Information Propagation and Simulation Preorders

Guillaume Theyssier

LAMA (UMR CNRS, Univ. Savoie)

February 19, 2007

Content of the talk

- 2 tools:
  - a simulation preorder on the set of CA

    (Mazoyer and Rapaport '98, Ollinger '02, T. '05)
  - **C**ommunication **C**omplexity applied to CA : *a way to measure information propagation*

    (Dürr, Rapaport, T. '04)
- calculus of CC for some classes of CA
- links between CC and the preorder structure

Subsystem

(Σ, F^t) is a subsystem of $(A^{\mathbb{Z}}, F)$ if Σ is (weakly) stable for F:

$$F^t(\Sigma) \subseteq \Sigma$$

Factor

(Σ', G) is a factor of $(A^{\mathbb{Z}}, F)$ if:

$$\phi \circ F = G \circ \phi$$

where $\phi : A^{\mathbb{Z}} \to \Sigma'$ is continuous, shift-commuting and onto

$(A^{\mathbb{Z}}, F)$ is at least as complex as (Σ, F^t) and (Σ', G)

Subautomata ($\sqsubseteq$)

$F_A \sqsubseteq F_B \iff \exists \iota : A \to B$ injective s.t. $\forall x \in A^{\mathbb{Z}}$:

$$F_B \circ \overline{\iota}(x) = \overline{\iota} \circ F_A(x).$$

Local factors ($\trianglelefteq$)

$F_A \trianglelefteq F_B \iff \exists \pi : B \to A$ surjective s.t. $\forall y \in B^{\mathbb{Z}}$:

$$F_A \circ \overline{\pi}(y) = \overline{\pi} \circ F_B(y).$$

e.g. $\forall i \leq n : MAX_i \sqsubseteq MAX_n$ and $MAX_i \trianglelefteq MAX_n$

Subautomata ($\sqsubseteq$)

$F_A \sqsubseteq F_B \iff \exists \iota : A \to B$ injective s.t. $\forall x \in A^{\mathbb{Z}}$:

$$F_B \circ \overline{\iota}(x) = \overline{\iota} \circ F_A(x).$$

Local factors ($\trianglelefteq$)

$F_A \trianglelefteq F_B \iff \exists \pi : B \to A$ surjective s.t. $\forall y \in B^{\mathbb{Z}}$:

$$F_A \circ \overline{\pi}(y) = \overline{\pi} \circ F_B(y).$$

- **Limitation:** $F_A \trianglelefteq F_B$ or $F_A \sqsubseteq F_B$ implies F_A is syntactically smaller than F_B

A preorder on CA

- **Idea:** change definitions to
  1. ensure (Σ, F) and (Σ', G) are CA
  2. capture more than subautomata and local factors

- Two points of view:
  - specialization of subsystems and factors
  - notions of subautomata and local factors **up to** space-time transformations

Definition

If $n > 0$ and $W \subseteq B^n$, let

$$L_W = \{u : \exists v \in \left(B^n\right)^* \text{ and } u \subseteq v\}.$$

The subshift Σ_W of language L_W is the block subshift associated to W.

Definition

If $n > 0$ and $W \subseteq B^n$, let

$$L_W = \{u : \exists v \in \left(B^n\right)^* \text{ and } u \subseteq v\}.$$

The subshift Σ_W of language L_W is the block subshift associated to W.

- **Remarks:**
  - Σ_W is not always of finite type (*e.g.* when $W = \{01, 00\}$);
  - Σ_W is always sofic (1-block factor of the SFT obtained by adding markers on the end of each block).

- Consider a subsystem (Σ_W, F^t) of $(A^{\mathbb{Z}}, F)$: $F^t(\Sigma_W) \subseteq \Sigma_W$.

- Consider a subsystem (Σ_W, F^t) of $(A^{\mathbb{Z}}, F)$: $F^t(\Sigma_W) \subseteq \Sigma_W$.
- Let $\Sigma_0 = \{x \in \Sigma_W : \forall k \in \mathbb{Z}, x_{kn}x_{kn+1} \cdots x_{(k+1)n-1} \in W\}$
  $\Sigma_0 \equiv$ *configurations "aligned" on* 0 *(not a subshift but fixed by* σ_A^n*).*
- **Fact:** $\exists k \in \mathbb{Z}$ s.t. $F^t \circ \sigma^k(\Sigma_0) \subseteq \Sigma_0$

  proof: consider $c \in \Sigma_0$ *with* $L(c) = L_W$

- Consider a subsystem (Σ_W, F^t) of $(A^{\mathbb{Z}}, F)$: $F^t(\Sigma_W) \subseteq \Sigma_W$.
- Let $\Sigma_0 = \{x \in \Sigma_W : \forall k \in \mathbb{Z}, x_{kn}x_{kn+1}\cdots x_{(k+1)n-1} \in W\}$
  $\Sigma_0 \equiv$ *configurations "aligned" on* 0 *(not a subshift but fixed by* σ_A^n*).*
- **Fact:** $\exists k \in \mathbb{Z}$ s.t. $F^t \circ \sigma^k(\Sigma_0) \subseteq \Sigma_0$
  proof: consider $c \in \Sigma_0$ *with* $L(c) = L_W$
- $(\Sigma_0, \sigma_A^n, F^t \circ \sigma^k)$ is isomorphic to a CA $(W^{\mathbb{Z}}, \sigma_W, F')$.

