Post-surjectivity: an example of "almost dualization"

Silvio Capobianco
Institute of Cybernetics, Tallinn, Estonia
silvio@cs.ioc.ee

4^{th} Joint Estonian-Latvian Theory Days in Lilaste
13–14–15–**16** October 2016

Joint work with Jarkko Kari (University of Turku, Finland)
and Siamak Taati (Leiden University, The Netherlands)

Revision: 19 October 2016

Introduction

- Cellular automata (CA) are synchronous distributed systems on a regular grid, where the next state of a point is a function of the current state of its neighbors.
- A CA is called pre-injective if finitely many errors in the source configuration *can never be corrected* in finite time.
  This is a *weakening* of injectivity of the global function.
- Post-surjectivity is introduced as an "almost dual" of pre-injectivity: given a source-target pair, finitely many errors in the target *can always be obtained* by finitely many errors in the source.
  This is a *strengthening* of surjectivity of the global function.
- We prove that pre-injective, post-surjective CA are reversible.
  This is an "almost dual" to a well-known fact.
- We then show that, on a class of groups without known counterexamples, post-surjective CA are pre-injective.
  This is an "almost dual" to a famous conjecture.
- Our work: arxiv:1507.02472 [math.DS] (submitted to *DMTCS*)

Notation

Lambda-notation

Let x take values in a set X, and t take values in a set Y, and possibly depend on x. Then

$$\lambda x \,.\, t : X \to Y$$

is the function that associates to each value of $x \in X$ the corresponding value $t \in Y$.

Iverson brackets

The *Iverson brackets* are the function

$$[\cdot] : \{\mathrm{true}, \mathrm{false}\} \to \{0, 1\}$$

defined by:

$$[\mathrm{true}] = 1 \quad , \quad [\mathrm{false}] = 0$$

That is: $[\cdot] = \lambda x \,.\, (1 \text{ if true else } 0)$.

Configurations and patterns over groups

Let $\mathbb{G}$ be a group, $1_{\mathbb{G}}$ its identity element, and S a finite nonempty set.

- For $E, M \subseteq \mathbb{G}$: $EM = \{x \cdot y \mid x \in E, y \in M\}, E^{-1} = \{x^{-1} \mid x \in E\}$.
- A *configuration* is a function $c : \mathbb{G} \to S$. We set $\mathcal{C} = S^{\mathbb{G}}$.
- For $c, c' \in \mathcal{C}$ let $\Delta(c, c') = \{g \in \mathbb{G} \mid c(g) \neq c'(g)\}$.
  c and c' are *asymptotic* if $\Delta(c, c')$ is finite.
- A *pattern* is a function $p : E \to S$ with $E \subseteq \mathbb{G}, 0 < |E| < \infty$.

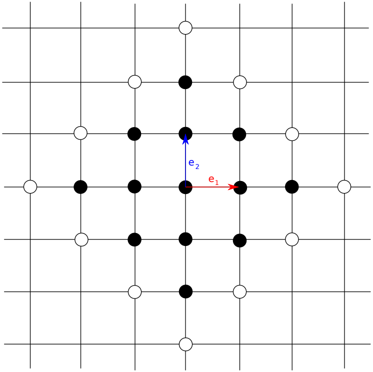
$B \subseteq \mathbb{G}$ *generates* $\mathbb{G}$ if words over $B \cup B^{-1}$ represent all elements of $\mathbb{G}$.

- The *length* of $g \in \mathbb{G}$ is the minimum length $\|g\|$ of such a word.
  We set $D_n = \{g \in \mathbb{G} \mid \|g\| \leq n\}$.
- This also induces a distance on $\mathcal{C}$ by

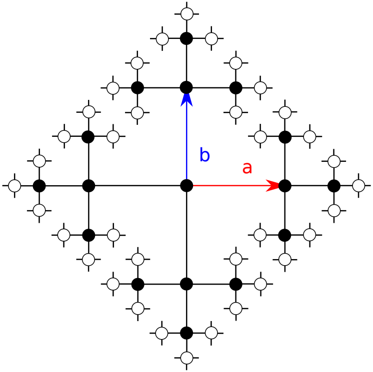
$$d_B(c, c') = 2^{-N} \text{ where } N = \inf\{\|g\| \mid g \in \mathbb{G},\ c(g) \neq c'(g)\}$$

In this talk, we will *only* consider *infinite, finitely generated* groups.

