Radboud University

# Cyclic properties of even-period $\chi$

Joan Daemen, Jan Schoone

Radboud University

ESCADA meeting

25 March 2020

ESCADA

# Part I

Consider the space $\mathbb{F}_2^{\mathbb{N}}$ of infinite binary sequences.

**Definition**

A state $\sigma \in \mathbb{F}_2^{\mathbb{N}}$ is called *n*-periodic if

$$\sigma \ll n = \sigma.$$

We write $\Sigma_n$ for the set of all *n*-periodic states.

**Lemma**

*For each $n \geq 1$ we find that $\Sigma_n$ is an $\mathbb{F}_2$-vector space of dimension $n$.*

# Introduction and goal - II

We consider, for even $n$, the quadratic map $\chi_n$:

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

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

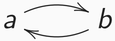
This $\chi_n$ corresponds to $\chi_{|\Sigma_n} \colon \Sigma_n \to \Sigma_n$.

We will study graphs of $\chi_n$ for $n = 2^k \cdot 3$ in this presentation.

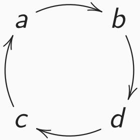
# Example: $k = 1$, $n = 6$

1 time:

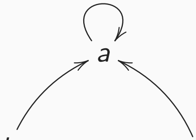

Name: 1-cycle 12 times:




Name: 2-cycle 6 times:




Name: 4-cycle 1 time:



# Example: $k = 1$, $n = 6$ 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 |

$$S_0 := \{x \in \mathbb{F}_2^n \mid x_i = 0 \text{ when } i \equiv 0 \pmod 2\}$$
$$S_1 := \{x \in \mathbb{F}_2^n \mid x_i = 0 \text{ when } i \equiv 1 \pmod 2\}$$
$$T := \mathbb{F}_2^n \setminus (S_0 \cup S_1)$$

We know that $\chi_n$ is bijective on $T$.

Also $\chi_n(S_i) \subset S_i$, and every non-zero element in $S_0$ has two preimages.

Since $\chi_n$ is shift-invariant ( $\chi_n(x \lll 1) = \chi_n(x) \lll 1$ ), we can focus on $S_1$ only.

Removing all zeroes in odd positions:

$$\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^{n/2},\ (x_0, x_1, \ldots, x_{n-1}) \mapsto (x_0, x_2, \ldots, x_{n-2})$$

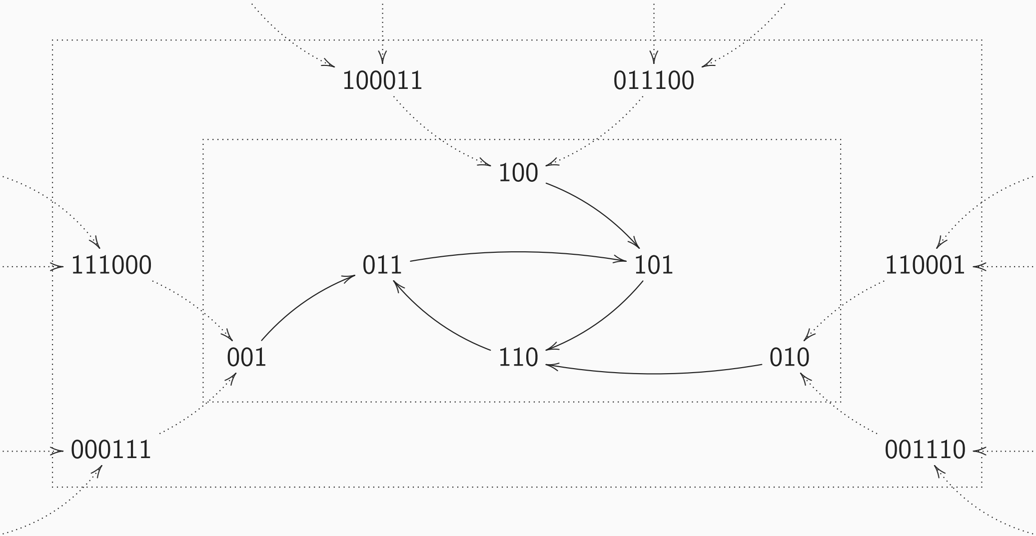
This is bijective on $S_1$.

