Bijective properties of χ

Joan Daemen, Jan Schoone

Radboud University (The Netherlands)

ESCADA meeting

10 September 2020

Part I

Introduction and goal

We consider the quadratic map χ_n:

$$\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$$
$$(a_0, \ldots, a_{n-1}) \mapsto (b_0, \ldots, b_{n-1})$$

where $b_i = a_i + (a_{i+1} + 1)a_{i+2}$ (indices modulo n).

Goal: To determine for which n the map χ_n is injective/surjective/bijective.

Examples

- χ_2: $\chi_2(00) = 00$, $\chi_2(01) = 00$, $\chi_2(10) = 00$, $\chi_2(11) = 11$.
- χ_3:

(a_0, a_1, a_2)	$\chi_3(a_2, a_1, a_0)$
000	000
001	101
010	011
011	010
100	110
101	001
110	100
111	111

Lemma

Let A and B be **finite** *sets of equal cardinality, i.e., $A \sim B$. Let $f : A \to B$ be a map from A to B.*

If f is injective, then f is bijective.

If f is surjective, then f is bijective.

This is not true for infinite sets, e.g.,

$$f : \mathbb{N} \to \mathbb{N}, \ x \mapsto x + 1.$$

So if χ_n is surjective, it is also injective and hence bijective.

By checking some small values for n, one can see that χ_n is bijective iff n is odd.

Lemma

If $\chi_n(a)_i = 1$, then $a_{i-1} = \chi_n(a)_{i-1}$.

Proof.

Case 1: $a_i = 1$. Then $\chi_n(a)_{i-1} = a_{i-1} + (a_i + 1)a_{i+1} = a_{i-1}$, as required. Case 2: $a_i = 0$. Then $1 = \chi_n(a)_i = (a_{i+1} + 1)a_{i+2}$. So $a_{i+1} = 0$. Then $\chi_n(a)_{i-1} = a_{i-1} + (a_i + 1)a_{i+1} = a_{i-1}$, as required. □

Lemma

We can express a_{i-2} in terms of a_i and $\chi_n(a)$ as:

$$\begin{cases} a_{i-2} = \chi_n(a)_{i-2} & \text{if } a_i = 0; \\ a_{i-2} = \chi_n(a)_{i-1} + \chi_n(a)_{i-2} + 1 & \text{if } a_i = 1. \end{cases}$$

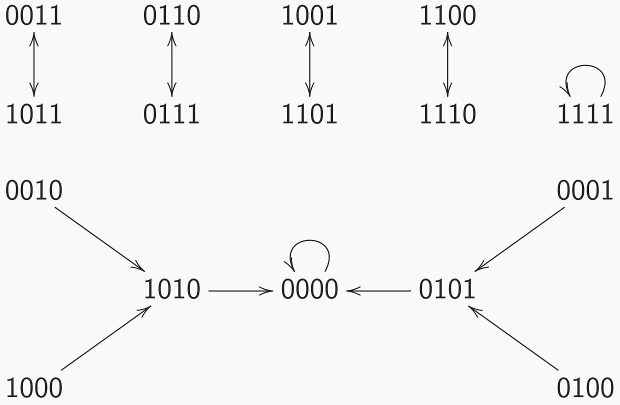
Results so far

- Algorithmically determine preimages under χ_n when n is odd
  - when state contains at least one 1
- Algorithmically determine preimages under χ_n when n is even
  - when state contains at least one 1 in an odd position, *and*
  - when state contains at least one 1 in an even position

More examples

Let n be even. Then $\chi_n((01)^{n/2}) = \chi_n((10)^{n/2}) = \chi_n(0^n) = 0^n$.

Can we determine a preimage of 0001 under χ_4?



