Noname manuscript No.
(will be inserted by the editor)

The state diagram of χ

Jan Schoone (✉) · Joan Daemen

Received: date / Accepted: date

Abstract In symmetric cryptography, block ciphers, stream ciphers and permutations often make use of a round function and many round functions consist of a linear and a non-linear layer. One that is often used is based on the cellular automaton that is denoted by χ as a Boolean map on bi-infinite sequences, $\mathbb{F}_2^{\mathbb{Z}}$. It is defined by $\sigma \mapsto \nu$ where each $\nu_i = \sigma_i + (\sigma_{i+1} + 1)\sigma_{i+2}$. A map χ_n is a map that operates on n-bit arrays with periodic boundary conditions. This corresponds with χ restricted to periodic infinite sequences with period that divides n. This map χ_n is used in various permutations, e.g., KECCAK-f (the permutation in SHA-3), ASCON (the NIST standard for lightweight cryptography), Xoodoo, Rasta and Subterranean (2.0).

In this paper, we characterize the graph of χ on periodic sequences. It turns out that χ is surjective on the set of *all* periodic sequences.

We will show what sequences will give collisions after one application of χ. We prove that, for odd n, the order of χ_n (in the group of bijective maps on $\mathbb{F}_2^n$) is $2^{\lceil \lg(\frac{n+1}{2}) \rceil}$.

A given periodic sequence lies on a cycle in the graph of χ, or it can be represented as a polynomial. By regarding the divisors of such a polynomial one can see whether it lies in a cycle, or after how many iterations of χ it will.

Furthermore, we can see, for a given σ, the length of the cycle in its component in the state diagram. Finally, we extend the surjectivity of χ to $\mathbb{F}_2^{\mathbb{Z}}$, thus to include non-periodic sequences.

Keywords boolean maps · cellular automata · chi · cryptography · state diagram · symmetric cryptography

Acknowledgements This research is supported by the European Research Council under the ERC advanced grant agreement under grant ERC-2017-ADG Nr. 788980 ESCADA. The

Jan Schoone
Digital Security, Radboud University, Nijmegen
E-mail: jan.schoone@ru.nl

Joan Daemen
Digital Security, Radboud University, Nijmegen

authors would like to thank Wieb Bosma and Marloes Venema for proofreading (parts of) the text and helpful suggestions.

Data availability statement
This manuscript has no associated data.

1 Introduction

Block ciphers or permutations are usually iterative, often they are SPNs. Those repeat a simple round function, that usually consists of a linear (affine) layer and a non-linear layer. This non-linear layer is often based on one of the Boolean maps χ_n. For each n, the map $\chi_n \colon \mathbb{F}_2^n \to \mathbb{F}_2^n,\ x \mapsto y$ are defined by $y_i = x_i + (x_{i+1} + 1)x_{i+2}$, where the indices are taken modulo n. It is used as χ_5 in Keccak-f [1], the permutation in SHA-3 [10], and also χ_5 in ASCON [7], the NIST standard for lightweight cryptography [11]. In Xoodoo [4], the value of n is 3, i.e., χ_3, while in Rasta [6], it is equal to the block length (always odd). The width of permutation in each of these permutations is larger than the circle length of χ_n, so the bits of the sequence are partitioned in n-bit circles and χ_n is applied to each of these circles in parallel. In Subterranean [2] and Subterranean 2.0 [5], χ_{257} is applied on the entire state as one circle. We study these maps by considering the map on bi-infinite sequences, as the map $\chi \colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}},\ \sigma \mapsto \nu$ that is defined by $\nu_i = \sigma_i + (\sigma_{i+1} + 1)\sigma_{i+2}$. This map is actually the state updating transformation of a cellular automaton as in [15].

It is known from [3], that χ_n is bijective if and only if n is odd. We revisit a proof of this in Section 4. The examples above use χ_n for odd n, as iterating an invertible round function gives a permutation, but using a non-invertible round function will result in collisions. Having collisions might result in finding concrete distinguishers to attack ciphers.

However, it may just be interesting to have χ_n where, e.g., $n = 512$, to have χ operate on states of lengths a power of 2. In this case, however, it is necessary to know how many collisions we have, or, equivalently, how many states have more than one preimages. If we characterize the state diagram of χ, we can observe this for each n. In particular χ_n is the restriction of χ to sequences with period dividing n. For instance, the sequence that follows the pattern '01' infinitely in both directions is a sequence of period 2.

By randomizing the input, like in the Even-Mansour construction ([8]), we can use that χ_n is a "near-permutation" on, e.g., $n = 512$ bits. By a "near-permutation", we mean that out of the 2^{512}, only a negligible number of $2^{257} - 1$ states do not have a unique preimage. Since the inputs are randomized, there is only a very small probability (2^{-257}) of collisions.

Our contributions We show that the order of χ_n (in the group of bijections on $\mathbb{F}_2^n$) is $2^{\lceil \lg(\frac{n+1}{2}) \rceil}$, when n is odd. An application is then that the inverse of χ_n is just a composition of χ_n with itself $2^{\lceil \lg(\frac{n+1}{2}) \rceil} - 1$ times.

We furthermore prove that χ is surjective on $\mathbb{F}_2^{\mathbb{Z}}$. This is done with a linearization technique in Section 4 and extended to nonperiodic states with a topological argument in Section 7.

For each state whereupon χ has exactly one preimage, we can immediately observe by the degrees of associated polynomials what the length of its cycle (orbit) is.

Furthermore, using linearization techniques similar to those in Section 4, we are able to deduce that the non-invertible component of the state diagram for states of period 2^k for any k is a binary tree, where the root is mapped to itself.

Lastly, we combine these techniques, to find the remaining components of the state diagram with the states of even period $2^k \cdot m$ with $m > 1$. The states in the cycle of a component all have the same period. The further one goes away from the cycle (by taking preimages), the larger the period grows by factors 2.

We can determine whether a state lies in the cycle, by checking whether it is divisble by a certain polynomial or after how many applications of χ it will become part of the cycle. For the length of the cycle when $n = 2m$ with m odd, we see that it always is a divisor of $2^o - 1$, where o is the multiplicative order of 2 modulo $n/2$. The length of a cycle when $n = 2^k \cdot m$ is just 2^{k-1} times the length of the cycle for $n = 2m$.

2 Notations and conventions

For a map $F\colon X \to Y$ and a subset $A \subset X$ we write $F_{|A}\colon A \to F(A)$ for the map F restricted to A. Given two maps $F\colon X \to Y$ and $G\colon Y \to Z$, we write $G \circ F\colon X \to Z$ for the composition of the maps.

With $\mathbb{Z}$ we denote the ring of integers, and by $\mathbb{N}$ the set of natural numbers. We write $\mathbb{N}^*$ for the set of positive integers. We denote an arbitrary field by $\mathbb{F}$ and the finite field of two elements by $\mathbb{F}_2$. Additionally, we have the notation $\mathbb{F}_2^n$ for the standard n-dimensional $\mathbb{F}_2$-vector space, obtained as the Cartesian product of n copies of $\mathbb{F}_2$. For the vector space of infinitely long binary sequences, we write $\mathbb{F}_2^{\mathbb{Z}}$, since we see infinitely long binary sequences as infinite in both directions.

The elements of $\mathbb{F}_2$ are called *bits*. The elements of $\mathbb{F}_2^{\mathbb{Z}}$, or (for any positive integer n), $\mathbb{F}_2^n$ we call *states*. For those in $\mathbb{F}_2^n$, we use Latin lowercase symbols as x, y. For infinitely long states, we use Greek lowercase symbols as σ, ν, ρ.

We write $0^n \in \mathbb{F}_2^n$ for a state of n bits 0, and 1^n for a state of n bits 1.

A state $\sigma \in \mathbb{F}_2^{\mathbb{Z}}$ that has a repeating part $\sigma_0, \sigma_1, \ldots, \sigma_{n-1}$, for a certain n, we write $\sigma = (\sigma_0\sigma_1 \cdots \sigma_{n-1})^*$. Most often we take the shortest possible n. For example, for the bi-infinite state of all zeroes we write 0^*. In the same fashion we can write $(01)^*$ for a bi-infinite state of repeating pattern '01' and not $(0101)^*$. If we write $(*1)^n$, we mean a state of length $2n$ where each second bit is 1 and each other bit can be either 0 or 1. A $*$ denotes that it can be either 0 or 1.

The number of ones in a finite state $x \in \mathbb{F}_2^n$ is called the *Hamming weight* and is denoted as $\mathrm{hw}(x)$.

When V is a vector space over $\mathbb{F}$, then we use $[\![v_1, \ldots, v_n]\!]$ as notation for the set spanned by the vectors $v_1, \ldots, v_n \in V$, i.e.,

$$[\![v_1, \ldots, v_n]\!] = \left\{ \sum_i \lambda_i v_i \mid \lambda_i \in \mathbb{F} \right\}.$$

Furthermore, we write $\mathbb{F}_2[X]$ for the ring of polynomials in the indeterminate X with coefficients in $\mathbb{F}_2$. If we write $\mathbb{F}_2[X]/(f(X))$, we mean the quotient ring of

$\mathbb{F}_2[X]$ by the ideal generated by the polynomial $f(X)$. For any commutative ring R, we write R^* for its group of units.

Lastly, we write lg for the binary logarithm, i.e., the logarithm with base 2, gcd for the greatest common divisor in a Euclidean ring and lcm for the least common multiple.

3 Shift maps, periodicity and state diagrams

Here, we discuss shift maps, and from those define which states are periodic. Next, we discuss shift-invariant maps and their state diagrams. We start with giving the definition of χ, the subject of this paper.

Definition 1 (χ) The map $\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}},\ \sigma \mapsto \nu$ is, for all $i \in \mathbb{Z}$, given by $\nu_i = \sigma_i + (\sigma_{i+1} + 1)\sigma_{i+2}$.

We see that χ is a map of degree two, in particular nonlinear.

3.1 Shift maps and periodic states

To study the state diagram of χ, we will use shift maps, as they partition the vector space $\mathbb{F}_2^{\mathbb{Z}}$. The state diagram then consists of many isomorphic components, as per this partition.

Definition 2 (Shift maps) For any field $\mathbb{F}_2$ we define a shift map τ on $\mathbb{F}_2^{\mathbb{Z}}$ as:

$$\tau\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}},\ \sigma \mapsto \nu, \qquad \text{where } \nu_i = \sigma_{i+1}.$$

For any integer $k > 0$ we can define τ^k by iteration τ. For $k < 0$, we define τ^k on $\mathbb{F}_2^{\mathbb{Z}}$ by iterating $\tau^{-1}(\sigma) = \nu$ where $\nu_i = \sigma_{i-1}$.

These shift maps are linear. The group $\{\tau^k \mid k \in \mathbb{Z}\}$ under composition is isomorphic to $(\mathbb{Z}, +)$. Some of the infinite states in $\mathbb{F}_2^{\mathbb{Z}}$ are invariant under a subgroup of shifts.

Definition 3 (Periodic states) A state $\sigma \in \mathbb{F}_2^{\mathbb{Z}}$ is called *periodic* when there exists an integer $n > 0$ such that $\tau^n(\sigma) = \sigma$. The minimal such integer n for which σ is periodic, is called the *period* of σ. We then write $\mathrm{per}(\sigma) = n$. We furthermore write $\mathfrak{P}_n$ for the set of all states of period n. We lastly denote the set of all periodic states by $\bigcup_n \mathfrak{P}_n = \widehat{\mathbb{F}_2}$.

We extend the definition of Hamming weight for finite length binary strings to periodic infinite strings by setting $\mathrm{hw}((\sigma_1, \ldots, \sigma_n)^*) = \mathrm{hw}(\sigma_1, \ldots, \sigma_n)$ for σ of period n.

For example, $\mathfrak{P}_1 = \{0^*, 1^*\}$ and $\mathfrak{P}_2 = \{(01)^*, (10)^*\}$.

We define $\mathfrak{S}_n = \bigcup_{d|n} \mathfrak{P}_d$ for the set of all states that have a period that divides n.

