Algebraic Structure of the Iterates of χ

Björn Kriepke[1] and Gohar Kyureghyan[1]

Institute of Mathematics, University of Rostock, Germany
{bjoern.kriepke, gohar.kyureghyan}@uni-rostock.de

Abstract. We consider the map $\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ for n odd given by $y = \chi(x)$ with $y_i = x_i + x_{i+2}(1 + x_{i+1})$, where the indices are computed modulo n. We suggest a generalization of the map χ which we call generalized χ-maps. We show that these maps form an Abelian group which is isomorphic to the group of units in $\mathbb{F}_2[X]/(X^{(n+1)/2})$. Using this isomorphism we easily obtain closed-form expressions for iterates of χ and explain their properties.

1 Introduction

Consider the map $\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ given by $y = \chi(x)$ where $y_i = x_i + x_{i+2}(1 + x_{i+1})$. It is known that χ is a permutation if and only if n is odd [2]. Therefore, in this paper we assume that n is odd.

The map χ is used in several cryptographic primitives, for example in SHA-3 [6] and Ascon [3]. A number of recent papers contributed to a better understanding of cryptological properties of the map χ, see for example [5,7,8].

In this paper we study the iterates of χ, that is $\chi^j = \chi \circ \ldots \circ \chi$. We observe that these iterates are linear combinations of special maps which we call γ_{2k} for $k \geq 0$. Then we consider the set Γ of all linear combinations of the maps γ_{2k} for $k \geq 0$ and show that these maps have strong arithmetic properties. We show that a subset $G \subseteq \Gamma$ forms an Abelian group with respect to composition. This group is isomorphic to the group of units of the ring $\mathbb{F}_2[X]/(X^{(n+1)/2})$ in a straightforward way. Furthermore the iterates of χ are elements of G. This isomorphism explains in a direct way some properties of χ and its iterates. We expect, that our results can be used to get more insights on security of cryptological applications based on χ.

The paper is structured as follows: In Section 2 we start by computing the first iterates of χ. This gives an insight into why the maps γ_{2k} are important subjects to study in this context. In Section 3 we consider the vector space Γ spanned by γ_{2k} for $k \geq 0$ and study a certain subset $G \subseteq \Gamma$ consisting of bijective maps. In Section 4 we apply the results of the previous section to describe properties of some special maps from G, including χ.

2 Warm-up: Iterates of χ

As a warm-up, we start by computing the first few iterates of χ. Let $x \in \mathbb{F}_2^n$ and set $x^{(j)} = \chi^j(x)$ for $j \geq 1$. Then $x^{(2)} = \chi^1(x^{(1)})$ is given by

$$\begin{aligned} x_i^{(2)} &= x_i^{(1)} + x_{i+2}^{(1)} \cdot (1 + x_{i+1}^{(1)}) \\ &= x_i + x_{i+2} \cdot (1 + x_{i+1}) \\ &\quad + (x_{i+2} + x_{i+4} \cdot (1 + x_{i+3})) \cdot (1 + (x_{i+1} + x_{i+3} \cdot (1 + x_{i+2}))), \end{aligned}$$

using the definition of $x^{(1)} = \chi(x)$. We pay special attention to the last summand. Note that $x_{i+2} \cdot (1 + x_{i+2}) = 0$ because $x_{i+2} \in \mathbb{F}_2$. Similarly, $(1 + x_{i+3}) \cdot x_{i+3} = 0$. We obtain

$$\begin{aligned} &(x_{i+2} + x_{i+4} \cdot (1 + x_{i+3})) \cdot (1 + (x_{i+1} + x_{i+3} \cdot (1 + x_{i+2}))) \\ &\quad = (x_{i+2} + x_{i+4} \cdot (1 + x_{i+3})) \cdot ((1 + x_{i+1}) + x_{i+3} \cdot (1 + x_{i+2})) \\ &\quad = x_{i+2} \cdot (1 + x_{i+1}) + \underbrace{x_{i+2} \cdot x_{i+3} \cdot (1 + x_{i+2})}_{=0} \\ &\qquad + x_{i+4} \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}) + \underbrace{x_{i+4} \cdot (1 + x_{i+3}) \cdot x_{i+3} \cdot (1 + x_{i+1})}_{=0} \\ &\quad = x_{i+2} \cdot (1 + x_{i+1}) + x_{i+4} \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}) \end{aligned}$$

and hence

$$\begin{aligned} x_i^{(2)} &= x_i + x_{i+2} \cdot (1 + x_{i+1}) + x_{i+2} \cdot (1 + x_{i+1}) + x_{i+4} \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}) \\ &= x_i + x_{i+4} \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}). \end{aligned}$$

In a similar manner we can compute $x^{(3)}$ and $x^{(4)}$ and obtain

$$\begin{aligned} x_i^{(3)} &= x_i + x_{i+2} \cdot (1 + x_{i+1}) + x_{i+4} \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}) \\ &\qquad + x_{i+6} \cdot (1 + x_{i+5}) \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}) \\ x_i^{(4)} &= x_i + x_{i+8} \cdot (1 + x_{i+7}) \cdot (1 + x_{i+5}) \cdot (1 + x_{i+3}) \cdot (1 + x_{i+1}). \end{aligned}$$

