Radboud University

Order of odd-period χ

Joan Daemen, Jan Schoone

Radboud University

ESCADA meeting

10 February 2021

ESCADA

χ_n and shift invariance

$$\chi_n\colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto y$$
$$y_i = x_i + (x_{i+1}+1)x_{i+2} \qquad \text{(indices modulo } n\text{)}$$
$$\tau_n\colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto y$$
$$y_i = x_{i+1} \qquad \text{(indices modulo } n\text{)}$$
$$\tau_n\colon (x_0, x_1, \ldots, x_{n-1}) \mapsto (x_1, \ldots, x_{n-1}, x_0)$$

We have $\chi_n \circ \tau_n = \tau_n \circ \chi_n$. (*Shift invariance*)

Example

$\chi_5(00101) = (10001)$, then $\chi_5(01010) =$?0?0?0?1?.1.

Lemma

Write $\chi_n(x) = y$. *If* $y_i = 1$, *then* $y_{i-1} = x_{i-1}$.

Proposition

Write $\chi_n(x) = y$. *Then* $x_{i-2} = y_{i-2} + x_i(y_{i-1} + 1)$.

Corollary

If n *is odd, then* χ_n *is invertible.*

Example

$\chi_5^{-1}(10001) = ?0?0?1?0?.1$.

Let X be a set. We denote $\mathrm{Sym}(X)$ for the set of all permutations on X.

Proposition

The set $\mathrm{Sym}(\mathbb{F}_2^n)$ *is a group under composition, with* $\mathrm{id}\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *as neutral element.*

Proposition

$\#\,\mathrm{Sym}(\mathbb{F}_2^n) = 2^n!$

For odd n, we have $\chi_n \in \mathrm{Sym}(\mathbb{F}_2^n)$.

By Lagrange's Theorem, χ_n has a finite order that is a divisor of $2^n!$.

In particular $\chi_n^{\mathrm{ord}(\chi_n)} = \mathrm{id}$ and $\chi_n^{-1} = \chi_n^{\mathrm{ord}(\chi_n)-1}$.

Theorem (Order of χ_n)

Let $n > 0$ be odd. Then

$$\operatorname{ord}(\chi_n) = 2^{\lceil \lg(\frac{n+1}{2}) \rceil}$$

Example

- $\operatorname{ord}(\chi_3) = 2^{\lceil \lg(\frac{4}{2}) \rceil} = 2^{\lceil 1 \rceil} = 2$;
- $\operatorname{ord}(\chi_5) = 2^{\lceil \lg(\frac{6}{2}) \rceil} = 2^{\lceil \lg 3 \rceil} = 4$;
- $\operatorname{ord}(\chi_7) = 2^{\lceil \lg(\frac{8}{2}) \rceil} = 2^2 = 4$;
- $\operatorname{ord}(\chi_9) = 2^{\lceil \lg(\frac{10}{2}) \rceil} = 2^{\lceil \lg 5 \rceil} = 8$.

$1, 2, 4, 4, 8, 8, 8, 8, 16, 16, \ldots$

Orbits and Sierpinski's triangle

Definition (Orbit)

Given a map $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and an element $a \in \mathbb{F}_2^n$, the *orbit of a under F* is the set $\mathcal{O}_F(a) = \{F^k(a) \mid k \geq 0\}$.

Proposition

$$\operatorname{ord}(F) = \operatorname*{lcm}_{x \in \mathbb{F}_2^n}(\#\mathcal{O}_F(x))$$

We conjecture that:
$\#\mathcal{O}_{\chi_n}(0^{n-1}1) = 2^{\lceil \lg(\frac{n+1}{2}) \rceil}$.

							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

Lemma

Let $\sigma = (0^{n-1}1)^*$, where n is odd. Then for all $i \geq 0$ we have:

- *For all $1 \leq k \leq \frac{n-1}{2}$ we have $\chi_n^i(\sigma)_{n-2k} = 0$;*
- *$\chi_n^i(\sigma)_{n-1} = 1$.*

Proof.

