1/4	1/4	1/4
101	-	1/4	-	1/4	1/4	-	1/4	-
110	-	-	1/4	1/4	1/4	1/4	-	-
111	-	1/4	1/4	-	1/4	-	-	1/4

Differential distribution for χ

Proposition (Differential probabilities for χ [Daemen,1995])

Let $n > 1$ be an arbitrary odd integer. Let $a \in \mathbb{F}_2^n$ be arbitrary. Then for any compatible $b \in \mathbb{F}_2^n$ we have $\mathrm{DP}_{\chi_n}(a, b) = 2^{-w(a)}$, where

$$w(a) = \begin{cases} n - 1 & \text{if } a = 1^n; \\ \mathrm{wt}(a) + r & \text{else,} \end{cases}$$

where r is the number of (cyclic) 001-substrings in a.

Differential distribution for χ

Proposition (Differential probabilities for χ [Daemen,1995])

Let $n > 1$ be an arbitrary odd integer. Let $a \in \mathbb{F}_2^n$ be arbitrary. Then for any compatible $b \in \mathbb{F}_2^n$ we have $\mathrm{DP}_{\chi_n}(a, b) = 2^{-w(a)}$, where

$$w(a) = \begin{cases} n-1 & \text{if } a = 1^n; \\ \mathrm{wt}(a) + r & \text{else,} \end{cases}$$

where r is the number of (cyclic) 001-substrings in a.

Let $n > 3$ be odd.

- $a = 110^{n-2} \implies$

Differential distribution for χ

Proposition (Differential probabilities for χ [Daemen,1995])

Let $n > 1$ be an arbitrary odd integer. Let $a \in \mathbb{F}_2^n$ be arbitrary. Then for any compatible $b \in \mathbb{F}_2^n$ we have $\mathrm{DP}_{\chi_n}(a, b) = 2^{-w(a)}$, where

$$w(a) = \begin{cases} n-1 & \text{if } a = 1^n; \\ \mathrm{wt}(a) + r & \text{else,} \end{cases}$$

where r is the number of (cyclic) 001-substrings in a.

Let $n > 3$ be odd.

- $a = 110^{n-2} \implies \mathrm{DP}_{\chi_n}(a, b) = \frac{1}{8}$;

Differential distribution for χ

Proposition (Differential probabilities for χ [Daemen,1995])

Let $n > 1$ be an arbitrary odd integer. Let $a \in \mathbb{F}_2^n$ be arbitrary. Then for any compatible $b \in \mathbb{F}_2^n$ we have $\mathrm{DP}_{\chi_n}(a, b) = 2^{-w(a)}$, where

$$w(a) = \begin{cases} n - 1 & \text{if } a = 1^n; \\ \mathrm{wt}(a) + r & \text{else}, \end{cases}$$

where r is the number of (cyclic) 001-substrings in a.

Let $n > 3$ be odd.

- $a = 110^{n-2} \implies \mathrm{DP}_{\chi_n}(a, b) = \frac{1}{8}$;
- $a' = 10^{n-1} \implies$

Proposition (Differential probabilities for χ [Daemen,1995])

Let $n > 1$ be an arbitrary odd integer. Let $a \in \mathbb{F}_2^n$ be arbitrary. Then for any compatible $b \in \mathbb{F}_2^n$ we have $\mathrm{DP}_{\chi_n}(a, b) = 2^{-w(a)}$, where

$$w(a) = \begin{cases} n - 1 & \text{if } a = 1^n; \\ \mathrm{wt}(a) + r & \text{else,} \end{cases}$$

where r is the number of (cyclic) 001-substrings in a.

Let $n > 3$ be odd.

- $a = 110^{n-2} \implies \mathrm{DP}_{\chi_n}(a, b) = \frac{1}{8}$;
- $a' = 10^{n-1} \implies \mathrm{DP}_{\chi_n}(a', b) = \frac{1}{4}$.

Invariant

Proposition (Differential probabilities under linear isomorphisms)

Let $G \cong H$ be isomorphic groups. Let $f : G \to G$ be a map and let $\hat{f} : H \to H$ be the map induced through the isomorphism φ. Then $\mathrm{DP}_{\hat{f}}(g, h) = \mathrm{DP}_f(\varphi^{-1}(g), \varphi^{-1}(h))$ for all $g, h \in H$.

Proposition (Differential probabilities under linear isomorphisms)

Let $G \cong H$ be isomorphic groups. Let $f\colon G \to G$ be a map and let $\hat{f}\colon H \to H$ be the map induced through the isomorphism φ. Then $\mathrm{DP}_{\hat{f}}(g, h) = \mathrm{DP}_f(\varphi^{-1}(g), \varphi^{-1}(h))$ for all $g, h \in H$.

Proposition (Differential probabilities for power functions [Blondeau, Canteaut, Charpin, 2010])

Let $0 \leq e \leq 2^n - 1$ and let $f = (\cdot)^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a power function. Then $\mathrm{DP}_f(a, b) = \mathrm{DP}_f(ya, y^e b)$ for all $y \in \mathbb{F}_{2^n}^*$.

Proposition (Differential probabilities under linear isomorphisms)

Let $G \cong H$ be isomorphic groups. Let $f : G \to G$ be a map and let $\hat{f} : H \to H$ be the map induced through the isomorphism φ. Then $\mathrm{DP}_{\hat{f}}(g, h) = \mathrm{DP}_f(\varphi^{-1}(g), \varphi^{-1}(h))$ for all $g, h \in H$.

Proposition (Differential probabilities for power functions [Blondeau, Canteaut, Charpin, 2010])

Let $0 \leq e \leq 2^n - 1$ and let $f = (\cdot)^e : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a power function. Then $\mathrm{DP}_f(a, b) = \mathrm{DP}_f(ya, y^e b)$ for all $y \in \mathbb{F}_{2^n}^*$.