Lemma 1 *The set $\mathfrak{S}_n$ is a linear subspace of the vector space $\mathbb{F}_2^{\mathbb{Z}}$ and we have $\mathfrak{S}_n \cong \mathbb{F}_2^n$.*

Proof Since τ^k is a linear map for every $k \geq 1$, and $\mathfrak{S}_n$ is the set of all vectors invariant under τ^n, we find that $\mathfrak{S}_n$ is a linear subspace of $\mathbb{F}_2^{\mathbb{Z}}$. We have $\#\mathfrak{S}_n = 2^n$, and since $\mathfrak{S}_n$ is a vector space, the isomorphism holds. □

We can specify the isomorphism as

$$\phi\colon \mathfrak{S}_n \to \mathbb{F}_2^n,\ (\sigma_0 \cdots \sigma_{n-1})^* \mapsto (\sigma_0, \ldots, \sigma_{n-1}).$$

We now see that $\widehat{\mathbb{F}_2} = \bigcup_{n=1}^{\infty} \mathfrak{P}_n = \bigcup_{n=1}^{\infty} \mathfrak{S}_n \cong \bigcup_{n=1}^{\infty} \mathbb{F}_2^n$. In particular the sets $\mathfrak{P}_n$ form a partition of $\widehat{\mathbb{F}_2}$.

We can now define an equivalent of χ on $\mathbb{F}_2^n$:

Definition 4 (χ_n) We define $\chi_n\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ as $\chi_n := \phi^{-1} \circ \chi_{\big|_{\mathfrak{S}_n}} \circ \phi$. That is, $\chi_n(x) = y$ where $y_i = x_i + (x_{i+1} + 1)x_{i+2}$ with indices taken modulo n.

The cryptographic functions mentioned in the introduction all use one of the maps χ_n on some $\mathfrak{S}_n$ for some odd n.

The shift maps make for a further partition of the sets $\mathfrak{S}_n$.

Definition 5 (Shift equivalent) Two states $\sigma, \rho \in \mathbb{F}_2^{\mathbb{Z}}$ are *shift equivalent* if and only if $\sigma = \tau^k(\rho)$ for some $k \in \mathbb{Z}$.

Shift equivalence can be used it to partition each $\mathfrak{P}_n$ into equivalence classes of cardinality n. We call these *necklaces*.

Example 1 Consider $\mathfrak{P}_5$. Then $(00101)^*$ and $(01010)^*$ are shift equivalent. Since all states $\sigma \in \mathfrak{P}_5$ have period 5, their necklaces have 5 elements. The number of states in $\mathfrak{P}_5$ is $2^5 - 2^1 = 30$ and therefore $\mathfrak{P}_5$ has six shift classes. A system of representatives is given by the states in Figure 1, that also contains their propagation under χ.

Let n be any positive integer, then the number of states in $\mathfrak{P}_n$ can be computed from the number of states in $\mathfrak{S}_d$ with $d \mid n$ by the principle of inclusion-exclusion:

$$\#\mathfrak{P}_n = \sum_{d|n} \mu(n/d)\#\mathfrak{S}_d = \sum_{d|n} \mu(n/d)2^d.$$

The μ in this formula is the Möbius-function ([9]).

3.2 Shift-invariant maps and state diagrams

We will now discuss maps that are invariant under shift maps. Such a map has a simplified state diagram, where several components are isomorphic and can be translated into each other by a shift map.

Definition 6 (Shift-invariant maps) A map $G\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is called shift invariant if we have $G \circ \tau = \tau \circ G$.

A shift-invariant map always maps elements in a certain necklace to elements in the same necklace. Any shift-invariant map can therefore be studied by studying the induced quotient map on these necklaces.

One finds that χ and χ_n are shift invariant.

Lemma 2 *Both* $\chi\colon \widehat{\mathbb{F}_2} \to \widehat{\mathbb{F}_2}$ *and for each* n, $\chi_n\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *are shift invariant.*

One can recognize a shift-invariant map by seeing that for each y_i we have the same formula with respect to i with y is the image under the function. Note that a shift-invariant map does not necessarily has to be given in this form, thus it cannot always be recognized as such.

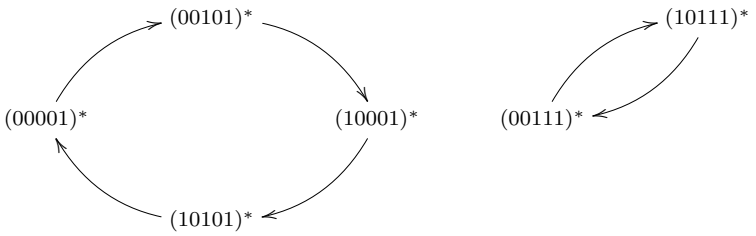


Fig. 1 Canonical states in $\mathfrak{P}_5$ and their propagation under χ.

The image of a state of period n under a shift-invariant map will have a period that is a divisor of n:

Lemma 3 *Let a state* $\sigma \in \widehat{\mathbb{F}_2}$ *have* $\mathrm{per}(\sigma) = n$. *Let* $\psi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ *be a shift-invariant map. Then the period of* $\psi(\sigma)$ *divides* n.

Proof We have $\tau^n(\psi(\sigma)) = \psi(\tau^n(\sigma)) = \psi(\sigma)$. □

Definition 7 (State diagram) Let S be a set. The *state diagram* for a map $F\colon S \to S$ is a directed graph (V, A) containing all elements in S as vertices, i.e., $V = S$. Arrows exist from a vertex a to a vertex b if and only if $F(a) = b$. Thus $A = \{(a, F(a)) \mid a \in S\}$.

When a map F is shift invariant, the state diagram can be depicted by giving the state diagram of the induced quotient map on necklaces. In that sense, Figure 1 represents the state diagram of χ_5. When a necklace has k elements, then each (connected) component of the state diagram of the induced quotient map occurs k times in the state diagram of F. For instance, the 4-cycle and 2-cycle in Figure 1 each appear 5 times.

Orbits of elements are clearly visible in the state diagram of a map.

Definition 8 (Orbit) Let S be a set. Given a map $F\colon S \to S$ and an element $a \in S$, the *orbit* of a under F is the set $\mathcal{O}_F(a) = \{F^k(a) \mid k \geq 0\}$.

Note that for any $F\colon S \to S$, any orbit has cardinality at most $\#S$. When F is a bijective map on a finite set, it is a standard result that the state diagram of F consists of disjoint cycles. In this case, all orbits are cycles. Hence, for bijective F, we can determine the order of F by looking at the state diagram and the lengths of the cycles:

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

Any finite component of a graph, is either a cycle or of the form a cycle with trees on its vertices. We can therefore talk about the number k of applications of F needed on an element $a \in S$ such that $F^k(a)$ is on the cycle.

Definition 9 (Layer numbers) Let S be a set and $F\colon S \to S$ be a map. Let C be a component of the state diagram of F. We define the *layers* of the component as follows:

$$\mathcal{L}_0(C) := \{a \in C \mid \exists k : F^k(a) = a\}$$
$$\mathcal{L}_i(C) := \{a \in C \mid F(a) \in \mathcal{L}_{i-1}(C)\}$$

Thus, for a bijective map $F\colon S \to S$ on a finite set, all components C have only one layer, $\mathcal{L}_0(C)$. When it is clear about which component we speak, we may leave out the C, and just write $\mathcal{L}_k$.

We furthermore say that a component C is *of period* n if the elements in $\mathcal{L}_0(C)$ all have period n. Note that all elements in $\mathcal{L}_0(C)$ necessarily have the same period.

4 Invertibility and cycles in the state diagram of χ

In this section we are going to investigate the state diagram of χ on a certain large class of periodic states. Namely, those that have a unique preimage (or, where χ acts bijectively) occur in a cyclic component. As a corollary, we obtain a direct formula for the order of χ_n for odd n.

Daemen showed that χ is invertible on states that have period dividing n when n is odd ([3]). We give a new proof here, because this new proof gives a direct formula for the order of χ_n.

4.1 Dynamic bits

For two bit positions i and j, we set $d = j - i$ to be the *distance* from bit i to bit j. Furthermore the *next* 1*-bit* from a bit position i, is the smallest bit position $j > i$ such that $\sigma_j = 1$. Note that any bit position in a periodic state σ has a next 1-bit, as long as σ has period $n > 1$.

Definition 10 (Dynamic and static bits) A bit is called *dynamic* if the distance to the next 1-bit is even. When the distance to the next 1-bit is odd, we call the bit *static*. A static bit that has the value 1 is called an *anchor*.

To explain the terminology for dynamic and static, we have the following lemma.

Lemma 4 *Static bits are invariant under* χ.

Proof A bit changes under χ if and only if the distance to the next 1-bit is 2. A static bit has odd distance to the next 1-bit, hence remains unchanged. □

Definition 11 (Dynamicity pattern) Given a state σ of period n, then its *dynamicity pattern* is a string $x \in \{0, 1, *\}^n$, where $x_i = \sigma_i$ if σ_i is static, and $x_i = *$ otherwise.

We show that the dynamicity pattern is invariant under applications of χ. For that we use a lemma, simplifying χ on dynamic bits:

Lemma 5 *Let $\sigma \in \widehat{\mathbb{F}_2}$ and σ_i be a dynamic bit. Let $\nu = \chi(\sigma)$, then $\nu_i = \sigma_i + \sigma_{i+2}$.*

Proof Since σ_i is dynamic, $\sigma_{i+1} = 0$. □

Proposition 1 *The dynamicity pattern of a state is invariant under χ.*

Proof Let $\sigma \in \widehat{\mathbb{F}_2}$ be arbitrary non-zero and $\nu = \chi(\sigma)$. Pick some σ_i arbitrary. We make a case distinction on the basis of the distance to the next 1-bit.

1. First, assume that the distance is larger than 2. That means that σ_i is followed by 0^n1 for some $n \geq 2$. Then ν_i is followed by $0^{n-2}10*$, where $*$ is an undetermined value. Since n and $n-2$ have the same parity, the dynamicity of σ_i is the same as ν_i.
2. Assume that the distance to the next 1-bit is equal to 2. That means that σ_i is followed by 01, i.e., σ_i is dynamic. Assume that ν_i is static, thus ν_i is followed by $(00)^n1$ for some $n \geq 0$. By Lemma 5, we have two options for σ_i, it is either followed by $(00)^{n+1}1$, or by $(10)^n1$. In both cases, σ_i would be static, a contradiction.
3. Lastly, assume that the distance to the next 1-bit is 1. Now, σ_i is static. Assume that ν_i is dynamic, hence followed by $0(00)^n1$ for some $n \geq 0$. By Lemma 5, we now have two options for σ_i, it is either followed by $0(00)^{n+1}1$, or by $0(10)^n1$. In both cases, σ_i is not followed by 1, a contradiction. □

Example 2 (Dynamicity pattern) Take for example the state $(001011110001)^*$, then we locate the dynamic bits and replace them by $*$:

$$\sigma = (001011110001)^* \rightsquigarrow *0*0111*0*01$$
$$\nu = (100011110101)^* \rightsquigarrow *0*0111*0*01$$

Here $\nu = \chi(\sigma)$, and we see that the dynamicity pattern remains the same.

Lemma 6 (Distance to anchors - No. 1) *Let $\sigma \in \widehat{\mathbb{F}_2}$ be a periodic state with at least one anchor. Then the distance from a dynamic bit to the next anchor is even.*

Proof Let σ_i be an arbitrary dynamic bit. Then the next 1-bit has even distance from σ_i by definition. If this bit is static, it is an anchor. If it is not an anchor, then the distance to the next 1-bit is even again. Iterate this process until one arrives at an anchor, all the while keeping an even distance. Since we have at least one anchor by hypothesis, this process will stop. □

Lemma 7 (Distance to anchors - No. 2) *Let $\sigma \in \widehat{\mathbb{F}_2}$ be a periodic state with at least one anchor. Then the distance from an anchor to the next anchor is odd.*

Proof Let σ_i be an arbitrary anchor. Then by definition, the next 1-bit has odd distance from σ_i by definition. Then either, this 1-bit is an anchor, in which case we are done. In the other case, this 1-bit is not an anchor, hence it is a dynamic bit and the result follows from applying Lemma 6. □

4.2 Anchor polynomials and the uniqueness of preimages under χ

Since the dynamicity pattern is invariant under application of χ, and anchors are static bits, we can uniquely split up a state at its anchors.

For example, if we take $(11011)^*$, we can split it up like 101-1-1. On the other hand, the state $(11010)^*$ can only be split up as 10101. It is a single substring, as it has precisely one anchor.

For each anchor, we can create a corresponding polynomial:

Definition 12 (Anchor polynomial) Let $\sigma \in \widehat{\mathbb{F}_2}$ be a periodic state with at least one anchor. Let σ_i be an anchor and let $\sigma_{i-(2d_i+1)}$ be the previous anchor. (Lemma 7.) Then $a^{(i)}(X) := \sum_{j=0}^{d_i-1} \sigma_{i-2j} X^j$ is the *anchor polynomial of* σ_i and d_i is the *anchor degree of* σ_i.

