On simulation in Automata Networks

Florian Bridoux, Université Aix-Marseille, LIS
Maximilien Gadouleau, Durham University (UK)
Guillaume Theyssier, Université Aix-Marseille, I2M

Written version

- On simulation in Automata Networks, *2020, CIE'20, Florian Bridoux, Maximilien Gadouleau, Guillaume Theyssier*

How do you compute the swap function $(a, b) \mapsto (b, a)$ updating one register at the time? Solutions:

- With additional registers:
  - $c \leftarrow a$
  - $a \leftarrow b$
  - $b \leftarrow c$

$$(a, b, c) \to (a, b, a) \to (b, b, a) \to (b, a, a).$$

- A memoryless solution:
  - $a \leftarrow a \oplus b$
  - $b \leftarrow a \oplus b.$
  - $a \leftarrow a \oplus b$

  $(a, b) \to (a \oplus b, a) \to (a \oplus b, a \oplus a \oplus b) = (a \oplus b, a) \to (a \oplus b \oplus a, a) = (b, a).$

Related results

Question: memoryless solution in general

Can you compute any function $h : \mathbb{A}^n \mapsto \mathbb{A}^n$ updating one register at the time without additional registers?

Theorem: *Memoryless computation: new results, constructions, and extensions, 2015, Gadouleau M. and Riis S.*

For all functions $h : \mathbb{A}^n \to \mathbb{A}^n$, there are $m \leq 4n - 3$ functions $g^{(1)}, \dots, g^{(m)}$ such that:

- $h = g^{(m)} \circ \cdots \circ g^{(1)}$
- each $g^{(i)} : \mathbb{A}^n \to \mathbb{A}^n$ is an instruction (*i.e.* modifies a single register).

If h is bijective, we have $m \leq 2n - 1$ (optimal for $h = (0^n) \leftrightarrow (1^n)$).

Question

What happens if we always update the i-th register with the same function $f^{(i)}$?

Automata Networks: our definition

Definition: Automata networks

$f : \mathbb{A}^n \to \mathbb{A}^n$ with $\mathbb{A}$ a finite alphabet.

$\mathrm{F}(n, q)$: Set of automata networks of size n and alphabet size q

$$\mathrm{F}(n, q) = \{f : \mathbb{A}^n \to \mathbb{A}^n \mid \mathbb{A} = \{0, \ldots, q-1\}\}.$$

f can be seen as n *local functions* $f_i : \mathbb{A}^n \to \mathbb{A}$ such that

$$f(x) = (f_1(x), \ldots, f_n(x)) \text{ for all } x = (x_1, \ldots, x_n) \in \mathbb{A}^n.$$

Sequential updates

Definition: sequential update $f^{(i)}$

For all $i \in [1, n]$, $f^{(i)} : x \mapsto (x_1, \dots, x_{i-1}, f_i(x), x_{i+1}, \dots, x_n)$.

Definition: update schedule w

For all $w = w_1 w_2, \dots, w_m \in [1, n]^*$, $f^w = f^{(w_m)} \circ \dots \circ f^{(w_2)} \circ f^{(w_1)}$.

Let $f \in \mathrm{F}(m, q)$ and $g \in \mathrm{F}(n, q)$ with $m \geq n$.

Definition: simulation

Let $w \in \{0, 1\}^*$, $f \rhd_w g$ iff $\varphi_{[1,n]} \circ f^w = g \circ \varphi_{[1,n]}$.

In particular, if $m = n$, $f \rhd_w$ iff $f^w = g$.

- $f \rhd g$: $\exists w \in \{0, 1\}^*$ such that $f \rhd_w g$
- $f \rhd_{\mathrm{seq}} g$: $\exists w \in \pi([1, m])$ such that $f \rhd_w g$.

Previous results

Theorem: *Sequentialization and Procedural Complexity in Automata Networks, submitted, Bridoux F.*

- For all $g \in \mathrm{F}(n,q)$, $\exists f \in \mathrm{F}(3n/2 + \log_q(n), q)$ such that $f \triangleright_{\mathrm{seq}} g$.
- For all $n, q \geq 4$, $\exists g \in \mathrm{F}(n,q)$ such that if $f \in \mathrm{F}(m,q) \triangleright_{\mathrm{seq}} g$ then $m \geq 3/2n - \log_q(n)$.

