Abstract
In this paper, we derived subsets of natural numbers as periods and subsets of infinite two sided sequences as periodic points of Linear (additive) cellular automata in the simplest form and possible cardinality of the set of periods.

Keywords: Dynamical systems, Linear cellular automata, Periods, periodic points.

Introduction
We have a good number of papers that gives the periods of various dynamical systems like on periods of interval maps [see 8], on linear operators in [see 2,7], Moothathu 2006 and Akbar et al., 2009 toral automorphism in [see 3,4], onto cellular automata in [see 5]. In [1] author investigated the periods of linear cellular automata on prime modulo. We are going to find

Definition

Per (F) = \{ n \in \mathbb{N} \mid n is a period for some point \alpha \ in \mathbb{A} \}

P(F) = \{ S \in \mathbb{A} \mid \text{Every point in } S \text{ is a periodic point of } F \}

for the linear cellular automata in the specific form for

A = \{0, 1, 2, \ldots, m - 1\}

where \( m \geq 2 \) is and

\[ F(x_i) = ax_i + r \pmod{m} \]

Preliminaries

Definition

\((X, f)\) is topological dynamical system where \( X \) is topological space and \( f \) is a continuous self-map on \( X \).

Kannan et al., 2011 stated that, If Assume \((X, f)\) is a topological dynamical system and define basic preliminaries.

Definition

If \( f^n(x) = x \)

Then \( x \) is called periodic point and least such \( n \) is called the period of \( x \).

Definition

A periodic point of 1 is called the fixed point fixed and \( f^k(x) \) is fixed for some natural number \( k \geq 2 \) is called eventually fixed point.

Definition

The set of periods denoted by

Per (f) = \{ n \in \mathbb{N} \mid \text{there is a period in } (X, f) \text{ with period } n \}

Definition

For an integer \( m \geq 1 \). Let

\( \mathcal{A} = \{0, 1, 2, \ldots, m - 1\} \)

We call \( \mathcal{A} \) as an alphabet and its elements as symbols.

Let \( \Sigma = \mathcal{A}^\mathbb{Z} \) be the additive group of

Modulo \( m \) of infinite two-sided sequences of symbols in \( \mathcal{A} \)

We can define metric on these spaces which induces the same topology.

The Metric is

\[ d(a, b) = \frac{1}{2^k} \]

Where \( k = \min \{|i| \mid a_i \neq b_i \} \).

Given a two-sided sequence \( a = (a_n) \), let \( \sigma(a) \) be the sequence given by

\[ \sigma(a_n) = a_{n+1} \]

This defines a continuous self-map \( \Sigma \) called the shift map. The dynamical

System \((\Sigma, \sigma)\) is called the two-sided shift-map [see 6].

The infinite two-sided sequence

\( x = \ldots x_{-2}x_{-1}x_0x_1 \ldots \)

Here \( x_0 \) term starts after dot.
Definition

Pillai et al., 2010, studied and arises that, cellular automata is a dynamic system \((A^Z, F)\), such that it commutes with shift map (6)

\[ F \circ \sigma = \sigma \circ F \]

Where \(A\) is an alphabet and \(\sigma\) is shift map on \(A^Z\).

Another equivalent definition is \(F: A^Z \to A^Z\) is a cellular automata if there is

\[ r \in \mathbb{N} \text{ (radius) and a local rule} \]

\[ f : A^{2r + 1} \to A \text{ such that} \]

\[ F(x)_i = f(x_{i-2r}, \ldots, x_0, \ldots, x_{i+2r}) \]

For every \(x \in A^Z\) and \(i \in \mathbb{Z}\).

Definition

Let \(m \geq 2\) be an integer and

\[ A = \{0, 1, 2, \ldots, m - 1\} \]

Linear Cellular automata is a map from \(F: A^Z \to A^Z\), which has the form

\[ F(x) = \sum_{i=r}^{m} a_{x_i+1} \mod m' \] \( (7) \)

For some natural number \(m' \leq m\) and fixed \(k \geq 1\) and fixed integers \(a_r\). With out loss of generality we consider \(m' = m\).

We can write the equation (7) in the expansion

\[ F(0) = \sum_{i=r}^{m} a_{x_i+1} \mod m' \]

Holmgren 2000, Define \(F: A^Z \to A^Z\) as

\[ F(x)_i = 2x_i + 3x_{i+1} \]

Saradhi 1997, consider shorter form of the linear cellular automaton and determines the possible periods and periodic points.

Definition

Euler function \(\phi(m)\) denotes number of natural numbers less than \(m\) and coprime to \(m\).

Euler theorem as a generalisation to Fermat theorem, is \(a^{\phi(m)} \equiv 1 \mod m\) where \(a, m\) are coprime. (see 9). Fermat little theorem is same as Euler’s theorem for prime \(m\).

Main problem

Block et al., 2006, found the periods of linear cellular automata for the alphabet set modulo prime number using combinatorics in [see 1].

In this paper we are going to find \(\text{Per}(F)\) and \(P(F)\) as defined in equations (1) and (2) for the linear cellular automata defined in (3).