Proof.

Substitute $x := yy^{-1}x =: yx'$ in

$\mathrm{DP}_f(ya, y^e b) = \#\{x \in \mathbb{F}_{2^n} \mid x^e + (x + ya)^e = y^e b\}/2^n$. □

Invariant

Proposition (Differential probabilities under linear isomorphisms)

Let $G \cong H$ be isomorphic groups. Let $f\colon G \to G$ be a map and let $\hat{f}\colon H \to H$ be the map induced through the isomorphism φ. Then $\mathrm{DP}_{\hat{f}}(g, h) = \mathrm{DP}_f(\varphi^{-1}(g), \varphi^{-1}(h))$ for all $g, h \in H$.

Proposition (Differential probabilities for power functions [Blondeau, Canteaut, Charpin, 2010])

Let $0 \leq e \leq 2^n - 1$ and let $f = (\cdot)^e\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a power function. Then $\mathrm{DP}_f(a, b) = \mathrm{DP}_f(ya, y^e b)$ for all $y \in \mathbb{F}_{2^n}^*$.

Thus, we have that the rows of the DDT all have the same number of occurrences of $0, 2, 4, \ldots$.

χ is not a power function and corollary

Theorem

Let $n \neq 1, 3$ *be a positive integer. Then* χ_n^u *is not a power function.*

χ is not a power function and corollary

Theorem

Let $n \neq 1, 3$ be a positive integer. Then χ_n^u is not a power function.

Corollary

There is no function F_n that is extended affine equivalent to χ_n (i.e., $AF_nB + C = \chi_n$), such that F_n^u is a power function.

Bounds on univariate forms of χ_n

Bounds on degrees

- Fact: Since χ_n has degree 2, all exponents in $\chi_n^u(X)$ need to have binary Hamming weight at most 2.

Bounds on degrees

- Fact: Since χ_n has degree 2, all exponents in $\chi_n^u(X)$ need to have binary Hamming weight at most 2.
- The degree of χ_n^u is bounded by $2^n - 1$ $(= \#\mathbb{F}_{2^n}^*)$.

Bounds on degrees

- Fact: Since χ_n has degree 2, all exponents in $\chi_n^u(X)$ need to have binary Hamming weight at most 2.
- The degree of χ_n^u is bounded by $2^n - 1$ $(= \#\mathbb{F}_{2^n}^*)$.
- Combining, yields maximum degrees for χ_n^u: $2^{n-1} + 2^{n-2}$.

- Fact: Since χ_n has degree 2, all exponents in $\chi_n^u(X)$ need to have binary Hamming weight at most 2.
- The degree of χ_n^u is bounded by $2^n - 1$ $(= \#\mathbb{F}_{2^n}^*)$.
- Combining, yields maximum degrees for χ_n^u: $2^{n-1} + 2^{n-2}$.

n	3	5	7	9	11	13	15	17
$\max\deg(\chi_n^u)$	6	24	96	384	1,536	6,144	24,576	98,304
$2^n - 1$	7	31	127	511	2,047	8,191	32,767	131,071

Bounds on sparsity

- Fact: Since χ_n has degree 2, all exponents in $\chi_n^u(X)$ need to have binary Hamming weight at most 2.

- Fact: Since χ_n has degree 2, all exponents in $\chi_n^u(X)$ need to have binary Hamming weight at most 2.
- $\chi_n(0^n) = 0^n$, so no constant term in $\chi_n^u(X)$.

Bounds on sparsity

- Fact: Since χ_n has degree 2, all exponents in $\chi_n^u(X)$ need to have binary Hamming weight at most 2.
- $\chi_n(0^n) = 0^n$, so no constant term in $\chi_n^u(X)$.
- Number of monomials bounded by $\binom{n}{1} + \binom{n}{2}$.

Bounds on sparsity

- Fact: Since χ_n has degree 2, all exponents in $\chi_n^u(X)$ need to have binary Hamming weight at most 2.
- $\chi_n(0^n) = 0^n$, so no constant term in $\chi_n^u(X)$.
- Number of monomials bounded by $\binom{n}{1} + \binom{n}{2}$.

n	3	5	7	9	11	13	15	17
max. mon. in χ_n^u	6	15	28	45	66	91	120	153
2^n	8	32	128	512	2,048	8,192	32,768	131,072

Number of univariate representations of χ_n

Normal elements and normal bases

Definition (Normal basis)

Consider $\mathbb{F}_2 \subset \mathbb{F}_{2^n}$. Then $\beta \in \mathbb{F}_{2^n}$ is called a *normal element* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ if the set $\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{n-1}}\}$ is a linearly independent set.

Definition (Normal basis)

Consider $\mathbb{F}_2 \subset \mathbb{F}_{2^n}$. Then $\beta \in \mathbb{F}_{2^n}$ is called a *normal element* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ if the set $\{\beta, \beta^2, \beta^{2^2}, \dots, \beta^{2^{n-1}}\}$ is a linearly independent set. When considered as an ordered set, it is called a *normal basis* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Definition (Normal basis)

Consider $\mathbb{F}_2 \subset \mathbb{F}_{2^n}$. Then $\beta \in \mathbb{F}_{2^n}$ is called a *normal element* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ if the set $\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{n-1}}\}$ is a linearly independent set. When considered as an ordered set, it is called a *normal basis* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Theorem

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a shift-invariant map.

