An Introduction to Symbolic Dynamics

Michel Coornaert

IRMA, Université de Strasbourg

Galatasaray University, Istanbul

General Notation

General Notation

$$\mathbb{Z} := \{\ldots, -1, 0, 1, 2, \ldots\}$$

is the set of integers.

General Notation

$$\mathbb{Z} := \{\dots, -1, 0, 1, 2, \dots\}$$

is the set of integers.
Given $m, n \in \mathbb{Z}$, we write

$$[m, n] := \{k \in \mathbb{Z} \mid m \leq k \leq n\}.$$

General Notation

$$\mathbb{Z} := \{\dots, -1, 0, 1, 2, \dots\}$$

is the set of integers.
Given $m, n \in \mathbb{Z}$, we write

$$[m, n] := \{k \in \mathbb{Z} |\ m \leq k \leq n\}.$$

$$\mathbb{N} := \{0, 1, 2, \dots\}$$

is the set of non-negative integers.

General Notation

$$\mathbb{Z} := \{\dots, -1, 0, 1, 2, \dots\}$$

is the set of integers.
Given $m, n \in \mathbb{Z}$, we write

$$[m, n] := \{k \in \mathbb{Z} |\ m \leq k \leq n\}.$$

$$\mathbb{N} := \{0, 1, 2, \dots\}$$

is the set of non-negative integers.
Given a map $f : X \to Y$ and a subset $Z \subset X$,

General Notation

$$\mathbb{Z} := \{\dots, -1, 0, 1, 2, \dots\}$$

is the set of integers.
Given $m, n \in \mathbb{Z}$, we write

$$[m, n] := \{k \in \mathbb{Z} | \ m \leq k \leq n\}.$$

$$\mathbb{N} := \{0, 1, 2, \dots\}$$

is the set of non-negative integers.
Given a map $f\colon X \to Y$ and a subset $Z \subset X$, the restriction of f to Z is the map $f|_Z\colon Z \to Y$ defined by $f|_Z(z) = f(z)$ for all $z \in Z$.

General Notation

$$\mathbb{Z} := \{\dots, -1, 0, 1, 2, \dots\}$$

is the set of integers.
Given $m, n \in \mathbb{Z}$, we write

$$[m, n] := \{k \in \mathbb{Z} | \ m \leq k \leq n\}.$$

$$\mathbb{N} := \{0, 1, 2, \dots\}$$

is the set of non-negative integers.
Given a map $f \colon X \to Y$ and a subset $Z \subset X$, the restriction of f to Z is the map $f|_Z \colon Z \to Y$ defined by $f|_Z(z) = f(z)$ for all $z \in Z$.
Given a map $f \colon X \to X$, we write $\mathrm{Fix}(f) := \{x \in X | \ f(x) = x\}$.

General Notation

$$\mathbb{Z} := \{\dots, -1, 0, 1, 2, \dots\}$$

is the set of integers.
Given $m, n \in \mathbb{Z}$, we write

$$[m, n] := \{k \in \mathbb{Z} | \ m \leq k \leq n\}.$$

$$\mathbb{N} := \{0, 1, 2, \dots\}$$

is the set of non-negative integers.
Given a map $f \colon X \to Y$ and a subset $Z \subset X$, the restriction of f to Z is the map $f|_Z \colon Z \to Y$ defined by $f|_Z(z) = f(z)$ for all $z \in Z$.
Given a map $f \colon X \to X$, we write $\mathrm{Fix}(f) := \{x \in X | \ f(x) = x\}$.
If X is a finite set, $|X|$ denotes the cardinality of X.

Configurations

Configurations

A is a finite set, called the alphabet.

Configurations

A is a finite set, called the alphabet.

$$A^{\mathbb{Z}} = \{x \colon \mathbb{Z} \to A\}$$

is called the set of configurations (over the alphabet A).

Configurations

A is a finite set, called the alphabet.

$$A^{\mathbb{Z}} = \{x \colon \mathbb{Z} \to A\}$$

is called the set of configurations (over the alphabet A).
Thus, a configuration $x \in A^{\mathbb{Z}}$ is a bi-infinite sequence

$$\dots x(-1)x(0)x(1)x(2)\dots$$

whose terms are elements of A.

A is a finite set, called the alphabet.

$$A^{\mathbb{Z}} = \{x \colon \mathbb{Z} \to A\}$$

is called the set of configurations (over the alphabet A).
Thus, a configuration $x \in A^{\mathbb{Z}}$ is a bi-infinite sequence

$$\dots x(-1)x(0)x(1)x(2)\dots$$

whose terms are elements of A.

Exercise 1

Show that if $|A| \geq 2$ then $A^{\mathbb{Z}}$ is uncountable.

The Topology on $A^{\mathbb{Z}}$

The Topology on $A^{\mathbb{Z}}$

Given configurations $x, y \in A^{\mathbb{Z}}$, we put

$$v(x, y) \coloneqq \sup\{n \in \mathbb{N} | \; x|_{[-n+1, n-1]} = y|_{[-n+1, n-1]}\}.$$

The Topology on $A^{\mathbb{Z}}$

Given configurations $x, y \in A^{\mathbb{Z}}$, we put

$$v(x, y) := \sup\{n \in \mathbb{N} \mid x|_{[-n+1,n-1]} = y|_{[-n+1,n-1]}\}.$$

Thus $v(x, y) \in \mathbb{N} \cup \{\infty\}$.

The Topology on $A^{\mathbb{Z}}$

Given configurations $x, y \in A^{\mathbb{Z}}$, we put

$$v(x,y) \coloneqq \sup\{n \in \mathbb{N} | \; x|_{[-n+1,n-1]} = y|_{[-n+1,n-1]}\}.$$

Thus $v(x,y) \in \mathbb{N} \cup \{\infty\}$.
We define $d(x,y)$ by

$$d(x,y) \coloneqq 2^{-v(x,y)},$$

where we use the convention $2^{-\infty} = 0$.

The Topology on $A^{\mathbb{Z}}$

Given configurations $x, y \in A^{\mathbb{Z}}$, we put

$$v(x,y) \coloneqq \sup\{n \in \mathbb{N} \mid x|_{[-n+1,n-1]} = y|_{[-n+1,n-1]}\}.$$

Thus $v(x,y) \in \mathbb{N} \cup \{\infty\}$.
We define $d(x,y)$ by

$$d(x,y) \coloneqq 2^{-v(x,y)},$$

where we use the convention $2^{-\infty} = 0$.
Thus

$$d(x,y) \in \{0, 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots\}.$$

The Topology on $A^{\mathbb{Z}}$

Given configurations $x, y \in A^{\mathbb{Z}}$, we put

$$v(x,y) \coloneqq \sup\{n \in \mathbb{N} \mid x|_{[-n+1,n-1]} = y|_{[-n+1,n-1]}\}.$$

Thus $v(x,y) \in \mathbb{N} \cup \{\infty\}$.
We define $d(x,y)$ by

$$d(x,y) \coloneqq 2^{-v(x,y)},$$

where we use the convention $2^{-\infty} = 0$.
Thus

$$d(x,y) \in \{0, 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots\}.$$

We have that $d(x,y) = \dfrac{1}{2^n}$ if and only if

$$(x(k) = y(k) \quad \forall k \in [-n+1, n-1]) \text{ and } (x(n) \neq y(n) \text{ or } x(-n) \neq y(-n)).$$

The Topology on $A^{\mathbb{Z}}$ (continued)

The Topology on $A^{\mathbb{Z}}$ (continued)

Proposition 1

d is a metric on $A^{\mathbb{Z}}$.

