Jean Berstel

# Transductions and Context-Free Languages

December 14, 2009

# Preface to the electronic edition

This electronic edition contains the first four chapters of the book which is no more available. These are considered to be still relevant for students.

The following modifications to the printed versions appear.

## Notational modifications

$$
\begin{aligned}
X, Y, Z &\to A, B, C \\
A, B, C &\to X, Y, Z \\
f, g, h &\to w, x, y
\end{aligned}
$$

## Improvements in English

| | | |
|---|---|---|
| achieves | → | completes |
| unicity | → | uniqueness |
| i.e. | → | that is |
| iff | → | if and only if |
| system of generators | → | set of generators |
| lexicographical | → | lexicographic |

## Improvements in proofs

Proof of Lemma II.3.2 has been simplified (argument of G. Cousineau).
The automaton of Example I.4.1 has been corrected.

## Errors in exercises

Exercise III.8.3 has been removed since I am not sure it is correct as stated.

## Acknowledgement

Thanks to Belen Soler for having detected so many typos.

## Books

There exist several excellent introductions and presentations of the modern theory of automata, languages, machines, formal series, transductions. The book by J. Sakarovitch is the latest achievement in this series. It reports recent results and replaces older theory in a new perspective.

Paris, Winter 2006 — 2009 J. Berstel

# Preface

This book present a theory of formal languages with main emphasis on rational transductions and their use for the classification of context-free languages. The level of presentation corresponds to that of beginning graduate or advanced undergraduate work. Prerequisites for this book are covered by a "standard" first-semester course in formal languages and automata theory, e.g. a knowledge of Chapters 1–3 of Ginsburg (1966), or Chapters 3–4 of Hopcroft and Ullman (1969), or Chapter 2 of Salomaa (1973), or Chapters 2 and 4 of Becker and Walter (1977) would suffice. The book is self-contained in the sense that complete proofs are given for all theorems stated, except for some basic results explicitly summarized at the beginning of the text. Chapter IV and Chapters V–VIII are independent from each other.

The subject matter is divided into two preliminary and six main chapters. The initial two chapters contain a general survey of the "classical" theory of regular and context-free languages with a detailed description of several special languages. Chapter III deals with the general theory of rational transductions, treated in an algebraic fashion along the lines of Eilenberg, and which will be used systematically in subsequent chapters. Chapter IV is concerned with the important special case of rational functions, and gives a full treatment of the latest developments, including subsequential transductions, unambiguous transducers and decision problems.

The study of families of languages (in the sense of Ginsburg) begins with Chapter V.(. . . )

The notes from which this book derives were used in courses at the University of Paris and at the University of Saarbrücken. I want to thank Professor G. Hotz for the opportunity he gave me to stay with the Institut für angewandte Mathematik und Informatik, and for his encouragements to write this book. I am grateful to the following people for useful discussions or comments concerning various parts of the text: J.-M. Autebert, J. Beauquier, Ch. Choffrut, G. Cousineau, K. Estenfeld, R. Linder, M. Nivat, D. Perrin, J.-F. Perrot, J. Sakarovitch, M. Soria, M. Stadel, H. Walter. I am deeply indebted to M.-P. Schützenberger for his constant interest in this book and for many fruitful discussions. Special thanks are due to L. Boasson whose comments have been of an invaluable help in the preparation of many sections of this book. I want to thank J. Messerschmidt for his careful reading of the manuscript and for many pertinent comments, and Ch. Reutenauer for checking the galley proofs. I owe a special debt to my wife for her active contribution at each step of the preparation of the book, and to Bruno and Clara for their indulgence.

Paris, Spring 1978 J. Berstel

# Contents

# Chapter I

# Preliminaries

This chapter is a short review of some basic concepts used in the sequel. Its aim is to agree on notation and terminology. We first consider monoids, especially free monoids, and morphisms. Then a collection of definitions and results is given, dealing with finite automata and regular languages.

## 1 Some Notations

$\mathbb{N} = \{0, 1, 2, \ldots\}$ is the set of nonnegative integers. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, \ldots\}$ is the set of integers. Let $E$ be a set. Then $\mathrm{Card}(E)$ is the number of its elements. The empty set is denoted by $\emptyset$. If $X, Y$ are subsets of $E$, then we write $X \subset Y$ if and only if $x \in X \implies x \in Y$, and $X \subsetneq Y$ if $X \subset Y$ and $X \neq Y$. Further

$$X \setminus Y = \{x \in E \mid x \in X \text{ and } x \notin Y\} .$$

A *singleton* is a subset of $E$ consisting of just one element. If no confusion can arise, we shall not distinguish elements of $E$ from singletons. The set of all subsets of $E$, that is the powerset of $E$ is denotes by $\mathfrak{P}(E)$ or $2^E$. With the preceding convention, $E \subset \mathfrak{P}(E)$.