For $k \geq 1$ we define the map $\gamma_{2k}(x)$ with $y = \gamma_{2k}(x)$ given by

$$y_i = x_{i+2k} \cdot (1 + x_{i+2k-1}) \cdot (1 + x_{i+2k-3}) \cdots (1 + x_{i+1})$$

for all indices $i = 1, \ldots, n$. Then notice that we can write χ^j for $j = 1, 2, 3, 4$ in the following form:

$$\begin{aligned} \chi(x) &= x + \gamma_2(x) \\ \chi^2(x) &= x \qquad\qquad + \gamma_4(x) \\ \chi^3(x) &= x + \gamma_2(x) + \gamma_4(x) + \gamma_6(x) \\ \chi^4(x) &= x \qquad\qquad\qquad\qquad + \gamma_8(x). \end{aligned}$$

If we put γ_0 to denote the identity map, then the above calculations show that the first iterates of χ are linear combinations of γ_{2k} over $\mathbb{F}_2$. In the following section we confirm this observation for all iterates of χ by showing the following theorem. Let $j = j_0 + 2j_1 + 2^2 j_2 + \ldots + 2^s j_s$ and $k = k_0 + 2k_1 + 2^2 k_2 + \ldots + 2^s k_s$ be two integers, written in base 2. Write $j \preceq k$ if for all $i = 0, \ldots, s$ it holds that $j_i \leq k_i$. Equivalently, $j_i = 1$ implies $k_i = 1$. In such cases we say that j is covered by k.

Theorem 1. *Let $k \geq 1$. Then*

$$\chi^k = \sum_{j=0}^{\min\{k,(n-1)/2\}} a_j \gamma_{2j}$$

with $a_j = 1$ if and only if $j \preceq k$. The algebraic degree of χ^k is $j+1$ with the largest $j \leq (n-1)/2$ such that $j \preceq k$.

3 Vector space Γ generated by maps γ_{2k}

Motivated by the computations in the previous section we consider the linear span of the maps γ_{2k} for $k \geq 0$. We start by defining some notation which was partly introduced in [4].

We denote the vector $(1, \ldots, 1) \in \mathbb{F}_2^n$ by $\mathbb{1}$. Let $S : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be the cyclic left shift operator, i.e., $S(x_1, \ldots, x_n) = (x_2, \ldots, x_n, x_1)$. With the symbol $\odot$ we denote the elementwise multiplication of two vectors $x, y \in \mathbb{F}_2^n$, which is also called the Hadamard product. More precisely, $z = x \odot y$ denotes the vector with $z_i = x_i \cdot y_i$ for all $i = 1, \ldots, n$. Note that S is linear. Furthermore, $S(x \odot y) = S(x) \odot S(y)$. The Hadamard product $\odot$ is commutative and distributive over addition, that is, $x \odot y = y \odot x$ and $x \odot (y + z) = x \odot y + x \odot z$.

Note that for any $y \in \mathbb{F}_2^n$ we have $y \odot (\mathbb{1} + y) = 0$. In particular also

$$S^j \odot (\mathbb{1} + S^j) = 0$$

for every $j \geq 0$.

Observe that for $2k \geq 2$ the previously defined maps $\gamma_{2k} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are given by

$$\gamma_{2k} = S^{2k} \odot (\mathbb{1} + S^{2k-1}) \odot (\mathbb{1} + S^{2k-3}) \odot \ldots \odot (\mathbb{1} + S^1),$$

and $\gamma_0 = S^0 = \mathrm{id}$ is the identity map. With this notation, we have

$$\chi = \mathrm{id} + S^2 \odot (\mathbb{1} + S) = \gamma_0 + \gamma_2.$$

3.1 Some basic observations on the maps γ_{2k}

Remark 1. Let $x \in \mathbb{F}_2^n$ and $y = \gamma_{2k}(x)$ for $k \geq 1$. Then the components of y are given by

$$y_i = x_{i+2k} \cdot (1 + x_{i+2k-1}) \cdot (1 + x_{i+2k-3}) \cdot \ldots \cdot (1 + x_{i+1}).$$

Therefore $y_i = 1$ if and only if $(x_{i+1}, \ldots, x_{i+2k}) = (0, *, 0, *, \ldots, 0, *, 0, 1)$ where we put $*$ to denote an arbitrary element in $\mathbb{F}_2$.

The next two lemmas imply in particular that the set of the maps $\gamma_{2k} : \mathbb{F}_2^n \to \mathbb{F}_2^n, k \geq 0$, contains exactly $(n+1)/2$ nonzero functions.

Lemma 1. *Let $2k > n$. Then $\gamma_{2k} = 0$.*

Proof. Consider the function γ_{2k} with $2k > n$. Then $S^{2k} = S^{2k-n}$ and $2k - n$ is odd. Therefore

$$\begin{aligned}\gamma_{2k} &= S^{2k-n} \odot (\mathbb{1} + S^{2k-1}) \odot (\mathbb{1} + S^{2k-3}) \odot \ldots \odot (\mathbb{1} + S^{2k-n}) \odot \ldots \odot (\mathbb{1} + S) \\ &= S^{2k-n} \odot (\mathbb{1} + S^{2k-n}) \odot (\ldots) = 0.\end{aligned}$$

□

Recall that the algebraic degree of a map $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is the maximal multivariate degree of its component functions.

