Surjective Two-Neighbor Cellular Automata on Prime Alphabets

Jarkko Kari, Ville Salo, Ilkka Törmä

Department of Mathematics and Statistics
University of Turku, Finland
and
TUCS – Turku Center for Computer Science

A one-dimensional cellular automaton

$$f : S^{\mathbb{Z}} \longrightarrow S^{\mathbb{Z}}$$

is **surjective** if there are no Garden-of-Eden configurations.

Examples of surjective CA:

- All **injective** CA (a.k.a. **reversible** CA)
- All **permutive** CA

No structure theorem is known to **characterize local rules** that make the CA surjective.

We show that in some cases (size two neighborhood, prime number of states) all surjective CA are permutive.

We consider two parameters: **Number of states** n and the **neighborhood range** m

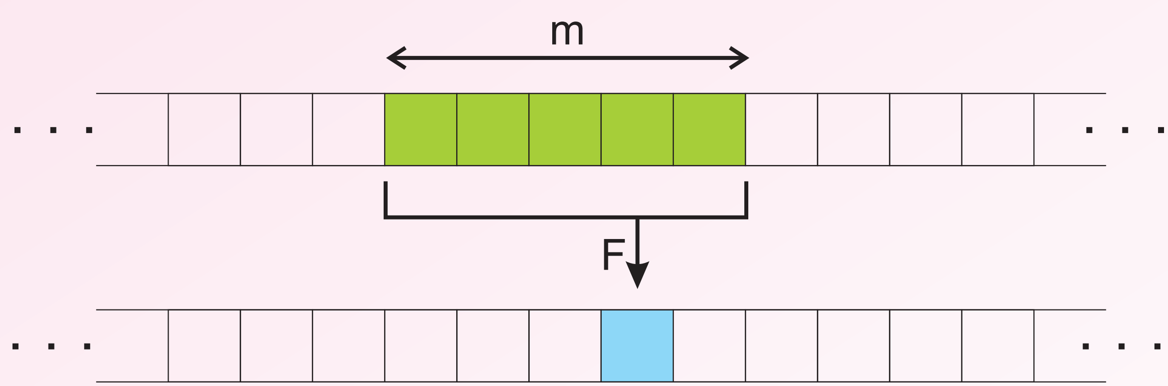
A **range** m **local rule** of a CA f is a function

$$F : S^m \longrightarrow S$$

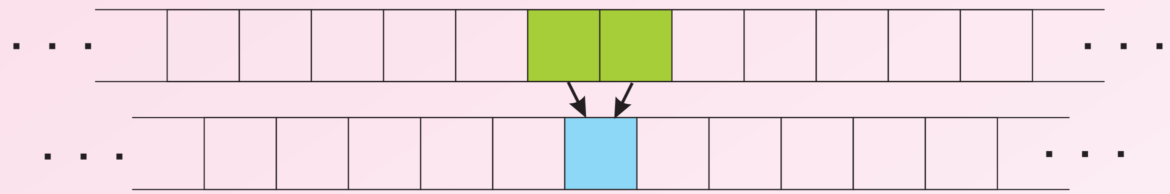
such that for all $c \in S^{\mathbb{Z}}$ and all $i \in \mathbb{Z}$

$$f(c)_i = F(c_{[i-k,i-k+m)}).$$

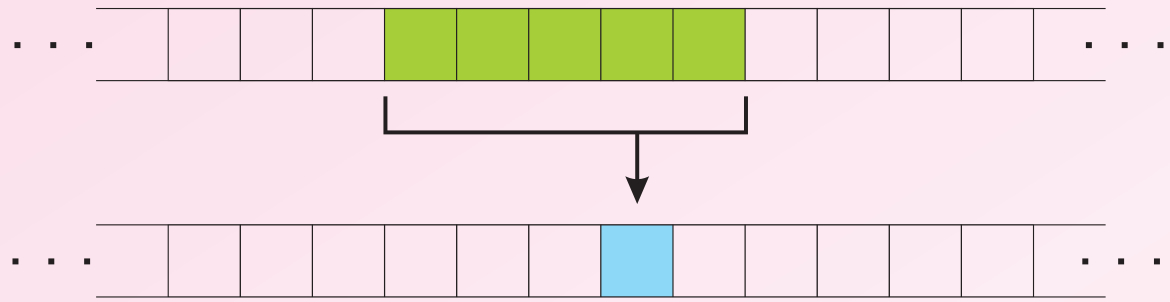
(Constant k aligns the neighborhood relative to the cell.)



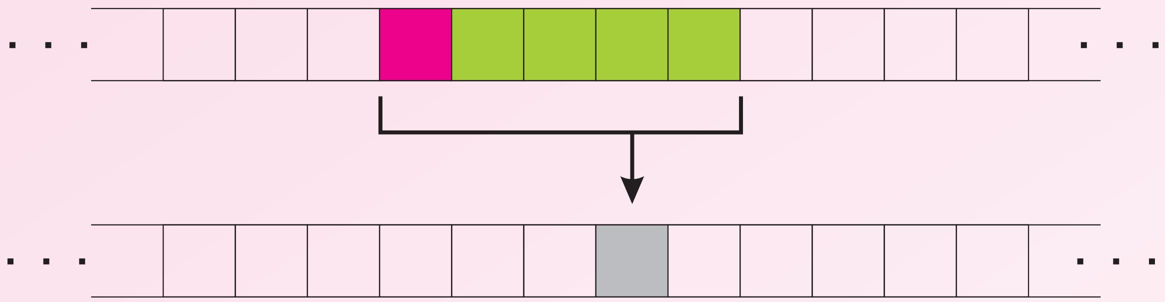
The case $m = 2$ is the smallest non-trivial neighborhood range. In pictures, we usually stagger the rows to make the neighborhood symmetric:



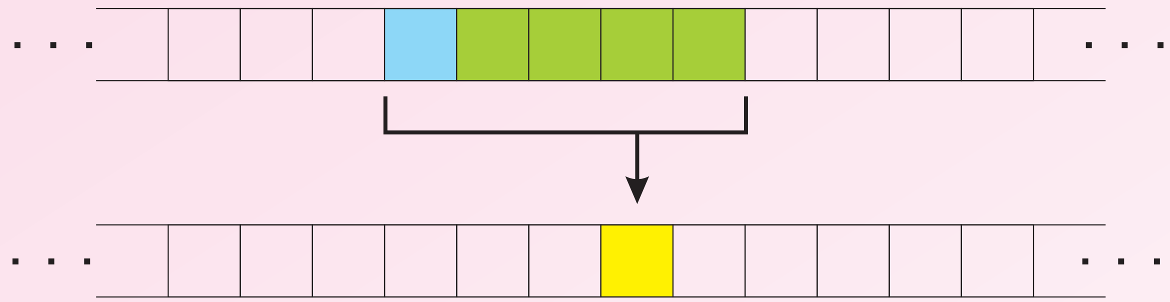
A CA is **left permutive** it has a local rule F with the property that changing the state of the leftmost neighbor changes the image under F.



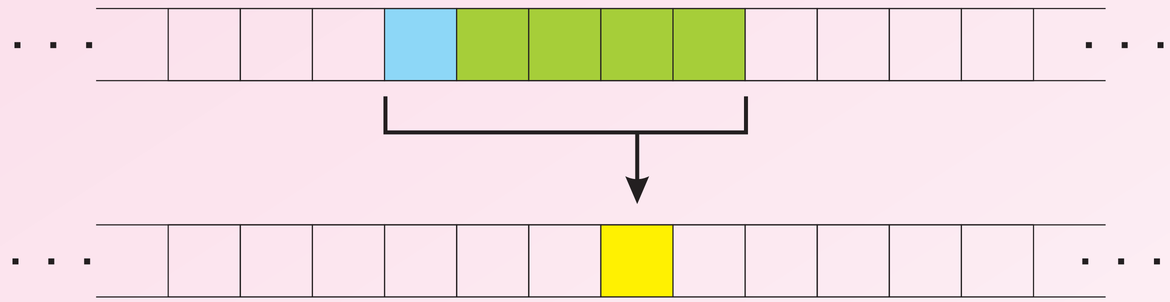
A CA is **left permutive** it has a local rule F with the property that changing the state of the leftmost neighbor changes the image under F.



A CA is **left permutive** it has a local rule F with the property that changing the state of the leftmost neighbor changes the image under F.



A CA is **left permutive** it has a local rule F with the property that changing the state of the leftmost neighbor changes the image under F.



Right permutive CA are defined analogously.

A CA is **permutive** if it is left or right permutive.

Example. The XOR automaton has state set $S = \{0, 1\}$, neighborhood range $m = 2$ and local rule

$$F(a, b) = a + b \pmod 2.$$

It is both left and right permutive.

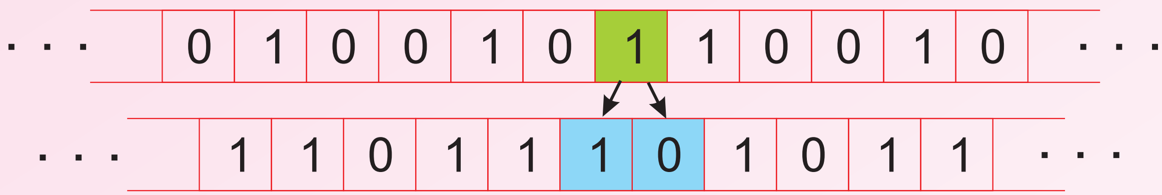
$$\cdots \; \boxed{}\boxed{0}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{1}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{} \; \cdots$$

$$\cdots \; \boxed{}\boxed{1}\boxed{1}\boxed{0}\boxed{1}\boxed{1}\boxed{1}\boxed{0}\boxed{1}\boxed{0}\boxed{1}\boxed{1}\boxed{} \; \cdots$$

Example. The XOR automaton has state set $S = \{0, 1\}$, neighborhood range $m = 2$ and local rule

$$F(a, b) = a + b \pmod 2.$$

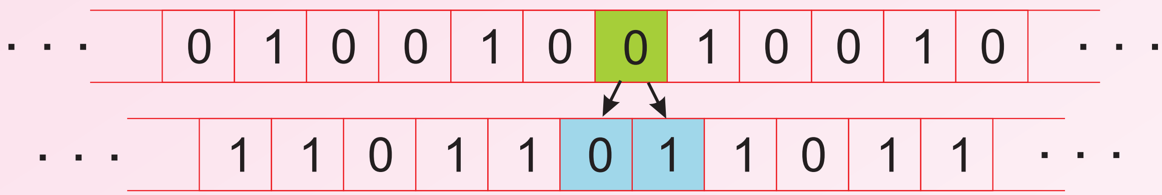
It is both left and right permutive.



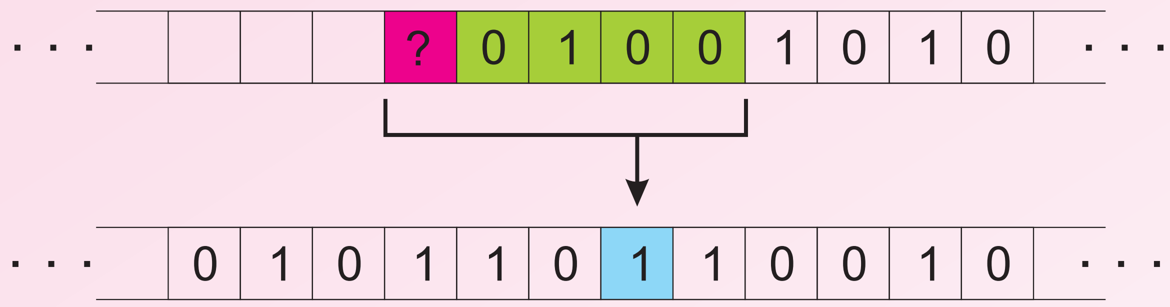
Example. The XOR automaton has state set $S = \{0, 1\}$, neighborhood range $m = 2$ and local rule