Examples of configurations on $\mathbb{Z}^2$ and $\mathbb{F}_2$



(a) The square grid, with the canonical generators $\mathbf{e}_1$ and $\mathbf{e}_2$



(b) The free group on two generators a and b

The disks of radius 2 are marked in black.
The elements of length 3 are marked in white.

Cellular automata over generic groups

A *cellular automaton* (CA) over a group $\mathbb{G}$ is a triple $\mathcal{A} = \langle S, \mathcal{N}, f \rangle$ where:

- S is a finite *set of states* with two or more elements.
- The *neighborhood* $\mathcal{N} = \{\nu_1, \ldots, \nu_m\} \subseteq \mathbb{G}$ is finite and nonempty.
- $f : S^m \to S$ is the *local update rule*.

The *global transition function* $F_\mathcal{A} : \mathcal{C} \to \mathcal{C}$ is defined by the formula

$$F_\mathcal{A}(c) = \lambda(g : \mathbb{G}) \,.\, f\left(c(g \cdot \nu_1), \ldots, c(g \cdot \nu_m)\right) \;\; \forall c \in \mathcal{C}$$

A pattern $q : M \to S$ is a *preimage* of $p : E \to S$ if $E\mathcal{N} \subseteq M$ and

$$f\left(q(x \cdot \nu_1), \ldots, q(x \cdot \nu_m))\right) = p(x) \;\; \forall x \in E$$

Nomenclature

- *Curtis-Lyndon-Hedlund theorem:*
  CA global rules are precisely the functions from $\mathcal{C}$ to $\mathcal{C}$ that are continuous with respect to the distancd d_B and commute with the *translations*
  $$\sigma_g = \lambda c \,.\, (\lambda x \,.\, c(g \cdot x))$$
- *Reversible cellular automaton:*
  a cellular automaton $\mathcal{A}$ for which a CA $\mathcal{B}$ exists such that $F_{\mathcal{B}} \circ F_{\mathcal{A}} = F_{\mathcal{A}} \circ F_{\mathcal{B}} = \mathrm{id}_{\mathcal{C}}$.
  It turns out that *every bijective CA is reversible*.
- *Garden of Eden:* A configuration that has no preimage.
- *Orphan:* A pattern that has no preimage.
  It turns out that *every garden of Eden contains an orphan*.

Pre-injectivity

A cellular automaton $\mathcal{A}$ is *pre-injective* if:

$$\begin{array}{c} \text{for every } c, c' \in \mathcal{C} \text{ with } c \neq c', \\ \text{if } |\Delta(c, c')| < \infty, \\ \text{then } F(c) \neq F(c'). \end{array}$$

That is: If *finitely many errors* are made *during initialization*, then *at no point in time* the correct computation will be *resumed*.

The Garden of Eden theorem

- *Moore, 1962:*
  Every surjective 2D CA is pre-injective.
- *Myhill, 1963:*
  Every pre-injective 2D CA is surjective.
- The arguments hold for d-dimensional CA for every $d \geq 1$.
- Consequence:

  Injective d-dimensional CA are surjective.

But $\mathbb{Z}^d$ is a *very* special group:

- It is a free object in the category of abelian groups.
- It is isomorphic to all its subgroups of finite index.

CA on generic groups: the good and the bad

What still holds:

- The Curtis-Lyndon-Hedlund theorem.
- Reversibility of bijective CA.

What does not hold anymore:

- *Both parts* of the Garden of Eden theorem. (Machì and Mignosi, 1993)
- The certainty that injective CA are surjective.

However, *no counterexample* to the latter is known ...