Lemma 2. *Let $0 \leq 2k < n$. Then the algebraic degree of γ_{2k} is $k + 1$. In particular, the maps $\gamma_0, \gamma_2, \ldots, \gamma_{n-1}$ are linear independent over $\mathbb{F}_2$.*

Proof. If $k = 0$ then $\gamma_{2k} = \gamma_0 = \mathrm{id}$ and the claim is clear. The entries of $y = \gamma_{2k}(x)$ for $k = 1, \ldots, (n-1)/2$ are given by

$$y_i = x_{i+2k} \cdot (1 + x_{i+2k-1}) \cdot (1 + x_{i+2k-3}) \cdots (1 + x_{i+1}).$$

As all variables x_j appearing in the product are distinct it follows that the algebraic degree of γ_{2k} is $k + 1$. □

Next we study the set of linear combinations of maps $\gamma_{2k}, k \geq 0$, which we denote by Γ, i.e.

$$\Gamma = \left\{ \sum_{k=0}^{\ell} a_k \gamma_{2k} : a_k \in \mathbb{F}_2, \ell \in \mathbb{N}_0 \right\} = \left\{ \sum_{k=0}^{(n-1)/2} a_k \gamma_{2k} : a_k \in \mathbb{F}_2 \right\}$$

where the second equality follows directly from Lemma 1. Recall that $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$ is the set of natural numbers including 0.

Lemma 3. *Γ is a vector space over $\mathbb{F}_2$ of dimension $(n+1)/2$ with basis $\{\gamma_0, \gamma_2, \ldots, \gamma_{n-1}\}$.*

Proof. It is clear that Γ is a subspace of the space V of all functions on $\mathbb{F}_2^n$. Lemma 2 immediately implies that $\{\gamma_0, \gamma_2, \ldots, \gamma_{n-1}\}$ is a basis of Γ. The dimension of Γ follows. □

3.2 Composition of maps in Γ

Later we show that the composition of certain elements in Γ remains in Γ. For this we need some preliminary results which are stated in the next several lemmas. We start with the following observation which is crucial for having nice closed formulas for these compositions.

We write $S^m \gamma_{2k}$ to denote the composition $S^m \circ \gamma_{2k}$.

Lemma 4. *Let $k \geq 0$ and $j, m \geq 1$. Then it holds that*

$$S^m \gamma_{2k} \odot S^{m-1} \gamma_{2j} = 0.$$

Proof. First assume $k \geq 1$. Let us write out what $S^m \gamma_{2k}$ and $S^{m-1}\gamma_{2j}$ are. We have

$$\begin{aligned} S^m \gamma_{2k} &= S^{2k+m} \odot (\mathbb{1} + S^{2k+m-1}) \odot \ldots \odot (\mathbb{1} + S^{m+3}) \odot (\mathbb{1} + S^{m+1}) \\ S^{m-1}\gamma_{2j} &= S^{2j+m-1} \odot (\mathbb{1} + S^{2j+m-2}) \odot \ldots \odot (\mathbb{1} + S^{m+2}) \odot (\mathbb{1} + S^m). \end{aligned}$$

Note that $2k + m$ and $2j + m - 1$ have a different parity. Further note that $2j + m - 1 \geq m + 1$ and $2k + m \geq m$ because $j \geq 1$ and $k \geq 0$, respectively.

If $2j - 1 < 2k$, then $m + 1 \leq 2j + m - 1 < 2k + m$ and the term $\mathbb{1} + S^{2j+m-1}$ appears in $S^m \gamma_{2k}$. Using the commutativity of $\odot$ and that $y \odot (\mathbb{1} + y) = 0$ for all $y \in \mathbb{F}_2^n$ it follows that

$$S^m \gamma_{2k} \odot S^{m-1} \gamma_{2j} = S^{2j+m-1} \odot (\mathbb{1} + S^{2j+m-1}) \odot (\ldots) = 0.$$

Similarly, if $2k < 2j - 1$, then $m \leq 2k + m < 2j + m - 1$ and the term $\mathbb{1} + S^{2k+m}$ appears in $S^{m-1}\gamma_{2j}$ and they cancel out by the same argument.

For $k = 0$ we have $S^m \gamma_{2k} = S^m \gamma_0 = S^m$ and the term $\mathbb{1} + S^m$ appears in $S^{m-1}\gamma_{2j}$. Again by the same argument as above we get $S^m \gamma_{2k} \odot S^{m-1}\gamma_{2j} = 0$. □

Lemma 5. *Let $m \geq 2$ be even and $k \geq 1$. Then we have*

$$S^m \gamma_{2k} \odot (\mathbb{1} + S^{m-1}) = S^{m-2} \gamma_{2k+2}.$$

Proof. Remember that $S(\mathbb{1}) = \mathbb{1}$ and that $S(x \odot y) = S(x) \odot S(y)$. It follows that

$$\begin{aligned} S^m \gamma_{2k} &= S^m \left(S^{2k} \odot (\mathbb{1} + S^{2k-1}) \odot (\mathbb{1} + S^{2k-3}) \odot \ldots \odot (\mathbb{1} + S) \right) \\ &= S^{m+2k} \odot (\mathbb{1} + S^{m+2k-1}) \odot (\mathbb{1} + S^{m+2k-3}) \odot \ldots \odot (\mathbb{1} + S^{m+1}) \end{aligned}$$

and then

$$\begin{aligned} &S^m \gamma_{2k} \odot (\mathbb{1} + S^{m-1}) \\ &\quad = S^{m+2k} \odot (\mathbb{1} + S^{m+2k-1}) \odot (\mathbb{1} + S^{m+2k-3}) \odot \ldots \odot (\mathbb{1} + S^{m+1}) \odot (\mathbb{1} + S^{m-1}) \\ &\quad = S^{m-2} \left(S^{2k+2} \odot (\mathbb{1} + S^{2k+1}) \odot (\mathbb{1} + S^{2k-1}) \odot \ldots \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S) \right) \\ &\quad = S^{m-2} \gamma_{2k+2}. \end{aligned}$$