Definition (Normal basis)

Consider $\mathbb{F}_2 \subset \mathbb{F}_{2^n}$. Then $\beta \in \mathbb{F}_{2^n}$ is called a *normal element* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ if the set $\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{n-1}}\}$ is a linearly independent set. When considered as an ordered set, it is called a *normal basis* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Theorem

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a shift-invariant map. Let β be a normal element of $\mathbb{F}_{2^n}$ and $\varphi_\beta : \mathbb{F}_2^n \to \mathbb{F}_{2^n}, \ (x_0, \ldots, x_{n-1}) \mapsto x_0\beta + \ldots + x_{n-1}\beta^{2^{n-1}}$.

Definition (Normal basis)

Consider $\mathbb{F}_2 \subset \mathbb{F}_{2^n}$. Then $\beta \in \mathbb{F}_{2^n}$ is called a *normal element* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ if the set $\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{n-1}}\}$ is a linearly independent set. When considered as an ordered set, it is called a *normal basis* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Theorem

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ *be a shift-invariant map. Let* β *be a normal element of* $\mathbb{F}_{2^n}$ *and* $\varphi_\beta : \mathbb{F}_2^n \to \mathbb{F}_{2^n},\ (x_0, \ldots, x_{n-1}) \mapsto x_0\beta + \ldots + x_{n-1}\beta^{2^{n-1}}$. *Consider the map* $F^u : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *defined by* $F^u := \varphi_\beta \circ F \circ \varphi_\beta^{-1}$.

Definition (Normal basis)

Consider $\mathbb{F}_2 \subset \mathbb{F}_{2^n}$. Then $\beta \in \mathbb{F}_{2^n}$ is called a *normal element* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ if the set $\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{n-1}}\}$ is a linearly independent set. When considered as an ordered set, it is called a *normal basis* of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

Theorem

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a shift-invariant map. Let β be a normal element of $\mathbb{F}_{2^n}$ and $\varphi_\beta\colon \mathbb{F}_2^n \to \mathbb{F}_{2^n}$, $(x_0, \ldots, x_{n-1}) \mapsto x_0\beta + \ldots + x_{n-1}\beta^{2^{n-1}}$. Consider the map $F^u\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $F^u := \varphi_\beta \circ F \circ \varphi_\beta^{-1}$. Then F^u is a polynomial function with $F^u(X) \in \mathbb{F}_2[X]$.

Different univariate expressions

- For $\mathbb{F}_{2^n} := \mathbb{F}_2[X]/(f(X))$ with $\deg f = n$.

Different univariate expressions

- For $\mathbb{F}_{2^n} := \mathbb{F}_2[X]/(f(X))$ with $\deg f = n$. The choice of the polynomial does not matter!

Different univariate expressions

- For $\mathbb{F}_{2^n} := \mathbb{F}_2[X]/(f(X))$ with $\deg f = n$. The choice of the polynomial does not matter!
- Choosing an (ordered) normal basis gives $\chi_n^u \in \mathbb{F}_2[X]$.

Different univariate expressions

- For $\mathbb{F}_{2^n} := \mathbb{F}_2[X]/(f(X))$ with $\deg f = n$. The choice of the polynomial does not matter!
- Choosing an (ordered) normal basis gives $\chi_n^u \in \mathbb{F}_2[X]$.
- Different normal elements possible.

Different univariate expressions

- For $\mathbb{F}_{2^n} := \mathbb{F}_2[X]/(f(X))$ with $\deg f = n$. The choice of the polynomial does not matter!
- Choosing an (ordered) normal basis gives $\chi_n^u \in \mathbb{F}_2[X]$.
- Different normal elements possible.
- Different orderings of the normal basis possible.

- For $\mathbb{F}_{2^n} := \mathbb{F}_2[X]/(f(X))$ with $\deg f = n$. The choice of the polynomial does not matter!
- Choosing an (ordered) normal basis gives $\chi_n^u \in \mathbb{F}_2[X]$.
- Different normal elements possible.

Theorem (Number of normal elements (Ore, 1934))

Let $n \geq 1$ be an integer. There exist precisely $\Phi_2(X^n - 1)/n$ normal elements in $\mathbb{F}_{2^n}$ (w.r.t. $\mathbb{F}_2$).

- Different orderings of the normal basis possible.

Different univariate expressions

- For $\mathbb{F}_{2^n} := \mathbb{F}_2[X]/(f(X))$ with $\deg f = n$. The choice of the polynomial does not matter!
- Choosing an (ordered) normal basis gives $\chi_n^u \in \mathbb{F}_2[X]$.
- Different normal elements possible.

Theorem (Number of normal elements (Ore, 1934))

Let $n \geq 1$ be an integer. There exist precisely $\Phi_2(X^n - 1)/n$ normal elements in $\mathbb{F}_{2^n}$ (w.r.t. $\mathbb{F}_2$).

- Different orderings of the normal basis possible.
  There are $\varphi(n)$ different orderings given a normal element.

Number of normal elements

Theorem (Number of normal elements (Ore, 1934))

Let $n \geq 1$ be an integer. There exist precisely $\Phi_2(X^n - 1)/n$ normal elements in $\mathbb{F}_{2^n}$ (w.r.t. $\mathbb{F}_2$).

Number of normal elements

Theorem (Number of normal elements (Ore, 1934))

Let $n \geq 1$ be an integer. There exist precisely $\Phi_2(X^n - 1)/n$ normal elements in $\mathbb{F}_{2^n}$ (w.r.t. $\mathbb{F}_2$).

Definition

For a polynomial $f(X) \in \mathbb{F}_2[X]$ we have $\Phi_2(f(X)) = \#(\mathbb{F}_2[X]/(f(X))^*$.

Number of normal elements

Theorem (Number of normal elements (Ore, 1934))

Let $n \geq 1$ be an integer. There exist precisely $\Phi_2(X^n - 1)/n$ normal elements in $\mathbb{F}_{2^n}$ (w.r.t. $\mathbb{F}_2$).