Theorem 1: Finding \(\text{Per}(F)\) and \(P(F)\) when \(F(x)_i = ax_i\), when \(a\) is idempotent element.

Proof. Given \(a\) is idempotent so \(a^2 \equiv a \mod m\).

Then \(a^2 \equiv a^2 \mod m\) \(\equiv a \mod m\) \(\mod m\)

Similarly, \(a^4 \equiv a \mod m\) and so on.

So, for every positive natural number \(n\), we get

\[ F^n(x)_i = a x_i \]

Case 1: If \(a \equiv 1 \mod m\) then it is identity mapping and every sequence in \(A^Z\) is fixed for \(F\).

\[ \text{Per}(F) = \{1\} \]

\[ P(F) = \{0 \in A^Z; 0 = \ldots 00000.000 \ldots\} \]

Example: For \(A = \{0, 1, 2, 3, 4\} \mod 5\)

Define function as \(F(x)_i = 3x_i \mod m\).

Clearly \(3\) is idempotent as \(3^2 = 9 \equiv 3 \mod m\)

It has period 1 and periodic point is zero sequence.

The same is true for the function \(F(x)_i = 4x_i \mod m\) as 4 is idempotent element.

Theorem 2: Finding \(\text{Per}(F)\) and \(P(F)\) when \(F(x)_i = (m - 1)x_i \mod m\)

Proof: For \(F^2(x)_i = (m - 1)^2x_i \mod m\)

But \((m - 1)^2 \equiv 1 \mod m\) as \(m\) divides \((m - 1)^2 - 1\).

So \(F^2(x)_i = x_i \mod m\).

Every sequence in \(A^Z\) is of period 2 except zero sequence.

\[ \text{Per}(F) = \{1, 2\}, \]

\[ P(F) = A^Z \]

Example: For \(A = \{0, 1, 2, 3\} \mod 4\)

Define function as \(F(x)_i = 3x_i \mod 4\)

Then \(F^2(x)_i = x_i \mod 4\) as \(3^2 = 1 \mod 4\)

Theorem 3: Finding \(\text{Per}(F)\) and \(P(F)\) when \(F(x)_i = (m - 1)x_i \mod m\) and \(m\) is a prime number.

Proof: We know that by Wilson theorem [see 9], \(m\) is a prime number iff \((m - 1)\)! \(-1\) \(\mod m\).

Then the \(F(x)_i = (m - 1)!x_i \mod (m)\)

\[ = (-1)x_i \mod (m) \]

Then this is like the theorem (2) we get \(F^2(x)_i = x_i \mod m\).

\[ \text{Per}(F) = \{1, 2\}, \]

\[ P(F) = A^Z \]

Example: For \(A = \{0, 1, 2, 3, 4, 5, \ldots, 96\} \mod 96\)

Define function as \(F(x)_i = 96!x_i \mod 96\)

As 97 is prime by the Wilson theorem \(96! = -1\) \(\mod 97\)

So \(F^2(x)_i = (-1)^2(x)_i = x_i \mod 96\)

\[ \text{Per}(F) = \{1, 2\}, \]

\[ P(F) = A^Z \]
Theorem 4: Finding $\text{Per}(F)$ and $P(F)$, when $F(x)_i = ax_i \mod (m)$ and $a$ and $m$ are not relatively prime.

Proof: As specified in [see 1], if $m$ is a prime then $a^{m-1} \equiv 1 \mod (m)$ and if $a$ and $m$ are relatively prime then $a^{\varphi(m)} \equiv 1 \mod (m)$ by Euler's theorem in number theory. [see 9].

Gallian 2010 suggested that, where $\varphi(m)$ is Euler function and which denotes number of natural numbers less than $m$ and co prime to $m$ [see 9].

Consider $a \not\equiv 1 \pmod {m}$. Otherwise, it is an identity map that we can solve by theorem (1).

But here given that GCD of $a$ and $m$ not equal to 1.

For every natural number $n$ we get $a^n \not\equiv 1 \pmod {m}$.

We will not get any other periodic point other than $0$.

Then

$\text{Per}(F) = \{1\}$,

$P(F) = \{0 \in \mathbb{Z}: 0 = \ldots 0000000 \ldots \}$.

Example: $A = \{0, 1, 2, 3, 4, 5\} \mod (6)$

Define $F(x)_i = 3x_i \mod (6)$.

Here $3$ and $6$ are not $1$ so for every natural number $n$, $3^n \not\equiv 1 \pmod {6}$.

So other than $0$, we will not get any periodic sequence.

$\text{Per}(F) = \{1\}$,

$P(F) = \{0 \in \mathbb{Z}: 0 = \ldots 0000000 \ldots \}$.

Theorem 5: Finding $\text{Per}(F)$ and $P(F)$, when $F(x)_i = ax_{i+1} \mod (m)$.

Proof: We prove it by several cases.

Case 1: If $m$ is prime then $a^{\varphi(m)} \equiv 1$ by Fermat theorem [see 9].

$a^{m-1} \equiv 1 \pmod {m}$.