Note that a periodic state with at least one anchor can now be completely represented by the positions of its anchors and their corresponding anchor polynomials. Furthermore, using these anchor polynomials, we can describe the operation of χ in an elegant way:

Proposition 2 (χ is multiplication by $X+1$) *Let $\sigma \in \widehat{\mathbb{F}_2}$ be a periodic state with at least one anchor and $\nu = \chi(\sigma)$. Let $a^{(i)}(X)$ be the anchor polynomial with anchor degree d_i of the anchor σ_i. Then $b^{(i)}(X) := (1+X)a^{(i)}(X) \bmod X^{d_i}$ is the anchor polynomial of ν_i.*

Proof We need to show that $b_0^{(i)} = a_0^{(i)}$, as the anchor is static. This is immediate. Furthermore, we need to show that $b_j^{(i)} = \nu_{i-2j}$. For that, by Lemma 5, we have $b_j^{(i)} = a_j^{(i)} + a_{j-1}^{(i)} = \sigma_{i-2j} + \sigma_{i-(2j+2)} = \nu_{i-2j}$. □

The polynomial $1+X$ is invertible in the ring $\mathbb{F}_2[X]/(X^d)$ for any $d \geq 1$. The inverse of $1+X$ in such a ring is $1 + X + X^2 + \ldots + X^{d-1}$.

Theorem 1 (States with an anchor have a unique preimage) *Let $\nu \in \widehat{\mathbb{F}_2}$ be a periodic state with at least one anchor. Then ν has precisely one preimage.*

Proof We need to show that there is a unique way to obtain the anchor polynomials of σ such that $\chi(\sigma) = \nu$. To do this, let $b^{(i)}(X)$ be an anchor polynomial of ν. Then $a^{(i)}(X) = (1 + X + X^2 + \ldots + X^{k-1})b^{(i)}(X) \bmod X^{d_i}$ is the anchor polynomial for σ. The uniqueness follows from uniqueness of inverses in a ring. □

We have reduced the question of finding states with unique preimages to finding states with at least one anchor. A first result is that all non-zero states of odd period have an anchor:

Proposition 3 *Let $\sigma \in \widehat{\mathbb{F}_2}$ be non-zero and have odd period. Then it has at least one anchor.*

Proof The sum of the distances between all 1-bits in σ together sum to the period. Since the period is odd, there has to be at least one of those distances that is odd, hence at least one anchor. □

Secondly, we can concretely define the non-zero states of even period that have an anchor.

We partition $\widehat{\mathbb{F}_2}$ into subsets $\{0\}, (S_{n,0} \setminus \{0\})_{n\in\mathbb{N}^*}, (S_{n,1} \setminus \{0\})_{n\in\mathbb{N}^*}, (T_n)_{n\in\mathbb{N}^*}$ as follows

$$\begin{aligned} S_{n,0} &:= \{\sigma = (\sigma_0, \sigma_1, \ldots, \sigma_{n-1})^* \in \mathfrak{P}_n \mid \sigma_i = 0 \text{ when } i \equiv 0 \pmod 2\}; \\ S_{n,1} &:= \{\sigma = (\sigma_0, \sigma_1, \ldots, \sigma_{n-1})^* \in \mathfrak{P}_n \mid \sigma_i = 0 \text{ when } i \equiv 1 \pmod 2\}; \\ T_n &:= \mathfrak{P}_n \setminus (S_{n,0} \cup S_{n,1}). \end{aligned}$$

In addition, we define $\mathcal{S}_0 := \bigcup_{n=2}^{\infty} S_{n,0}$, $\mathcal{S}_1 := \bigcup_{n=2}^{\infty} S_{n,1}$, and $\mathcal{T} := \bigcup_{n=1}^{\infty} T_n$.

Then we have

Lemma 8 *Let σ be a nonzero state of even period n.*

1. *If $\sigma \in \mathcal{T}$, then σ has an anchor.*
2. *If $\sigma \in \mathcal{S}_0$, then σ has no anchors.*
3. *If $\sigma \in \mathcal{S}_1$, then σ has no anchors.*

Proof 1. Let $\sigma_i = 1$ and $\sigma_j = 1$ be 1-bits, where i is even and j is odd or vice versa and $i < j$. In both cases, the distance $d = d(\sigma_i, \sigma_j) = j - i$ is odd. If $d = 1$, then σ_i is an anchor. So suppose that $d > 1$. If there exists a $\sigma_k = 1$ with $i < k < j$ and $i \equiv k \pmod 2$, then we can instead take σ_k instead of σ_i. If there exists a $\sigma_k = 1$ with $i < k < j$ and $k \equiv j \pmod 2$, then we can instead take σ_k instead of σ_j. Hence all bits between σ_i and σ_j can be assumed to be 0. There is an even number of them, hence σ_i is an anchor.

2. Let $\sigma_i = 1$ be an arbitrary 1-bit in σ. By definition of $S_{n,0}$, it is followed by a repeating pattern of $0*$. Therefore, it cannot be followed by an even number of zeroes, and hence not an anchor.
3. Similar to the case for $\mathcal{S}_0$. □

4.3 Cycle lengths in the state diagram

In this subsection we investigate the lengths of the cyclic components in the state diagram of χ. We will prove

Theorem 2 *Periodic states that have an anchor lie in cycles in the state diagram of χ. These cycles have a length that is a power of two and this length ranges from 1 to the largest power of two not larger than n.*

Recall that χ operates as multiplication of all anchor polynomials $a^{(i)}(X)$ by $1 + X$ modulo X^{d_i}. Since the dynamicity pattern is invariant under χ, the length of the cycle that contains σ is therefore the least common multiple of the order of $1 + X$ in the rings $\mathbb{F}_2[X]/(X^{d_i})$.

Lemma 9 *Let $R := \mathbb{F}_2[X]/(X^d)$. Then $\#R^* = 2^{d-1}$.*

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

By Lagrange's Theorem, we now know that the order of $X+1$ is a power of 2. Since $(X+1)^{2^k} = X^{2^k}+1$, we find that the order of $X+1$ is the smallest power of 2 larger than or equal to d. This is then $2^{\lceil \lg(d) \rceil}$.

We can now prove Theorem 2.

Proof (of Theorem 2.) Let σ be a nonzero state in $\widehat{\mathbb{F}_2}$ with an anchor. Let $2d_i+1$ be the distance from the $(i-1)$th anchor to the ith anchor and consider $\{d_0, \ldots, d_k\}$. By the above, we have

$$\begin{aligned} \#\mathcal{O}_\chi(\sigma) &= \operatorname*{lcm}_{i\in\{1,\ldots,k\}} (2^{\lceil \lg(d_i-1)\rceil}) \\ &= \max_{i\in\{1,\ldots,k\}} (2^{\lceil \lg(d_i-1)\rceil}) \\ &= 2^{\lceil \lg(d_{i_0}-1)\rceil} \end{aligned}$$

where i_0 is chosen such that $d_{i_0} \geq d_i$ for all $i \in \{0, \ldots, k\}$. We now find that indeed a cycle of length any power of two exists. □

5 Preimages for states without anchors

In this subsection, we study states with even period. Therefore, n is assumed to be a positive even integer. We are going to investigate χ on $\mathfrak{P}_n$ to see whether χ is surjective. This is a next step into understanding the full state diagram of χ.

We know from Theorem 1 that a state σ has a unique preimage if there is at least one anchor: $\sigma \in T_n$.

Therefore, the states where zero or multiple preimages may exists are exactly those in $\bigcup_n (S_{n,1} \cup S_{n,0})$ They fall into three categories:

1. The state has two preimages of the same period;
2. The state has two preimages of double period;
3. The state has one preimage of the same period and two preimages of double period.

The third case is only applicable to 0^*, as we shall see.

5.1 Linearization of χ

When n is fixed, we can omit it as an index, to obtain $T := T_n$ and $S_i := S_{n,i}$ for $i \in \{0, 1\}$.

Lemma 10 *For $\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ we have $\chi(S_1) \subset S_1$ and $\chi(S_0) \subset S_0$.*

Proof Let $\sigma \in S_0$ be arbitrary with $\sigma = (\sigma_0, \sigma_1, \ldots, \sigma_{n-1})^*$. Then each even position σ_i is 0. Since these zeroes are followed by $*0$, they cannot be followed by 01. Hence these bits remain 0 under χ. The statement for S_1 is similar. □

Since χ is invertible on T, we are mostly interested in $\chi_{\big|S_0}$ and $\chi_{\big|S_1}$. Both of these are linear maps:

$$\chi_{\big|S_0}: S_0 \to S_0,\ (\sigma_0 0 \sigma_2 0 \cdots \sigma_{n-2} 0)^* \mapsto ((\sigma_0+\sigma_2)0(\sigma_2+\sigma_4)0\cdots 0(\sigma_{n-2}+\sigma_0))^*$$
$$\chi_{\big|S_1}: S_1 \to S_1,\ (0\sigma_1 0 \sigma_3 \cdots 0 \sigma_{n-1})^* \mapsto (0(\sigma_1+\sigma_3)0(\sigma_3+\sigma_5)\cdots(\sigma_{n-1}+\sigma_1)0)^*$$

By projecting S_0 (respectively S_1) on the subspace we find two maps of a similar form:

Definition 13 Let $k \geq 1$. We write $\chi_k^L: \mathbb{F}_2^k \to \mathbb{F}_2^k,\ x \mapsto y$ for the *linearized even period* χ. Here $y_i = x_i + x_{i+2 \bmod k}$. We write $L_k := \operatorname{Im} \chi_k^L$ for its image.

Since χ_k^L is a linear map, we can investigate it using linear algebra. For instance, we can represent it by a $k \times k$ matrix:

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

We can also easily determine its kernel:

Lemma 11 $\operatorname{Ker} \chi_k^L = \{0^k, 1^k\}$.

Proof For $\chi_k^L(x) = 0$ to hold, we must have $x_0 = x_1 = x_2 = \ldots = x_{k-1}$. □

To return from a result about χ_k^L to results about $\chi_{\big|S_0}$, we can use:

$$\pi_0: \mathbb{F}_2^{2k} \to \mathbb{F}_2^k,\ (x_0, x_1, \ldots, x_{2k-1}) \mapsto (x_0, x_2, \ldots, x_{2k-2})$$
$$\pi_1: \mathbb{F}_2^{2k} \to \mathbb{F}_2^k,\ (x_0, x_1, \ldots, x_{2k-1}) \mapsto (x_1, x_3, \ldots, x_{2k-1})$$

that are bijective when restricted to S_1 and S_0 respectively.

Since we know $\operatorname{Ker} \chi_k^L$, we find that $\dim L_k = k - 1$ using the isomorphism theorem.

We have the following proposition to help us in achieving our goal.

Proposition 4 *Let $k \geq 1$. Then L_k is the $k-1$-dimensional subspace of all vectors in $\mathbb{F}_2^k$ of even Hamming weight.*

Proof We know that L_k is spanned by the columns of χ_k^L. Therefore, we know that L_k is spanned by vectors of Hamming weight 2. Since the sum of two vectors of even Hamming weight is again a vector of even Hamming weight, it follows that all elements in L_k are vectors of even Hamming weight. Furthermore, since $\dim L_k = k - 1$ we see that L_k contains half of the vectors of $\mathbb{F}_2^k$, so all vectors of even Hamming weight. □

From Proposition 4 it follows that $\chi(\mathfrak{S}_n) \subsetneq \mathfrak{S}_n$ for even n.

5.2 Finding preimages for states of even period

We in this section explore some theoretical results that yield an efficient method to find all preimages to a give periodic state.

By Proposition 4, the elements not reached by χ_k^L are exactly the elements with odd Hamming weight.

We then immediately obtain:

Theorem 3 *Let $n > 1$ be even. Then $\mathfrak{S}_n \setminus \chi(\mathfrak{S}_n)$ consists of states with odd Hamming weight such that either:*

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

We know that χ is not injective. Furthermore, since χ is bijective on $\bigcup_{n\in\mathbb{N}^*} T_n$, we know that χ is not injective on $(S_0 \cup S_1)_{n\in\mathbb{N}^*}$.

For the linearized χ, we have that if $\chi_k^L(u) = \chi_k^L(v)$ then $u = v$ or $u = v + 1^k$, by Lemma 11. We also know that $\chi(S_0) \subset S_0$ and $\chi(S_1) \subset S_1$ by Lemma 10.