$$F(a, b) = a + b \pmod 2.$$

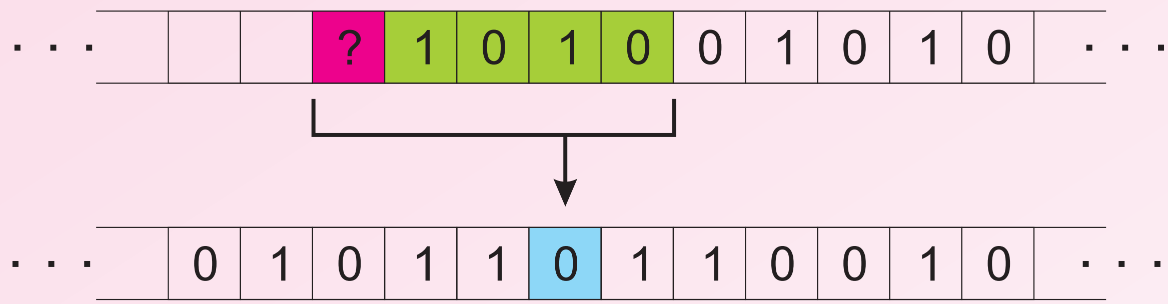
It is both left and right permutive.



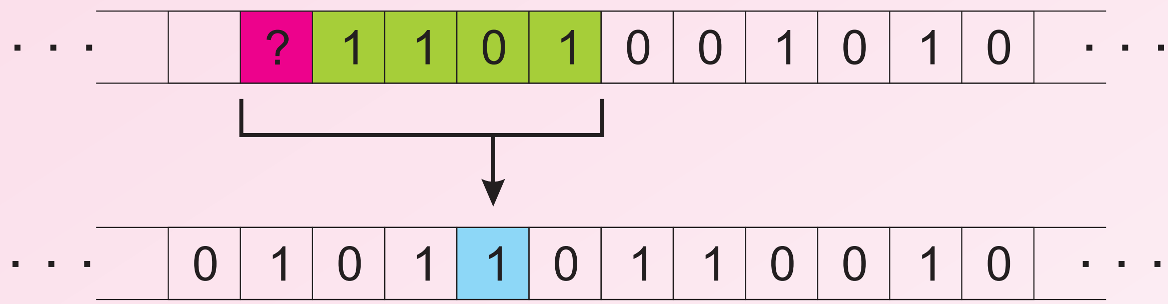
All permutive CA are surjective. A pre-image can be formed by a one-way sweep across the configuration:



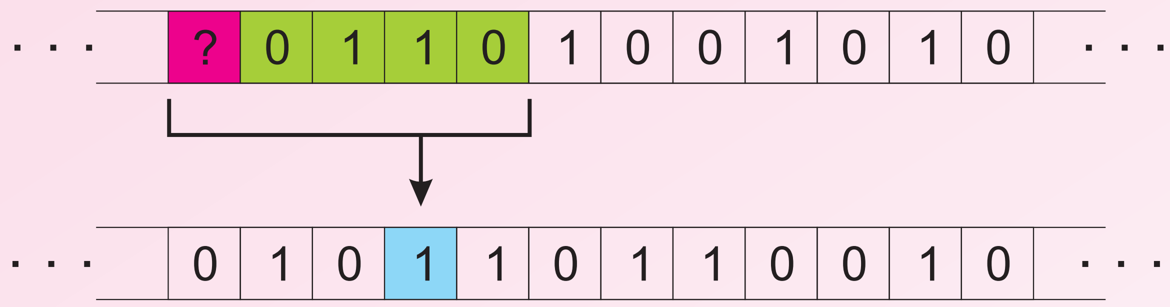
All permutive CA are surjective. A pre-image can be formed by a one-way sweep across the configuration:



All permutive CA are surjective. A pre-image can be formed by a one-way sweep across the configuration:



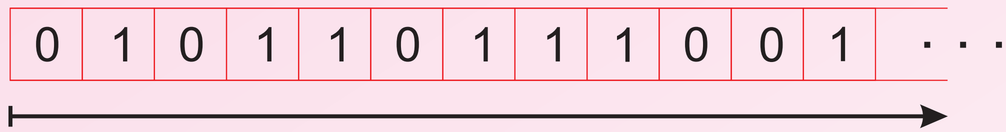
All permutive CA are surjective. A pre-image can be formed by a one-way sweep across the configuration:



Theorem. Let f be a one-dimensional surjective CA with neighborhood range $m = 2$ and with a prime number n of states. Then f is permutive.

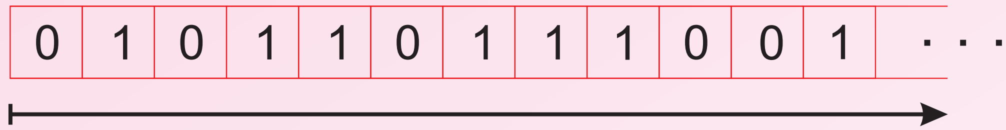
In the proof we use some old results concerning transitive configurations on surjective CA.

A right infinite $x \in S^{\mathbb{N}}$ is **transitive** if every word $w \in S^*$ occurs in it.



We define analogously transitivity of a left infinite $y \in S^{-\mathbb{N}}$.

A right infinite $x \in S^{\mathbb{N}}$ is **transitive** if every word $w \in S^*$ occurs in it.



We define analogously transitivity of a left infinite $y \in S^{-\mathbb{N}}$.

A configuration $c \in S^{\mathbb{Z}}$ is **doubly transitive** if both tails $c_{[0,\infty)}$ and $c_{(-\infty,0]}$ are transitive.