$$\begin{array}{ccc} \mathbb{F}_2^n & \xrightarrow{\ \pi\ } & \mathbb{F}_2^{n/2} \\ {\scriptstyle \chi_n}\downarrow & & \downarrow{\scriptstyle ?} \\ \mathbb{F}_2^n & \xrightarrow[\ \pi\ ]{} & \mathbb{F}_2^{n/2} \end{array} \qquad\qquad \begin{array}{ccc} S_1 & \xhookrightarrow{\ \pi\ } & \mathbb{F}_2^{n/2} \\ {\scriptstyle \chi_n}\downarrow & & \downarrow{\scriptstyle \chi^L} \\ S_1 & \xhookrightarrow[\ \pi\ ]{} & \mathbb{F}_2^{n/2} \end{array}$$

$$\chi_k^L\colon \mathbb{F}_2^k \to \mathbb{F}_2^k,\ (x_0, x_1, \ldots, x_{k-1}) \mapsto (x_0 + x_1, x_1 + x_2, \ldots, x_{k-1} + x_0)$$

# Part II

# Example: $k = 1, n = 6$ revisited



# A new vector space

Vector space isomorphism

$$\varphi\colon \mathbb{F}_2^n \to \mathbb{F}_2[X]/(X^n+1)$$
$$(a_0,\dots,a_{n-1}) \mapsto \sum_{i=0}^{n-1} a_i X^{n-(i+1)}$$

Since $n = 2^k \cdot 3$, by the Chinese Remainder Theorem:

$$\mathbb{F}_2[X]/(X^n+1) \cong \mathbb{F}_2[X]/(X+1)^{2^k} \times \mathbb{F}_2[X]/(X^2+X+1)^{2^k}$$

# Equivalence of maps

1) A left-shift is just a multiplication by $X$;

We have

$$X \cdot \varphi(a_0, \dots, a_{n-1}) = X \cdot \sum_{i=0}^{n-1} a_i X^{n-(i+1)} = \sum_{i=0}^{n-1} a_i X^{n-i} = \sum_{j=-1}^{n-2} a_{j+1} X^{n-(j+1)}$$

while

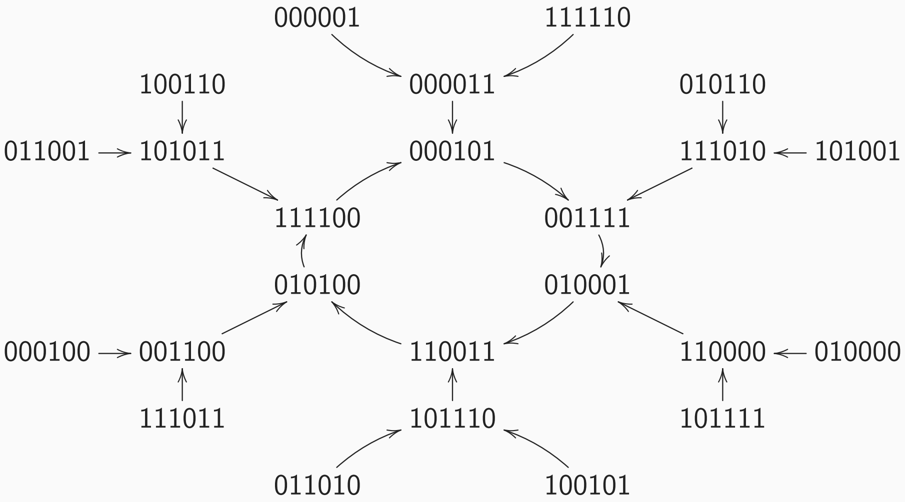
$$\varphi((a_0, \dots, a_{n-1}) \ll 1) = \varphi(a_1, \dots, a_{n-1}, a_0) = \sum_{i=0}^{n-1} a_{i+1} X^{n-(i+1)}$$

These terms are equal for all indices from 0 to $n-2$. We compare the term for $j=-1$ and $i=n-1$ and check if they are equal. They are: $a_0 X^n = a_0$ and $a_n X^0 = a_0$ since indices are modulo $n$.

