*Fundamenta Informaticae XXI (2001) 1001–1021*
*IOS Press*


# Theory of Additive Cellular Automata

**Niloy Ganguly**

*Department of Computer Science and Engineering, Indian Institute of Technology, Waragpur, India*

**Biplab K Sikdar**

*Department of Computer Science & Technology, Bengal Engineering College (DU), Botanic Garden, Howrah,West Bengal, India*

**P Pal Chaudhuri**

*Flat E4, Block H30, BP Township, Calcutta - 700 094. India.*

**Abstract.** This paper reports the complete characterization of additive cellular automata ($ACA$) that employ $xor$ and $xnor$ logic as the next state function. Compared to linear cellular automata ($LCA$) [3], which employs only $xor$ logic in its next state function, an $ACA$ display much wider varieties of state transition behavior and enhanced computing power. An analytical framework is developed to characterize the cyclic vector subspaces generated by an $ACA$ with reference to $LCA$. It identifies the conditions on which the state transition behavior of an $ACA$ differs from that of the corresponding $LCA$ and also provides the theoretical analysis of the nature of difference.

## I. Introduction

*This work develops the theory of additive cellular automata ($ACA$). The theoretical framework proposed, provides the complete characterization of the cyclic state space generated by an $ACA$. An $ACA$ is additive in the sense that it employs affine (also referred to as additive) transformation rather than a linear transformation implemented in a typical linear cellular automata ($LCA$). The theory of $LCA$ provides the foundation of the proposed characterization of $ACA$.*

$ACA$ which employ $xor$ and $xnor$ logic to generate its next state function has been specially popular among researchers. Both $ACA$ and its subset $LCA$ (which employ only $xor$ logic) have been used to develop a lot of applications in $VLSI$ and related fields. They have been used to develop pseudo-random

Address for correspondence:
Department of Computer Science and Engineering,
Indian Institute of Technology,
Kharagpur, India 721302

test pattern generators [18, 19], signature analyzers [6], finite state machines $FSM$ [1], error correcting codes [5] etc. Moreover, researchers have designed $CA$ based cipher system[15], message authenticators [9], $CA$ based pattern classifier [11] with the help of $ACA$. In the process of developing the applications, there has been several works to characterize the state transition behavior of both $LCA$ and $ACA$.

The analysis of linear $CA$, has been extensively investigated by Stone [21] as part of the exploration of linear machine. Vector space theoretic analysis of state transition behavior of this class of $CA$ has been reported by Das [8] and subsequently by a number of researchers [3, 6, 11]. The partial characterization of $ACA$, that employs both the $xor$ and $xnor$ logic in its next state function, has been introduced in [3, 15]. However, complete characterization of the cyclic state space generated by such a $CA$ remains untouched.

In this background, this paper reports a complete vector space theoretic analysis of $ACA$. We develop an elegant solution to derive its cycle structure from analysis of the given rules, defining the $ACA$. An $ACA$ can have both the cyclic and non-cyclic state space. However, in the current work, we only consider the characterization of cyclic state space as the non-cyclic subspace generated by an $ACA$ is isomorphic to that of $LCA$ [3].

We next provide a brief introduction to additive $CA$ along with some important results on linear $CA$ that are relevant for the characterization of $ACA$ in *section III*. The vector space theoretic analysis targeting complete characterization of $ACA$, is reported in *section III*.

## II. Cellular Automata Characterization

Cellular Automata ($CA$) consist of a number of interconnected cells arranged spatially in a regular manner. In most general case, a $CA$ cell can exhibit $s$ different states and the next state of each cell depends on the present states of its $k$ neighbors including itself. Such a $CA$ is called an $s$-state $k$-neighborhood $CA$. However, Wolfram [12] worked with several features of finite $CA$ known as 3-neighborhood (left, right and self) $CA$ having 2 states for each cell. The state (next state) $q \in \{0,1\}$ of the $i^{th}$ cell at time $(t+1)$ is denoted as

$$q_i^{t+1} = f_i(q_{i-1}^t, q_i^t, q_{i+1}^t),$$

where $q_i^t$ denotes the state of the $i^{th}$ cell at time *t* and $f_i$ is the next state function called the rule of the automata [22]. Since *f* is a function of 3 variables, there are $2^{2^3}$ or 256 possible next state functions. The structure of a 3-neighborhood $CA$ cell is shown in ***Fig. 1***.

Out of total 256 $CA$ rules, 14 rules that can be realized by $xor/xnor$ logic are called additive rules [3]. A $CA$ designed with such rules are called additive $CA$ ($ACA$). The $ACA$ has been of special interest to researchers, as it can be characterized by matrix algebraic tools. Matrix algebraic tools are used to represent $ACA$ *that uses different rules in different cells*. In the current work, we concentrate on characterizing such hybrid $CA$. A brief overview of this model is next outlined [3].

An $n$-cell 1-dimensional $ACA$ is characterized by a linear operator $[T]_{n\times n}$ matrix and an $n$-dimensional inversion vector $F$. $T$ is the *characteristic* matrix of the cellular automata. The $i^{th}$ row of $T$ corresponds to the neighborhood relation of the $i^{th}$ cell, where

$$T[i,j] = \begin{cases} 1, & \text{if the next state of the } i^{th} \text{ cell depends on the present state of the } j^{th} \text{ cell} \\ 0, & \text{otherwise.} \end{cases}$$

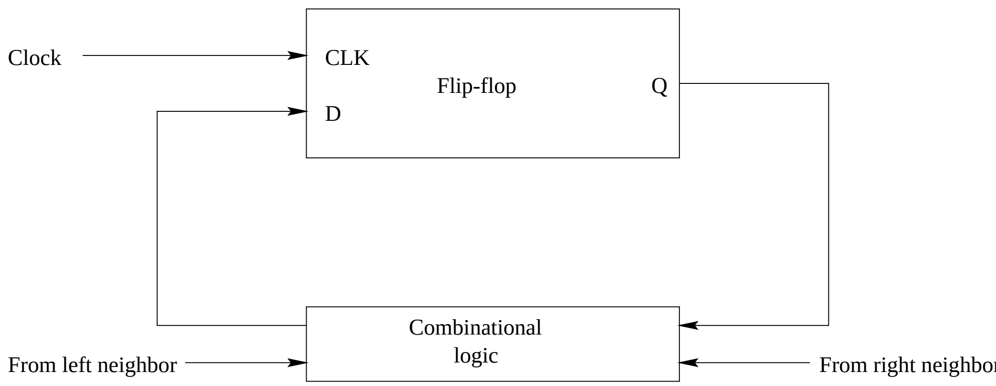


Figure 1. A 3-neighborhood $CA$ cell

Since the $CA$ is restricted to 3-neighborhood dependency, $T[i, j]$ can have non-zero values for $j$ = $(i-1)$, $i$, $(i+1)$. The inversion vector $F$ of an $ACA$ is defined as

$$F_i = \begin{cases} 1, & \text{if the next state of the } i^{th} \text{ cell results from inversion } (xnor) \\ 0, & \text{otherwise } (xor) \end{cases}$$

If $s_t$ represents the state of the $CA$ at the $t^{th}$ instant of time, then the next state - that is, the state at the $(t+1)^{th}$ time instant, is given by :

$$s_{(t+1)} = T \cdot s_t + F. \;\; Therefore, \quad s_{(t+p)} = T^p \cdot s_t + (I + T + T^2 + \cdots + T^{p-1})F, \tag{1}$$

where $s_{(t+p)}$ is the state of $CA$ at $(t+p)^{th}$ instant of time. For an $n$-cell $CA$, $F$ is the $n$ bit *inversion vector* with its $i^{th}$ $(0 \leq i \leq n-1)$ bit as 1, if $xnor$ rule is applied on the $i^{th}$ cell; whereas 0 implies $xor$ (linear) rules. The operators (**.**, **+**) follow the rules defined in binary arithmetic for multiplication and addition respectively.