Definition

For a polynomial $f(X) \in \mathbb{F}_2[X]$ we have $\Phi_2(f(X)) = \#(\mathbb{F}_2[X]/(f(X))^*$.

Example

If f is irreducible, then $\Phi_2(f(X)) = 2^{\deg f} - 1$.

Number of normal elements

Theorem (Number of normal elements (Ore, 1934))

Let $n \geq 1$ be an integer. There exist precisely $\Phi_2(X^n - 1)/n$ normal elements in $\mathbb{F}_{2^n}$ (w.r.t. $\mathbb{F}_2$).

Definition

For a polynomial $f(X) \in \mathbb{F}_2[X]$ we have $\Phi_2(f(X)) = \#(\mathbb{F}_2[X]/(f(X))^*$.

Example

If f is irreducible, then $\Phi_2(f(X)) = 2^{\deg f} - 1$.

Let $f(X) = X^4 + X^3 + X + 1$, then $\Phi_2(f)$.

Theorem (Number of normal elements (Ore, 1934))

Let $n \geq 1$ be an integer. There exist precisely $\Phi_2(X^n - 1)/n$ normal elements in $\mathbb{F}_{2^n}$ (w.r.t. $\mathbb{F}_2$).

Definition

For a polynomial $f(X) \in \mathbb{F}_2[X]$ we have $\Phi_2(f(X)) = \#(\mathbb{F}_2[X]/(f(X))^*$.

Example

If f is irreducible, then $\Phi_2(f(X)) = 2^{\deg f} - 1$.

Let $f(X) = X^4 + X^3 + X + 1$, then $\Phi_2(f) = \Phi_2(X^2 + 1)\Phi_2(X^2 + X + 1)$.

Theorem (Number of normal elements (Ore, 1934))

Let $n \geq 1$ be an integer. There exist precisely $\Phi_2(X^n - 1)/n$ normal elements in $\mathbb{F}_{2^n}$ (w.r.t. $\mathbb{F}_2$).

Definition

For a polynomial $f(X) \in \mathbb{F}_2[X]$ we have $\Phi_2(f(X)) = \#(\mathbb{F}_2[X]/(f(X))^*$.

Example

If f is irreducible, then $\Phi_2(f(X)) = 2^{\deg f} - 1$.

Let $f(X) = X^4 + X^3 + X + 1$, then $\Phi_2(f) = \Phi_2(X^2 + 1)\Phi_2(X^2 + X + 1) = 2 \cdot 3 = 6$.

Number of orderings of the normal basis

Let $\gcd(k, n) = 1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$.

Number of orderings of the normal basis

Let $\gcd(k, n) = 1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0) = 0$, since χ_n is shift-invariant.

Number of orderings of the normal basis

Let $\gcd(k, n) = 1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0) = 0$, since χ_n is shift-invariant.

$n = 5,\ k = 3$:

Number of orderings of the normal basis

Let $\gcd(k, n) = 1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0) = 0$, since χ_n is shift-invariant.

$n = 5,\ k = 3$:

$$\begin{array}{ccc}
(x_0, x_1, x_2, x_3, x_4) & \xmapsto{\varphi_\beta^\sigma} & x_0\beta + x_1\beta^{2^{\sigma(1)}} + x_2\beta^{2^{\sigma(2)}} + x_3\beta^{2^{\sigma(3)}} + x_4\beta^{2^{\sigma(4)}} \\
\tau^3 \Big\downarrow & & \\
(x_3, x_4, x_0, x_1, x_2) & \xmapsto[\varphi_\beta^\sigma]{} & x_3\beta + x_4\beta^{2^{\sigma(1)}} + x_0\beta^{2^{\sigma(2)}} + x_1\beta^{2^{\sigma(3)}} + x_2\beta^{2^{\sigma(4)}}
\end{array}$$

Number of orderings of the normal basis

Let $\gcd(k, n) = 1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0) = 0$, since χ_n is shift-invariant.

$n = 5,\ k = 3$:

$$(x_0, x_1, x_2, x_3, x_4) \xmapsto{\varphi_\beta^\sigma} x_0\beta + x_1\beta^{2^{\sigma(1)}} + x_2\beta^{2^{\sigma(2)}} + x_3\beta^{2^{\sigma(3)}} + x_4\beta^{2^{\sigma(4)}}$$

$$x_0\beta + x_1\beta^{2^{\sigma(1)}} + x_2\beta^{2^{\sigma(2)}} + x_3\beta^{2^{\sigma(3)}} + x_4\beta^{2^{\sigma(4)}} \xmapsto{(\cdot)^2} x_0\beta^2 + x_1\beta^{2^{\sigma(1)+1}} + x_2\beta^{2^{\sigma(2)+1}} + x_3\beta^{2^{\sigma(3)+1}} + x_4\beta^{2^{\sigma(4)+1}}$$

$$(x_0, x_1, x_2, x_3, x_4) \xmapsto{\tau^3} (x_3, x_4, x_0, x_1, x_2)$$

$$(x_3, x_4, x_0, x_1, x_2) \xmapsto{\varphi_\beta^\sigma} x_3\beta + x_4\beta^{2^{\sigma(1)}} + x_0\beta^{2^{\sigma(2)}} + x_1\beta^{2^{\sigma(3)}} + x_2\beta^{2^{\sigma(4)}}$$

Number of orderings of the normal basis

Let $\gcd(k, n) = 1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0) = 0$, since χ_n is shift-invariant.

