Master 2 Mathematics and Computer Science Symbolic Dynamics. Lecture 1

Marie-Pierre Béal

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

Université Gustave Eiffel

Topology and shift transformation

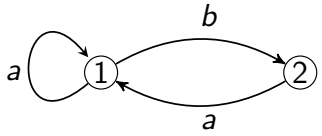
The set $A^{\mathbb{Z}}$ of two-sided infinite sequences of elements of A is a metric space for the distance defined for $x \neq y$ by $d(x, y) = 2^{-r(x,y)}$ where

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

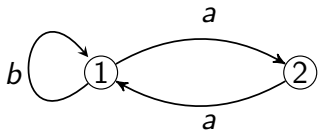
The topology induced by this metric coincides with the product topology on $A^{\mathbb{Z}}$, using the discrete topology on A.
Since a product of compact spaces is compact, $A^{\mathbb{Z}}$ is a compact metric space.

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.

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



Example of a sofic shift: the even shift



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.

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 $\mathsf{X}(L)$ 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: $\mathcal{B}(\mathsf{X}(L)) = L$, and $\mathsf{X}(\mathcal{B}(X)) = X$.

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).

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 $uav \in \mathcal{B}(X)$.

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).

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. □

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.

Master 2 Mathematics and Computer Science Symbolic Dynamics. Lecture 2

Marie-Pierre Béal

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

Université Gustave Eiffel

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. □

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 $X = X_F$ 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). □

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.

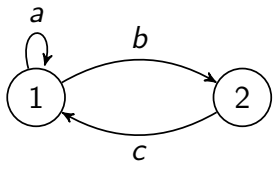
- $Q' = Q \setminus \{s\} \cup \{s_1, s_2\}$,
- E' contains all edges of E neither starting at or ending in s,
- E' contains the edge (s_1, a, t) for each edge $(s, a, t) \in E_1$, and the edge (s_2, a, t) for each edge $(s, a, t) \in E_2$, if $t \neq s$.
- E' contains the edges (t, a, s_1) and (t, a,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

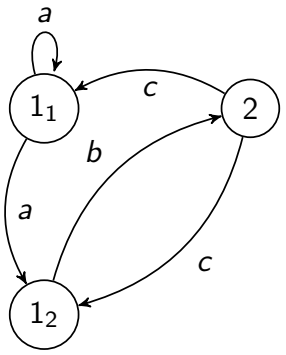
State splitting of an automaton

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*.

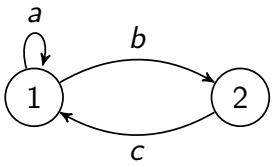
Output state splitting of an automaton

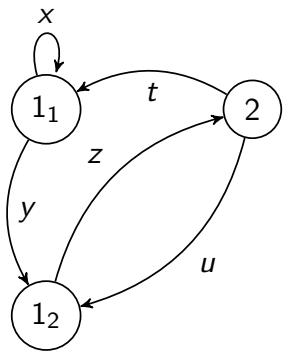




The state 1 is split into two states 1_1 and 1_2 with $E_1 = \{(1, a, 1)\}$ and $E_2 = \{(1, b, 2)\}$.

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. □

Marie-Pierre Béal Master 2 Mathematics and Computer Science Symbolic Dynamic

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)

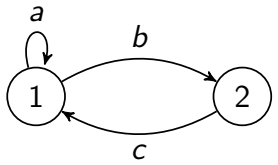
Two edge shifts defined by matrices M and N are conjugate if and only if M and N are strong shift equivalent.

Marie-Pierre Béal Master 2 Mathematics and Computer Science Symbolic Dynamic

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.



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

Marie-Pierre Béal Master 2 Mathematics and Computer Science Symbolic Dynamic

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.

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.

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.

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).

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 of a shift of finite type

Theorem

Let G be a graph with adjacency matrix M. Then

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

Master 2 Mathematics and Computer Science Symbolic Dynamics. Lecture 3

Marie-Pierre Béal

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

Université Gustave Eiffel

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.

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'.

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.

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.

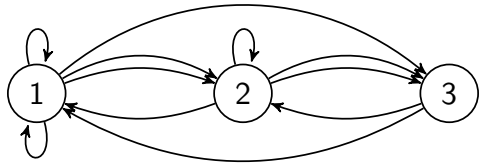
Let us assume that there is an out-merging of G with adjacency matrix M into G' with adjacency matrix M', obtained by merging s_1 and s_2 into s_1, and an out-merging of G into G'' with adjacency matrix M'', obtained by merging s_3 and s_4 into s_3.
We may assume that the set $\{s_3, s_4\}$ is distinct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

□

Total amalgamation

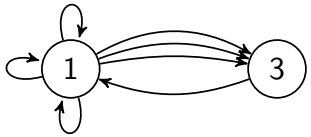
If G is the following graph:



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

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

Lettre coding

A substitution $\sigma\colon A^* \to B^*$ 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 $\sigma\colon A^* \to B^*$, 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 $\sigma\colon A^* \to B^*$ 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 $\sigma\colon B^* \to C^*$ and $\tau\colon A^* \to B^*$ 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 $\sigma\colon a \mapsto ab, b \mapsto aa$ is

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

Iteration of a substitution

A substitution $\sigma\colon A^* \to A^*$ 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 $\sigma\colon A^* \to A^*$ 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 $\sigma\colon A^* \to A^*$ be an iterable substitution.
The *substitution shift* defined by σ is the shift space $\mathrm{X}(\sigma)$ 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

$$\sigma(\mathrm{X}(\sigma)) \subseteq \mathrm{X}(\sigma). \qquad (5)$$

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 $\sigma\colon a \mapsto ab, b \mapsto b$. 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 $\sigma\colon A^* \to A^*$ 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, $\lim_{n\to+\infty} |\sigma^n(a)| = +\infty$.

Primitive substitutions

An iterable substitution $\sigma\colon A^* \to A^*$ 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 $\mathcal{L}(\sigma) = \mathcal{B}(X(\sigma))$ 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 $\mathcal{R}_X(u)$.

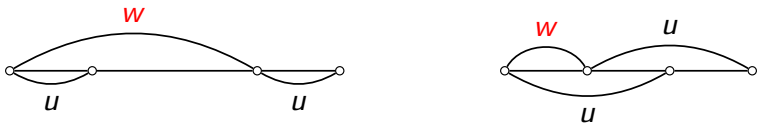


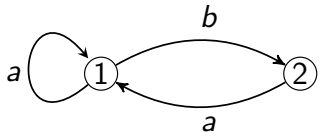
Figure: Return word to u.

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.

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. □

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 $X(\sigma)$ 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 $\mathcal{B}(X(\sigma)) = \mathcal{L}(\sigma)$.
Let $n \geq 1$ be such that every $b \in A$ occurs in every $\sigma^n(a)$ for $a \in A$. □

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.

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.

□

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 = σ^ω(a) and w ∈ R_X(u)
2  ▷ Returns in R the set R_X(u)
3  R ← ∅
4  S ← {w}
5  ▷ S is the set of return words to be processed
6  while S ≠ ∅ do
7        r ← an element of S
8        S ← S \ {r}
9        R ← R ∪ {r}
10       r(1), ··· , r(k) ← σ(r)
11       ▷ The words r(i) are the decomposition of σ(r) in return words to u
12       for i ← 1 to k do
13             if r(i) ∉ R ∪ S then
14                   S ← S ∪ r(i)
15 return R
```


Example

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

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 $\max p_x(n)$.

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* $\mathcal{B}_2(\mathrm{X}(\sigma))$*.*

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 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* $n \geq n_0$*.*

Master 2 Mathematics and Computer Science Symbolic Dynamics. Lecture 6

Marie-Pierre Béal

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

Université Gustave Eiffel

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 $0 \leq k < |\sigma(x_0)|$.

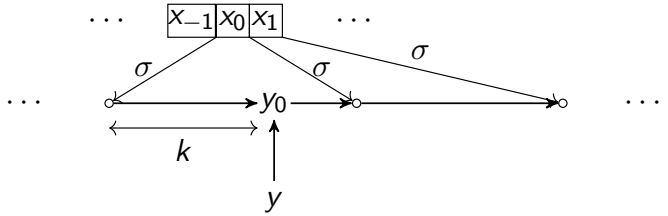


Figure: A centered σ-representation (x, k) of y.

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 $\sigma\colon A^* \to B^*$ 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 $\sigma\colon a \mapsto a, b \mapsto ab, c \mapsto abb$ 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.

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 $y = S^k\phi(x)$. □

Existence of a representation

Proposition

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

Elementary substitution

A substitution $\sigma\colon A^* \to C^*$ 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).

Elementary substitution

Note that the property of being elementary is decidable.
Indeed, if $\sigma\colon A^* \to C^*$ 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

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

Elementary substitution

By a symmetric version, an elementary substitution $\sigma\colon A^* \to C^*$ 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 $\sigma\colon A^* \to C^*$ is injective on $A^{\mathbb{Z}}$.

Recognizability for aperiodic points

A substitution $\sigma\colon A^* \to B^*$ 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.

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 $X(\sigma)$.

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

An elementary substitution is fully recognizable 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 $X(\sigma)$.

Marie-Pierre Béal Master 2 Mathematics and Computer Science Symbolic Dynamic

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.

Marie-Pierre Béal Master 2 Mathematics and Computer Science Symbolic Dynamic