Hence we know, if $\chi(\sigma) = \chi(\rho)$ with $\sigma \neq \rho$, then $\sigma, \rho \in S_0$ or $\sigma, \rho \in S_1$, with the exception of $(01)^*$ and $(10)^*$ that both map to 0^*. We have shown

Lemma 12 *If $\sigma \neq \rho \in \mathbb{F}_2^{\mathbb{Z}}$ have period n and are such that $\chi(\sigma) = \chi(\rho) \neq 0$, then either*

- *$\sigma, \rho \in S_0$ and $\sigma + \rho = (01)^*$; or*
- *$\sigma, \rho \in S_1$ and $\sigma + \rho = (10)^*$.*

From this lemma, we conclude that every nonzero element in $\chi(\widehat{\mathbb{F}_2})$ has at most two preimages.

Corollary 1 *Let k be an odd integer and let $\nu \in \mathbb{F}_2^{\mathbb{Z}}$ have period $2k$. Assume that ν has two preimages σ, ρ under χ. Then* $\mathrm{hw}(\sigma) \neq \mathrm{hw}(\rho) \pmod 2$.

Proof If $\mathrm{hw}(\sigma)$ is odd, then $\rho = \sigma + (01)^*$ is the sum of two states of odd Hamming weight. Therefore $\mathrm{hw}(\rho)$ is even. If $\mathrm{hw}(\sigma)$ is even, then $\rho = \sigma + (01)^*$ is the sum a state of odd and a state of even Hamming weight. Therefore $\mathrm{hw}(\rho)$ is odd. □

To explicitly find the preimages of a state $\sigma \in \chi(\widehat{\mathbb{F}_2})$, we use a method based on Daemen's seed-and-leap method [3].

Lemma 13 *Let $\chi(\sigma) = \nu$. Then we have*

1. *If $\nu_i = 1$, then $\sigma_{i-1} = \nu_{i-1}$;*
2. *$\sigma_{i-2} = \nu_{i-2} + (\nu_{i-1} + 1)\sigma_i$,*

where, in both cases, indices are modulo $\mathrm{per}(\sigma)$.

Whenever an element in this preimage has all bits with odd (or all even) indices zero, one finds both preimages.

To do this, basically loop twice: once over the odd indices and once over the even indices. It makes a choice whenever there are no ones on an even (or odd) position and continues the cycle from that choice.

Example 3 Consider that we want to determine the preimages of $(100010)^*$. We start by filling in blanks and look for a 1. We apply Lemma 13.1 to obtain $(?????0)^*$. By applying Lemma 13.2 repeatedly we obtain $(?0?0?0)^*$. Next we have to make a choice, because there are no ones in the even positions. We get $(00?0?0)^*$ and $(10?0?0)^*$. By applying Lemma 13.2 repeatedly to both, we get $(001010)^*, (100000)^* \mapsto (100010)^*$. (See also Figure 2.)

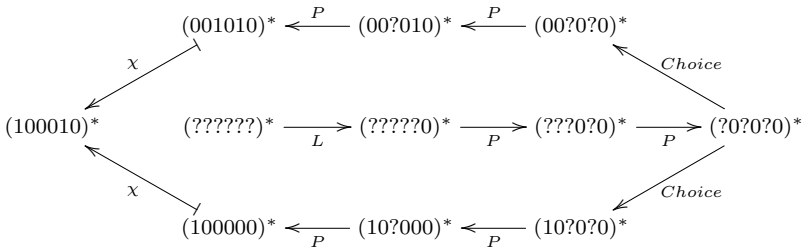


Fig. 2 Finding the preimages for $(100010)^*$ under χ.

Remark that by Lemma 12, it does not matter which choice is made, as the second preimage can be determined from the first.

Lemma 14 *Let ν be a state of period n that has no preimages of period n. Let σ, ρ be the preimages of period $2n$ of ν. Then $\rho = \tau^{-n}(\sigma)$.*

Proof Since χ_{2n} is shift invariant and ν has period dividing n, we have

$$\begin{aligned}\chi(\tau^{-n}(\sigma)) &= \tau^{-n}(\chi(\sigma)) \\ &= \chi(\sigma)\end{aligned}$$

The result then follows from Lemma 12. □

We can now divide the preimage $\sigma = (x)^*$ into two parts $\sigma = (x_0|x_1)^*$ and we have $\rho = (x_1|x_0)^*$.

Corollary 2 *Let ν be a state of period n that has no preimages of period n. Let $(x_0|x_1)^*$ and $(x_1|x_0)^*$ be the preimages of ν under χ. Then $x_0 = x_1 + (01)^{n/2}$ when $z \in S_0$ or $x_0 = x_1 + (10)^{n/2}$ when $z \in S_1$.*

Only one preimage needs to be determined by Lemma 14 and by Corollary 2 only half of the state needs to be constructed.

Remark that when using the method on length n, a preimage of double length can be found by just writing the wrong preimage of length n as a_0 and applying Corollary 2. To make this more clear, we present an example.

Example 4 Let us try to find the preimages of the state $\sigma = (\texttt{010000})^*$. Since the Hamming weight is odd, we expect double-length preimages. By Lemma 10, we know that the preimage should look like $(\texttt{0?0?0?})^*$. We now set the last position to be 0: $(\texttt{0?0?00})^*$ and apply Lemma 13.2 two times again. We then obtain $(\texttt{010000})^*$. By Corollary 2 we now can conclude that the preimages of σ under χ are $(\texttt{010000000101})^*$ and $(\texttt{000101010000})^*$.

5.3 Surjectivity of χ

Here, we prove that χ is surjective on $\widehat{\mathbb{F}_2}$, while we know that $\chi(\mathfrak{S}_n) \subsetneq \mathfrak{S}_n$.

Theorem 4 *(χ is surjective on periodic states) The map $\chi\colon \widehat{\mathbb{F}_2} \to \widehat{\mathbb{F}_2}$ is surjective.*

Proof Let $\nu \in \widehat{\mathbb{F}_2}$ be arbitrary. Let $n = \mathrm{per}(\nu)$. By Theorem 3, either $\nu \in \chi(\mathfrak{S}_n)$ or $\nu \notin \chi(\mathfrak{S}_n)$. In the latter case, note that ν has odd Hamming weight and zeroes on all even (or odd) positions. If we view $\nu = (\nu_0, \ldots, \nu_{n-1}, \nu_0, \ldots, \nu_{n-1})^*$, then its Hamming weight is even. Thus $\nu \in \chi(\mathfrak{S}_{2n})$. Hence in both cases, ν is in the image of χ. □

Corollary 3 *Let $\sigma \in \widehat{\mathbb{F}_2}$, then* $\mathrm{per}(\chi(\sigma)) = \mathrm{per}(\sigma)$ *or* $2\,\mathrm{per}(\chi(\sigma)) = \mathrm{per}(\sigma)$.

Proof From Corollary 1, we know that a non-zero state has at most two preimages. From Theorem 4, the result then follows. □

In particular, a state of period 30, say, cannot be mapped onto a state of period 3 or 5, no matter how often χ is (re-)applied.

Furthermore, we know that for an arbitrary state of period $n = 2^k \cdot m$ in $S_{n,0}$, after enough iterations of χ, will end up in a cycle. This is due to Corollary 3, where the period will decrease until it is $2m$, with $m > 0$ odd:

Lemma 15 *Let $m > 1$ be an odd integer and let σ be a state of period $2m$. Then $\chi(\sigma)$ is also a state of period $2m$.*

Proof We know that $\chi(\sigma)$ has period dividing $2m$, since χ is shift invariant (Lemma 2). By Corollary 3, what remains to show is that $\chi(\sigma)$ does not have period m. Suppose that $\chi(\sigma)$ has period m. We know, by Theorem 1, that since m is odd, χ operates bijectively on $\mathfrak{S}_m$. That means that $\chi(\sigma)$ has a unique preimage that has period m, a contradiction. □

6 Full characterization of the state diagram of χ

Before we have dealt will all cyclic components of the state diagram of χ. In this section, we will deal with the other components, that all have the shape of a cycle with (binary) trees on those cycles. The arrows point inwards to the cycle.

We start with choosing a suitable linearization in Section 6.1, then follow that with a treatment of the states of period 2^k in Section 6.2. In Section 6.3 we will take on the components with states of period $2^k \cdot m$ with $m > 1$.

6.1 Polynomial linearization of χ on states of even period

Since χ operates cyclically on states in T_n, we only need to understand how χ operates on states in $S_{n,0}$ (as $S_{n,1}$ is just $S_{n,0}$ shifted and χ is shift invariant).

In Figure 3 we depict what χ_3^L looks like on $S_{6,0}$. (Note that we leave out the part that has period 1 or 2.)

Before we give an explicit description of these, we consider a new representation of the vector space $\mathbb{F}_2^n$ as a quotient of a polynomial ring.

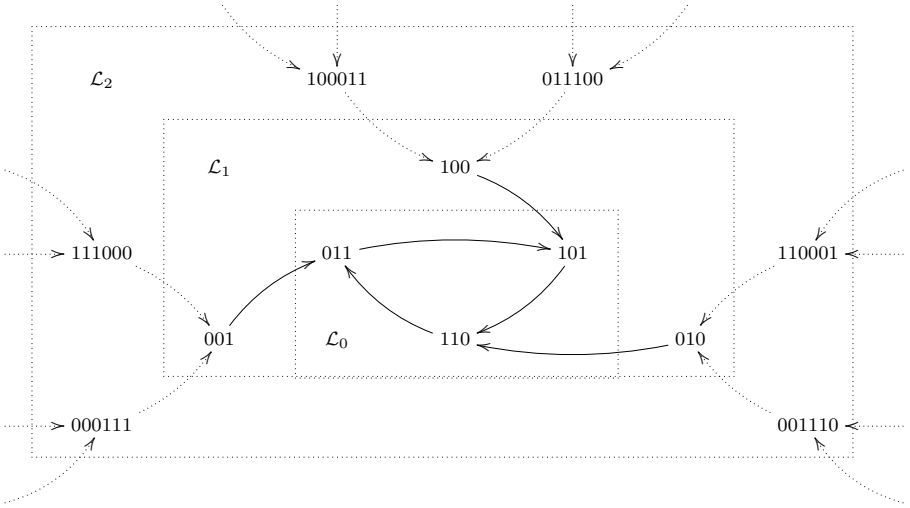


Fig. 3 Layers $\mathcal{L}_0, \mathcal{L}_1, \mathcal{L}_2$ of a component of the diagram for χ_3^L on $S_{6,0}$. Dotted lines indicate preimages of double period.

We consider the vector space isomorphism $\varphi\colon \mathbb{F}_2^n \to \mathbb{F}_2[X]/(X^n+1)$ defined by

$$(a_0, \ldots, a_{n-1}) \mapsto \sum_{i=0}^{n-1} a_i X^{n-(i+1)}.$$

Under this isomorphism, a left shift τ_n corresponds to a multiplication by X modulo X^n+1. Similarly, since $\chi_k^L = \mathrm{Id} + \tau_n$, we find that the corresponding $\chi_k^L\colon \mathbb{F}_2[X]/(X^n+1) \to \mathbb{F}_2[X]/(X^n+1)$ is just a multiplication by $1+X$ modulo X^n+1

Definition 14 (Polynomial representation of states) Let $n > 0$ be an even integer. Let $\sigma \in S_{n,0}$ and write $\sigma' \in \mathbb{F}_2^n$ under the isomorphism from Lemma 1. Then we write $f_\sigma(X) := \varphi(\pi_1(\sigma'))$.

Remark 1 In particular, if $\sigma = (x)^*$ is given, we then remove the zeroes in odd positions of x by appling φ, to obtain a state of length $\frac{n}{2}$. That, we then make into a univariate polynomial.

From Theorem 3, we can conclude the following corollary:

Corollary 4 *Let $n > 0$ be an even integer and $\sigma \in S_{n,0}$. Then σ has two preimages of the same period if and only if $X+1 \mid f_\sigma(X)$.*

Proof

σ has two preimages of the same period iff $\mathrm{hw}(\sigma') \equiv 0 \pmod 2$
iff $f_\sigma(X)$ has an even number of terms
iff $f_\sigma(1) = 0$
iff $X + 1 \mid f_\sigma(X)$.

□

For a given state that has period dividing n, we can now express that the state has period dividing $\frac{n}{2}$ as well:

Proposition 5 *Let $n = 2^k \cdot m$ for positive integers $k > 1$ and m odd. Let $\sigma \in S_{n,0}$ and let $f_\sigma(X)$ be the polynomial representation of σ. Then σ has period dividing $\frac{n}{2}$ if and only if $X^{\frac{n}{4}} + 1 \mid f_\sigma(X)$.*

Proof $\Leftarrow$:) Since $X^{\frac{n}{4}} + 1 \mid f_\sigma(X)$, we can determine a polynomial $c(X)$ such that $f_\sigma(X) = c(X) \cdot X^{\frac{n}{4}} + 1$. Then the coefficients of the righthandside correspond to a vector of the form

$$(c_0 + c_{\frac{n}{4}}, c_1 + c_{1+\frac{n}{4}}, \ldots, c_{\frac{n}{4}-1} + c_{\frac{n}{2}-1}, c_{\frac{n}{4}} + c_0, \ldots, c_{\frac{n}{2}-1} + c_{\frac{n}{4}-1})$$

which is a state of period dividing $\frac{n}{2}$.