□

Lemma 6. *Let m be even, $f = \sum_{i=0}^{k} a_i \gamma_{2i} \in \Gamma$ and $g = \gamma_0 + \sum_{j=1}^{s} b_j \gamma_{2j} \in \Gamma$. Then*

$$S^m(f) \odot (\mathbb{1} + S^{m-1}(g)) = S^{m-2} \left(\sum_{i=0}^{k} a_i \gamma_{2i+2} \right)$$

with $\tilde{f} = \sum_{i=0}^{k} a_i \gamma_{2i+2} \in \Gamma$.

Proof. We have

$$\begin{aligned}
&S^m(f) \odot (\mathbb{1} + S^{m-1}(g)) \\
&\quad = S^m\left(\sum_{i=0}^{k} a_i\gamma_{2i}\right) \odot \left(\mathbb{1} + S^{m-1}\left(\gamma_0 + \sum_{j=1}^{s} b_j\gamma_{2j}\right)\right) \\
&\quad = S^m\left(\sum_{i=0}^{k} a_i\gamma_{2i}\right) \odot (\mathbb{1} + S^{m-1}\gamma_0) + S^m\left(\sum_{i=0}^{k} a_i\gamma_{2i}\right) \odot \left(S^{m-1}\left(\sum_{j=1}^{s} b_j\gamma_{2j}\right)\right) \\
&\quad = \sum_{i=0}^{k} a_i \underbrace{S^m\gamma_{2i} \odot (\mathbb{1} + S^{m-1})}_{=S^{m-2}\gamma_{2i+2}} + \sum_{i=0}^{k}\sum_{j=1}^{s} a_i b_j \underbrace{S^m\gamma_{2i} \odot S^{m-1}\gamma_{2j}}_{=0} \\
&\quad = S^{m-2}\left(\sum_{i=0}^{k} a_i\gamma_{2i+2}\right)
\end{aligned}$$

where we use Lemma 4 and Lemma 5. □

Let $\mathcal{C}$ be the subspace

$$\mathcal{C} = \langle \gamma_2, \gamma_4, \ldots, \gamma_{n-1} \rangle$$

and G be the coset

$$G = \gamma_0 + \mathcal{C}.$$

Observe that Lemma 6 only holds for maps $g \in G$ and not for all $g \in \Gamma$.

Since $\chi = \gamma_0 + \gamma_2$ we have $\chi \in G$. Therefore we call the maps $g \in G$ generalized χ-maps. The next lemma gives a closed formula for the composition of the maps γ_{2k} with elements in G.

Lemma 7. *Let $m \geq 2$ be even and $f = \gamma_0 + \sum_{i=1}^{k} a_i\gamma_{2i} \in G$. Then*

$$\gamma_m \circ f = \sum_{i=0}^{k} a_i\gamma_{2i+m} \in \mathcal{C}.$$

Proof. We use Lemma 6 repeatedly. More precisely,

$$\begin{aligned}
\gamma_m \circ f &= [S^m \odot (\mathbb{1} + S^{m-1}) \odot (\mathbb{1} + S^{m-3}) \odot \ldots \odot (\mathbb{1} + S)] \circ f \\
&= S^m f \odot (\mathbb{1} + S^{m-1}f) \odot (\mathbb{1} + S^{m-3}f) \odot \ldots \odot (\mathbb{1} + Sf) \\
&= S^{m-2}\left(\sum_{i=0}^{k} a_i\gamma_{2i+2}\right) \odot (\mathbb{1} + S^{m-3}f) \odot (\mathbb{1} + S^{m-5}f) \odot \ldots \odot (\mathbb{1} + Sf) \\
&= S^{m-4}\left(\sum_{i=0}^{k} a_i\gamma_{2i+4}\right) \odot (\mathbb{1} + S^{m-5}f) \odot \ldots \odot (\mathbb{1} + Sf) = \ldots = \\
&= \sum_{i=0}^{k} a_i\gamma_{2i+m}.
\end{aligned}$$

□

Remember that a monoid $(M, *)$ is a set together with an associative operation $* : M \times M \to M$ such that there exists a neutral element $e \in M$ with respect to $*$.

Theorem 2. *Let $f, g \in G$. Then $f \circ g \in G$. In particular G is a monoid with respect to composition.*

Proof. Write $f = \gamma_0 + \sum_{i=1}^{k} a_i \gamma_{2i}$ and $g = \gamma_0 + \sum_{j=1}^{s} b_j \gamma_{2j}$. Then

$$\begin{aligned} f \circ g &= \left(\gamma_0 + \sum_{i=1}^{k} a_i \gamma_{2i}\right) \circ g \\ &= \underbrace{\gamma_0 \circ g}_{=g} + \left(\sum_{i=1}^{k} a_i \gamma_{2i}\right) \circ g \\ &= \gamma_0 + \underbrace{\sum_{j=1}^{s} b_j \gamma_{2j}}_{\in \mathcal{C}} + \sum_{i=1}^{k} a_i \underbrace{\gamma_{2i} \circ g}_{\in \mathcal{C}} \in \gamma_0 + \mathcal{C} = G \end{aligned}$$

where we use Lemma 7 to conclude that $\gamma_{2i} \circ g \in \mathcal{C}$ for $i = 1, \ldots, k$.