Theorem: *Complete Simulation of Automata Networks, 2020, Bridoux F., Castillo-Ramirez A., Gadouleau M.*

For all n, q, $\exists f \in \mathrm{F}(n+1, q)$ such that $f \triangleright \mathrm{F}(n,q)$.

Let $\mathrm{Sym} = \{h \in \mathrm{F}(n,q) \mid h \text{is bijective}\}$.

Theorem: *Computing in permutation groups without memory, 2014, Cameron, P.J., Fairbairn, B., Gadouleau, M.*

For all $n, q \neq 2, 2$, $\exists f \in \mathrm{F}(n,q)$ such that $f \triangleright \mathrm{Sym}(n,q)$.

Previous results

Theorem

For all $n \geq 2, q$, there is no $f \in \mathrm{F}(n,q)$ such that $f \triangleright \mathrm{F}(n,q)$.

Proof:

- If $f \triangleright \mathrm{F}(n,q)$ then $f \triangleright_w g = (0^n \leftrightarrow 1^n)$ and $f \triangleright_{w'} = (0^n \to 1^n)$ for some, $w, w' \in [1,n]^*$.
- All registers $i \in [1,n]$ are updated in w. Indeed, if i is not updated in w , then $(f^w(0^n))_i = 0 \neq 1 = g_i(0^n)$.
- Since $h = f^{w'_m} \circ \cdots \circ f^{w'_2} \circ f^{w'_1}$ is not bijective then there exists w_j such that f^{w_j} is not bijective.
- Taking $i = w_j$, i is updated by w. Therefore $g = \cdots \circ f^{(i)} \circ \ldots$ is not bijective which is a contradiction. □

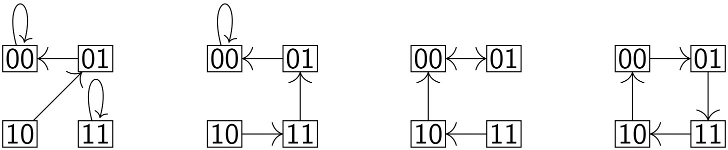
Questions: simulation without memory

For all $g \in \mathrm{F}(n,q)$, can you find $f \in \mathrm{F}(n,q)$ such that $f \triangleright g$?

Questions: simulation without memory

For all $g \in \mathrm{F}(n,q)$, can you find $f \in \mathrm{F}(n,q)$ such that $f \triangleright g$?

For $n = q = 2$, one can check that there are 26 $h \in \mathrm{F}(n,q)$ that cannot be simulated without memory. All are symmetric to one of these 4:

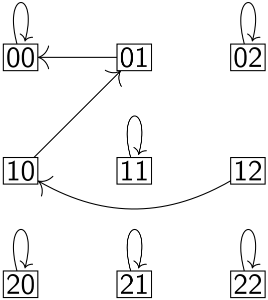


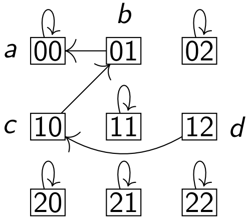
Theorem

For all $q \geq 3, n \geq 2$, $\exists g \in \mathrm{F}(n,q)$ that cannot be simulated by a function $f \in \mathrm{F}(n,q)$.

- For any $n \geq 2$, let $g = (120^{n-2} \to 10^{n-1} \to 010^{n-2} \to 0^n)$. We will prove that g is not simulated by any $f \in \mathrm{F}(n,q)$.

Transition digraph for $n = 2$:





- We have $g = (d \to c \to b \to a)$.
- Suppose that there is $f \in \mathrm{F}(n, q)$ such that $f \rhd_w g$.
- One can prove that there exists 4 distinct configurations a', b', c', d' equals to a, b, c, d on the second register such that $f^{(2)} = (d' \to c' \to b' \to a')$.
- Since $f^{(2)}$ updates only the register 2, we have $a'_1 = b'_1 = c'_1 = d'_1$.
- Since $a'_2 = c'_2$ and $a'_1 = c'_1$, $a' = c'$ which is a contradiction.

