Master 2 Mathematics and Computer Science Symbolic Dynamics. Lecture 1

Marie-Pierre Béal

University Gustave Eiffel
Laboratoire d'informatique Gaspard-Monge UMR 8049

Overview

- Shift spaces. Shifts of finite type. Sofic shifts.
- Irreducible sofic shifts. Minimal deterministic presentation.

Words and languages

Let A be a finite alphabet. The elements of A are called letters or symbols.

A word on A is a finite sequence of elements of A, denoted by $a_0 a_1 \cdots a_{n-1}$.

The set of words on A is denoted by A^*, the *empty word* by ε, and he set of nonempty words by A^+.

A word u *occurs in* a word w, or is a *block* of w if $w = pus$ for some words p, s.

A *language* is a set of words.

Sequences

Let A be a finite alphabet.

A two-sided sequence is a sequence $x = (x_n)_{n\in\mathbb{Z}} \in A^{\mathbb{Z}}$.

For $i \leq j$, we write

$$x_{[i,j]} = x_i x_{i+1} \cdots x_j \text{ and } x_{[i,j)} = x_i x_{i+1} \cdots x_{j-1}.$$

A word u *occurs in* a sequence x if $u = x_{[i,j)}$ for some i, j. One also says that u is a *block* of x, and that the integer i is an *occurrence* of u in x.

Topology and shift transformation

The set $A^{\mathbb{Z}}$ of two-sided infinite sequences of elements of A is a metric space for the distance defined for $x \neq y$ by $d(x, y) = 2^{-r(x,y)}$ where

$$r(x, y) = \inf\{|n| \mid n \in \mathbb{Z}, x_n \neq y_n\}. \tag{1}$$

The topology induced by this metric coincides with the product topology on $A^{\mathbb{Z}}$, using the discrete topology on A.
Since a product of compact spaces is compact, $A^{\mathbb{Z}}$ is a compact metric space.

Let S denote the *shift transformation*, defined for $x \in A^{\mathbb{Z}}$ by $S(x) = y$ if $y_n = x_{n+1}$ for $n \in \mathbb{Z}$. It is continuous and one-to-one from $A^{\mathbb{Z}}$ to itself.

Shift spaces

A set $X \subseteq A^{\mathbb{Z}}$ is *shift-invariant* if $S(X) = X$ (or, equivalently $S^{-1}(X) = X$).

A *shift space* on the alphabet A is a subset of $A^{\mathbb{Z}}$ which is

(i) topologically closed,

(ii) shift-invariant.

For a language $F \subseteq A^*$, the set of sequences $x \in A^{\mathbb{Z}}$ such that no word of F occurs in it is denoted by X_F.

Shift spaces

Proposition

A set $X \subseteq A^{\mathbb{Z}}$ is a shift space if and only if $X = \mathsf{X}_F$ for some $F \subseteq A^*$.

Proof.

Exercise. □

Solution

Assume first that X is a shift space on A and let F be the set of words on A that do not occur in the elements of X. Then $X \subseteq \mathsf{X}_F$. Conversely, let $x \in \mathsf{X}_F$. For every $n \geq 1$, the word $x_{[-n,n]}$ is not in F and is thus a block of some $y^{(n)} \in X$. Since X is shift-invariant, we may choose $y^{(n)}$ such that $y^{(n)}_{[-n,n]} = x_{[-n,n]}$. The sequence $y^{(n)}$ converges to x, and since X is closed, this implies $x \in X$.

Conversely, consider $X = \mathsf{X}_F$. Then X is clearly closed and shift-invariant, and thus it is a shift space.

Examples

The *full shift* $A^{\mathbb{Z}}$.

The *golden mean shift* is the set X of two-sided infinite sequences on $A = \{a, b\}$ with no consecutive b.

In other terms, $X = \mathsf{X}_F$ with $F = \{bb\}$.

Shifts of finite type and sofic shifts

A *shift of finite type* is a shift $X = \mathsf{X}_F$ for some finite set F.
The golden mean shift is a shift of finite type.

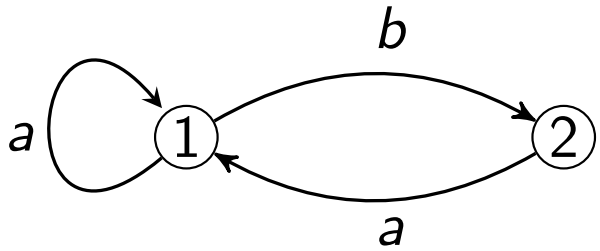
An easy way to define a shift space is to use a finite graph $\mathcal{A}$ with edges labeled by letters in A. Then the set $\mathsf{X}(\mathcal{A})$ of labels of two-sided infinite paths in $\mathcal{A}$ is easily seen to be shift-invariant.

It can be shown to be also closed (Exercise).

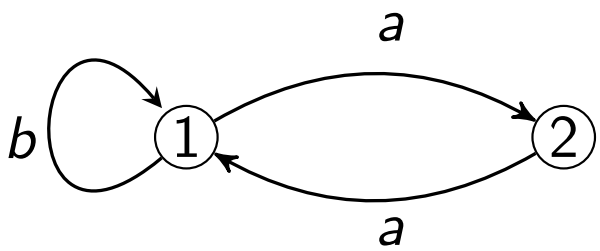
Thus, it is a shift space, called a *sofic* shift.

A shift of finite type is sofic but the converse is not true (Exercise).

Example of a shift of finite type: the golden mean shift



Example of a sofic shift: the even shift



$X(\mathcal{A})$ is a shift space: Solution

Let $\mathcal{A}$ be a graph with edges labeled by letters in A.

Let E be the set of edges of the graph $\mathcal{A}$. The set of bi-infinite paths in $\mathcal{A}$ is the shift X_F on the alphabet E, with F being the words of length 2 of the form ef, where e, f are not consecutive. Thus, it is a shift space.

The set $X(\mathcal{A})$ is the image of X_F under the map which assigns to a path its label. Since this map is continuous, the conclusion follows.

A shift of finite type is sofic: solution

Let $X = \mathsf{X}_F$ with $F \subseteq A^*$ a finite set. Let $\mathcal{A} = (Q, I, T)$ be a trim automaton recognizing the language $A^* \setminus A^* F A^*$. The set of labels of two-sided infinite paths in $\mathcal{A}$ is equal to X.
The automaton is *trim* if every state is accessible and coaccessible.
Note: the proof holds when F is only regular.

A shift of finite type is sofic: another solution

Let $X = \mathsf{X}_F$ with $F \subseteq A^*$ a finite set.
Let n be the maximal size of words in F.
Let $\mathcal{A}$ be the graph whose states are the words of length $n-1$ that do not contain any word of F, and with edges

$$a_0 a_1 \dots a_{n-2} \xrightarrow{a_0} a_1 \dots a_{n-2} a,$$

where $a_0 a_1 \dots a_{n-2} a$ does not contain any word of F. The set of labels of two-sided infinite paths in $\mathcal{A}$ is equal to $X = \mathsf{X}_F$.

Example with $F = \{bb\}$ on the board.

The even shift is not of finite type: solution

Assume that $X = X_F$ with $F \subseteq A^*$ formed of words of length at most n.
Then every block of length n of $x = {}^{\omega}a \cdot ba^{2n+1}ba^{\omega}$ is in $\mathcal{B}_n(X)$, and thus x has no block in F, a contradiction since $x \notin X$.

Language of a shift space

If X is a shift space, the set of blocks of sequences in X is denoted by $\mathcal{B}(X)$. The set of blocks of length n of sequences in X is denoted by $\mathcal{B}_n(X)$.
A language L is called *factorial* if it contains the words occurring as blocks in its elements, that is, if $uvw \in L$, then $v \in L$.
It is *extendable* if every $u \in L$ is *extendable*, that is, there are letters $a, b \in A$ such that $aub \in L$.

Proposition

The language of a shift space is factorial and extendable. Conversely, for every factorial and extendable language L, there is a unique shift space X such that $\mathcal{B}(X) = L$. It is the set $\mathrm{X}(L)$ of sequences $x \in A^{\mathbb{Z}}$ with all their blocks in L. For every factorial and extendable language L and every shift space X, the following equalities hold: $\mathcal{B}(\mathrm{X}(L)) = L$, and $\mathrm{X}(\mathcal{B}(X)) = X$.

Solution

Let L be a factorial extendable language. Let $\mathrm{X}(L)$ be the set of all sequences with all their blocks in L. Clearly, $\mathrm{X}(L)$ is a shift space and $\mathcal{B}(\mathrm{X}(L)) \subseteq L$.
For $u \in L$, since L is extendable, there are sequences $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ such that $a_n \cdots a_0 u b_0 \cdots b_n \in L$. Since L is factorial, the sequence $\cdots a_0 \cdot u b_0 b_1 \cdots$ is in $X(L)$. This shows that $L \subseteq \mathcal{B}(\mathrm{X}(L))$, and thus that $\mathcal{B}(\mathrm{X}(L)) = L$.

The second equality holds because for any $x \in \mathrm{X}(\mathcal{B}(X))$, one has $x_{|-n,n]} \in \mathcal{B}(X)$ and thus x belongs to the closure of X, whence to X. Thus, the map $L \mapsto \mathrm{X}(L)$ is the inverse of the map $X \mapsto \mathcal{B}(X)$.

Example

Find an example of a language L such that $\mathcal{B}(\mathrm{X}(L)) \neq L$.

Solution

Set $L = a^*ba^*$. Then L is not factorial and $\mathrm{X}(L)$ is empty.

Cylinders

Let X be a shift space. For two words u, v such that $uv \in \mathcal{B}(X)$, the set

$$[u \cdot v]_X = \{x \in X \mid x_{[-|u|,|v|)} = uv\}$$

is nonempty. It is called the *cylinder* with basis (u, v). For $v \in \mathcal{B}(X)$, we also define

$$[v]_X = \{x \in X \mid x_{[0,|v|)} = v\}$$

in such a way that $[v]_X = [\varepsilon \cdot v]_X$. The set $[v]_X$ is called the *right cylinder* with basis v.

The open sets contained in X are the unions of cylinders and the clopen sets are the finite unions of cylinders (Exercises).

Solutions

Every cylinder is an open set, and thus every union of cylinders is open. Next, in any metric space, every open set is a union of open balls. But the open balls in X are cylinders.

Every cylinder is a clopen set because the complement of $[u \cdot v]$ is the union of the cylinders $[u' \cdot v']$ with $u' \neq u$ of the same length as u and $v = v'$, or $u' = u$ and $v' \neq v$ of the same length as v. Conversely, if U is clopen, it is, as an open set, a union of cylinders $[u \cdot v]$ for a set of pairs (u, v) such that $uv \in \mathcal{B}(X)$. Since U is closed, it is compact. Thus, there is a finite set of pairs (u, v) such that the union is equal to U.

Irreducible shift

A nonempty shift space X is *irreducible* if, for every $u, v \in \mathcal{B}(X)$, there is a word w such that $uwv \in \mathcal{B}(X)$.

Example

The golden mean shift X is irreducible. Indeed, if $u, v \in \mathcal{B}(X)$, then $uav \in \mathcal{B}(X)$.

Reducible shift

Example

The shift X formed of the labels of two-sided infinite paths in the graph below is reducible. Indeed, there is no word u such that $bua \in \mathcal{B}(X)$.

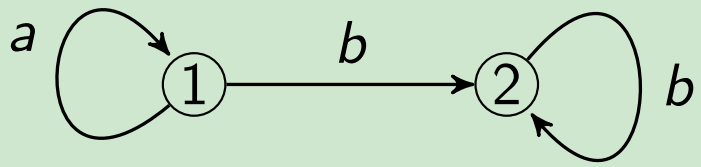


Figure: A reducible shift.

Uniformly recurrent shift

A nonempty shift space X is *uniformly recurrent* if for every $w \in \mathcal{B}(X)$ there is an integer $n \geq 1$ such that w occurs in every word of $\mathcal{B}_n(X)$.

As an equivalent definition, a shift space X is uniformly recurrent if for every $n \geq 1$ there is an integer $N = R_X(n)$ such that every word of $\mathcal{B}_n(X)$ occurs in every word of $\mathcal{B}_N(X)$. The function R_X is called the *recurrence function* of X.

Example

Example

The golden mean shift X is not uniformly recurrent since b is in $\mathcal{B}(X)$ although b does not occur in any $a^n \in \mathcal{B}(X)$.

Deterministic automaton in symbolic dynamics

An automaton $\mathcal{A} = (Q, E)$ is a finite directed (multi)graph with edges labeled on A. The set of edges is included in $Q \times A \times Q$.

It is *trim* if each state has at least one outgoing edge and at least one incoming edge.

It is (uncomplete) *deterministic* if, for each state $p \in Q$ and each letter $a \in A$, there is at most one edge labeled by a going out of p.

It is *irreducible* if its graph is strongly connected.

It is a *presentation* of a sofic shift X if X is the set of labels of bi-infinite paths of $\mathcal{A}$.

Minimal automaton in symbolic dynamics

Proposition

Every sofic shift has a trim deterministic presentation.

Proposition

Every irreducible sofic shift has a unique minimal deterministic presentation (irreducible deterministic and with the fewest number of states among these presentations).

Deterministic automaton in symbolic dynamics

Proposition

Every sofic shift has a trim deterministic presentation.

Proof.

Start with a trim presentation $\mathcal{A} = (Q, E)$. Apply the subset construction: $\mathcal{D} = (\mathfrak{P}(Q) \setminus \emptyset, \Delta)$. There is an edge $P \xrightarrow{a} P'$ in Δ is $P' = \{q \in Q \mid \exists p \in P, p \xrightarrow{a} q\}$. Start from $P = Q$. □

Minimal automaton in symbolic dynamics

Proposition

Every irreducible sofic shift has a unique minimal deterministic presentation.

Proof.

Start with a trim deterministic presentation $\mathcal{A} = (Q, E)$ of X.
For $q \in Q$, let
$\mathrm{Fut}(q) = \{w \in A^* \mid \text{there is a path labeled by } w \text{ starting at } q\}$.
We say that $\mathcal{A}$ is *reduced* if $p \neq q$ implies $\mathrm{Fut}(p) \neq \mathrm{Fut}(q)$.
If $\mathcal{A}$ is not reduced, there are two states $p \neq q$ with
$\mathrm{Fut}(p) = \mathrm{Fut}(q)$.
Merge p, q: let $\mathcal{A}' = (Q', E')$ with $Q' = Q \setminus \{p, q\} \cap \{(p, q)\}$,
where (p, q) is a new state and E' is the set of edges $(\pi(r), a, \pi(s))$
with (r, a, s) in E, $\pi(t) = t$ if $t \neq p, q$, $\pi(p) = \pi(q) = (p, q)$.
The automaton $\mathcal{A}'$ is still a trim deterministic presentation
of X. □

Minimal automaton in symbolic dynamics

proof continued.

Let $\mathcal{A}$ be a reduced trim deterministic presentation of X.
The automaton $\mathcal{A}$ has a *synchronizing word*: a word w such that all paths labeled by w end in the same state q_w.
Indeed, let
$\mathrm{rank}(w) = \mathrm{Card}\{q \mid \exists \text{ a path labeled by } w \text{ ending in } q\}$.
Let w be a word of minimal non-null rank. Let us show that $\mathrm{rank}(w) = 1$.
If $\mathrm{rank}(w) > 1$, let (p, w, q), (p', w, q') be two paths with $q \neq q'$.
Since $\mathrm{Fut}(q) \neq \mathrm{Fut}(q')$, let u be a word such that
$u \in \mathrm{Fut}(q) \setminus \mathrm{Fut}(q')$ (or the converse).
Then, $\mathrm{rank}(wu) < \mathrm{rank}(w)$ and $\mathrm{rank}(wu) \neq 0$.

□

Minimal automaton in symbolic dynamics

proof continued.

Let $\mathcal{B}$ be the irreducible part of $\mathcal{A}$ containing q_w. Then $\mathcal{B}$ is an irreducible deterministic presentation of X that is reduced.
Indeed, let u be a block in $\mathcal{B}(X)$. There are blocks v, v' such that $wvuv'w \in \mathcal{B}(X)$. Hence, there is a path in $\mathcal{A}$ labeled $vuv'w$ from q_w to q_w, implying that u is the label of a path in $\mathcal{B}$. Conversely, labels of bi-infinite paths of $\mathcal{B}$ belong to X.

Finally, let $\mathcal{C} = (Q', E')$ be another reduced irreducible deterministic presentation of X.
Let w be a synchronizing word for $\mathcal{B}$ and w' be a synchronizing word for $\mathcal{C}$. There is a word u such that $wuw' \in \mathcal{B}(X)$. Thus $z = wuw'$ is a synchronizing word for both $\mathcal{B}$ and $\mathcal{C}$.
We define a bijection f from Q to Q' as follows: $f(q_z) = q'_z$. If $q \in Q$ and u is the label of a path from q_z to q, we define $f(q)$ as the end of the unique path labeled by u going out of q'_z in $\mathcal{C}$.

□

Local automaton

A deterministic automaton $\mathcal{A} = (Q, E)$ is *local* if there is an integer n such that, for each word w of length n, all paths labeled by w end in the same state q_w.

Proposition

An irreducible shift X is of finite type if and only if its minimal deterministic automaton is local.

Proof.

Exercise. □

Proof.

Let $X = \mathrm{X}_F$ be an irreducible shift of finite type. Without loss of generality, we may assume that all words of F have the same length n.
Let $\mathcal{A} = (Q, E)$, where Q is the set of words of length $n-1$ with edges

$$a_0 a_1 \dots a_{n-2} \xrightarrow{a} a_1 \dots a_{n-2} a,$$

where $a_0 a_1 \dots a_{n-2} a \notin F$. We keep only the trim part of this automaton.

Then $\mathcal{A}$ is deterministic and irreducible. Indeed, let $p = u$, $q = v$. Then u, v are blocks of X (say why). Since X is irreducible, there is a word w such that $uwv \in \mathcal{B}(X)$. By construction, there is a path from p to q in $\mathcal{A}$ labeled by wv. □

solution

Proof.

The automaton $\mathcal{A}$ is local. Indeed, by construction, any path labeled by w of length $n-1$ ends in the state w.
Since $\mathcal{A}$ is local, after a reduction (two states with the same future are identified), it remains local.
The (unique) minimal deterministic automaton of X can be obtained with a reduction of $\mathcal{A}$. It is thus local.

Conversely, if the minimal deterministic automaton $\mathcal{B}$ of X is local: there is an integer $k \geq 0$ such that for each w of length k, all paths of $\mathcal{B}$ labeled by w end in the same state q_w.
Let F be the set of words of length $k+1$ that do not label any path in $\mathcal{B}$.
Then $X = \mathsf{X}_F$ (say why).

□

Local automaton

Proposition

An irreducible deterministic automaton is local if and only if it has at most one cycle with a given label.

Proof.

Exercise. □

cycle : path $p = p_0 \xrightarrow{a_0} p_1 \xrightarrow{a_1} p_2 \dots \xrightarrow{a_{m-1}} p_m = p$.
m is the length of the cycle.

Solution

Proof.

Let $\mathcal{A}$ be a deterministic irreducible automaton. If $\mathcal{A}$ has two cycles sharing the same label w.

$$p = p_0 \xrightarrow{a_0} p_1 \xrightarrow{a_1} p_2 \dots \xrightarrow{a_{m-1}} p_m = p',$$
$$p' = p'_0 \xrightarrow{a_0} p'_1 \xrightarrow{a_1} p'_2 \dots \xrightarrow{a_{m-1}} p'_m = p'.$$

We have $p_i \neq p'_i$ for some $0 \leq i < m$.
Since $\mathcal{A}$ is deterministic, $p_i \neq p'_i$ for all $0 \leq i < m$.
Then, for any $n = k|w| + j$, $0 \leq j < |w|$, $w^k w_{[0,j)}$ is the label of a path ending in p_j and of a path ending in $p'_j \neq p_j$.
Thus, $\mathcal{A}$ cannot be local.

□

Solution

Proof.

Conversely, if $\mathcal{A}$ is not local, then, for any integer n there are two paths labeled by a word $w^{(n)}$ of length n ending in distinct states. We choose $n = (\text{Card } Q)^2$. These two paths are

$$p = p_0 \xrightarrow{a_0} p_1 \xrightarrow{a_1} p_2 \dots \xrightarrow{a_{n-1}} p_n = p',$$
$$p' = p'_0 \xrightarrow{a_0} p'_1 \xrightarrow{a_1} p'_2 \dots \xrightarrow{a_{n-1}} p'_n = p'.$$

If $p_i = p'_i$ for some $0 \leq i < n$, then $p = p'$, a contradiction. Hence $p_i \neq p'_i$ for all $0 \leq i < n$. By the pigeonhole principle, there are $0 \leq i < j < n$ such that $(p_i, p'_i) = (p_j, p'_j)$, implying the existence of two cycles sharing the same label.

□

Master 2 Mathematics and Computer Science Symbolic Dynamics. Lecture 2

Marie-Pierre Béal

University Gustave Eiffel
Laboratoire d'informatique Gaspard-Monge UMR 8049

Overview

- Conjugacy and state-splitting
- Perron-Frobenius theorem
- Conjugacy invariants.

Conjugacy and state-splitting

Block maps

Let X be a shift space on the alphabet A, and let B be another alphabet. Given integers m, a with $m + a \geq 0$, a *block map* is a map $f : \mathcal{B}_{m+a+1}(X) \to B$. The *sliding block code* defined by f and (m, a) is the map $\varphi : X \to B^{\mathbb{Z}}$ defined by $\varphi(x) = y$ if for every $i \in \mathbb{Z}$,

$$y_i = f(x_{[i-m,i+a]}).$$

Thus y is computed from x by sliding a window of length $m + a + 1$ on x. The integer m is the *memory* of φ and a is its *anticipation*.

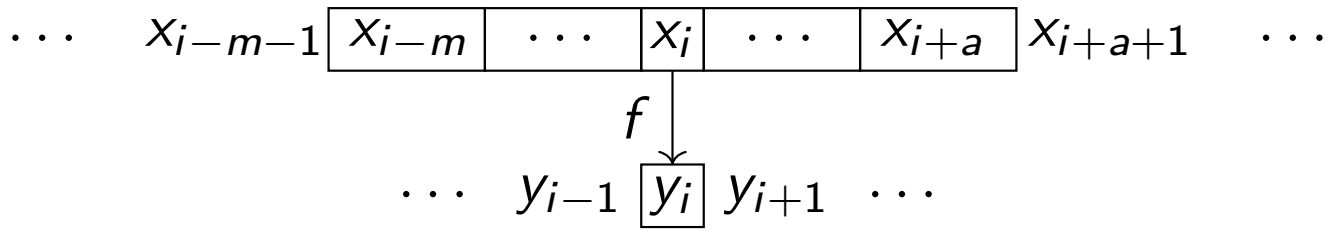


Figure: The sliding block code.

Sliding block code

Proposition

Let X be a shift space on the alphabet A and let $\varphi : X \to B^{\mathbb{Z}}$ be a sliding block code. Then $\varphi(X)$ is a shift space.

Proof.

The map φ is clearly continuous and commutes with the shift, that is, $\varphi \circ S = S \circ \varphi$. Thus $Y = \varphi(X)$ is closed (because the continuous image of a compact space is compact and thus closed). It is shift-invariant because, if $y = \varphi(x)$ with $x \in X$, then $S(y) = S \circ \varphi(x) = \varphi(S(x))$ and thus $S(y) \in Y$. □

Curtis-Hedlund-Lyndon theorem

Let X, Y be shift spaces. A map $\varphi\colon X \to Y$ is a *morphism* if φ is continuous and commutes with the shift map.

Theorem (Curtis, Hedlund, Lyndon)

Let X, Y be shift spaces. A map $\varphi\colon X \to Y$ is a morphism systems if and only if it is a sliding block code from X into Y.

Proof.

