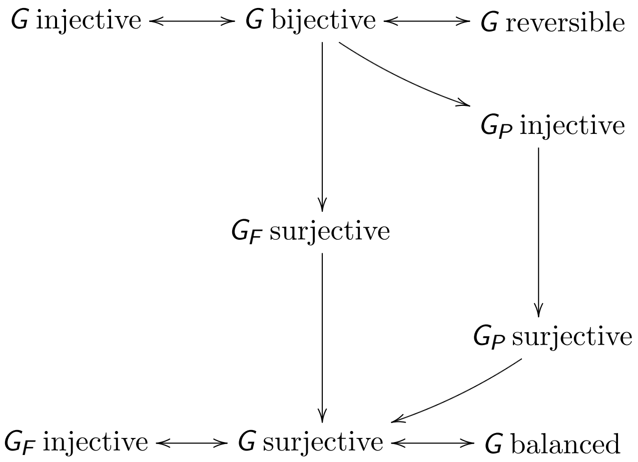
ITT8040 — Cellular Automata
Lecture 4

Silvio Capobianco

Institute of Cybernetics at TUT

April 3, 2013

Implications betweeen CA properties



G surjective $\not\Rightarrow$ G_F surjective

Counterexample: elementary CA rule 102:

$$f(x, y, z) = y + z - 2yz = y \operatorname{xor} z$$

Every configuration has two preimages:

- Start with arbitrary c.
- Set $e(0)$ arbitrarily.
- For $i > 0$ put $e(i) = c(i-1) \operatorname{xor} e(i-1)$.
- For $i < 0$ put $e(i) = c(i) \operatorname{xor} e(i+1)$.
- Then $G(e) = c$.

However, neither preimage of $\ldots 0001000 \ldots$ is finite.

G_F surjective $\not\Rightarrow$ G injective

Define the controlled xor by $S = \{0,1\} \times \{0,1\}$, $d = 1$, $N = \{0,1\}$, and

$$f((x_0, x_1), (y_0, y_1)) = \begin{cases} (x_0 \,\mathrm{xor}\, y_0, 1) & \text{if } x_1 = 1\,, \\ (x_0, 0) & \text{if } x_1 = 0\,. \end{cases}$$

One-dimensional surjective CA

Let G be a one-dimensional surjective CA global function.
Then the quantity $|G^{-1}(c)|$, $c \in S^{\mathbb{Z}}$, is bounded.

- Suppose G is defined by a neighborhood $N = \{-r, \ldots, r\}$. Suppose $c \in S^{\mathbb{Z}}$ has $|S|^{2r} + 1$ distinct preimages $e_0, \ldots, e_{|S|^{2r}}$.
- There exists $k > 0$ such that, for every $0 \leq i < j \leq |S|^{2r}$, there exists $n = n(i,j) \in D = \{-k, \ldots, k\}$ such that $e_i(n) \neq e_j(n)$.
- But then, $p = (D', g')$ with $D' = \{-k + r, \ldots, k - r\}$ and $g' = g|_{D'}$ has more than $|S|^{2r} = |S|^{|D|-|D'|}$ preimages.

One-dimensional surjective CA (cont.)

Let G be a one-dimensional surjective CA global function.
If $G(c)$ is spatially periodic then so is c.

- Let $n > 0$ satisfy $\tau_n(G(c)) = G(c)$.
  Then $\tau_{in}(G(c)) = G(c)$ as well, for every $i \in \mathbb{Z}$.
- But $\tau_{in}(G(c)) = G(\tau_{in}(c))$, so every $\tau_{in}(c)$ is a preimage for $G(c)$.
- As G is surjective, such preimages must be finitely many, so there must be $i < j$ with $\tau_{in}(c) = \tau_{jn}(c)$.
- But this is the same as saying that $\tau_{(j-i)n}(c) = c$.

Difference with higher dimension

Let $S = \{0, 1\}$, $d = 2$, $N = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ and

$$f(a, b, c, d) = (a + b + c + d) \mod 2$$

This is a surjective CA:

- Let $c, e : \mathbb{Z}^2 \to S$ satisfy $c \neq e$ and $G(c) = G(e)$.
- Consider a point $(i, j) \in \mathbb{Z}^2$ such that $c(i, j) \neq e(i, j)$.
- Then c and e must also differ at least in one of the points $(i + 1, j)$, $(i, j + 1)$, $(i + 1, j + 1)$ ...