As the $LCA$ is a special case of $ACA$, where the inversion vector $F$ is an all 0s vector, the next state function (eq. (1)) for the $LCA$ gets simplified to

$$s_{t+1} = T \cdot s_t \Rightarrow s_{t+p} = T^p \cdot s_t \tag{2}$$

The state transition eqs. (1) and (2) results in some global state transition behavior of the $CA$ on the basis of which we can classify $CA$[1] into two categories - group and non-group $CA$.

## II.1. Group and non-group $CA$

A $CA$ that generates only cyclic states during its state transitions is known as *group* $CA$, whereas a $CA$ generating both cyclic and non-cyclic subspaces is the *non-group* $CA$. The state transition diagram of an $ACA$ can be characterized from its $T$ matrix and the inversion vector $F$. However, the characteristic matrix ($T$) can directly determine whether the $CA$ is a group or non-group $CA$ -

$$\begin{aligned} if \;\; det(T) &= 1, \text{ the } CA \text{ is a group } CA \\ &= 0, \text{ the } CA \text{ is a non group } CA \end{aligned}$$

[1]Henceforth, unless otherwise mentioned, the term $ACA$ and $CA$ are synonymously used.

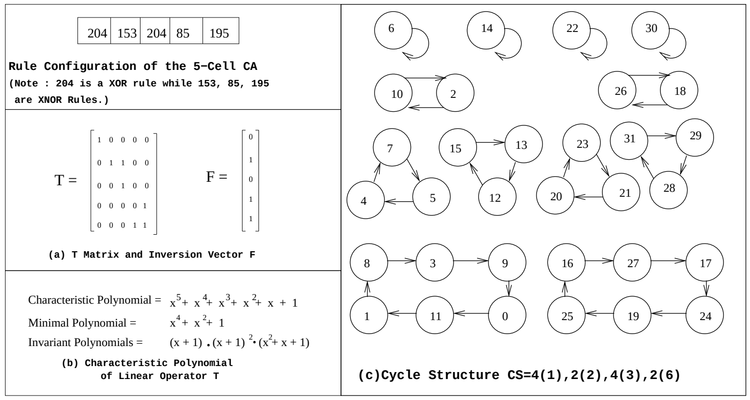


Figure 2. A 5-cell group $CA$ and its cycle structure [4(1),2(2),4(3),2(6)]
Note : The $LCA$ formed from the $T$ matrix also have the same cycle structure CS = [4(1),2(2),4(3),2(6)]

**Group CA** : For a group $CA$ (*Fig. 2*), each $CA$ state has a unique predecessor. That is, all the states lie on a disjoint set of cycles. The state transition behavior of a group $CA$ is represented by the cycle structure (CS) = $[\mu_{k_1}(k_1), \mu_{k_2}(k_2), \cdots \mu_{k_m}(k_m)]$, where $k_i$ is the cycle length of the $i^{th}$ cyclic component of $CS$ and $\mu_{k_i}$ is the number of such components. *Fig. 2(c)* illustrates the cycle structure of the 5-cell group $CA$. It has 4 cycles of length 1, 2 cycles of length 2, 3 cycles of length 3 and 2 cycles of length 6. The complete cycle structure is denoted as $CS$ = [4(1), 2(2), 4(3), 2(6)].
**Problem Definition :-** tackled in this paper. In this work, we analytically compute the $CS = [\mu_{k_1}(k_1), \mu_{k_2}(k_2), \cdot\cdot\cdot\mu_{k_m}(k_m)]$ from a given additive $CA$ - that is from a $T$ matrix and the $F$ vector. Computation of $CS$ for a linear $CA$ has been widely studied [3, 6, 7, 20]. We consider those studies as the base while formulating our proposed scheme.

The reported analysis show that the cycle structure of $LCA$ and $ACA$ follows some definite relation and can be divided into two distinct categories - (1) The cycle structure repeated and not the sequence of $LCA$ and $ACA$ are identical (*Fig. 2*); (2) The cycle structure of $LCA$ and $ACA$ are different (*Fig. 3*). Details of these two aspects are reported in *section III*.

Scheme to analyze cycle structure for $LCA$ has been developed with the underlying concept of characteristic polynomial, minimal polynomial and invariant polynomials.
*Characteristic polynomial :* The characteristic polynomial $f(x)$ of a $CA$ is det$(T + Ix)$, where $T$ is the characteristic matrix.
*Minimal polynomial:* The minimal polynomial is the minimum degree polynomial which annihilates $T$.
*Invariant polynomials (IP):* The characteristic polynomial $f(x)$ comprises of polynomials $\phi_i(x)^{n_i}$ invariant to the linear operator $T$, where $\phi_i(x)$ is irreducible.

The example $CA$ of *Fig. 2* illustrates $T$, its characteristic polynomial, minimal polynomial and the invariant polynomials.

If the characteristic polynomial $f(x)$ of a $CA$ is expressed as a product of its invariant polynomials ($IP$), then

$$f(x) = x^{n_1} \cdot x^{n_2} \cdot \cdot x^{n_l} \phi_{l+1}(x)^{n_{l+1}} \cdot \cdot \phi_{\mathcal{N}}(x)^{n_{\mathcal{N}}}$$

where $\phi_i(x)$ is irreducible ($i$ = 1,2,$\cdot\cdot\cdot$,$\mathcal{N}$). The number of $IP$ comprising the characteristic polynomial is denoted by $\mathcal{N}$. A factor $x^{n_i}$ ($i$ = 1,2,$\cdots$, $l$), ($l \leq \mathcal{N}$), of $f(x)$ represents a non-cyclic subspace whereas $\phi_i(x)^{n_i}$ corresponds to a cyclic subspace. For a group $CA$, there is not a single $x^{n_i}$ components in $f(x)$. That is, for a group $CA$, the characteristic polynomial is

$$f(x) = \phi_1(x)^{n_1}\phi_2(x)^{n_2} \cdots \phi_{\mathcal{N}}(x)^{n_{\mathcal{N}}} \tag{3}$$

The characterization of $LCA$ state transition behavior is reported in [2, 3, 4, 6, 13, 14]. Some of the fundamental results reported in [3] and [20] are noted below. These results are important while building the analysis scheme for additive $CA$, described in *section III*.

## II.2. Vector Space Theoretic Analysis of $LCA$

The following theorem, noted from [20], is one of the fundamental results reported for the $LCA$.

**Theorem 1.** The cycle structure of an $LCA$ can be represented as

$$CS = [1(1) + \sum_{k_i} \sum_{j=0}^{m_{k_i}} \mu_{2^j \cdot k_i}(2^j \cdot k_i)] \tag{4}$$

where $k_i$ is odd.

**Example 1.** The cycle structure of the $LCA$ noted in *Fig. 2* is $CS$ = [4(1), 2(2), 4(3), 2(6)]. We can also represent it as $CS$ = [1(1), [3(1), 2(2)], [4(3), 2(6)]]. Here $k_i$s, the odd cycles, are 1 and 3. Corresponding to each odd cycle ($k_i$), there is a cycle of length $2^j \cdot k_i$, in this case, $j$ = 1 for both the odd cycles 1 and 3.

The above discussion demands definition of the following terminologies - primary cycles, secondary cycles and cycle family that are essential for the analysis of cycle structure of a $CA$.

**Definition 1.** Primary and secondary cycles : Each odd cycle ($k_i$) in the cycle structure is referred to as a primary cycle and the cycles which are of the form $2^j \cdot k_i$ ($j \geq 1$) are referred to as secondary cycles.

**Definition 2.** $k$ cycle family : All the cycles of the form $2^j \cdot k$ ($j \geq 0$), where $k$ is the length of a primary cycle, are the member of a family of cycles referred to as $k$-cycle family. It is also referred to as primary cycle family.

The basic scheme for extracting the cycle structure of an $LCA$ from its characteristic matrix $T$ has been reported in [20]. Further, a more efficient and compact algorithm is presented in [11]. The execution steps of the algorithm are next illustrated through an example.