A sliding block code is clearly continuous and commutes with the shift.

Conversely, let $\varphi\colon X \to Y$ be a morphism . For every letter b from the alphabet B of Y, the set $[b]_Y$ is clopen and thus $\varphi^{-1}([b]_Y)$ is also clopen. Since a clopen set is a finite union of cylinders, there is an integer n such that $\varphi(x)_0$ depends only on $x_{[-n,n]}$. Set $f(x_{[-n,n]}) = \varphi(x)_0$. Then φ is the sliding block code associated with the block map f. □

Conjugacy

Let X, Y be shift spaces. A map $\varphi : X \to Y$ is a *conjugacy* if φ is a bijective morphism.

Its inverse is also a morphism.

It follows from the Curtis-Hedlund-Lyndon theorem that a conjugacy between shift spaces X and Y is the same as a sliding block code from X to Y which is invertible (the inverse is also a sliding block code since the inverse of a conjugacy is a morphism).

Example

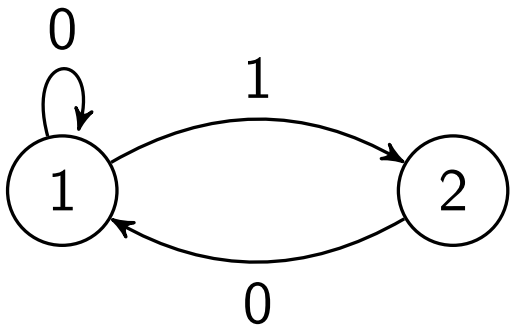
We say that $f : A^{m+a+1} \to B$ is a *k-block map*, where $k = m + a + 1$, and that the corresponding sliding block code is a *k-block code*.

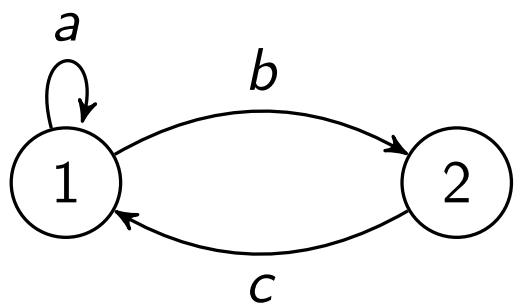
The simplest form of a sliding block code, called a 1-*block code*, occurs when $m = a = 0$. In this case, we use the same symbol to denote the 1-block map $\phi : A \to B$ and the 1-block code $\phi : A^{\mathbb{Z}} \to B^{\mathbb{Z}}$. In this way, we have for every $x \in X$ and $n \in \mathbb{Z}$, $\phi(x)_n = \phi(x_n)$.

Conjugacy: example

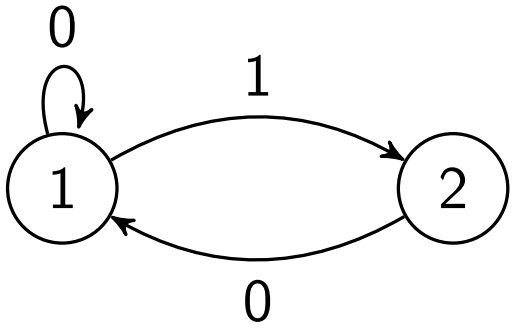
Example

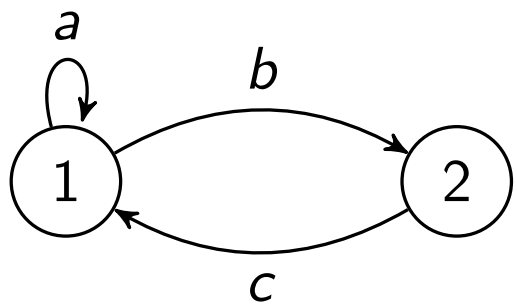
X_F with $F = \{11\}$ is a shift of finite (the golden mean shift).
X_G with $G = \{ac, ba, bb, cc\}$ is a shift of finite.

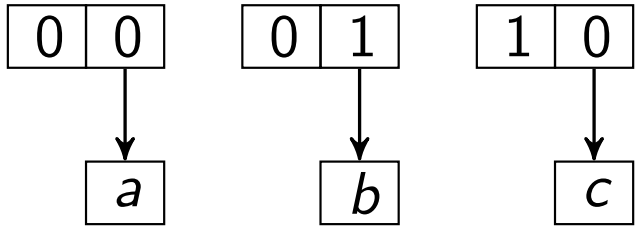




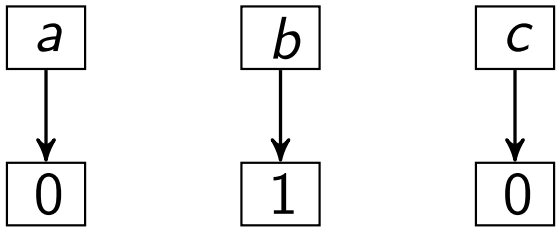
Conjugacy: example







$$\varphi : X_F \to X_G .$$



$$\varphi^{-1} : X_G \to X_F .$$

Edge shifts

An *edge shift* is the set of bi-infinite paths of a directed (multi)graph.

Proposition

Every shift of finite type is conjugate to an edge shift.

Proof.

Let $X = \mathsf{X}_F$ with F finite, and let n be the maximal size of words in F. We may assume that all words in F have size n.
Let $\mathcal{A} = (Q, E)$, where Q is the set of words of length $n-1$ with edges $a_0a_1 \dots a_{n-2} \xrightarrow{a} a_1 \dots a_{n-2}a$, where $a_0a_1 \dots a_{n-2}a \notin F$. We keep only the trim part of this automaton.

Then $\mathcal{A}$ is deterministic and local (all paths labeled by a word w of length $n-1$ end in the same state q_w). □

proof continued.

Let Y be the set of bi-infinite paths of $\mathcal{A}$.
Let $\phi\colon Y \to X$ defined by the 1-block map $f : E \to A$ with $f(e = (p, a, q)) = a$.
Then the sliding block code $\varphi\colon X \to Y$ with anticipation 0 and memory $n-1$ defined by the n-block map $g\colon A^n \to E$ with $g(a_0 a_1 \dots a_{n-1}) = (p, a_{n-1}, q)$, where $p = a_0 a_1 \dots a_{n-2}$ and $q = a_1 a_2 \dots a_{n-1}$.
The map φ is the inverse of ϕ.

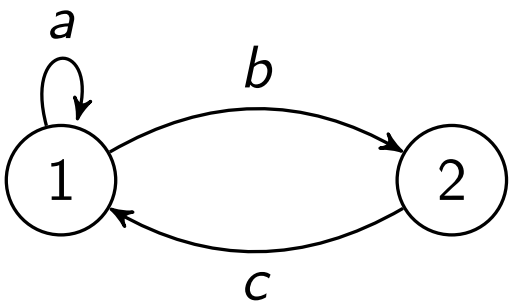
□

Edge shifts

If we take a minimal deterministic presentation of an irreducible shift of finite type, then, up to a conjugacy, one may assume that all labels are distinct and the shift can be defined by the transition matrix of the graph G of the presentation.

Transition matrix of an automaton

$M = (m_{pq})_{p,q \in Q}$, where m_{pq} is the number of edges from p to q.



$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

If G is an automaton or a graph, the edge shift defined by G is denoted X_G.

State splitting of an automaton

An *out-splitting* of an automaton $\mathcal{A} = (Q, E)$ is a local transformation of $\mathcal{A}$ into an automaton $\mathcal{B} = (Q', E')$ obtained by selecting a state s and partitioning the set of edges going out of s into two non-empty sets E_1 and E_2.

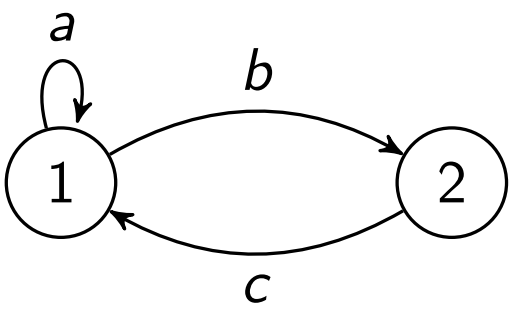
- $Q' = Q \setminus \{s\} \cup \{s_1, s_2\}$,
- E' contains all edges of E neither starting at or ending in s,
- E' contains the edge (s_1, a, t) for each edge $(s, a, t) \in E_1$, and the edge (s_2, a, t) for each edge $(s, a, t) \in E_2$, if $t \neq s$.
- E' contains the edges (t, a, s_1) and (t, a, s_2) if (t, a, s) in E, when $t \neq s$,
- E' contains the edges (s_1, a, s_1) and (s_1, a, s_2) if (s, a, s) in E_1, and the edges (s_2, a, s_1) and (s_2, a, s_2) if $(s, a, s) \in E_2$.

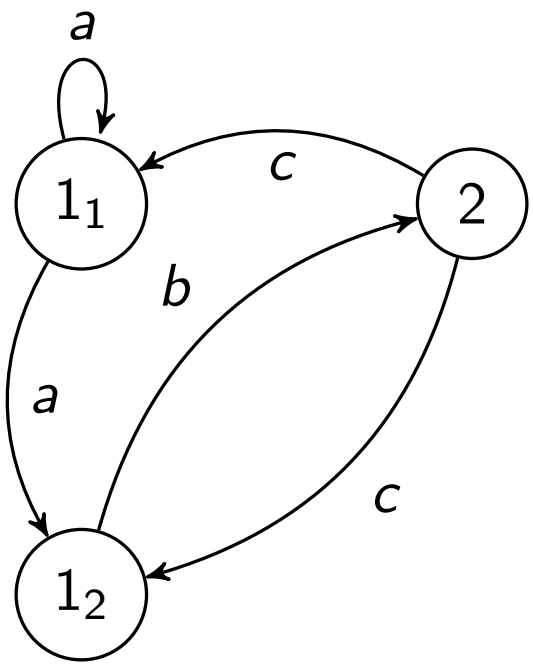
State splitting of an automaton

An *input state splitting* is defined similarly.

The inverse operation is called an *output merging*, possible whenever s_1 and s_2 have the *same input edges*.

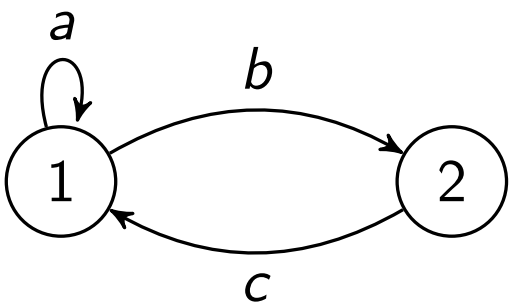
Output state splitting of an automaton

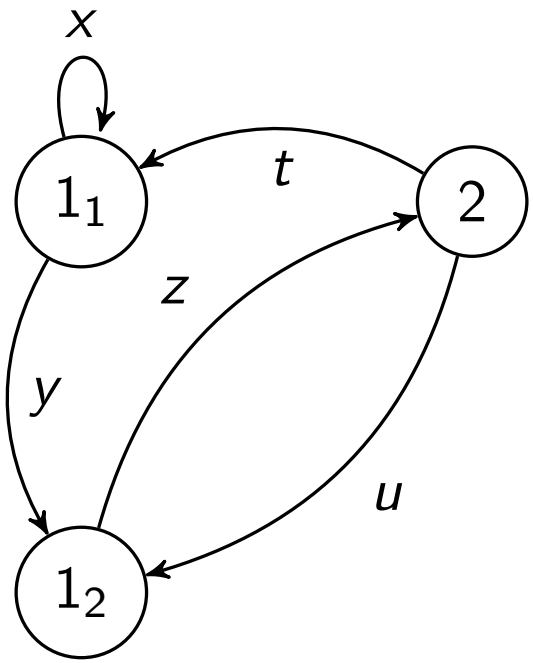




The state 1 is split into two states 1_1 and 1_2 with $E_1 = \{(1, a, 1)\}$ and $E_2 = \{(1, b, 2)\}$.

Output state splitting of a graph





State splitting

Proposition

Let G be a graph and H a split graph of G. Then X_G and X_H are conjugate.

Proof.

Let $G = (Q, E)$ (all labels are distinct).
Let $H = (Q', E')$ be an outsplit of G, obtained after splitting the state s into s_1, s_2 according to the partition E_1, E_2 of edges going out of s.
Let X_G be the edge shift defined by G and X_H be the edge shift defined by H.
Then X_G and X_H are conjugate. □

State splitting

Proof.

Indeed, let $\varphi_{GH} : \ : E^{\mathbb{Z}} \to E'^{\mathbb{Z}}$ be the $(0,1)$-sliding block code defined by the 2-block map $f : \mathcal{B}_2(X_G) \to E'$, where

$$
\begin{aligned}
f((t,a,u)(u,b,v)) &= (t,a,u) && \text{if } t,u \neq s,\\
f((t,a,s)(s,b,v)) &= (t,a,s_1) && \text{if } t \neq s \text{ and } (s,b,v) \in E_1,\\
f((t,a,s)(s,b,v)) &= (t,a,s_2) && \text{if } t \neq s \text{ and } (s,b,v) \in E_2,\\
f((s,a,t)(t,b,u)) &= (s_1,a,t) && \text{if } t \neq s \text{ and } (s,a,t) \in E_1,\\
f((s,a,t)(t,b,u)) &= (s_2,a,t) && \text{if } t \neq s \text{ and } (s,a,t) \in E_2,\\
f((s,a,s)(s,b,t)) &= (s_1,a,s_1) && \text{if } (s,b,t) \in E_1,\\
f((s,a,s)(s,b,t)) &= (s_1,a,s_2) && \text{if } (s,b,t) \in E_2.
\end{aligned}
$$

defines a conjugacy from X_G onto X_H. Its inverse is the sliding block code defined by the 1-block map $g : E' \to E$, where $g(t,a,u) = (\pi(t),\pi(a),\pi(u))$, with $\pi(t) = t$ if $t \neq s_1, s_2$, $\pi(s_1) = \pi(s_2) = s$, $\pi(a) = a$.

Complete out-splitting

Let $G = (Q, E)$ be a graph. All edges have distinct labels; we may omit them.

The *complete out-splitting* of G is the graph $H = (Q', E')$ where

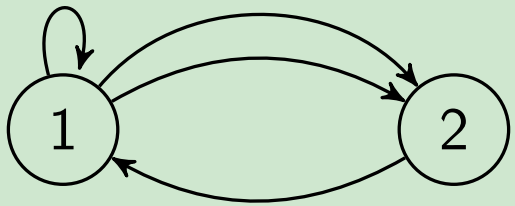
- $Q' = \{s_e \mid s \in Q, e = (s, t) \in E\}$,
- $E' = \{(s_e, t_f) \mid e = (s, t)\}$

Proposition

Let G be a graph and H the complete out-splitting of G. Then X_G and X_H are conjugate. There is a sequence of out-splittings from G to H.

Example

Compute the complete out-splitting of



Decomposition Theorem

An *trim graph* is a graph such that each state has at least one incoming edge and at least one outgoing edge.

Theorem (Decomposition Theorem, R. Williams 1973)

Two edge shifts X_G and X_H defined by trim graphs G and H are conjugate if and only if there is a sequence of (input and output) state splittings and (input and output) state mergings from G to H.

Higher block shift

Let X be a shift space on the alphabet A and let $k \geq 1$ be an integer.

The map $\gamma_k : X \to \mathcal{B}_k(X)^{\mathbb{Z}}$ defined for $x \in X$ by $y = \gamma_k(x)$ if, for every $n \in \mathbb{Z}$,

$$y_n = \langle x_n \cdots x_{n+k-1} \rangle, \tag{1}$$

is the k-th *higher block code*.
One also says that γ_k is a *coding by overlapping blocks* of length k.

The set $X^{(k)} = \gamma_k(X)$ is a shift space on $\mathcal{B}_k(X)$, called the k-th *higher block shift* of X.

Higher block code

The higher block code is an isomorphism of shift spaces, and the inverse of γ_k is the map $\pi_k : y \mapsto x$ such that, for all n, x_n is the first letter of the word u such that $y_n = \langle u \rangle$.

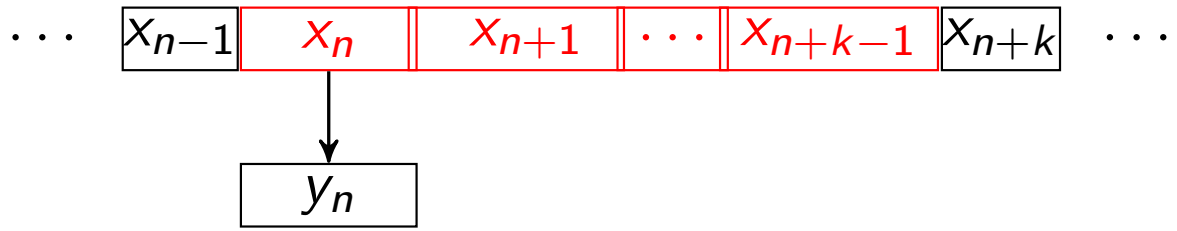


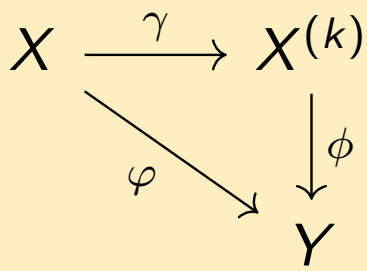
Figure: The k-th higher block code.

Thus, $X^{(k)}$ is conjugate to X.

Reduction to a 1-block code

Lemma

Let $\varphi\colon X \to Y$ be a sliding block code. Then there is a higher block shift $X^{(k)}$ of X, a conjugacy $\gamma\colon X \to X^{(k)}$ and a 1-block code $\phi\colon X^{(k)} \to Y$ such that $\phi \circ \gamma = \varphi$.



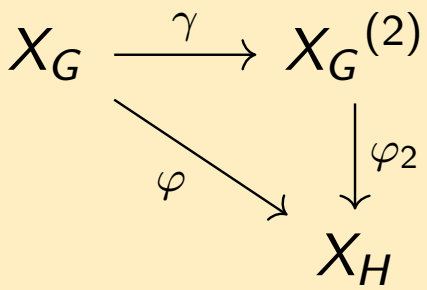
Proof.

Let $\varphi\colon X \to Y$ be a (m, a)-sliding block code.
Set $k = m + a + 1$ and $\gamma = \gamma_k \circ S^{-m}$.
Thus, $\gamma(x)_i = \langle x_{i-m} \cdots x_{i+a} \rangle$.
Put $\phi = \varphi \circ \gamma^{-1}$.
ϕ is a 1-block code.

Reduction to a 1-block code

Lemma

Let $\varphi : X_G \to X_H$ be a $(0, a)$-sliding block code with $a > 0$. Then there is an out-splitting G' of G such $X_{G'} = X_G{}^{(2)}$ and a conjugacy $\gamma : X_G \to X_G{}^{(2)}$ and a $(0, a-1)$-sliding block code $\varphi_2 : X_G{}^{(2)} \to X_H$ such that $\varphi_2 \circ \gamma = \varphi$.



Reduction to a 1-block code

Proof.

Let $G' = (Q', E')$ be the complete out-splitting of G. Let $H = (R, F)$. Assume that φ is defined by the block map $f : E^{a+1} \to F$.

- $Q' = \{s_e \mid s \in Q, e = (s,t) \in E\}$,
- $E' = \{(s_e, t_f) \mid e = (s,t)\}$

We define $\varphi_2 : E' \to F$ by the $(0, a-1)$-block map $g : E'^a \to F$ with $g((s_{e_0}, s_{e_1})(s_{e_1}, s_{e_2}) \dots (s_{e_{a-1}}, s_{e_a})) = f(e_0 e_1 \dots e_a)$.

We get $\varphi_2 \circ \gamma = \varphi$.

We check that $X_{G'}$ is equal to $X_G^{(2)}$, up to a renaming of the states.

Let $\phi : E' \to \mathcal{B}_2(X_G)$ be the 1-block code defined by $\phi((s_e, t_f)) = (e, f)$. The inverse $\phi^{-1} : \mathcal{B}_2(X_G) \to E'$ is the 1-block code defined by $\phi^{-1}((e,f)) = (s_e, t_f)$, where $e = (s,t)$.

Reduction of the anticipation of ϕ^{-1}

Lemma

Let $\phi\colon X_G \to X_H$ be a 1-block conjugacy whose inverse has memory m' and anticipation $a' \geq 1$.
Then, there are out-splitting G' of G and H' of H and a 1-block conjugacy $\phi'\colon X_{G'} \to X_{H'}$ such that

$$\phi = \varphi_{H'H} \circ \phi' \circ \varphi_{GG'}.$$

$$\begin{array}{ccc} X_G & \xrightarrow{\varphi_{GG'}} & X_{G'} \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi'} \\ X_H & \xleftarrow{\varphi_{H'H}} & X_{H'} \end{array}$$

and whose inverse has memory m' and anticipation $a' - 1$.

Reduction of the anticipation of ϕ^{-1}

Proof.

Let $\phi\colon X_G \to X_H$ be a 1-block conjugacy whose inverse ϕ^{-1} has memory m' and anticipation $a' \geq 1$.

Let $H' = (Q_{H'}, E_{H'})$ be the complete out-splitting of H. The edges of H' are (s_e, t_f) where $e = (s, t)$, $f = (t, u)$ are edges of H.

Let $G' = (Q_{G'}, E_{G'})$ be the out-splitting of G obtained by splitting each state v into states v_e, where e is an edge of H.
The edges going out of each state v of G are partitioned into the sets $\Delta(v)_e = \{(v, w) \text{ edge of } G \mid \phi((v, w)) = e\}$. The edges of G' are (v_e, w_f) where $\phi((v, w)) = e$.

We define $\phi'\colon E_{G'} \to E_{H'}$ by $\phi'((v_e, w_f)) = (s_e, t_f)$, where $e = (s, t)$. Then ϕ' is a 1-block conjugacy.

Reduction of the anticipation of ϕ^{-1}

Proof.

By hypothesis, ϕ^{-1} has memory m' and anticipation a'.
With $e_i = (s_i, s_{i+1})$, $f_i = (v_i, v_{i+1})$, we have

$$\begin{array}{ccc} \ldots f_{-1} \cdot f_0 f_1 \ldots & \xrightarrow{\varphi_{GG'}} & \ldots((v_{-1})_{e_{-1}}, (v_0)_{e_0}) \cdot ((v_0)_{e_0}, (v_1)_{e_1})((v_1)_{e_1}, (v_2)_{e_2}) \ldots \\ \Big\downarrow \phi & & \Big\downarrow \phi' \\ \ldots e_{-1} \cdot e_0 e_1 \ldots & \xleftarrow{\varphi_{H'H}} & \ldots((s_{-1})_{e_{-1}}, (s_0)_{e_0}) \cdot ((s_0)_{e_0}, (s_1)_{e_1})((s_1)_{e_1}, (s_2)_{e_2}) \ldots \end{array}$$

Hence ϕ'^{-1} has memory m' and anticipation $a' - 1$. □

Proof of the decomposition theorem

Proof of the decomposition theorem.

Let us assume that there is a conjugacy $\varphi\colon X_G \to X_H$. We may assume that φ is a $(0, m+a)$-block code (with a composition with S^{-m}).