The Topology on $A^{\mathbb{Z}}$ (continued)

Proposition 1

d is a metric on $A^{\mathbb{Z}}$.

Proof.

Since the other properties are obvious, it suffices to check that d satisfies the triangle inequality.

Proposition 1

d is a metric on $A^{\mathbb{Z}}$.

Proof.

Since the other properties are obvious, it suffices to check that d satisfies the triangle inequality.
For all $x, y, z \in A^{\mathbb{Z}}$, we have that

$$v(x, y) \geq \min(v(x, z), v(z, y)).$$

The Topology on $A^{\mathbb{Z}}$ (continued)

Proposition 1

d is a metric on $A^{\mathbb{Z}}$.

Proof.

Since the other properties are obvious, it suffices to check that d satisfies the triangle inequality.
For all $x, y, z \in A^{\mathbb{Z}}$, we have that

$$v(x, y) \geq \min(v(x, z), v(z, y)).$$

This implies

$$d(x, y) \leq \max(d(x, z), d(z, y)) \quad \text{(ultrametric inequality)}$$

The Topology on $A^{\mathbb{Z}}$ (continued)

Proposition 1

d is a metric on $A^{\mathbb{Z}}$.

Proof.

Since the other properties are obvious, it suffices to check that d satisfies the triangle inequality.
For all $x, y, z \in A^{\mathbb{Z}}$, we have that

$$v(x, y) \geq \min(v(x, z), v(z, y)).$$

This implies

$$d(x, y) \leq \max(d(x, z), d(z, y)) \quad \text{(ultrametric inequality)}$$

and hence

$$d(x, y) \leq d(x, z) + d(z, y) \quad \text{(triangle inequality)}.$$

□

Proposition 1

d is a metric on $A^{\mathbb{Z}}$.

Proof.

Since the other properties are obvious, it suffices to check that d satisfies the triangle inequality.
For all $x, y, z \in A^{\mathbb{Z}}$, we have that

$$v(x, y) \geq \min(v(x, z), v(z, y)).$$

This implies

$$d(x, y) \leq \max(d(x, z), d(z, y)) \quad \text{(ultrametric inequality)}$$

and hence

$$d(x, y) \leq d(x, z) + d(z, y) \quad \text{(triangle inequality).}$$

□

We equip $A^{\mathbb{Z}}$ with the topology defined by d.

The Topology on $A^{\mathbb{Z}}$ (continued)

Proposition 1

d is a metric on $A^{\mathbb{Z}}$.

Proof.

Since the other properties are obvious, it suffices to check that d satisfies the triangle inequality.
For all $x, y, z \in A^{\mathbb{Z}}$, we have that

$$v(x, y) \geq \min(v(x, z), v(z, y)).$$

This implies

$$d(x, y) \leq \max(d(x, z), d(z, y)) \quad \text{(ultrametric inequality)}$$

and hence

$$d(x, y) \leq d(x, z) + d(z, y) \quad \text{(triangle inequality).}$$

□

We equip $A^{\mathbb{Z}}$ with the topology defined by d. This topology is called the prodiscrete topology on $A^{\mathbb{Z}}$.

The Topology on $A^{\mathbb{Z}}$ (continued)

The Topology on $A^{\mathbb{Z}}$ (continued)

Exercise 2

Let $x \in A^{\mathbb{Z}}$. Show that the sets

$$V_n(x) := \{y \in A^{\mathbb{Z}} \mid \; x|_{[-n,n]} = y|_{[-n,n]}\},$$

with n running over $\mathbb{N}$, form a base of neighborhoods of x. Show that each $V_n(x)$ is both closed and open in $A^{\mathbb{Z}}$.

Exercise 2

Let $x \in A^{\mathbb{Z}}$. Show that the sets

$$V_n(x) := \{y \in A^{\mathbb{Z}} \mid \; x|_{[-n,n]} = y|_{[-n,n]}\},$$

with n running over $\mathbb{N}$, form a base of neighborhoods of x. Show that each $V_n(x)$ is both closed and open in $A^{\mathbb{Z}}$.

Exercise 3

Show that if $|A| \geq 2$ then $A^{\mathbb{Z}}$ has no isolated points.

The Topology on $A^{\mathbb{Z}}$ (continued)

Exercise 2

Let $x \in A^{\mathbb{Z}}$. Show that the sets

$$V_n(x) := \{y \in A^{\mathbb{Z}} \mid x|_{[-n,n]} = y|_{[-n,n]}\},$$

with n running over $\mathbb{N}$, form a base of neighborhoods of x. Show that each $V_n(x)$ is both closed and open in $A^{\mathbb{Z}}$.

Exercise 3

Show that if $|A| \geq 2$ then $A^{\mathbb{Z}}$ has no isolated points.

Exercise 4

Show that a sequence $(x_n)_{n\in\mathbb{N}}$ of elements of $A^{\mathbb{Z}}$ converges to $y \in A^{\mathbb{Z}}$ if and only if

$$\forall k \in \mathbb{Z}, \exists n_0 = n_0(k) \in \mathbb{N} \text{ such that } n \geq n_0 \implies x_n(k) = y(k).$$

The Topology on $A^{\mathbb{Z}}$ (continued)

Exercise 2

Let $x \in A^{\mathbb{Z}}$. Show that the sets

$$V_n(x) := \{y \in A^{\mathbb{Z}} \mid x|_{[-n,n]} = y|_{[-n,n]}\},$$

with n running over $\mathbb{N}$, form a base of neighborhoods of x. Show that each $V_n(x)$ is both closed and open in $A^{\mathbb{Z}}$.

Exercise 3

Show that if $|A| \geq 2$ then $A^{\mathbb{Z}}$ has no isolated points.

Exercise 4

Show that a sequence $(x_n)_{n\in\mathbb{N}}$ of elements of $A^{\mathbb{Z}}$ converges to $y \in A^{\mathbb{Z}}$ if and only if

$$\forall k \in \mathbb{Z}, \exists n_0 = n_0(k) \in \mathbb{N} \text{ such that } n \geq n_0 \implies x_n(k) = y(k).$$

Exercise 5

Show that $A^{\mathbb{Z}}$ is compact.

The Topology on $A^{\mathbb{Z}}$ (continued)

Exercise 6

For $k \in \mathbb{Z}$, let $\pi_k \colon A^{\mathbb{Z}} \to A$ be the map defined by $\pi_k(x) = x(k)$ for all $x \in A^{\mathbb{Z}}$. Equip A with its discrete topology. Show that the topology on $A^{\mathbb{Z}}$ is the coarsest topology on $A^{\mathbb{Z}}$ such that all maps π_k are continuous.

The Topology on $A^{\mathbb{Z}}$ (continued)

Exercise 6

For $k \in \mathbb{Z}$, let $\pi_k \colon A^{\mathbb{Z}} \to A$ be the map defined by $\pi_k(x) = x(k)$ for all $x \in A^{\mathbb{Z}}$. Equip A with its discrete topology. Show that the topology on $A^{\mathbb{Z}}$ is the coarsest topology on $A^{\mathbb{Z}}$ such that all maps π_k are continuous.