**Example 2.** Let the T matrix of a 5-cell $LCA$ is

$$T = \begin{pmatrix} [1] & 0 & 0 & 0 & 0 \\ 0 & \lceil 1 & 1 \rceil & 0 & 0 \\ 0 & \lfloor 0 & 1 \rfloor & 0 & 0 \\ 0 & 0 & 0 & \lceil 0 & 1 \rceil \\ 0 & 0 & 0 & \lfloor 1 & 1 \rfloor \end{pmatrix}$$

The following steps are to be executed to find the cycle structure of the $LCA$ from its $T$ matrix.
Step 1 : Find out the characteristic polynomial the $CA$, illustrating each invariant polynomial separately. For the example $CA$, it is $(x+1)(x+1)^2(x^2+x+1)$.
Step 2 : Find out the cycle structure for each of the invariant polynomials. For the current example, these are

$$CS_{LCA(x+1)} = [1(1), 1(1)],\ \ CS_{LCA(x+1)^2} = [1(1), 1(1), 1(2)],\ \ CS_{LCA(x^2+x+1)} = [1(1), 1(3)]$$

Step 3 : Enumerate the complete cycle structure of the $CA$ by successively performing cross product of cycle structures generated by each invariant polynomial [20]. Therefore, the example $CA$ has the following cycle structure

$$CS_{LCA} = [1(1), 1(1)] \times [1(1), 1(1), 1(2)] \times [1(1), 1(3)] = [4(1), 2(2), 4(3), 2(6)].$$

where $\times$ represents the cross product operation and is defined as

**Definition 3.** Cross Product ($\times$) of two cycle structures $CS_1$ and $CS_2$, where

$$CS_1 = [1(1) + \sum_{i_1=1}^{m_{k_{i_1}}} \mu_{k_{1i_1}}(k_{1i_1})]\ \ and\ \ CS_2 = [1(1) + \sum_{i_2=1}^{m_{k_{i_2}}} \mu_{k_{1i_2}}(k_{1i_2})],$$

is the product of each ${i_1}^{th}$ term of $CS_1$ and the ${i_2}^{th}$ term of $CS_2$. The product of $\mu_{k_{1i_1}}(k_{1i_1})$ and $\mu_{k_{2i_2}}(k_{2i_2})$ results in the cyclic component $\mu_k$ of length $k$ following the equations [20]

$$\mu_k = \mu_{k_{1i_1}}.\mu_{k_{2i_2}}.gcd(k_{1i_1}, k_{2i_2})\ \ and\ \ k = lcm(k_{1i_1}, k_{2i_2}) \tag{5}$$

Based on the results provided in this section, we report detail analysis of the state transition behavior of $ACA$ that follows.

## III. Vector Space Theoretic Analysis of Additive $CA$

Complete characterization of the state transition behavior of an $ACA$ is reported in this section. An $ACA$, as noted in *section II*, is represented by the characteristic matrix $T$ and the non-zero inversion vector $F$. The $ACA$ generates more varieties of cycle structure than that of linear $CA$ ($LCA$). *Fig. 3* gives a typical example of cycle structure generated by $ACA$ which is not available from an $LCA$. This section also highlights the variation of $ACA$ cycle structure with that of its linear counterpart.

An $ACA$ - $C'$ is a group $CA$ iff its linear counterpart $C$ (represented by the same characteristic matrix $T$ of $C'$ with all 0s $F$ Vector) is a group $CA$ [3]. It signifies that the cycle structure of an $ACA$ can be figured out from the analysis of state transition behavior of the corresponding $LCA$. Moreover, the concept of null space and its relationship with cycle length of an $LCA$ is necessary for further analysis of cycle structure of $ACA$. These are reproduced from [10, 17].

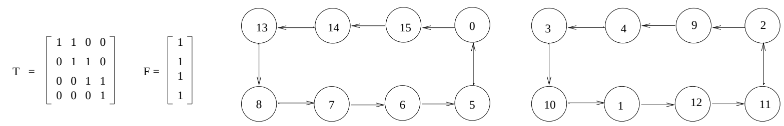


Figure 3. Additive $CA$ and its state transition behavior. The cycle structure is $CS'$ = 2(8). The cycle structure of the corresponding $LCA$ is $CS$ = [2(1), 1(2), 3(4)]

**Definition 4.** Null space : The null space of a matrix ($T$) consists of all such vectors that are transformed to the all-zero vector when premultiplied by the matrix.

**Theorem III.1.** [16] If an $LCA$ represented by $T$ has a cycle of length $k$, then the cardinality of the null space of ($T^k$ + I) denotes the number of states forming cycles of length $k$ or sub-multiple of $k$.

**Theorem III.2.** [10] If an $LCA$ is represented by $T$ and for any state $\chi \neq 0$, $g(T) \cdot \chi = 0$, then $g(x)$ and the characteristic polynomial $f(x)$ have some common factor $h(x)$.

The analysis of $ACA$ state transition behavior is done with the solutions of following issues :

A. To check whether a particular cycle length $(k)$ is present in the cycle structure of an $ACA$.

B. To find the special class of $ACA$ ($C'$) having the cycle structure as that of its linear counterpart $C$ irrespective of its inversion vector $F$.

C. To identify the class of $C'$ whose cycle structure differs from that of $C$, and the properties of $F$ vectors which impart this difference.

D. To enumerate the cycle structure and depth of $C'$.

The following subsections report the analysis and results of above four issues.

## III.1. Identification of a cycle of length ($k$) in $ACA$ cycle structure

The following theorem enables us to determine whether a cycle of length $k$ exists in an $ACA$ or not.

**Theorem 2.** *[16]* In an $ACA$ with characteristic matrix $T$ and the inversion vector $F$, a cycle of length $k$ exists if

$$rank([T^k + I]) = rank([T^k + I, \mathcal{F}]),\ where\ \mathcal{F} = [I + T + T^2 + \cdots + T^{k-1}]F$$

**Proof:**
Let $\chi$ be a state in a cycle of length $k$ in an $ACA$ $C'$. Hence, as per eq. (1) in *section II*,

$$\chi = [I + T + T^2 + \cdots + T^{k-1}]F + T^k \cdot \chi$$

It can be written as

$$[T^k + I] \cdot \chi = \mathcal{F},\ where\ \mathcal{F} = [I + T + T^2 + \cdots + T^{k-1}]F \quad (6)$$

If a cycle of length $k$ is to exist in $C'$, eq. (6) should be consistent. The condition for consistency is

$$rank([T^k + I]) = rank([T^k + I, \mathcal{F}]) \tag{7}$$

Hence the proof. □

## III.2. Class of $ACA$ with the cycle structure identical to corresponding linear $CA$

*Theorem 2* is utilized to explore a special class of $C'$ ($ACA$) that has cycle structure identical to that of $C$ ($LCA$) irrespective of the inversion vector $F$. The following theorem defines such a class of $C'$.

**Theorem 3.** The cycle structures of $C'$ ($ACA$) and $C$ ($LCA$) are identical if the characteristic polynomial $f(x)$ of the $T$ matrix does not have a factor $(x + 1)$.

**Proof:**
Let $k$ be the length of a cycle of the linear $CA$ - $C$ with characteristic matrix $T$; characteristic polynomial $f(x)$ of which does not have a factor ($x$ + 1). To have a cycle of length $k$ in the corresponding $ACA$ - $C'$, eq. (7) has to be satisfied.
The number of vectors, forming a cycle of length $k$ or sub-multiple of $k$, in the $ACA/LCA$ are derived from the enumeration of *null space* of $\alpha_1 = (T^k + I)$ [17].
Let ($x^k$ + 1) = $g(x) \cdot \phi_c(x)$; $\phi_c(x)$ is the largest factor of the characteristic polynomial $f(x)$ that divides $(x^k + 1)$. Therefore $g(x)$ and $f(x)$ don't have any common factor. Hence for each state $\chi$, where $(T^k + I) \cdot \chi$ = 0, there is a corresponding unique state $\tilde{\chi}$, where $\phi_c(T) \cdot \tilde{\chi}$ = 0 (from *theorem III.2*). Hence, the cardinality of null space of $\alpha_2$ = $\phi_c(T)$ is same as $\alpha_1$.
Since $f(x)$ does not have a factor $(x + 1)$ and $x^k + 1$ = $(x + 1) \cdot (1 + x + x^2 + \cdots + x^{k-1})$, therefore similarly the cardinality of the null space of $\alpha_3 = [I + T + T^2 \cdots T^{k-1}]$ = $\alpha_1$ = $\alpha_2$ . Hence,

$$rank(T^k + I) = rank(T^k + I, I + T + T^2 \cdots T^{k-1})$$

that is,

$$rank(T^k + I) = rank(T^k + I, \mathcal{F})$$

directly follows for any $F$.