We reduce the anticipation of ${\phi'_i}^{-1}$ with out-splittings and the memory of ${\phi'_j}^{-1}$ with in-splittings, and get

$$\begin{array}{ccccccccccc}
X_G & \xrightarrow{\gamma} & (X_G)^{(m+a)} & \xrightarrow{\varphi_{GG'_1}} & X_{G'_1} & \xrightarrow{\varphi_{G'_1G'_2}} & X_{G'_2} & \longrightarrow & \cdots & \longrightarrow & X_{G'_{m'+a'}} \\
 & \searrow^{\varphi} & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi'_1} & & \downarrow{\scriptstyle \phi'_2} & & & & \downarrow{\scriptstyle \phi'_{m'+a'}} \\
 & & X_H & \xleftarrow{\varphi_{H'_1H}} & X_{H'_1} & \xleftarrow{\varphi_{H'_2H'_1}} & X_{H'_2} & \longleftarrow & \cdots & \longleftarrow & X_{H'_{m'+a'}}
\end{array}$$

Thus $\phi'_{m'+a'}$ is a 1-block conjugacy whose inverse is a 1-block conjugacy, implying that the graphs $G'_{m'+a'}$ and $H'_{m'+a'}$ are equal since they are trim.

Conversely, if there is a sequence of splittings and mergings from G to H, then X_G and X_H are conjugate. □

Out-mergings and in-mergings do not commute

Let G be the graph with transition matrix

$$M = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

We can perform an out-merging of the states 2 and 3 of G (since the columns 2 and 3 are identical) and get G_1 with transition matrix

$$M_1 = \begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix}.$$

We can perform an in-merging of the states 2 and 3 of G (since the rows 2 and 3 are identical) and get G_2 with transition matrix

$$M_2 = \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}.$$

And no mergings are possible from G_1 or G_2.

Open problem

Open problem

It is not known whether conjugacy between shifts of finite type is decidable, even for irreducible shifts of finite type.

Strong shift equivalence

Two nonnegative integer matrices M, N are *elementary equivalent* if there are, possibly nonsquare, matrices R, S such that

$$M = RS, N = SR.$$

Two nonnegative integer matrices M, N are *strong shift equivalent* if there is a sequence of elementary equivalences from M to N:

$$\begin{aligned} M &= R_0 S_0, S_0 R_0 = M_1, \\ M_1 &= R_1 S_1, S_1 R_1 = M_2, \\ &\vdots \\ M_\ell &= R_\ell S_\ell, S_\ell R_\ell = N. \end{aligned}$$

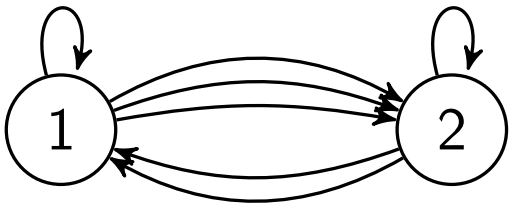
Theorem (Classification Theorem, R. Williams 1973)

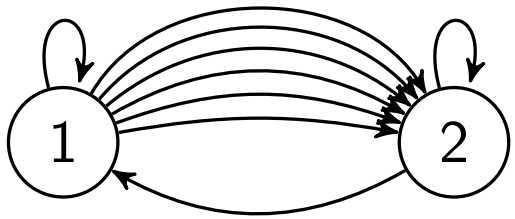
Two edge shifts defined by matrices M and N are conjugate if and only if M and N are strong shift equivalent.

Conjugacy: examples

Let X and Y be the edge shifts defined by the graphs given by the matrices M and N respectively:

$$M = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}, \quad N = \begin{bmatrix} 1 & 6 \\ 1 & 1 \end{bmatrix}$$





We may see these graphs as automata where all edge labels are distinct.

The shifts X and Y are conjugate (K. Baker, using computer research to prove strong shift equivalence).

Conjugacy: examples

It is not known whether X and Y defined by M_k and N_k are conjugate for $k \geq 4$.

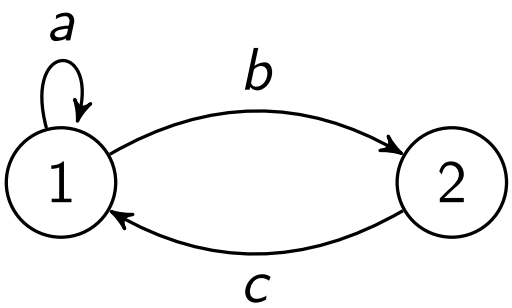
$$M_k = \begin{bmatrix} 1 & k \\ k-1 & 1 \end{bmatrix}, \quad N_k = \begin{bmatrix} 1 & k(k-1) \\ 1 & 1 \end{bmatrix}$$

Perron-Frobenius theorem

Transition matrix of a graph

Let $G = (Q, E)$ be a graph. Its transition matrix is a nonnegative integer matrix M where

$M = (m_{pq})_{p,q \in Q}$, where m_{pq} is the number of edges from p to q.



$$M = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Irreducible and primitive matrices

A nonnegative square matrix (with real coefficients) M is *irreducible* if for every pair s, t of indices, there is an integer $n \geq 1$ such that $M^n_{s,t} > 0$. Otherwise, M is *reducible*.
A matrix M is reducible if and only if, up to a permutation of the indices, it can be written

$$M = \begin{bmatrix} U & V \\ 0 & W \end{bmatrix}$$

for some matrices U, V, W with U, W being square matrices of dimension ≥ 1.

A nonnegative square matrix M is *primitive*, if there is some integer $n \geq 1$ such that all entries of M^n are positive.
The least such n is called the *exponent* of M, denoted $\exp(M)$.
A primitive matrix is irreducible but the converse is not necessarily true.

Irreducible matrix

Lemma

If M is a nonnegative $Q \times Q$ irreducible matrix, then $(I + M)^{n-1} > 0$, where $n = \text{Card}\, Q$.

Proof.

Let G be the graph whose adjacency matrix is $I + M$.
Thus, $s \to t$ is an edge if and only if $(I + M)_{st} > 0$.
Since M is irreducible, there is a path of length at most $n - 1$ from s to t in G.
Since the state s has a self-loop, there is a path of length $n - 1$ from s to t in G.
Hence, $(I + M)^{n-1}_{st} > 0$ for all states $s, t \in Q$. □

Periods

The *period* of an irreducible nonnegative square matrix $M \neq 0$ is the greatest common divisor of the integers n such that M^n has a positive diagonal coefficient. By convention, the period of $M = 0$ is 1. If M has period p, then M and M^p have, up to a permutation of indices, the forms:

$$M = \begin{bmatrix} 0 & M_1 & 0 & \dots & 0 \\ 0 & 0 & M_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & M_{p-1} \\ M_p & 0 & 0 & \cdots & 0 \end{bmatrix}, \quad M^p = \begin{bmatrix} D_1 & 0 & 0 & \dots & 0 \\ 0 & D_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & D_{p-1} & 0 \\ 0 & 0 & \dots & 0 & D_p \end{bmatrix}$$

Thus M^p is block diagonal, with each diagonal block D_i primitive. An irreducible matrix is primitive if and only if it has period 1.

Periods

Example

The three matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

are nonnegative. The first one is reducible. The second one is irreducible but not primitive since it has period 2. The third one is primitive with exponent 2.

The Perron-Frobenius theorem

Theorem

Let M be a nonnegative real $Q \times Q$-matrix. Then

1. *M has an eigenvalue λ_M such that $|\mu| \leq \lambda_M$ for every eigenvalue μ of M.*
2. *There corresponds to λ_M a nonnegative eigenvector v, and a positive one if M is irreducible. If M is irreducible, λ_M is the only eigenvalue with a nonnegative eigenvector.*
3. *If M is primitive, the sequence (M^n/λ_M^n) converges to the matrix yx where x, y are positive left and right eigenvectors relative to λ_M with $\sum_{s\in Q} y_s = 1$ and $\sum_{s\in Q} x_s y_s = 1$.*

If M is irreducible, then λ_M is simple. The matrix M is primitive if and only if $|\mu| < \lambda_M$ for every other eigenvalue μ of M.

Spectral radius

An *eigenvector* of a square real matrix M for the eigenvalue λ (a real or complex number) is a **non null** vector v (with real or complex coefficients) such that $Mv = \lambda v$.

The *spectral radius* of a square real matrix is the real number

$$\rho(M) = \max\{|\lambda| \mid \lambda \text{ eigenvalue of } M\}.$$

The theorem states in particular that if a matrix M is irreducible, $\rho(M)$ is an eigenvalue of M that is algebraically simple. Furthermore, if M is primitive, any eigenvalue of M other than $\rho(M)$ has modulus less than $\rho(M)$.

Proof of Perron-Frobenius Points 1 and 2

Proposition

Any nonnegative matrix M has a real eigenvalue λ_M such that $|\lambda| \leq \lambda_M$ for any eigenvalue λ of M, and there corresponds to λ_M a nonnegative eigenvector v.
If M is irreducible, there corresponds to λ_M a positive eigenvector v, and λ_M is the only eigenvalue with a nonnegative eigenvector.

Proof of Perron-Frobenius Points 1 and 2

Proof.

We first assume that M **is irreducible**.
For any nonnegative real vector $v \neq 0$, let

$$r_M(v) = \min\{(Mv)_s / v_s \mid v_s \neq 0\}.$$

Thus $r_M(v)$ is the largest real number r such that $Mv \geq rv$.
One has $r_M(\lambda v) = r_M(v)$ for any nonnegative nonzero real number λ.
Moreover, the mapping $v \to r_M(v)$ is continuous on the set of nonnegative nonzero vectors.
The set X of nonnegative vectors v such that $\|v\| = 1$ is compact.
Define $\lambda_M = \max\{r_M(v) \mid v \in X\}$.
Since a continuous function on a compact set reaches its maximum on this set, there is an $x \in X$ such that $r_M(x) = \lambda_M$.
Since $r_M(v) = r_M(\lambda v)$ for $\lambda \geq 0, \lambda \neq 0$, we have
$\lambda_M = \max\{r_M(v) \mid v \geq 0, v \neq 0\}$. □

Proof of Perron-Frobenius Points 1 and 2

Proof.

We show that $Mx = \lambda_M x$.
By the definition of the function r_M, we have $Mx \geq \lambda_M x$.
Set $y = Mx - \lambda_M x$. Then $y \geq 0$.
Assume $Mx \neq \lambda_M x$. Then $y \neq 0$.
Since $(I + M)^n > 0$ for some $n \geq 1$, this implies that $(I + M)^n y > 0$.
But $(I + M)^n y = (I + M)^n (Mx - \lambda_M x) =$
$M(I + M)^n x - \lambda_M (I + M)^n x = Mz - \lambda_M z$ with $z = (I + M)^n x$.
This shows that $Mz > \lambda_M z$, which implies that $r_M(z) > \lambda_M$, a contradiction.
Thus, λ_M is an eigenvalue with a nonnegative eigenvector x.
Since $(I + M)^n x = (1 + \lambda_M)^n x$ is positive, we get $x > 0$. □

Proof of Perron-Frobenius Points 1 and 2

Proof.

Let us now show that $\lambda_M \geq |\lambda|$ for each real or complex eigenvalue λ of M.

Indeed, let v be an eigenvector corresponding to λ.

Then $Mv = \lambda v$.

Let $|v|$ be the nonnegative vector with coordinates $|v_s|$. Then $M|v| \geq |\lambda||v|$ by the triangular inequality.

By the definition of the function r_M, this implies $r_M(|v|) \geq |\lambda|$ and consequently $\lambda_M \geq |\lambda|$.

□

Proof of Perron-Frobenius (If M is irreducible, then λ_M is simple)

Proof.

We show that if M is irreducible, λ_M is a simple eigenvalue.

Let v be an eigenvector of M for λ_M (with complex coefficients).
We have seen that $w = |v|$ is a nonnegative eigenvector of M for λ_M.
We have $w > 0$. Indeed, since $(I + M)^n > 0$ and $w \neq 0$, we have $(I + M)^n w > 0$, And $(I + M)^n w = (1 + \lambda_M)^n w$, implying $w > 0$.
Hence, v has no null coefficient and $|v|$ is a positive eigenvector of M for λ_M.

Now let w, w' be two eigenvectors of M for λ_M.
Let $z = w'_s w - w_s w'$. Then $Mz = \lambda_M z$ and $z_s = 0$, implying $z = 0$ and w is colinear to w'.

□

Proof of Perron-Frobenius Points 1 and 2

Proof.

We show that if M is irreducible, λ_M is the only eigenvalue with a nonnegative eigenvector.

Let $Mv = \lambda v$ with $v \geq 0$, $v \neq 0$. Hence λ is a nonnegative real number.
Then $(I + M)^n v = (1 + \lambda)^n v > 0$ implying $v > 0$.

Let D be the diagonal matrix with coefficients v_s and $N = D^{-1}MD$.
We have $n_{st} = m_{st} v_t / v_s$ and $\sum_t n_{st} = \sum_t m_{st} v_t / v_s = \lambda$.
If w is a positive eigenvector of M for λ_M, then $D^{-1}w$ be a positive eigenvector of N for λ_M.
Let w be a positive eigenvector of N for λ_M, normalized in such a way that $w_s \leq 1$ for all s and $w_{s_0} = 1$ for some s_0.
Then $\lambda_M = \lambda_M w_{s_0} = \sum_t n_{s_0 t} w_t \leq \sum_t n_{s_0 t} = \lambda$.
Thus $\lambda = \lambda_M$.

Proof of Perron-Frobenius Points 1 and 2

Proof.

If M **is reducible**, we may consider a triangular decomposition:

$$M = \begin{bmatrix} U & V \\ 0 & W \end{bmatrix}.$$

Applying by induction the theorem to U and W, we obtain nonnegative eigenvectors u and w for the eigenvalues λ_U and λ_W of U and W. We prove that $\max(\lambda_U, \lambda_W)$ is an eigenvalue of M with some nonnegative eigenvector.

If $\lambda_U \geq \lambda_W$, then λ_U is an eigenvalue of M with nonnegative eigenvector $\begin{bmatrix} u \\ 0 \end{bmatrix}$.

Proof of Perron-Frobenius Points 1 and 2

Proof.

If $\lambda_U < \lambda_W$, then λ_W is an eigenvalue of M with nonnegative eigenvector $\begin{bmatrix} u' \\ w \end{bmatrix}$, where $u' = \sum_{n\geq 0}(U/\lambda_W)^n \lambda_W{}^{-1} Vw$.
Indeed, the spectral radius of U/λ_W is < 1, implying the convergence of $\sum_{n\geq 0}(U/\lambda_W)^n$ (Berstel Lemma).

Conversely, if λ is an eigenvalue of M with corresponding eigenvector $\begin{bmatrix} u \\ w \end{bmatrix}$, then λ is an eigenvalue of W if $w \neq 0$, and is an eigenvalue of U if $w = 0$.

We set $\lambda_M = \max(\lambda_U, \lambda_W)$.
Hence, $\max\{|\lambda| \mid \lambda \text{ eigenvalue of } M\} = \lambda_M$. □

Example

Example

The following matrix M is primitive (hence irreducible).

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

The eigenvalues are the roots φ, φ' of $\det(zI - M) = z^2 - z - 1$, where

$$\varphi = \frac{1+\sqrt{5}}{2}, \quad \varphi' = \frac{1-\sqrt{5}}{2}.$$

The vector $\begin{bmatrix} \varphi \\ 1 \end{bmatrix}$ is a (right) positive eigenvector for φ.

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \varphi \\ 1 \end{bmatrix} = \begin{bmatrix} \varphi + 1 \\ \varphi \end{bmatrix} = \begin{bmatrix} \varphi^2 \\ \varphi \end{bmatrix} = \varphi \begin{bmatrix} \varphi \\ 1 \end{bmatrix}.$$

Conjugacy invariants

Entropy

The (topological) entropy of a shift space X is

$$h(X) = \lim_{n \to \infty} \frac{1}{n} \log \mathrm{Card}(\mathcal{B}_n(X)).$$

The limit exists.

Lemma (Fekete Lemma)

Let $a_1, a_2, \ldots$ be a sequence of nonnegative numbers such that $a_{m+n} \leq a_m + a_n$ for $m, n \geq 1$, then $\lim_{n\to\infty} a_n/n$ exists and is equal to $\inf_{n\geq 1} a_n/n$.

Proof.

Let $\alpha = \inf_{n\geq 1} a_n/n$. We have $\inf_{n\geq 1} a_n/n \geq \alpha$ for all $n \geq 1$.
Fix $\varepsilon > 0$. There is $k \geq 1$ such that $a_k/k < \alpha + \varepsilon/2$.
Then for $0 \leq j < k$ and $m \geq 1$,

$$\begin{aligned}\frac{a_{mk+j}}{mk+j} &\leq \frac{a_{mk}}{mk+j} + \frac{a_j}{mk+j} \leq \frac{a_{mk}}{mk} + \frac{a_j}{mk} \\ &\leq \frac{ma_k}{mk} + \frac{ja_1}{mk} \leq \frac{a_k}{k} + \frac{a_1}{m} < \alpha + 1/2\varepsilon + \frac{a_1}{m}.\end{aligned}$$

For $n = mk + j$ large enough, $a_1/m < \varepsilon/2$ and $a_n/n < \alpha + \varepsilon$. □

Entropy

Lemma

If X is a shift space,

$$h(X) = \lim_{n\to\infty} \frac{1}{n} \log \mathrm{Card}(\mathcal{B}_n(X)).$$

exists and is equal to

$$\inf_{n\geq 1} \frac{1}{n} \log \mathrm{Card}(\mathcal{B}_n(X)).$$

Proof.

Let $m, n \geq 1$,

$$\mathrm{Card}(\mathcal{B}_{m+n}(X)) \leq \mathrm{Card}(\mathcal{B}_m(X)) \times \mathrm{Card}(\mathcal{B}_n(X)).$$

□

Entropy

Proposition

If there is a sliding block map $\varphi\colon X \to Y$ which is onto, then $h(Y) \leq h(X)$.

Proof.

If φ is a (m, a)-sliding block code, every block in $\mathcal{B}_n(Y)$ is the image of a block in $\mathcal{B}_{n+m+a}(X)$.
Hence, $\mathrm{Card}(\mathcal{B}_n(Y)) \leq \mathrm{Card}(\mathcal{B}_{n+m+a}(X))$.
Thus,

$$\begin{aligned} h(Y) &= \lim_{n\to\infty} \frac{1}{n} \log \mathrm{Card}(\mathcal{B}_n(Y)) \\ &\leq \lim_{n\to\infty} \frac{1}{n} \log \mathrm{Card}(\mathcal{B}_{n+m+a}(X)) \\ &= \lim_{n\to\infty} \left(\frac{n+m+a}{n}\right) \frac{1}{n+m+a} \log \mathrm{Card}(\mathcal{B}_{n+m+a}(X)) \\ &= h(X). \end{aligned}$$

Entropy

Corollary

If X and Y are conjugate, then $h(X) = h(Y)$.

Example

If X is the full shift $A^{\mathbb{Z}}$, then $h(X) = \log \mathrm{Card}(A)$.

Hence, the full shift on two letters is not conjugate to the full shift on three letters.

Computation of the entropy of a sofic shift

Proposition

Let $\mathcal{A} = (Q, E)$ be a trim deterministic automaton presenting a sofic shift X and $G = (Q, F)$ be the graph of $\mathcal{A}$. Then $h(X) = h(X_G)$.

Proof.

There is a 1-block sliding block code from X_G onto X (with no memory and no anticipation). Thus $h(X) \leq h(X_G)$.
If $\mathcal{A}$ has k states, and since $\mathcal{A}$ is deterministic, $\mathrm{Card}(\mathcal{B}_n(X_G)) \leq k\,\mathrm{Card}(\mathcal{B}_n(X))$. Thus $h(X) \geq h(X_G)$. □

Computation of the entropy of a sofic shift

Let $G = (Q, E)$ be a graph with adjacency matrix M, we have

$$\mathcal{B}_n(X_G) = \sum_{s,t \in Q} (M^n)_{st}.$$

If G is strongly connected, i.e. if M is irreducible, there is a positive eigenvector v for λ_M.
Let $c = \min v_q$, $d = \max v_q$.
Since $\sum_{t \in Q} (M^n)_{st} v_t = \lambda_M^n v_s$,

$$\sum_{s,t \in Q} (M^n)_{st} v_t = \sum_{s \in Q} \lambda_M^n v_s.$$

$$c \sum_{s,t \in Q} (M^n)_{st} \leq \sum_{s,t \in Q} (M^n)_{st} v_t \leq d \operatorname{Card}(Q) \lambda_M^n.$$

$$\sum_{s,t \in Q} (M^n)_{st} \leq (d/c) \operatorname{Card}(Q) \lambda_M^n.$$

Computation of the entropy of a sofic shift

Similarly

$$(c/d)\lambda_M^n \leq \sum_{s,t \in Q} (M^n)_{st}.$$

Proposition

Let $\mathcal{A} = (Q, E)$ be an irreducible deterministic automaton presenting an irreducible sofic shift X and M its adjacency matrix. Then $h(X) = \log \lambda_M$.

The result holds for a trim deterministic automaton presenting a sofic shift X with a reduction to the irreducible components of M (exercise).

Computation of the entropy of a sofic shift: example

Example

For the even shift,

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

$$h(X) = \log \varphi, \text{ where } \varphi = \frac{1+\sqrt{5}}{2}.$$

The even shift and the golden mean shift have the same entropy but are not conjugate.

Periodic points in a shift space

A point x of a shift space X is *periodic* if $S^n(x) = x$ for some $n \geq 1$ and we say that x has *period* n.
If x is periodic, the smallest positive integer n for which $S^n(x) = x$, called the least period of x, divides all periods of x.
Let

$$p_n(X) = \text{Card}\{x \in X \mid S^n(x) = x\}.$$

Proposition

Let $\varphi : X \to Y$ be a sliding block map. If x is a periodic point of X and has period n, then $\varphi(x)$ is periodic and has period n and the least period of $\varphi(x)$ divides the least period of x. If X and Y are conjugate, then $p_n(X) = p_n(Y)$ for each $n \geq 1$.

Proposition

Let G be a graph of transition matrix M, the number of cycles of length n in G is $\text{tr}(M^n)$ and this equals the number of points in X_G with period n.

Zeta function

The zeta function of a shift space X is the formal series

$$\zeta_X(z) = \exp\left(\sum_{n=1}^{\infty} \frac{p_n(X)}{n} z^n\right).$$

Proposition

If X and Y are conjugate, then $\zeta_X = \zeta_Y$.

Zeta function

Example

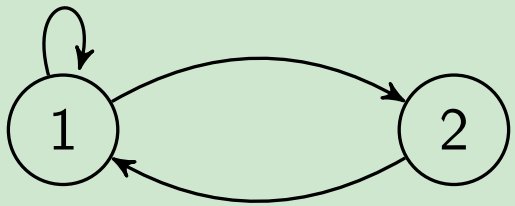
Let X be the full shift on a 2-letter alphabet.
Then, $p_n(X) = 2^n$ for each $n \geq 1$.

$$\zeta_X(z) = \exp\left(\sum_{n=1}^{\infty} \frac{2^n}{n} z^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{(2z)^n}{n}\right)$$
$$= \exp(-\log(1-2z)) = \frac{1}{1-2z}.$$

Zeta function

Example

Let G be the graph



Its transition matrix is

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

We have $p_n(X_G) = \mathrm{tr}(M^n) = \varphi^n + \varphi'^n$, where

$$\varphi = \frac{1+\sqrt{5}}{2}, \quad \varphi' = \frac{1-\sqrt{5}}{2}.$$

are the roots of $\det(zI - M) = z^2 - z - 1$.

Zeta function

Example

$$\zeta_{X_G}(z) = \exp\left(\sum_{n=1}^{\infty} \frac{\varphi^n + \varphi'^n}{n} z^n\right) = \exp\left(\sum_{n=1}^{\infty} \frac{\varphi^n}{n} + \frac{\varphi'^n}{n} z^n\right)$$

$$= \exp(-\log(1-\varphi z) - \log(1-\varphi' z)) = \frac{1}{(1-\varphi z)(1-\varphi' z)}$$

$$= \frac{1}{1-z-z^2} = \frac{1}{\det(I - Mz)}.$$

Zeta function of a shift of finite type

Theorem

Let G be a graph with adjacency matrix M. Then

$$\zeta_{X_G}(z) = \frac{1}{\det(I - Mz)}.$$

Zeta function of a shift of finite type

Proof.