The *domain* $\mathrm{dom}(\alpha)$ of a partial function $\alpha : E \to F$ is the set of elements $x$ in $E$ for which $\alpha(x)$ is defined. $\alpha$ can be viewed as a (total) function from $E$ into $\mathfrak{P}(F)$, and with the convention $F \subset \mathfrak{P}(F)$, as a total function from $E$ into $F \cup \{\emptyset\}$. Then $\mathrm{dom}(\alpha) = \{x \in \ \mid \alpha(x) \neq \emptyset\}$.

## 2 Monoids, Free Monoids

A *semigroup* consists of a set $M$ and a binary operation on $M$, usually denoted by multiplication, and which is postulated to be *associative*: For any $m_1, m_2, m_3 \in M$, $m_1(m_2m_3) = (m_1m_2)m_3$. A *neutral element* or a *unit* is an element $1_M \in M$ (also noted 1 for short) such that $1_M m = m1_M = m$ for all $m \in M$. A semigroup which has a neutral element is a *monoid*. The neutral element of a monoid is unique. Indeed, if $1'$ is another neutral element, then $1' = 11' = 1$.

Given two subsets $X, Y$ of a monoid $M$, the product $XY$ is defined by

$$XY = \{z \in M \mid \exists x \in X, \exists y \in Y : z = xy\} . \tag{2.1}$$

This definition converts $\mathfrak{P}(M)$ into a monoid with unit $\{1_M\}$. A subset $X$ of $M$ is a *subsemigroup* (*submonoid*) of $M$ if $X^2 \subset X$ ($1 \in X$ and $X^2 \subset X$). Given any subset $X$ of $M$, the sets

$$X^+ = \bigcup_{n \geq 1} X^n\,, \quad X^* = \bigcup_{n \geq 0} X^n\,,$$

where $X^0 = \{1\}$ and $X^{n+1} = X^n X$, are a subsemigroup resp. a submonoid of $M$. In fact, $X^+$ (resp. $X^*$) is the least subsemigroup (resp. submonoid) for the order of set inclusion containing $X$. It is called the subsemigroup (submonoid) *generated* by $X$. If $M = X^*$ for some $X \subset M$, then $X$ is a *set of generators* of $M$. A monoid is *finitely generated* if it has a finite set of generators. The unary operations $X \mapsto X^+$ and $X \mapsto X^*$ on subsets of $M$ are called the (Kleene) *plus* and *star* operations. The formulas $X^+ = XX^* = X^*X$ and $X^* = 1 \cup X^+$. are readily verified.

For any set $A$, the *free monoid* $A^*$ generated by $A$ or with *base* $A$ is defined as follows. The elements of $A^*$ are $n$-tuples

$$u = (a_1, a_2, \ldots, a_n) \quad (n \geq 0) \tag{2.2}$$

of elements of $A$. If $v = (b_1, \ldots, b_m)$ is another element of $A^*$, the product $uv$ is by defined by concatenation, that is

$$uv = (a_1, a_2, \ldots, a_n, b_1, \ldots, b_m)\,.$$

This produces a monoid with the only 0-tuple $1 = ()$ as neutral element. We shall agree to write $a$ instead of the 1-tuple $(a)$. Thus (2.2) may be written as:

$$u = a_1 a_2 \cdots a_n\,.$$

Because of this, $u$ is called a *word*, $a \in A$ is called a *letter* and $A$ itself is called an *alphabet*. By the convention $a = (a)$, $A$ can be considered as a subset of $A^*$. This justifies the notation $A^*$, since indeed $A^*$ is the only submonoid of $A^*$ containing $A$. Further, $A^+ = A^* \setminus 1$. In the sequel, and unless otherwise indicated, an alphabet will be supposed to be *finite* and *nonempty*.