A pre-injective, non-surjective CA on $\mathbb{F}_2$

Ceccherini-Silberstein, Machì and Scarabotti, 1999:

- Let $\mathbb{F}_2$ be the free group on two generators a, b.
- Let $S = \mathbb{Z}_2 \times \mathbb{Z}_2$. Let $\mathcal{N} = \{a, b, a^{-1}, b^{-1}\}$, in this order.
- Let $f : S^4 \to S$ be defined by:

$$f((x_1, x_2), (y_1, y_2), (z_1, z_2), (w_1, w_2)) = (x_1 + y_2 + z_1 + w_2, 0) \,.$$

Then $\mathcal{A} = \langle \mathbb{F}_2, S, \mathcal{N}, f \rangle$ is not surjective. However, it is pre-injective.

- $(\mathbb{Z}_2 \times \mathbb{Z}_2)^{\mathbb{F}_2}$, with pointwise operations, is an abelian group, and $F_{\mathcal{A}}$ is a group endomorphism.
- Then $\mathcal{A}$ is *not* pre-injective iff the zero configuration has a nontrivial preimage which is nonzero only finitely many times.
- By exploiting that every point in $\mathbb{F}_2$ of length n has three neighbors of length $n+1$, one checks that this is not the case.

Post-surjectivity

A cellular automaton $\mathcal{A}$ is *post-surjective* if:

$$\begin{array}{c}\text{for every } c, e : \mathbb{G} \to S \text{ with } F_{\mathcal{A}}(e) = c \\ \text{and every } c' : \mathbb{G} \to S \textit{ asymptotic to } c \\ \text{there exists } e' : \mathbb{G} \to S \textit{ asymptotic to } e \text{ with } F_{\mathcal{A}}(e') = c'\end{array}$$

That is: every *target* configuration with *finitely many* errors can be produced by a *source* configuration with *finitely many* errors.

Post-surjectivity as a strengthening of surjectivity

Post-surjective CA are surjective

- Let $s_0, s_1 \in S$ be such that $F(\lambda x \,.\, s_0) = \lambda x \,.\, s_1$.
- A preimage of a given pattern p can be found by pasting it on $\lambda x \,.\, s_1$, and looking for a preimage of the entire configuration which coincides with $\lambda x \,.\, s_0$ except in finitely many points.

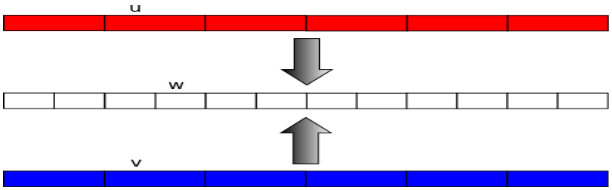
Not all surjective CA are post-surjective

- The $\textsc{xor}$ with the right-hand neighbor (rule 90) is surjective.
- However, $\lambda x \,.\, [x = 0]$ has no 0-finite preimage.

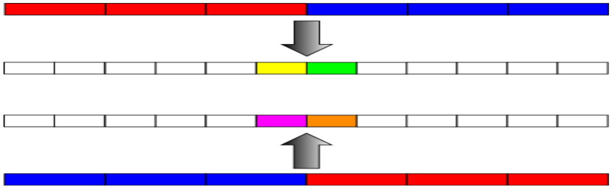
Is that just a case?

Post-surjectivity + 1D = reversibility

Fact: A non-reversible 1D CA is non-injective on periodic configurations:

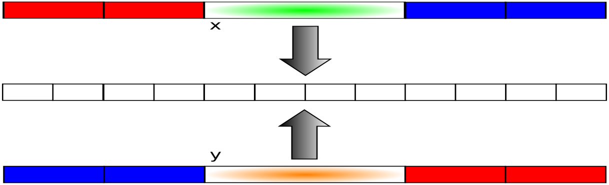


We may suppose each block length to be multiple of the neighborhood radius. The situation below is also valid:

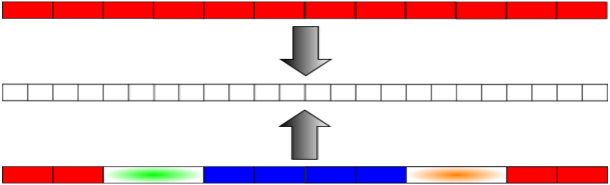


Post-surjectivity + 1D reversibility (cont.)