However, the 0-configuration has uncountably many preimages.

Asymptotics

Let $c, e : \mathbb{Z} \to S$ be one-dimensional configurations.
We say that c and e are:

- positively asymptotic if there exists k such that $c(i) = e(i)$ for every $i > k$;
- negatively asymptotic if there exists k such that $c(i) = e(i)$ for every $i < k$;
- positively n-separated if there exists k such that for every $i > k$ there exists $j \in \{i, i+1, \ldots, i+n-1\}$ such that $c(j) \neq e(j)$;
- negatively n-separated if there exists k such that for every $i < k$ there exists $j \in \{i, i+1, \ldots, i+n-1\}$ such that $c(j) \neq e(j)$;
- totally n-separated if for every i there exists $j \in \{i, i+1, \ldots, i+n-1\}$ such that $c(j) \neq e(j)$.

Characterization of preimages for surjective 1D CA

Let $(S, 1, N, f)$ be a 1D surjective CA with $N = \{k, k+1, \ldots, k+m-1\}$ and global function G.
If $c \neq e$ but $G(c) = G(e)$ then exactly one of the following happens:

1. c and e are positively asymptotic and negatively $(m-1)$-separated.
2. c and e are negatively asymptotic and positively $(m-1)$-separated.
3. c and e are positively and negatively $(m-1)$-separated.

Proof of the characterization

Suppose $c(n) \neq e(n)$.
Then c and e must be $(m-1)$-separated on at least one side.

- Suppose otherwise. Let $k_1 < n < k_2$ such that $c(i) = e(i)$ for every i in
$$\{k_1 - (m-1) + 1, \ldots, k_1\} \cup \{k_2, \ldots, k_2 + (m-1) - 1\}$$
- As $G(c) = G(e)$ and $N = \{k, \ldots, k+m-1\}$, if we put $c'(i) = e(i)$ for $k_1 \leq i \leq k_2$ and $c'(i) = c(i)$ otherwise, then $G(c') = G(c) = G(e)$.
- This is impossible, because G is surjective and c and c' are asymptotic.

Proof of the characterization (cont.)

But it is also impossible that c and e are neither positively asymptotic nor positively $(m-1)$-separated.

- Otherwise, there would be k_1 such that $c(i) = e(i)$ for $k_1 - (m-1) < i \leq k_1$ ...
- ...then, as c and e are not positively asymptotic, $n > k_1$ such that $c(n) \neq e(n)$ ...
- ...and finally, as c and e are not positively $(m-1)$-separated, $k_2 > n$ such that $c(i) = e(i)$ for $k_2 \leq i < k_2 + (m-1)$
  ...which is precisely the situation in the previous slide!

Symmetrically, c and e must be either negatively asymptotic or negatively $(m-1)$-separated.

A crucial example

Let $S = \{0, 1, 2\}$, $N = \{0, 1\}$, and

$$f(a, b) = \begin{cases} 2 & \text{if } a = 2\,, \\ (a + b) \mod 2 & \text{otherwise}\,. \end{cases}$$

This CA is surjective.

- Suppose $c \neq e$ but $G(c) = G(e)$.
- Let $c(n) \neq e(n)$. Then neither of them is 2, and $c(n+1) \neq e(n+1)$ as well—so c and e cannot be asymptotic.

The next two configurations have same image:

$$\begin{array}{c} \ldots 000020000 \ldots \\ \ldots 000021111 \ldots \end{array}$$

So do these two:

$$\begin{array}{c} \ldots 000000000 \ldots \\ \ldots 111111111 \ldots \end{array}$$

The importance of the quiescent state

In the CA from the previous slide, both $q = 0$ and $q = 2$ satisfy $f(q, q) = q$.

The CA is surjective on 2-finite configurations:

- $c(i)$ and $G(c)(i)$ are either both equal to 2, or both different from 2.
- If k points have non-2 value, then there are 2^k such configurations, and G is a surjective transformation of such set.

...but it is not surjective on 0-finite configurations!