Conclusions

- For odd n:
  - All-but-one state have at least one 1
  - All those states have a (unique) preimage
  - χ_n maps 0^n to 0^n
  - So we have shown that χ_n is bijective if n is odd
- For even n:
  - There are $2^{n/2}$ states with no 1 in an even position ($\rightarrow S_0$)
  - There are $2^{n/2}$ states with no 1 in an odd position ($\rightarrow S_1$)
  - 0^n satisfies both conditions and has three originals
  - $2^{n/2+1} - 1$ states are not proven to have a (unique) preimage
  - Everywhere else χ_n is bijective ($\rightarrow T$)

Goal is met

- Goal:
  - To determine for which n the map χ_n is injective/surjective/bijective.
  - When n is odd, the map χ_n is bijective.
  - When n is even, the map χ_n is not injective/surjective/bijective.
- New goals:
  - For even n,
    - to determine the states not in $\operatorname{Im} \chi_n$.
    - to determine all many-to-one states in $\mathbb{F}_2^n$.

Part II

Studying S_0 and S_1

- $\mathbb{F}_2^n = S_0 \cup S_1 \cup T$
- $\chi_n\big|_T : T \to T$ is bijective
- States not reached are in $S_0 \cup S_1$
- S_0 and S_1 are similar, so we just look at S_0

Intermezzo: Shift-invariant maps

Let $(\ggg 1)\colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ (x_0, \ldots, x_{n-1}) \mapsto (x_{n-1}, x_0, \ldots, x_{n-2})$ be the *right-shift* map.

- $(\ggg 1)$ is linear;
- We can define $(\ggg k) := (\ggg 1)^k$;
- $(\ggg 1)$ is bijective, $(\lll 1) = (\ggg 1)^{-1} = (\ggg n-1) = (\ggg 1)^{n-1}$.

Definition

A map $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called shift-invariant if for all $k(< n)$ we have

$$F \circ (\ggg k) = (\ggg k) \circ F.$$

Lemma

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a map such that $F \circ (\gg 1) = (\gg 1) \circ F$. Then F is shift-invariant.

Proof.

Induction to k. □

Lemma

χ_n is shift-invariant (for any $n \geq 1$).

Proof.

$$\begin{aligned}
\chi_n((a_0, \ldots, a_{n-1}) \gg 1) &= \chi_n(a_{n-1}, a_0, \ldots, a_{n-2}) \\
&= (a_{n-1} + (a_0 + 1)a_1, \ldots, a_{n-2} + (a_{n-1} + 1)a_0) \\
&= (a_0 + (a_1 + 1)a_2, \ldots, a_{n-1} + (a_0 + 1)a_1) \gg 1
\end{aligned}$$

$S_0 = \{x \in \mathbb{F}_2^n \mid x_i = 0 \text{ when } i \equiv 0 \pmod 2\}$.

$$\chi_n(0, x_1, 0, x_3, 0, \ldots, x_{n-3}, 0, x_{n-1}) = (y_0, y_1, \ldots, y_{n-2}, y_{n-1})$$

where

$$\begin{aligned}
y_0 &= 0 + (x_1 + 1) \cdot 0 = 0, \\
y_1 &= x_1 + (0 + 1)x_3 = x_1 + x_3, \\
y_2 &= 0 + (x_3 + 1) \cdot 0 = 0, \\
&\ldots \\
y_{n-2} &= 0 + (x_{n-1} + 1) \cdot 0 = 0 \\
y_{n-1} &= x_{n-1} + (0 + 1)x_1 = x_{n-1} + x_1
\end{aligned}$$

We see: $\chi_n(S_0) \subset S_0$!

If we restrict the map

$$\pi_0 \colon \mathbb{F}_2^{2k} \to \mathbb{F}_2^k,\ (x_0, x_1, \ldots, x_{2k-1}) \mapsto (x_1, x_3, \ldots, x_{2k-1})$$

to S_0, we get a bijection.

Then we define $\chi_k^L := \pi_0|_{S_0}^{-1} \circ \chi_{2k} \circ \pi_0$.

Definition

Let $k \geq 1$. We write $\chi_k^L \colon \mathbb{F}_2^k \mapsto \mathbb{F}_2^k,\ (x_0, \ldots, x_{k-1}) \mapsto (x_0 + x_1, x_1 + x_2, \ldots, x_{k-1} + x_0)$ for the linearized even-length χ on S_0 (or S_1).

Let $\mathbb{F}$ be a field and V, W finite-dimensional $\mathbb{F}$-vector spaces. Let $L\colon V \to W$ be a linear map.