By post-surjectivity, we can obtain two more preimages of the original configuration as follows:



Then a violation of the Garden of Eden theorem occurs:



Post-surjectivity = pre-image within bounded radius

Lemma 1.

Let $\mathcal{A}$ be a post-surjective CA on $\mathbb{G}$ with global function F.
There exists $N \geq 0$ such that, for every two configurations c, c' with $\Delta(c, c') = \{1_{\mathbb{G}}\}$ and every preimage e of c, there exists a preimage e' of c' such that $\Delta(e, e') \subseteq D_N$.

By repeated application we get:

Corollary 1.

In the hypotheses of Lemma 1, there exists $N \geq 0$ such that, for every $r \geq 0$, if $\Delta(c, c') \subseteq D_r$ and $F(e) = c$, then c' has a preimages e' such that $\Delta(e, e') \subseteq D_{r+N}$.

If, in addition, $\mathcal{A}$ is pre-injective, we obtain:

Corollary 2.

Every pre-injective, post-surjective CA admits a finite $M \subseteq \mathbb{G}$ such that:
For every pair e, e' of asymptotic configurations, if $\Delta(F(e), F(e')) \subseteq K$, then $\Delta(e, e') \subseteq KM$.

Proof of Lemma 1

- By contradiction, for every $n \geq 0$ let c_n ,e_n, c'_n satisfy:
  1. $F(e_n) = c_n$.
  2. $\Delta(c_n, c'_n) = \{1_{\mathbb{G}}\}$.
  3. Every preimage of c'_n differs from e_n in some point outside D_n.
- Take $\{n_i\}_{i \geq 0}$ such that $c = \lim_{i \to \infty} c_{n_i}$, $e = \lim_{i \to \infty} e_{n_i}$, and $c' = \lim_{i \to \infty} c'_{n_i}$ all exist. Then $F(e) = c$ *and* $\Delta(c, c') = \{1_{\mathbb{G}}\}$.
- Take $e' \in \mathcal{C}$ and $m \geq 0$ s.t. $F(e') = c'$ and $\Delta(e, e') \subseteq D_m$.
- Take $\ell \gg m$ and choose k large enough that, on D_ℓ, c'_{n_k} coincides with c', and e_{n_k} with e.
- Let now $\overline{e}$ agree with e' on D_ℓ and with e_{n_k} outside D_m. Such $\overline{e}$ exists because e, e', and e_{n_k} agree on $D_\ell \setminus D_m$.
- Then $F(\overline{e}) = c'_{n_k}$ and $\overline{e}|_{D_{n_k}} = e_{n_k}|_{D_{n_k}}$: contradiction.

Post-surjectivity + pre-injectivity = reversibility

Let $\mathcal{A} = \langle S, \mathcal{N}, f \rangle$ a CA on a group $\mathbb{G}$ with global function F.

- Suppose $\mathcal{A}$ is both pre-injective and post-surjective. Let $F = F_{\mathcal{A}}$.
- Let M be as by Corollary 2.
- Let $\mathcal{N} = M^{-1}$. Fix a uniform configuration u and set $v = F(u)$.
- Given $g \in \mathbb{G}$ and $p : \mathcal{N} \to S$, for every $i \in \mathbb{G}$ let

$$y_{g,p}(i) = \begin{cases} p(g^{-1}i) & \text{if } i \in g\mathcal{N}, \\ v(i) & \text{otherwise} \end{cases}$$

Post-surjectivity + pre-injectivity = reversibility (cont.)

- By post-surjectivity and pre-injectivity, there exists a *unique* preimage $x_{g,p} : \mathbb{G} \to S$ of $y_{g,p}$ asymptotic to u. Let then
$$h(p) = x_{g,p}(g)$$
- The value $h(p)$ depends on p, *but not on g* because F is pre-injective and commutes with translations.
- Consider then the CA $\mathcal{B} = \langle S, \mathcal{N}, h \rangle$ on $\mathbb{G}$, and its global function H.
- We can infer (Automata 2015) that $(F \circ H)(y) = y$ *whenever y is asymptotic to v*. As the set of the latter is *dense* in $\mathcal{C}$, $F \circ H = \mathrm{id}_{\mathcal{C}}$.
- If, on the other hand, x is asymptotic to u, then so is $H(F(x))$, which is also a preimage of $F(x)$ because of the previous point.
- By pre-injectivity, $(H \circ F)(x) = x$ *whenever x is asymptotic to u*.
- Then, again by density, $H \circ F = \mathrm{id}_{\mathcal{C}}$ too, and $\mathcal{B}$ is the reverse of $\mathcal{A}$.