We have

$$p_n(X_G) = \mathrm{tr}(M^n) = \lambda_1^n + \lambda_2^n + \cdots + \lambda_{|Q|}^n,$$

where $\lambda_1, \lambda_2, \ldots \lambda_{|Q|}$ are the roots of the characteristic polynomial of M listed with multiplicities.

$$\begin{aligned}
\zeta_{X_G}(z) &= \exp\left(\sum_{n=1}^{\infty} \frac{\lambda_1^n + \lambda_2^n + \cdots + \lambda_{|Q|}^n}{n} z^n\right) \\
&= \exp\left(\sum_{n=1}^{\infty} \frac{(\lambda_1 z)^n}{n} + \cdots + \sum_{n=1}^{\infty} \frac{(\lambda_{|Q|} z)^n}{n}\right) \\
&= \prod_{k=1}^{|Q|} \frac{1}{1-\lambda_k z} = \frac{1}{\det(I - Mz)}.
\end{aligned}$$

Observe that the zero eigenvalues "do not count".

The zeta function is an invariant stronger than entropy

If two edge shifts have the same zeta function, then they have the same entropy.
We have

$$\zeta_{X_G}(z) = \prod_{k=1}^{|Q|} \frac{1}{1-\lambda_k z} = \frac{1}{\det(I - Mz)}.$$

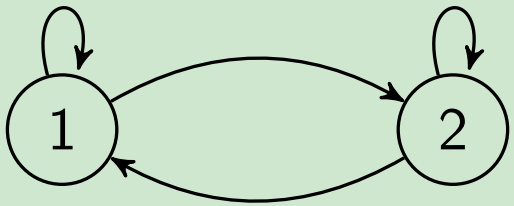
So the zeta function determines the list of nonzero eigenvalues of the M (with repeated eigenvalues listed according to their multiplicity), called the *nonzero spectrum of* M.

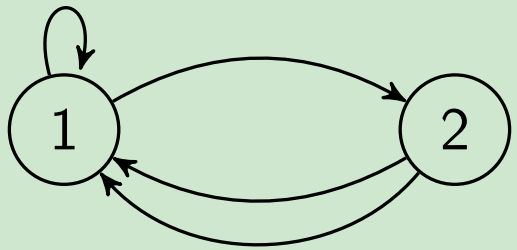
Thus, it determines the largest eigenvalue of M, and thus the entropy.
If G is strongly connected $h(X_G) = \log \lambda_M$. Otherwise $h(X_G) = \max \log \lambda_{M_i}$, where M_i is the adjacency matrix of all strongly connected components of G.

Applications

Example

Let G and H be the graphs





Show that the two edge shifts X_G and X_H are not conjugate although they have the same entropy.

Applications

Let M be the adjacency matrix of G and N the adjacency matrix of N.

$$\zeta_{X_G}(z) = \frac{1}{\det(I - Mz)}, \zeta_{X_H}(z) = \frac{1}{\det(I - Nz)}.$$

We have

$$\det(I - Mz) = \det \begin{bmatrix} 1-z & -z \\ -z & 1-z \end{bmatrix} = 1 - 2z.$$

$$\det(I - Nz) = \det \begin{bmatrix} 1-z & -z \\ -2z & 1 \end{bmatrix} = 1 - z - 2z^2.$$

Hence X_G and X_H have not the same zeta function, and thus are not conjugate.
We can also see that $p_2(X_G) = 4$ and $p_2(X_H) = 5$.

Applications

We have

$$\det(zI - M) = \det \begin{bmatrix} z-1 & -1 \\ -1 & z-1 \end{bmatrix} = z^2 - 2z = z(z-2).$$

Also obtained directly from $\det(I - Mz)$ by changing z into $1/\lambda$ and mutiplying by λ^2: $\lambda^2(1 - 2/\lambda) = \lambda(\lambda - 2)$.

$$\det(zI - N) = \det \begin{bmatrix} z-1 & -1 \\ -2 & z \end{bmatrix} = z^2 - z - 2 = (z-2)(z+1).$$

Hence, M and N have the same largest eigenvalue. Thus, X_G and X_H have the same entropy.

Master 2 Mathematics and Computer Science Symbolic Dynamics. Lecture 3

Marie-Pierre Béal

University Gustave Eiffel
Laboratoire d'informatique Gaspard-Monge UMR 8049

One-sided shift spaces

Overview

- One-sided shift spaces
- Decidability of conjugacy of one-sided shifts of finite type

One-sided shift spaces

A *one-sided shift space* is a closed subset X of $A^{\mathbb{N}}$ such that $S(X) \subseteq X$.

One-sided shift spaces are usually defined as closed subsets such that $S(X) = X$, but we do not require this stronger condition here.

The set $A^{\mathbb{N}}$ itself is a one-sided shift space, called the *one-sided full shift*.

For a two-sided sequence $x \in A^{\mathbb{Z}}$, we define $x^+ = x_0 x_1 \cdots$.
If X is a two-sided shift space, then the set $X^+ = \{x^+ \mid x \in X\}$ is a one-sided shift space.

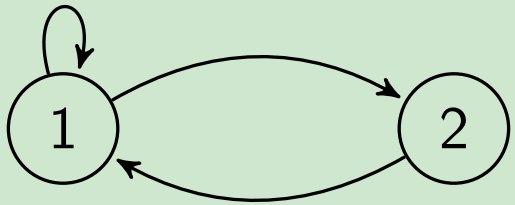
One-sided shift spaces of finite type

A one-sided shift space is *of finite type* if it is the set X_F of one-sided sequences over A avoiding all words of some finite set $F \subseteq A^*$.

A *one-sided edge shift* is the set X_G of right-infinite paths in a finite directed graph G. Note that the paths may start at any state.

Example

The one-sided edge shift X_G represented by the directed graph G:



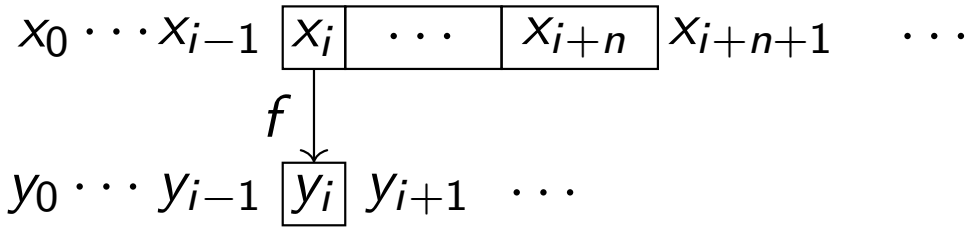
is also defined by the adjacency matrix of G, that is, by the matrix

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

One-sided conjugacy

The *one-sided (sliding) block code* defined by f is the map $\varphi : X \to B^{\mathbb{N}}$ defined by $\varphi(x) = y$ if for every $i \in \mathbb{N}$, $y_i = f(x_{[i,i+n]})$, where $f : \mathcal{B}_{n+1}(X) \to B$.

n is the anticipation, and no memory is allowed.



A *one-sided conjugacy* $\varphi : X \to Y$ is a bijective one-sided block code. Its inverse is also a one-sided block code.

One-sided edge shifts

Proposition

Any one-sided shift of finite type is conjugate to a one-sided edge shift.

Proof.

Almost the same proof as for two-sided edge shifts.

Let $X = \mathsf{X}_F$ with F finite, and let n be the maximal size of words in F. We may assume that all words in F have size n.
Let $\mathcal{A} = (Q, E)$, where Q is the set of words of length $n-1$ with edges $a_0 a_1 \dots a_{n-2} \xrightarrow{a_0} a_1 \dots a_{n-2} a$, where $a_0 a_1 \dots a_{n-2} a \notin F$. We keep only the trim part of this automaton, that is, only the states having at least one outgoing edge.

Then all paths of $\mathcal{A}$ labeled by a word w of length $n-1$ start at the same state q_w. □

proof continued.

Let Y be the set of right-infinite paths of $\mathcal{A}$.
Let $\phi\colon Y \to X$ defined by the 1-block map $f : E \to A$ with $f(e = (p, a, q)) = a$.
Then the one-sided sliding block code $\varphi\colon X \to Y$ with memory 0 and anticipation $n-1$ defined by the n-block map $g\colon A^n \to E$ with $g(a_0 a_1 \dots a_{n-1}) = (p, a_0, q)$, where $p = a_0 a_1 \dots a_{n-2}$ and $q = a_1 a_2 \dots a_{n-1}$.
The map φ is the inverse of ϕ.

□

Out-splitting (reminder, see Lecture 2)

Let X_G be a one-sided edge shift defined by a directed graph $G = (V, E)$. We may assume that the graph is *trim*, that is, that each vertex has at least one outgoing edge.

An *out-splitting* of G is a transformation of G into a graph $G' = (V', E')$ obtained by selecting a vertex s and partitioning the set of edges going out of s into two non-empty sets E_1 and E_2.

- $V' = V \setminus \{s\} \cup \{s_1, s_2\}$,
- E' contains all edges of E neither starting at or ending in s,
- E' contains the edge (s_1, a, t) for each edge $(s, a, t) \in E_1$, and the edge (s_2, a, t) for each edge $(s, a, t) \in E_2$, so long as $t \neq s$,
- E' contains the edges (t, a, s_1) and (t, a, s_2) if (t, a, s) in E, when $t \neq s$,
- E' contains the edges (s_1, a, s_1) and (s_1, a, s_2) if (s, a, s) in E_1, and the edges (s_2, a, s_1) and (s_2, a, s_2) if $(s, a, s) \in E_2$.

Out-splitting (reminder, see Lecture 2)

Example

The graph G' in the right part of the figure is an out-split of the graph G in the left part of the figure. Here, $s = 1$, and the partition of the outgoing edges of 1 is $\{E_1, E_2\}$, where E_1 contains the loop around 1, and E_2 contains the two edges going from 1 to 2.

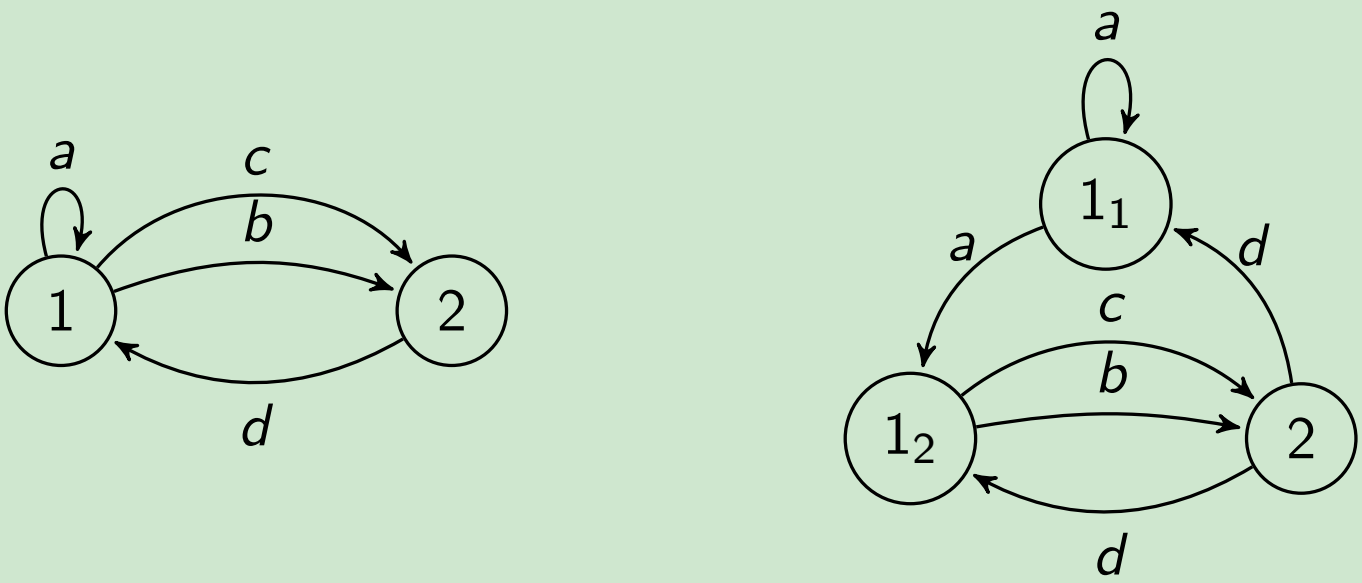


Figure: An out-splitting.

Out-merging

The inverse operation of an out-splitting is referred to as an *out-merging*. An out-merging of a directed graph $G' = (V', E')$ can be performed if there are two vertices s_1, s_2 of G' such that the adjacency matrix M' satisfies:

- the column of index s_1 is equal to the column of index s_2 of M'.

The adjacency matrix of G is thus the matrix M obtained by adding the rows of index s_2 to the row of index s_1 of M' and then removing the column of index s_2 afterward.

The graph G is called an *elementary amalgamation* of G'. Notice that even if M' has 0-1 entries, M may not have 0-1 entries.

General amalgamation

Let M' be the adjacency matrix of a directed graph G', and $(V_1, V_2, \ldots, V_k)$ be a partition of V' into classes such that if s, t belong to the same class, then the columns of indices s and t of M' are identical.

When at least one set of the partition has a size greater than 1, we can perform a *general merging*. We define a graph K of adjacency matrix N obtained by merging all states of each $V_i = \{s_{i,1}, \ldots s_{i,k_i}\}$ into a single state $s_{i,1}$.

The row in N corresponding to $s_{i,1}$ is obtained by summing the rows of the states of V_i in M' and removing the columns $s_{i,2}, \cdots, s_{i,k_i}$.

The graph K is called a *general amalgamation* of G'.

Decomposition theorem

Proposition (R. Williams 1973)

Let X (resp. Y) be a one-sided edge shift defined by an irreducible directed graph G (resp. H), Then X and Y are conjugate if and only if there is a sequence of out-splittings and out-mergings from G to H.

Proof.

The same proof as the proof for two-sided edge shifts. Here we use only out-splittings and out-mergings. □

Two out-merging transformations commute

Proposition (R. Williams 1973)

If G and H are amalgamations of a common directed graph L, then they have a common amalgamation K.

Proposition (R. Williams 1973)

Let G and H be irreducible directed graphs that define one-sided edge shifts X_G and X_H. Then X_G and X_H are conjugate if and only if G and H have the same total amalgamation.

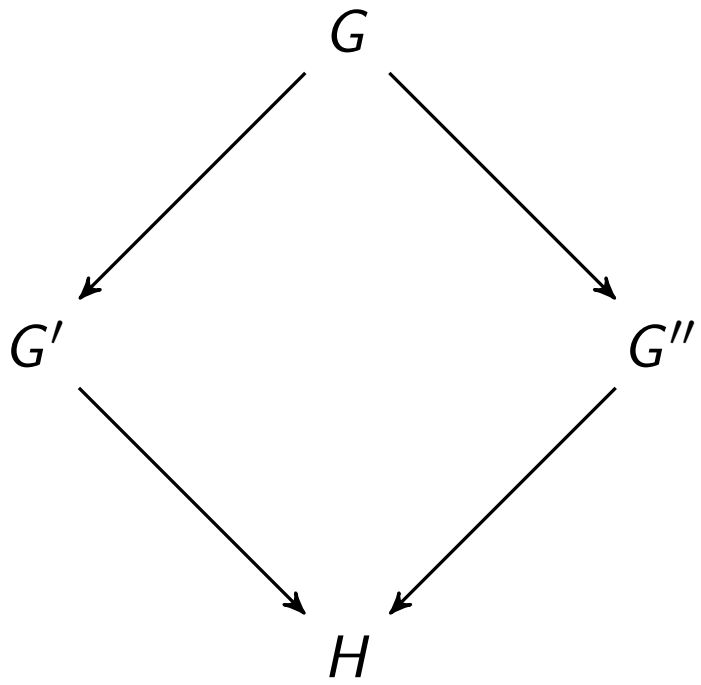
It also holds for one-sided edge shifts defined by trim directed graphs.

Decidability of conjugacy of one-sided shifts of finite type

Corollary (R. Williams 1973)

It is decidable whether two one-sided shifts of finite are conjugate.

One-sided conjugacy



Two out-merging transformations commute.

There is a unique graph, up to a renaming of the vertices, obtained by performing elementary out-mergings until we cannot perform anymore. This graph is called the *total amalgamation* of G.

Two out-merging transformations commute

Proposition (R. Williams 1973)

If G and H are amalgamations of a common directed graph L, then they have a common amalgamation K.

Proof.

Let us assume that there is an out-merging of G with adjacency matrix M into G' with adjacency matrix M', obtained by merging s_1 and s_2 into s_1, and an out-merging of G into G'' with adjacency matrix M'', obtained by merging s_3 and s_4 into s_3.
We may assume that the set $\{s_3, s_4\}$ is distinct from the set $\{s_1, s_2\}$.

Let us show that there is a graph H that is an out-merging of both G' and G''.

Two out-merging transformations commute

Proof.

Thus, by hypothesis,

- the columns of index s_1 and s_2 of M are equal.
- the columns of index s_3 and s_4 of M are equal.

The matrix M' obtained by adding the rows of index s_2 to the row of index s_1 of M and then removing the column of index s_2 afterward.
The matrix M'' obtained by adding the rows of index s_4 to the row of index s_3 of M and then removing the column of index s_3 afterward. □

Two out-merging transformations commute

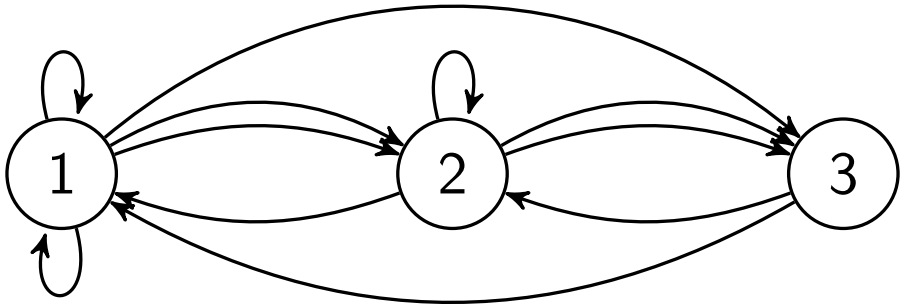
Proof.

- If both s_3, s_4 are distinct from s_1 and s_2, we define H as the out-merging of G' obtained by merging s_3 and s_4 into s_3. It is trivial that H is also the out-merging of G'' obtained by merging s_1 and s_2 into s_1.
- If $s_3 = s_1$, then we define H as the out-merging of G' obtained by merging s_1 and s_4 into s_1.
  Indeed, the columns of index s_1, s_2, s_3 and s_4 of M are equal.
  Hence, the columns of index s_1 and s_4 of M' are equal.
  It is clear that H is also the out-merging of G'' obtained by merging s_1 and s_2 into s_1.

□

Total amalgamation

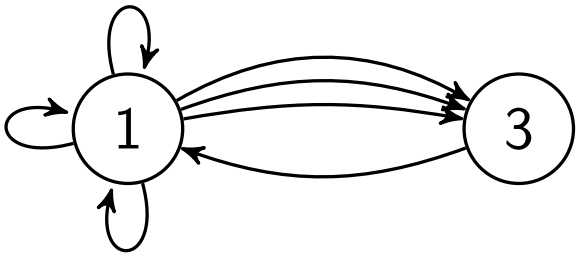
If G is the following graph:



$$M = \begin{bmatrix} 2 & 2 & 1 \\ 1 & 1 & 2 \\ 1 & 1 & 0 \end{bmatrix}$$

Total amalgamation

Its total amalgamation is H:



$$N = \begin{bmatrix} 3 & 3 \\ 1 & 0 \end{bmatrix}$$

Master 2 Mathematics and Computer Science Symbolic Dynamics. Lecture 5

Marie-Pierre Béal

University Gustave Eiffel
Laboratoire d'informatique Gaspard-Monge UMR 8049

Overview

- Substitutions, substitution shifts.
- Primitive substitutions, linear recurrence, minimality, and uniform recurrence, return words, block complexity.

Substitutions, substitution shifts

Substitutions

Given two finite alphabets A, B, a *substitution* $\sigma : A^* \to B^*$ is a monoid morphism from A^* to B^*.
Thus $\sigma(\varepsilon) = \varepsilon$ and $\sigma(uv) = \sigma(u)\sigma(v)$ for every $u, v \in A^*$.
The substitution is determined by the images $\sigma(a)$ of the letters $a \in A$.
Indeed, we have $\sigma(a_0 a_1 \cdots a_{n-1}) = \sigma(a_0)\sigma(a_1)\cdots\sigma(a_{n-1})$ for $a_i \in A$ and $n \geq 0$.

Extension to infinite sequences

Such a substitution σ extends to a partial map from $A^{\mathbb{N}}$ to $B^{\mathbb{N}}$.
It is defined by $\sigma(x_0x_1\cdots) = \sigma(x_0)\sigma(x_1)\cdots$ if the righthand side is infinite, that is, if $\sigma(x_0)\sigma(x_1)\cdots \in B^{\mathbb{N}}$.
The right-hand side is possibly a finite word (if $\sigma(x_n) = \varepsilon$ for all n sufficiently large). In this case, $\sigma(x_0x_1\cdots)$ is undefined.
A substitution $\sigma\colon A^* \to B^*$ also extends to a partial map from $A^{\mathbb{Z}}$ to $B^{\mathbb{Z}}$ by

$$\sigma(\cdots x_{-1} \cdot x_0x_1\cdots) = \cdots\sigma(x_{-1}) \cdot \sigma(x_0)\sigma(x_1)\cdots \qquad (1)$$

The result is a two-sided infinite sequence provided $\sigma(x_n) \neq \varepsilon$ for an infinite number of negative and positive indices n.

Extension to infinite sequences

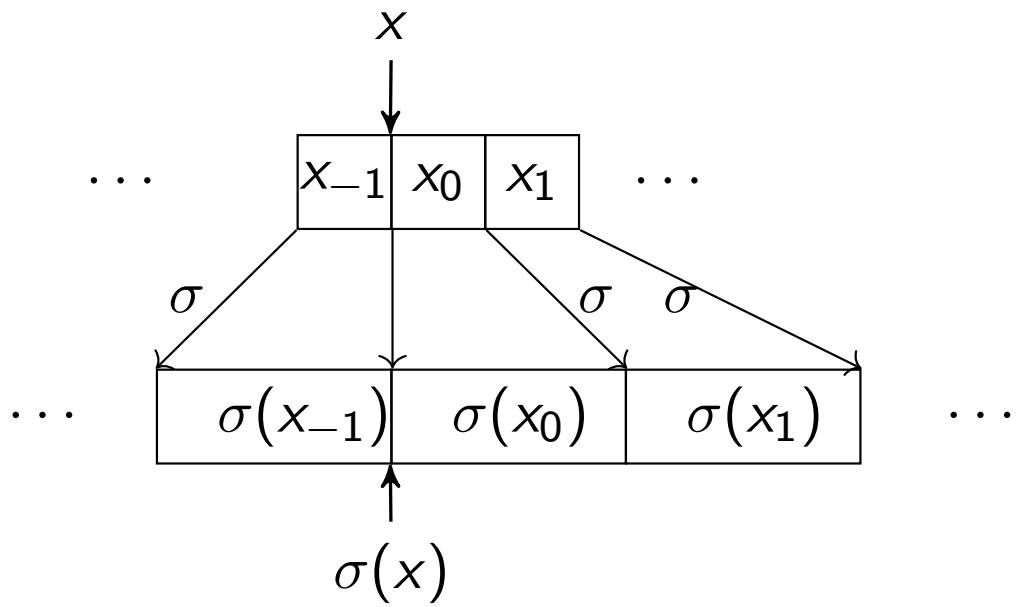


Figure: The two-sided sequence $\sigma(x)$.