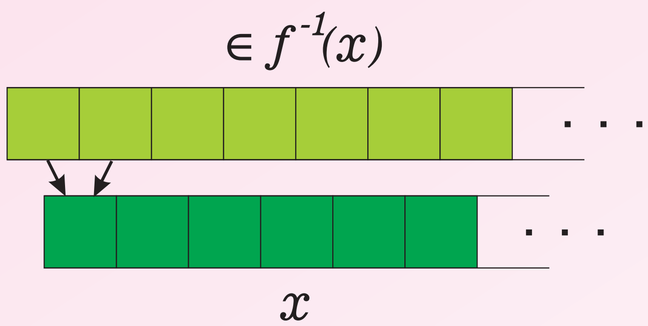
Every word appears infinitely often to the left and to the right

Let f be surjective. The following facts were proved in [Hedlund 69]:

- There exists constant $M = M(f)$ such that $|f^{-1}(c)| = M$ for all doubly transitive c.
- For all configurations c we have $|f^{-1}(c)| \geq M$.

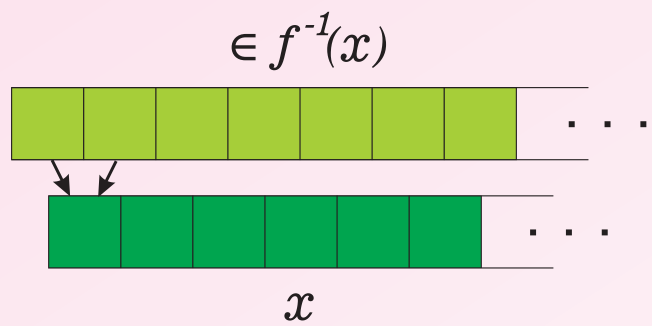
Assume neighborhood range $m = 2$.

For $x \in S^{\mathbb{N}}$ we denote by $f^{-1}(x)$ the set of right-infinite configurations that are mapped to x by the local rule:

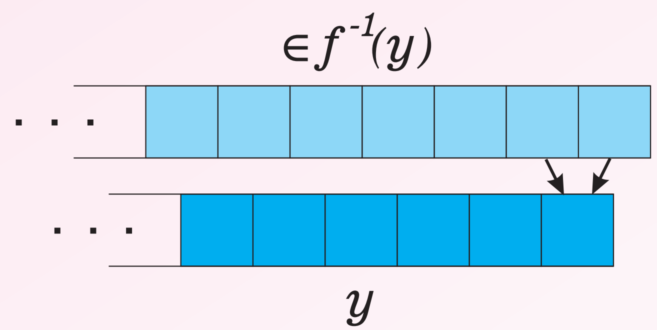


Assume neighborhood range $m = 2$.

For $x \in S^{\mathbb{N}}$ we denote by $f^{-1}(x)$ the set of right-infinite configurations that are mapped to x by the local rule:

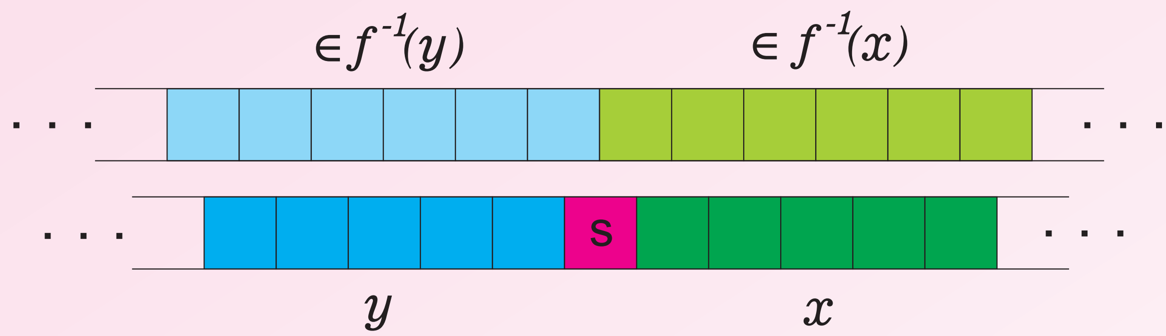


Analogously, for left-infinite $y \in S^{-\mathbb{N}}$ we define $f^{-1}(y)$:



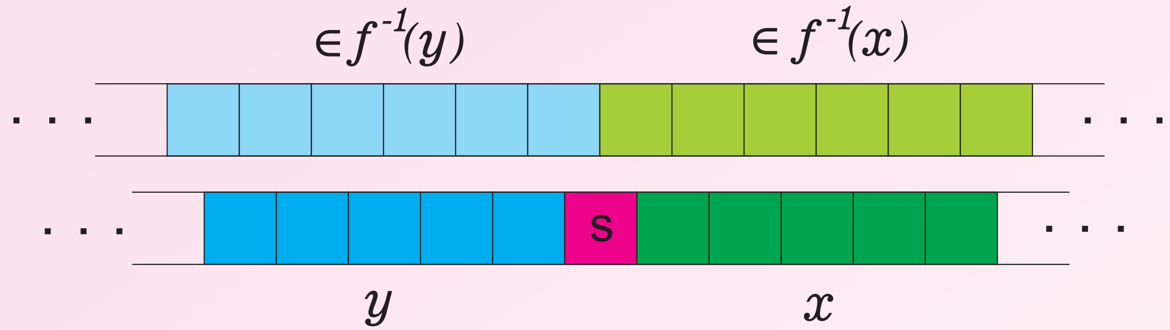
For any fixed transitive $y \in S^{-\mathbb{N}}$ and $x \in S^{\mathbb{N}}$ let us count the pre-images of the configurations in

$$A = ySx.$$



For any fixed transitive $y \in S^{-\mathbb{N}}$ and $x \in S^{\mathbb{N}}$ let us count the pre-images of the configurations in