$n = 5,\ k = 3$:

$$(x_0, x_1, x_2, x_3, x_4) \overset{\varphi_\beta^\sigma}{\longmapsto} x_0\beta + x_1\beta^{2^{\sigma(1)}} + x_2\beta^{2^{\sigma(2)}} + x_3\beta^{2^{\sigma(3)}} + x_4\beta^{2^{\sigma(4)}}$$

$$\downarrow \tau^3 \qquad\qquad \downarrow (\cdot)^2$$

$$x_0\beta^2 + x_1\beta^{2^{\sigma(1)+1}} + x_2\beta^{2^{\sigma(2)+1}} + x_3\beta^{2^{\sigma(3)+1}} + x_4\beta^{2^{\sigma(4)+1}}$$

$$\|$$

$$(x_3, x_4, x_0, x_1, x_2) \underset{\varphi_\beta^\sigma}{\longmapsto} x_3\beta + x_4\beta^{2^{\sigma(1)}} + x_0\beta^{2^{\sigma(2)}} + x_1\beta^{2^{\sigma(3)}} + x_2\beta^{2^{\sigma(4)}}$$

Number of orderings of the normal basis

Let $\gcd(k, n) = 1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0) = 0$, since χ_n is shift-invariant.

$n = 5,\ k = 3$:

$$
\begin{array}{ccc}
(x_0, x_1, x_2, x_3, x_4) & \xmapsto{\varphi_\beta^\sigma} & x_0\beta + x_1\beta^{2^{\sigma(1)}} + x_2\beta^{2^{\sigma(2)}} + x_3\beta^{2^{\sigma(3)}} + x_4\beta^{2^{\sigma(4)}} \\
\Big\downarrow \tau^3 & & \Big\downarrow (\cdot)^2 \\
 & & x_0\beta^2 + x_1\beta^{2^{\sigma(1)+1}} + x_2\beta^{2^{\sigma(2)+1}} + x_3\beta^{2^{\sigma(3)+1}} + x_4\beta^{2^{\sigma(4)+1}} \\
 & & \Big\| \\
(x_3, x_4, x_0, x_1, x_2) & \xmapsto[\varphi_\beta^\sigma]{} & x_3\beta + x_4\beta^{2^{\sigma(1)}} + x_0\beta^{2^{\sigma(2)}} + x_1\beta^{2^{\sigma(3)}} + x_2\beta^{2^{\sigma(4)}}
\end{array}
$$

$$0 = \sigma(3) + 1,$$

Number of orderings of the normal basis

Let $\gcd(k, n) = 1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0) = 0$, since χ_n is shift-invariant.

$n = 5,\ k = 3$:

$$(x_0, x_1, x_2, x_3, x_4) \overset{\varphi_\beta^\sigma}{\longmapsto} x_0\beta + x_1\beta^{2^{\sigma(1)}} + x_2\beta^{2^{\sigma(2)}} + x_3\beta^{2^{\sigma(3)}} + x_4\beta^{2^{\sigma(4)}}$$

$$\Big\downarrow (\cdot)^2$$

$$x_0\beta^2 + x_1\beta^{2^{\sigma(1)+1}} + x_2\beta^{2^{\sigma(2)+1}} + x_3\beta^{2^{\sigma(3)+1}} + x_4\beta^{2^{\sigma(4)+1}}$$

$$\Big\| \qquad \qquad \tau^3 : (x_0, x_1, x_2, x_3, x_4) \mapsto (x_3, x_4, x_0, x_1, x_2)$$

$$(x_3, x_4, x_0, x_1, x_2) \underset{\varphi_\beta^\sigma}{\longmapsto} x_3\beta + x_4\beta^{2^{\sigma(1)}} + x_0\beta^{2^{\sigma(2)}} + x_1\beta^{2^{\sigma(3)}} + x_2\beta^{2^{\sigma(4)}}$$

$$0 = \sigma(3) + 1, \quad \sigma(1) = \sigma(4) + 1,$$

Let $\gcd(k,n)=1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0)=0$, since χ_n is shift-invariant.

$n=5,\ k=3$:

$$\begin{array}{ccc}
(x_0,x_1,x_2,x_3,x_4) & \xmapsto{\varphi_\beta^\sigma} & x_0\beta + x_1\beta^{2^{\sigma(1)}} + x_2\beta^{2^{\sigma(2)}} + x_3\beta^{2^{\sigma(3)}} + x_4\beta^{2^{\sigma(4)}} \\
\Big\downarrow \tau^3 & & \Big\downarrow (\cdot)^2 \\
 & & x_0\beta^2 + x_1\beta^{2^{\sigma(1)+1}} + x_2\beta^{2^{\sigma(2)+1}} + x_3\beta^{2^{\sigma(3)+1}} + x_4\beta^{2^{\sigma(4)+1}} \\
 & & \Big\| \\
(x_3,x_4,x_0,x_1,x_2) & \xmapsto[\varphi_\beta^\sigma]{} & x_3\beta + x_4\beta^{2^{\sigma(1)}} + x_0\beta^{2^{\sigma(2)}} + x_1\beta^{2^{\sigma(3)}} + x_2\beta^{2^{\sigma(4)}}
\end{array}$$

$$0=\sigma(3)+1, \quad \sigma(1)=\sigma(4)+1, \quad \sigma(2)=1,$$

Number of orderings of the normal basis

Let $\gcd(k,n)=1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0)=0$, since χ_n is shift-invariant.