A substitution $\sigma : A^* \to B^*$ is *non-erasing* if $\sigma(a)$ is nonempty for every $a \in A$.
A substitution $\sigma : A^* \to B^*$ has *constant length* k (or is *uniform*) if $|\sigma(a)| = k$ for every $a \in A$. A substitution of constant length $k \geq 1$ is non-erasing.

Lettre coding

A substitution $\sigma : A^* \to B^*$ is a *letter coding* if it is of constant length 1. Letter codings, also called *letter-to-letter* substitutions, play an important role in the definition of morphic sequences (see later).
They are the substitutions preserving length, meaning that $|\sigma(w)| = |w|$ for every $w \in A^*$. They also correspond to 1-block sliding block codes.

For a substitution $\sigma : A^* \to B^*$, we define

$$|\sigma| = \max_{a \in A} |\sigma(a)|, \quad \text{and} \quad \langle \sigma \rangle = \min_{a \in A} |\sigma(a)| \tag{2}$$

Composition matrix

Let $\sigma : A^* \to B^*$ be a substitution. The *composition matrix* of σ is the $(B \times A)$-matrix $M = M(\sigma)$ defined by

$$M_{b,a} = |\sigma(a)|_b,$$

where $|\sigma(a)|_b$ is the number of occurrences of the letter b in the word $\sigma(a)$. Thus, the composition vector of each $\sigma(a)$ is the column of index a of the matrix $M(\sigma)$.
If $\sigma : B^* \to C^*$ and $\tau : A^* \to B^*$ are substitutions, we have

$$M(\sigma \circ \tau) = M(\sigma)M(\tau).$$

Indeed, for every $a \in A$ and $c \in C$, we have

$$M(\sigma \circ \tau)_{c,a} = |\sigma \circ \tau(a)|_c = \sum_{b \in B} |\sigma(b)|_c |\tau(a)|_b = (M(\sigma)M(\tau))_{c,a}.$$

The transpose of $M(\sigma)$ is called the *adjacency matrix*.

Composition matrix

For a word $w \in A^*$, we denote by $\ell(w)$ the column vector $(|w|_a)_{a \in A}$, called the *composition vector* of w.
The composition matrix satisfies, for every $w \in A^*$, the equation

$$\ell(\sigma(w)) = M(\sigma)\ell(w). \tag{3}$$

Example

The composition matrix of $\sigma : a \mapsto ab, b \mapsto aa$ is

$$M(\sigma) = \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}.$$

Iteration of a substitution

A substitution $\sigma : A^* \to A^*$ from A^* into itself is an endomorphism of the monoid A^*. It can be iterated, that is, its powers σ^n for $n \geq 1$ are also substitutions.

Let $\sigma : A^* \to A^*$ be an iterable substitution. The *language* of σ, denoted by $\mathcal{L}(\sigma)$ is the set of words occurring as blocks in the words $\sigma^n(a)$ for some $n \geq 0$ and some $a \in A$.
It follows from the definition that

$$\sigma(\mathcal{L}(\sigma)) \subseteq \mathcal{L}(\sigma). \tag{4}$$

The language $\mathcal{L}(\sigma)$ is decidable (exercise).

Substitution shift

Let $\sigma : A^* \to A^*$ be an iterable substitution.
The *substitution shift* defined by σ is the shift space $\mathsf{X}(\sigma)$ consisting of all $x \in A^{\mathbb{Z}}$ whose finite blocks belong to $\mathcal{L}(\sigma)$.

Show that it is a shift space.

Since $\sigma(\mathcal{L}(\sigma)) \subseteq \mathcal{L}(\sigma)$ by (4), we have also

$$\sigma(\mathsf{X}(\sigma)) \subseteq \mathsf{X}(\sigma). \tag{5}$$

Example: Fibonacci

Example

The substitution $\sigma : a \mapsto ab, b \mapsto a$ is the *Fibonacci substitution*. The shift $X = \mathrm{X}(\sigma)$ is the *Fibonacci shift*.

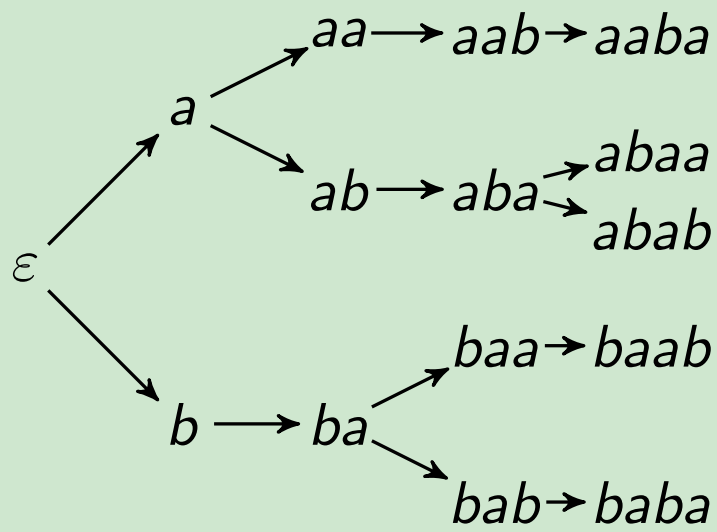


Figure: The words of $\mathcal{B}(X)$ for the Fibonacci shift.

Example: Thue-Morse

Example

The substitution $\sigma : a \mapsto ab, b \mapsto ba$ is the *Thue-Morse substitution*.
The shift $X = \mathrm{X}(\sigma)$ is the *Thue-Morse shift*.

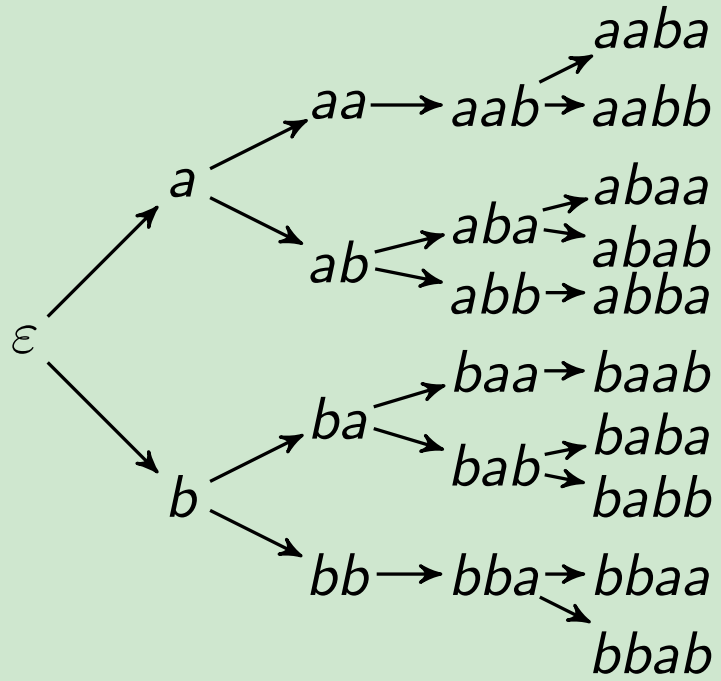


Figure: The words of $\mathcal{B}(X)$ for the Thue-Morse shift.

Blocks of a substitution shift

Note that $\mathcal{B}(\mathrm{X}(\sigma)) \subseteq \mathcal{L}(\sigma)$, but the converse inclusion may not hold, as shown in the example below.

Example

Consider the substitution $\sigma : a \mapsto ab, b \mapsto b$. We have $\mathcal{L}(\sigma) = ab^* \cup b^*$ but $\mathrm{X}(\sigma) = b^\infty$, and thus $\mathcal{B}(\mathrm{X}(\sigma)) = b^*$.

Erasable and growing letters

Let $\sigma : A^* \to A^*$ be an iterable substitution. A letter $a \in A$ is *erasable* if $\sigma^n(a) = \varepsilon$ for some $n \geq 1$.
A word is *erasable* if it is formed of erasable letters.

A word $w \in A^*$ is *growing* for σ if the sequence $(|\sigma^n(w)|)_n$ is unbounded.
A word is growing if and only if at least one of its letters is growing.
The substitution σ itself is said to be *growing* if all letters are growing.
We have the following property of growing letters.

Proposition

If $a \in A$ is growing for σ, then for every $r \geq 0$, $\sigma^{r\,\mathrm{Card}(A)}(a)$ contains at least $r+1$ non-erasable letters. In particular, $\lim_{n\to+\infty} |\sigma^n(a)| = +\infty$.

Lemma growing

Proof.

Set $k = \mathrm{Card}(A)$.

- Assume first that $\sigma^k(a)$ contains only one non-erasable letter. Then this letter has to be growing.
  Next, by the pigeonhole principle, there are i, p with $i + p \leq k$ and $p \geq 1$ such that $\sigma^i(a) = ubv$ and $\sigma^p(b) = rbs$ with u, v, r, s erasable and b a growing letter.
  Since r, s are erasable, $\sigma^k(r) = \varepsilon$ and $\sigma^k(s) = \varepsilon$.
  Set $w = \sigma^{kp}(b) = \sigma^{(k-1)p}(r) \cdots \sigma^p(r) rbs \sigma^p(s) \cdots \sigma^{(k-1)p}(s)$.
  Then $\sigma^p(w) = w$, a contradiction with the fact that b is growing. This proves the statement for $r = 1$.
- Assume that $\sigma^{rk}(a)$ contains $s \geq r + 1$ non-erasable letters $a_1, \ldots, a_s$. One of them, say a_i, must be growing. Then each of the $\sigma(a_1), \ldots, \sigma(a_s)$ contains a non-erasing letter and $\sigma^k(a_i)$ contains at least two due (case $r = 1$). Therefore, $\sigma^{(r+1)k}(a)$ contains at least $r + 2$ non-erasing letters.

The graph $G(\sigma)$

We associate with an iterable substitution $\sigma : A^* \to A^*$ the graph $G(\sigma)$ having A as the set of vertices and $|\sigma(a)|_b$ edges from a to b. The adjacency matrix of $G(\sigma)$ is the adjacency matrix of σ.

Example

Let $\sigma : a \mapsto ab, b \mapsto a$ be the Fibonacci substitution.

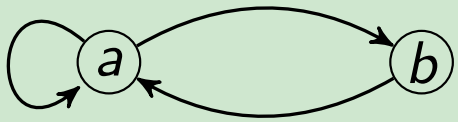


Figure: The graph $G(\sigma)$.

The adjacency matrix of σ is

$$M = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Part 2

Primitive substitutions, linear recurrence, minimality, and uniform recurrence, return words, block complexity.

Primitive substitutions

An iterable substitution $\sigma : A^* \to A^*$ is *primitive* if there is an integer $n \geq 1$ such that for every $a, b \in A$ one has $|\sigma^n(a)|_b \geq 1$.

For a primitive substitution σ, except the trivial case $A = \{a\}$ and $\sigma(a) = a$, every letter is growing and $\mathcal{L}(\sigma) = \mathcal{B}(\mathrm{X}(\sigma))$ (exercise).

A substitution shift $X = \mathrm{X}(\sigma)$ is *primitive* if σ is primitive, and not the identity on a one-letter alphabet.

Exercise

Show that $\mathcal{L}(\sigma) = \mathcal{B}(\mathrm{X}(\sigma))$ if and only if $\mathcal{L}(\sigma)$ is extendable, *i.e.* if for each $u \in \mathcal{L}(\sigma)$, there are letters a, b such that $aub \in \mathcal{L}(\sigma)$.

Minimal shift spaces

A shift space X is *minimal* if it is nonempty and if, for every subshift $Y \subseteq X$, one has $Y = \emptyset$ or $Y = X$.

Equivalently, X is minimal if and only if the closure of the orbit $\mathcal{O}(x) = \{S^n(x) \mid n \in \mathbb{Z}\}$ of x is equal to X, for every $x \in X$.

A shift space is minimal if and only if the closure $\mathcal{O}^+(x) = \{S^n(x) \mid n \in \mathbb{N}\}$ of x is equal to X, for every $x \in X$.

Indeed, if X is minimal and Y equal to the closure of $\mathcal{O}^+(x)$, then $Z = \cap_{n \geq 0} S^n(Y)$ is nonempty shift contained in X, thus equal to X. (It is nonempty by compacity as a decreasing sequence of nonempty compact sets).

Return words

Let X be a shift space. Given a word $u \in \mathcal{B}(X)$, a *return word* to u in X is a nonempty word w such that $wu \in \mathcal{B}(X)$ and wu has exactly two occurrences of u: one as a prefix and one as a suffix.

By convention, a return word to the empty word is a letter. The set of return words to u in X is denoted by $\mathcal{R}_X(u)$.

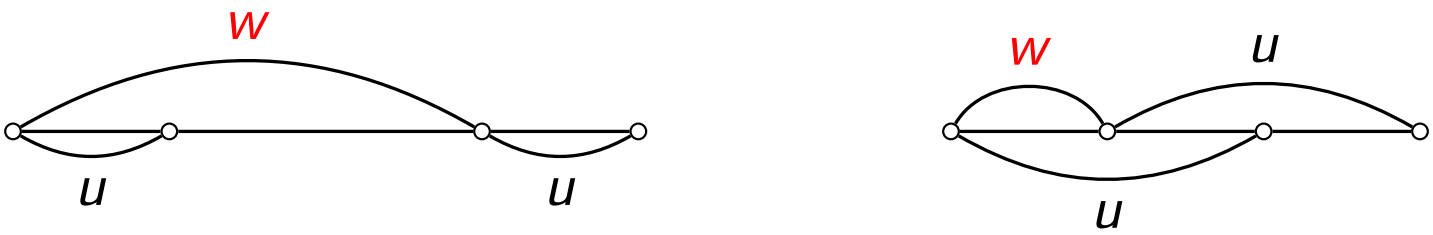


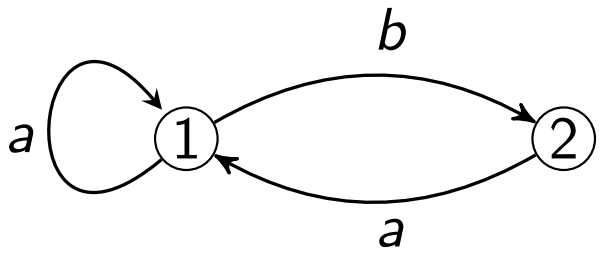
Figure: Return word to u.

The set of return words to u is a *suffix code*, that is, a set S of nonempty words such that no element of S is a proper suffix of another one.

Example

Example

The set of return words to b in the golden mean shift X is $\mathcal{R}_X(b) = ba^+$.



Uniform recurrence

A nonempty shift space X is *recurrent* if it is irreducible, that is, for every $u, v \in \mathcal{B}(X)$ there is a block $w \in \mathcal{B}(X)$ such that $uwv \in \mathcal{B}(X)$.

A nonempty shift space X is *uniformly recurrent* if for every $w \in \mathcal{B}(X)$ there is an integer $n \geq 1$ such that w occurs in every word of $\mathcal{B}_n(X)$.

As an equivalent definition, a shift space X is uniformly recurrent if for every $n \geq 1$ there is an integer $N = R_X(n)$ such that every word of $\mathcal{B}_n(X)$ occurs in every word of $\mathcal{B}_N(X)$. The function R_X is called the *recurrence function* of X.

Remark: Uniform recurrence implies recurrence

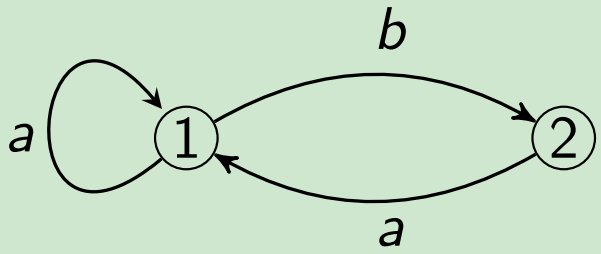
Uniform recurrence implies recurrence.

Indeed, let $u, v \in \mathcal{B}(X)$ and $n \geq 1$ such that u and v occur in every word of $\mathcal{B}_n(X)$.
Then every word w in $\mathcal{B}_{2n}(X)$ contains a block uzv for some block z, since u appears in the first half of w and v in the second half.

Example

Example

The golden mean shift X is recurrent but not uniformly recurrent since b is in $\mathcal{B}(X)$ although b does not occur in any $a^n \in \mathcal{B}(X)$.



Minimality and uniform recurrence

Proposition

A shift space is minimal if and only if it is uniformly recurrent.

Proof.

Assume first that X is a minimal shift space and consider $u \in \mathcal{B}(X)$. Since X is minimal, the forward orbit $\mathcal{O}^+(x) = \{S^n(x) \mid n \geq 0\}$ of every $x \in X$ is dense, and thus the integer $n(x) = \min\{n > 0 \mid S^n x \in [u]_X\}$ exists.
The map $x \mapsto n(x)$ is continuous since the set of x such that $n(x) = n$ is the open set $S^{-n}([u]_X) \setminus \cup_{i=1}^{n-1} S^{-i}([u]_X)$. Since the map $x \mapsto n(x)$ is continuous on a compact space, the integers $n(x)$ are bounded. Then u occurs in every word $w \in \mathcal{B}(X)$ of length $|u| + \max n(x)$. Thus, X is uniformly recurrent.
Conversely, if X is uniformly recurrent, the orbit of every $x \in X$ is dense, and thus X is minimal. □

Example

Example

The golden mean shift is not minimal since it contains the one-point set $\{a^\infty\}$ which is closed and shift-invariant.

Example

The periodic shift generated by $(abc)^\infty$ is minimal.

We define $u^\infty = \cdots uu \cdot uuu \cdots$

Primitive substitution shifts are minimal

Proposition

Let $\sigma : A^* \to A^*$ be a substitution distinct from the identity on a one-letter alphabet. If σ is primitive, then it is growing, and $\mathrm{X}(\sigma)$ is minimal. The converse is true if, additionally, every letter is in $\mathcal{B}(X)$.

Proof.

Let $\sigma : A^* \to A^*$ be primitive. Since the trivial case $A = \{a\}$ and $\sigma(a) = a$ is excluded, we have $\mathcal{B}(\mathrm{X}(\sigma)) = \mathcal{L}(\sigma)$.
Let $n \geq 1$ be such that every $b \in A$ occurs in every $\sigma^n(a)$ for $a \in A$. □

Primitive substitution shifts are minimal

Proof.

For $u \in \mathcal{L}(\sigma)$, let $m \geq 1$ and $b \in A$ be such that u occurs in $\sigma^m(b)$.
Then u occurs in every $\sigma^{n+m}(a)$.
Let v be a block of $X(\sigma)$ of length $2|\sigma|^{n+m}$.
Then v is a block of eveny $\sigma^{n+m+p}(c)$ for $c \in A$ and $p \geq 0$ large enough.
Thus, v is a block of some $\sigma^{n+m}(z)$, with $z \in A^*$.
Since the size of v is larger than or equal to the size of $\sigma^{n+m}(ab)$, for any letters a, b, it contains $\sigma^{n+m}(a)$, for some letter a, and thus it contains u as a block.
This shows that X(σ) is uniformly recurrent, and thus minimal.

□

.

Primitive substitution shifts are minimal

Proof.

Conversely, if $X = \mathrm{X}(\sigma)$ is minimal, and every letter is in $\mathcal{B}(X)$ and there is an $n \geq 1$ such that every letter appears in every word of $\mathcal{B}_n(X)$.
Since σ is growing, there is m such that $\langle \sigma^m \rangle \geq n$. Then every letter $b \in A$ occurs in every $\sigma^m(a)$ with $a \in A$. □

.

Examples

Example

The Fibonacci substitution $\sigma : a \mapsto ab, b \mapsto a$ is primitive.
According to the proposition, the Fibonacci shift $\mathrm{X}(\sigma)$ is minimal.

Example

The Thue-Morse substitution $\sigma : a \mapsto ab, b \mapsto ba$, is primitive.
Accordingly to the proposition, the Thue-Morse shift $\mathrm{X}(\sigma)$ is minimal.

Prolongable

A substitution $\sigma : A^* \to A^*$ is *prolongable* (or *right prolongable*) on $u \in A^+$ if $\sigma(u)$ begins with u and u is growing.

In this case, there is a unique right-infinite sequence, denoted $\sigma^\omega(u)$ such that each $\sigma^n(u)$ is a prefix of $\sigma^\omega(u)$.

One has, of course $\sigma^\omega(u) = \lim_{n\to\infty} \sigma^n(u)$.

Note also that $\sigma^\omega(u)$ is a right-infinite fixed point of σ.

Fibonacci

Example

The substitution $\sigma : a \mapsto ab, b \mapsto a$ is the Fibonacci substitution and $x = \sigma^\omega(a)$ is the *Fibonacci sequence*.

$$x = \sigma^\omega(a) = abaababaabaababaababaabaab \dots$$

Chacon

Example

The substitution $\sigma : a \mapsto aaba, b \mapsto b$ is the *Chacon binary substitution* and $x = \sigma^\omega(a)$ is the *Chacon binary sequence*.

The Chacon binary substitution is not primitive, but the shift $\mathrm{X}(\sigma)$, called the *Chacon binary shift*, is minimal.

This can be proved either directly (Exercise) or by exhibiting a primitive substitution τ such that $\mathrm{X}(\sigma)$ is conjugate to $\mathrm{X}(\tau)$ (Exercise, next slide).

Chacon is minimal

Example

The primitive substitution $\tau : 0 \to 0012, 1 \to 12, 2 \to 012$ is the *Chacon ternary substitution*.

Show that $w_n = \tau^n(0)$ satisfies the recurrence relation $w_{n+1} = w_n w_n 1 w'_n$, where w'_n is obtained from w_n by changing the initial letter 0 into a 2.

Deduce from this that the 1-block map $\theta : 0, 2 \to 0, 1 \to 1$ defines a conjugacy from the substitution shift $\mathrm{X}(\tau)$ called the *Chacon ternary shift*, to the Chacon binary shift $\mathrm{X}(\sigma)$.

As a consequence, the Chacon binary shift is minimal.

Chacon is minimal

Proof.

Set $w_n = 0t_n$ and thus $w'_n = 2t_n$ for $n \geq 0$. Then we have

$$w_{n+1} = \tau(w_n) = 0012\tau(t_n) = 0\tau(2t_n) = 0\tau(w'_n)$$

showing that $t_{n+1} = \tau(w'_n)$ for $n \geq 0$. Thus

$$\begin{aligned} w_{n+1} &= \tau(w_{n-1}w_{n-1}1w'_{n-1}) = w_nw_n12\tau(w'_{n-1}) \\ &= w_nw_n12t_n = w_nw_n1w'_n. \end{aligned}$$

The map θ sends the infinite word $\tau^\omega(0)$ to $\sigma^\omega(a)$ and thus maps $\mathrm{X}(\tau)$ to $\mathrm{X}(\sigma)$. Its inverse is the map that replaces 0 by 2 whenever it is immediately preceded by 1. Thus θ is a conjugacy. □

Return words

Proposition

A shift space X is uniformly recurrent if and only if it is irreducible, and for every $u \in \mathcal{B}(X)$ the set of return words to u is finite.

Proof.

Assume first that X is uniformly recurrent. Let $u \in \mathcal{B}_n(X)$ and let $v \in \mathcal{B}(X)$ be of length $R_X(n) - n + 1$ with $vu \in \mathcal{B}(X)$. Then vu has length $R_X(n) + 1$ and thus u has a second occurrence in vu. This shows that v has a suffix in $\mathcal{R}_X(u)$. Thus $\max\{|w| + n - 1 \mid w \in \mathcal{R}_X(u), u \in \mathcal{B}_n(X)\} \leq R_X(n)$ and $\mathcal{R}_X(u)$ is finite.

□

Return words

Proof.