$$A = ySx.$$

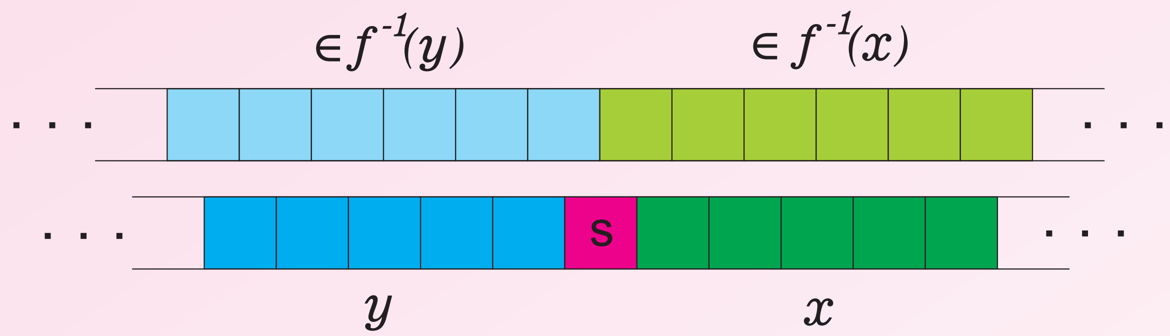


All elements of A are doubly transitive and $|A| = n$ so

$$|f^{-1}(A)| = nM.$$

For any fixed transitive $y \in S^{-\mathbb{N}}$ and $x \in S^{\mathbb{N}}$ let us count the pre-images of the configurations in

$$A = ySx.$$



All elements of A are doubly transitive and $|A| = n$ so

$$|f^{-1}(A)| = nM.$$

But $f^{-1}(A)$ consists of exactly the concatenations of $f^{-1}(y)$ and $f^{-1}(x)$ so also

$$|f^{-1}(A)| = |f^{-1}(y)| \cdot |f^{-1}(x)|.$$

We have

$$|f^{-1}(y)| \cdot |f^{-1}(x)| = nM.$$

Conclusion: all transitive $x \in S^{\mathbb{N}}$ have the same number L of pre-images, and all transitive $y \in S^{-\mathbb{N}}$ have the same number R of pre-images, and

$$LR = nM.$$

We have

$$|f^{-1}(y)| \cdot |f^{-1}(x)| = nM.$$

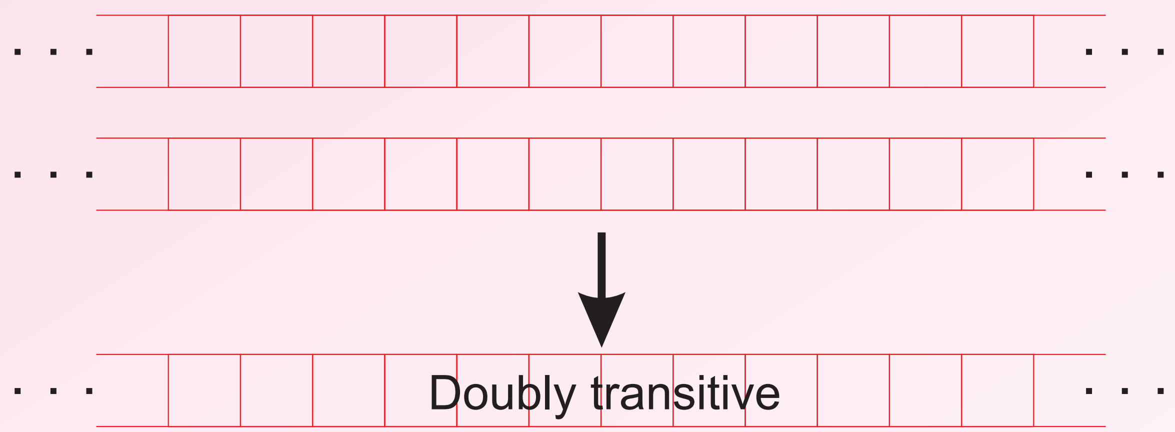
Conclusion: all transitive $x \in S^{\mathbb{N}}$ have the same number L of pre-images, and all transitive $y \in S^{-\mathbb{N}}$ have the same number R of pre-images, and

$$LR = nM.$$

Observe that if n is prime then it divides L or R.

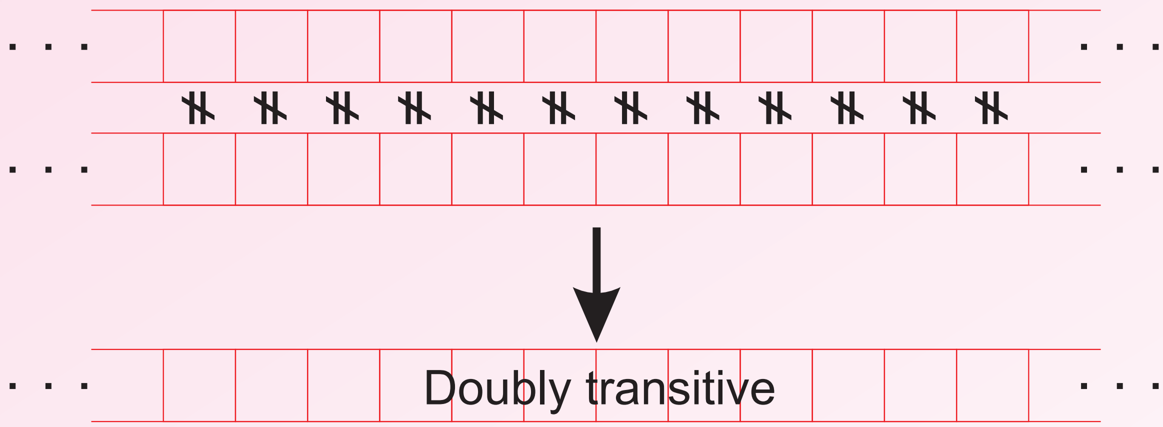
From [Hedlund 69] we also know the following, if the neighborhood range is $m = 2$:

- If c, e are different configurations such that $f(c) = f(e)$ is doubly transitive then $c_i \neq e_i$ for all $i \in \mathbb{Z}$.