Exercise 7

Show that $A^{\mathbb{Z}}$ is totally disconnected, that is, every non-empty connected subset of $A^{\mathbb{Z}}$ is reduced to a single configuration.

The Shift on $A^{\mathbb{Z}}$

The Shift on $A^{\mathbb{Z}}$

The shift on $A^{\mathbb{Z}}$ is the map

$$\begin{aligned}\sigma \colon A^{\mathbb{Z}} &\to A^{\mathbb{Z}} \\ x &\mapsto \sigma(x) = y,\end{aligned}$$

where

$$y(k) = x(k-1) \quad \forall k \in \mathbb{Z}.$$

The Shift on $A^{\mathbb{Z}}$

The shift on $A^{\mathbb{Z}}$ is the map

$$\begin{aligned} \sigma \colon A^{\mathbb{Z}} &\to A^{\mathbb{Z}} \\ x &\mapsto \sigma(x) = y, \end{aligned}$$

where

$$y(k) = x(k-1) \quad \forall k \in \mathbb{Z}.$$

Example

Here $A = \{0, 1\}$.

$$\begin{aligned} x &= \dots 11100101001101110000100011 \dots \text{ then} \\ \sigma(x) &= \dots ?1110010100110111000010001 \dots \end{aligned}$$

The Shift on $A^{\mathbb{Z}}$ (continued)

The Shift on $A^{\mathbb{Z}}$ (continued)

The shift σ is bijective with inverse map

$$\begin{aligned}\sigma^{-1}\colon A^{\mathbb{Z}} &\to A^{\mathbb{Z}} \\ x &\mapsto \sigma^{-1}(x) = z,\end{aligned}$$

where

$$z(k) = x(k+1) \quad \forall k \in \mathbb{Z}.$$

The Shift on $A^{\mathbb{Z}}$ (continued)

The shift σ is bijective with inverse map

$$\begin{aligned} \sigma^{-1}\colon A^{\mathbb{Z}} &\to A^{\mathbb{Z}} \\ x &\mapsto \sigma^{-1}(x) = z, \end{aligned}$$

where

$$z(k) = x(k+1) \quad \forall k \in \mathbb{Z}.$$

Example

Here $A = \{0, 1\}$.

$$\begin{aligned} x &= \dots 111001010011011100001000 11 \dots \text{ then} \\ \sigma^{-1}(x) &= \dots 11001010011011100001000 11? \dots \end{aligned}$$

The Shift on $A^{\mathbb{Z}}$ (continued)

The Shift on $A^{\mathbb{Z}}$ (continued)

Proposition 2

The shift $\sigma \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a homeomorphism.

The Shift on $A^{\mathbb{Z}}$ (continued)

Proposition 2

The shift $\sigma\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a homeomorphism.

Proof.

Observe that

$$v(x,y) - 1 \leq v(\sigma(x), \sigma(y)) \leq v(x,y) + 1$$

so that

$$\frac{1}{2} d(x,y) \leq d(\sigma(x), \sigma(y)) \leq 2d(x,y)$$

for all $x, y \in A^{\mathbb{Z}}$. □

The Shift on $A^{\mathbb{Z}}$ (continued)

The Shift on $A^{\mathbb{Z}}$ (continued)

Exercise 8

Let $n \geq 1$ be an integer. Show that $\mathrm{Fix}(\sigma^n)$ *is finite and has cardinality* $|\mathrm{Fix}(\sigma^n)| = |A|^n$.

Exercise 8

Let $n \geq 1$ be an integer. Show that $\mathrm{Fix}(\sigma^n)$ is finite and has cardinality $|\mathrm{Fix}(\sigma^n)| = |A|^n$.

One says that a configuration $x \in A^{\mathbb{Z}}$ is periodic if there exists an integer $n \geq 1$ such that $x \in \mathrm{Fix}(\sigma^n)$.

The Shift on $A^{\mathbb{Z}}$ (continued)

Exercise 8

Let $n \geq 1$ be an integer. Show that $\mathrm{Fix}(\sigma^n)$ is finite and has cardinality $|\mathrm{Fix}(\sigma^n)| = |A|^n$.

One says that a configuration $x \in A^{\mathbb{Z}}$ is periodic if there exists an integer $n \geq 1$ such that $x \in \mathrm{Fix}(\sigma^n)$.

Exercise 9

Show that the set of periodic configurations is a countable dense subset of $A^{\mathbb{Z}}$.

Exercise 8

Let $n \geq 1$ be an integer. Show that $\mathrm{Fix}(\sigma^n)$ *is finite and has cardinality* $|\mathrm{Fix}(\sigma^n)| = |A|^n$.

One says that a configuration $x \in A^{\mathbb{Z}}$ is periodic if there exists an integer $n \geq 1$ such that $x \in \mathrm{Fix}(\sigma^n)$.

Exercise 9

Show that the set of periodic configurations is a countable dense subset of $A^{\mathbb{Z}}$.

Exercise 10

Show that there exists $x \in A^{\mathbb{Z}}$ *whose positive* σ*-orbit* $\{\sigma^n(x) | n \geq 1\}$ *is dense in* $A^{\mathbb{Z}}$.

Cellular Automata

Definition

A map $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton

Definition

A map $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton if there exists a finite subset $M \subset \mathbb{Z}$ and a map $A^M \to A$ such that

$$(\tau(x))(k) = \mu((\sigma^{-k}(x))|_M) \quad \forall k \in \mathbb{Z}.$$

Definition

A map $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton if there exists a finite subset $M \subset \mathbb{Z}$ and a map $A^M \to A$ such that

$$(\tau(x))(k) = \mu((\sigma^{-k}(x))|_M) \quad \forall k \in \mathbb{Z}.$$

Such a set M is called a memory set for τ and μ is the associated local defining map.

Definition

A map $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton if there exists a finite subset $M \subset \mathbb{Z}$ and a map $A^M \to A$ such that

$$(\tau(x))(k) = \mu((\sigma^{-k}(x))|_M) \quad \forall k \in \mathbb{Z}.$$

Such a set M is called a memory set for τ and μ is the associated local defining map.

Let $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton with memory set M. Then:

Definition

A map $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton if there exists a finite subset $M \subset \mathbb{Z}$ and a map $A^M \to A$ such that

$$(\tau(x))(k) = \mu((\sigma^{-k}(x))|_M) \quad \forall k \in \mathbb{Z}.$$

Such a set M is called a memory set for τ and μ is the associated local defining map.

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton with memory set M. Then:

- if $x \in A^{\mathbb{Z}}$, then the value of $\tau(x)$ at $k \in \mathbb{Z}$ only depends on $x|_{k+M}$;

Definition

A map $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton if there exists a finite subset $M \subset \mathbb{Z}$ and a map $A^M \to A$ such that

$$(\tau(x))(k) = \mu((\sigma^{-k}(x))|_M) \quad \forall k \in \mathbb{Z}.$$

Such a set M is called a memory set for τ and μ is the associated local defining map.