Conversely, let $N = \max\{|w| + n - 1 \mid w \in \mathcal{R}_X(u), u \in \mathcal{B}_n(X)\}$. Let $u \in \mathcal{B}_n(X)$ and $r \in \mathcal{B}_N(X)$. Since X is irreducible, there are words s, t such that $usrtu \in \mathcal{B}(X)$. If r has no block equal to u, this implies that r occurs in some uvu, where r is not a prefix or a suffix of uvu and $uv \in \mathcal{R}_X(u)$. This implies
$|uv| + n - 1 \leq N = |r| \leq |uvu| - 2$, whence
$n - 1 \leq |u| - 2 = n - 2$, a contradiction. Thus, $R_X(n) \leq N$. □

Example

Let $\sigma : a \mapsto ab, b \mapsto ba$ be the Thue-Morse substitution and $X = \mathsf{X}(\sigma)$ be the Thue-Morse shift.

We have

$$\begin{aligned} \mathcal{R}_X(ab) &= \{ab, aba, abb, abba\}, \\ \mathcal{R}_X(aa) &= \{aababb, aababbbab, aabb, aabbab\} \end{aligned}$$

with the elements of $\mathcal{R}_X(ab)ab$ colored in green in Figure 6 and those of $\mathcal{R}_X(aa)aa$ colored in red. Thus, the maximal length R of return words of length 2 is 8.

Thue-Morse

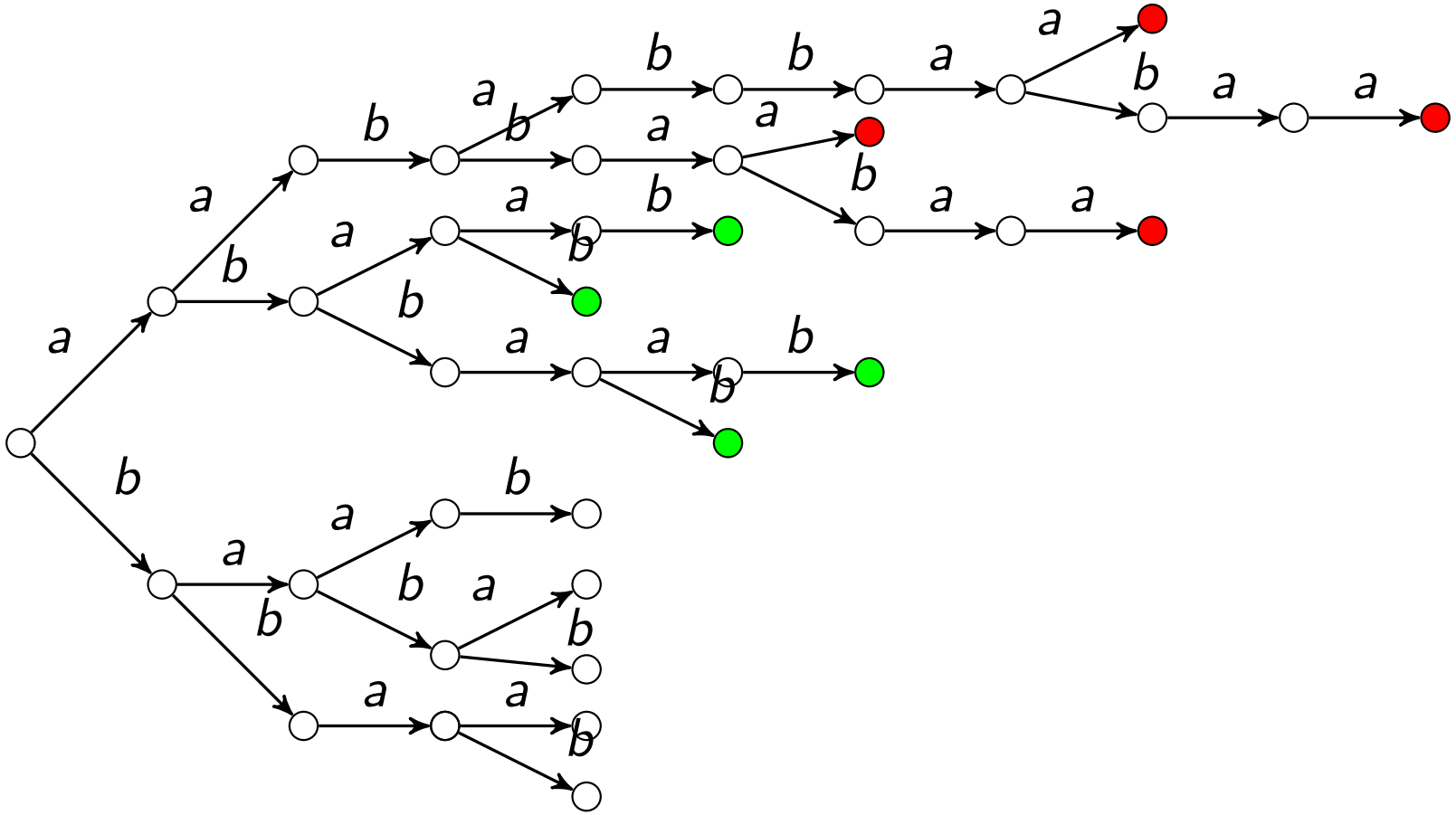


Figure: The words of $\mathcal{B}(X)$ for the Thue-Morse shift.

Computation of the return words of prefixes of a fixed point

Computation of $\mathcal{R}_X(u)$ when $X = \mathrm{X}(\sigma)$ is minimal, u is a **prefix** of a fixed point x of σ and $w \in \mathcal{R}_X(u)$.
The word w can be an arbitrary element of $\mathcal{R}_X(u)$, for instance the prefix of x in $\mathcal{R}_X(u)$.

Computation of the return words of prefixes of a fixed point

ReturnWords(u, w)

1 ▷ u is a prefix of $x = \sigma^\omega(a)$ and $w \in \mathcal{R}_X(u)$
2 ▷ Returns in R the set $\mathcal{R}_X(u)$
3 $R \leftarrow \emptyset$
4 $S \leftarrow \{w\}$
5 ▷ S is the set of return words to be processed
6 **while** $S \neq \emptyset$ **do**
7 $r \leftarrow$ an element of S
8 $S \leftarrow S \setminus \{r\}$
9 $R \leftarrow R \cup \{r\}$
10 $r(1), \cdots, r(k) \leftarrow \sigma(r)$
11 ▷ The words $r(i)$ are the decomposition of $\sigma(r)$ in return words to u
12 **for** $i \leftarrow 1$ **to** k **do**
13 **if** $r(i) \notin R \cup S$ **then**
14 $S \leftarrow S \cup r(i)$
15 **return** R

Example

Let $\sigma : a \mapsto ab, b \mapsto ba$ be the Thue-Morse substitution.
$\sigma^\omega(a) = abbabaabbaababbba \ldots$.
$u = ab$.
$w = abb$. $S = \{abb\}$.

1. $r = abb$. $S = \emptyset$. $R = \{abb\}$. $\sigma(abb) = abb\ aba$. $S = \{aba\}$
2. $r = aba$. $S = \emptyset$. $R = \{abb, aba\}$. $\sigma(aba) = abba\ ab$.
   $S = \{abba, ab\}$
3. $r = ab$. $S = \{abba\}$. $R = \{abb, aba, abba, ab\}$.
   $\sigma(ab) = abba$. $S = \{abba\}$
4. $r = abba$. $S = \emptyset$. $R = \{abb, aba, abba, ab\}$.
   $\sigma(abba) = abb\ aba\ ab$. $S = \emptyset$

Thus, $\mathcal{R}_X(ab) = \{ab, aba, abb, abba\}$.

Block complexity

The *block complexity*, or just *complexity*, of a shift space X is the sequence $(p_X(n))_{n\geq 0}$ with $p_X(n) = \mathrm{Card}(\mathcal{B}_n(X))$.

We also write $p_x(n) = \mathrm{Card}(\mathcal{B}_n(x))$ for an individual sequence x.

Morse-Hedlund

Theorem (Morse, Hedlund)

Let x be a two-sided sequence. The following conditions are equivalent.

(i) *For some $n \geq 1$, one has $p_x(n) \leq n$.*

(ii) *For some $n \geq 1$, one has $p_x(n) = p_x(n+1)$.*

(iii) *x is periodic.*

Moreover, in this case, the least period of x is $\max p_x(n)$.

Proof.

(i) $\Rightarrow$ (ii). If $p_x(1) = 1$, then $p_x(n) = 1$ for all n. Assume $p_x(1) > 1$. Note that $p_x(n) \leq p_x(n+1)$ for all $n \geq 0$. If the inequality is strict for all $n \geq 1$, we have $p_x(n) > n$ for all $n \geq 1$. Thus $p_x(n) \leq n$ for some $n \geq 1$ implies $p_x(n) = p_x(n+1)$ for some $n \geq 1$.

(ii) $\Rightarrow$ (iii). For every $w \in \mathcal{B}_n(x)$, there is a unique letter $a \in A$ such that $wa \in \mathcal{B}_{n+1}(x)$. This implies that two consecutive occurrences of a word u of length n in x are separated by a fixed word depending only on u and thus that x is periodic.

(iii) $\Rightarrow$ (i) is obvious.

Let n be the least period of x. Since a primitive word of length n has n distinct conjugates, we have $p_x(n) = n$ and $p_x(m) = n$ for all $m \geq n$. This proves the final assertion. $\square$

Linear recurrence

A shift space is *linearly recurrent* if it is minimal and if there is an integer $n \geq 1$ and a real number $K \geq 0$ such that, for every $u \in \mathcal{B}_{\geq n}(X)$, the length of every return word to u in X is bounded by $K|u|$.
We say that X is (K, n)-linearly recurrent.

We say that X is linearly recurrent with constant K. We say that X is linearly recurrent if it is K-linearly recurrent for some $K \geq 1$.

The lower bound of the numbers K such that X is K-linearly recurrent is called the *minimal constant* of linear recurrence.

Primitive substitution shifts are linearly recurrent

Proposition

A primitive substitution shift $\mathrm{X}(\sigma)$ *is linearly recurrent.*

Proposition

A primitive substitution shift $\mathrm{X}(\sigma)$ *is linearly recurrent with minimal constant* $K(\sigma) \leq kR|\sigma|$*, where* k *is such that* $|\sigma^n| \leq k\langle\sigma^n\rangle$ *for all* $n \geq 1$ *and* R *is the maximal length of a return word to a word of* $\mathcal{B}_2(\mathrm{X}(\sigma))$*.*

Primitive substitution shifts are linearly recurrent

Proof.

Let $\sigma : A^* \to A^*$ be a primitive substitution, and let $X = \mathrm{X}(\sigma)$ be the corresponding shift space. Since σ is primitive, it follows that there is a constant k such that, for all $n \geq 1$,

$$|\sigma^n| \leq k\langle\sigma^n\rangle \tag{6}$$

Indeed, let $\lambda = \lambda_{M(\sigma)}$.
By the Perron-Frobenius theorem, the sequence $(M(\sigma)^n/\lambda^n)$ converges to the matrix yx where x, y are positive left and right eigenvectors relative to λ with $\sum_{a\in A} y_a = 1$ and $\sum_{a\in A} x_a y_a = 1$.

This implies that $\lim_{n\to\infty} \frac{|\sigma^n(a)|}{\lambda^n} = x_a$.

Indeed,
$\lim_{n\to\infty} \frac{|\sigma^n(a)|}{\lambda^n} = \sum_{b\in A} \lim_{n\to\infty} \frac{M(\sigma)^n_{b,a}}{\lambda^n} = \sum_{b\in A} (x \cdot y)_{b,a} = x_a$. □

Primitive substitution shifts are linearly recurrent

Proof.

Consider $w \in \mathcal{B}(X)$. The substitution σ being primitive, the sequence $(\langle \sigma^n \rangle)_{n \geq 0}$ is nondecreasing and unbounded. There is an integer n such that

$$\langle \sigma^{n-1} \rangle \leq |w| \leq \langle \sigma^n \rangle. \tag{7}$$

Let v be a return word to w. Let $u \in \mathcal{B}(X)$ be such that vw occurs in $\sigma^n(u)$.
Since, by Inequality (7), $|w|$ is at most equal to every $|\sigma^n(a)|$, and we may assume that w occurs in the image by σ^n of the prefix ab of length 2 of u. We may also assume that u contains a second occurrence of ab. Set $\sigma^n(ab) = pwq$. Then the prefix of length $|v|$ of $\sigma^n(u)$ occurs in a word of $\sigma^n(\mathcal{R}_X(ab))$ (see Figure). □

Primitive substitution shifts are linearly recurrent

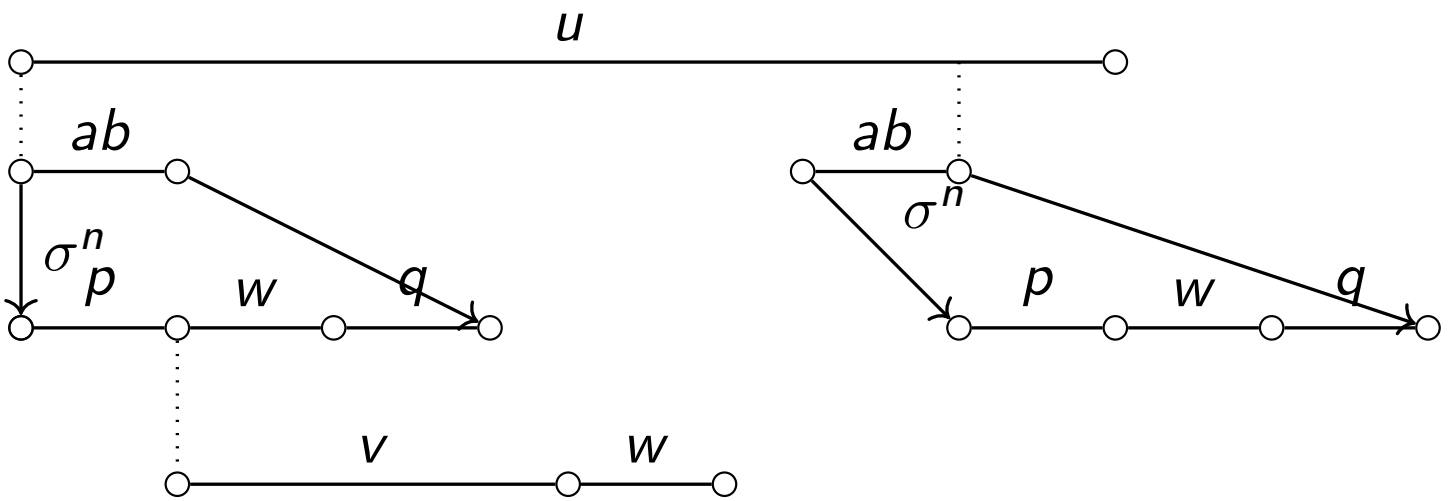


Figure: The words u, v, w.

Primitive substitution shifts are linearly recurrent

Proof.

Thus,

$$|v| \leq R|\sigma^n| \leq Rk\langle\sigma^n\rangle \leq Rk|\sigma|\langle\sigma^{n-1}\rangle \leq Rk|\sigma||w|,$$

where R is the maximal length of return words to a word of length 2. This shows that X is linearly recurrent with minimal constant

$$K(\sigma) \leq kR|\sigma|. \tag{8}$$

□

Left and right-special words

Let X be a shift space on A. For $w \in \mathcal{B}(X)$, let

$$\ell_X(w) = \mathrm{Card}\{a \in A \mid aw \in \mathcal{B}(X)\}, \quad r_X(w) = \mathrm{Card}\{a \in A \mid wa \in \mathcal{B}(X)\}$$

A word $w \in \mathcal{B}(X)$ is *left-special* with respect to X, or with respect to $\mathcal{B}(X)$, if $\ell_X(w) \geq 2$ (resp. $r_X(w) \geq 2$). It is *bispecial* if it is both left-special and right-special.

We define $s_X(n) = p_X(n+1) - p_X(n)$.

Left and right-special words

Then, one has

$$s_X(n) = \sum_{w \in \mathcal{B}_n(X)} (\ell_X(w) - 1) = \sum_{w \in \mathcal{B}_n(X)} (r_X(w) - 1). \qquad (9)$$

Indeed,

$$\begin{aligned} s_X(n) &= p_X(n+1) - p_X(n) = \mathrm{Card}(\mathcal{B}_{n+1}(X)) - \mathrm{Card}(\mathcal{B}_n(X)) \\ &= \sum_{w \in \mathcal{B}_n(X)} (\ell_X(w) - 1). \end{aligned}$$

If the sequence $s_X(n)$ is bounded, the complexity $p_X(n)$ is at most linear, that is $p_X(n) \leq kn$ for some $k \geq 1$. The converse is true, by an important result that we quote without proof.

Proposition (Cassaigne)

If the complexity of a shift X is at most linear, then $s_X(n)$ is bounded.

Block complexity of primitive substitution shifts

Proposition

If $\sigma\colon A^* \to A^*$ is a primitive substitution that is not the identity on a one-letter alphabet and such that $X = \mathrm{X}(\sigma)$ is not periodic, then $p_X(n) = \Theta(n)$.

Proof.

Since X is not periodic, we have $p_X(n) \geq n+1$ for every $n \geq 1$ by the Morse-Hedlund theorem. Thus $p_X(n) = \Omega(n)$. □

Block complexity of primitive substitution shifts

Proof.

To prove the upper bound, let λ be the maximal eigenvalue of $M(\sigma)$.
Let $c, d > 0$ be such that $\ell_n = c\lambda^n \leq |\sigma^n(a)| \leq d\lambda^n = L_n$ for every $a \in A$. Changing σ for some of its powers, we may assume that $L_n \leq \ell_{n+1}$.
In order to bound $p_X(k)$, consider n such that $\ell_n \leq k < \ell_{n+1}$. Let $w \in \mathcal{L}_k(\sigma)$. No word $\sigma^{n+1}(a)$ with $a \in A$ can occur in w since otherwise $\ell_{n+1} \leq k$, a contradiction. Thus there exist $a, b \in A$ such that $\sigma^{n+1}(ab) = pws$ with $|p| < |\sigma^{n+1}(a)|$. Since w is determined by a, b and $|p|$, this implies that

$$\begin{aligned} p_X(k) &\leq \mathrm{Card}(A)^2 L_{n+1} \leq \mathrm{Card}(A)^2 d\lambda^{n+1} \leq \mathrm{Card}(A)^2 \lambda \frac{d}{c} c\lambda^n \\ &\leq \mathrm{Card}(A)^2 \lambda \frac{d}{c} \ell_n \leq \mathrm{Card}(A)^2 \lambda \frac{d}{c} k, \end{aligned}$$

showing that $p_X(k) = O(k)$. □

Example

Example

The Fibonacci substitution $\sigma : a \mapsto ab, b \mapsto a$ is primitive. The complexity of the Fibonacci shift $X = \mathrm{X}(\sigma)$ is $p_X(n) = n + 1$.

Proof.

The words $F_n = \sigma^n(a)$ are left-special. Indeed, this is true for $n = 0$ since $aa, ba \in \mathcal{L}(\sigma)$. Next, $aF_{n+1} = \sigma(bF_n), \quad abF_{n+1} = \sigma(aF_n)$ show the claim by induction on n. It is easy to see (again by induction) that conversely, every left-special word is a prefix of some F_n. This implies that there is exactly one left-special word of each length and thus that $p_X(n) = n + 1$. □

Block complexity of linearly recurrent shift

Proposition

Every linearly recurrent shift has at most linear complexity. More precisely, a shift X is (K, n_0)-linearly recurrent if and only if, for $n \geq n_0$, every word of $\mathcal{B}_n(X)$ occurs in every word of $\mathcal{B}_m(X)$ when $m > (K+1)n - 2$. In this case, $p_X(n) \leq Kn$ for every $n \geq n_0$.

Block complexity of linearly recurrent shift

Proof.

Assume first that the shift X is (K, n_0)-linearly recurrent. Since, for $n \geq n_0$, the length of return words to $u \in \mathcal{B}_n(X)$ is at most Kn, the length of a word in $\mathcal{B}(X)$ without any occurrence of u is at most $n - 1 + Kn - 1 = (K + 1)n - 2$. Thus, every word of length $m > (K + 1)n - 2$ contains an occurrence u.

Conversely, if the condition is satisfied, let $n \geq n_0$ and let $u \in \mathcal{B}_n(X)$. Then X is minimal. Moreover, two consecutive occurrences of u in $\mathcal{B}(X)$ cannot be separated by more than Kn letters, and thus a return word to u is of length at most Kn.

We have $R_X(n) \geq p_X(n) + n - 1$ for $n \geq n_0$.
Indeed, the number of distinct words of length n occurring in a word of length N is at most $N - n + 1$. Therefore, $p_x(n) \leq R_X(n) - n + 1$. Hence $p_X(n) \leq Kn$ for $n \geq n_0$. □

Generalizations (admitted)

Theorem (Maloney and Rust 2018 for non-erasing substitutions)

Let σ be an iterable substitution. If $\mathsf{X}(\sigma)$ is minimal, then it is conjugate to $\mathsf{X}(\zeta)$, where ζ is a primitive substitution that is computable. Furthermore, for some $n \geq 1$, the dominant eigenvalues of σ^n and ζ coincide.

Corollary

A minimal substitution shift is linearly recurrent.

Master 2 Mathematics and Computer Science Symbolic Dynamics. Lecture 6

Marie-Pierre Béal

University Gustave Eiffel
Laboratoire d'informatique Gaspard-Monge UMR 8049

Recognizability

σ-representation

Let $\sigma : A^* \to B^*$ be a substitution. A *σ-representation* of $y \in B^{\mathbb{Z}}$ is a pair (x, k) of a sequence $x \in A^{\mathbb{Z}}$ and an integer k such that

$$y = S^k(\sigma(x)). \tag{1}$$

The σ-representation (x, k) is *centered* if $0 \leq k < |\sigma(x_0)|$.

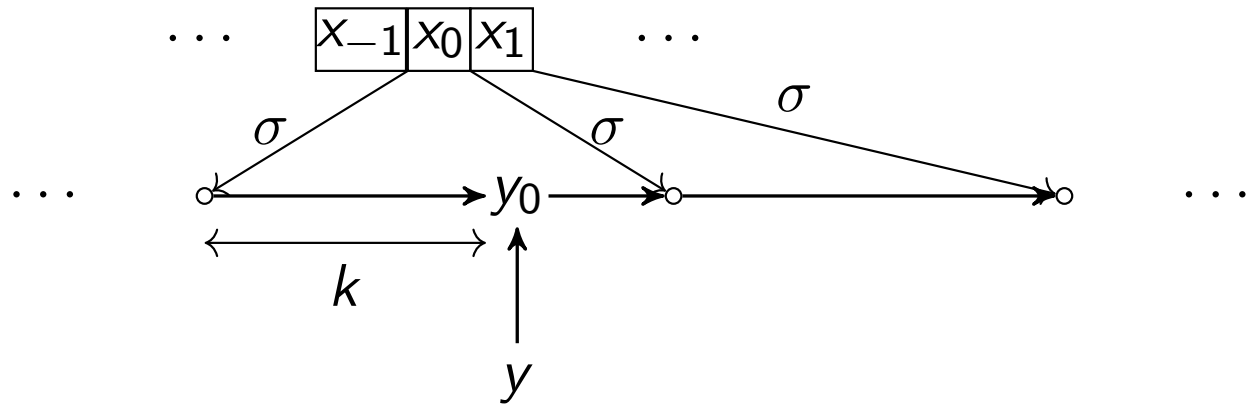


Figure: A centered σ-representation (x, k) of y.

Note, in particular, that a centered σ-representation (x, k) is such that $\sigma(x_0) \neq \varepsilon$.

σ-representation

Note that if y has a (not necessarily centered) σ-representation (x, ℓ), then it has also a centered σ-representation (x', k), where x' a shift of x.

