Radboud University

The state diagram of χ

Joan Daemen, Jan Schoone
Radboud University

FrisiaCrypt

26 September 2022

ESCADA

What do KECCAK-f, Ascon, Rasta, Subterranean 2.0 and Xoodyak have in common?

$$\chi \text{ (on } \mathbb{F}_2^n \text{ for (different) odd } n)$$

Determine the state diagram of χ, by techniques involving:

- Linearization;
- Topology.

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

We have $\chi \circ \tau = \tau \circ \chi$. (*Shift invariance*)

Example

Since $\chi((10111)^*) = (00111)^*$ we have $\chi((01111)^*) = (01110)^*$.

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 then more specifically say that σ is *n-periodic*.
- The minimal such integer 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 $\mathbb{F}_2^n$.

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

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 $\Delta_n = \Delta_{-n}$.

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

Theorem (Daemen, 1995)

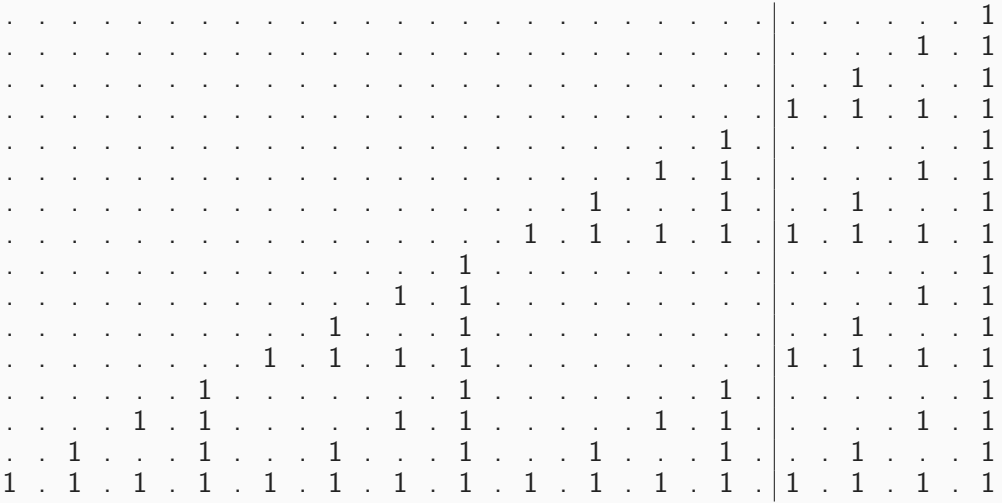
If n is odd, then χ_n is invertible.

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 $2^{\lfloor \lg(n) \rfloor}$.

Visualisation



Cycle lengths in state diagram

The cycle length is based upon the longest strand in the strand decomposition of a state.

Definition

An *anchor* is a 1 that is followed by an even number of 0s. A *strand* is a substring that starts with an anchor and stops just before the next anchor. The *strand decomposition* is a decomposition of the state σ as s_1-s_2-...-s_k, where each s_i is a strand.

Example

Consider $(100001001)^*$: $\implies$ $\underline{1}0000\underline{1}00\underline{1}$ $\implies$ 10000-100-1. Thus cycle length 4.

Example

Consider $(1000010110)^*$: $\implies$ $\underline{1}000010\underline{1}10$ $\implies$ 1000010-110. Thus cycle length 4.

χ is surjective on periodic states

For odd n, χ_n is surjective.

For even n, χ_n is not surjective.

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}.

Proposition

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

Finding preimages

Write $\chi(x) = y$.

Proposition

- *If* $y_i = 1$, *then* $x_{i-1} = y_{i-1}$.
- $x_{i-2} = y_{i-2} + x_i(y_{i-1} + 1)$.

Corollary

- *If* n *is odd, then* x *can be uniquely determined from* y.
- *If* n *is even and there exist* $i \not\equiv j \pmod 2$ *with* $y_i = y_j = 1$, *then* x *can be uniquely determined from* y.

Other cases, there has is a guess to be made, hence two preimages.

Definition

A *topology* on a set X is a collection $\mathcal{T}$ of subsets of X, called the *open sets*, satisfying:

- $\varnothing, X \in \mathcal{T}$;
- any union of elements in $\mathcal{T}$ is again in $\mathcal{T}$;
- any finite intersection of elements in $\mathcal{T}$ is again in $\mathcal{T}$.

Example

The real numbers with the Euclidean distance metric make a topological space when the open sets are defined as:

A set E is open if and only if for every $x \in E$, there exists some $B_r(x) \subset E$, where $B_r(x) = \{y \in \mathbb{R} \mid 0 < |y - x| < r\}$.

Example

For any indexed family of topological spaces $(X_i)_{i \in I}$, we can define a topological space on the product $X = \prod X_i$ of those sets.

Definition

The *product topology* consists of basis-open-sets of the form $\prod U_i$, where each U_i is open in X_i, and for all but finitely many coordinates, we have $U_i = X_i$. The open sets are these basis-open-sets and any unions of them.

Definition

A map $f : X \to Y$ between topological spaces is continuous, if for every open $V \subset Y$, we have that $f^{-1}(V)$ is open in X.