Cases where $q = 2$

Result

For all $n = 3, q = 2$, for all $g \in \mathrm{F}(n, q)$ there exists $f \in \mathrm{F}(n, q)$ such that $f \triangleright g$.

We check this result by computer. The program uses brute force:

- Take all $f \in \mathrm{F}(n, q)$ (there are 16 777 216).
- Compute the bigger S_f such that $f \triangleright S_f$.
- Check that the unions of all the S_f is $\mathrm{F}(n, q)$.
- (you can save some computation time using symmetries)

Conjecture:

For all $n \geq 3$, $q = 2$, for all $g \in \mathrm{F}(n, q)$ there exists $f \in \mathrm{F}(n, q)$ such that $f \triangleright g$.

Simulations with larger alphabet

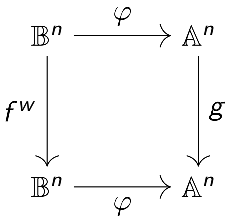
Consider $f \in \mathrm{F}(n, q')$ and $g \in \mathrm{F}(n, q)$ with $q' > q$.

Question?

What does it means for f to simulates g?

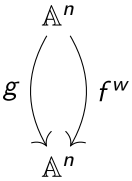
Let $\mathbb{A} = \{0, \ldots, q-1\}$ and $\mathbb{B} = \{0, \ldots, q'-1\}$, we have $\mathbb{A} \subseteq \mathbb{B}$.
Let $\varphi : \mathbb{B} \mapsto \mathbb{A}$ be surjective and let $\varphi : x \mapsto (\varphi(x_1), \ldots, \varphi(x_n))$.

by factor:



$\varphi \circ f^w = g \circ \varphi$
for some $w \in [1, n]^*$.

by initialization:



$\forall x \in \mathbb{A}^n, f^w(x) = g(x)$
for some $w \in [1, n]^*$.

Simulations by factor: Results

Let $\mathbb{A} = \{0, \ldots, q-1\}$ and $\mathbb{B} = \{0, \ldots, q'-1\}$, we have $\mathbb{A} \subseteq \mathbb{B}$.
Let $\varphi : \mathbb{B} \mapsto \mathbb{A}$ be surjective and let $\varphi : x \mapsto (\varphi(x_1), \ldots, \varphi(x_n))$.

by factor:

$$\begin{array}{ccc} \mathbb{B}^n & \xrightarrow{\varphi} & \mathbb{A}^n \\ {\scriptstyle f^w}\downarrow & & \downarrow{\scriptstyle g} \\ \mathbb{B}^n & \xrightarrow[\varphi]{} & \mathbb{A}^n \end{array}$$

$$\varphi \circ f^w = g \circ \varphi$$

for some $w \in [1, n]^*$.

Theorem

For any $q \geq 2$ and $n \geq 3$, there exists $f \in \mathrm{F}(n, 2q)$ which simulates all $\mathrm{F}(n, q)$ by factor.

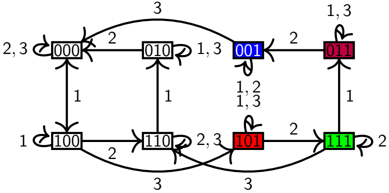
Simulations by factor: proof (sketch)

Decompose $z \in \mathbb{B}^n$ as $x \in \mathbb{A}^n$ and $y \in \{0,1\}^n$.

x_1	x_2	x_3	x_4	x_5	x_6
y_1	y_2	y_3	y_4	y_5	y_6

Decompose $z \in \mathbb{B}^n$ as $x \in \mathbb{A}^n$ and $y \in \{0,1\}^n$.

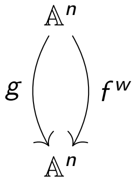
x_1	x_2	x_3	x_4	x_5	x_6
y_1	y_2	y_3			



- f realizes distinct transformations of x depending on the controlling states (y_1, y_2, y_3).
- In particular, we can realizes:
  - a circular permutation c of $\mathbb{A}^n$ with $1, 2, 2, 1, 3, 4, \ldots, n$.
  - the transposition $k = (0^n \leftrightarrow 10^{n-1})$ with $2, 1, 1$.
  - the assignment $d = (0^n \rightarrow 10^{n-1})$ with $2, 1, 2, 1$.
- We can generate $\mathrm{F}(n, q)$ by combinations of these operations.
- ⚠ The first state of (y_1, y_2, y_3) is uninitialized: we first use a synchronization word $((3)^q, 2, 3, 1, 1, 2, 1, 3)$ to put it in the state 101 without modifying x.