$n=5,\ k=3$:

$$(x_0,x_1,x_2,x_3,x_4) \xmapsto{\varphi_\beta^\sigma} x_0\beta + x_1\beta^{2^{\sigma(1)}} + x_2\beta^{2^{\sigma(2)}} + x_3\beta^{2^{\sigma(3)}} + x_4\beta^{2^{\sigma(4)}}$$

$$\tau^3 \downarrow \qquad\qquad \downarrow (\cdot)^2$$

$$x_0\beta^2 + x_1\beta^{2^{\sigma(1)+1}} + x_2\beta^{2^{\sigma(2)+1}} + x_3\beta^{2^{\sigma(3)+1}} + x_4\beta^{2^{\sigma(4)+1}}$$

$$\|$$

$$(x_3,x_4,x_0,x_1,x_2) \xmapsto[\varphi_\beta^\sigma]{} x_3\beta + x_4\beta^{2^{\sigma(1)}} + x_0\beta^{2^{\sigma(2)}} + x_1\beta^{2^{\sigma(3)}} + x_2\beta^{2^{\sigma(4)}}$$

$$0=\sigma(3)+1, \quad \sigma(1)=\sigma(4)+1, \quad \sigma(2)=1, \quad \sigma(3)=\sigma(1)+1,$$

Let $\gcd(k, n) = 1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0) = 0$, since χ_n is shift-invariant.

$n = 5,\ k = 3$:

$$
\begin{array}{ccc}
(x_0, x_1, x_2, x_3, x_4) & \overset{\varphi_\beta^\sigma}{\longmapsto} & x_0\beta + x_1\beta^{2^{\sigma(1)}} + x_2\beta^{2^{\sigma(2)}} + x_3\beta^{2^{\sigma(3)}} + x_4\beta^{2^{\sigma(4)}} \\
 & & \downarrow (\cdot)^2 \\
\tau^3 \downarrow & & x_0\beta^2 + x_1\beta^{2^{\sigma(1)+1}} + x_2\beta^{2^{\sigma(2)+1}} + x_3\beta^{2^{\sigma(3)+1}} + x_4\beta^{2^{\sigma(4)+1}} \\
 & & \parallel \\
(x_3, x_4, x_0, x_1, x_2) & \underset{\varphi_\beta^\sigma}{\longmapsto} & x_3\beta + x_4\beta^{2^{\sigma(1)}} + x_0\beta^{2^{\sigma(2)}} + x_1\beta^{2^{\sigma(3)}} + x_2\beta^{2^{\sigma(4)}}
\end{array}
$$

$$0 = \sigma(3) + 1, \quad \sigma(1) = \sigma(4) + 1, \quad \sigma(2) = 1, \quad \sigma(3) = \sigma(1) + 1, \quad \sigma(4) = \sigma(2) + 1.$$

Number of orderings of the normal basis

Let $\gcd(k, n) = 1$. Solve the equation $\varphi_\beta^\sigma \circ \tau^k = (\cdot)^2 \circ \varphi_\beta^\sigma$ for $\sigma \in S_n$. We have $\sigma(0) = 0$, since χ_n is shift-invariant.

$n = 5,\ k = 3$:

$$\begin{array}{ccc}
(x_0, x_1, x_2, x_3, x_4) & \xmapsto{\varphi_\beta^\sigma} & x_0\beta + x_1\beta^{2^{\sigma(1)}} + x_2\beta^{2^{\sigma(2)}} + x_3\beta^{2^{\sigma(3)}} + x_4\beta^{2^{\sigma(4)}} \\
\big\downarrow \tau^3 & & \big\downarrow (\cdot)^2 \\
 & & x_0\beta^2 + x_1\beta^{2^{\sigma(1)+1}} + x_2\beta^{2^{\sigma(2)+1}} + x_3\beta^{2^{\sigma(3)+1}} + x_4\beta^{2^{\sigma(4)+1}} \\
 & & \Vert \\
(x_3, x_4, x_0, x_1, x_2) & \xmapsto[\varphi_\beta^\sigma]{} & x_3\beta + x_4\beta^{2^{\sigma(1)}} + x_0\beta^{2^{\sigma(2)}} + x_1\beta^{2^{\sigma(3)}} + x_2\beta^{2^{\sigma(4)}}
\end{array}$$

Thus: $\sigma = (1\ 3\ 4\ 2)$.

Polynomial automorphisms

Motivation

- For what finite fields $\mathbb{F}$ is a map $\xi_n \colon \mathbb{F}^n \to \mathbb{F}^n$, defined by

$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

  invertible?

Motivation

- For what finite fields $\mathbb{F}$ is a map $\xi_n \colon \mathbb{F}^n \to \mathbb{F}^n$, defined by

$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

  invertible?
- Not for characteristic $p > 2$:

Motivation

- For what finite fields $\mathbb{F}$ is a map $\xi_n \colon \mathbb{F}^n \to \mathbb{F}^n$, defined by
$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$
invertible?
- Not for characteristic $p > 2$:
REASON: $0^n \mapsto 0^n$ and $(p-2)^n \mapsto 0^n$,

Motivation

- For what finite fields $\mathbb{F}$ is a map $\xi_n \colon \mathbb{F}^n \to \mathbb{F}^n$, defined by

$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

  invertible?
- Not for characteristic $p > 2$:
  REASON: $0^n \mapsto 0^n$ and $(p-2)^n \mapsto 0^n$, as
  $y_i = p - 2 + (p-1)(p-2) = p(p-2)$. $\triangle$

Motivation

- For what finite fields $\mathbb{F}$ is a map $\xi_n \colon \mathbb{F}^n \to \mathbb{F}^n$, defined by

$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

  invertible?
- Most general way to view such a map is as a polynomial map:

- For what finite fields $\mathbb{F}$ is a map $\xi_n \colon \mathbb{F}^n \to \mathbb{F}^n$, defined by

$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

  invertible?
- Most general way to view such a map is as a polynomial map:

Definition (Polynomial map)

Let $\mathbb{F}[X_1, \ldots, X_n]$ be the polynomial ring in n indeterminates.