Therefore, all the cycle lengths of $C$ also exist in $C'$. Since the number of vectors forming each cycle length is same for the both (directly derived from the cardinality of null space), the cycle structures for both the $CA$ are identical. Hence the proof. □

The following example illustrates the result of *theorem 3*.

**Example 3.** Let consider a 5-cell $ACA$ with characteristic matrix $T$ and the inversion vector $F \neq 0$, where

$$T = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The characteristic polynomial of $T$ is $(x^3+x+1)(x^2+x+1)$. The cycle structure of the corresponding $LCA$ is [1(1),1(3),1(7),1(21)]. The $ACA$, as per *theorem 3*, has the identical cycle structure as that of the $LCA$, irrespective of $F$.

Let us consider a particular cycle of length 7. As per the theorem, we enumerate $\alpha_1 = T^7 + I$, $\alpha_2 = T^3 + T + 1$ and $\alpha_3 = T^6 + T^5 + T^4 + T^3 + T^2 + T + I$, where

$$T^7 + I = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \qquad T^3 + T + 1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \text{ and}$$

$$T^6 + T^5 + T^4 + T^3 + T^2 + T + I = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

All the three matrices with $3^{rd}$, $4^{th}$ & $5^{th}$ rows as all zeros, have cardinality of null space as 8. Therefore, rank($\alpha_1$) = rank($\alpha_2$,$\alpha_3$) and rank($\alpha_1$) = rank($\alpha_2$,$\mathcal{F}$); $\mathcal{F}$=$(I + T + T^2 + T^3 + T^4 + T^5 + T^6) \cdot F$. That is, both the $C'$ and $C$ have cycles of length 7. The number of states having cycle length 7 or submultiple of 7 (here it is 1) is 8. Therefore, the $CA$ cyclic components of cycle length 7 = $\frac{(8-1)}{7}$ =1 (as one state forms a self loop). The complete cycle structure of $C^{'}$ can be shown as $CS'$ = [1(1), 1(3), 1(7), 1(21)], which is same as that of C.

## III.3. Class of $ACA$ with cycle structure different from that of $LCA$

From *theorem 3,* it is obvious that the cycle structure of the linear $CA$ - $C$ and the $ACA$ - $C'$ can differ only if the characteristic polynomial of the $CA$ has a factor of $(x+1)$. The study of the role of $(x+1)$ factor helps identification of the class of $ACA$ for which the cycle structure differs from that of the corresponding $LCA$. Let us concentrate on the $LCA/ACA$ having a single invariant polynomial as $(x+1)^n$. The generalization follows subsequently. The following terminologies are defined relating the cycle structure of $LCA$/$ACA$.

- $\mathbf{C(x+1)^n}$ : The $LCA$ with characteristic matrix $T$, the characteristic & minimal polynomial as $(x+1)^n$ has the cycle structure [3]

$$CS = [1(1) + \sum_{j=0}^{m} \mu_{2^j}(2^j)], \quad where\, m = \lceil log_2(n) \rceil, \tag{8}$$

$$rank\ of\ (T+I)\ =\ n-1,\ and\, rank\ of\ (T+I)^i\ =\ n-i. \tag{9}$$

The $C\phi(x)$ and $C'\phi(x)$ represent the $LCA$ and $ACA$ respectively with characteristic polynomial $\phi(x)$.

- $[\mathbf{F^k}]$ : The set of inversion vectors which annihilates only $(x+1)^k$ - that is,

$$(T+I)^k \cdot \chi = 0,\ where\ (T+I)^{k'} \cdot \chi \neq 0\ and\ k' < k\ \&\ \chi \in [F^k]. \tag{10}$$

- $\mathbf{Car}[\mathbf{F^k}]$ : Cardinality of the set $F^k$.

Based on the results of the *theorem 2*, we next identify the condition responsible for the difference in cycle structure of $C(x+1)^n$ and $C'(x+1)^n$.

**Theorem 4.** The $ACA\ C'(x+1)^n$, characterized by $T$ and the inversion vector $F$, and $LCA\ C(x+1)^n$ have the identical cycle structure if

$$rank(T+I) = rank((T+I), F) \tag{11}$$

**Proof:**
In order to test whether the cycle structure of $LCA\ C(x+1)^n$ and $ACA\ C'(x+1)^n$ are identical, the consistency of eq. (6) is checked for the existence of a cycle of length $k$ in $C'$. The $LCA\ C$ has cycle(s) of length $k$, where from eq. (8),

$$k = 2^j, \quad j = (0, 1, 2, \cdots, m), \ \ m \ = \ \lceil log_2(n) \rceil.$$

Since the cycle length ($k$) of $C(x+1)^n$ is of the form $2^j$, the relation for consistency (eq. (6)) can be rewritten as

$$(T^{2^j} + I) \cdot \chi = (I + T + T^2 + \cdots + T^{2^j - 1})F \tag{12}$$

where $j$ = (0, 1, 2, $\cdots$, $m$) and $m$ = $\lceil log_2(n) \rceil$. The relation has to be consistent $\forall\ j$ to establish the equivalence of cycle structures of $C\ \&\ C'$. Since

$$(T^{2^j} + I) = (T+I)^{2^j}\ and\ (I + T + T^2 + \cdots + T^{2^j - 1}) = (T+I)^{2^j - 1},$$

eq. (12) can be rewritten as

$$(T+I)^{2^j} \cdot \chi = (T+I)^{2^j - 1} F \Rightarrow (T+I)^{2^j - 1}[(T+I) \cdot \chi = F] \tag{13}$$

It implies

$$(T+I) \cdot \chi = F \tag{14}$$

is to be consistent. That is, it should satisfy rank($T$ + $I$) = rank(($T$ + $I$), $F$).
Hence the proof. □

Eq. (11) characterizes the $F$ vector responsible for imparting the difference in cycle structure between $LCA$ and $ACA$. The following theorem notes the characterization of $F$ vectors.

**Theorem 5.** The cycle structure of $ACA\ C'(x+1)^n$ differs from that of its linear counterpart $C(x+1)^n$ if and only if the inversion vector $F$ of $ACA \in [F^n]$.

**Proof:**
In order to prove the theorem, the consistency of eq. (14) is checked for inversion vector (1) $F \in [F^{n'}]$, where $n' < n$, and (2) $F \in [F^n]$.

Comment: The proof establishes the fact that in the first case both $C$ and $C'$ have the same cycle structure while in the second case the cycle structure of $C'$ differs from that of $C$. The proof is established by checking consistency for every cycle length ($k$ = $2^j$, $j$ = $\{0,1,2,\cdots,m\}$)

*Case 1: Inversion vector $F \in [F^{n'}]$, where $n' < n$.* We show that eq. 14 (($T$ + $I$) $\cdot$ $\chi$ = $F$) is consistent iff $\chi \in [F^{n'+1}]$.
If $\chi \in [F^{n'+1}]$, then

$$(T+I)^{n'+1} \cdot \chi = 0 \Rightarrow (T+I)^{n'} \cdot [(T+I) \cdot \chi] = 0 \tag{15}$$

As per the definition of $[F^{n'+1}]$ (noted in page 1010), the constituent vectors become zero only when premultiplied by $(T+I)^{n'+1}$ and higher factors. Therefore, $(T+I) \cdot \chi \neq 0$ and the vector $y$ is formed by enumerating the equation

$$(T+I) \cdot \chi = y \tag{16}$$

Moreover, eq. (15) can be rewritten as

$$(T+I)^{n'} \cdot y = 0 \quad \Rightarrow \quad y \in [F^{n'}] \quad i.e. \quad (T+I)^{n''} \cdot y \neq 0 \quad n'' < n \tag{17}$$