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton with memory set M. Then:

- if $x \in A^{\mathbb{Z}}$, then the value of $\tau(x)$ at $k \in \mathbb{Z}$ only depends on $x|_{k+M}$;
- the local defining map $\mu \colon A^M \to A$ is entirely determined by τ and M;

Definition

A map $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton if there exists a finite subset $M \subset \mathbb{Z}$ and a map $A^M \to A$ such that

$$(\tau(x))(k) = \mu((\sigma^{-k}(x))|_M) \quad \forall k \in \mathbb{Z}.$$

Such a set M is called a memory set for τ and μ is the associated local defining map.

Let $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton with memory set M. Then:

- if $x \in A^{\mathbb{Z}}$, then the value of $\tau(x)$ at $k \in \mathbb{Z}$ only depends on $x|_{k+M}$;
- the local defining map $\mu\colon A^M \to A$ is entirely determined by τ and M;
- every finite subset of $\mathbb{Z}$ containing M is also a memory set for τ;

Definition

A map $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton if there exists a finite subset $M \subset \mathbb{Z}$ and a map $A^M \to A$ such that

$$(\tau(x))(k) = \mu((\sigma^{-k}(x))|_M) \quad \forall k \in \mathbb{Z}.$$

Such a set M is called a memory set for τ and μ is the associated local defining map.

Let $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton with memory set M. Then:

- if $x \in A^{\mathbb{Z}}$, then the value of $\tau(x)$ at $k \in \mathbb{Z}$ only depends on $x|_{k+M}$;
- the local defining map $\mu\colon A^M \to A$ is entirely determined by τ and M;
- every finite subset of $\mathbb{Z}$ containing M is also a memory set for τ;
- if M_1 and M_2 are memory sets for τ, then $M_1 \cap M_2$ is also a memory set for τ;

Definition

A map $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton if there exists a finite subset $M \subset \mathbb{Z}$ and a map $A^M \to A$ such that

$$(\tau(x))(k) = \mu((\sigma^{-k}(x))|_M) \quad \forall k \in \mathbb{Z}.$$

Such a set M is called a memory set for τ and μ is the associated local defining map.

Let $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton with memory set M. Then:

- if $x \in A^{\mathbb{Z}}$, then the value of $\tau(x)$ at $k \in \mathbb{Z}$ only depends on $x|_{k+M}$;
- the local defining map $\mu\colon A^M \to A$ is entirely determined by τ and M;
- every finite subset of $\mathbb{Z}$ containing M is also a memory set for τ;
- if M_1 and M_2 are memory sets for τ, then $M_1 \cap M_2$ is also a memory set for τ;
- there is a unique memory set for τ with minimal cardinality. This memory set is called the minimal memory set of τ. It is contained in every memory set of τ.

Example 1

Example 1

Take $A := \{0, 1\}$ and consider the map $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by

Example 1

Take $A := \{0,1\}$ and consider the map $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by

$$(\tau(x))(k) := x(k) \cdot x(k+1) = \begin{cases} 1 & \text{if } x(k) = x(k+1) = 1, \\ 0 & \text{otherwise} \end{cases} \quad \forall x \in A^{\mathbb{Z}}, k \in \mathbb{Z}.$$

Example 1

Take $A := \{0, 1\}$ and consider the map $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by

$$(\tau(x))(k) := x(k) \cdot x(k+1) = \begin{cases} 1 & \text{if } x(k) = x(k+1) = 1, \\ 0 & \text{otherwise} \end{cases} \quad \forall x \in A^{\mathbb{Z}}, k \in \mathbb{Z}.$$

For example, if

$$x = \ldots 11100101001101110000100011 \ldots \text{ then}$$
$$\tau(x) = \ldots 1100000000100110000000001? \ldots$$

Example 1

Take $A := \{0,1\}$ and consider the map $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by

$$(\tau(x))(k) := x(k) \cdot x(k+1) = \begin{cases} 1 & \text{if } x(k) = x(k+1) = 1, \\ 0 & \text{otherwise} \end{cases} \qquad \forall x \in A^{\mathbb{Z}}, k \in \mathbb{Z}.$$

For example, if

$$x = \dots 11100101001101110000100011 \dots \text{ then}$$
$$\tau(x) = \dots 11000000001001100000000001? \dots$$

τ is a cellular automaton

Example 1

Take $A := \{0, 1\}$ and consider the map $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by

$$(\tau(x))(k) := x(k) \cdot x(k+1) = \begin{cases} 1 & \text{if } x(k) = x(k+1) = 1, \\ 0 & \text{otherwise} \end{cases} \quad \forall x \in A^{\mathbb{Z}}, k \in \mathbb{Z}.$$

For example, if

$$\begin{aligned} x &= \ldots 11100101001101110000100011 \ldots \text{ then} \\ \tau(x) &= \ldots 1100000000100110000000001? \ldots \end{aligned}$$

τ is a cellular automaton with minimal memory set $M = \{0, 1\}$ and local defining map $\mu\colon A^M = A^2 \to A$ given by

$$00 \mapsto 0, \quad 01 \mapsto 0, \quad 10 \mapsto 0, \quad 11 \mapsto 1.$$

Example 2

Example 2

Take $A := \{0,1\}$ and $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by

Example 2

Take $A := \{0,1\}$ and $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by

$$(\tau(x))(k) := x(k) + x(k+1) \mod 2 \quad \forall x \in A^{\mathbb{Z}}, k \in \mathbb{Z}.$$

Example 2

Take $A := \{0, 1\}$ and $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by

$$(\tau(x))(k) := x(k) + x(k+1) \mod 2 \quad \forall x \in A^{\mathbb{Z}}, k \in \mathbb{Z}.$$

For example, if

$$x = \ldots 11100101001101110000100011 \ldots \text{ then}$$
$$\tau(x) = \ldots 0010111101011001000110010? \ldots$$

Example 2

Take $A := \{0, 1\}$ and $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by

$$(\tau(x))(k) := x(k) + x(k+1) \quad \text{mod } 2 \quad \forall x \in A^{\mathbb{Z}}, k \in \mathbb{Z}.$$

For example, if

$$x = \ldots 11100101001101110000100011 \ldots \text{ then}$$
$$\tau(x) = \ldots 0010111101011001000110010? \ldots$$

τ is a cellular automaton

Example 2

Take $A := \{0,1\}$ and $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ given by

$$(\tau(x))(k) := x(k) + x(k+1) \quad \mod 2 \quad \forall x \in A^{\mathbb{Z}}, k \in \mathbb{Z}.$$

For example, if

$$x = \ldots 1110010100110111000010001 1\ldots \text{ then}$$
$$\tau(x) = \ldots 001011110101100100011001 0?\ldots$$

τ is a cellular automaton with minimal memory set $M = \{0,1\}$ and local defining map $\mu\colon A^M = A^2 \to A$ given by

$$00 \mapsto 0, \quad 01 \mapsto 1, \quad 10 \mapsto 1, \quad 11 \mapsto 0.$$

Example 3

Example 3

Take $A := \{(\text{shape}, \text{color})\}$, where

Example 3

Take $A \coloneqq \{(\text{shape}, \text{color})\}$, where

$$\text{shape} \in \{\text{square}, \text{disc}\} \quad \text{color} \in \{\text{green}, \text{red}, \text{yellow}\}.$$

Example 3

Take $A := \{(\text{shape}, \text{color})\}$, where

$$\text{shape} \in \{\text{square}, \text{disc}\} \quad \text{color} \in \{\text{green}, \text{red}, \text{yellow}\}.$$

Thus the alphabet A has cardinality $2 \times 3 = 6$.