Motivation

- For what finite fields $\mathbb{F}$ is a map $\xi_n \colon \mathbb{F}^n \to \mathbb{F}^n$, defined by

$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

  invertible?
- Most general way to view such a map is as a polynomial map:

Definition (Polynomial map)

Let $\mathbb{F}[X_1, \ldots, X_n]$ be the polynomial ring in n indeterminates. A polynomial map $F \colon \mathbb{F}^n \to \mathbb{F}^n$ is a map of the form

- For what finite fields $\mathbb{F}$ is a map $\xi_n \colon \mathbb{F}^n \to \mathbb{F}^n$, defined by

$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

  invertible?
- Most general way to view such a map is as a polynomial map:

Definition (Polynomial map)

Let $\mathbb{F}[X_1, \ldots, X_n]$ be the polynomial ring in n indeterminates. A polynomial map $F \colon \mathbb{F}^n \to \mathbb{F}^n$ is a map of the form

$$(x_1, \ldots, x_n) \mapsto (F_1(x_1, \ldots, x_n), \ldots, F_n(x_1, \ldots, x_n)),$$

where $F_i(X_1, \ldots, X_n) \in \mathbb{F}[X_1, \ldots, X_n]$.

Motivation

- For what finite fields $\mathbb{F}$ is a map $\xi_n \colon \mathbb{F}^n \to \mathbb{F}^n$, defined by

$$y_i = x_i + (x_{i+1} + 1)x_{i+2}$$

  invertible?
- Most general way to view such a map is as a polynomial map:

Definition (Polynomial map)

Let $\mathbb{F}[X_1, \dots, X_n]$ be the polynomial ring in n indeterminates. A polynomial map $F \colon \mathbb{F}^n \to \mathbb{F}^n$ is a map of the form

$$(x_1, \dots, x_n) \mapsto (F_1(x_1, \dots, x_n), \dots, F_n(x_1, \dots, x_n),$$

where $F_i(X_1, \dots, X_n) \in \mathbb{F}[X_1, \dots, X_n]$.

- Related to the Jacobian conjecture!

- A polynomial map is a polynomial automorphisms if there exists a polynomial map $G\colon \mathbb{F}^n \to \mathbb{F}^n$ such that $X_i = G(F_1, \ldots, F_n)$.

Jacobian conjecture

- A polynomial map is a polynomial automorphisms if there exists a polynomial map $G\colon \mathbb{F}^n \to \mathbb{F}^n$ such that $X_i = G(F_1, \ldots, F_n)$.
- By the chain rule of calculus, the determinant of the Jacobian of a polynomial automorphism has to be invertible.

- A polynomial map is a polynomial automorphisms if there exists a polynomial map $G\colon \mathbb{F}^n \to \mathbb{F}^n$ such that $X_i = G(F_1, \ldots, F_n)$.
- By the chain rule of calculus, the determinant of the Jacobian of a polynomial automorphism has to be invertible.

Conjecture (Jacobian conjecture, characteristic 0)

If the determinant of the Jacobian of a polynomial map is invertible, then the polynomial map is a polynomial automorphism.

- A polynomial map is a polynomial automorphisms if there exists a polynomial map $G\colon \mathbb{F}^n \to \mathbb{F}^n$ such that $X_i = G(F_1, \ldots, F_n)$.
- By the chain rule of calculus, the determinant of the Jacobian of a polynomial automorphism has to be invertible.

Conjecture (Jacobian conjecture, characteristic 0)

If the determinant of the Jacobian of a polynomial map is invertible, then the polynomial map is a polynomial automorphism.

- False in characteristic p. However,

- A polynomial map is a polynomial automorphisms if there exists a polynomial map $G\colon \mathbb{F}^n \to \mathbb{F}^n$ such that $X_i = G(F_1, \ldots, F_n)$.
- By the chain rule of calculus, the determinant of the Jacobian of a polynomial automorphism has to be invertible.

Conjecture (Jacobian conjecture, characteristic 0)

If the determinant of the Jacobian of a polynomial map is invertible, then the polynomial map is a polynomial automorphism.

- False in characteristic p. However,

Theorem

Let $\mathbb{F}$ be an algebraically closed field and $F\colon \mathbb{F}^n \to \mathbb{F}^n$ an invertible polynomial function, then F is a polynomial automorphism.

Consequence(s)

- The map $\xi_n \colon \overline{\mathbb{F}_2}^n \to \overline{\mathbb{F}_2}^n$, regarded as a polynomial map has a non-invertible Jacobian.

Consequence(s)

- The map $\xi_n \colon \overline{\mathbb{F}_2}^n \to \overline{\mathbb{F}_2}^n$, regarded as a polynomial map has a non-invertible Jacobian.
- By previous theorem, as a polynomial function ξ_n is not invertible.

Consequence(s)

- The map $\xi_n \colon \overline{\mathbb{F}_2}^n \to \overline{\mathbb{F}_2}^n$, regarded as a polynomial map has a non-invertible Jacobian.
- By previous theorem, as a polynomial function ξ_n is not invertible.
- There exists a (finite) field extension $\mathbb{F}_{2^k}$ of $\mathbb{F}_2$ where ξ_n is not invertible.

Consequence(s)

- The map $\xi_n \colon \overline{\mathbb{F}_2}^n \to \overline{\mathbb{F}_2}^n$, regarded as a polynomial map has a non-invertible Jacobian.
- By previous theorem, as a polynomial function ξ_n is not invertible.
- There exists a (finite) field extension $\mathbb{F}_{2^k}$ of $\mathbb{F}_2$ where ξ_n is not invertible.

Conjecture

Let n, k be positive integers greater than 1 and n odd. Then $\xi_n \colon \mathbb{F}_{2^k}^n \to \mathbb{F}_{2^k}^n$ is not invertible.

