On linear cellular automata (with special focus on rule 90)

Silvio Capobianco

Institute of Cybernetics at TUT

September 25, 2014

Revision: September 25, 2014

Introduction

- Cellular automata (CA) are models of synchronous parallel computation, where the next state of a cell depends on the current state of finitely many neighbors.
- In a linear CA, the set of states is a commutative ring, and the local update rule is linear in its arguments.
  An example of such is rule 90 (exclusive OR of the two nearest neighbors).
- We will discuss the algebraic theory of linear cellular automata.
- We will then discuss the results by Martin, Odlyzko and Wolfram about the behavior of rule 90 on finitely many cells.

Cellular automata

A d-dimensional cellular automaton (CA) is a triple $\mathcal{A} = \langle Q, \mathcal{N}, f \rangle$ where:

- Q is a finite set of states.
- $\mathcal{N} = \{n_1, \ldots, n_m\} \subseteq \mathbb{Z}^d$ is a finite neighborhood.
- $f : Q^m \to Q$ is a finitary local update rule.

Call $\mathcal{C} = \{c : \mathbb{Z}^d \to Q\} = \mathcal{C}(d, Q)$.
The local update rule induces a global transition function $F : \mathcal{C} \to \mathcal{C}$ by

$$F_{\mathcal{A}}(c)(x) = f\left(c(x + n_1), \ldots, c(x + n_m)\right)$$

Linearity

Suppose $Q = R$ is a commutative ring with identity.

It is then possible to have local update rules of the form

$$f\left(q_1, \ldots, q_m\right) = \sum_{i=1}^{m} a_i q_i$$

where $a_1, \ldots, a_m \in R$.

We then say that the CA is linear.

More algebra

If $Q = R$ is a commutative ring with identity, then $\mathcal{C}$ is an *R-module*:

- $c_1 + c_2 = \lambda(x : \mathbb{Z}^d) \,.\, c_1(x) + c_2(x)$ makes $\mathcal{C}$ an abelian group.
- $a \cdot c = \lambda(x : \mathbb{Z}^d) \,.\, a \cdot c(x)$ satisfies:

$$\begin{aligned}
a \cdot (c_1 + c_2) &= a \cdot c_1 + a \cdot c_2 \\
(a_1 + a_2) \cdot c &= a_1 \cdot c + a_2 \cdot c \\
(a_1 \cdot a_2) \cdot c &= a_1 \cdot (a_2 \cdot c) \\
1 \cdot c &= c
\end{aligned}$$

The superposition principle

A cellular automaton is linear if and only if

$$F_{\mathcal{A}}(r \cdot c + s \cdot e) = r \cdot F_{\mathcal{A}}(c) + s \cdot F_{\mathcal{A}}(e)$$

for every $r, s \in R$ and $c, e \in \mathcal{C}$.

In other words:

a cellular automaton is locally linear
if and only if it is globally linear

As a consequence:

the behavior of a linear CA is completely determined
by its behavior on a single 1 in a sea of zeros

Laurent series

A Laurent series in d variables is an expression of the form

$$\begin{aligned} \mathcal{L}(z_1, \ldots, z_d) &= \sum_{i_1, \ldots, i_d \in \mathbb{Z}} a_{i_1, \ldots, i_d} z_1^{i_1} \cdots z_d^{i_d} \\ &= \sum_{i \in \mathbb{Z}^d} a_i z^i \end{aligned}$$

where, in the last expression, $i = (i_1, \ldots, i_d)$ is used as a multiindex.
We indicate as $[z^i]\mathcal{L}(z)$ the coefficient a_i.

A Laurent polynomial is a Laurent series where the a_i's are all zero except for finitely many $i \in \mathbb{Z}^d$.

Laurent series for linear CA

We may identify the d-dimensional configuration c with the Laurent series in d variables

$$\mathcal{L}_c(z) = \sum_{i \in \mathbb{Z}^d} c(i) z^i$$

In addition, if $\mathcal{A}$ is a d-dimensional linear CA with

$$f(q_1, \ldots, q_m) = \sum_{i=1}^{m} a_i q_i$$

we may identify it with the Laurent polynomial in d variables

$$p_{\mathcal{A}}(z) = \sum_{i=1}^{m} a_i z^{-n_i}$$

Observe the use of the inverse neighborhood.