We shall use the following terminology concerning a free monoid $A^*$ generated by an alphabet $A$. A (formal) *language* over $A$ is any subset of $A^*$. The *length* $|u|$ of a word $u \in A^*$ is the number of letters composing it. The neutral element of $A^*$ is called the *empty word*, and is noted 1 or $\varepsilon$. It is the only word of length 0. Clearly $|uv| = |u| + |v|$. If $B \subset A$, then $|u|_B$ is the number of occurrences of letters $b \in B$ in $u$. Thus

$$|u| = \sum_{a \in A} |u|_a\,.$$

The reversal of a word $u = a_1 a_2 \cdots a_n$ ($n \geq 0, a_i \in A$) is denoted by $\tilde{u}$ or $u\tilde{}$, and is defined by $\tilde{u} = a_n a_{n-1} \cdots a_2 a_1$. Clearly $\tilde{\tilde{u}} = u$, $\tilde{1} = 1$, $(uv)\tilde{} = \tilde{v}\tilde{u}$. For $X \subset A^*$, $\tilde{X} = \{\tilde{u} \mid u \in X\}$. If $Y \subset A^*$, then $(XY)\tilde{} = \tilde{Y}\tilde{X}$, and $(X^*)\tilde{} = (\tilde{X})^*$.

Let $u \in A^*$. Then a word $v$ is a *factor* of $u$ if $u = xvy$ for some $x, y \in A^*$. If $x = 1$, then $v$ is a *prefix*; if $y = 1$, then $v$ is a *suffix* of $u$. $v$ is a *proper* factor (proper prefix, proper suffix) of $u$ if further $v \neq u$. A word $v$ may occur at several places as a factor of $u$. A fixed occurrence of $v$ as a factor of $u$ is called a *segment*. This definition always refers to some previously defined factorization $u = xvy$. If $u = x'v'y'$ is another factorization, then the segment $v'$ is *contained* in the segment $v$ if and only if $x$ is a prefix of $x'$ and $y$ is a suffix of $y'$. Finally, $v$ is a *subword* of $u$ if $u = w_0a_1w_1 \cdots a_nw_n$, ($n \geq 0$, $a_1, \ldots, a_n \in A$, $w_0, \ldots, w_n \in A^*$) and $v = a_1 \cdots a_n$.

Let $M$ be a submonoid of $A^*$. Then $X = (M \setminus 1) \setminus (M \setminus 1)^2$ is a set of generators of $M$, that is $X^* = M$. Further $X$ is minimal with this property, that is $Y^* = M$ implies $Y \supset X$. A submonoid $M$ of $A^*$ is *free* with *base* $Z$ if any word $u \in M$ has one and only one factorization $u = z_1z_2 \cdots z_n$, with $n \geq 0$ and $z_1, \ldots, z_n \in Z$. The base of a free submonoid $M$ is unique and is equal to $(M \setminus 1) \setminus (M \setminus 1)^2$. Thus $A^*$ is free with base $A$. A base of a free submonoid is called a *code*. Examples of codes are supplied by prefix and suffix sets. A subset $X$ of $A^+$ is *prefix* if and only if $XA^+ \cap X = \emptyset$, that is if $X$ contains no proper prefix of some of its words, and $X$ is *suffix* if and only if $A^+X \cap X = \emptyset$. $X$ is *bifix* if it is both prefix and suffix. Any prefix or suffix subset is a code.

Let $M$ be any monoid, and let $X, Y \subset M$. The *left* and *right quotients* $Y^{-1}X$ and $XY^{-1}$ are the sets

$$\begin{aligned} Y^{-1}X &= \{z \in M | \exists x \in X, \exists y \in Y, x = yz\}\,, \\ XY^{-1} &= \{z \in M | \exists x \in X, \exists y \in Y, x = zy\}\,. \end{aligned}$$

If $M$ is a group and $u, v \in M$, then $v^{-1}u$ and $uv^{-1}$ are always singletons. If $M$ is a free monoid, then $uv^{-1}$ is non empty if and only if $v$ is a suffix of $u$; thus $uM^{-1}$ is the set of prefixes of $u$.

Sometimes, we shall need the notion of semiring. A *semiring* consists of a set $S$ and of two binary operations, called addition and multiplication, noted $+$ and $\cdot$, and satisfying the following conditions:

(i) $S$ is a commutative monoid for the addition ($s+t = t+s$ for all $s, t \in S$) with neutral element $0$;

(ii) $S$ is a monoid for the multiplication;

(iii) the multiplication is distributive with respect to the addition:

$$s(t_1 + t_2) = st_1 + st_2\,,\ \ (t_1 + t_2)s = t_1s + t_2s \text{ for all } s, t_1, t_2 \in S;$$

(iv) for all $s \in S$, $0 \cdot s = s \cdot 0 = 0\,.$

If $M$ is a monoid, then $\mathfrak{P}(M)$ is a semiring with set union for addition and the multiplication (2.1).