Indeed, assume $\ell \geq 0$ (the case $\ell < 0$ is symmetric). Let $i \geq 0$ be such that $|\sigma(x_0 \cdots x_{i-1})| \leq \ell < |\sigma(x_0 \cdots x_i)|$. Set $k = \ell - |\sigma(x_0 \cdots x_{i-1})|$ and $x' = S^i x$. Then $S^k \sigma(x') = S^{k+|\sigma(x_0 \cdots x_{i-1})|} \sigma(x) = S^\ell \sigma(x) = y$ and $0 \leq k < |\sigma(x'_0)|$. Thus, (x', k) is a centered σ-representation of y.

σ-representation

For a shift space X on A, the set of points in $B^{\mathbb{Z}}$ having a σ-representation (x, k) with $x \in X$ is a shift space on B, which is the closure under the shift of $\sigma(X)$.
Indeed, if (x, k) is a σ-representation of y, then $S(y)$ has the σ-representation (x', k') with

$$(x', k') = \begin{cases} (x, k+1) & \text{if } k+1 < |\sigma(x_0)| \\ (S(x), 0) & \text{otherwise.} \end{cases}$$

Recognizability

Let X be a shift space on A.
The substitution $\sigma : A^* \to B^*$ is *recognizable* in X if every $y \in B^{\mathbb{Z}}$ has **at most one** centered σ-representation (x, k) such that $x \in X$.

Thus, in informal terms, for a sequence y on B, there is at most one way to desubstitute y to obtain a sequence in X.

Example

Example

The substitution $\sigma : a \mapsto a, b \mapsto ab, c \mapsto abb$ is recognizable in the full shift $X = \{a, b, c\}^{\mathbb{Z}}$.
Indeed, let Y be the closure under the shift of $\sigma(X)$.
Any two consecutive occurrences of a are separated by a block of zero, one or two b, which determines the rule of σ to be used for desubstitution. Formally, we have

$$\begin{aligned}
\sigma([a]_X) &= [aa]_Y, \\
\sigma([b]_X) &= [aba]_Y, \quad S\sigma([b]_X) = [a \cdot ba]_Y \\
\sigma([c]_X) &= [abba]_Y, \quad S\sigma([c]_X) = [a \cdot bba]_Y, \quad S^2\sigma([c]_X) = [ab \cdot ba]_Y
\end{aligned}$$

and these sets form a partition of Y.

Example

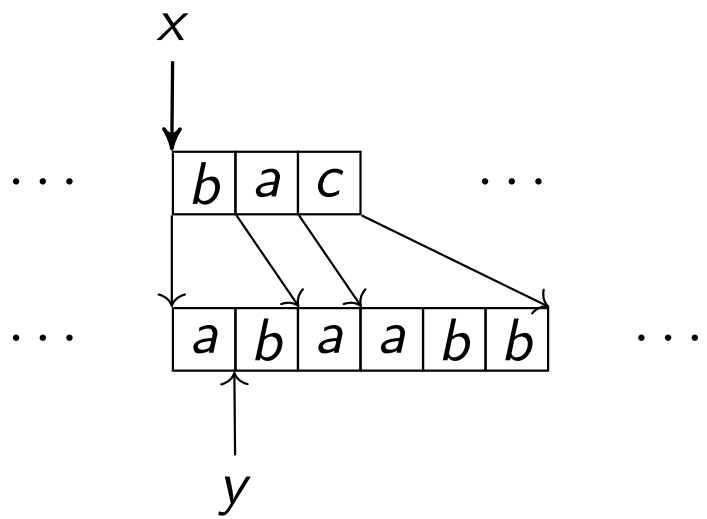


Figure: A centered σ-representation of $y = \cdots a \cdot baabb \cdots$.

Fully recognizable substitutions

Let $\sigma : A^* \to B^*$ be a substitution. Assume that σ is erasing, but that not all letters are erasable. Then σ cannot be recognizable in $A^{\mathbb{Z}}$. Indeed, if $\sigma(a) \neq \varepsilon$, and $\sigma(b) = \varepsilon$, then $\sigma({}^{\omega}ab \cdot a^{\omega}) = \sigma(a^{\infty})$.

Let $\sigma : A^* \to B^*$ be a non-erasing substitution. We say that σ is *fully recognizable* or *circular* if it is recognizable in $A^{\mathbb{Z}}$.

Thus, in particular, a circular substitution is injective.

Example

Example

The substitution $\sigma : a \mapsto a, b \mapsto ab, c \mapsto abb$ is fully recognizable.

A *coding substitution* for a set U of nonempty words on A is a substitution $\phi\colon B^* \to A^*$ such that its restriction to B is a bijection onto U. The set U is called a *code* if ϕ is injective and a *circular code* if ϕ is circular.

Proposition

Let X be a minimal shift space on A and let $u \in \mathcal{B}(X)$. Any coding substitution $\phi\colon B^* \to A^*$ for the set $\mathcal{R}_X(u)$ of return words to u is circular.

Proof.

Since wu contains exactly two occurrences of u for each $w \in \mathcal{R}_X(u)$, for each $y \in X$, there is a unique sequence $z = \cdots w_{-1} \cdot w_0 w_1 \cdots$ with $w_i \in \mathcal{R}_X(u)$, and a unique integer k such that $y = S^k(z)$ with $0 \leq k < |w_0|$. Since ϕ is a coding substitution, for each $w_i \in \mathcal{R}_X(u)$, there is a unique $b_i \in B$ such that $\phi(b_i) = w_i$. Hence, there is a unique $x \in B^{\mathbb{Z}}$ and k with $0 \leq k < |\phi(x_0)|$ such that $y = S^k\phi(x)$. □

Representability

Existence of a representation

Proposition

Let $\sigma : A^* \to A^*$ be a substitution. Every point y in $\mathsf{X}(\sigma)$ has a σ-representation $y = S^i(\sigma(x))$ for some $i \geq 0$, and x in $\mathsf{X}(\sigma)$.

Existence of a representation

Proof.

Let $k = |\sigma|$ and let y be in $X(\sigma)$. For every $n \geq 1$, there is an integer $m \geq 1$ such that $y_{[-n,n]}$ occurs in $\sigma^m(a)$ for some letter $a \in A$.

For every $n > 2k$, there is an integer $0 \leq i \leq k$ such that, for an infinity of $n > 2k$, there are words u_n, v_n with $u_n v_n \in \mathcal{L}(\sigma)$ such that $y_{[-n+k,-i)}$ is a suffix of $\sigma(u_n)$ and $y_{[-i,n-k]}$ is a prefix of $\sigma(v_n)$. Further, $|u_n| \geq (n-k-i)/k$ and $|v_n| \geq (n-k+i)/k$.

Therefore, there are infinitely many $n > 2k$ for which the value of i is the same.

By a compactness argument, we get that there is a point $x \in X(\sigma)$ such that $y = S^i(\sigma(x))$. □

Elementary substitutions

Elementary substitution

A substitution $\sigma : A^* \to C^*$ is *elementary* if for every alphabet B and every pair of substitutions $A^* \xrightarrow{\beta} B^* \xrightarrow{\alpha} C^*$ such that $\sigma = \alpha \circ \beta$, one has $\mathrm{Card}(B) \geq \mathrm{Card}(A)$.

In this case, one has in particular $\mathrm{Card}(C) \geq \mathrm{Card}(A)$.

Moreover, σ is non-erasing (Exercise).

Example

Example

The Thue-Morse substitution $\sigma : a \mapsto ab, b \mapsto ba$ is elementary. Indeed, if $\sigma = \alpha \circ \beta$ with $\beta : \{a, b\}^* \to c^*$, then $ab = \alpha(c^i)$ and $ba = \alpha(c^j)$ which is impossible.

Example

The substitution $\sigma : a \mapsto ab, b \mapsto abc, c \mapsto cc$ is not elementary. Indeed, we have $\sigma = \alpha \circ \beta$ with $\alpha : u \mapsto ab, v \mapsto c$ and $\beta : a \mapsto u, b \mapsto uv, c \mapsto vv$.

Elementary substitution

Note that the property of being elementary is decidable.
Indeed, if $\sigma : A^* \to C^*$ is a substitution consider the finite family $\mathcal{F}$ of sets $U \subset C^*$ such that $\sigma(A) \subset U^* \subset C^*$ with every $u \in U$ occurring in some $\sigma(a)$ for $a \in A$.
Then σ is elementary if and only if $\mathrm{Card}(U) \geq \mathrm{Card}(A)$ for every $U \in \mathcal{F}$.

Elementary substitution

Proposition

Let $A^* \xrightarrow{\beta} B^* \xrightarrow{\alpha} C^*$ be substitutions. If $\alpha \circ \beta$ is elementary, then β is elementary.

Proof.

Let $A^* \xrightarrow{\gamma} D^* \xrightarrow{\delta} B^*$ be such that $\beta = \delta \circ \gamma$. Then $\alpha \circ \beta = \alpha \circ (\delta \circ \gamma) = (\alpha \circ \delta) \circ \gamma$. This implies $\mathrm{Card}(D) \geq \mathrm{Card}(A)$. Thus β is elementary. □

Elementary substitution

A sufficient condition for a substitution to be elementary can be formulated in terms of its composition matrix.

Proposition

If the rank of $M(\sigma)$ is equal to $\mathrm{Card}(A)$*, then σ is elementary.*

Proof.

Indeed, if $\sigma = \alpha \circ \beta$ with $\beta\colon A^* \to B^*$ and $\alpha\colon B^* \to C^*$, then $M(\sigma) = M(\alpha)M(\beta)$. If $\mathrm{rank}(M(\sigma)) = \mathrm{Card}(A)$, then

$$\mathrm{Card}(A) = \mathrm{rank}(M(\sigma)) \leq \mathrm{rank}(M(\alpha)) \leq \mathrm{Card}(B).$$

Thus σ is elementary. □

This condition is not necessary. For example, the Thue-Morse substitution $\sigma\colon a \mapsto ab, b \mapsto ba$ is elementary, but its composition matrix has rank one.

Elementary substitution

If $\sigma\colon A^* \to C^*$ is a substitution, we define

$$\ell(\sigma) = \sum_{a\in A}(|\sigma(a)| - 1). \tag{2}$$

We say that a decomposition $\sigma = \alpha \circ \beta$ with $\alpha\colon B^* \to C^*$ and $\beta\colon A^* \to B^*$ is *trim* if

(i) α is non-erasing,

(ii) for each $b \in B$ there is an $a \in A$ such that $\beta(a)$ contains b.

Proposition

Let $\sigma = \alpha \circ \beta$ with $\alpha\colon B^* \to C^*$ and $\beta\colon A^* \to B^*$ be a trim decomposition of σ. Then

$$\ell(\alpha \circ \beta) \geq \ell(\alpha) + \ell(\beta). \tag{3}$$

Proof

Proof.

Set $\sigma = \alpha \circ \beta$. We have

$$\begin{aligned}
\ell(\sigma) - \ell(\beta) &= \sum_{a \in A} (|\sigma(a)| - |\beta(a)|) \\
&= \sum_{a \in A} \sum_{b \in B} (|\alpha(b)||\beta(a)|_b - |\beta(a)|_b) \\
&= \sum_{a \in A} \sum_{b \in B} (|\alpha(b)| - 1)|\beta(a)|_b \\
&= \sum_{b \in B} ((|\alpha(b)| - 1) \sum_{a \in A} |\beta(a)|_b).
\end{aligned}$$

Since every b occurs in some $\beta(a)$, every factor $\sum_{a \in A} |\beta(a)|_b$ is positive, whence the conclusion. □

Elementary substitution

Proposition

An elementary substitution $\sigma : A^* \to C^*$ is injective on $A^{\mathbb{N}}$.

follows from:

Proposition

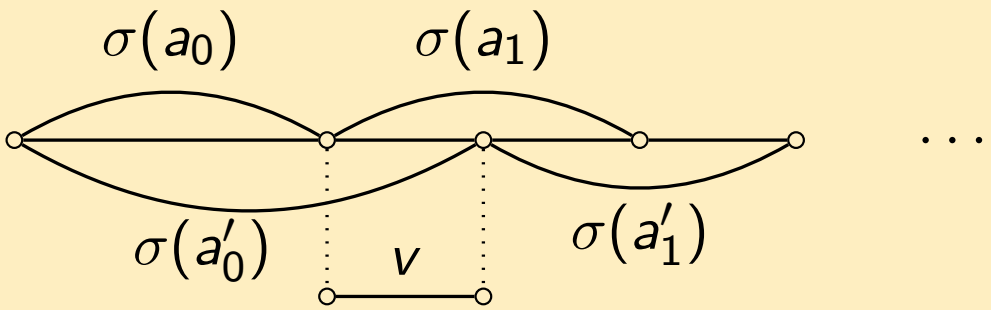
If a substitution $\sigma : A^* \to C^*$ is not injective on $A^{\mathbb{N}}$, there is a trim decomposition $\sigma = \alpha \circ \beta$ with $\alpha : B^* \to C^*$ and $\beta : A^* \to B^*$ such that α is injective on $B^{\mathbb{N}}$, $\mathrm{Card}(B) < \mathrm{Card}(A)$ and every $b \in B$ occurs as the first letter of $\beta(a)$ for some $a \in A$.

Proof

Proof.

Assume first that σ is non-erasing. We use an induction on $\ell(\sigma)$. If $\ell(\sigma) = 0$, set $B = \sigma(A)$. Let α be the identity on B^* and let $\beta = \sigma$. All conditions are clearly satisfied.

Assume now that the statement is true for $\ell < \ell(\sigma)$. Since σ is not injective on $A^{\mathbb{N}}$, we have $\sigma(a_0 a_1 \cdots) = \sigma(a'_0 a'_1 \cdots)$ for some $a_i, a'_i \in A$ with $a_0 \neq a'_0$. We can assume that $\sigma(a_0)$ is a prefix of $\sigma(a'_0)$. Set $\sigma(a'_0) = \sigma(a_0)v$. If v is empty, set $B = A \setminus \{a_0\}$. Let α be the restriction of σ to B and let β be defined by $\beta(a'_0) = a_0$ and $\beta(a) = a$ for $a \neq a'_0$. Clearly, $\sigma = \alpha \circ \beta$, and all conditions are satisfied.



Proof

Proof.

Next, assume that v is nonempty. Define $\alpha_1 : A^* \to C^*$ by $\alpha_1(a'_0) = v$ and $\alpha_1(a) = \sigma(a)$ for $a \neq a'_0$. Next, define $\beta_1 : A^* \to A^*$ by $\beta_1(a'_0) = a_0 a'_0$ and $\beta_1(a) = a$ for $a \neq a'_0$. Then $\sigma = \alpha_1 \circ \beta_1$ since

$$\alpha_1 \circ \beta_1(a'_0) = \alpha_1(a_0 a'_0) = \sigma(a_0)v = \sigma(a'_0),$$

and $\alpha_1 \circ \beta_1(a) = \alpha_1(a) = \sigma(a)$ if $a \neq a'_0$. The substitution β_1 is injective on $A^{\mathbb{N}}$ because no word in $\beta_1(A)$ begins with a'_0. Thus α_1 is not injective on $A^{\mathbb{N}}$. By Equation (3), since the decomposition is trim, we have $\ell(\alpha_1) < \ell(\sigma)$. By induction hypothesis, we have a decomposition $\alpha_1 = \alpha_2 \circ \beta_2$ for $\beta_2 : A^* \to B^*$ and $\alpha_2 : B^* \to C^*$ with $\mathrm{Card}(B) < \mathrm{Card}(A)$, the substitution α_2 being injective on $B^{\mathbb{N}}$ and every letter $b \in B$ occurring as initial letter in the word $\beta_2(a)$ for some $a \in A$. Note that, since α_1 is non-erasing, β_2 is non-erasing. □

Proof

Proof.

Set $\beta = \beta_2 \circ \beta_1$. Since β_1, β_2 are non-erasing, β is non-erasing. Then $\sigma = \alpha_1 \circ \beta_1 = \alpha_2 \circ \beta_2 \circ \beta_1 = \alpha_2 \circ \beta$. The decomposition $\sigma = \alpha_2 \circ \beta$ satisfies all the required conditions.

Indeed, let $b \in B$. Then there is $a \in A$ such that b is the first letter of $\beta_2(a)$.

If $a \neq a'_0$, we have $\beta_1(a) = a$ and thus b is the first letter of $\beta(a)$.

Suppose next that $a = a'_0$. Since $\sigma(a_0 a_1 \cdots) = \sigma(a'_0 a'_1 \cdots)$ and since α_2 is injective on $B^{\mathbb{N}}$, we have $\beta(a_0 a_1 \cdots) = \beta(a'_0 a'_1 \cdots)$. Since $\beta_1(a_0) = a_0$ and $\beta_1(a'_0) = a_0 a'_0$, we obtain $\beta_2(a_0)\beta(a_1 \cdots) = \beta_2(a_0 a'_0)\beta(a'_1 \cdots)$ and thus

$$\beta(a_1 \cdots) = \beta_2(a'_0)\beta(a'_1 \cdots),$$

showing, since β is non-erasing, that b is the initial letter of $\beta(a_1)$. □

Proof

Proof.

Now consider a substitution σ such that the set $B = \{a \in A \mid \sigma(a) \neq \varepsilon\}$ is strictly contained in A. Let $\beta\colon A^* \to B^*$ be defined by $\beta(a) = a$ if $a \in B$ and $\beta(a) = \varepsilon$ otherwise. Let α be the restriction of σ to B^*. Then $\sigma = \alpha \circ \beta$ and α is non-erasing. If α is injective on $B^{\mathbb{N}}$, we are done. Otherwise, by the first part of the proof, we have $\alpha = \alpha_1 \circ \beta_1$ with $\alpha_1\colon B_1^* \to C^*$ and $\beta_1\colon B^* \to B_1^*$ with α_1 injective on $B_1^{\mathbb{N}}$, $\mathrm{Card}(B_1) < \mathrm{Card}(B)$ and every $b_1 \in B_1$ occurs as the first letter of some $\beta_1(b)$. Then the decomposition $\sigma = \alpha_1 \circ (\beta_1 \circ \beta)$ satisfies all the conditions. □

Elementary substitution

By a symmetric version, an elementary substitution $\sigma : A^* \to C^*$ is injective on $A^{-\mathbb{N}}$. Since a substitution which is injective on $A^{\mathbb{N}}$ and on $A^{-\mathbb{N}}$ is injective on $A^{\mathbb{Z}}$, we obtain the following corollary of Proposition 6.

Proposition

An elementary substitution $\sigma : A^* \to C^*$ is injective on $A^{\mathbb{Z}}$.

Recognizability for aperiodic points

A substitution $\sigma : A^* \to B^*$ is *recognizable in X for aperiodic points* if **every aperiodic point** $y \in B^{\mathbb{Z}}$ has at most one centered representation **in** X.

We say that σ is *fully recognizable for aperiodic points* if it is recognizable in the full shift for aperiodic points.

Example

Example

The substitution $\sigma : a \mapsto aa, b \mapsto ab, c \mapsto ba$ is not fully recognizable for aperiodic points.
Indeed, every sequence without occurrence of bb has two factorizations in words of $\{aa, ab, ba\}$.

Proposition

The family of substitutions that are fully recognizable for aperiodic points is closed under composition.

Aperiodic substitution

A substitution σ is *aperiodic* if $X(\sigma)$ contains no periodic point.

Theorem (B. Mossé 1992, B. Mossé 1996)

Any aperiodic substitution is recognizable in $X(\sigma)$.

Recognizability for aperiodic points

Theorem (J. Karhumäki, J. Maňuch, W. Plandowski 2003)

An elementary substitution is fully recognizable for aperiodic points.

Proof

A substitution $\sigma : A^* \to B^*$ with no erasable letter is *left-marked* if each word $\sigma(a)$, for $a \in A$, begins with a distinct letter.

In particular, if σ is left-marked, σ is injective on A and $\sigma(A)$ is a prefix code.

It is clear that a left-marked substitution is elementary.

Left-marked substitution

Proposition

If $\sigma : A^* \to B^*$ is left-marked, then it is fully recognizable for aperiodic points.

Proof.

Assume that $y \in B^{\mathbb{Z}}$ has two distinct σ-representations (x, k) and (x', k'). We may assume $k = 0$. We will prove that y is periodic. Let P be the set of proper prefixes of the elements of $U = \sigma(A)$. For $p \in P$ and $a \in A$, there is at most one $q \in P$ such that $p\sigma(a) \in U^* q$. We write $q = p \cdot a$ when such a q exists. Let $p_0 = y_{-k'} \cdots y_{-1}$ (with $p_0 = \varepsilon$ if $k' = 0$). Since $y = \sigma(x) = S^{k'}(\sigma(x'))$, we have (see Figure)

$$\sigma(\cdots x'_{-2}x'_{-1})p_0 = \sigma(\cdots x_{-1}), \quad p_0\sigma(x_0x_1\cdots) = \sigma(x'_0x'_1\cdots).$$

As a consequence, there exists, for each $n \in \mathbb{Z}$, a word $p_n \in P$ such that $p_n \cdot x_n = p_{n+1}$.

□

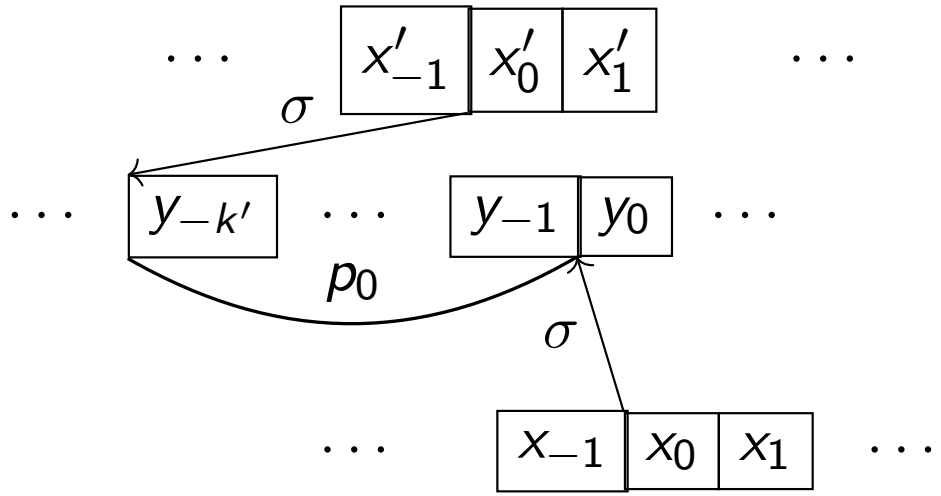


Figure: The two centered σ-representations of y.

Proof.

Consider the labeled graph G with P as set of vertices and edges (p, a, q) if $p \cdot a = q$. Since σ is left-marked, there is for every nonempty $p \in P$ at most one $a \in A$ such that $p \cdot a$ exists. In particular, since all edges going out of ε end in ε, G is a disjoint union of simple cycles in $P \setminus \{\varepsilon\}$ and loops on ε. As a consequence, either the path is a cycle, and thus x and y are periodic, or $k' = 0$ and thus $x = x'$ since σ is left-marked.

□

Example

Example

The Thue-Morse substitution $\sigma : a \to ab, b \to ba$ is left-marked. Thus, it is fully recognizable for aperiodic points. The graph used in the proof is:

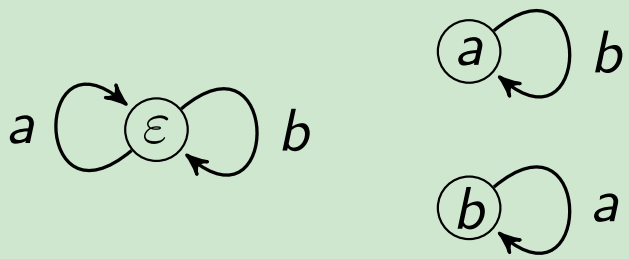


Figure: The graph associated with the Thue-Morse substitution.

An elementary substitution is fully recognizable for aperiodic points

Proof.