Example 3

Take $A := \{(\text{shape}, \text{color})\}$, where

$$\text{shape} \in \{\text{square}, \text{disc}\} \quad \text{color} \in \{\text{green}, \text{red}, \text{yellow}\}.$$

Thus the alphabet A has cardinality $2 \times 3 = 6$. The map $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$, defined by

$$\text{shape}((\tau(x))(k)) = \text{shape}(x(k-1)) \quad \text{color}((\tau(x))(k)) = \text{color}(x(k+1)) \quad \forall x \in A^{\mathbb{Z}}, k \in \mathbb{Z},$$

Example 3

Take $A := \{(\text{shape}, \text{color})\}$, where

$$\text{shape} \in \{\text{square}, \text{disc}\} \quad \text{color} \in \{\text{green}, \text{red}, \text{yellow}\}.$$

Thus the alphabet A has cardinality $2 \times 3 = 6$. The map $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$, defined by

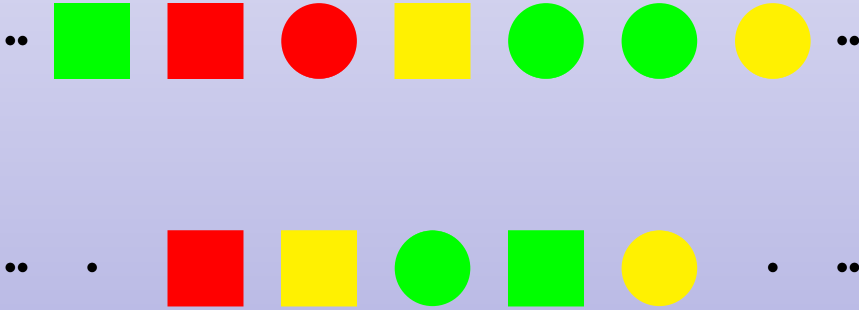
$$\text{shape}((\tau(x))(k)) = \text{shape}(x(k-1)) \quad \text{color}((\tau(x))(k)) = \text{color}(x(k+1)) \quad \forall x \in A^{\mathbb{Z}}, k \in \mathbb{Z},$$

is a cellular automaton with minimal memory set $M = \{-1, 1\}$.

Example 3 (continued)

$x :=$

$\tau(x) =$



Topological Characterization of Cellular Automata

Theorem 1 (Curtis-Hedlund-Lyndon Theorem)

Let $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a map. Then the following conditions are equivalent:

(a) *τ is a cellular automaton;*

(b) *τ is continuous and $\sigma \circ \tau = \tau \circ \sigma$.*

Topological Characterization of Cellular Automata (continued)

Topological Characterization of Cellular Automata (continued)

A subset $X \subset A^{\mathbb{Z}}$ is called a subshift if X is closed in $A^{\mathbb{Z}}$ and $\sigma(X) = X$.

Topological Characterization of Cellular Automata (continued)

A subset $X \subset A^{\mathbb{Z}}$ is called a subshift if X is closed in $A^{\mathbb{Z}}$ and $\sigma(X) = X$.

Corollary 1

If $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton, then $\tau(A^{\mathbb{Z}})$ is a subshift.

Topological Characterization of Cellular Automata (continued)

A subset $X \subset A^{\mathbb{Z}}$ is called a subshift if X is closed in $A^{\mathbb{Z}}$ and $\sigma(X) = X$.

Corollary 1

If $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton, then $\tau(A^{\mathbb{Z}})$ is a subshift.

Corollary 2

Let $\tau_1, \tau_2 \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be cellular automata. Then $\tau_1 \circ \tau_2$ is a cellular automaton.

Topological Characterization of Cellular Automata (continued)

A subset $X \subset A^{\mathbb{Z}}$ is called a subshift if X is closed in $A^{\mathbb{Z}}$ and $\sigma(X) = X$.

Corollary 1

If $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is a cellular automaton, then $\tau(A^{\mathbb{Z}})$ is a subshift.

Corollary 2

Let $\tau_1, \tau_2 \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be cellular automata. Then $\tau_1 \circ \tau_2$ is a cellular automaton.

Corollary 3

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a bijective cellular automaton. Then $\tau^{-1} \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is also a cellular automaton.

Topological Characterization of Cellular Automata (continued)

Exercise 11

Show that the image of the cellular automaton in Example 1 is the subshift $X \subset \{0,1\}^{\mathbb{Z}}$ *consisting of all configurations* $x \in \{0,1\}^{\mathbb{Z}}$ *such that* $(x(k), x(k+1), x(k+2)) \neq (1,0,1)$ *for every* $k \in \mathbb{Z}$.

Exercise 11

Show that the image of the cellular automaton in Example 1 is the subshift $X \subset \{0,1\}^{\mathbb{Z}}$ *consisting of all configurations* $x \in \{0,1\}^{\mathbb{Z}}$ *such that* $(x(k), x(k+1), x(k+2)) \neq (1,0,1)$ *for every* $k \in \mathbb{Z}$.

Exercise 12

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ *be a cellular automaton and let* $n \geq 1$ *be an integer. Show that* $\tau(\mathrm{Fix}(\sigma^n)) \subset \mathrm{Fix}(\sigma^n)$.

Exercise 11

Show that the image of the cellular automaton in Example 1 is the subshift $X \subset \{0,1\}^{\mathbb{Z}}$ *consisting of all configurations* $x \in \{0,1\}^{\mathbb{Z}}$ *such that* $(x(k), x(k+1), x(k+2)) \neq (1,0,1)$ *for every* $k \in \mathbb{Z}$.

Exercise 12

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ *be a cellular automaton and let* $n \geq 1$ *be an integer. Show that* $\tau(\mathrm{Fix}(\sigma^n)) \subset \mathrm{Fix}(\sigma^n)$.

Exercise 13

Let $\tau_1, \tau_2 \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ *be cellular automata. Show that if* M_1 *is a memory set for* τ_1 *and* M_2 *is a memory set for* τ_2*, then* $M_1 + M_2$ *is a memory set for* $\tau_1 \circ \tau_2$.

Pre-injectivity

Pre-injectivity

One says that the configurations $x, y \in A^{\mathbb{Z}}$ are almost equal and one writes $x \sim y$ if the set

$$\{k \in \mathbb{Z} | \; x(k) \neq y(k)\}$$

is finite.

Pre-injectivity

One says that the configurations $x, y \in A^{\mathbb{Z}}$ are almost equal and one writes $x \sim y$ if the set

$$\{k \in \mathbb{Z} | \ x(k) \neq y(k)\}$$

is finite.
$\sim$ is an equivalence relation on $A^{\mathbb{Z}}$.

Pre-injectivity

One says that the configurations $x, y \in A^{\mathbb{Z}}$ are almost equal and one writes $x \sim y$ if the set

$$\{k \in \mathbb{Z} |\ x(k) \neq y(k)\}$$

is finite.
$\sim$ is an equivalence relation on $A^{\mathbb{Z}}$.

Definition

One says that a cellular automaton $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is pre-injective if the restriction of τ to each equivalence class of $\sim$ is injective.

The Garden of Eden Theorem

The following theorem is due to Moore [Mo-1963] and Myhill [My-1963].