A preorder on CA

Buried subautomata

- Consider a subsystem (Σ_W, F^t) of $(A^{\mathbb{Z}}, F)$: $F^t(\Sigma_W) \subseteq \Sigma_W$.
- Let $\Sigma_0 = \{x \in \Sigma_W : \forall k \in \mathbb{Z}, x_{kn}x_{kn+1} \cdots x_{(k+1)n-1} \in W\}$
  $\Sigma_0 \equiv$ *configurations "aligned" on* 0 *(not a subshift but fixed by* σ_A^n*).*
- **Fact:** $\exists k \in \mathbb{Z}$ s.t. $F^t \circ \sigma^k(\Sigma_0) \subseteq \Sigma_0$

  proof: consider $c \in \Sigma_0$ *with* $L(c) = L_W$
- $(\Sigma_0, \sigma_A^n, F^t \circ \sigma^k)$ is isomorphic to a CA $(W^{\mathbb{Z}}, \sigma_W, F')$.

Definition

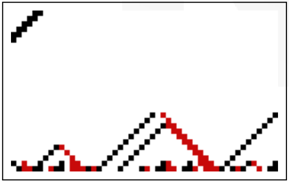
$(W^{\mathbb{Z}}, F')$ *is a buried subautomaton of* $(A^{\mathbb{Z}}, F)$*.*

► **Remark:** (Σ_W, F^t) contains $n-1$ copies of $(W^{\mathbb{Z}}, F')$ which possibly share some orbits.

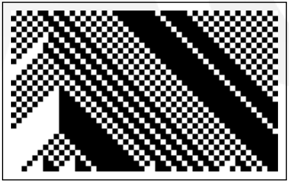
Definition

$F_A \preceq F_B$ if F_A is a local factor of some buried subautomaton of F_B.

- **Example:**



$$\preceq$$



$$W = \{\square\blacksquare\square\blacksquare\square\blacksquare, \square\blacksquare\square\square\square\blacksquare, \square\blacksquare\blacksquare\blacksquare\square\blacksquare\}$$

A preorder on CA

Alternative definition

- $$\left.\begin{array}{r} \mathbf{o}_m^{-1} : A^{\mathbb{Z}} \to \left(A^m\right)^{\mathbb{Z}} \\ \mathbf{o}_m : \left(A^m\right)^{\mathbb{Z}} \to A^{\mathbb{Z}} \end{array}\right\}$$ "power block transformation maps"

Proposition

$F_A \preceq F_B$ if and only if $\exists m, t, z$ such that $F_A \trianglelefteq\sqsubseteq \mathbf{o}_m^{-1} \circ \sigma^z \circ F_B^t \circ \mathbf{o}_m$.

A preorder on CA

Alternative definition

- $$\left.\begin{array}{r} \mathbf{o}_m^{-1} : A^{\mathbb{Z}} \rightarrow (A^m)^{\mathbb{Z}} \\ \mathbf{o}_m : (A^m)^{\mathbb{Z}} \rightarrow A^{\mathbb{Z}} \end{array}\right\}$$ "power block transformation maps"

Proposition

$F_A \preceq F_B$ if and only if $\exists m, t, z$ such that $F_A \trianglelefteq\sqsubseteq \mathbf{o}_m^{-1} \circ \sigma^z \circ F_B^t \circ \mathbf{o}_m$.

- $\preceq$ is a preorder (with induced equivalence relation $\sim$)
- we study the order $(AC/\sim, \preceq)$
  - top and bottom
  - topology (open = up-set, closed = down-set)
  - induced orders (chains, lattices, etc)

A preorder on CA

Alternative definition

- $$\left.\begin{array}{r} \mathbf{o}_m^{-1} : A^{\mathbb{Z}} \to \left(A^m\right)^{\mathbb{Z}} \\ \mathbf{o}_m : \left(A^m\right)^{\mathbb{Z}} \to A^{\mathbb{Z}} \end{array}\right\}$$ "power block transformation maps"