If $m$ is a prime then $\varphi(m) = m - 1$ as every natural less than $m$ is coprime to it.

So $P^m = \{1, (m-1), \ldots \} \mod (m)$.

To get periodic point in the sequence $x \in \mathbb{Z}$, $x = x_1x_2\ldots x_{m-1} \ldots \{\frac{x}{m}\} \ldots$ repeated $m - 1$ symbols from $A$.

$\text{Per}(F) = \{1, m-1\}$,

$P(F) = \{x \in \mathbb{Z}: x = \frac{x}{m}\}$.

Case 2: If GCD of $a$ and $m$ is 1.

Then $\varphi(m) \equiv 1 \pmod {m}$.

Here the periodic points are $\varphi(m)$ repeated symbols from $A$.

$\text{Per}(F) = \{1, \varphi(m)\}$,

$P(F) = \{x \in \mathbb{Z}: x = \frac{x}{m}\}$.

Theorem 6: Finding $\text{Per}(F)$ and $P(F)$, when $F(x)_i = ax_{i+2} \mod (m)$.

Proof: It is similar to theorem (5) but shifts left side one unit.

We prove it by several cases.

Case 1: If $m$ is prime then $a^{\varphi(m)} \equiv 1 \pmod {m}$.

$a^{m-1} \equiv 1 \pmod {m}$.

If $m$ is a prime then $\varphi(m) = m - 1$ as every natural less than $m$ is coprime to it.

So $P^m = \{1, (m-1), \ldots \} \mod (m)$.

To get periodic point in the sequence $x \in \mathbb{Z}$, $x = x_1x_2\ldots x_{m-1} \ldots \{\frac{x}{m}\} \ldots$ repeated $m - 1$ symbols from $A$.

$\text{Per}(F) = \{1, m-1\}$,

$P(F) = \{x \in \mathbb{Z}: x = \frac{x}{m}\}$.

Case 2: If GCD of $a$ and $m$ is 1.

Then $\varphi(m) \equiv 1 \pmod {m}$.

Here the periodic points are $\varphi(m)$ repeated symbols from $A$.

$\text{Per}(F) = \{1, \varphi(m)\}$,

$P(F) = \{x \in \mathbb{Z}: x = \frac{x}{m}\}$.

Theorem 7: Finding $\text{Per}(F)$ and $P(F)$, when $F(x)_i = (\frac{x}{a})_i \mod (m)$.

Proof: It is similar to theorem (5) but shifts left side one unit.

We prove it by several cases.

Case 1: If $m$ is prime then $a^{\varphi(m)} \equiv 1 \pmod {m}$.

$a^{m-1} \equiv 1 \pmod {m}$.

If $m$ is a prime then $\varphi(m) = m - 1$ as every natural less than $m$ is coprime to it.

So $P^m = \{1, (m-1), \ldots \} \mod (m)$.

To get periodic point in the sequence $x \in \mathbb{Z}$, $x = x_1x_2\ldots x_{m-1} \ldots \{\frac{x}{m}\} \ldots$ repeated $m - 1$ symbols from $A$.

$\text{Per}(F) = \{1, m-1\}$,

$P(F) = \{x \in \mathbb{Z}: x = \frac{x}{m}\}$.

Case 2: If GCD of $a$ and $m$ is 1.

Then $\varphi(m) \equiv 1 \pmod {m}$.

Here the periodic points are $\varphi(m)$ repeated symbols from $A$.

$\text{Per}(F) = \{1, \varphi(m)\}$,

$P(F) = \{x \in \mathbb{Z}: x = \frac{x}{m}\}$.

Theorem 8: Finding $\text{Per}(F)$ and $P(F)$, when $F(x)_i = (\frac{x}{a})_{i+1} \mod (m)$.

Proof: It is similar to theorem (5) but shifts left side one unit.

We prove it by several cases.

Case 1: If $m$ is prime then $a^{\varphi(m)} \equiv 1 \pmod {m}$.

$a^{m-1} \equiv 1 \pmod {m}$.

If $m$ is a prime then $\varphi(m) = m - 1$ as every natural less than $m$ is coprime to it.

So $P^m = \{1, (m-1), \ldots \} \mod (m)$.

To get periodic point in the sequence $x \in \mathbb{Z}$, $x = x_1x_2\ldots x_{m-1} \ldots \{\frac{x}{m}\} \ldots$ repeated $m - 1$ symbols from $A$.

$\text{Per}(F) = \{1, m-1\}$,

$P(F) = \{x \in \mathbb{Z}: x = \frac{x}{m}\}$.

Case 2: If GCD of $a$ and $m$ is 1.

Then $\varphi(m) \equiv 1 \pmod {m}$.

Here the periodic points are $\varphi(m)$ repeated symbols from $A$.

$\text{Per}(F) = \{1, \varphi(m)\}$,

$P(F) = \{x \in \mathbb{Z}: x = \frac{x}{m}\}$.

Summary

In this paper we characterised the periods and periodic points of additive cellular automata in the form of equation (3) and came to know that cardinality of set of periods is maximum 2.

References