Example

In the Euclidean metric space, the above definition of continuous coincides with the 'regular' $\varepsilon - \delta$-definition of continuous function.

Theorem

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 $f_{|A} : A \to A$ is surjective. Then f is surjective.

Definition

A topological space $(X, \mathcal{T})$ is *compact* if for every $(U_i)_{i \in I} \in \mathcal{T}$ with $\bigcup_{i \in I} U_i = X$, there exists some $J \subset I$ finite, with $\bigcup_{i \in J} U_i = X$.

Example

Any finite topological space $(X, \mathcal{T})$ is compact.

Any set X with the discrete topology is compact if and only if X is finite.

Namely, take $(\{x\})_{x \in X}$ as open cover.

Example

The real line $\mathbb{R}$ is not compact. Take $(B_2(n))_{n \in \mathbb{Z}}$ as open cover.

χ is continuous and surjective

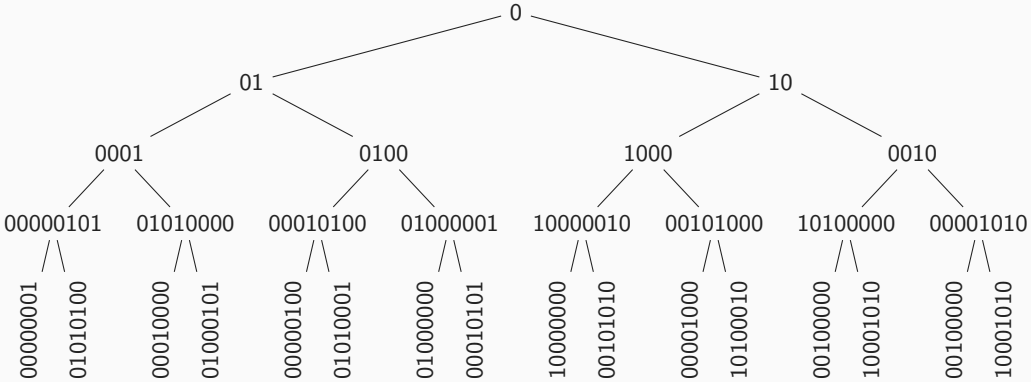
χ is a continuous map from $\mathbb{F}_2^{\mathbb{Z}}$ to $\mathbb{F}_2^{\mathbb{Z}}$ using this product topology.

$\widehat{\mathbb{F}_2}$ is dense in $\mathbb{F}_2^{\mathbb{Z}}$

Theorem

$\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}},\ (x_i)_{i\in\mathbb{Z}} \mapsto (y_i)_{i\in I}$ *with* $y_i = x_i + (x_{i+1}+1)x_{i+2}$ *is surjective.*

States with period 2^n: I



States with period 2^n: II

The sets $S_{2^n,0}$ and $S_{2^n,1}$ together contain all the 2^n-periodic states where χ does not act bijectively.

Proposition

The 2^n-periodic states in $S_{2^n,0} \cup S_{2^n,1}$ occupy the first $2^{n-1}+1$ rows in the binary tree.

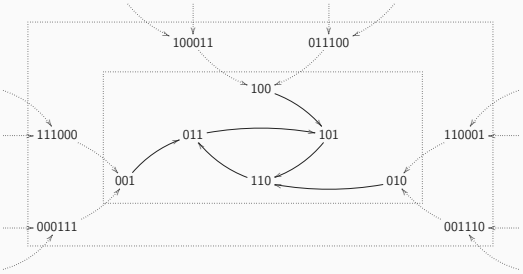
For a state σ in $S_{n,0}$, one can represent the state by a polynomial. We denote this polynomial by $f_\sigma(X)$.

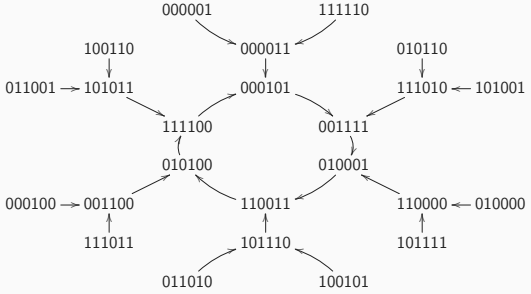
Proposition

For a state in $S_{2^n,0}$ or $S_{2^n,1}$ it is now possible to deduce where in the tree it is, by computing $\gcd(f_\sigma(X), X^{2^{\frac{n}{2}}}+1)$ with the Euclidean algorithm.

Disregarding 0s in even positions, χ becomes
$(x_0, \ldots, x_{k-1}) \mapsto (x_0 + x_1, x_1 + x_2, \ldots, x_{k-1} + x_0)$.

Thus, χ becomes linear.





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 $S_{n,0}$ (or $S_{n,1}$). 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.

Conclusions

The order of χ_n is $2^{\lfloor \lg(n) \rfloor}$ for odd n.

Given a state upon which χ acts bijectively, find the cycle length.

$\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective.

We have deduced the structure of the snowflakes in the state diagram of χ.