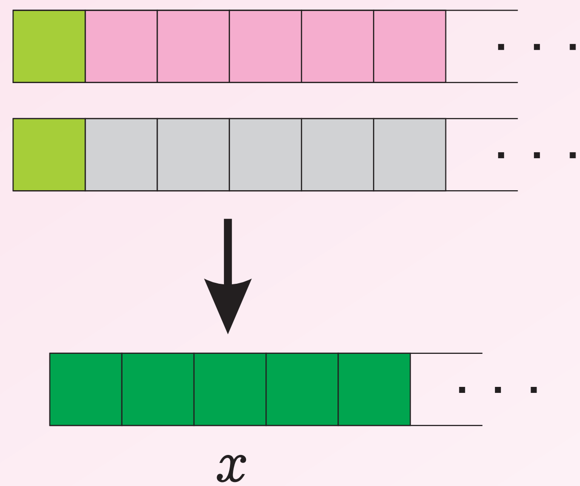
From [Hedlund 69] we also know the following, if the neighborhood range is $m = 2$:

- If c, e are different configurations such that $f(c) = f(e)$ is doubly transitive then $c_i \neq e_i$ for all $i \in \mathbb{Z}$.



- If c, e are different configurations such that $f(c) = f(e)$ is doubly transitive then $c_i \neq e_i$ for all $i \in \mathbb{Z}$.

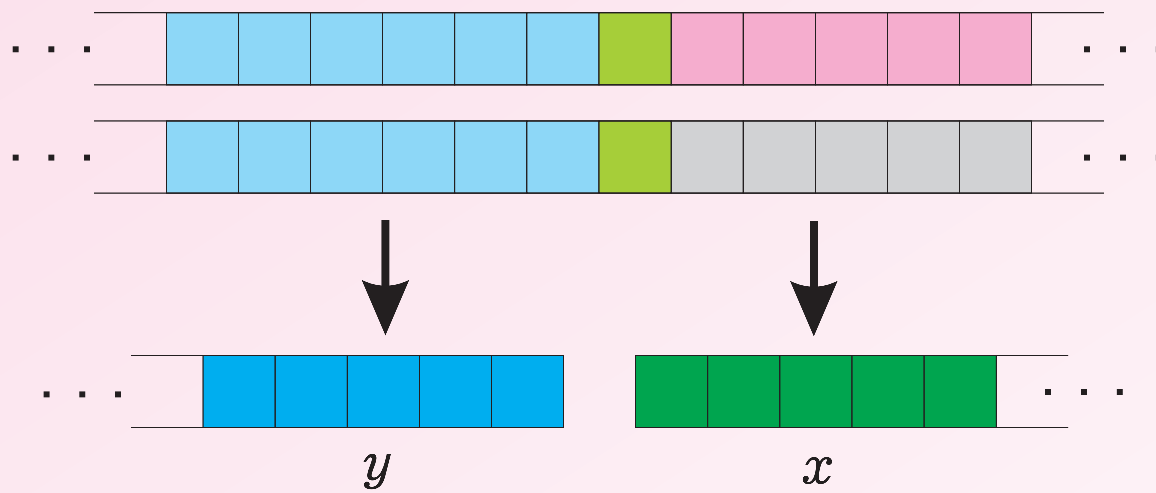
It follows that $L \leq n$: Assume, in contrary, that transitive $x \in S^{\mathbb{N}}$ has more than n pre-images.



Then two of the pre-images start with the same symbol.

- If c, e are different configurations such that $f(c) = f(e)$ is doubly transitive then $c_i \neq e_i$ for all $i \in \mathbb{Z}$.

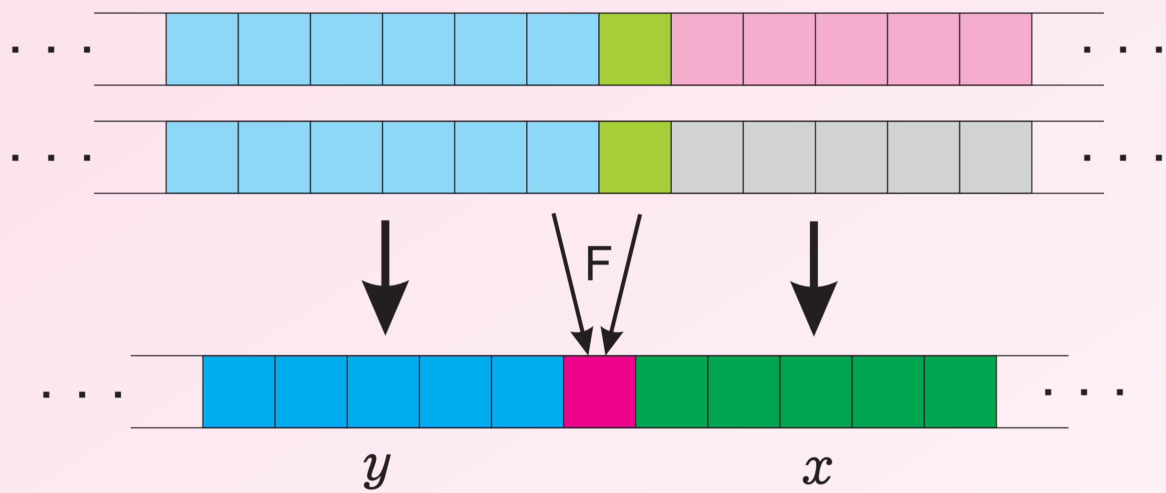
It follows that $L \leq n$: Assume, in contrary, that transitive $x \in S^{\mathbb{N}}$ has more than n pre-images.



Concatenate on the left a left-infinite sequence whose image y is transitive.