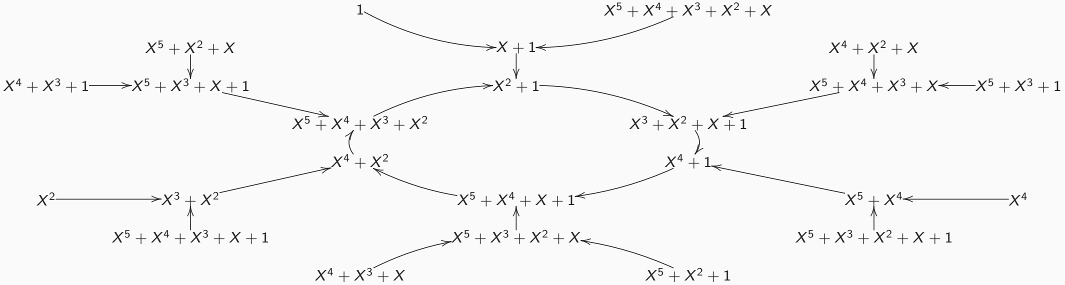
2) $\chi_k^L = \mathrm{Id} + (\ll 1)$;

We have $\chi_k^L(x_0, x_1, \dots, x_{n-1}) = (x_0 + x_1, x_1 + x_2, \dots, x_{n-1} + x_0)$, while on the other

# Example for $k = 2, n = 12$



# Example for $k = 2, n = 12$; polynomially



# Part III

**Lemma**

*Let for a state $\sigma$ be denoted $f_\sigma(X)$ for its polynomial representation.*

*Then $\sigma$ has two preimages of the same period if and only if $X+1 \mid f_\sigma(X)$.*

**Proof.**

$$\begin{aligned}\sigma \text{ has two preimages of the same period } & \text{iff } \mathcal{H}(\sigma) \equiv 0 \pmod 2 \\ & \text{iff } f_\sigma(X) \text{ has an even number of terms} \\ & \text{iff } f_\sigma(1) = 0 \\ & \text{iff } X+1 \mid f_\sigma(X).\end{aligned}$$

□

**Lemma**

*Let $\sigma$ be a $2^k \cdot 3$-periodic state and $f_\sigma(X)$ be its polynomial representation.*

*We have: $X^{2^{k-2} \cdot 3} + 1 \mid f_\sigma(X)$, if and only if $\sigma$ is $2^{k-1} \cdot 3$-periodic.*

**Proof.**

Sketch fFor $k = 2$:

$\Longrightarrow$ :) Let $f_\sigma(X)$ be given for a certain $\sigma$ be divisible by $X^3 + 1$. Let $c(X)$ be such that $f_\sigma(X) = c(X) \cdot (X^3 + 1)$. Then the coefficients of the right-handside correspond to a bit-vector:

$$\sigma = (c_0 + c_3, c_1 + c_4, c_2 + c_5, c_3 + c_0, c_4 + c_1, c_5 + c_2)$$

Hence we see that $\sigma$ is indeed 6-periodic. $\Leftarrow$:) Let $\sigma$ be 6-periodic. Then $\sigma = (\sigma_0, \sigma_1, \sigma_2, \sigma_0, \sigma_1, \sigma_2)$. We can solve the system $\sigma_0 = c_0 + c_3$, $\sigma_1 = c_1 + c_4$, $\sigma_2 = c_2 + c_5$ for its two solutions. They are each others complement, so both will

**Lemma**

*Let* $k \in \{1, 2\}$. *Let* $\sigma$ *be a state of period* $2^k \cdot 3$ *and* $f_\sigma(X)$ *be its polynomial representation. If* $X^k + 1 \mid f_\sigma(X)$, *then* $\sigma$ *appears in a cycle.*

**Conjecture**

*The above lemma is true for all* $k \geq 1$, *albeit with* $X^{2^{k-1}} + 1$ *instead of* $X^k + 1$.

The previous results hold for $2^k \cdot p$.

**Question**

*Do similar results also hold for $2^k \cdot pq$ with $p$ and $q$ different primes?*

**Question**

*Do similar results also hold for $2^k \cdot p^2$?*

Thank you for your attention!