Proposition

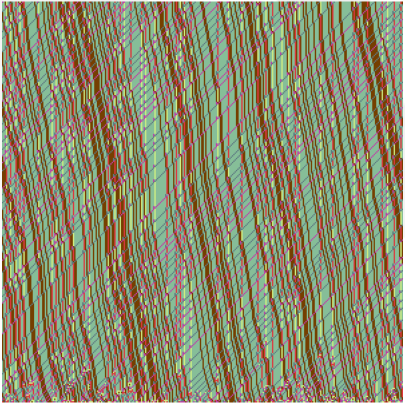
$F_A \preceq F_B$ if and only if $\exists m, t, z$ such that $F_A \trianglelefteq\sqsubseteq \mathbf{o}_m^{-1} \circ \sigma^z \circ F_B^t \circ \mathbf{o}_m$.

- $\preceq$ is a preorder (with induced equivalence relation $\sim$)
- we study the order $(AC/\sim, \preceq)$
  - top and bottom
  - topology (open = up-set, closed = down-set)
  - induced orders (chains, lattices, etc)

▶ **Remark:** many similar (but $\neq$) versions of preorders, *e.g.*

$$F_A \leq F_B \iff \exists m, m', t, t', z : \mathbf{o}_{m'}^{-1} \circ F_A^{t'} \circ \mathbf{o}_{m'} \trianglelefteq\sqsubseteq \mathbf{o}_m^{-1} \circ \sigma^z \circ F_B^t \circ \mathbf{o}_m.$$

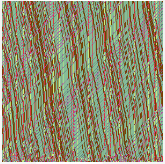
- $\preceq$ posseses a maximum class (intrinsic universality)



A preorder on CA

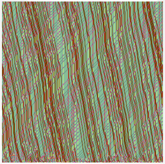
Some properties of $\preceq$

- $\preceq$ posseses a maximum class (intrinsic universality)



- some remarkable closed sets: *surjective CA, injective CA, linear CA, equicontinuous CA, nilpotent CA*
- a remarkable open set: *Turing-unversal CA*

- $\preceq$ posseses a maximum class (intrinsic universality)



- some remarkable closed sets: *surjective CA, injective CA, linear CA, equicontinuous CA, nilpotent CA*
- a remarkable open set: *Turing-unversal CA*
- infinite chains (MAX_n)
- Turing machines lattice
- ...

- **General question:** how to prove negative results?
  - F_A **can't** simulate F_B
  - F_A **isn't** intrinsically universal

A preorder on CA

Complexity parameters

- **General question:** how to prove negative results?
  - F_A **can't** simulate F_B
  - F_A **isn't** intrinsically universal

Definition

A good complexity parameter is an order morphism ρ from $(AC, \preceq)$ to some (total) order $(E, \leq)$.

- gives necessary conditions for simulations, *e.g.*

$$F_A \text{ intrinsically universal} \Rightarrow \rho(F_A) \geq e_U.$$

- **General question:** how to prove negative results?
  - F_A **can't** simulate F_B
  - F_A **isn't** intrinsically universal

Definition

A good complexity parameter is an order morphism ρ from $(AC, \preceq)$ to some (total) order $(E, \leq)$.

- gives necessary conditions for simulations, *e.g.*

$$F_A \text{ intrinsically universal} \Rightarrow \rho(F_A) \geq e_U.$$

- **"bad" complexity parameters:** *number of states, kolmogorov complexity of the transition table, (complexity of the limit set?)*

Communication complexity

Definition (Yao '79)

- **Informally:**
  - $f(x, y)$ a finite function
  - A knows f and x, B knows f and y
  - $CC(f) =$ "min #bits A and B must exchange to know $f(x, y)$"

Communication complexity

Definition (Yao '79)

- **Informally:**
  - $f(x, y)$ a finite function
  - A knows f and x, B knows f and y
  - $CC(f) =$ "min #bits A and B must exchange to know $f(x, y)$"
- **Formally:**
  - a protocol P for $f : X \times Y \to Z$ is a labelled binary tree
    - **internal nodes**: a predicate over x or a predicate over y
    - **leaves**: a value in Z
  - $P(x, y) =$ value of leaf reached by descending left/right according to predicates at nodes
  - $size(P) =$ depth of tree

Communication complexity

Definition (Yao '79)

- **Informally:**
  - $f(x, y)$ a finite function
  - A knows f and x, B knows f and y
  - $CC(f) =$ "min #bits A and B must exchange to know $f(x, y)$"
- **Formally:**
  - a protocol P for $f : X \times Y \rightarrow Z$ is a labelled binary tree
    - **internal nodes**: a predicate over x or a predicate over y
    - **leaves**: a value in Z
  - $P(x, y) =$ value of leaf reached by descending left/right according to predicates at nodes
  - $size(P) =$ depth of tree