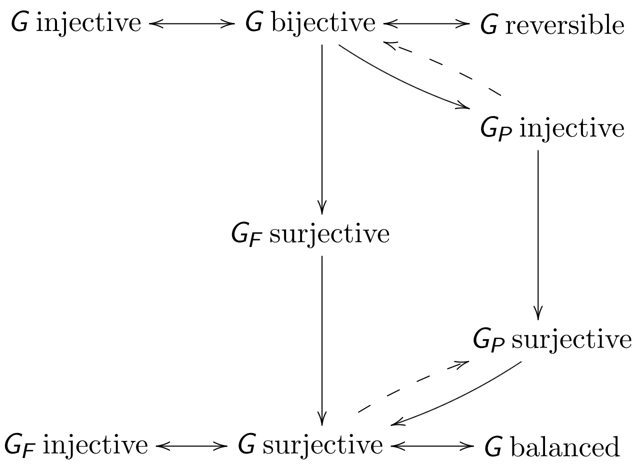
- A preimage of $\ldots 000010000 \ldots$ cannot be 0-finite.

More properties of 1D CA rules

Let G be a one-dimensional CA rule.
If G_P is injective then so is G.

- Suppose $c \neq e$ but $G(c) = G(e)$.
- As G_P is injective, it is also surjective, so G itself is surjective.
- Let G have neighborhood range m. Let c and e be positively $(m-1)$-separated. (The other case is symmetric.)
- There exist $k_1 \leq k_2 - m$ such that: **(prove it!)**
  - for $0 \leq i < m-1$, both $c(k_1+i) = c(k_2+i)$ and $e(k_1+i) = e(k_2+i)$, and
  - for at least one $0 \leq i < m-1$, $c(k_1+i) \neq e(k_1+i)$.
- Consider then c_P, e_P of period $k_2 - k_1$ coinciding with c and e, respectively, on $\{k_1, \ldots, k_2 - 1\}$: by construction, $G(c_P) = G(e_P)$ but $c_P \neq e_P$, against injectivity of G_P.

Implications betweeen 1D CA properties



de Bruijn graphs

We recall that a directed graph is defined by

- a set V of vertices (or nodes),
- a set E of edges, and
- two functions $t, h : E \to V$, the tail and head of each edge.

The de Bruijn graph of width m over a finite set S is the directed graph (V, E) such that:

- $V = S^{m-1}$,
- $E = S^m$,
- $t(s_1 \ldots s_m) = s_1 \ldots s_{m-1}$, and
- $h(s_1 \ldots s_m) = s_2 \ldots s_m$.

There is a bijection between configurations $c : \mathbb{Z} \to S$ and two-way infinite paths on the de Bruijn graph of width $m > 1$ over S.

Labeled de Bruijn graph of a 1D CA

Let $A = (S, 1, N, f)$ be a 1D CA with neighborhood range m.
The labeled de Bruijn graph of A is

- the de Bruijn graph of width m over S,
- together with a labeling $\mathcal{L} : E \to S$ of the edges defined as

$$\mathcal{L}(s_1 \dots s_m) = f(s_1, \dots, s_m)$$

The bi-infinite paths on the labeled de Bruijn graph of A represent

the images of the corresponding configurations
by the global function of A,
up to a fixed translation

Injectivity, surjectivity, and the labeled de Bruijn graph

Let $A = (S, 1, N, f)$ be a 1D CA with neighborhood range m. A diamond for (the labeled de Bruijn graph of) A is a pair of distinct paths with equal label, starting in the same node and ending in the same node.

- A is injective if and only if different paths always have different labels.
- A is surjective if and only if every configuration is the label of some path.
  By the Garden-of-Eden theorem, this is the same as saying that A has no diamonds.
- A word on S is an orphan if and only if it is not the label of any path.

The pair graph construction

The pair graph of a labeled graph $(V, E, \mathcal{L})$ is a graph where

- the set of states is $V \times V$, and
- there is an edge from (v_1, v_2) to (v_1', v_2') with label ℓ if and only if there are an edge from v_1 to v_2 and an edge from v_1' to v_2', both labeled ℓ.

We call $\Delta = \{(v, v) \mid v \in V\}$ the set of diagonal vertices.

Pair graphs and 1D cellular automata

Let $A = (S, 1, N, f)$ be a 1D CA with neighborhood range m.
Let $\mathcal{G} = (V, E, \mathcal{L})$ be the pair graph of the labeled de Bruijn graph of A.

1. A is injective if and only if there is no cycle in $\mathcal{G}$ through a point not in Δ.
2. A is surjective if and only if there is no cycle in $\mathcal{G}$ through both a point not in Δ and a point in Δ.