- If c, e are different configurations such that $f(c) = f(e)$ is doubly transitive then $c_i \neq e_i$ for all $i \in \mathbb{Z}$.

It follows that $L \leq n$: Assume, in contrary, that transitive $x \in S^{\mathbb{N}}$ has more than n pre-images.



We get a contradiction with [Hedlund 69]: the two configurations have the same doubly transitive image.

We have

$$\begin{aligned} LR &= nM, \\ L, R &\leq n \end{aligned}$$

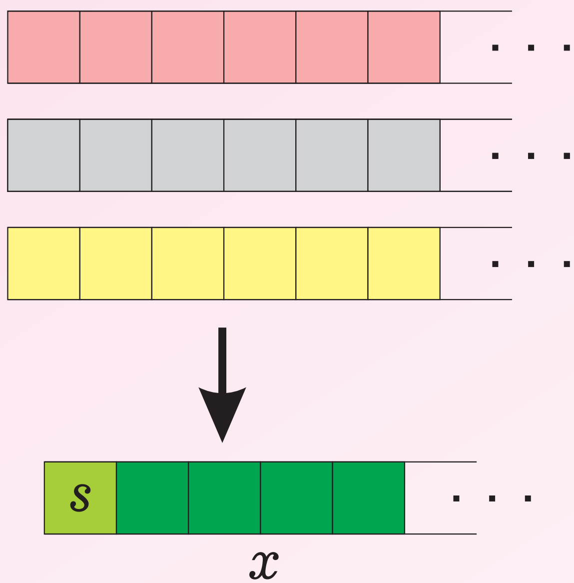
We have

$$\begin{aligned} LR &= nM, \\ L, R &\leq n \end{aligned}$$

Conclusion: If n is a prime number then $L = n$ or $R = n$.

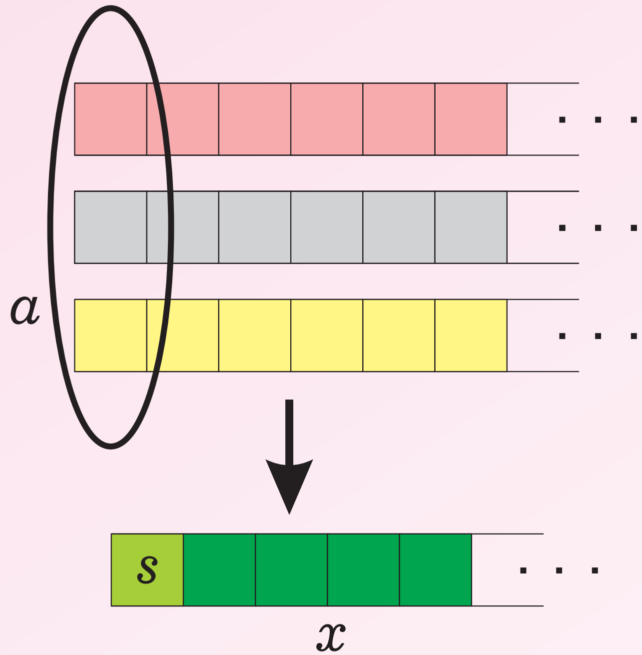
Assume $L = n$. Let $x \in S^{\mathbb{N}}$ be transitive.

For every $s \in S$ the sequence sx is transitive, so it has n pre-images, all beginning with a different symbol.



Assume $L = n$. Let $x \in S^{\mathbb{N}}$ be transitive.

For every $s \in S$ the sequence sx is transitive, so it has n pre-images, all beginning with a different symbol.



Hence sx has pre-images beginning with all $a \in S$.

Conclusion: For all $s, a \in S$ there exists $b \in S$ such that $F(a, b) = s$. The CA is **right permutive.** $\square$

m \ n	2	3	4	5	6	7	8	9	...
2	P	P		P		P			
3									
4									
5									
⋮									

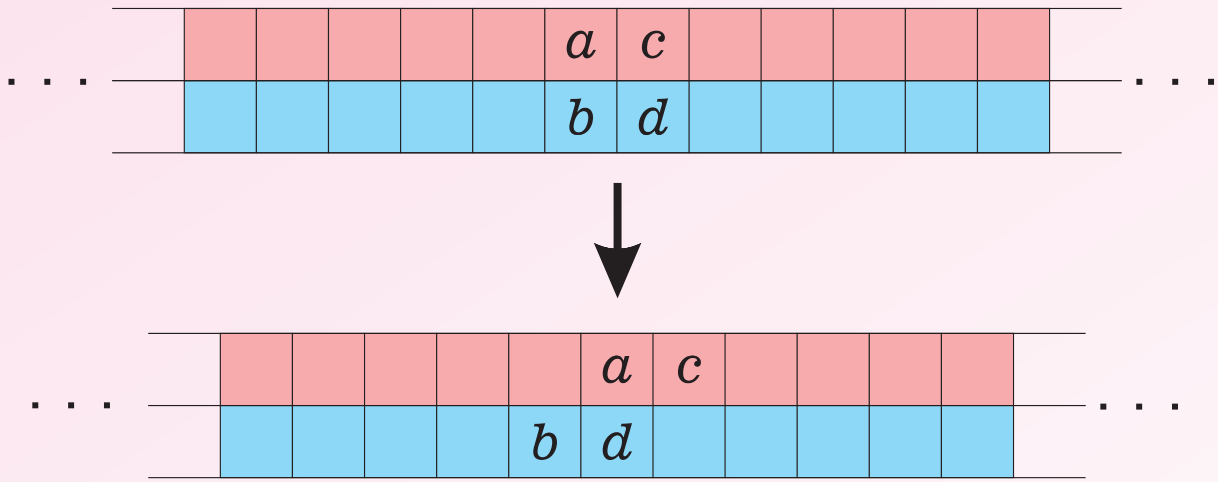
m \ n	2	3	4	5	6	7	8	9	⋯
2	P	P		P		P			
3									
4									
5									
⋮									

What about when $n = pq$ is composite ?