$\Rightarrow$:) Consider that the state σ can be written as $\sigma' = (\sigma_0, \sigma_1, \ldots, \sigma_{n-1})$. Then since σ has period dividing $\frac{n}{2}$, we know that $\sigma_{\frac{n}{4}+i} = \sigma_i$ for $i \in \{0, \ldots, \frac{n}{4} - 1\}$. We can write $\sigma_i = c_i + c_{i+\frac{n}{4}}$ and solve the gained system for the c_i. This will give two possible solutions that are each other's complement. Then $f_\sigma(X) = c(X) \cdot (X^{\frac{n}{4}} + 1)$ for any of the $c(X)$. □

Example 5 Let $\sigma \in S_{12,0}$. Consider $\sigma = (0,1,0,0,0,1,0,1,0,0,0,1)^* \in \mathfrak{P}_{12}$. Then removing the even zeroes, we get $\sigma' = (1,0,1,1,0,1)$ and therefore the polynomial $f_\sigma(X) = X^5 + X^3 + X^2 + 1$. We want to show that $X^3 + 1 \mid f_\sigma(X)$, as it is obvious that $\sigma \in \mathfrak{P}_6$.

We know that we can write $\sigma' = (c_0 + c_3, c_1 + c_4, c_2 + c_5, c_0 + c_3, c_1 + c_4, c_2 + c_5)$. Upon choosing c_0, the system gives the following solutions:

$$\mathbf{c} = (1,1,1,0,1,0) \text{ and } \mathbf{d} = (0,0,0,1,0,1).$$

They correspond to $X^5 + X^4 + X^3 + X$ and $X^2 + 1$. Both $f_{\mathbf{c}}(X) \cdot (X^3 + 1) = f_\sigma(X)$ and $f_{\mathbf{d}}(X) \cdot (X^3 + 1) = f_\sigma(X)$ modulo $X^6 + 1$.

6.2 States of period 2^k

Another component of the state diagram looks like a binary tree on a 1-cycle, that we will find in the states that have period a power of 2. Therefore, assume in this section that σ is a state of period $n = 2^k$ for some $k \geq 0$. We split up $\mathfrak{S}_n$ into $T_n, S_{n,0}$ and $S_{n,1}$, where we recall that we already discussed the components of states in T_n. For the states in $S_{n,0}$ and $S_{n,1}$, we have seen that χ behaves like a (linear) multiplication of $f_\sigma(X)$ by $X + 1$. In Corollary 4, we found that a state

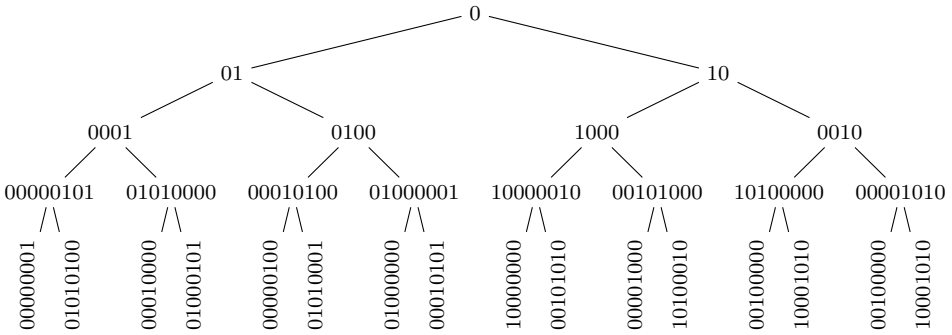


Fig. 4 The component for $S_{2^k,0}$ and $S_{2^k,1}$ for $k \geq 3$. At 0^*, there is a cycle. The notation with parentheses and asterisks has been ommitted to make the figure fit better.

in $S_{n,0}$ or $S_{n,1}$ has two preimages of the same period, exactly when $X+1$ is a divisor of $f_\sigma(X)$. The states in $S_{2^3,0}$ and $S_{2^3,1}$ are depicted in Figure 4.

One can see from the polynomial representation $f_\sigma(X)$ in what layer σ is in this tree. Therefore, one also knows how often χ has to be applied to σ for $\chi^k(\sigma) = 0^*$. To do this, we define the following:

Definition 15 (Rooted sets) Let $d \geq 0$ be an integer and define the set of polynomials of degree less than d as $\mathcal{P}_d := \{f \in \mathbb{F}_2[X] \mid \deg f < d\}$. Let $i \geq 1$. We define the *i-th rooted subset in* 0 as $\mathcal{N}_d^{(i)}$ for the subset of $\mathcal{P}_d$ that consists of those polynomials that have at least i roots at $0 \in \mathbb{F}_2$.

Example 6 For $d = 3$, we have eight polynomials

$$\mathcal{P}_3 = \{0, 1, X, X+1, X^2, X^2+1, X^2+X, X^2+X+1\}.$$

Only the polynomials $0, X, X^2, X^2+X$ have a root at 0, hence we find that $\mathcal{N}_3^{(1)} = \{0, X, X^2, X^2+X\}$. Of those, only 0 and X^2 have a double root at 0, hence we have $\mathcal{N}_3^{(2)} = \{0, X^2\}$. For all $i \geq 3$ we have $\mathcal{N}_{2,3}^{(i)} = \{0\}$.

In fact $\mathcal{P}_d$ is a set of representatives of the elements of $\mathbb{F}_2[X]/(X^d)$. We have $\#\mathcal{P}_d = 2^d$, hence an immediate upper bound for $\mathcal{N}_d^{(i)}$ is found as 2^d. We compute the cardinalities of $\mathcal{N}_d^{(i)}$.

Proposition 6 (Cardinalities of rooted sets) *We have*

$$\#\mathcal{N}_d^{(i)} = \begin{cases} 2^{d-i} & \text{if } d \geq i-1; \\ 1 & \text{else.} \end{cases}$$

Proof Let $i \geq 1$ and $d \geq 0$ be arbitrary. For any i, the zero polynomial has i roots in 0. When $d < i-1$, then it is impossible to have i roots, because of the degree of the polynomial being $< d$. So assume $d \geq i-1$. In order for $f(X)$ to have a root at 0 with multiplicity i, we need to have $X^i \mid f(X)$. This implies that the coefficients for $X^{i-1}, \ldots, X, 1$ must be equal to 0. The remaining $d-i$ coefficients can be arbitrary elements from $\mathbb{F}_2$. □

Lemma 16 (Point invariance of rooted set cardinalities) *Consider the rooted set $\mathcal{N}_d^{(i)}$ and the set of all polynomials that have i roots at 1 (denoted as ${}^1\mathcal{N}_d^{(i)}$). They have equal cardinality for any i, d.*

Proof The automorphism $\varphi\colon \mathbb{F}_2[X] \to \mathbb{F}_2[X],\ f(X) \mapsto f(X+1)$ maps $\mathcal{N}_d^{(i)}$ bijectively to ${}^1\mathcal{N}_d^{(i)}$ for all i, d. Hence $\#{}^1\mathcal{N}_d^{(i)} = \#\mathcal{N}_d^{(i)}$ and the result follows. □

Remark 2 Definition 15 up to (and including) Lemma 16 can be generalized for $\mathbb{F}_p$ instead of $\mathbb{F}_2$.

We saw in Corollary 4 that the states σ whose corresponding polynomial $f_\sigma(X)$ has no root at 1 have two preimages of double period.

We see that there are four rows in the tree that contain states of period 16, two rows that contain states of period 8, and one row (each) of states of period 4, 2 and 1. This observation is formalized in the following corollary, where we define $\mathbb{S}_n = \bigcup_{k=1}^{n} S_{2^k,0} \cup S_{2^k,1}$ and $\mathbb{S} := \bigcup_{n=1}^{\infty} \mathbb{S}_n$.

Corollary 5 *We have $\#\mathcal{L}_k = 2^k$ for $k \geq 0$. The states in $\mathbb{S}_n$ occupy the first $\frac{n}{2}+1$ layers of the component. This coincides with the $\sum_{i=0}^{\frac{n}{2}} 2^i = 2^{\frac{n}{2}} - 1$ states in $\mathbb{S}_n$.*

For a state σ in $\mathbb{S}_n$ it is now possible in what layer it lies, by computing $\gcd(f_\sigma(X), X^{\frac{n}{2}} + 1)$ with the Euclidean algorithm.

Proposition 7 *Let $k > 1$ and let $q = 2^k$. Let $\sigma \in S_{q,0}$ and $f_\sigma(X)$ its polynomial representation. Let $\gcd(f_\sigma(X), X^{\frac{q}{2}} + 1) = (X+1)^d$. Then $\sigma \in \mathcal{L}_{\frac{q}{2}+\frac{q}{4}+1-d}$.*

Proof Proposition 5 gives a criterion to see whether $\chi(\sigma)$ has a shorter period than σ. Let $\sigma \in S_{q,0}$ with $\gcd(f_\sigma(X), X^{\frac{q}{2}} + 1) = (X+1)^d$. Set $s := \frac{q}{2} - d$. Then $\chi^s(\sigma) \in S_{\frac{q}{2},0}$. Therefore $\chi^{s-1}(\sigma) \in \mathcal{L}_{\frac{q}{4}+1}$ and $\sigma \in \mathcal{L}_{\frac{q}{4}+\frac{q}{2}+1-d}$. □

6.3 Snowflakes in the state diagram of χ

All the remaining components of the state diagram of χ look like snowflakes. A *snowflake* in this sense is a short cycle where on each state in the cycle grows a (binary) tree of preimages.

Here, let n be an even integer of the form $2^k m$, where $m > 1$ is odd. We investigate the state diagram of χ over $S_{n,0}$. For the states in $S_{n,0}$ (or $S_{n,1}$), we find that their components have a shape as in Figures 3 and 5.

By the previous discussion, from the cycle there is first one preimage fanning out (the other one is in the cycle itself), and after that always two preimages.

In this subsection, for a component C, we give formulas for the lengths of the cycle ($\#\mathcal{L}_0$), as well for a state σ, for which $k \geq 0$ we have $\sigma \in \mathcal{L}_k$.

Remark 3 The diagram for $S_{n,0}$ is equivalent to $S_{n,1}$ since $\tau(S_{n,0}) = S_{n,1}$. If we have states σ and $\tau(\sigma)$, then the component that contains $\tau(\sigma)$ has the same shape and size as the component of σ.

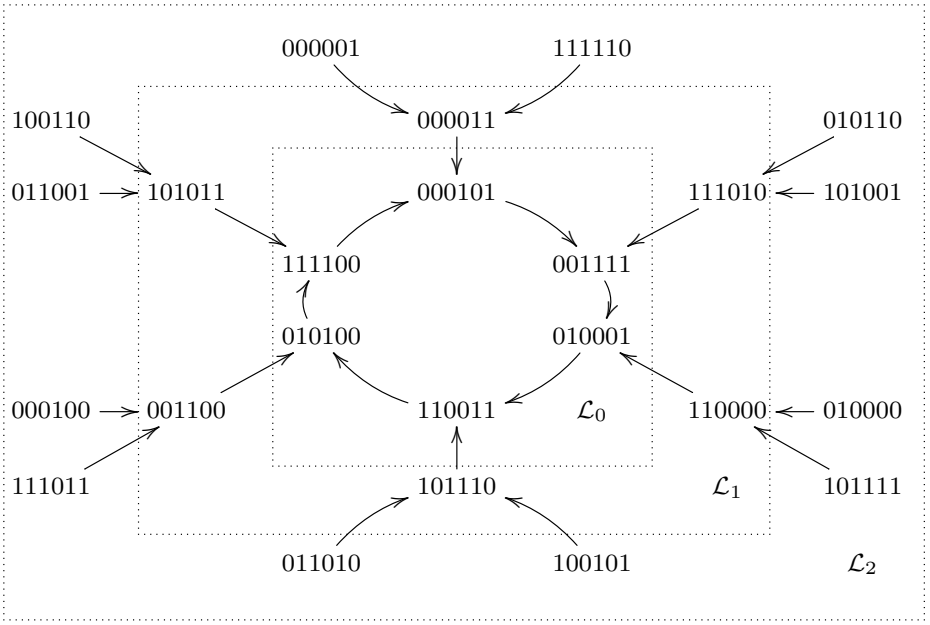
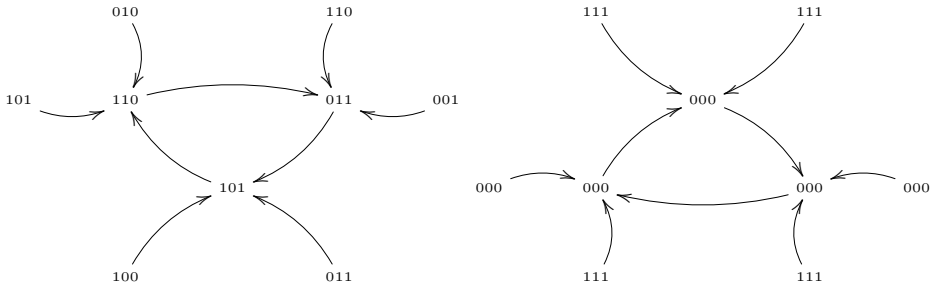


Fig. 5 Layers in a snowflake component in the state diagram for χ. The states without any incoming arrow have preimages of double period. The states given have period 12.