Algebraic operations with linear CA

If c is a d-dimensional configuration and $\mathcal{A}$ is a d-dimensional linear CA, then

$$\mathcal{L}_{F_{\mathcal{A}}(c)}(z) = p_{\mathcal{A}}(z) \cdot \mathcal{L}_c(z)$$

where the product on the right-hand side is the convolution

$$[z^i](\mathcal{L}_1 \cdot \mathcal{L}_2)(z) = \sum_{j \in \mathbb{Z}^d} ([z^{i+j}]\mathcal{L}_1(z)) \cdot ([z^{-j}]\mathcal{L}_2(z)) \;\; \forall i \in \mathbb{Z}^d$$

which is well defined if either $\mathcal{L}_1$ or $\mathcal{L}_2$ is a Laurent polynomial.

As a consequence,

any two d-dimensional linear CA commute

Reversibility of linear CA

Let $\mathcal{A} = \langle R, \mathcal{N}, f \rangle$ be a linear CA. The following are equivalent:

- $\mathcal{A}$ is injective—eqv., reversible.
- $p_{\mathcal{A}}(z)$ has a multiplicative inverse as a Laurent polynomial. In this case, $\mathcal{A}^{-1}$ is linear and $p_{\mathcal{A}^{-1}}(z) = (p_{\mathcal{A}})^{-1}(z)$.
- Sato, 1993: Every maximal ideal of R contains all the coefficients of $p_{\mathcal{A}}(z)$ except exactly one.
- For every $a \in R \setminus \{0\}$ there exists $b \in R$ such that $a \cdot b \cdot p_{\mathcal{A}}(z)$ is a monomial.

As a consequence:

reversibility of linear CA is decidable

If $R = \mathbb{Z}/n\mathbb{Z}$, then the above are equivalent to:

- Ito, Osatu and Nasu, 1983: Every prime factor of n divides every coefficient of $p_{\mathcal{A}}(z)$ except exactly one.

Surjectivity of linear CA

Let $\mathcal{A} = \langle R, \mathcal{N}, f \rangle$ be a linear CA. The following are equivalent:

- $\mathcal{A}$ is surjective.
- $p_{\mathcal{A}}(z)$ is not a zero divisor as a Laurent polynomial.
- Sato, 1993: No maximal ideal of R contains all the coefficients of $p_{\mathcal{A}}(z)$.
- $a \cdot p_{\mathcal{A}}(z) \neq 0$ for every $a \in R \setminus 0$.

As a consequence:

surjectivity of linear CA is decidable

If $R = \mathbb{Z}/n\mathbb{Z}$ and $U = \{i \in \mathbb{Z}^d \mid [z^i]p_{\mathcal{A}}(z) \neq 0\} = \{i_1, \ldots, i_r\}$, then the above are equivalent to:

- Ito, Osatu and Nasu, 1983: $\gcd\left(n, [z^{i_1}]p_{\mathcal{A}}(z), \ldots, [z^{i_r}]p_{\mathcal{A}}(z)\right) = 1$.

Linear CA on finite support

Suppose the cellular space has N cells, displaced on a circle.

- This is like saying that the cellular space is not $\mathbb{Z}$, but $\mathbb{Z}/N\mathbb{Z}$.
- Equivalently, the configurations we consider have period N.
- This, in turn, means that our $c \in \mathcal{C}$ satisfy

$$\begin{aligned}
\mathcal{L}_c(z) &= \sum_{i \in \mathbb{Z}} c(i) z^i \\
&= \sum_{i \in \mathbb{Z}} c\,(i \bmod N)\, z^i \\
&= \left(\sum_{k=0}^{N-1} c(k) z^k \right) \cdot \left(\sum_{i \in \mathbb{Z}} z^{Ni} \right)
\end{aligned}$$

We can still apply the theory seen before by working modulo

$$z^N - 1 = (z-1)(1 + z + \ldots + z^{N-1})$$

Wolfram's elementary CA

For $d = 1$ and $\mathcal{N} = \{-1, 0, +1\}$ we can enumerate the local update rules as follows:

- Interpret each binary string abc as the corresponding number $4 \cdot a + 2 \cdot b + c$.
- Suppose $f(i) = b_i$ for $i = 0, \ldots, 7$
- Then the rule number of f is

$$n = \sum_{i=0}^{7} b_i \cdot 2^i$$

Rule 90

As $90 = 64 + 16 + 8 + 2$, the look-up table of rule 90 is:

a	1	1	1	1	0	0	0	0
b	1	1	0	0	1	1	0	0
c	1	0	1	0	1	0	1	0
$f_{90}(a, b, c)$	0	1	0	1	1	0	1	0

We observe that this has the algebraic expression:

$$f_{90}(a, b, c) = a \operatorname{xor} c = a + c - 2ac$$

Rule 90 is thus a linear CA, whose Laurent polynomial is

$$p_{90}(z) = z + z^{-1}$$

Preimages

Suppose c has a preimage e:

$$
\begin{aligned}
e &= 10100101000111 \\
c &= 10011000101100
\end{aligned}
$$

We may always get a new preimage by flipping each bit of e:

$$
\begin{aligned}
\bar{e} &= 01011010111000 \\
c &= 10011000101100
\end{aligned}
$$

More preimages

Suppose c has a preimage e:

$$\begin{array}{rcl} e & = & 10100101000111 \\ c & = & 10011000101100 \end{array}$$

If the number of sites is even, then we may get two more new preimages, by flipping either the even-indexed sites of e, or the odd-indexed ones:

$$\begin{array}{rcl} e_E & = & 00001111101101 \\ e_O & = & 11110000010010 \\ c & = & 10011000101100 \end{array}$$

No more preimages!

Theorem (Martin, Odlyzko and Wolfram, 1984)

- Every configuration with an odd number of sites taking value 1 is a garden of Eden.
- If N is odd, then 2^{N-1} configurations are not gardens of Eden.
- If N is even, then 2^{N-2} configurations are not gardens of Eden.

Intuition: Each value is used twice when computing the image.

As a corollary:

- For N odd, each reachable configuration has exactly two preimages.
- For N even, each reachable configuration has exactly four preimages.

Supporting intuition with theory

Suppose c has a predecessor e.

- Then $\mathcal{L}_c(z) = (z^2+1)B(z) + (z^N - 1)R(z)$.
- Then $\mathcal{L}_c(1) = 0$, *i.e.*, $\sum_{x=0}^{N-1} c(x) = 0 \mod 2$.
- This is the same as saying that $\mathcal{L}_c(z) = (z+1)D(z)$.

If N is odd:

- $(z + z^{-1})(z^2 + z^4 + \ldots + z^{N-1}) = z + 1$.
- Then e with $\mathcal{L}_e(z) = (z^2 + z^4 + \ldots + z^{N-1})D(z)$ is a preimage for c.

If N is even:

- By applying the **Frobenius automorphism** in characteristic 2, $z^N - 1 = (z^{N/2} - 1)^2$, thus $z^N - 1 = (z^2+1)E(z)$.
- Consequently, $\mathcal{L}_c = (z^2+1)S(z)$ for some $S(z)$ of degree $< N-2$.
- There are exactly 2^{N-2} polynomials of degree $< N-2$ over $\{0,1\}$.

The shape of the orbits

For N odd:

- Orbits are cycles, with single edges reaching each point of the cycle.
- Each such edge can be the root of a binary tree.

For N even:

- Orbits are cycles, with three edges reaching each point of the cycle.
- Each such edge can be the root of a quaternary tree.

The size of the trees

Theorem (Martin, Odlyzko and Wolfram, 1984)

- For given N, all such trees are **equal**.
- If N is odd, then the height of the trees is 1.
  That is: orbits are cycles, with single edges connected to each point.
- If N is even, then the height of the trees is $D/2$, where D is the highest power of 2 that divides N.
-

In particular, if N is even, then:

- Exactly 2^{N-2t} configurations are reachable at time $t = 1, \ldots, D/2$.
- Exactly 2^{N-D} configurations are reachable at arbitrary time $t \geq D/2$.