Let $\sigma : A^* \to B^*$ be an elementary substitution. We use an induction on $\ell(\sigma) = \sum_{a \in A}(|\sigma(a)| - 1)$ (see (2)). Since σ is elementary, it has no erasable letter, and the minimal possible value of $\ell(\sigma)$ is 0. In this case, σ is a bijection from A into B, and thus it is fully recognizable.

Assume now that σ is not fully recognizable for aperiodic points. Thus, there exist $x, x' \in A^{\mathbb{Z}}$, $a' = x'_0 \in A$ and w with $0 < |w| < |\sigma(x_0)|$ such that $\sigma(x) = w\sigma(x')$ for some proper suffix w of $\sigma(a')$. Set $\sigma(a') = vw$ (see Figure). We can then write $\sigma = \sigma_1 \circ \tau_1$ with $\tau_1 : A^* \to A_1^*$ and $\sigma_1 : A_1^* \to B^*$ and $A_1 = A \cup \{a''\}$ where a'' is a new letter. We have $\tau_1(a') = a'a''$ and $\tau_1(a) = a$ otherwise. In particular, τ_1 is left-marked. Next $\sigma_1(a') = v$, $\sigma_1(a'') = w$ and $\sigma_1(a) = \sigma(a)$ otherwise. Since $\ell(\tau_1) > 0$, we have $\ell(\sigma_1) < \ell(\sigma)$ by Equation (3). □

Proof.

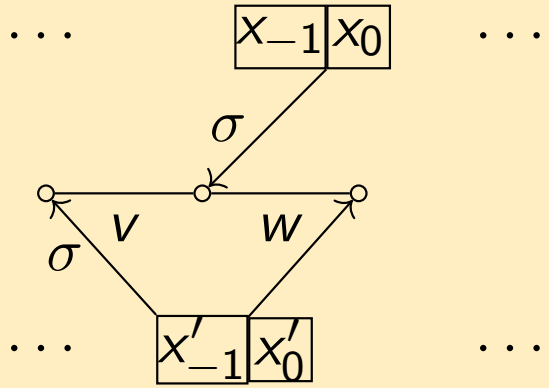


Figure: The words v, w.

Since

$$\sigma_1(a'')\sigma_1(\tau_1(x')) = \sigma_1(\tau_1(x)),$$

and since $\tau_1(x_0)$ does not begin with a'', σ_1 is not injective on $A_1^{\mathbb{N}}$. □

Proof.

By Proposition 7, we can write $\sigma_1 = \sigma_2 \circ \tau_2$ with $\sigma_2 : A_2^* \to B^*$ and $\tau_2 : A_1^* \to A_2^*$ for some alphabet A_2 such that $\mathrm{Card}(A_2) < \mathrm{Card}(A_1)$ and that every letter $c \in A_2$ appears as the first letter of some $\tau_2(a)$ for $a \in A_1$. Then, by Equation (3), we have

$$\ell(\sigma_1) \geq \ell(\sigma_2) + \ell(\tau_2). \tag{4}$$

Moreover, since σ_1 is non-erasing, τ_2 is non-erasing and thus $\ell(\tau_2) \geq 0$. This implies $\ell(\sigma_1) \geq \ell(\sigma_2)$.
Since σ is elementary, we have $\mathrm{Card}(A_2) \geq \mathrm{Card}(A)$. Since $\mathrm{Card}(A_2) < \mathrm{Card}(A_1) = \mathrm{Card}(A) + 1$, this forces $\mathrm{Card}(A_2) = \mathrm{Card}(A)$. We may also assume that σ_2 and $\tau_2 \circ \tau_1$ are elementary since otherwise σ is not elementary.

□

Proof.

Since σ_2 is elementary and since $\ell(\sigma_2) \leq \ell(\sigma_1) < \ell(\sigma)$, by the induction hypothesis, σ_2 is fully recognizable for aperiodic points. The decomposition $\sigma = \sigma_1 \circ (\tau_2 \circ \tau_1)$ is trim. Indeed, σ_2 is elementary and thus non-erasing. Next, every letter of A_2 appears in some $\tau_2(a)$ and, by definition of τ_1, it appears also in some $\tau_2 \circ \tau_1(a)$. Thus, we have also

$$\ell(\sigma) \geq \ell(\sigma_2) + \ell(\tau_2 \circ \tau_1). \tag{5}$$

Thus, if $\ell(\sigma_2) > 0$, the inequality $\ell(\tau_2 \circ \tau_1) < \ell(\sigma)$ holds. Since $\tau_2 \circ \tau_1$ is elementary, we obtain that $\tau_2 \circ \tau_1$ is fully recognizable for aperiodic points by induction hypothesis. Since the family of substitutions that are fully recognizable for aperiodic points is closed under composition, we get that that σ is fully recognizable for aperiodic points. □

Proof.

Let us finally assume that $\ell(\sigma_2) = 0$. Since $\sigma_1(a'') = w$ is a prefix of $\sigma(x_0) = \sigma_1(\tau_1(x_0)) = \sigma_1(x_0)$ with $x_0 \in A$, and since σ_2 is a bijection from A_2 onto B, the first letter of $\tau_2(a'')$ is equal to the first letter of $\tau_2(x_0)$. Further, each letter of A_2 appears as the first letter of $\tau_2(c)$ for some letter $c \in A_1$. Thus, each letter of A_2 is the first letter of $\tau_2(a)$ for some letter $a \in A$. Consequently, each letter of B is the first letter of $\sigma(a)$ for some $a \in A$. Since $\mathrm{Card}(A) = \mathrm{Card}(B)$, it follows that σ is left-marked.
We obtain the conclusion by the proposition for left-marked substitutions. □

Recognizability for aperiodic points

Recognizability for aperiodic points

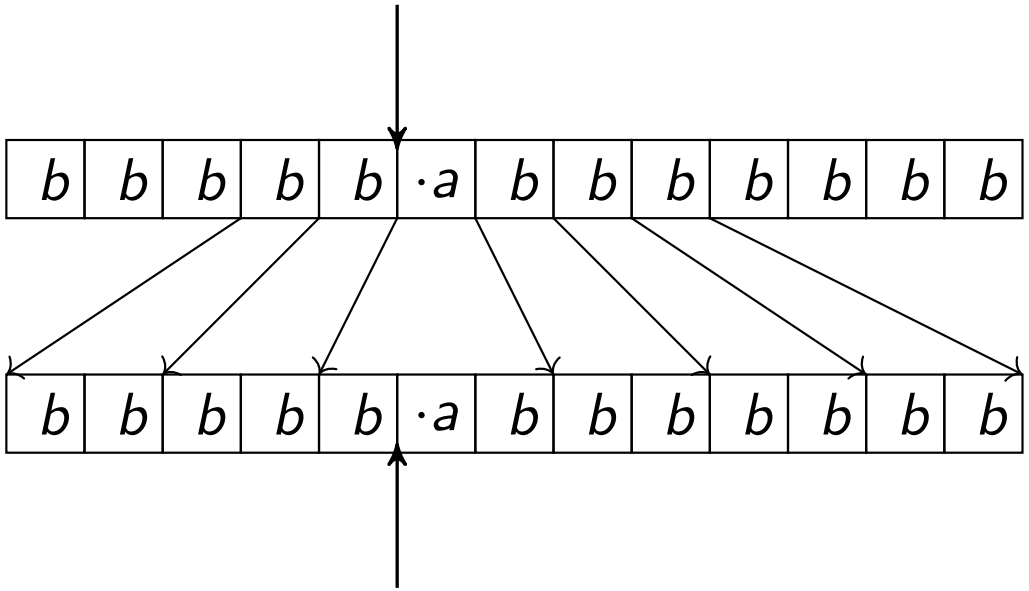
Theorem (Berthé et al. 2018 for non-erasing substitutions, B. et al. 2022)

Any morphism $\sigma : A^* \to A^*$ is recognizable for aperiodic points in $X(\sigma)$.

Recognizability for aperiodic points

Example

Let $\sigma : a \mapsto bab, b \mapsto bb$.

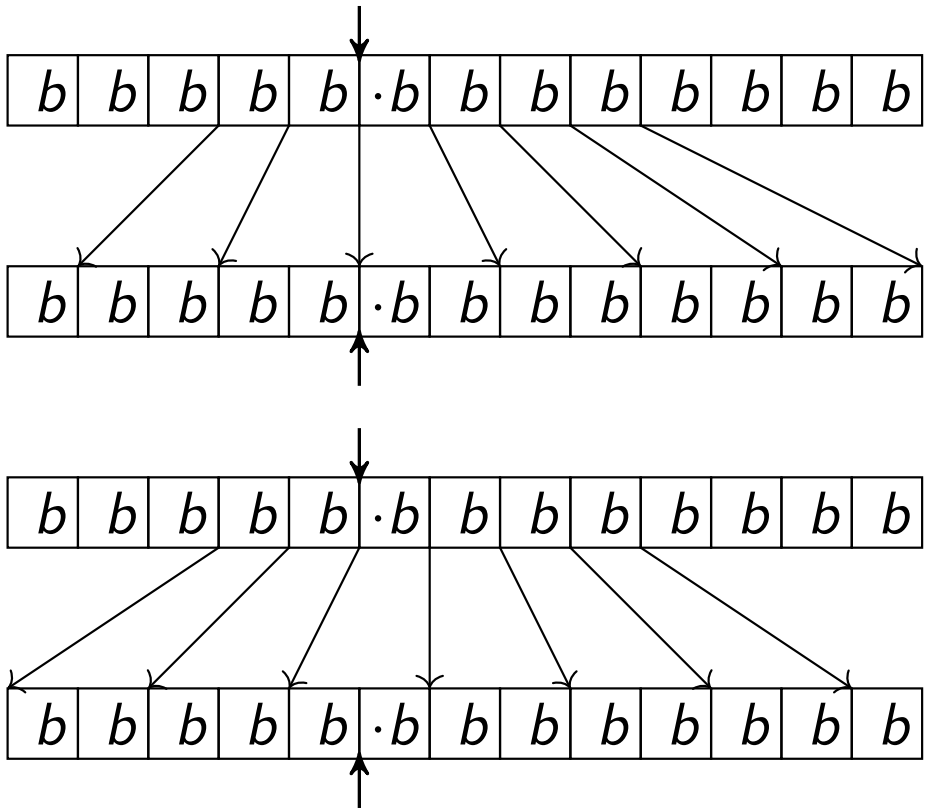


The point $y = \cdots bbbb \cdot abbbb \cdots = S(\sigma(y))$ has a unique centered σ-representation $(y, 1)$.

Example

Example

Let $\sigma : a \mapsto bab, b \mapsto bb$.

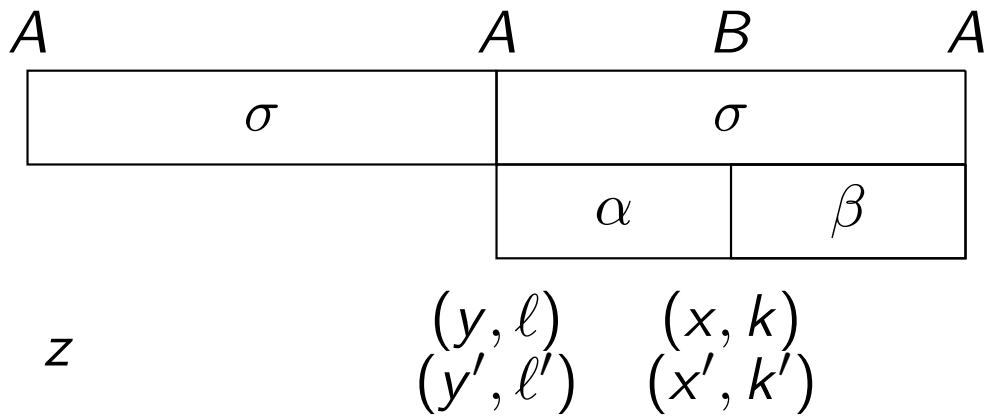


The point $y = \cdots bbbb \cdot bbbbb \cdots = \sigma(y) = S(\sigma(y))$ has a two centered σ-representation $(y, 0)$ and $(y, 1)$.

Lemma

Let $\sigma : A^* \xrightarrow{\sigma} A^*$ *be a substitution and* $A^* \xrightarrow{\beta} B^* \xrightarrow{\alpha} A^*$ *such that* $\sigma = \alpha \circ \beta$. *If* σ *is not recognizable in* $X(\sigma)$, *then* $\sigma \circ \alpha$ *is not fully recognizable. The same statement holds for the recognizability for aperiodic points.*

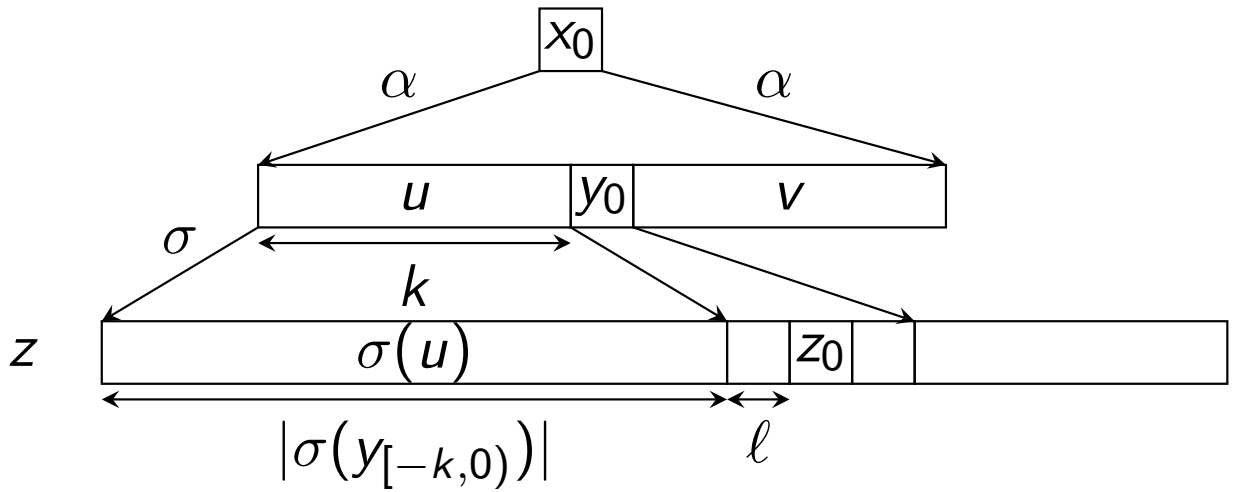
Proof



Proof of the lemma

If σ is not recognizable in $X(\sigma)$ then there exists $z \in X(\sigma)$ with two centered σ-representations $(y, \ell) \neq (y', \ell')$ in $X(\sigma)$. Let (x, k) and (x', k') be centered α-representations in $B^{\mathbb{Z}}$ of y and y' respectively (They exist since (x, k) and (x', k') have σ-representations in $X(\sigma)$).
Then $(x, |\sigma(y_{[-k,0)})|+\ell)$ and $(x', |\sigma(y'_{[-k',0)})|+\ell')$ are centered $\sigma \circ \alpha$-representations of z in $B^{\mathbb{Z}}$.

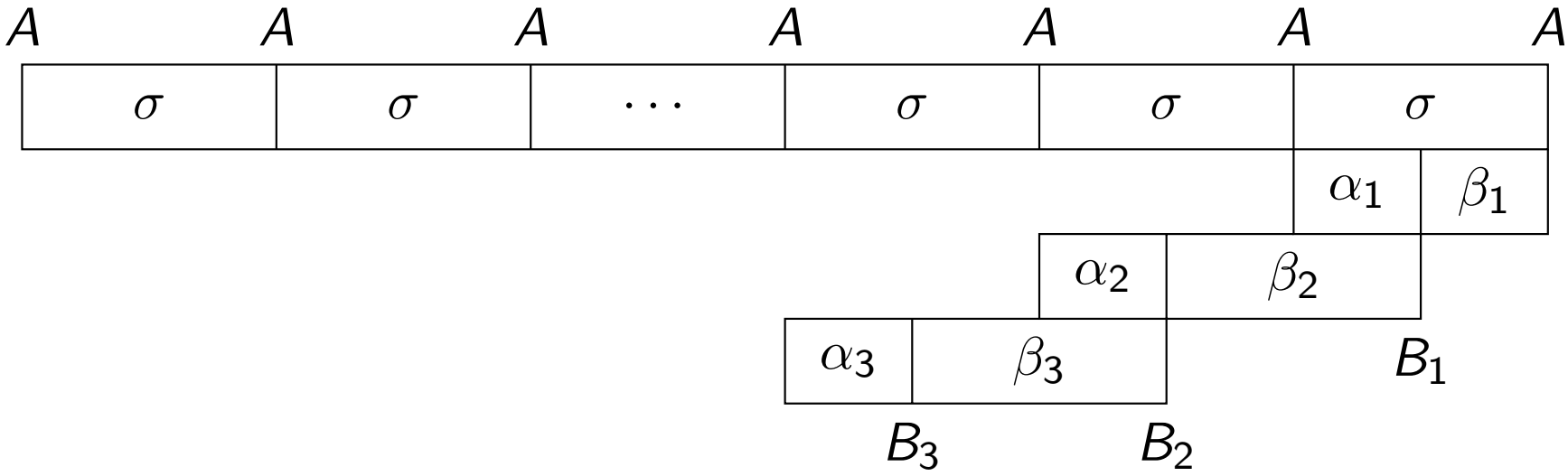
Proof



Proof of the lemma

If $(x, |\sigma(y_{[-k,0)})|+\ell) = (x', |\sigma(y'_{[-k',0)})|+\ell')$, then $x = x'$, $u = u'$, $y_0 = y'_0$, $v = v'$. Thus, $k = k'$, $\ell = \ell'$, and $y = y'$.
Further, if z is aperiodic, y also since $z = S^{\ell}(y)$.

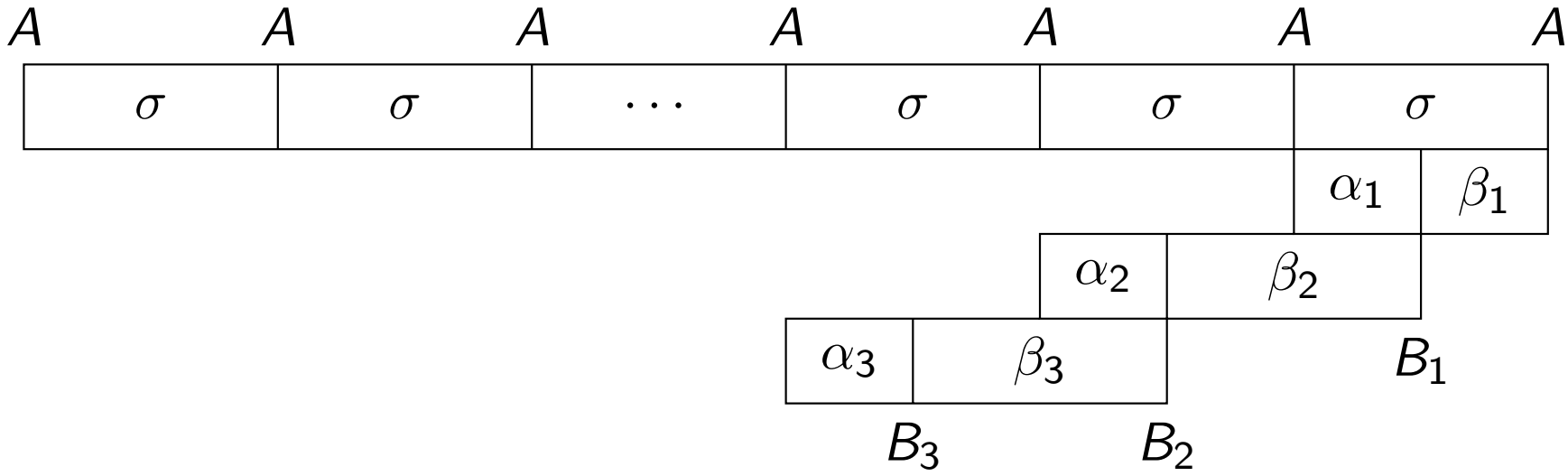
Proof



Proof of the theorem

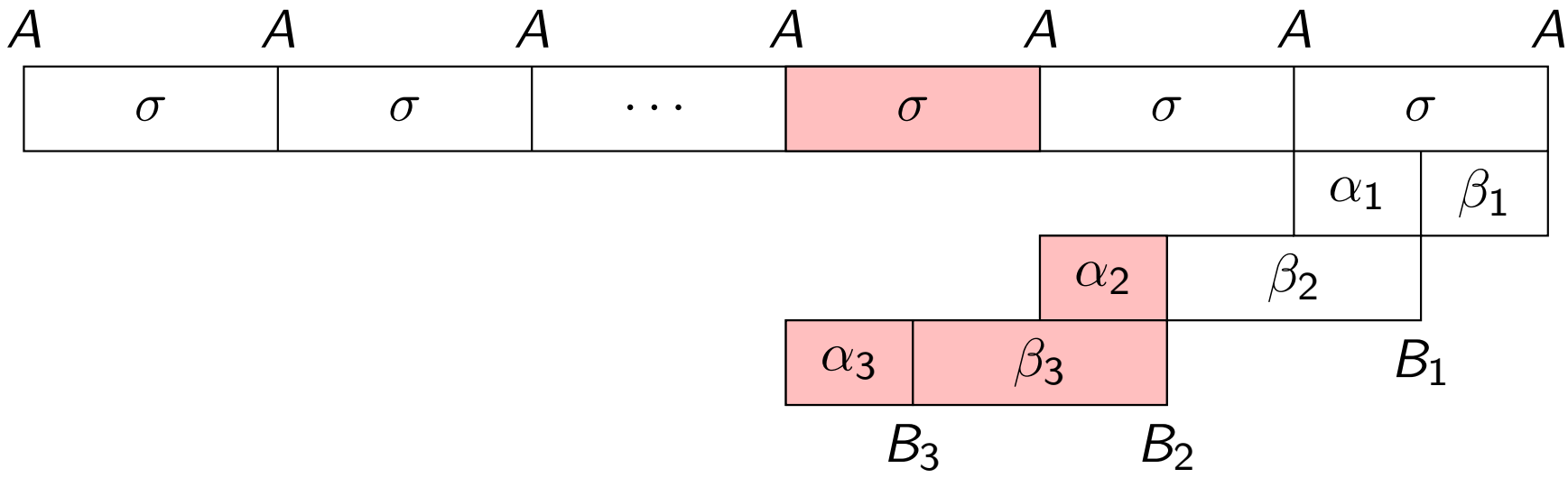
Let $\sigma : A^* \to A^*$ be a substitution.

Let us assume that σ is not recognizable in $X(\sigma)$ for aperiodic points.



Proof of the theorem

Let $\sigma : A^* \to A^*$ be a substitution.
Let us assume that σ is not recognizable in $X(\sigma)$ for aperiodic points.
We define $\alpha_0 : A^* \to A^*$ as the identity substitution.
Thus, $\sigma = \sigma \circ \alpha_0$ is not elementary. We decompose it into $\alpha_1 \circ \beta_1$ through B_1 such that $\mathrm{Card}(B_1) < \mathrm{Card}(A)$.
Then, $\sigma \circ \alpha_1$ is not fully recognizable for aperiodic points by the above lemma.
Thus, $\sigma \circ \alpha_1$ is not elementary.



Proof of the theorem

We decompose it into $\sigma \circ \alpha_1 = \alpha_2 \circ \beta_2$ through B_2 such that $\mathrm{Card}(B_2) < \mathrm{Card}(B_1)$.
Again, $\sigma \circ \alpha_2$ is not fully recognizable for aperiodic points and thus not elementary.

Inductively, we define $\sigma \circ \alpha_i = \alpha_{i+1} \circ \beta_{i+1}$ through B_{i+1} such that $\mathrm{Card}(B_{i+1}) < \mathrm{Card}(B_i)$.
We get a contradiction since $\mathrm{Card}(A) < \infty$.