Since rank of ($T + I$) is ($n$ -1), $\chi_i$ ( $i$ = 1, 2 and $\chi_1$, $\chi_2 \in [F^{n'+1}]$), while premultiplied with ($T + I$) generates the same $y$ in eq. (16). That is,

$$(T+I) \cdot \chi_1 = (T+I) \cdot \chi_2 = y$$

Hence, exploiting the all possible pairs of $\chi$, we obtain the set of $y$ having cardinality $\frac{Car(F^{n'+1})}{2}$, where the cardinality of $[F^{n'+1}]$ is denoted as Car($F^{n'+1}$).
Since rank of $(T+I)^{n'+1}$ is one less than that of $(T+I)^{n'}$ (eq. (9)), therefore

$$Car(F^{n'+1}) = 2 \times Car(F^{n'})$$

Therefore, $Car(y) = Car(F^{n'})$ - that is, the full set of ($F^{n'}$) is represented by $y$. It implies, the relation

$$(T+I) \cdot \chi = F$$

is consistent for all values of $F \in [F^{n'}]$ and consequently, eq. (13) is consistent for all $F \in [F^{n'}]$, $n' < n$.
*Case 2* : *Checking consistency of cycle length for $ACA$ $C'(x+1)^n$ with inversion vector $F \in [F^n]$* : In this case, it is shown that eq. (14) is inconsistent for all cycle length $2^j \leq n$. Multiplying either side of eq. (14) with $(T+I)^{n-1}$ we obtain

$$(T+I)^n \chi = (T+I)^{n-1} F. \tag{18}$$

It is inconsistent since the $left\ hand\ side\ (LHS) = 0$ while $right\ hand\ side\ (RHS) \neq 0$. □

*Theorem 5* leads to the following corollary that specifies the cycle structure of $C'(x+1)^n$.

**Corollary III.1.** The cycle structure of $C'(x+1)^n$ with $F \in F^n$ is

$$CS' = \mu'(2^{\mathcal{M}}); \quad \mu' = 2^{n-\mathcal{M}} \quad and \quad \mathcal{M} = \lfloor log_2(n) \rfloor + 1 \tag{19}$$

where the cycle structure of $C(x+1)$ (eq. (8), page 1009) is

$$CS = [1(1) + \sum_{j=0}^{m} \mu_{2^j}(2^j)] \quad where\ m = \lceil log_2(n) \rceil.$$

**Proof:**
Since the characteristic and minimal polynomial of $C$ is $(x+1)^n$ - that is, $(T+I)^n$ is always = 0. Therefore, eq. (14) becomes consistent ($LHS$ = $RHS$ = 0), when we premultiply both sides by $(T+I)^n$. Consequently, eq. (13) is consistent if $2^j - 1 \geq n$ - that is, cycles of length $2^j$ exist in $C'$ if $2^j - 1 \geq n$. The minimum value of $j$ for which the equation becomes consistent is represented by $\mathcal{M}$, where $2^{\mathcal{M}-1} \leq n < 2^{\mathcal{M}}$.

1. If $n = 2^{\lceil log_2 n \rceil}$, then $n$ is of the form $2^j$; where $j$ is an integer. Therefore, $\lceil log_2 n \rceil$ = $\lfloor log_2 n \rfloor$ = $log_2 n$. In that case, $\mathcal{M}$= $\lfloor log_2 n \rfloor$ +1.

2. If $n < 2^{\lceil log_2 n \rceil}$, then $\mathcal{M} = \lceil log_2 n \rceil$ = $\lfloor log_2 n \rfloor$ +1.

Considering (1) and (2), it can be found that $\mathcal{M}$ = $\lfloor log_2 n \rfloor$ +1.

Since all the states fall in the null space of $(T+I)^{2^{\mathcal{M}}}$, as per *theorem III.1*, the $ACA$ can have cycles only of length $2^{\mathcal{M}}$ and the number of cyclic components ($\mu'$) is $2^n/2^{\mathcal{M}}$ = $2^{n-\mathcal{M}}$. □

The $\mathcal{M}$ is denoted as the *minimum additive factor*. The following example illustrates the results of *theorem 5* and *corollary III.1*.

**Example 4.** Let us consider the following $T$ matrix and two inversion vectors $F_1$ and $F_2$ of the 4-cell $ACA$ -

$$T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \; F_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \; F_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$

The characteristic polynomial and minimal polynomial of the $T$ is $(x+1)^4$.
The cycle structure of the $LCA$ counterpart with characteristic matrix $T$ is $CS$ = [2(1),1(2),3(4)].
The inversion vector $F_1$ annihilates $(T+I)^4$. The $ACA$ with characteristic matrix $T$ and the inversion vector $F_1$ has the cycle structure [2(8)] (*Fig. 3*). However, $F_2$ cannot annihilate $(T+I)^4$. The $ACA$ with characteristic matrix $T$ and the inversion vector $F_2$ has its cycle structure $CS'$ identical to $CS$ generated by the $LCA$.

*Theorem 5* & *corollary III.1* can be extended to a more generalized class of $LCA/ACA$. As per *theorem 3*, it is noted that the cycle structure of $ACA$ - $C'$ can differ from $C$ only if the characteristic polynomial of $C/C'$ contains a factor of $(x+1)$. That is, the characteristic polynomial can be represented as

$$f(x) = (x+1)^{n_1} \cdot \cdot (x+1)^{n_l} \phi_{l+1}(x)^{n_{l+1}} \cdot \cdot \phi_{\mathcal{N}}(x)^{n_{\mathcal{N}}}$$

where (i) each $\phi_i(x)^{n_i}$ is an invariant polynomial and (ii) the irreducible factor of the first $l$ invariant polynomials is $(x+1)$. The following theorem states the nature of cycle structure of such $LCA$ and $ACA$.

**Theorem III.3.** The cycle structure of $LCA$, with characteristic matrix $T$ and a factor $(x+1)$ in the characteristic polynomial, is

$$CS = [1(1) + \sum_{k_i} \sum_{j=0}^{m_{k_i}} \mu_{2^j \cdot k_i}(2^j \cdot k_i)]; \quad k_1 = 1; \tag{20}$$

whereas the cycle structure of $ACA$, with the characteristic matrix $T$ & inversion vector $F$ and having the largest $(x+1)$-invariant polynomial annihilated by $F$ as $(x+1)^{n_i}$, is

$$CS' = \sum_{k_i} \sum_{j=\mathcal{M}}^{m_{k_i}} \mu'_{2^j \cdot k_i}(2^j \cdot k_i), \quad k_1 = 1 \tag{21}$$

where

$$\mu'_{2^{\mathcal{M}} \cdot k_i} = \begin{cases} \dfrac{\sum_{j=0}^{\mathcal{M}} (\mu_{2^j . k_i} \times 2^j \cdot k_i) + 1}{2^{\mathcal{M}} . k_i} & \text{for } k = 1 \\ \dfrac{\sum_{j=0}^{\mathcal{M}} \mu_{2^j \cdot k_i} \times 2^j \cdot k_i}{2^{\mathcal{M}} \cdot k_i} & \text{otherwise} \end{cases}$$

$$and \quad \mu'_{2^j \cdot k_i} = \mu_{2^j \cdot k_i} \quad j > \mathcal{M}, \quad \mathcal{M} = \lfloor log_2 n_i \rfloor + 1.$$

**Proof:**
The proof is developed with the assumption that the $(x+1)^{n_i}$ is the *only* factor annihilated by $F$. The generalization can be done where $(x+1)^{n_i}$ is the *largest* factor annihilated by $F$.
The characteristic polynomial $f(x)$ of such a $CA$ is denoted as

$$f(x) = (x+1)^{n_i} \times \tilde{\phi}(x); \;\; \tilde{\phi}(x) = \phi_1(x)^{n_1} \cdot \cdot \phi_{i-1}(x)^{n_{i-1}} \cdot \phi_{i+1}(x)^{n_{i+1}} \cdot \cdot \phi_{\mathcal{N}}(x)^{n_{\mathcal{N}}}$$