Note that G contains the identity γ_0 which is a neutral element with regards to composition. Furthermore composition is associative. Hence $(G, \circ)$ is a monoid. □

Remark 2. Note that Γ is not closed under composition.

If $f \in \mathcal{C} = \Gamma \setminus G$ and $g \in G$ then $f \circ g \in \mathcal{C}$. For example, $\gamma_2 \circ (\gamma_0 + \gamma_2) = \gamma_2 + \gamma_4 \in \mathcal{C}$ by Lemma 7. The general case $f = \sum_{i=1}^{k} a_i \gamma_{2i}$ follows by left-distributivity of $\circ$, i.e. $(f + g) \circ h = f \circ h + g \circ h$, and $\mathcal{C}$ being a vector space.

However, if $g \in \mathcal{C}$, then it can happen that $f \circ g \notin \Gamma$. For example, if $f = \gamma_2 \in \mathcal{C}$, then

$$\begin{aligned} \gamma_2 \circ \gamma_2 &= (S^2 \odot (\mathbb{1} + S)) \circ (S^2 \odot (\mathbb{1} + S)) \\ &= S^4 \odot (\mathbb{1} + S^3) \odot (\mathbb{1} + S^3 \odot (\mathbb{1} + S^2)) \\ &= S^4 \odot (\mathbb{1} + S^3) + S^4 \odot (\mathbb{1} + S^3) \odot S^3 \odot (\mathbb{1} + S^2) \\ &= S^4 \odot (\mathbb{1} + S^3) \notin \Gamma \end{aligned}$$

and also for $f = \gamma_0 + \gamma_2 \in G$ it follows that

$$(\gamma_0 + \gamma_2) \circ \gamma_2 = \gamma_2 + S^4 \odot (\mathbb{1} + S^3) \notin \Gamma.$$

3.3 A connection between Γ and a quotient ring of $\mathbb{F}_2[X]$

Next we show that the monoid $(G, \circ)$ is in fact an Abelian group. We achieve this by showing that it is isomorphic as a monoid to an Abelian group. In particular this implies that all maps in G are permutations of $\mathbb{F}_2^n$. Note that from Lemma 7

the composition of maps in G is reminiscent of polynomial multiplication, hence we could hope that there is a correspondence $\Gamma \to \mathbb{F}_2[X]$ of the form

$$\sum_{i=0}^{k} a_i \gamma_{2i} \mapsto \sum_{i=0}^{k} a_i X^i.$$

However, by Lemma 1 we have $\gamma_{2k} = 0$ for $2k > n$ and therefore such a map would not be well-defined. However, if we take the right-hand side polynomial modulo $X^{(n+1)/2}$, then we have a map. More precisely, we consider the ideal $(X^{(n+1)/2})$ generated by $X^{(n+1)/2}$ in $\mathbb{F}_2[X]$. We denote by R the factor ring $R = \mathbb{F}_2[X]/(X^{(n+1)/2})$ and the coset of f by $f + (X^{(n+1)/2}) = [f]$. Now we let $\varphi : \Gamma \to R$ be the map with

$$\varphi\left(\sum_{i=0}^{k} a_i \gamma_{2i}\right) = \left[\sum_{i=0}^{k} a_i X^i\right].$$

This map φ is well-defined.

Lemma 8. *Let $f \in \Gamma, g \in G$. Then $\varphi(f \circ g) = \varphi(f) \cdot \varphi(g)$. In particular, the restriction of φ to G is a monoid homomorphism.*

Proof. Let first $f = \gamma_{2k}$ and $g = \gamma_0 + \sum_{i=1}^{s} a_i \gamma_{2i} \in G$. Then with Lemma 7 we have

$$\varphi(\gamma_{2k} \circ g) = \varphi\left(\sum_{i=0}^{s} a_i \gamma_{2i+2k}\right) = \left[\sum_{i=0}^{s} a_i X^{i+k}\right] = \left[X^k\right] \cdot \left[\sum_{i=0}^{s} a_i X^i\right] = \varphi(\gamma_{2k}) \cdot \varphi(g).$$

The general case follows by linearity of φ. Let $f = \sum_{i=0}^{k} a_i \gamma_{2i}$. Then

$$\begin{aligned}\varphi(f \circ g) &= \varphi\left(\sum_{i=0}^{k} a_i \gamma_{2i} \circ g\right) = \sum_{i=0}^{k} a_i \varphi(\gamma_{2i} \circ g) \\ &= \sum_{i=0}^{k} a_i \varphi(\gamma_{2i}) \cdot \varphi(g) = \varphi\left(\sum_{i=0}^{k} a_i \gamma_{2i}\right) \cdot \varphi(g) = \varphi(f) \cdot \varphi(g).\end{aligned}$$

Note that $\varphi(\gamma_0) = [1] \in \mathbb{F}_2[X]$ which is the neutral element with respect to multiplication. □

We recall the next well-known lemma.