Consequence(s)

- The map $\xi_n \colon \overline{\mathbb{F}_2}^n \to \overline{\mathbb{F}_2}^n$, regarded as a polynomial map has a non-invertible Jacobian.
- By previous theorem, as a polynomial function ξ_n is not invertible.
- There exists a (finite) field extension $\mathbb{F}_{2^k}$ of $\mathbb{F}_2$ where ξ_n is not invertible.

Conjecture

Let n, k be positive integers greater than 1 and n odd. Then $\xi_n \colon \mathbb{F}_{2^k}^n \to \mathbb{F}_{2^k}^n$ is not invertible.

- If the conjecture holds for prime k, then it holds.

Consequence(s)

- The map $\xi_n \colon \overline{\mathbb{F}_2}^n \to \overline{\mathbb{F}_2}^n$, regarded as a polynomial map has a non-invertible Jacobian.
- By previous theorem, as a polynomial function ξ_n is not invertible.
- There exists a (finite) field extension $\mathbb{F}_{2^k}$ of $\mathbb{F}_2$ where ξ_n is not invertible.

Conjecture

Let n, k be positive integers greater than 1 and n odd. Then $\xi_n \colon \mathbb{F}_{2^k}^n \to \mathbb{F}_{2^k}^n$ is not invertible.

- If the conjecture holds for prime k, then it holds.
- The conjecture holds for $k = 2, 3$.

Consequence(s)

- The map $\xi_n \colon \overline{\mathbb{F}_2}^n \to \overline{\mathbb{F}_2}^n$, regarded as a polynomial map has a non-invertible Jacobian.
- By previous theorem, as a polynomial function ξ_n is not invertible.
- There exists a (finite) field extension $\mathbb{F}_{2^k}$ of $\mathbb{F}_2$ where ξ_n is not invertible.

Conjecture

Let n, k be positive integers greater than 1 and n odd. Then $\xi_n \colon \mathbb{F}_{2^k}^n \to \mathbb{F}_{2^k}^n$ is not invertible.

- If the conjecture holds for prime k, then it holds.
- The conjecture holds for $k = 2, 3$.
- If the conjecture holds for prime n, then it holds, [Otal, 2023]

Consequence(s)

- The map $\xi_n \colon \overline{\mathbb{F}_2}^n \to \overline{\mathbb{F}_2}^n$, regarded as a polynomial map has a non-invertible Jacobian.
- By previous theorem, as a polynomial function ξ_n is not invertible.
- There exists a (finite) field extension $\mathbb{F}_{2^k}$ of $\mathbb{F}_2$ where ξ_n is not invertible.

Conjecture

Let n, k be positive integers greater than 1 and n odd. Then $\xi_n \colon \mathbb{F}_{2^k}^n \to \mathbb{F}_{2^k}^n$ is not invertible.

- If the conjecture holds for prime k, then it holds.
- The conjecture holds for $k = 2, 3$.
- If the conjecture holds for prime n, then it holds, [Otal, 2023]
- The conjecture holds. [Graner, Kriepke, Krompholz, Kyureghyan, 2024]

Conclusions

- The map χ_n has order $2^{\lfloor \lg(n) \rfloor}$.

Conclusions

- The map χ_n has order $2^{\lfloor \lg(n) \rfloor}$.
- The state diagram of χ is known, and

Conclusions

- The map χ_n has order $2^{\lfloor \lg(n) \rfloor}$.
- The state diagram of χ is known, and
- χ is surjective.

Conclusions

- The map χ_n has order $2^{\lfloor \lg(n) \rfloor}$.
- The state diagram of χ is known, and
- χ is surjective.
- The map χ_n is never a power function for $n \neq 1, 3$.

Conclusions

- The map χ_n has order $2^{\lfloor \lg(n) \rfloor}$.
- The state diagram of χ is known, and
- χ is surjective.
- The map χ_n is never a power function for $n \neq 1, 3$.
- There are clear bounds on the degree and sparsity.

Conclusions

- The map χ_n has order $2^{\lfloor \lg(n) \rfloor}$.
- The state diagram of χ is known, and
- χ is surjective.
- The map χ_n is never a power function for $n \neq 1, 3$.
- There are clear bounds on the degree and sparsity.
- The number of different univariate expressions for χ_n^u is given by

Conclusions

- The map χ_n has order $2^{\lfloor \lg(n) \rfloor}$.
- The state diagram of χ is known, and
- χ is surjective.
- The map χ_n is never a power function for $n \neq 1, 3$.
- There are clear bounds on the degree and sparsity.
- The number of different univariate expressions for χ_n^u is given by

$$\frac{\Phi_2(X^n - 1) \cdot \varphi(n)}{n}.$$

Conclusions

- The map χ_n has order $2^{\lfloor \lg(n) \rfloor}$.
- The state diagram of χ is known, and
- χ is surjective.
- The map χ_n is never a power function for $n \neq 1, 3$.
- There are clear bounds on the degree and sparsity.
- The number of different univariate expressions for χ_n^u is given by

$$\frac{\Phi_2(X^n - 1) \cdot \varphi(n)}{n}.$$

- ξ_n is almost never invertible.

Conclusions

- The map χ_n has order $2^{\lfloor \lg(n) \rfloor}$.
- The state diagram of χ is known, and
- χ is surjective.
- The map χ_n is never a power function for $n \neq 1, 3$.
- There are clear bounds on the degree and sparsity.
- The number of different univariate expressions for χ_n^u is given by

$$\frac{\Phi_2(X^n - 1) \cdot \varphi(n)}{n}.$$

- ξ_n is almost never invertible.

Thank you for your attention!