Surjunctive groups

A group $\mathbb{G}$ is *surjunctive* if for every set of states S, every injective CA on $S^{\mathbb{G}}$ is surjective.

- Every group where the Garden of Eden theorem holds is surjunctive.
- In particular, $\mathbb{Z}^d$ is surjunctive for every $d \geq 1$.
- Every *residually finite* group is surjunctive.
  Reason: $\mathbb{G}$ is r.f. if and only if *periodic* configurations are dense.
  (c is periodic if and only if $\{g \in \mathbb{G} \mid c^g = c\}$ has finite index.)
- In particular: *free groups* are surjunctive. No fear for $\mathbb{F}_2$!
- Actually, no non-surjunctive groups are known ...

Conjecture: (Gottschalk, 1973)

All groups are surjunctive.

Is there a post-surjective, non-pre-injective CA?

The classical counterexamples on the free group fail.

- The first neighbors majority rule on the free group is surjective (Ceccherini-Silberstein, Machì and Scarabotti, 1999)
- . . . but not post-surjective.

Maybe we only searched superficially . . .

. . . but maybe, they are *hidden too deeply?*

. . . or maybe, *there is nothing to find?*

The majority rule on $\mathbb{F}_2$

- Let $\mathbb{F}_2$ be the free group on two generators a, b.
- Let $S = \mathbb{Z}_2 = \{0, 1\}$. Let $\mathcal{N} = \{1, a, b, a^{-1}, b^{-1}\}$, in this order.
- Let $f : S^5 \to S$ be defined by:

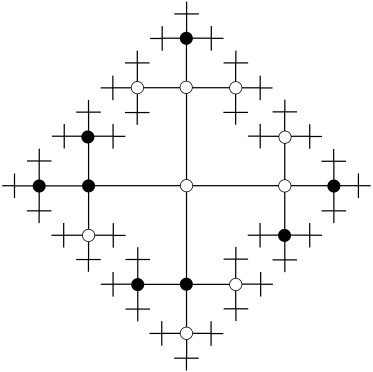
$$f(x, y, z, w, v) = (x + y + z + w + v) \mod 3$$

Then $\mathcal{A} = \langle \mathbb{F}_2, S, \mathcal{N}, f \rangle$ is not pre-injective. However, it is surjective.

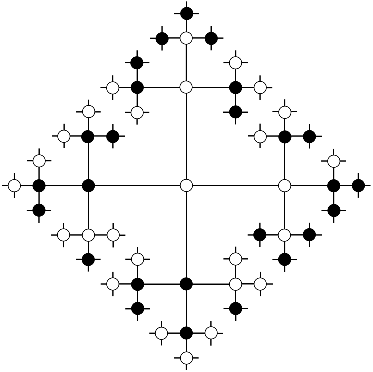
- Every point of length $n \geq 1$ has one neighbor of length $n - 1$, and three of length $n + 1$.
- Then a preimage for an arbitrary pattern on D_n can be constructed by first constructing a preimage for its restriction to D_{n-1}, then setting the remaining points of D_{n+1} so that the update yields the desired pattern.

The majority rule on $\mathbb{F}_2$ is not post-surjective

- Every configuration c has a "critical" preimage e where, at each point, exactly three of the five neighbors have the new state.
- If every point in c has neighbors "one step away" of both "opinions",
- then every single error in c "propagates indefinitely" in e.



(a) A configuration.



(b) A "critical" preimage.

Sofic groups

Gromov, 1999; Weiss, 2000 for finitely generated groups.