## Exercises

**2.1** Let $M_1$ and $M_2$ be monoids. Show that the Cartesian product $M_1 \times M_2$ is a monoid when multiplication is defined by $(m_1, m_2)(m'_1, m'_2) = (m_1m'_1, m_2, m'_2)$.

**2.2** Show that if $S$ is a semiring, then the set $S^{n\times n}$ of square matrices of size $n$ with coefficients in $S$ can be made a semiring, for addition and multiplication of matrices induced by the operations in $S$.

**2.3** Let $M$ be a monoid, and let $X, Y, Z \subset M$. Prove the following formulas: $(XY)^{-1}Z$ $= Y^{-1}(X^{-1}Z)$, $(X^{-1}Y)Z^{-1} = X^{-1}(YZ^{-1})$.

**2.4** Let $A$ be an alphabet, $X \subset A^+$, $X \neq \emptyset$. Show that $X$ is prefix if and only if $X^{-1}X = 1$.

**2.5** Let $A$ be an alphabet, and let $x, y \in A^+$. Show that the three following conditions are equivalent:
(i) $x = z^r$, $y = z^s$ for some word $z$ and $r, s \geq 1$;
(ii) $xy = yx$;
(iii) $x^m = y^n$ for some $m, n \geq 1$.

**2.6** Two words $x$ and $y$ are *conjugate* if $xz = zy$ for some word $z$. Show that this equation holds if and only if $x = uv$, $y = vu$, $z = (uv)^k u$ for some words $u, v$ and $k \geq 0$.

**2.7** A word $x$ is *primitive* if and only if it is not a nontrivial power of another word, that is if $x = z^n$ implies $n = 1$.
a) Show that any word $x \neq 1$ is a power of a unique primitive word.
b) Show that if $x$ and $y$ are conjugate, and $x$ is primitive, then $y$ is also primitive.
c) Show that if $xz = zy$ and $x \neq 1$, then there are unique primitive words $u, v$ and integers $p \geq 1, k \geq 0$ such that $x = (uv)^p$, $y = (vu)^p$, $z = (uv)^k u$.

## 3 Morphisms, Congruences

If $M, M'$ are monoids, a (monoid) *morphism* $\alpha : M \to M'$ is a function satisfying

$$\alpha(m_1 m_2) = \alpha(m_1)\alpha(m_2) \quad \text{for all } m_1, m_2 \in M \tag{3.1}$$
$$\alpha(1_M) = 1_{M'} .$$

Then clearly $\alpha(M)$ is a submonoid of $M'$. If only (3.1) is postulated, then $\alpha$ is called a *semigroup morphism* and $\alpha(M)$ is a subsemigroup of $M'$. Unless otherwise indicated, morphism always means monoid morphism. A morphism $\alpha : A^* \to M'$, where $A$ is an alphabet, is completely defined by the values $\alpha(a)$ of the letters $a \in A$. We now review some formulas. Let $\alpha : M \to M'$ be a function, and let $X, Y \subset M$, $X', Y' \subset M'$. Then

$$\alpha(X \cup Y) = \alpha(X) \cup \alpha(Y) , \quad \alpha^{-1}(X' \cup Y') = \alpha^{-1}(X') \cup \alpha^{-1}(Y') ,$$
$$\alpha^{-1}(X' \cap Y') = \alpha^{-1}(X') \cap \alpha^{-1}(Y') , \quad \alpha(\alpha^{-1}(X') \cap Y) = X' \cap \alpha(Y) .$$

Next, if $\alpha$ is a semigroup morphism, then

$$\alpha(XY) = \alpha(X)\alpha(Y) , \quad \alpha(X^+) = (\alpha(X))^+ .$$

If $\alpha$ is a morphism, then $\alpha(X^*) = (\alpha(X))^*$.

Note that the formula $\alpha^{-1}(X'Y') = \alpha^{-1}(X')\alpha^{-1}(Y')$ is in general false. This observation leads to the definition of particular morphisms, for which that formula holds.

Let $A, B$ be alphabets, and let $\alpha : A^* \to B^*$ be a morphism. Then $\alpha$ is called
*alphabetic* if $\alpha(A) \subset B \cup 1$;
*strictly alphabetic* if $\alpha(A) \subset B$;
*continuous* or *$\varepsilon$-free* if $\alpha(A) \subset B^+$;
a *projection* if $B \subset A$, and if $\alpha(b) = b$ for $b \in B$, and $\alpha(a) = 1$ for $a \in A \setminus B$.