The cycle structure $CS\tilde{\phi}(x)$ corresponding to $\tilde{\phi}(x)$ is same for both the $LCA$ and $ACA$. Let $F$ be the inversion vector which annihilates the factor $(x+1)^{n_i}$.
As per the *theorem 5*, the cycle structures generated due to the factor $(x+1)^{n_i}$ differ in $C$ & $C'$ and these are $CS'(x+1)^{n_i}$ and $CS(x+1)^{n_i}$ (from *corollary III.1*). From the eqs. (19) & (*8)*, we have

$$CS'(x+1)^{n_i} = \mu'(2^{\mathcal{M}}), \quad \mu' = 2^{n_i - \mathcal{M}} \quad \& \quad \mathcal{M} = \lfloor log_2(n_i) \rfloor + 1$$

$$and \quad CS(x+1)^{n_i} = [1(1) + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j)], \quad where\ m = \lceil log_2(n_i) \rceil.$$

The cycle structure of $C\tilde{\phi}(x)$ follows from eq. (4) and forms a *linear cycle structure*

$$CS\tilde{\phi}(x) = [1(1) + \sum_{k_i} \sum_{j=0}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i)]$$

Therefore, the cycle structures $CS$ and $CS'$ are represented as

$$CS \quad = \quad CS\tilde{\phi}(x) \times CS(x+1)^{n_i} = [1(1) + \sum_{k_i} \sum_{j=0}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i)] \times [1(1) + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j)] \tag{22}$$

$$CS' \quad = \quad CS\tilde{\phi}(x) \times CS'(x+1)^{n_i} = [1(1) + \sum_{k_i} \sum_{j=0}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i)] \times [\mu'(2^{\mathcal{M}})] \tag{23}$$

The above two cross products[2] produce $CS$ and $CS'$ specified in the eqs. (20) and (21) respectively. □

The results of *theorem III.3* are illustrated below.

**Example 5.** Let us consider the $T$ matrix of the 5-cell $CA$ of *Fig. 2* as shown below

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Consider the three $ACA$ with the characteristic matrix as $T$ having these inversion vectors

$$F_1 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad F_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \text{and } F_3 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

- The characteristic polynomial $f(x)$ of the example $LCA/ACA$, in invariant polynomial form, is $f(x) = (x+1)(x+1)^2(x^2+x+1)$.
- The inversion vector $F_1$= [01100] annihilates only $(x+1)^2$. Therefore, $\mathcal{M} = \lfloor log_2(2) \rfloor + 1 = 2$ (*corollary III.1*). For this case,

[2]note the appendix for details

  - $f(x)$ can be expressed as $\tilde{\phi}(x) \times (x+1)^2$, where $\tilde{\phi}(x) = (1+x) \cdot (x^2+x+1)$.
  - The cycle structure $CS\tilde{\phi}(x) = CS(1+x) \times CS(x^2+x+1) = [1(1), 1(1)] \times [1(1), 1(3)] = [2(1), 2(3)]$.
  - The cycle structure $CS(1+x)^2 = [1(1), 1(1), 1(2)]$, whereas $CS'(1+x)^2 = [1(4)]$.
  - The resultant cycle structure $CS = CS\tilde{\phi}(x) \times CS(1+x)^2 = [[4(1), 2(2)], [4(3), 2(6)]]$ while $CS' = CS\tilde{\phi}(x) \times CS'(1+x)^2 = [2(4), 2(12)]$.

- Similarly, $F_2 = [11100]$ annihilates both the invariant polynomials $(x+1)$ and $(x+1)^2$. This is, the case where $(x+1)^2$ is the **largest** factor annihilated by $F_2$. Therefore, $CS' = CS'(x+1) \times CS'(x+1)^2 \times CS(x^2+x+1) = [1(4)] \times [1(2)] \times [1(1), 1(3)] = [2(4), 2(12)]$. It is same as that of the cycle structure generated by $F_1$.

- The changes in cycle structure of each cycle family $k_i$ in $CS$ and $CS'$ respectively are as per eq. (21) of *theorem III.3*. For example, 2(4) where $k_1 = 1$ and $2^{\mathcal{M}} = 4$, the corresponding cycle structure in $C$ which have got merged in $C'$ is [4(1),2(2)]. The cyclic component of $\mu_{2^2 \cdot 1}$ has been formed as per eq. 21. Here $\mu_{2^2 \cdot 1} = \frac{4 \times 1 + 2 \times 2}{4} = 2$.

- Consider $F_3 = [01000]$. It doesn't annihilate either $(x+1)$ or $(x+1)^2$. Therefore, the cycle structure of $C$ and $C'$ are the same - [4(1), 2(2), 4(3), 2(6)].

*Theorem III.3* and the earlier example identify the nature of cycle structure of $ACA$. The complete algorithm to compute cycle structure of an $ACA$ is described next.

## III.4. Enumerating cycle structure of an $ACA$

The scheme to enumerate cycle structure of an $ACA$ is developed based on the theory reported in the earlier subsections. *Theorem 3* reports that the cycle structures of $ACA$ and the corresponding $LCA$ are identical if the characteristic polynomial of the linear operator $T$ doesn't contain the factor $(x+1)$. On the other hand, if the characteristic polynomial is having the factor $(x+1)$, then the cycle structure of the $ACA$ is to be computed from eq. (21). However, it requires evaluation of $\mathcal{M}$ - the minimum additive factor.

**Definition 5.** The least cycle length of any primary cycle ($k$) in $CS'$ (cycle structure of $ACA$) is given by $2^{\mathcal{M}} \cdot k$; where $\mathcal{M}$ is denoted as minimum additive factor.

The value of $\mathcal{M}$ can be deduced from *theorem 2*. The rank of $[T^k+I]$ and $[T^k+I, \mathcal{F}]$ is successively compared for all $k = 2^m \cdot k_1$, $m \geq 0$, until the ranks become equal. The value of $k$ at which both the ranks become equal provides the value of $\mathcal{M}$. The algorithm to deduce $\mathcal{M}$ is next elaborated.

**Algorithm 1.** *Enum_$\mathcal{M}$($T, F$)*
Input : $T$ matrix, $F$ Vector
Output : $\mathcal{M}$
$\mathcal{M}$ = -1
$I, \mathcal{F}]$
do {

$\mathcal{M}$ = $\mathcal{M}$ + 1
Evaluate $\mathcal{F}$ = $[I + T + T^2 + .... + T^{2^{\mathcal{M}}-1}]F$
Evaluate R1 = rank$[T^{2^{\mathcal{M}}-1} + 1]$ and R2 = rank$[T^{2^{\mathcal{M}}-1} + I, \mathcal{F}]$
$\}$while ( $R1 < R2$)
return $\mathcal{M}$

Once the $\mathcal{M}$ is enumerated, the cycle structure of $ACA$ - $C'$ for each $k_i$-cycle family constituting $CS'$ is evaluated from the $CS$ of $LCA$ - $C$ (*theorem III.3*).

**Algorithm 2.** Enum_CS$'$_of_ACA$(T, F, CS')$
Input : Characteristic matrix $T$ and inversion vector $F$
Output : The cycle structure of $ACA$ - $C'$
Enumerate cycle structure $CS$ of $LCA$, where

$$CS = [1(1) + \sum_{k_i}\sum_{j=0}^{m_{k_i}} \mu_{2^j \cdot k_i}(2^j \cdot k_i)];\ k_i\ is\ odd\ and\ [CL]\ is\ the\ set\ of\ odd\ cycles\ of\ length\ k_i.$$

If characteristic polynomial of $T$ doesn't have a factor of $(x + 1)$, then
  Output the cycle structure $CS$ of $C$ as $CS'$ of $C'$.
else
  $\mathcal{M}$ = $Enum\_\mathcal{M}(T, F)$
  for each $k_i \in [CL]$
  $\{$
    Evaluate $\mu'_{2^{\mathcal{M}} \cdot k_i}$ for each $k_i$ following eq. (21)
    $\mu'_{2^j \cdot k_i}$ = $\mu_{2^j \cdot k_i}$ for $\forall\ j > \mathcal{M}$
  $\}$
  Output CS$'$ = $\sum_{k_i}\sum_{j=\mathcal{M}}^{m_{k_i}} \mu_{2^j \cdot k_i}(2^j \cdot k_i)$,    $k_1$ = 1

The next example illustrates the execution steps of the algorithm. The $ACA$ is represented by its $T$ matrix and $F$ vector; the $T$ matrix of this example is the one used in the *example 2*.