6.3.1 The size of $\mathcal{L}_0$ in snowflake components

In this section we will reuse the polynomial representation $f_\sigma(X)$ for a state σ as in Section 6. Let σ be an anchorless state of period n. Under this representation, we find that an application of χ to σ corresponds to multiplying $f_\sigma(X)$ by $X+1$ modulo $X^{\frac{n}{2}}+1$. We can apply χ multiple times at once, by looking at substrings of σ.

Example 7 Consider Figure 5 and take for each of the 6-tuples the even or odd bits. Furthermore, take the composition of two arrows every time. This coincides with χ^2. It yields three times the left diagram and once the right diagram:



The latter diagram can be simplified to $111 \longrightarrow 000 \circlearrowright$. The former diagram will be simplified to the diagram of χ_3^L on $S_{6,0}$ in Figure 3. We thus see, that for

$n = 12$, we have a component of the diagram of period 2, and a component of period 6, if we apply χ twice.

To go back from the smaller diagrams to the big one, we define an intertwining map $\mathcal{I}$. The intertwining map combines several polynomials into one bigger polynomial in the following way.

Definition 16 (Intertwining map) Let p be a positive integer. The *intertwining map* $\mathcal{I}\colon (\mathbb{F}_2[X]/(X^p+1))^2 \to \mathbb{F}_2[X]/(X^{2p}+1)$ is defined by

$$\mathcal{I}(f_0(X), f_1(X)) = f_0(X)^2 + Xf_1(X)^2.$$

Proposition 8 (Intertwining is bijective) *The map $\mathcal{I}$ is bijective.*

Proof Writing $f_0(X)^2 + Xf_1(X)^2 = \sum a_i X^i$, the coefficients a_i with odd index specify the coefficients of $f_1(X)$ and the coefficients a_i with even index specify the coefficients of $f_2(X)$. Therefore, $\mathcal{I}$ is bijective. □

Since intertwining is bijective, we will give the name *detwining* to the inverse operation. This detwining operation behaves exactly like in Example 7.

Proposition 9 *Let p be an integer and σ be a state of period n with $\frac{n}{2} = 2 \cdot p$ in $S_{n,0}$. Write $\sigma = (\sigma_0, \sigma_1, \ldots, \sigma_{n-1})$. Let $\tau = \pi_0(\sigma) = (\tau_0, \tau_1, \ldots, \tau_{\frac{n}{2}-1})$. For $j = 0, 1$ let $\tau^{(j)} = (\tau_i)_{i \equiv j \pmod 2}$. Then the following are equivalent:*

1. *multiplication of $f_\tau(X)$ by (X^2+1) modulo $X^{\frac{n}{2}}+1$;*
2. *multiplication of $f_{\tau^{(0)}}(X)$ and $f_{\tau^{(1)}}(X)$ by $X+1$ modulo X^m+1 simultaneously.*

Proof 1. If we multiply $f_\sigma(X)$ by X^2+1, then we get

$$\sum_{i=0}^{\frac{n}{2}-1} \tau_i X^i \cdot (X^2+1) \equiv \sum_{i=0}^{\frac{n}{2}-1} (\tau_i + \tau_{i-2}) X^i \pmod{X^{\frac{n}{2}}+1}.$$

2. On the other hand, we have, for both $j = 0, 1$:

$$\sum_{i=0}^{p-1} \tau_i^{(j)} X^i (X+1) \equiv \sum_{i=0}^{p-1} (\tau_i^{(j)} + \tau_{i-1}^{(j)}) X^i \pmod{X^p+1}.$$

This last expression, for $j = 0$, is equal to $\sum_{i=0}^{p-1} (\tau_{2i} + \tau 2i - 2) X^i$, and for $j = 1$, $\sum_{i=0}^{p-1} (\tau_{2i+1} + \tau 2i - 1) X^i$. Then we see by intertwining these expressions that we get the same result as in 1. □

To illustrate this proposition, we have the following example.

Example 8 Let $n = 12 = 2^2 \cdot 3$. Then $\frac{n}{2} = 2^1 \cdot 3$. Consider a state σ of the form

$$\sigma = (\sigma_0, 0, \sigma_2, 0, \sigma_4, 0, \sigma_6, 0, \sigma_8, 0, \sigma_{10}, 0).$$

We then have $\tau = (\sigma_0, \sigma_2, \sigma_4, \sigma_6, \sigma_8, \sigma_{10})$, and respectively $\tau^{(0)} = (\sigma_0, \sigma_4, \sigma_8)$, and $\tau^{(1)} = (\sigma_2, \sigma_6, \sigma_{10})$. Multiplying $f_\tau(X)$ by X^2+1 modulo X^6+1 will yield

$$\begin{aligned}(X^2+1) \cdot f_\tau(X) &= (X^2+1)(\sigma_0 X^5 + \sigma_2 X^4 + \sigma_4 X^3 + \sigma_6 X^2 + \sigma_8 X + \sigma_{10}) \\ &\equiv (\sigma_4 + \sigma_0) X^5 + (\sigma_6 + \sigma_2) X^4 + (\sigma_8 + \sigma_4) X^3 + (\sigma_{10} + \sigma_6) X^2 \\ &\quad + (\sigma_0 + \sigma_8) X + (\sigma_2 + \sigma_{10}) \pmod{X^6+1}\end{aligned}$$

The other part will go like this:

$$\begin{aligned}(X+1)\cdot f_{\tau^{(0)}} &= (X+1)(\sigma_0 X^2+\sigma_4 X+\sigma_8)\\ &\equiv (\sigma_4+\sigma_0)X^2+(\sigma_4+\sigma_8)X+(\sigma_0+\sigma_8) \pmod{X^3+1}\end{aligned}$$

and

$$\begin{aligned}(X+1)\cdot f_{\tau^{(1)}} &= (X+1)(\sigma_2 X^2+\sigma_6 X+\sigma_{10})\\ &\equiv (\sigma_6+\sigma_2)X^2+(\sigma_{10}+\sigma_6)X+(\sigma_2+\sigma_{10}) \pmod{X^3+1}\end{aligned}$$

and then we intertwine them again into

$$\begin{aligned}\mathcal{I}((X+1)\cdot f_{\tau^{(1)}},(X+1)\cdot f_{\tau(0)}) = (\sigma_4+\sigma_0)X^5+(\sigma_6+\sigma_2)X^4+(\sigma_4+\sigma_8)X^3\\ +(\sigma_{10}+\sigma_6)X^2+(\sigma_0+\sigma_8)X+(\sigma_2+\sigma_{10}).\end{aligned}$$

We see that the result from the above proposition holds.

We can use Proposition 9 to understand the cycle lengths in snowflakes.

Corollary 6 *The length of the cycle in snowflakes of period n with $\frac{n}{2}=2^k\cdot m$ with $k,m>1$ odd, is 2 times the length of the cycle in the snowflakes of period n with $\frac{n}{2}=2^{k-1}\cdot m$.*

Proof Suppose that $\sigma=(\sigma_0,\sigma_1,\ldots,\sigma_{n-1})^*$ appears in a cycle. Write $\tau=\pi_0(\sigma)=(\tau_0,\tau_1,\ldots,\tau_{\frac{n}{2}-1})$. Then set $\ell=2\cdot p$, where p is the cycle length in the component of period n with $\frac{n}{2}=2^{k-1}\cdot m$. Then $(X+1)^\ell=(X+1)^{2p}=(X^2+1)^p$. By Proposition 9, we then find

$$f_\sigma(X)=\mathcal{I}((f_{\tau^{(0)}},f_{\tau^{(1)}})=\mathcal{I}\left((X+1)^p f_{\tau^{(0)}},(X+1)^p f_{\tau^{(1)}}\right)=(X+1)^{2p}f_\sigma(X).$$

Thus the cycle length of the cycle that contains σ divides $2p$. Furthermore, since we replace each two arrows by one arrow, when we detwine, we will obtain cycles of length p again. This detwining thus halves the cycle length. Therefore, the cycle length of the cycle containing σ is equal to $2p$. □

Now, we show a bound for the cycle length for $n=2m$ with m odd.

Proposition 10 *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 $o=\mathrm{ord}_{\mathbb{Z}/m\mathbb{Z}}(2)$.*

Proof Let $\sigma=(\sigma_0,\sigma_1,\ldots,\sigma_n)^*\in S_0$ be in a cycle. By removing all the odd/even zeroes, we have $\tau=\pi_0(\sigma)=(\tau_0,\ldots,\tau_{m-1})$. Since application of χ is equal to multiplication by $X+1$ modulo X^m+1, we find that

$$\chi^k(\sigma)=\pi_0^{-1}(\psi^{-1}(((X+1)^k\cdot f_\sigma(X))).$$

Thus when $\chi^k(\sigma)=\sigma$ for some k, we have $(X+1)^k f_\sigma(X)\equiv f_\sigma(X) \pmod{X}^m+1$. We may assume that $f_\sigma(X)$ is invertible, since χ is shift invariant. So we find $(X+1)^k\equiv 1 \pmod{X^m+1}$. When $k=2^o-1$, we find:

$$\begin{aligned}(X+1)^k\equiv 1 \pmod{X^m+1} &\iff (X+1)^{2^{\mathrm{ord}_{\mathbb{Z}/m\mathbb{Z}}(2)}}\equiv X+1 \pmod{X^m+1}\\ &\iff X^{2^{\mathrm{ord}_{\mathbb{Z}/m\mathbb{Z}}(2)}}\equiv X \pmod{X^m+1}\\ &\iff 2^{\mathrm{ord}_{\mathbb{Z}/m\mathbb{Z}}(2)}\equiv 1 \pmod{m}.\end{aligned}$$

Thus we may conclude that the length of the cycle is a divisor of 2^o-1. □

There are many values for m where this length is exactly $2^o - 1$, but also many values of m where it is a proper divisor of $2^o - 1$. In Tables 2 and 3 in Appendix 9.1 we list several of these values.

We now give the number of states in the cyclic parts:

Proposition 11 *Let $n = 2m$ with m odd. Then from the states in $S_{n,0}$ that have period n, exactly half lie in $\mathcal{L}_0(C)$ for each component C.*

Proof We know that the states σ such that $X + 1 \mid f_\sigma(X)$ have two preimages. One of those preimages ρ is such that $X + 1 \mid f_\rho(X)$, while the other, ρ' has $X+1 \nmid f_{\rho'}(X)$. (See Corollary 1.) If we restrict χ to $\{\sigma \in C : X+1 \mid f_\sigma(X)\}$, then this restriction is bijective, as every element has a unique preimage. Therefore these elements lie on disjoint cycles, hence in $\mathcal{L}_0(C)$. Thus at least half of the states in $S_{n,0}$ lie in $\mathcal{L}_0(C)$. If $X + 1 \nmid f_\sigma(X)$, then σ has no preimage of the same period (see Corollary 4). Therefore, $\sigma \notin \mathcal{L}_0(C)$. Hence at most half of the states in $S_{n,0}$ lie in $\mathcal{L}_0(C)$. □

We can use Proposition 9 to figure out the same for larger periods.