Definition

$$CC(f) = \min_P \{ size(P) : \forall x, y, P(x, y) = f(x, y) \}$$

Communication complexity

Examples

- $X = Y = \{0, 1, \cdots, n\}$
- $f(x, y) = xy \bmod 2$

- $X = Y = \{0, 1, \cdots, n\}$
- $f(x, y) = xy \bmod 2$
- $CC(f) = 1$

- $X = Y = \{0, 1, \cdots, n\}$
- $f(x, y) = xy \bmod 2$
- $CC(f) = 1$

- $X = Y = \{0, 1\}^n$
- $f(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{else} \end{cases}$

- $X = Y = \{0, 1, \cdots, n\}$
- $f(x, y) = xy \bmod 2$
- $CC(f) = 1$

- $X = Y = \{0, 1\}^n$
- $f(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{else} \end{cases}$
- $CC(f) = n$

- $(A^{\mathbb{Z}}, F)$ with local function δ and radius r
- many ways to see δ as a function of 2 variables:

$$\delta_i : A^i \times A^{2r+1-i} \to A.$$

- $CC(F) = \max_i CC(\delta_i)$

Communication complexity

Application to CA

- $(A^{\mathbb{Z}}, F)$ with local function δ and radius r
- many ways to see δ as a function of 2 variables:

$$\delta_i : A^i \times A^{2r+1-i} \to A.$$

- $CC(F) = \max_i CC(\delta_i)$

Definition

$\rho(F) = t \mapsto CC(F^t)$

- $f \lesssim g \iff \exists K_1, K_2, \forall t : f(t) \leq K_1 g(K_2 t)$

- $(A^{\mathbb{Z}}, F)$ with local function δ and radius r
- many ways to see δ as a function of 2 variables:

$$\delta_i : A^i \times A^{2r+1-i} \to A.$$

- $CC(F) = \max_i CC(\delta_i)$

Definition

$\rho(F) = t \mapsto CC(F^t)$

- $f \lesssim g \iff \exists K_1, K_2, \forall t : f(t) \leq K_1 g(K_2 t)$

Proposition

$(\rho, \lesssim)$ *is a good complexity parameter*

Proposition

F linear $\Rightarrow \rho(F)$ bounded.

Proposition

F linear $\Rightarrow \rho(F)$ *bounded.*

Proof.

- $\delta : A^n \times A^m \rightarrow A$ linear
- A sends $\delta(x, 0)$ to B (cost: $\log(\#A)$ bits)
- B knows $\delta(0, y)$
- $\delta(x, y) = \delta(x, 0) + \delta(0, y)$
- B knows $\delta(x, y)$

□

Proposition

F equicontinuous $\Rightarrow \rho(F)$ *bounded.*

Proposition

F equicontinuous $\Rightarrow \rho(F)$ *bounded.*

Proof.

- $\exists K, \forall t : F^t$ has a minimal neighbourhood of size $\leq K$
- $\forall t, \delta_t$ depends only on K variables
- A tries all possible values for variables of B and sends the list of corresponding results (cost: at most $(\#A)^K \log(\#A)$ bits)
- B chooses the good result in the list

□

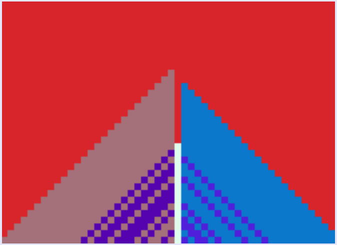
Proposition

There is a CA F with $\rho(F)$ growing linearly

Proposition

There is a CA F with $\rho(F)$ growing linearly

Proof.



□

Communication complexity

High complexity and universality

Proposition

There is a CA F with $\rho(F)$ growing linearly

Corollary

An intrinsically universal CA must have a linear CC

Proposition

There is a CA F with $\rho(F)$ growing linearly

Corollary

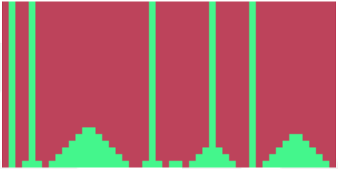
An intrinsically universal CA must have a linear CC

Corollary

Neither linear CA nor equicontinuous CA can be intrinsically universal

What's next?

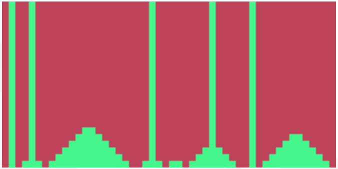
- other complexities:



$\rho(F) = \log$

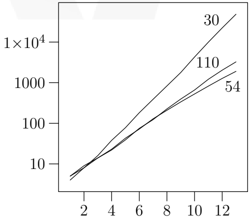
What's next?

- other complexities:



$$\rho(F) = \log$$

- experimentations:



Questions?