**Example 6.** Let the T matrix of a 5-cell $ACA$ be

$$T = \begin{pmatrix} [1] & 0 & 0 & 0 & 0 \\ 0 & \lceil 1 & 1 \rceil & 0 & 0 \\ 0 & \lfloor 0 & 1 \rfloor & 0 & 0 \\ 0 & 0 & 0 & \lceil 0 & 1 \rceil \\ 0 & 0 & 0 & \lfloor 1 & 1 \rfloor \end{pmatrix} \quad \text{and } F = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

The matrix $[T^k + I, \mathcal{F}]$ is referred to as *augmented matrix*.
Step 1 & 2 : Finding characteristic polynomial and cycle structure -
Characteristic polynomial $f(x)$ = $(x + 1)^3 \cdot (x^2 + x + 1)$
The cycle structure of the $LCA$ having the characteristic polynomial $f(x)$ is [4(1), 2(2), 4(3), 2(6)].
Step 3 : Finding the values of $\mathcal{M}$.

- Rank of $(T^1 + I)$ is 3, while the rank of the augmented matrix is 4. Hence, cycle of length 1 does not exist.
- Rank of $(T^2 + I)$ is 2, while the rank of the augmented matrix is 3. Hence, cycle of length 2 also does not exist in the $ACA$.
- Rank of $(T^4 + I)$ is 2, while the rank of the augmented matrix is 2. So, the value of $\mathcal{M}$ is 2.

*Step 4 : Finding the components*
**1.** $k_i$ =1 $\mu_{2^2 \cdot 1} = \frac{4\times1+2\times2+0\times4}{2^2\cdot1} = 2$.
**2.** $k_i$ =3 $\mu_{2^2 \cdot 3} = \frac{4\times3+2\times6+0\times12}{2^2\cdot3} = 2$.
Hence, the cycle structure becomes [2(4), 2(12)] .

# IV. Conclusion

This paper presents the complete scheme to compute the cycle structure of additive cellular automata ($ACA$). The similarities between the cycle structure of an $LCA$ and the cycle structure produced by the $ACA$ is explored. An analytical scheme has been devised to extract the similarities for enumeration of the cycle structure of $ACA$. The scheme can be used further to efficiently utilize $ACA$ for different purposes in the future.

# Appendix

**Elaboration of the steps to obtain the cross product of eq. (23)**

The cycle structure ($CS$) of an $LCA$ is evaluated from the expression referred in eq. (22). The expressions for $CS$ noted in eq. (22) is reproduced below along with the final result noted in eq. (20). The intermediate computation steps are not shown as it can be directly obtained through simple cross product [20].

$$\begin{aligned} CS &= CS\tilde{\phi}(x) \times CS(x+1)^{n_i} = [1(1) + \sum_{k_i}\sum_{j=0}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i)] \times [1(1) + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j)] \\ &= [1(1) + \sum_{k_i}\sum_{j=0}^{m_{k_i}} \mu_{2^j \cdot k_i}(2^j \cdot k_i)]; \quad k_1 = 1; \end{aligned}$$

The cycle structure ($CS'$) of $ACA$ is evaluated through eq. (23) reproduced below.

$$CS' = CS\tilde{\phi}(x) \times CS'(x+1)^{n_i} = [1(1) + \sum_{k_i}\sum_{j=0}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i)] \times [\mu'(2^{\mathcal{M}})]$$

The cross product of eq. (23) produces eq. (21) (page 1013). As can be seen from eq. (21), the cyclic components of $CS'$, ${\mu'}_{2^j \cdot k_i}$ has some relationship with $\mu_{2^j \cdot k_i}$ - the cyclic components of $CS$. This section establishes the relationship defined in eq. (21). The relationship between $\mu_{2^j \cdot k_i}$ and ${\mu'}_{2^j \cdot k_i}$ comprises of two parts - (a) where $j > \mathcal{M}$ and (b) where $j \leq \mathcal{M}$

Let us consider a particular cycle family $k_i$. We (1) first show that the number of states encompassed by a the family is same for both $CS$ and $CS'$. (2) Then we show $\mu_{2^j \cdot k_i} = {\mu'}_{2^j \cdot k_i}$ for $j > \mathcal{M}$ and finally (3) establish the relation between ${\mu'}_{2^{\mathcal{M}} \cdot k_i}$ and $\mu_{2^j \cdot k_i}$ for $j \le \mathcal{M}$.

1. Computing the number of states in a family $k_i$.

From eq. (5), product of $\mu_{k_{1i_1}}(k_{1i_1})$ and $\mu_{k_{2i_2}}(k_{2i_2})$ results in the cyclic component $\mu_k$ of length $k$, where $\mu_k = \mu_{k_{1i_1}}.\mu_{k_{2i_2}}.gcd(k_{1i_1}, k_{2i_2})$ and $k = lcm(k_{1i_1}, k_{2i_2})$. Therefore, the number of states involved in forming the cycle is given by

$$\mu \times k = (\mu_{k_{1i_1}}.\mu_{k_{2i_2}}.gcd(k_{1i_1}, k_{2i_2})) \times (lcm(k_{1i_1}, k_{2i_2})) = \mu_{k_{1i_1}}.\mu_{k_{2i_2}}.k_{1i_1}.k_{2i_2} \tag{24}$$

The above result can be applied to compute the number of states of a particular family $k_i$ in $CS$ and $CS'$. Let refer cycle structure of $k_i$ family as $CS(k_i)$ and $CS'(k_i)$ for $LCA$ and $ACA$ respectively. The number of states covered are considered as $S(k_i)$ and $S'(k_i)$ respectively in $CS(k_i)$ and $CS'(k_i)$. Therefore,

$$CS(k_i) = \sum_{j=0}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i) \times [1(1) + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j)] \Rightarrow S(k_i) = \sum_{j=0}^{m_{k_i}} (\hat{\mu}_{2^j \cdot k_i} \times 2^j \cdot k_i \times [1 \times 1 + \sum_{j=0}^{m} (\tilde{\mu}_{2^j} \times 2^j)])$$

Similarly,

$$CS'(k_i) = \sum_{j=0}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i) \times [\mu'(2^{\mathcal{M}})] \Rightarrow S'(k_i)] = \sum_{j=0}^{m_{k_i}} (\hat{\mu}_{2^j \cdot k_i} \times 2^j \cdot k_i \times \mu' \times 2^{\mathcal{M}})$$

From the eqs. (19) & (*8)*, we have

$$\mu' \times 2^{\mathcal{M}} = 1 + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j) \tag{25}$$

Therefore, $S(k_i) = S'(k_i)$ — Result (1).