Construct two track CA with p and q symbols on the tracks, respectively. Local rule

$$((a, b), (c, d)) \mapsto (a, d)$$

translates the tracks in opposite directions. The CA is reversible but not left or right permutive.



m \ n	2	3	4	5	6	7	8	9	. . .
2	P	P		P		P			
3									
4									
5									
⋮									

m \ n	2	3	4	5	6	7	8	9	…
2	P	P		P		P			
3									
4									
5									
⋮									

What about bigger neighborhood ranges m ?

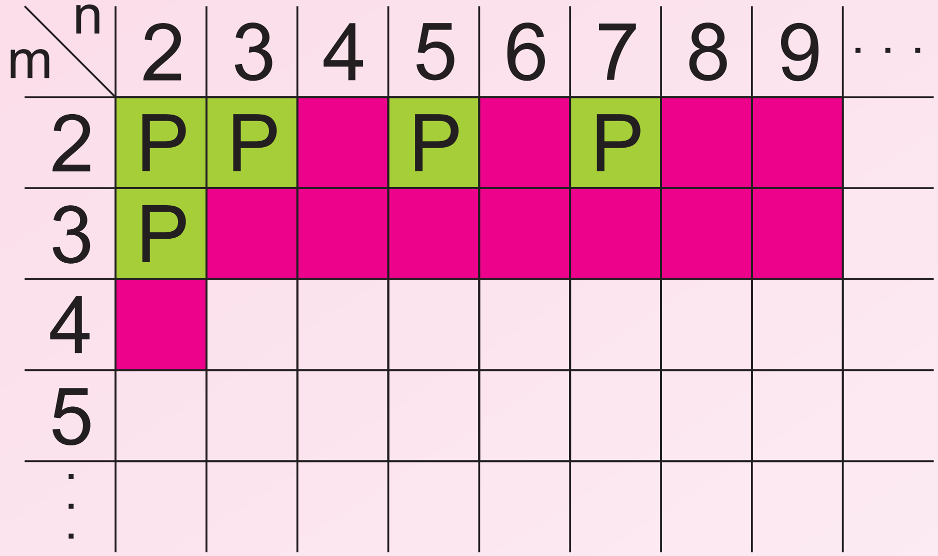
m \ n	2	3	4	5	6	7	8	9	...
2	P	P		P		P			
3	P								
4									
5									
⋮									

All surjective elementary CA are permutive.

m \ n	2	3	4	5	6	7	8	9	...
2	P	P		P		P			
3	P								
4									
5									
⋮									

With two states $n = 2$ and range $m = 4$ we have a non-permutive reversible CA:

Flip bit x in pattern $1x01$



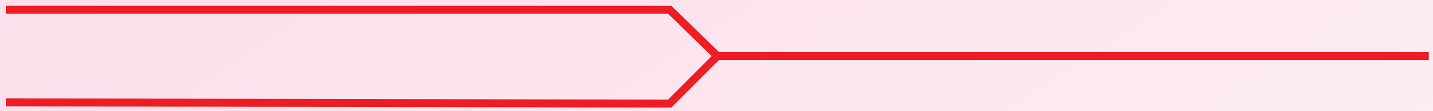
Also with $n > 2$ and $m = 3$ there exist non-permutive CA.

m \ n	2	3	4	5	6	7	8	9	...
2	P	P		P		P			
3	P								
4									
5									
⋮									

Hence the table is complete.

Two configurations $x, y \in S^{\mathbb{Z}}$ are **right-asymptotic** if for some k

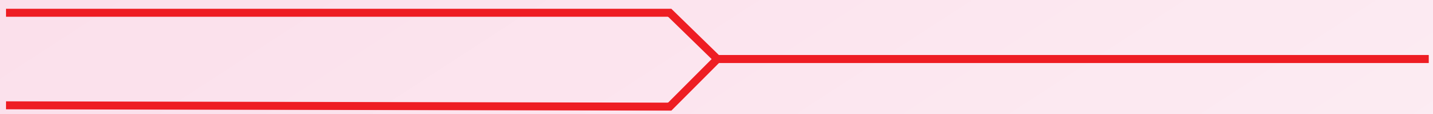
$$x_{[k,\infty)} = y_{[k,\infty)}$$



CA $f : S^{\mathbb{Z}} \longrightarrow S^{\mathbb{Z}}$ is **left-closing** if all distinct right-asymptotic configurations have distinct images.

Two configurations $x, y \in S^{\mathbb{Z}}$ are **right-asymptotic** if for some k

$$x_{[k,\infty)} = y_{[k,\infty)}$$



CA $f : S^{\mathbb{Z}} \longrightarrow S^{\mathbb{Z}}$ is **left-closing** if all distinct right-asymptotic configurations have distinct images.

Right-closingness is defined analogously.

A CA is called **closing** if it is left or right closing.

Easy to see:

- All left permutive CA are left-closing, as are all reversible CA.
- All left-closing CA are surjective.

m \ n	2	3	4	5	6	7	8	9	...
2	P	P		P		P			
3	P								
4	C								
5	?								
⋮	⋮								
11									
⋮	⋮								

A computer search shows that in case $n = 2$ and range $m = 4$ all surjective CA are closing.

With range $m = 11$ an example of a two state non-closing surjective CA can be constructed.

m \ n	2	3	4	5	6	7	8	9	…
2	P	P		P		P			
3	P								
4	C								
5	?								
⋮	⋮								
11									
⋮	⋮								

Other examples complete the table…

…except that: two state automata with ranges $5 \leq m \leq 10$ remain **open.**

m \ n	2	3	4	5	6	7	8	9	...
2	P	P		P		P			
3	P								
4	C								
5	?								
⋮	⋮								
11									
⋮	⋮								

Other examples complete the table...

...except that: two state automata with ranges $5 \leq m \leq 10$ remain **open.**

Thank You