Corollary 7 *Let $n = 2^k m$ with m odd. Then from the states in $S_{n,0}$ that have period n, exactly one in every 2^{2^k-1} lies in a cycle.*

Proof For $k = 1$, we have Proposition 11. Using Proposition 9, we find that if we replace in $S_{2m,0}$ every application of χ by 2^{k-1} applications of χ, we get the snowflake in $S_{n,0}$. This means that only the inner part is in a cycle, but there are 2^{k-1} layers of states outside the cycle. Furthermore, since all but the last layer has states with two preimages inside $S_{n,0}$, these layers get twice as big each layer. The outer layer has half of $S_{n,0}$ in it. Then each new layer decreases the number by another half. There are 2^{k-1} layers. □

We can also express when a state appears in a cycle in a diagram like in Figure 3.

Proposition 12 *Let $n = 2^k \cdot m$ where m is an odd integer and $k \geq 0$. Let σ be a state of period n in $S_{n,0}$, and $f_\sigma(X)$ its polynomial representation. If we have $X^{2^{k-1}} + 1 \mid f_\sigma(X)$, then σ appears in a cycle.*

Proof For $k = 1$, this follows from Proposition 11. When $k > 1$, we find from Corollary 7, that one in every 2^{2^k-1} lies in a cycle. By counting, the higher power of $X+1$, the polynomial $f_\sigma(X)$ is divisible by, the closer it is to a cycle. By Proposition 6, we then find that the one in every 2^{2^k-1} occurs exactly at $X^{2^{k-1}}+1 \mid f_\sigma(X)$. □

Lastly, we show that components are isomorphic (as graphs).

Proposition 13 *Let n be an arbitrary even integer and let C_0, C_1 be components of the state diagram of χ restricted to $S_{n,0} \cup S_{n,1}$. Then $\#\mathcal{L}_0(C_0) = \#\mathcal{L}_0(C_1)$.*

Proof Since $S_{n,0} = \tau(S_{n,1})$, we know that the components in $S_{n,0}$ also appear once in $S_{n,1}$. Therefore, we may assume C_0 and C_1 be components in the state diagram of χ restricted to $S_{n,0}$. Let $\sigma \in \mathcal{L}_0(C_0)$ and $\tau \in \mathcal{L}_0(C_1)$ be arbitrary. Write $f_\sigma(X)$ and $f_\tau(X)$ as the univariate polynomial representation for σ and τ. Applying χ

to σ is just multiplying $f_\sigma(X)$ by $X+1$ modulo X^n+1. We know that $f_\sigma(X)$ is divisible by $X+1$. Therefore, we can also regard $f'_\sigma(X)$ as $f_\sigma(X)/(X+1)$. Then applying χ is multiplying $f'_\sigma(X)$ by $X+1$ modulo $X^{n-1}+X^{n-2}+\ldots+X+1$. Now in this ring $\mathbb{F}_2[X]/(X^{n-1}+X^{n-2}+\ldots+X+1)$, we have that $X+1$ is invertible. Furthermore, $f'_\sigma(X)$ and $f'_\tau(X)$ differ by unit factor. I.e., there exists some $u(X) \in \mathbb{F}_2[X]/(X^{n-1}+X^{n-2}+\ldots+X+1)$ such that $f'_\sigma(X) = u(X)f'_\tau(X)$. Multiplication with a unit $u(X)$ is an automorphism. Hence the behaviour of $f'_\sigma(X)$ under (repeated) multiplication by $X+1$ is the same as the behaviour of $f'_\tau(X)$ under (repeated) multiplication by $X+1$. Hence the behaviours of σ and τ under repeated application of χ are the same. □

6.3.2 Towards the cycle

Next, it is interesting to know for a state that is not on a cycle in which layer it is.

Proposition 14 *Let $\sigma = (\sigma_0, \ldots, \sigma_{n-1})^*$ be a state in $S_{n,0}$ (or $S_{n,1}$) where $n = 2^k \cdot m$ with $m > 1$ odd. We have that $\chi^\ell(\sigma)$ is in the cycle ($\mathcal{L}_0$) if and only if $f_\sigma(X)$ has exactly $2^{k-1} - \ell$ divisors $X+1$. Furthermore, $\#\mathcal{L}_k = \#\mathcal{L}_0 \cdot 2^k$.*

Proof The first statement follows from Proposition 12 as an application of χ to σ is the same as a multiplication of $f_\sigma(X)$ by $X+1$. Since every state has exactly two preimages, the latter statement follows from this immediately. □

Corollary 8 *Let n be an arbitrary even integer and let C_0 and C_1 be components of the state diagram of χ restricted to $S_{n,0} \cup S_{n,1}$. Then $\#\mathcal{L}_k(C_0) = \#\mathcal{L}_k(C_1)$ for all $k \geq 0$.*

Proof By Proposition 13 we know the statement for $k = 0$. For other k, this follows from Proposition 14. □

6.3.3 Decreasing period under application of χ

We have seen that sometimes a state propagates to a state of smaller period under χ. If this happens, this decrease in period is only by a factor 2 (Corollary 3) per application of χ. In this subsection, we give a criterion to recognize whether this will happen.

For any integer d, we can associate the integer $\zeta(d)$ to d, by setting all bits after the first zero bit in its binary expansion to 0. For example, if we have $d = 53$, then $\zeta(d) = 48$, as $53 =_2 11010$ in binary will be translated to $11000 =_2 48$.

Proposition 15 *Let $n = 2^k \cdot m$ with $m > 1$ odd. Let σ be a state of period n in $\mathcal{S}_0$. Let η and c be maximal such that $g_m(X)^\eta \mid f_\sigma(X)$ and $(X+1)^c \mid f_\sigma(X)$. Write $s := \zeta(\eta) - c$. Then*

1. $\mathrm{per}(\chi^s(\sigma)) = \frac{n}{2^{\mathrm{hw}(\zeta(\eta))}}$. *In particular,* $\mathrm{per}(\chi^\ell(\sigma)) = \frac{n}{2^{\mathrm{hw}(\zeta(\eta))}}$ *when $\ell \to \infty$;*
2. $\sigma \in \mathcal{L}_s$.

Proof In Proposition 5, we have seen that a state in $S_{n,0}$ has period dividing $n/2$ when $X^{n/4}+1 \mid f_\sigma(X)$. This extends by induction to σ has period dividing $n/2^i$ when $(X^m+1)^\mu \mid f_\sigma(X)$, where

$$\mu = \sum_{j=k-i-1}^{k-2} 2^j = 2^{k-1} - 2^{k-i-1}.$$

This shows the first statement.

Since application of χ to σ corresponds to multiplication of $f_\sigma(X)$ by $X+1$, we deduct c from η^* to obtain the number of iterations s of χ needed ere $\chi^s(\sigma) \in \mathcal{L}_0$. This proves the second statement. □

Remark further, that (as in the binary tree), the number of layers for a given period doubles over time. Take the cycle in the snowflake of period 6. There is the inner cycle, and one layer of preimages outside of that, both of which have period 6. The next layer has period 12. After that, the next two layers have period 24, while the next four layers have period 48, and so on.

Example 9 (A state of period 48*)* Consider the state σ of period 48 given by

$$\sigma = (000000101000000010001000101010000010101000100010)^*.$$

Note that σ has a zero in each odd position. We can thus write it as

$$(0,0,0,1,1,0,0,0,1,0,1,0,1,1,1,0,0,1,1,1,0,1,0,1)$$

by eliminating those zeroes. Its corresponding polynomial in $\mathbb{F}_2[X]/(X^{24}+1)$ is

$$f_\sigma(X) = 1 + X^2 + X^4 + X^5 + X^6 + X^9 + X^{10} + X^{11} + X^{13} + X^{15} + X^{19} + X^{20}.$$

We have $f_\sigma(X) = (X+1)^3 \cdot (X^2+X+1)^7 \cdot (X^3+X^2+1)$. Thus, since $7 = 8-1$, but also $7 = 4+2+1$, we see that after one application of χ, we have $\chi(\sigma)$ of period 24, since then $(X+1)^4 \cdot (X^2+X+1)^4 = (X^3+1)^4$ divides $f_{\chi(\sigma)}(X)$. We have

$$\begin{aligned} f_{\chi(\sigma)}(X) &= (X^3+1)^4 \cdot X^9 + X^7 + X^4 + X^3 + X^2 + X + 1 \\ &\mapsto X^9 + X^7 + X^4 + X^3 + X^2 + X + 1 \end{aligned}$$

in $\mathbb{F}_2[X]/(X^{12}+1)$. The factorisation of this polynomial is then easily found as: $(X^2+X+1)^3 \cdot (X^3+X^2+1)$. Hence after two more applications of χ, we will have a state of period 12 in a similar fashion. Then after a final last application of χ, we end up in the inner cycle of a snowflake of period 6. To work with the notation in Proposition 15, we have $48 = 2^4 \cdot 3$, hence $k = 4$. We have $c = 3$. We see that $\ell_{1,4} = 2^{4-1} - 2^{4-1-1} = 4$, hence $\chi(\sigma)$ has period $48/2 = 24$. Similarly, $\ell_{3,4} = 2^{4-1} - 2^{4-3-1} = 7$, hence $\chi^4(\sigma)$ has period $48/8 = 6$.

7 Non-periodic states

By working only with periodic states, we have left out the largest part of the set $\mathbb{F}_2^{\mathbb{Z}}$, namely the non-periodic states.

Lemma 17 *The set of periodic states $\widehat{\mathbb{F}_2}$ is countable, hence $\mathbb{F}_2^{\mathbb{Z}} \backslash \widehat{\mathbb{F}_2}$ is uncountable.*

Proof We have $\#\mathfrak{S}_n = 2^n$. In particular, each $\mathfrak{S}_n$ is finite. Since $\widehat{\mathbb{F}_2} = \bigcup_{n\in\mathbb{N}^*} \mathfrak{S}_n$, we find that $\widehat{\mathbb{F}_2}$ is countable. Since $\mathbb{F}_2^{\mathbb{Z}}$ is uncountable, $\mathbb{F}_2^{\mathbb{Z}} \setminus \widehat{\mathbb{F}_2}$ is uncountable. □

As a result, if one would to pick one arbitrary element of $\mathbb{F}_2^{\mathbb{Z}}$ uniformly random, then it is almost certainly an element in $\mathbb{F}_2^{\mathbb{Z}} \setminus \widehat{\mathbb{F}_2}$. For practical reasons, we never need them, as the uses in cryptography always work with something that can be constructed. We do give an example of a state that has no finite period and see how χ operates on a state like this.

Example 10 We create a one-ended infinite string, recursively, by creating a sequence of finite states:

$$\Delta^{(0)} = 1; \qquad \Delta^{(n+1)} = \Delta^{(n)} \| 0^n 1.$$

The endresult, $\Delta := \lim_{n\to\infty} \Delta^{(n)}$ is then a string in $\mathbb{F}_2^{\mathbb{N}}$ that has no finite period. To make a string that is actually in $\mathbb{F}_2^{\mathbb{Z}}$, we just set $\Delta_n = \Delta_{-n}$ for $n < 0$.

For clarity, we print some bits of Δ, namely Δ_0 until Δ_{56}.

$$\Delta = \cdots 11010010001000010000010000001000000010000000010000000010\cdots$$

When we apply χ to Δ, we obtain the following, where - upon repeating - one observes where the anchors for χ are.

$$\chi(\Delta) = \cdots 10011010101001010001010000101000001010000001010000000101010\cdots$$
$$\chi^2(\Delta) = \cdots 11010000001100010100010010001000100010000100001000100000100010\cdots$$
$$\chi^3(\Delta) = \cdots 10010000101101000101011010101010101010010101010100010101010\cdots$$
$$\chi^4(\Delta) = \cdots 11010010001001010000010000000000000001100000001010000000010\cdots$$

We proved in Theorem 4 that χ is surjective on $\widehat{\mathbb{F}_2}$. In fact, we can prove that χ is surjective on $\mathbb{F}_2^{\mathbb{Z}}$.