Let $\operatorname{Ker} L = \{x \in V \mid L(x) = 0\}$, and $\operatorname{Im} L = \{y \in W \mid \exists x \in V : L(x) = y\}$.

Theorem (Isomorphism Theorem)

We have

$$V / \operatorname{Ker} L \cong \operatorname{Im} L.$$

Corollary

$\dim V - \dim \operatorname{Ker} L = \dim \operatorname{Im} L.$

Determining image of linearized χ

Reminder: If A is the matrix that corresponds to a linear map L, then $\operatorname{Im} L = \operatorname{col}(A)$.

Our case:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ \vdots & & & & \ddots & & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 & 1 \end{pmatrix}$$

All columns have even Hamming weight, so all vectors in $\operatorname{Im} L$ have even Hamming weight.

Determining kernel and image of χ_k^L

Reminder: $\chi_k^L(x_0, \dots, x_{k-1}) = (x_0 + x_1, x_1 + x_2, \dots, x_{k-1} + x_0)$.

For $\chi_k^L(x) = 0$ to hold, we must have

$$x_0 = x_1 = x_2 = \dots = x_{k-1}$$

hence $\operatorname{Ker} \chi_k^L = \{0^k, 1^k\}$.

By the isomorphism theorem we find that $\dim \operatorname{Im} L = k - 1$.

Thus $\operatorname{Im} L$ is exactly the set of all vectors of even Hamming weight.

Example for χ_3^L

χ_3^L is defined as

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_0 + x_1 \\ x_1 + x_2 \\ x_2 + x_0 \end{pmatrix}$$

Then $\operatorname{Im} \chi_3^L$ is the set

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\}$$

Now by using the definition of χ_k^L, or by just adding zeroes, we find

Theorem

Let $n > 1$ be even. Then $\operatorname{Im}\chi_n$ consists of elements with even Hamming weight such that either:

- *All odd positions are* 0*, or;*
- *All even positions are* 0*.*

We had $|T| = 2^n - (2^{n/2+1} - 1)$ states with a unique preimage.

We see that $\frac{1}{2}|S_0|$ states have no preimage, and $\frac{1}{2}|S_1|$ states have no preimage.

So $|S_0| = 2^{n/2}$ states with no preimage.

Remaining states: $2^{n/2} - 1$ that might have more than one preimage.

Part III

Goal and results so far

We determined the states that are not in $\operatorname{Im}\chi_n$.

They are those with odd Hamming weight in $S_0 \cup S_1$.

The remaining goal is to determine all many-to-one states in $\mathbb{F}_2^n$.

We already know that we need to look in $S_0 \cup S_1$.

A new lemma

Recall that $\operatorname{Ker} \chi_k^L = \{0^k, 1^k\}$.

We have: if $\chi_k^L(u) = \chi_k^L(v)$ then $u = v$ or $u = v + 1^k$.

By composing this with π_0^{-1}, (since $\chi_n(S_i) \subset S_i$) we find

Lemma

Let n be a positive integer. If $a, b \in \mathbb{F}_2^n$ are such that $\chi_n(a) = \chi_n(b) \neq 0$, then either

- *$a, b \in S_0$ and $a + b = (10)^{n/2}$; or*
- *$a, b \in S_1$ and $a + b = (01)^{n/2}$.*

So every non-zero element in $\mathbb{F}_2^n$ has at most two preimages under χ_n.

Counting and conclusions

We have $2^{n/2} - 1$ states that might have more than one preimage.

One of those has three preimages, namely 0^n.

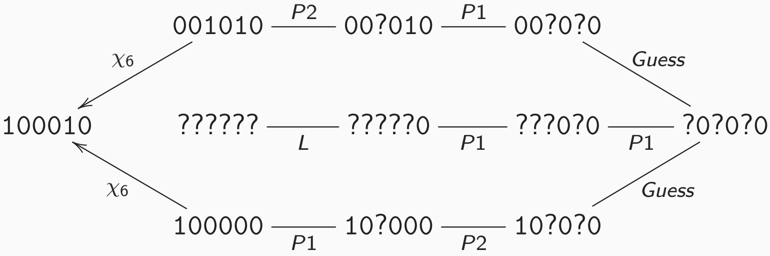
We have $2^{n/2+1} - 1$ states that have an *image*.