Induction on i. We start with $i = 1$ and make a case distinction on k to prove the first statement. For $k = 1$, we have

$\chi_n(\sigma)_{n-2} = \sigma_{n-2} + (\sigma_{n-1} + 1)\sigma_n = \sigma_{n-2} + 0 \cdot \sigma_n = 0$, since $\sigma_{n-1} = 1$.For $1 < k \leq \frac{n-1}{2}$, we consider $\chi_n(\sigma)_{n-2k}$. We have $\chi_n(\sigma)_{n-2k} = \sigma_{n-2k} + (\sigma_{n-2k+1} + 1) \cdot \sigma_{n-2k+2} = 0 + (\sigma_{n-2k+1} + 1) \cdot 0 = 0$.Now we prove the second statement for $i = 1$. We have

$$\chi_n(\sigma)_{n-1} = \sigma_{n-1} + (\sigma_0 + 1) \cdot \sigma_1 = 1 + 0 = 1.$$

Projection map $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^{\frac{n+1}{2}}$, $(x_0, \ldots, x_{n-1}) \mapsto (x_0, x_2, \ldots, x_{n-1})$

Bijective on $S = \{x \in \mathbb{F}_2^n \mid x_i = 0 \text{ when } i \equiv 1 \pmod 2\}$.

Then $\chi'_n = \pi \circ \chi_n \circ \pi^{-1}_{|S}$.

In a formula: $\chi'_n(a)_i = a_i + a_{i+1}$ for all $i = 0, \ldots, \frac{n-1}{2}$, and $\chi'_n(a)_{\frac{n+1}{2}} = a_{\frac{n+1}{2}}$.

Vector space isomorphism $\psi\colon \mathbb{F}_2^k \to \mathbb{F}_2[X]/(X^k)$, determined by

$$\psi\colon (a_0, a_1, \ldots, a_{k-1}) \mapsto a_0 X^{k-1} + a_1 X^{k-2} + \ldots + a_{k-2} X + a_{k-1}.$$

Set $L_{\chi_n} = \psi \circ \chi'_n \circ \psi^{-1}$.

Then:

$$L_{\chi_n}(f(X)) = f(X) \cdot (X+1).$$

$$
\begin{array}{ccc}
S(x_0, 0, \ldots, x_{n-3}, 0, x_{n-1}) & \xmapsto{\chi_n \quad \chi_n} & S(x_0 + x_2, 0, \ldots, x_{n-3} + x_{n-1}, \\
\downarrow \pi & & \downarrow \pi \\
\mathbb{F}_2^{\frac{n+1}{2}}(x_0, x_2, \ldots, x_{n-3}, x_{n-1}) & \xmapsto[\chi_n']{\chi_n'} & \mathbb{F}_2^{\frac{n+1}{2}}(x_0 + x_2, \ldots, x_{n-3} + x_{n-} \\
\downarrow \psi & & \downarrow \psi \\
\mathbb{F}_2[X]/(X^{\frac{n+1}{2}})x_0 X^{\frac{n-1}{2}} + x_2 X^{\frac{n-3}{2}} + \ldots + x_{n-1} & \xmapsto[L_{\chi_n}]{} & \mathbb{F}_2[X]/(X^{\frac{n+1}{2}})(x_0 + x_2)X^{\frac{n-1}{2}} + \ldots + (x_{n-}
\end{array}
$$

Proving the lower bound: algebra

Then $\#\mathcal{O}_{\chi_n}(0^{n-1}1) = \text{ord}(1+X)$.

Lemma

$\#\mathbb{F}_2[X]/(X^{\frac{n+1}{2}})^* = 2^{\frac{n-1}{2}}$.

Proof.