The Garden of Eden Theorem

The following theorem is due to Moore [Mo-1963] and Myhill [My-1963].

Theorem 2 (Garden of Eden Theorem)

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton. Then

$$\tau \text{ surjective} \iff \tau \text{ pre-injective.}$$

The Garden of Eden Theorem

The following theorem is due to Moore [Mo-1963] and Myhill [My-1963].

Theorem 2 (Garden of Eden Theorem)

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton. Then

$$\tau \text{ surjective} \iff \tau \text{ pre-injective.}$$

- $\Longrightarrow$ is due to Moore,

The Garden of Eden Theorem

The following theorem is due to Moore [Mo-1963] and Myhill [My-1963].

Theorem 2 (Garden of Eden Theorem)

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ *be a cellular automaton. Then*

$$\tau \text{ surjective} \iff \tau \text{ pre-injective.}$$

- $\Longrightarrow$ is due to Moore,
- $\Longleftarrow$ is due to Myhill.

The Garden of Eden Theorem

The following theorem is due to Moore [Mo-1963] and Myhill [My-1963].

Theorem 2 (Garden of Eden Theorem)

Let $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton. Then

$$\tau \text{ surjective} \iff \tau \text{ pre-injective.}$$

- $\Longrightarrow$ is due to Moore,
- $\Longleftarrow$ is due to Myhill.

Exercise 14

Show that the cellular automaton in Example 1 is not pre-injective (and hence not injective). Show directly that it is not surjective.

The Garden of Eden Theorem

The following theorem is due to Moore [Mo-1963] and Myhill [My-1963].

Theorem 2 (Garden of Eden Theorem)

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton. Then

$$\tau \text{ surjective} \iff \tau \text{ pre-injective.}$$

- $\Longrightarrow$ is due to Moore,
- $\Longleftarrow$ is due to Myhill.

Exercise 14

Show that the cellular automaton in Example 1 is not pre-injective (and hence not injective). Show directly that it is not surjective.

Exercise 15

Show that the cellular automaton in Example 2 is pre-injective but not injective. Show directly that it is surjective.

The Garden of Eden Theorem

The following theorem is due to Moore [Mo-1963] and Myhill [My-1963].

Theorem 2 (Garden of Eden Theorem)

Let $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton. Then

$$\tau \text{ surjective} \iff \tau \text{ pre-injective.}$$

- $\Longrightarrow$ is due to Moore,
- $\Longleftarrow$ is due to Myhill.

Exercise 14

Show that the cellular automaton in Example 1 is not pre-injective (and hence not injective). Show directly that it is not surjective.

Exercise 15

Show that the cellular automaton in Example 2 is pre-injective but not injective. Show directly that it is surjective.

Exercise 16

Show that the cellular automaton in Example 3 is injective (and hence pre-injective). Show directly that it is surjective.

The Garden of Eden Theorem (continued)

The Garden of Eden Theorem (continued)

As injectivity implies pre-injectivity, an immediate consequence of the GOE theorem is the following.

The Garden of Eden Theorem (continued)

As injectivity implies pre-injectivity, an immediate consequence of the GOE theorem is the following.

Corollary 4

Every injective cellular automaton $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ *is surjective (and hence bijective).*

As injectivity implies pre-injectivity, an immediate consequence of the GOE theorem is the following.

Corollary 4

Every injective cellular automaton $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ is surjective (and hence bijective).

Exercise 17 (An alternative proof)

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be an injective cellular automaton. Use Exercise 8 and Exercise 12 to prove that $\tau(\mathrm{Fix}(\sigma^n)) = \mathrm{Fix}(\sigma^n)$ for every integer $n \geq 1$. Use Exercise 9 to conclude that τ is surjective.

Proof of the Garden of Eden Theorem

Proof of the Garden of Eden Theorem

Let $X \subset A^{\mathbb{Z}}$ such that $\sigma(X) = X$.

Proof of the Garden of Eden Theorem

Let $X \subset A^{\mathbb{Z}}$ such that $\sigma(X) = X$.
For every integer $n \geq 1$, we write

$$X_n := \{x|_{[1,n]} \mid x \in X\}.$$

Proof of the Garden of Eden Theorem

Let $X \subset A^{\mathbb{Z}}$ such that $\sigma(X) = X$.
For every integer $n \geq 1$, we write

$$X_n := \{x|_{[1,n]} \mid x \in X\}.$$

Lemma 1

$$|X_{n+m}| \leq |X_n| \cdot |X_m|$$

for all integers $n, m \geq 1$.

Let $X \subset A^{\mathbb{Z}}$ such that $\sigma(X) = X$.
For every integer $n \geq 1$, we write

$$X_n := \{x|_{[1,n]} \mid x \in X\}.$$

Lemma 1

$$|X_{n+m}| \leq |X_n| \cdot |X_m|$$

for all integers $n, m \geq 1$.

Definition

The entropy of X is

$$\text{ent}(X) := \lim_{n\to\infty} \frac{\log |X_n|}{n}.$$

Proof of the Garden of Eden Theorem (continued)

Proof of the Garden of Eden Theorem (continued)

Remark

The limit in the definition of $\text{ent}(X)$ is a true limit since the sequence $(\log |X_n|)_{n \geq 1}$ is subadditive by Lemma 1.

Proof of the Garden of Eden Theorem (continued)

Remark

The limit in the definition of $\text{ent}(X)$ is a true limit since the sequence $(\log |X_n|)_{n \geq 1}$ is subadditive by Lemma 1.

Remark

We always have $\text{ent}(X) \leq \log |A|$ since $|X_n| \leq |A|^n$ and hence $\log |X_n| \leq n \log |A|$.

Proof of the Garden of Eden Theorem (continued)

Proof of the Garden of Eden Theorem (continued)

We shall prove the following more general version of the GOE theorem.

Proof of the Garden of Eden Theorem (continued)

We shall prove the following more general version of the GOE theorem.

Theorem 3

Let $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton and let $X := \tau(A^{\mathbb{Z}})$ denote the image of τ. Then the following conditions are equivalent:

(a) τ *is surjective;*

(b) $\mathrm{ent}(X) = \log |A|$*;*

(c) τ *is pre-injective.*

We shall prove the following more general version of the GOE theorem.

Theorem 3

Let $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton and let $X := \tau(A^{\mathbb{Z}})$ denote the image of τ. Then the following conditions are equivalent:

(a) τ *is surjective;*

(b) $\mathrm{ent}(X) = \log |A|$;

(c) τ *is pre-injective.*

Proof. We can assume $|A| \geq 2$.

Proof of the Garden of Eden Theorem (continued)

We shall prove the following more general version of the GOE theorem.

Theorem 3

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton and let $X := \tau(A^{\mathbb{Z}})$ denote the image of τ. Then the following conditions are equivalent:

(a) τ *is surjective;*

(b) $\mathrm{ent}(X) = \log |A|$;

(c) τ *is pre-injective.*

Proof. We can assume $|A| \geq 2$.
(a) $\implies$ (b).

Proof of the Garden of Eden Theorem (continued)

We shall prove the following more general version of the GOE theorem.