This requires some topological discussion:

Theorem 5 *Let $(X, \mathcal{T})$ be a compact Hausdorff space and let $A \subset X$ be dense. Let $f\colon X \to X$ be a continuous map such that $f_{|A}\colon A \to A$ is surjective. Then f is surjective.*

Proof Since the image under a continuous map of a compact set has to be compact again, the image of f needs to be compact (see [14], Theorem 17.7). Since $(X, \mathcal{T})$ is Hausdorff, this means that the image of f needs to be closed (see [14], Theorem 17.5(b)). As the image of f contains A by hypothesis, we find that the image of f is the entire space X, and hence f is surjective. □

Theorem 6 *The map $\chi\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is continuous and surjective.*

Proof We bestow the discrete topology on $\mathbb{F}_2$ and create from that the product topology on $\mathbb{F}_2^{\mathbb{Z}}$. Then by Tychonoff's Theorem (first proved in [12],[13], in more modern terminology [14], Theorem 17.8), we find that $\mathbb{F}_2^{\mathbb{Z}}$ is compact. Next, $\mathbb{F}_2^{\mathbb{Z}}$ is Hausdorff, as any product of Hausdorff spaces is again Hausdorff (see [14], Theorem 13.8(b)). We still have to show that $\widehat{\mathbb{F}_2}$ is dense in $\mathbb{F}_2^{\mathbb{Z}}$ w.r.t. the product topology and that χ is continuous, then the result follows from Theorem 5. Since $\mathbb{F}_2^{\mathbb{Z}}$ has the product topology, to show that χ is continuous, we only need to show that for every $i \in \mathbb{Z}$ the map

$$\pi_i \circ \chi = \chi_{(i)} \colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2,\ (x_n)_{n=-\infty}^{\infty} \mapsto x_i + (x_{i+1}+1)x_{i+2}$$

is continuous (see [14], Theorem 8.8). (Here π_i is the projection on the ith coordinate.) Let i be arbitrary. We need to show that for each of the four open sets in $\mathbb{F}_2$, that the preimage of that set is again open in the product space. For $\emptyset$ and $\mathbb{F}_2$ it is clear, as $\chi_{(i)}^{-1}(\emptyset) = \emptyset$ and $\chi_{(i)}^{-1}(\mathbb{F}_2) = \mathbb{F}_2^{\mathbb{Z}}$. Consider $\{0\}$ as an open set in $\mathbb{F}_2$. Since the output of $\chi_{(i)}$ depends only on three bits, the preimages are found as:

-----101-----
-----000-----
-----010-----
-----011-----

The indicated bits are those at positions i,$i+1$ and $i+2$. The places where there is a dash, can be freely chosen. We construct $\mathcal{U} = \prod_{j\in\mathbb{Z}} U_j$ where $U_j = \mathbb{F}_2$ when $j \neq i, i+1, i+2$, $U_j = \{1\}$ when $j = i, i+2$, and $U_j = \{0\}$ when $j = i+1$. Then this set $\mathcal{U}$ contains all preimages of the first form -----101----- while it is an open set. For the three forms of remaining preimages we can choose a similar open set that contains all of them, and is open. The union of these four sets is then again an open set in $\mathbb{F}_2^{\mathbb{Z}}$ and it is the entire preimage of $\{0\}$.

The case of $\{1\}$ as an open set in $\mathbb{F}_2$ is dealt with similarly, and then indeed, χ is continuous.

Then to show that $\widehat{\mathbb{F}_2}$ is dense in $\mathbb{F}_2^{\mathbb{Z}}$, we use the criterion that a subset is dense if and only if it intersects each base element of the topology.

The base sets of $\mathbb{F}_2^{\mathbb{Z}}$ are of the form $B = \prod_{i\in\mathbb{Z}} U_i$ with each U_i open and $U_i \neq \mathbb{F}_2$ for at most finitely many i. Take one such base set arbitrarily.

Without loss of generality, we may assume that $U_i \neq \emptyset$ for all i. Fix all (finitely many) i such that $U_i \neq \mathbb{F}_2$. This gives us a finite set $\mathcal{I} = \{i_0, \ldots, i_{n-1}\} \subset \mathbb{Z}$. We may assume $i_0 < \ldots < i_{n-1}$. Write $\ell = i_n - i_0$.

We construct $(z_k)_{k=i_0}^{i_n}$ by setting $z_k \in U_i$ when $k \in \{i_0, \ldots, i_n\}$. Then we have constructed a finite element $(z_k)_{k=i_0}^{i_n} \in \mathbb{F}_2^{\ell}$ that we can extend to a periodic element by repeated this $(z_k)_{k=i_0}^{i_n}$ on both sides. Write $(\tilde{z_k})_{k=-\infty}^{\infty}$ for this periodic element. Then $(\tilde{z_k})_{k=-\infty}^{\infty} \in \widehat{\mathbb{F}_2}$. Since $z_k \in U_k$ for each $i_0 < k < i_n$ and outside of these bounds $U_k = \mathbb{F}_2$, we find that $(z_k)_{k=-\infty}^{\infty} \in B$. Hence $B \cap \widehat{\mathbb{F}_2} \neq \emptyset$, and $\widehat{\mathbb{F}_2}$ is dense in $\mathbb{F}_2^{\mathbb{Z}}$. □

8 Applications

In this section we describe two applications of the results obtained before. One is the formula for the order of χ_n where n is odd. The other is to use χ_n as non-linear layer in ciphers for even n.

8.1 Order of χ_n for odd n

Since χ maps states of odd period bijectively onto states of the same period, the corresponding map χ_n is an element of the finite group of bijective maps on $\mathbb{F}_2^n$. Therefore χ_n has a finite order.

Corollary 9 (Order of χ_n) *Let $n > 0$ be odd. Then*

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

Proof With notations as in the proof of Theorem 2:

$$\begin{aligned}\mathrm{ord}(\chi_n) &= \operatorname*{lcm}_{\sigma \in \mathfrak{S}_n} (\#\mathcal{O}_\chi(\sigma)) \\ &= \max_{\sigma \in \mathfrak{S}_n} (2^{\lceil \lg(d_i - 1) \rceil}) \\ &= 2^{\lceil \lg(\frac{n+1}{2}) \rceil}\end{aligned}$$

as required. The last step follows from the fact that the distance between two anchors is maximal if the entire state contains just one anchor. □

Now that we have this formula $\mathrm{ord}(\chi_n) = 2^{\lceil \lg(\frac{n+1}{2}) \rceil}$, we see that this is just the smallest power of 2 that is greater than or equal to $\frac{n+1}{2}$, or in other words, the largest power of 2 that is smaller than n.

We conclude this subsection by referring to Table 1 for some values of the order of χ_n.

n	1	3	5	7	9	11	13	15	17	31	33	63	65	127	129
$\mathrm{ord}(\chi_n)$	1	2	4	4	8	8	8	8	16	16	32	32	64	64	128

Table 1 Some values of $\mathrm{ord}(\chi_n)$.

8.2 Using χ_n for even n as non-linear layer in ciphers

We can count the number of states in $\mathbb{S}_n := \bigcup_{d|n}(S_{d,0} \cup S_{d,1})$ for any n.

We know that $\#\mathfrak{S}_n = 2^n$ and furthermore that $\bigcup_{d|n} S_{d,0}$ contains precisely all elements that have period dividing n with zeroes on each even position. Therefore, there are $2^{\frac{n}{2}}$ such elements. The same holds for $\bigcup_{d|n} S_{n,1}$, hence $\#\mathbb{S}_n = 2^{\frac{n}{2}+1} - 1$.

If we draw an element uniformly random out of $\mathfrak{S}_n$ has a probability of $\frac{2^{\frac{n}{2}+1}-1}{2^n} \leq 2^{1-\frac{n}{2}}$ to be inside $\mathbb{S}_n$. For instance, when $n = 256$, we have a probability of 2^{-127} to draw an element in $\mathbb{S}_{256}$. We remark that when n goes to infinity, this expression converges exponentially to 0.

One way to randomize the inputs is by applying the Even-Mansour construction ([8]) to build a block cipher from a iterated permutation that has as its non-linear layer χ_n.

The Even-Mansour construction is built on a permutation F. On input P, one round in the Even-Mansour construction outputs $C := F(P \oplus K_1) \oplus K_2$. The additions of K_1 to P randomizes the input bits to F.

When Even-Mansour is a block cipher, the function F often needs to be a permutation. However, certain block cipher modes do not use the invertibility property of the function F. In these cases, one could use (a function built on) a single circle χ_n where n is an even number of bits, possibly 2^k for some $k \geq 1$. The probability of obtaining a collision after a single round - when taking two inputs uniformly random - is $\approx \frac{2^{n/2}}{2^{2n}}$, which for $n = 128$ is 2^{-192}. However, an attacker can choose their queries specifically to obtain a probability of a collision as large as possible. For instance, with the Even-Mansour construction where the internal function is χ_n with $n = 256$ bits, the attacker can choose two inputs with an input difference equal to $(01)^{\frac{n}{2}}$.

Thus one takes some inputs P and $P \oplus (01)^{\frac{n}{2}}$. From Lemma 12, we know that if $P \oplus K_1 \in S_{n,0}$, then $\chi_n(P \oplus K_1) = \chi_n(P \oplus (01)^{\frac{n}{2}} \oplus K_1)$, hence we find a collision. For a fixed key K_1, this happens in precisely $2^{\frac{n}{2}}$ choices for P. Therefore, one just needs to take $n = 256$ when striving for 128 bits of security.

References

1. Bertoni, G. and Daemen, J. and Peeters, M. and Van Assche, G.: KECCAK specifications, NIST SHA-3 Submission (2008). URL `http://keccak.noekeon.org/`
2. Claesen, L., Daemen, J., Genoe, M., Peeters, G.: Subterranean: A 600 mbit/sec cryptographic vlsi chip pp. 610–613 (1993)
3. Daemen, J.: Cipher and Hash Function Design Strategies based on linear and differential cryptanalysis. Ph.D. thesis, Katholieke Universiteit Leuven (1995)
4. Daemen, Joan and Hoffert, Seth and Van Assche, Gilles and Van Keer, Ronny: The design of Xoodoo and Xoofff. IACR Transactions on Symmetric Cryptology **2018**(4), 1–38 (2018). URL `https://tosc.iacr.org/index.php/ToSC/article/view/7359`
5. Daemen, Joan and Massolino, Pedro Maat Costa and Mehrdad, Alireza and Rotella, Yann: The Subterranean 2.0 Cipher Suite. IACR Transactions on Symmetric Cryptology **2020**(S1), 262–294 (2020). URL `https://tosc.iacr.org/index.php/ToSC/article/view/8622`
6. Dobraunig, Christoph and Eichlseder, Maria and Grassi, Lorenzo and Lallemand, Virginie and Leander, Gregor and List, Eik and Mendel, Florian and Rechberger, Christian: Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit. In: Shacham, Hovav and Boldyreva, Alexandra (ed.) Advances in Cryptology – CRYPTO 2018, pp. 662–692. Springer International Publishing, Cham (2018)
7. Dobraunig, Christoph and Eichlseder, Maria and Mendel, Florian and Schläffer, Martin: Ascon v1.2 Submission to NIST (2021)
8. Even, Shimon and Mansour, Yishay: A construction of a cipher from a single pseudorandom permutation. J. Cryptology (10), 151–161 (1997)
9. Möbius, August Ferdinand: Über eine besondere Art von Umkehrung der Reihen. Journal für die reine und angewandte Mathematik (8), 105–123 (1832)
10. NIST: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Fucntions. FIPS PUB 202 (2015). URL `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf`
11. NIST: Lightweight Cryptography Standardization Process: NIST Selects Ascon (2023). URL `https://csrc.nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon`

12. Tychonoff, Andrey: Über die topologische Erweiterung von Räumen. Mathematische Annalen (102), 544–561 (1930)
13. Tychonoff, Andrey: Über einen Funktionenraum. Mathematische Annalen (111), 762–766 (1935)
14. Willard, Stephen: General Topology. Addison-Wesley Publishing Company, Inc. (1970)
15. Wolfram, Stephen: A New Kind of Science. Wolfram Media (2002)

9 Appendix

9.1 Tables for cycle lengths in snowflakes

In this section we give tables with values of odd $m > 1$ that have a certain cycle length with respect to $2^o - 1$, where $o = \mathrm{ord}_m(2)$. The first table lists those values of m, where the cycle length is not equal to $2^o - 1$.

11	13	19	25	27	29	37	41	43	53
57	59	61	67	81	83	95	97	99	101
107	109	111	113	121	125	131	137	139	145
149	157	163	169	171	173	177	179	181	185
193	197	199	201	203	205	209	211	227	229
241	243	249	251	265	269	277	281	283	289
293	297	305	307	313	317	321	325	331	347
349	353	361	363	371	373	377	379	387	389

Table 2 Some values of m for which the cycle does not attain the length $2^o - 1$.

m	cycle length	$2^o - 1$	quotient
3	3	3	-
5	15	15	-
7	7	7	-
9	63	63	-
11	341	1023	3
13	819	4095	5
15	15	15	-
17	255	255	-
19	9709	262143	27
21	63	63	-
23	2047	2047	-
25	25575	1048575	41
27	13797	262143	19
29	475107	268435455	565
31	31	31	-
33	1023	1023	-
35	4095	4095	-
37	3233097	68719476735	21255

Table 3 For $1 < m < 39$ odd, some cycle lengths in the snowflakes in $S_{2m,0}$, in relation to $2^o - 1$, where o is the order of 2 modulo m.