Excluding the three states that map to 0^n, we have $2^{n/2+1} - 4$ states that need to map to the $2^{n/2} - 2$ non-zero states in $\operatorname{Im} \chi_n$ that we do not know yet.

This is exactly two-to-one.

Example

Consider the state 100010. What is its preimage under χ_6?



L: If $\chi_n(x)_i = 1$, then $x_{i-1} = \chi_n(x)_{i-1}$.

P1: If $x_i = 0$, then $x_{i-2} = \chi_n(x)_{i-2}$.

P2: If $x_i = 1$, then $x_{i-2} = \chi_n(x)_{i-1} + \chi_n(x)_{i-2} + 1$.

Conclusions

We have now determined the states not in $\operatorname{Im}\chi_n$: The states with odd Hamming weight in $S_0 \cup S_1$.

We have also determined all many-to-one states in $\mathbb{F}_2^n$. The elements in $(S_0 \cup S_1) \setminus \{0^n, (01)^{n/2}, (10)^{n/2}\}$ are mapped two-to-one to states with even Hamming weight in $S_0 \cup S_1$. The elements $0^n, (01)^{n/2}, (10)^{n/2}$ are mapped to 0^n.

New goal:

To determine whether χ is injective/surjective/bijective on infinite states.

Part IV

Introducing χ on infinite states and first result

We write $\widehat{\mathbb{F}_2}$ for the vector space of infinite binary sequences.

$\chi\colon \widehat{\mathbb{F}_2} \to \widehat{\mathbb{F}_2},\ (x_0, x_1, x_2, \ldots) \mapsto (y_0, y_1, y_2, \ldots)$

where

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

Examples:

$$\chi(\overline{01}) = \overline{0}$$
$$\chi(\overline{10}) = \overline{0}$$
$$\chi(\overline{0}) = \overline{0}$$

Clearly, χ is not injective.

Introducing period spaces

Definition

Let $n \geq 1$ be a positive integer. A state $\sigma \in \widehat{\mathbb{F}_2}$ is called *n-periodic* if $\sigma \ll n = \sigma$. We call the minimal such n the *period* of σ. We write Σ_n for the set of all n-periodic states.

$$\Sigma_1 = \{\overline{0}, \overline{1}\}$$
$$\Sigma_2 = \{\overline{0}, \overline{1}, \overline{01}, \overline{10}\}$$

Lemma

We have $\Sigma_n \subset \Sigma_{nk}$ for all $n, k \geq 1$. Furthermore Σ_n is a linear subspace of $\widehat{\mathbb{F}_2}$ for all $n \geq 1$ and we have the isomorphism $\Sigma_n \cong \mathbb{F}_2^n$.

Applying period spaces

- χ is shift-invariant (similar proof)
- $\chi(\Sigma_n) \subset \Sigma_n$
  - $\sigma \in \Sigma_n$: $\sigma \ll n = \sigma$;
  - $\chi(\sigma) = \chi(\sigma \ll n) = \chi(\sigma) \ll n$;
  - $\chi(\sigma) \in \Sigma_n$.
- $\chi_n = \chi\big|_{\Sigma_n}$

Reusable results

We can use the results from χ_n now:

- χ is bijective on states of odd period
- χ is bijective on states of even period that have a 1 in both an odd and an even position
- χ is surjective on non-zero states of even period that have even Hamming weight (two-to-one if even positions all 0 or odd positions all 0)
- χ is three-to-one on zero state

To investigate:

- χ on non-zero states of even period with odd Hamming weight with even positions all 0 (or odd positions all 0)

Theorem

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

Proof.

Let σ be a state of even period n with odd Hamming weight and even positions all 0 (or odd positions all 0). Then σ is also $2n$-periodic. The state $\sigma|\sigma$ has even Hamming weight, but still all even positions 0. Hence it has a preimage under χ_{2n}. Hence χ is surjective. $\square$

Outro

Conclusions

χ is surjective

χ_n is bijective if n is odd

χ_n is not surjective if n is even