Theorem 3

Let $\tau\colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton and let $X := \tau(A^{\mathbb{Z}})$ denote the image of τ. Then the following conditions are equivalent:

(a) *τ is surjective;*

(b) $\mathrm{ent}(X) = \log |A|$*;*

(c) *τ is pre-injective.*

Proof. We can assume $|A| \geq 2$.
(a) $\implies$ (b). Suppose that τ is surjective, that is, $X = A^{\mathbb{Z}}$.

Proof of the Garden of Eden Theorem (continued)

We shall prove the following more general version of the GOE theorem.

Theorem 3

Let $\tau \colon A^{\mathbb{Z}} \to A^{\mathbb{Z}}$ be a cellular automaton and let $X := \tau(A^{\mathbb{Z}})$ denote the image of τ. Then the following conditions are equivalent:

(a) *τ is surjective;*

(b) $\text{ent}(X) = \log|A|$;

(c) *τ is pre-injective.*

Proof. We can assume $|A| \geq 2$.
(a) $\implies$ (b). Suppose that τ is surjective, that is, $X = A^{\mathbb{Z}}$. Then $X_n = A^n$, so that

$$\text{ent}(X) = \lim_{n\to\infty} \frac{\log|X_n|}{n} = \lim_{n\to\infty} \frac{\log|A^n|}{n} = \lim_{n\to\infty} \frac{n\log|A|}{n} = \log|A|.$$

Proof of the Garden of Eden Theorem (continued)

Proof of the Garden of Eden Theorem (continued)

(b) $\implies$ (a).
Suppose that τ is not surjective.

Proof of the Garden of Eden Theorem (continued)

(b) $\implies$ (a).
Suppose that τ is not surjective.
As X is a closed subset of $A^{\mathbb{Z}}$ (cf. Corollary 1), the set $A^{\mathbb{Z}} \setminus X$ is a non-empty open subset of $A^{\mathbb{Z}}$.

Proof of the Garden of Eden Theorem (continued)

(b) $\implies$ (a).
Suppose that τ is not surjective.
As X is a closed subset of $A^{\mathbb{Z}}$ (cf. Corollary 1), the set $A^{\mathbb{Z}} \setminus X$ is a non-empty open subset of $A^{\mathbb{Z}}$. Consequently, there exists an integer $n \geq 1$ such that X_n is a proper subset of A^n, so that $|X_n| \leq |A|^n - 1$.

Proof of the Garden of Eden Theorem (continued)

(b) $\implies$ (a).
Suppose that τ is not surjective.
As X is a closed subset of $A^{\mathbb{Z}}$ (cf. Corollary 1), the set $A^{\mathbb{Z}} \setminus X$ is a non-empty open subset of $A^{\mathbb{Z}}$. Consequently, there exists an integer $n \geq 1$ such that X_n is a proper subset of A^n, so that $|X_n| \leq |A|^n - 1$.
For every integer $i \geq 1$, we then have

$$|X_{in}| \leq |X_n|^i \leq (|A|^n - 1)^i = |A|^{in} \left(1 - \frac{1}{|A|^n}\right)^i.$$

Proof of the Garden of Eden Theorem (continued)

(b) $\implies$ (a).
Suppose that τ is not surjective.
As X is a closed subset of $A^{\mathbb{Z}}$ (cf. Corollary 1), the set $A^{\mathbb{Z}} \setminus X$ is a non-empty open subset of $A^{\mathbb{Z}}$. Consequently, there exists an integer $n \geq 1$ such that X_n is a proper subset of A^n, so that $|X_n| \leq |A|^n - 1$.
For every integer $i \geq 1$, we then have

$$|X_{in}| \leq |X_n|^i \leq (|A|^n - 1)^i = |A|^{in} \left(1 - \frac{1}{|A|^n}\right)^i.$$

This implies

$$\mathrm{ent}(X) = \lim_{i \to \infty} \frac{\log |X_{in}|}{in} \leq \log |A| + \frac{1}{n} \log \left(1 - \frac{1}{|A|^n}\right) < \log |A|.$$

Proof of the Garden of Eden Theorem (continued)

(c) $\implies$ (b).

Proof of the Garden of Eden Theorem (continued)

(c) $\implies$ (b).
Suppose that (b) is not satisfied, i.e., $\text{ent}(X) < \log |A|$.

Proof of the Garden of Eden Theorem (continued)

(c) $\implies$ (b).
Suppose that (b) is not satisfied, i.e., $\text{ent}(X) < \log |A|$.
Let $m \in \mathbb{N}$ such that $[-m, m]$ is a memory set for τ.

Proof of the Garden of Eden Theorem (continued)

(c) $\implies$ (b).
Suppose that (b) is not satisfied, i.e., $\mathrm{ent}(X) < \log |A|$.
Let $m \in \mathbb{N}$ such that $[-m, m]$ is a memory set for τ.
Fix some $a_0 \in a$.

Proof of the Garden of Eden Theorem (continued)

(c) $\implies$ (b).
Suppose that (b) is not satisfied, i.e., $\mathrm{ent}(X) < \log |A|$.
Let $m \in \mathbb{N}$ such that $[-m, m]$ is a memory set for τ.
Fix some $a_0 \in a$. Let $n \geq 1$ and consider the set

$$Y := \{x \in A^{\mathbb{Z}} | \, x(k) = a_0 \quad \forall k \in \mathbb{Z} \setminus [1, n]\}.$$

(c) $\implies$ (b).
Suppose that (b) is not satisfied, i.e., $\mathrm{ent}(X) < \log |A|$.
Let $m \in \mathbb{N}$ such that $[-m, m]$ is a memory set for τ.
Fix some $a_0 \in a$. Let $n \geq 1$ and consider the set

$$Y := \{x \in A^{\mathbb{Z}} | \ x(k) = a_0 \quad \forall k \in \mathbb{Z} \setminus [1, n]\}.$$

We have that $|Y| = |A|^n$.

Proof of the Garden of Eden Theorem (continued)

(c) $\implies$ (b).
Suppose that (b) is not satisfied, i.e., $\mathrm{ent}(X) < \log |A|$.
Let $m \in \mathbb{N}$ such that $[-m, m]$ is a memory set for τ.
Fix some $a_0 \in a$. Let $n \geq 1$ and consider the set

$$Y := \{x \in A^{\mathbb{Z}} | \, x(k) = a_0 \quad \forall k \in \mathbb{Z} \setminus [1, n]\}.$$

We have that $|Y| = |A|^n$.
Observe that $|\tau(Y)| \leq |X_{n+2m}|$.