Lemma 9. *Let $f \in \mathbb{F}_2[X]$. Then $[f]$ is a unit in R if and only if the constant term of f is 1. The unit group R^* of R has $2^{(n-1)/2}$ elements.*

Proof. The element $[f]$ is a unit in R if and only if $\gcd(f, X^{(n+1)/2}) = 1$, equivalently, f does not have 0 as a root and therefore $f(0) = 1$. Each element in R has a unique representative with degree at most $(n-1)/2$. There are $2^{(n+1)/2}$ polynomials in $\mathbb{F}_2[X]$ with degree at most $(n-1)/2$ and half of them have constant term 1, therefore $|R^*| = 2^{(n-1)/2}$. □

Theorem 3. *$G = \gamma_0 + \langle \gamma_2, \gamma_4, \ldots, \gamma_{n-1} \rangle$ is an Abelian group which is isomorphic to $R^* = \left(\mathbb{F}_2[X]/(X^{(n+1)/2})\right)^*$.*

Proof. Note that the map $\varphi : G \to R^*$ is a monoid homomorphism by Lemma 8. Let $f = \left[1 + \sum_{i=1}^{k} a_i X^i\right] \in R^*$. Then $f = \varphi(\gamma_0 + \sum_{i=1}^{k} a_i \gamma_{2i})$ with $\gamma_0 + \sum_{i=1}^{k} a_i \gamma_{2i} \in G$ and hence φ is surjective. It holds that $|G| = |R^*| = 2^{(n-1)/2}$ which then implies that φ is also bijective. Therefore G and R^* are isomorphic as monoids. As R^* is in fact an Abelian group, it also follows that G is an Abelian group. □

Remark 3. Every map $f \in G = \gamma_0 + \langle \gamma_2, \gamma_4, \ldots, \gamma_{n-1} \rangle$ is a permutation $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$. To find the inverse of f we just need to find the inverse of $\varphi(f) \in R$, which can be effectively computed by using the Extended Euclidean Algorithm for polynomials.

4 Applications

In this section we present some applications of the tools developed in the previous section. We start by discussing the order of the elements in G. Then we obtain precise results on the order, algebraic degree and inverse of maps of the form $\gamma_0 + \gamma_{2k}$, generalizing the results on $\chi = \gamma_0 + \gamma_2$. Further we prove Theorem 1 on the expression for the iterates of χ, which allows us to describe the fixed points of χ^j and consequently the cycle structure of χ. Finally we illustrate a method similar to Horner's scheme to compute the maps in G more efficiently.

The following lemma gives the orders of the elements of R^*, hence by isomorphism also the order of all elements of G.

Lemma 10. *Let $f = [1 + X^j + \sum_{i=j+1}^{k} a_i X^i] \in R^*$. Then the order of f is given by $\mathrm{ord}(f) = 2^m$ with $2^m < \frac{n+1}{j} \leq 2^{m+1}$. In particular all elements of R^* have an order of at most $2^{\lfloor \log_2(n) \rfloor}$.*

Proof. By Lemma 9 the group R^* has $2^{(n-1)/2}$ elements. Hence by Lagrange's theorem the order of every element is a power of 2. For m arbitrary we then obtain

$$f^{2^m} = [1 + X^j + \sum_{i=j+1}^{k} a_i X^i]^{2^m} = [1 + X^{2^m j} + \sum_{i=j+1}^{k} a_i X^{2^m i}]$$

which equals [1] if and only if $2^m j \geq (n+1)/2$, or equivalently, $\frac{n+1}{j} \leq 2^{m+1}$. As we are interested in the smallest such m we obtain the claim. □

An interesting class of polynomials to study are binomials. The only binomials in R^* are of the form $[1 + X^k]$ which correspond to the maps $\gamma_0 + \gamma_{2k}$ in G. For these maps we can determine their order, inverse and algebraic degree.

Theorem 4. *Let $k \geq 1$ and $sk = \max\{tk : tk \leq (n-1)/2, t \in \mathbb{N}\}$ be the largest multiple of k which does not exceed $(n-1)/2$. Consider $f = \gamma_0 + \gamma_{2k} \in G$. Then the order of f is given by 2^m with $2^m < \frac{n+1}{k} \leq 2^{m+1}$. The inverse of f is $f^{-1} = \gamma_0 + \gamma_{2k} + \gamma_{4k} + \ldots + \gamma_{2sk}$. The algebraic degree of f is $k+1$ and the algebraic degree of f^{-1} is $sk+1$.*

Proof. Note that $\varphi(f) = [1 + X^k]$. The order of f then follows immediately by Lemma 10.

The inverse of $[1 + X^k]$ in R is given by

$$\begin{aligned}[1 + X^k]^{2^m - 1} &= \frac{[1 + X^k]^{2^m}}{[1 + X^k]} = \frac{\left[1 + \left(X^k\right)^{2^m}\right]}{[1 + X^k]} \\ &= \left[1 + X^k + X^{2k} + X^{3k} + \ldots + X^{(2^m-1)k}\right] \\ &= \left[1 + X^k + X^{2k} + \ldots + X^{sk}\right]\end{aligned}$$

and hence

$$f^{-1} = \varphi^{-1}\left(\left[1 + X^k + X^{2k} + \ldots + X^{sk}\right]\right) = \gamma_0 + \gamma_{2k} + \ldots + \gamma_{2sk}.$$

As the map γ_{2j} has algebraic degree $j+1$ by Lemma 2 the claim follows. □

If we let $k = 1$ in the previous theorem then we have $f = \gamma_0 + \gamma_2 = \chi$. Hence as a corollary we obtain the order of χ and a formula for its inverse χ^{-1}. The order of χ was previously proved in [8] using combinatorial considerations. A formula for the inverse of χ which was found in [5] by considering an affine variety associated to χ. Observe that the methods in [5,8] cannot be generalized in a straightforward manner to the general case which we consider in Theorem 4.