Simulations by initialization: Results

by initialization:



$$\forall x \in \mathbb{A}^n, f^w(x) = g(x)$$
for some $w \in [1, n]^*$.

Theorem

For all n, q with $n \geq 3q$, $\exists f \in \mathrm{F}(n, q+1)$ such that such that f simulates all $\mathrm{F}(n, q)$ by initialization.

Simulations by initialization: proof (sketch)

- Same principle: we want to use the bigger alphabet to encode 3 bits y_1, y_2, y_3 which will serve as controlling state.
- This time, the controlling state is initialized but its enconding is more complex.

Let $q = 3$, $n = 3q$. We have $\mathbb{A} = \{0, 1, 2\}$ and $\mathbb{B} = \{0, 1, 2, 3\}$.
Let $x = (0, 1, 2, 2, 1, 2, 0, 0, 0)$.

- If $y_1 = 0$ then $z_{1,\ldots,q} = x_{0,\ldots,q}$. Example with $y = (0, 0, 0)$.

  $z =$

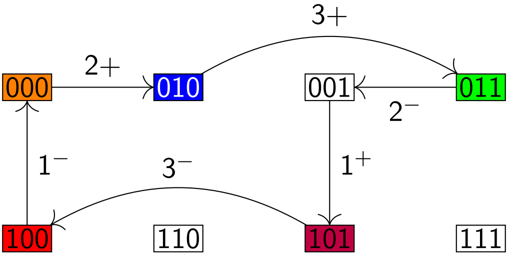
0	1	2	2	1	2	0	0	0

- If $y_1 = 1$ then $z_{i+1} = q$ with $i = x_1 + \ldots x_q \pmod{q}$.
  Example with $y = (1, 1, 1)$, we have $i_1 = 0 + 1 + 2 = 0$, $i_2 = 2 + 1 + 2 = 2$ and $i_3 = 0 + 0 + 0 = 0$.

  $z =$

3	1	2	2	1	3	3	0	0

Simulations by initialization: proof (sketch)



The construction is similar to the one used for the simulations by factor:

- f realizes distinct transformations of x depending on the controlling states (y_1, y_2, y_3).
- Thanks to this transformation, f can simulate all $\mathrm{F}(n, q)$.
- Additional difficulty: for technical reasons, if we have a transition $y_1 y_2 y_3 \to \overline{y_1} y_2 y_3$ then there is no transition $\overline{y_1} y_2 y_3 \to y_1 y_2 y_3$.

Conclusion

- Take away:
  - It is possible to simulate all $\mathrm{F}(n, q)$ by factor by an AN $f \in \mathrm{F}(n, 2q)$ $(n \geq 3)$.
  - It is possible to simulate all $\mathrm{F}(n, q+1)$ by initialization by an AN $f \in \mathrm{F}(n, q+1)$ $(n \geq 3q)$.
  - For any $q \geq 3, n \geq 2$, there exists $g \in \mathrm{F}(n, q)$ which is not simulated by any $f \in \mathrm{F}(n, q)$.
  - Conversely, all $g \in \mathrm{F}(3, 2)$ can be simulated by a $f \in \mathrm{F}(3, 2)$.
- Open question: What happens in the Boolean case for $n \geq 4$?

Conclusion

- Take away:
  - It is possible to simulate all $\mathrm{F}(n, q)$ by factor by an AN $f \in \mathrm{F}(n, 2q)$ $(n \geq 3)$.
  - It is possible to simulate all $\mathrm{F}(n, q+1)$ by initialization by an AN $f \in \mathrm{F}(n, q+1)$ $(n \geq 3q)$.
  - For any $q \geq 3, n \geq 2$, there exists $g \in \mathrm{F}(n, q)$ which is not simulated by any $f \in \mathrm{F}(n, q)$.
  - Conversely, all $g \in \mathrm{F}(3, 2)$ can be simulated by a $f \in \mathrm{F}(3, 2)$.
- Open question: What happens in the Boolean case for $n \geq 4$?

Thanks you for you attention.