Proof of the Garden of Eden Theorem (continued)

(c) $\implies$ (b).
Suppose that (b) is not satisfied, i.e., $\text{ent}(X) < \log |A|$.
Let $m \in \mathbb{N}$ such that $[-m, m]$ is a memory set for τ.
Fix some $a_0 \in a$. Let $n \geq 1$ and consider the set

$$Y := \{x \in A^{\mathbb{Z}} | \, x(k) = a_0 \quad \forall k \in \mathbb{Z} \setminus [1, n]\}.$$

We have that $|Y| = |A|^n$.
Observe that $|\tau(Y)| \leq |X_{n+2m}|$.
As

$$\lim_{n \to \infty} \frac{\log |X_{n+2m}|}{n} = \lim_{n \to \infty} \frac{\log |X_{n+2m}|}{n + 2m} = \text{ent}(X) < \log |A|,$$

Proof of the Garden of Eden Theorem (continued)

(c) $\implies$ (b).
Suppose that (b) is not satisfied, i.e., $\mathrm{ent}(X) < \log|A|$.
Let $m \in \mathbb{N}$ such that $[-m, m]$ is a memory set for τ.
Fix some $a_0 \in a$. Let $n \geq 1$ and consider the set

$$Y := \{x \in A^{\mathbb{Z}} | \, x(k) = a_0 \quad \forall k \in \mathbb{Z} \setminus [1, n]\}.$$

We have that $|Y| = |A|^n$.
Observe that $|\tau(Y)| \leq |X_{n+2m}|$.
As

$$\lim_{n\to\infty} \frac{\log|X_{n+2m}|}{n} = \lim_{n\to\infty} \frac{\log|X_{n+2m}|}{n+2m} = \mathrm{ent}(X) < \log|A|,$$

There exists $n \geq 1$ such that

$$|X_{n+2m}| < |A|^n.$$

Proof of the Garden of Eden Theorem (continued)

(c) $\implies$ (b).
Suppose that (b) is not satisfied, i.e., $\mathrm{ent}(X) < \log|A|$.
Let $m \in \mathbb{N}$ such that $[-m, m]$ is a memory set for τ.
Fix some $a_0 \in a$. Let $n \geq 1$ and consider the set

$$Y := \{x \in A^{\mathbb{Z}} | \, x(k) = a_0 \quad \forall k \in \mathbb{Z} \setminus [1, n]\}.$$

We have that $|Y| = |A|^n$.
Observe that $|\tau(Y)| \leq |X_{n+2m}|$.
As

$$\lim_{n\to\infty} \frac{\log|X_{n+2m}|}{n} = \lim_{n\to\infty} \frac{\log|X_{n+2m}|}{n+2m} = \mathrm{ent}(X) < \log|A|,$$

There exists $n \geq 1$ such that

$$|X_{n+2m}| < |A|^n.$$

this implies $|\tau(Y)| < |Y|$.

(c) $\implies$ (b).
Suppose that (b) is not satisfied, i.e., $\text{ent}(X) < \log |A|$.
Let $m \in \mathbb{N}$ such that $[-m, m]$ is a memory set for τ.
Fix some $a_0 \in a$. Let $n \geq 1$ and consider the set

$$Y := \{x \in A^{\mathbb{Z}} | \, x(k) = a_0 \quad \forall k \in \mathbb{Z} \setminus [1, n]\}.$$

We have that $|Y| = |A|^n$.
Observe that $|\tau(Y)| \leq |X_{n+2m}|$.
As

$$\lim_{n\to\infty} \frac{\log |X_{n+2m}|}{n} = \lim_{n\to\infty} \frac{\log |X_{n+2m}|}{n+2m} = \text{ent}(X) < \log |A|,$$

There exists $n \geq 1$ such that

$$|X_{n+2m}| < |A|^n.$$

this implies $|\tau(Y)| < |Y|$.
By the pigeon-hole principle, there exist distinct configurations $y_1, y_2 \in Y$ such that $\tau(y_1) = \tau(y_2)$.

Proof of the Garden of Eden Theorem (continued)

(c) $\implies$ (b).
Suppose that (b) is not satisfied, i.e., $\text{ent}(X) < \log |A|$.
Let $m \in \mathbb{N}$ such that $[-m, m]$ is a memory set for τ.
Fix some $a_0 \in a$. Let $n \geq 1$ and consider the set

$$Y := \{x \in A^{\mathbb{Z}} | \, x(k) = a_0 \quad \forall k \in \mathbb{Z} \setminus [1, n]\}.$$

We have that $|Y| = |A|^n$.
Observe that $|\tau(Y)| \leq |X_{n+2m}|$.
As

$$\lim_{n \to \infty} \frac{\log |X_{n+2m}|}{n} = \lim_{n \to \infty} \frac{\log |X_{n+2m}|}{n+2m} = \text{ent}(X) < \log |A|,$$

There exists $n \geq 1$ such that

$$|X_{n+2m}| < |A|^n.$$

this implies $|\tau(Y)| < |Y|$.
By the pigeon-hole principle, there exist distinct configurations $y_1, y_2 \in Y$ such that $\tau(y_1) = \tau(y_2)$.
As all configurations in Y are almost equal (they coincide outside of $[1, n]$), this shows that τ is not pre-injective.

Proof of the Garden of Eden Theorem (continued)

Proof of the Garden of Eden Theorem (continued)

(b) $\Longrightarrow$ (c).

(b) $\implies$ (c).
Suppose that τ is not pre-injective.

Proof of the Garden of Eden Theorem (continued)

(b) $\implies$ (c).
Suppose that τ is not pre-injective.
Then there exist an integer $n \geq 1$ and distinct elements $p, q \in A^{[1,n]}$ that are mutually erasable, i.e., if $x, y \in A^{\mathbb{Z}}$ coincide on $\mathbb{Z} \setminus [1, n]$ and satisfy $x|_{[1,n]} = p$ and $y|_{[1,n]} = q$, then $\tau(x) = \tau(y)$.

(b) $\implies$ (c).
Suppose that τ is not pre-injective.
Then there exist an integer $n \geq 1$ and distinct elements $p, q \in A^{[1,n]}$ that are mutually erasable, i.e., if $x, y \in A^{\mathbb{Z}}$ coincide on $\mathbb{Z} \setminus [1, n]$ and satisfy $x|_{[1,n]} = p$ and $y|_{[1,n]} = q$, then $\tau(x) = \tau(y)$.
We then deduce that, for every $i \geq 1$,

$$|X_{in}| \leq (|A|^n - 1)^i \, |A|^{2m},$$

where m is such that $[-m, m]$ is a memory set for τ.

(b) $\implies$ (c).
Suppose that τ is not pre-injective.
Then there exist an integer $n \geq 1$ and distinct elements $p, q \in A^{[1,n]}$ that are mutually erasable, i.e., if $x, y \in A^{\mathbb{Z}}$ coincide on $\mathbb{Z} \setminus [1, n]$ and satisfy $x|_{[1,n]} = p$ and $y|_{[1,n]} = q$, then $\tau(x) = \tau(y)$.
We then deduce that, for every $i \geq 1$,

$$|X_{in}| \leq (|A|^n - 1)^i \, |A|^{2m},$$

where m is such that $[-m, m]$ is a memory set for τ.
This implies

$$\mathrm{ent}(X) = \lim_{i \to \infty} \frac{\log |X_{in}|}{in} \leq \log |A| + \frac{1}{n} \log \left(1 - \frac{1}{|A|^n}\right) < \log |A|.$$

Exercise 18

Compute the entropy of the image subshift of the cellular automaton in Example 1.

References

[CC-2010] T. Ceccherini-Silberstein, M. Coornaert, *Cellular automata and groups*, Springer Monographs in Mahtematics, Springer, Berlin, 2010.

[LM-1995] D. Lind, B. Marcus, *An introduction to symbolic dynamics and coding*, Cambridge University Press, Cambridge, 1995.

[Mo-1963] E. F. Moore, *Machine models of self-reproduction*, vol. 14 of Proc. Symp. Appl. Math., American Mathematical Society, Providence, 1963, pp. 17–34.

[My-1963] J. Myhill, *The converse of Moore's Garden-of-Eden theorem*, Proc. Amer. Math. Soc. **14** (1963), 685–686.