Corollary 1 ([5,8]). *The map $\chi = \gamma_0 + \gamma_2$ has order 2^m with m given by $2^m < n < 2^{m+1}$, i.e., $m = \lfloor \log_2(n) \rfloor$. The inverse of χ is given by $\chi^{-1} = \gamma_0 + \gamma_2 + \ldots + \gamma_{n-1}$. The inverse χ^{-1} has algebraic degree $(n+1)/2$.*

It has been noted before in [8] that χ behaves like the polynomial $1 + X$ in a ring $\mathbb{F}_2[X]/(X^d)$ for some $d \leq (n+1)/2$, however in a different context. More precisely, for a given $y \in \mathbb{F}_2^n$, call y_i a dynamic bit if the distance to the next bit y_j with $y_j = 1$ is even, otherwise call it static. If y_i is a static bit with $y_i = 1$, then it is called an anchor. It can be shown that χ preserves static bits and anchors. For a given anchor y_i we can define a so-called anchor polynomial $a^{(i)}(X)$. Then if $a^{(i)}(X)$ is the anchor polynomial of y_i and $b^{(i)}(X)$ is the anchor polynomial of $\chi(y)_i$, then $b^{(i)} = (1 + X)a^{(i)} \mod X^{d_i}$ where d_i depends on the distance to the previous anchor. It is unclear to us how (and if at all) this and our perspective are related.

Although the next results could be formulated for general binomials, we present them only for the map χ due to its significance in cryptography.

Next we use that $\varphi(\chi) = [1+X]$ to prove Theorem 1 and thus obtain explicit formulas for the iterates of χ.

Proof (of Theorem 1). It is known from Lucas's theorem, that $\binom{k}{j}$ is odd if and only if $j \preceq k$. Hence, by the Binomial Theorem and Lucas's Theorem, we have

$$[1+X]^k = \left[\sum_{j=0}^{k} \binom{k}{j} X^j\right] = \left[\sum_{j=0}^{k} a_j X^j\right] = \left[\sum_{j=0}^{\min\{k,(n-1)/2\}} a_j X^j\right].$$

Now we simply apply φ^{-1}. □

Remark 4. Note that the algebraic degree of χ^{k+1} can be smaller than the algebraic degree of χ^k, even if $\chi^{k+1} \neq \mathrm{id}$. As an example, for $n = 11$ we have $\chi^5 = \gamma_0 + \gamma_2 + \gamma_8 + \gamma_{10}$ with algebraic degree 6 and $\chi^6 = \gamma_0 + \gamma_4 + \gamma_8$ with algebraic degree 5.

Another application of our technique is a description of the fixed points of the iterates χ^j. We call $x \in \mathbb{F}_2^n$ a fixed point of χ^j if $\chi^j(x) = x$. For $j = 1$ it is well-known that the only fixed points of χ are $x = 0, \mathbb{1}$. In particular it then follows that $\chi^j(0) = 0$ and $\chi^j(\mathbb{1}) = \mathbb{1}$ for all $j \geq 1$. Therefore we call $x = 0, \mathbb{1}$ trivial fixed points. Note, that a fixed point of χ^j lies in a cycle of length dividing j in the cycle decomposition of the map χ. Hence the study of the fixed points of iterates of χ is equivalent to the study of the cycle structure of χ, which appeared in Theorem 2 and its proof in [8]. The methods used in [8] are different from ours and apply also to the cases of $\chi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with n even or $\chi : \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$. We would like to emphasize again that our methods can also be applied for other maps in G.

Lemma 11. *The map χ^j has a nontrivial fixed point if and only if $j = 2^k$ for some $1 \leq k \leq m$. The vector $x \in \mathbb{F}_2^n$ is a fixed point of χ^{2^k} if and only if x does not contain a substring of the form $(0, *, 0, *, \ldots, 0, *, 0, 1)$ of length 2^{k+1}, where $*$ denotes an arbitrary element of $\mathbb{F}_2$. More precisely, if there exists no integer $i = 1, \ldots, n$ with $(x_{i+1}, \ldots, x_{i+2^{k+1}}) = (0, *, 0, *, \ldots, 0, *, 0, 1)$ and the indices are computed modulo n.*

Proof. As the order of χ is 2^m with $2^m < n < 2^{m+1}$, any cycle of χ has length 2^k for some $0 \leq k \leq m$. In particular χ^j does not have a nontrivial fixed point if j is not a power of 2. Therefore we consider χ^{2^k}. By Theorem 1 we obtain $\chi^{2^k} = \gamma_0 + \gamma_{2^{k+1}}$.

A vector $x \in \mathbb{F}_2^n$ is a fixed point of χ^{2^k} if and only if $x = \chi^{2^k}(x)$, or equivalently, $\gamma_{2^{k+1}}(x) = 0$. By Remark 1 we have that $\gamma_{2^{k+1}}(x)_i = 1$ if and only if $(x_{i+1}, \ldots, x_{i+2^{k+1}}) = (0, *, 0, *, \ldots, 0, *, 0, 1)$. As x by assumption does not contain such a substring, we have $\gamma_{2^{k+1}}(x) = 0$ and x is a fixed point of χ^{2^k}. □

We call $x \in \mathbb{F}_2^n$ a proper fixed point of χ^j if x is a fixed point of χ^j and x is not a fixed point of χ^ℓ for any $\ell < j$. A proper fixed point of χ^j lies in a cycle of length equal to j in the cycle decomposition of χ.