- Let $\mathbb{G}$ be a group and let B be a finite set of generators for $\mathbb{G}$.
- Let $r \geq 0$ be an integer and $\varepsilon > 0$ a real number.
- An *(r, ε)-approximation* of $\mathbb{G}$ is a B-labeled graph (V, E) together with a subset $U \subseteq V$ such that the following hold:
  1. For every $u \in U$, the neighborhood of radius r of u in (V, E) is isomorphic to $D_{B,r}$ as a labeled graph.
  2. $|U| > (1 - \varepsilon)|V|$.
- $\mathbb{G}$ is *sofic* if for every choice of $r \geq 0$ and $\varepsilon > 0$, there is an (r, ε)-approximation of $\mathbb{G}$.

Soficness *does not* depend on the choice of B.

- Groups where the Garden of Eden theorem holds are sofic.
- Free groups are sofic.
- **No non-sofic groups are known!**

Sofic groups and post-surjective CA

Lemma 2.
Let $\mathcal{A} = \langle S, D_R, f \rangle$ be a post-surjective CA on a sofic group $\mathbb{G}$.
Let N be as by Lemma 1. Let $r \geq N + 2R$.
Let (V, E) together with U be a (r, ε)-approximation of $\mathbb{G}$.
Every pattern $q : U \to S$ has a preimage $p : V \to S$.

Lemma 3. (Packing lemma; Weiss, 2000)
Let $\mathbb{G}$ be a group and B a finite set of generators.
Let (V, E) be a B-labeled graph and $U \subseteq V$ with $|U| \geq |V|/2$ such that:

for every $u \in U$,
the 2ℓ-neighborhood of u in (V, E) is isomorphic
to the disk of radius 2ℓ in the Cayley graph of $\mathbb{G}$.

Then, there is a set $W \subseteq U$ such that $|W| \geq |V|/2|D_{2\ell}|$ and the ℓ-neighborhoods of the elements of W are disjoint.

Post-surjectivity + soficness = pre-injectivity

- Let $\mathbb{G}$ be a sofic group and S a finite set with $s \geq 2$ elements.
- Suppose $\mathcal{A} = \langle S, D_R, f \rangle$ is post-surjective, but not pre-injective.
- Let $c, c' : \mathbb{G} \to S$ be different, equal outside D_m, and with same image. Let N be as by Lemma 1.
- Take $r \geq \max(N + 2R, m + 2R)$ and $\varepsilon > 0$ so small that

$$s^{\varepsilon} \cdot \left(1 - s^{-|D_R|}\right)^{\frac{1}{2|D_{2r}|}} < 1$$

- Let (V, E) and $U \subseteq V$ form an (r, ε)-approximation of $\mathbb{G}$.
- The labeled graph isomorphism between D_{2r} and the $2r$-neighborhood naturally induces a function $\phi : S^V \to S^U$ that "behaves like f".

Post-surjectivity + soficness = pre-injectivity (cont.)

- On the one hand, ϕ is surjective by Lemma 2, hence

$$|\phi(S^V)| = s^{|U|} \geq s^{(1-\varepsilon)|V|}$$

- On the other hand, by Lemma 3, there exists $W \subseteq U$ whose $|W| \geq \frac{|V|}{2|D_{2r}|}$ elements have disjoint r-neighborhoods.
- As there exist mutually erasable patterns on D_r,

$$|\phi(S^V)| \leq \left(s^{|D_r|} - 1\right)^{|W|} \cdot s^{|V|-|W|\cdot|D_r|}$$

- But the right-hand side is at most $\left(1 - s^{-|D_r|}\right)^{\frac{|V|}{2|D_{2r}|}} \cdot s^{|V|}$ ...
- ...which, in turn, is *strictly smaller* than $s^{(1-\varepsilon)|V|}$: contradiction.

Conclusion

- *Post*-surjectivity is a *strengthening* of surjectivity; *pre*-injectivity is a *weakening* of injectivity.
- Such "exchange of power" still allows to recover reversibility.
- On the class of sofic groups, where *injective* CA are *surjective*, it is also the case that *post-surjective* CA are *pre-injective*.
- No non-sofic groups are known!

We then formulate the following "almost dual" to Gottschalk's conjecture:

Every post-surjective CA is pre-injective.

Any counterexamples must be on some non-sofic group.

Thank you for attention!

Any questions?