Since $\mathbb{F}_2[X]$ is a Euclidean ring, we have that $f \in \mathbb{F}_2[X]/(X^{\frac{n+1}{2}})$ is invertible if and only if $\gcd(f, X^{\frac{n+1}{2}}) = 1$. If $f_0 = 0$ (the constant term of f), then $\gcd(f, X^{\frac{n+1}{2}}) \neq 1$, since X is a divisor of both f and $X^{\frac{n+1}{2}}$. Since only positive powers of X are divisors of $X^{\frac{n+1}{2}}$ and all these are not divisors of f with $f_0 = 1$, we find that when $f_0 = 1$, that $\gcd(f, X^{\frac{n+1}{2}}) = 1$.

In summary, since $f \in \mathbb{F}_2[X]/(X^{\frac{n+1}{2}})^*$ iff $f_0 = 1$, we find that $\#\mathbb{F}_2[X]/(X^{\frac{n+1}{2}})^* = 2^{\frac{n-1}{2}}$. □

By Lagrange's Theorem, we now know that the order of $1 + X$ is a power of 2.

Definition (Strand)

Every string of odd length that starts with a 1 that is followed by a repeated pattern of $*0$ is called a *strand*. Let $\mathfrak{S}_n$ be the set of strands of length $2n+1$.

Example

$\mathfrak{S}_0 = \{1\}$, $\mathfrak{S}_1 = \{100, 110\}$, $\mathfrak{S}_2 = \{10000, 11000, 10010, 11010\}$.

Proposition

Let σ be a non-zero state of odd period n. Then there exists a canonical way to split up σ into strands.

Notation

Let σ be a state of odd period. Then its unique decomposition into strands is denoted as s_1 - s_2 - $\cdots$ - s_l.

Full theorem: Strands II

Proposition

Let σ be a state of odd period n. Write $\sigma = s_1$ - s_2 - $\cdots$ - s_l as its decomposition into strands. Then $\chi_n(\sigma) = s'_1$ - s'_2 - $\cdots$ - s'_l, where $|s_i| = |s'_i|$.

Proof.

Fix some $1 \leq i \leq l$ arbitrarily. Write $s_i = (\sigma_j, \sigma_{j+1}, \ldots, \sigma_{j+|s_i|-1})$. We have $\sigma_j = 1$ and want to show that $\chi_n(\sigma)_j = 1$. If $|s_i| = 1$, then $\sigma_{j+1} = 1$, hence

$$\chi_n(\sigma)_j = \sigma_j + (1+1)\sigma_{j+2} = 1.$$

When $|s_i| > 1$, then $\sigma_{j+2} = 0$, hence

$$\chi_n(\sigma)_j = \sigma_j + (\sigma_{j+1} + 1) \cdot 0 = \sigma_j = 1.$$

Let $1 \leq k \leq \frac{|s_i|-1}{2}$ be arbitrary. We have $\sigma_{j+2l} = 0$ and we want to see that $\chi_n(\sigma)_{j+2k} = 0$. We have that $\sigma_{j+2k+2} = 0$, hence

Proof of full theorem

Let $\sigma = s_1 \text{ - } s_2 \text{ - } \cdots \text{ - } s_l$ be a non-zero state of length n. Then

$$\begin{aligned}
\#\mathcal{O}_{\chi_n}(\sigma) &= \operatorname*{lcm}_{i\in\{1,\dots,l\}} (\#\mathcal{O}_{\chi_{|s_i|+1}}(s_i\|1)) \\
&= \operatorname*{lcm}_{i\in\{1,\dots,l\}} (2^{\lceil \lg(\frac{|s_i|+1}{2}) \rceil}) \\
&= \max_{i\in\{1,\dots,l\}} (2^{\lceil \lg(\frac{|s_i|+1}{2}) \rceil}) \\
&= 2^{\lceil \lg(\frac{|s_{i_0}|+1}{2}) \rceil}
\end{aligned}$$

where i_0 is chosen such that $|s_{i_0}| = \max_i |s_i|$.

In particular $\operatorname{ord}(\chi_n) = \max_{\sigma\in\mathbb{F}_2^n} \#\mathcal{O}_{\chi_n}(\sigma) = 2^{\lceil \lg(\frac{n+1}{2}) \rceil}$.