2. The $\mu_{2^j \cdot k_i} = {\mu'}_{2^j \cdot k_i}$ for $j > \mathcal{M}$.

$$\begin{aligned} CS &= CS\tilde{\phi}(x) \times CS(x+1)^{n_i} = [1(1) + \sum_{k_i} \sum_{j=0}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i)] \times [1(1) + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j)] \\ &= [1(1) + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j) + \sum_{k_i} (\sum_{j=0}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i) \times [1(1) + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j)])] \\ &= [1(1) + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j) + \sum_{k_i} (\sum_{j=0}^{\mathcal{M}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i) \times [1(1) + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j)] + \sum_{j=\mathcal{M}+1}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i) \times [1(1) + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j)])] \end{aligned}$$

(i) Considering $2^j = 2^j \cdot k_i$, where $k_1 = 1$ & since $m \le \mathcal{M}$ (eqs. (19) & ( 8))

$$CS = [1(1) + \sum_{k_i} (\sum_{j=0}^{\mathcal{M}} \mu_{2^j \cdot k_i}(2^j \cdot k_i) + \sum_{j=\mathcal{M}+1}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i} \times [1(1) + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j)](2^j \cdot k_i))]$$

$$
\begin{aligned}
CS' &= CS\tilde{\phi}(x) \times CS'(x+1)^{n_i} = [1(1) + \sum_{k_i} \sum_{j=0}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i)] \times [\mu'(2^{\mathcal{M}})] \\
&= [\mu'(2^{\mathcal{M}})] + \sum_{k_i} [\sum_{j=0}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i) \times \mu'(2^{\mathcal{M}})] \\
&= [\mu'(2^{\mathcal{M}})] + \sum_{k_i} [(\sum_{j=0}^{\mathcal{M}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i) \times \mu'(2^{\mathcal{M}})) + (\sum_{j=\mathcal{M}+1}^{m_{k_i}} \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i) \times \mu'(2^{\mathcal{M}}))]
\end{aligned}
$$

(ii) Considering $2^{\mathcal{M}} = 2^{\mathcal{M}} \cdot k_i$, where $k_1 = 1$.

$$
CS' = \sum_{k_i} [(\sum_{j=0}^{\mathcal{M}} (\mu_{2^{\mathcal{M}} \cdot k_i}(2^{\mathcal{M}} \cdot k_i)) + \sum_{j=\mathcal{M}+1}^{m_{k_i}} \mu' \times 2^{\mathcal{M}} \times \hat{\mu}_{2^j \cdot k_i}(2^j \cdot k_i)]
$$

For $j > \mathcal{M}$

$$
\begin{aligned}
\mu_{2^j \cdot k_i} &= \hat{\mu}_{2^j \cdot k_i} \times [1 + \sum_{j=0}^{m} \tilde{\mu}_{2^j}(2^j)] \\
{\mu'}_{2^j \cdot k_i} &= \mu' \times 2^{\mathcal{M}} \times \hat{\mu}_{2^j \cdot k_i}
\end{aligned}
$$

Therefore, $\mu_{2^j \cdot k_i} = {\mu'}_{2^j \cdot k_i}$ for $j > \mathcal{M}$ (eq. (25)) – Result (2).

3. Computation of ${\mu'}_{2^{\mathcal{M}} \cdot k_i}$

Combining the results (1) and (2), the number of states covered by the cycles of length $\leq 2^{\mathcal{M}} \cdot k_i$ are same for both $LCA$ and $ACA$.

The states covered by $ACA$ are ${\mu'}_{2^{\mathcal{M}} \cdot k_i} \times 2^{\mathcal{M}} \cdot k_i$.

Similarly, the states covered by an $LCA$ for any $k_i \neq 1$ are $\sum_{j=0}^{\mathcal{M}} \mu_{2^j \cdot k_i} \times 2^j \cdot k_i$

Therefore,

$$
{\mu'}_{2^{\mathcal{M}} \cdot k_i} = \frac{\sum_{j=0}^{\mathcal{M}} \mu_{2^j \cdot k_i} \times 2^j \cdot k_i}{2^{\mathcal{M}} \cdot k_i}; \quad k_i \neq 1
$$

However, the states covered by the $LCA$ for $k_i = 1$ are $\sum_{j=0}^{\mathcal{M}} (\mu_{2^j \cdot k_i} \times 2^j \cdot k_i)$ +1 and, therefore,

$$
{\mu'}_{2^{\mathcal{M}} \cdot k_i} = \frac{1 + \sum_{j=0}^{\mathcal{M}} \mu_{2^j \cdot k_i} \times 2^j \cdot k_i}{2^{\mathcal{M}} \cdot k_i}; \quad k_i = 1
$$

# References


[1] Chakraborty, S., Chowdhury, D. R., Chaudhuri, P. P.: Theory and Application of Non-Group Cellular Automata for Synthesis of Easily Testable Finite State Machines, *IEEE Trans. on Computers*, **45**(7), July 1996, 769–781.

[2] Chattopadhyay, S.: *Some Studies on Theory and Applications of Additive Cellular Automata*, Ph.D. Thesis, I.I.T. Kharagpur, India, 1996.

[3] Chaudhuri, P. P., Chowdhury, D. R., Nandi, S., Chatterjee, S.: *Additive Cellular Automata – Theory and Applications*, vol. 1, IEEE Computer Society Press, CA, USA, ISBN 0-8186-7717-1, 1997.

[4] Chowdhury, D. R.: *Theory and Applications of Additive Cellular Automata for Reliable and Testable VLSI Circuit Design*, Ph.D. Thesis, I.I.T. Kharagpur, India, 1992.

[5] Chowdhury, D. R., Basu, S., Gupta, I. S., Chaudhuri, P. P.: Design of CAECC — Cellular Automata Based Error Correcting Code, *IEEE Trans. on Computers*, **43**(6), June 1994, 759–764.

[6] Das, A. K.: *Additive Cellular Automata : Theory and Application as a Built-in Self-test Structure*, Ph.D. Thesis, I.I.T. Kharagpur, India, 1990.

[7] Das, A. K., Chaudhuri, P. P.: Efficient Characterization of Cellular Automata, *Proc. IEE (Part E)*, **137**(1), January 1990, 81–87.

[8] Das, A. K., Chaudhuri, P. P.: Vector Space Theoretic Analysis of Additive Cellular Automata and Its Applications for Pseudo-Exhaustive Test Pattern Generation, *IEEE Trans. on Computers*, **42**(3), March 1993, 340–352.

[9] Dasgupta, P., Chattopadhyay, S., Sengupta, I.: Theory and Application of Nongroup Cellular Automata for Message Authentification, *Journal of Systems Architecture*, **47**(7), July 2001, 383–404.

[10] Datta, K. B. .: *Matrix and Linear Algebra*, BPB Publications, 1993.

[11] Ganguly, N.: *Cellular Automata Evolution: Theory and Applications in Pattern Classification*, Ph.D. Thesis, B. E. College (Deemed University), 2004.

[12] Martin, O., Odlyzko, A. M., Wolfram, S.: Algebraic Properties of Cellular Automata, *Comm. Math. Phys.*, **93**, 1984, 219–258.

[13] Misra, S.: *Theory and Application of Additive Cellular Automata for Easily Testable VLSI Circuit Design*, Ph.D. Thesis, I.I.T. Kharagpur, India, 1992.

[14] Nandi, S.: *Additive Cellular Automata : Theory and Application for Testable Circuit Design and Data Encryption*, Ph.D. Thesis, I.I.T. Kharagpur, India, 1994.

[15] Nandi, S., Kar, B. K., Chaudhuri, P. P.: Theory and Application of Cellular Automata in Cryptography, *IEEE Trans. on Computers*, **43**(12), December 1994, 1346–1357.

[16] Paul, K.: *Theory and Application of GF($2^p$) Cellular Automata*, Ph.D. Thesis, B. E. College, (Deemed University), Howrah, India, 2002.

[17] Paul, K., Chowdhury, D. R., Chaudhuri, P. P.: Theory of Extended Linear Machines, *IEEE Trans. on Computers*, **51**(9), 2002, 1106–1110.

[18] Serra, M., Chen, G. L.: Pseudo-Random Pattern Generation and Fault Coverage of Delay Faults with Non Linear Finite State Machines with High Entropy, *Proc. IEEE On-Line Testing Workshop,Crete, Greece*, 1997.

[19] Sikdar, B. K., Ganguly, N., Chaudhuri, P. P.: Design of Test Pattern Generator without Prohibited Pattern Set, *IEEE Trans on Computer Aided Design*, **23**, Dec 2004, 1650– 1660.

[20] Stone, H.: *Linear Machines*, Princeton Univ. Press, 1965.

[21] Stone, H.: *Discrete Mathematical Structures and Their Applications*, Science Research Associates Inc., 1973.

[22] Wolfram, S.: Statistical Mechanics of Cellular Automata, *Rev. Mod. Phys.*, **55**(3), July 1983, 601–644.