The size of the cycles

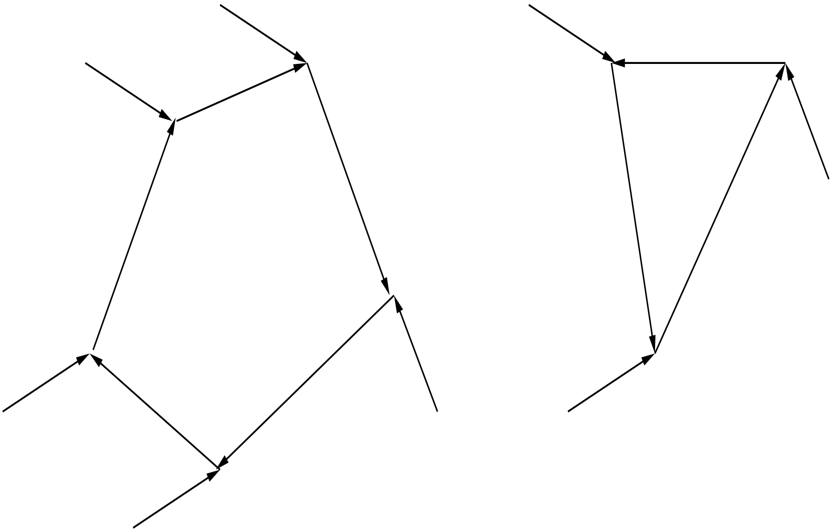
Theorem (Martin, Odlyzko and Wolfram, 1984)

Let Π_N be the length of the orbit starting from the configuration

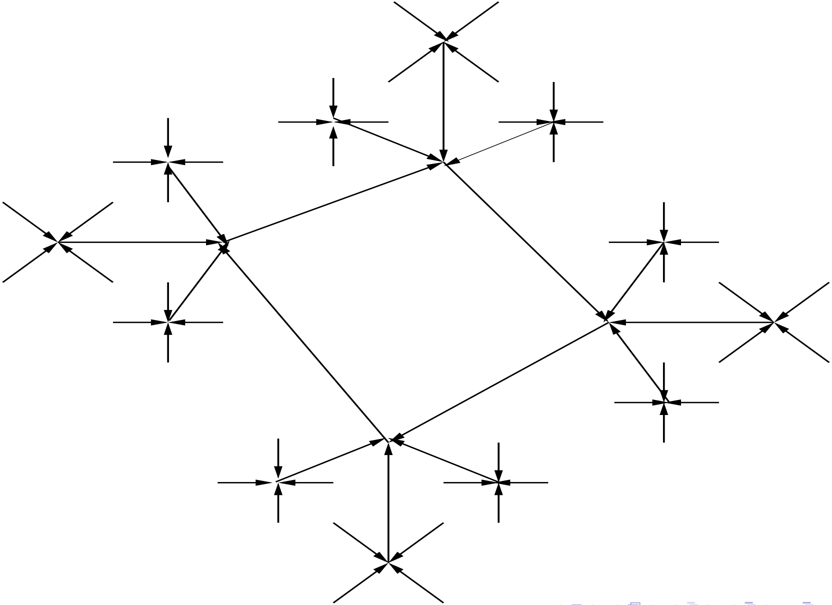
$$c_1 = \lambda(x : \mathbb{Z}/N\mathbb{Z}) \,.\, [x = 0]$$

- Each length of a cycle is a factor of Π_N.
- If N is a power of 2 then $\Pi_N = 1$.
- If $N = 2^k m$ is even, but not a power of 2, then $\Pi_N = 2\Pi_{N/2}$.
- If N is odd, then Π_N is a factor of $2^j - 1$, where $j \geq 1$ is the smallest integer such that 2^j is either $+1$ or -1 modulo N.

Shape of the orbits for $N = 17$



Shape of the orbits for $N = 12$



Conclusions

- Linear cellular automata can be studied with the tools of algebra.
- Linearity makes easier some things that are, in general, very difficult.

Thank you for attention!

Any questions?