Theorem 5. *Let $x \in \mathbb{F}_2^n \setminus \{0, \mathbb{1}\}$ and*

$$2^s = \max\{2^k : \exists i = 1, \ldots, n \text{ with } (x_{i+1}, \ldots, x_{i+2^k}) = (0, *, 0, *, \ldots, 0, *, 0, 1)\}.$$

Then x is a proper fixed point of χ^{2^s}.

Proof. Note that 2^s is well-defined, because any vector $x \in \mathbb{F}_2^n \setminus \{0, \mathbb{1}\}$ contains the substring $(0,1)$. From the definition of 2^s and Lemma 11 it follows that x is not a fixed point of $\chi^{2^{s-1}}$. However, x does not contain a substring $(0,*,0,*,\ldots,0,*,0,1)$ of length 2^{s+1} by maximality of 2^s and therefore x is a fixed point of χ^{2^s}, again by Lemma 11. □

We conclude the paper by observing, that the maps $f \in G$ can be evaluated by factoring them in a special way. The idea of this process is similar to Horner's scheme for polynomials. For ease of notation we only demonstrate this for an example. If $f = \gamma_0 + \gamma_2 + \gamma_4 + \gamma_6 + \gamma_8$, then

$$\begin{aligned} f &= \mathrm{id} + S^2 \odot (1+S) + S^4 \odot (1+S^3) \odot (1+S) \\ &\quad + S^6 \odot (1+S^5) \odot (1+S^3) \odot (1+S) \\ &\quad + S^8 \odot (1+S^7) \odot (1+S^5) \odot (1+S^3) \odot (1+S) \qquad (1) \\ &= \mathrm{id} + (S^2 + S^4 \odot (1+S^3) + S^6 \odot (1+S^5) \odot (1+S^3) \\ &\qquad + S^8 \odot (1+S^7) \odot (1+S^5) \odot (1+S^3)) \odot (1+S) \\ &= \mathrm{id} + (S^2 + (S^4 + S^6 \odot (1+S^5) + S^8 \odot (1+S^7) \odot (1+S^5)) \odot (1+S^3)) \odot (1+S) \end{aligned}$$

and hence

$$f = \mathrm{id} + (S^2 + (S^4 + (S^6 + S^8 \odot (1+S^7)) \odot (1+S^5)) \odot (1+S^3)) \odot (1+S) \quad (2)$$

or equivalently,

$$f(x)_i = x_i + (x_{i+2} + (x_{i+4} + (x_{i+6} + x_{i+8}(1+x_{i+7}))(1+x_{i+5}))(1+x_{i+3}))(1+x_{i+1}).$$

Note that for the choice $n = 9$ we have $f = \chi^7 = \chi^{-1}$, for which a similar formula already appeared in [1, Appendix D].

Formula (2) has only 4 Hadamard products $\odot$, while the original (1) has 10 such multiplications. Observe that f has algebraic degree 5, so 4 applications of $\odot$ is optimal. In general, if $f \in G$ has algebraic degree k, by using this process the number of applications of $\odot$ can be reduced to $k-1$ which is again optimal.

Acknowledgments. The authors thank the reviewers for their comments and suggestions which allowed to improve the presentation of this paper. We thank Lucas Krompholz for many interesting discussions and in particular for his idea to use the Hadamard product during our work on [4].

References

1. Biryukov, A., Bouillaguet, C., Khovratovich, D.: Cryptographic schemes based on the ASASA structure: Black-box, white-box, and public-key. Cryptology ePrint Archive, Report 2014/474 (2014), `https://eprint.iacr.org/2014/474`
2. Daemen, J.: Cipher and hash function design strategies based on linear and differential cryptanalysis. Ph.D. thesis, Doctoral Dissertation, March 1995, KU Leuven (1995)

3. Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: Ascon v1.2: Lightweight authenticated encryption and hashing. Journal of Cryptology **34**(3), 33 (Jul 2021). https://doi.org/10.1007/s00145-021-09398-9
4. Graner, A.M., Kriepke, B., Krompholz, L., Kyureghyan, G.M.: On the bijectivity of the map χ. Cryptology ePrint Archive, Paper 2024/187 (2024), https://eprint.iacr.org/2024/187
5. Liu, F., Sarkar, S., Meier, W., Isobe, T.: The inverse of χ and its applications to Rasta-like ciphers. Journal of Cryptology **35**(4), 28 (Oct 2022). https://doi.org/10.1007/s00145-022-09439-x
6. NIST: SHA-3 standard: Permutation-based hash and extendable-output functions. Tech. Rep. Federal Information Processing Standard (FIPS) 202, U.S. Department of Commerce (Aug 2015). https://doi.org/10.6028/NIST.FIPS.202
7. Schoone, J., Daemen, J.: Algebraic properties of the maps χ_n. Designs, Codes and Cryptography (2024). https://doi.org/10.1007/s10623-024-01395-w
8. Schoone, J., Daemen, J.: The state diagram of χ. Designs, Codes and Cryptography **92**, 1393–1421 (2024). https://doi.org/10.1007/s10623-023-01349-8