Thus projections are particular alphabetic morphisms. If $\alpha : A^* \to B^*$ is an alphabetic morphism, then

$$\alpha^{-1}(XY) = \alpha^{-1}(X)\alpha^{-1}(Y)\,, \quad \alpha^{-1}(X^+) = (\alpha^{-1}(X))^+$$

for $X, Y \subset B^*$. For the proof, it suffices to show that $\alpha^{-1} : B^* \to \mathfrak{P}(A^*)$ is a semigroup morphism. Define

$$\begin{aligned}&C = \{a \in A \mid \alpha(a) = 1\} = \alpha^{-1}(1) \cap A\,;\\ &C_b = \{a \in A \mid \alpha(a) = b\} = \alpha^{-1}(b) \cap A \quad \text{for } b \in B\,.\end{aligned}$$

Then

$$\alpha^{-1}(1) = C^*\,, \quad \alpha^{-1}(b) = C^*C_bC^* \quad (b \in B)\,.$$

If $y = b_1 \cdots b_n$, $(b_i \in B)$, then

$$\alpha^{-1}(y) = C^*C_{b_1}C^*C_{b_2}C^* \cdots C^*C_{b_n}C^*\,;$$

Thus $\alpha^{-1}(y_1y_2) = \alpha^{-1}(y_1)\alpha^{-1}(y_2)$ for all $y_1, y_2 \in B^*$. This completes the proof. Note that the formula $\alpha^{-1}(X^*) = (\alpha^{-1}(X))^*$ is only true if further $\alpha$ is continuous, or if $1 \in X$, that is if $X^* = X^+$.

We shall frequently use special morphisms called copies. Let $\alpha : A^* \to B^*$ be an isomorphism. Then $\alpha(A) = B$. For each subset $X$ of $A^*$, $\alpha(X)$ is called a *copy* of $X$ on $B$.

Another class of particular morphisms are substitutions. A *substitution* $\sigma$ from $A^*$ into $B^*$ is a (monoid) morphism from $A^*$ into $\mathfrak{P}(B^*)$; thus $\sigma$ verifies: $\sigma(a) \subset B^*$ for $a \in A$, and

$$\sigma(1) = 1\,, \quad \sigma(uv) = \sigma(u)\sigma(v) \quad \text{for } u, v \in A^*\,.$$

Thus, if $\alpha : B^* \to A^*$ is an alphabetic morphism, the function $\alpha^{-1}$ is a substitution if and only if $\alpha^{-1}(1) = 1$. A substitution $\sigma$ is extended to $\mathfrak{P}(A^*)$ by the convention

$$\sigma(X) = \bigcup_{x \in X} \sigma(x) \quad (X \subset A^*)\,.$$

For sake of simplicity, we write $\sigma : A^* \to B^*$ for a substitution from $A^*$ into $B^*$. If $\tau : B^* \to C^*$ is another substitution, then the function $\tau \circ \sigma$ from $A^*$ into $\mathfrak{P}(C^*)$ is a substitution.

Finally, we note that any finitely generated monoid is the homomorphic image of a free monoid. Consider indeed a monoid $M$, and let $S = \{m_1, \ldots, m_k\}$ be a set of generators of $M$. Set $A = \{a_1, \ldots, a_k\}$, and define a morphism $\alpha : A^* \to M$ by $\alpha(a_i) = s_i$ for $i = 1, \ldots, k$. Then $\alpha(A^*) = (\alpha(A))^* = S^* = M$. Clearly this result remains true for any monoid if infinite alphabets are considered.

Let $E$ and $F$ be two sets. A *relation* over $E$ and $F$ is a subset $\theta$ of $E \times F$. For $(x, y) \in \theta$, we also write $x\theta y$, $x \sim y \pmod{\theta}$ or $x \equiv y \pmod{\theta}$, or simply $x \sim y$ or $x \equiv y$ if no confusion can arise. If $E = F$, then $\theta$ is a relation over $E$. Relations are ordered by (set) inclusion.

Let $M$ be a monoid. A *congruence* over $M$ is an equivalence relation $\theta$ which is compatible with the monoid operation, that is which satisfies

$$m_1 \equiv m_1' (\text{mod } \theta), m_2 \equiv m_2' (\text{mod } \theta) \Rightarrow m_1 m_2 \equiv m_1' m_2' (\text{mod } \theta). \tag{3.2}$$

For each $m \in M$, the *class* of $m$ mod $\theta$ is

$$[m]_\theta = \{m' \in M \mid m \equiv m' \ (\text{mod } \theta)\}\,.$$

Then (3.2) is equivalent to

$$[m_1]_\theta [m_2]_\theta \subset [m_1 m_2]_\theta\,.$$

If $\theta$ is a congruence, then the function which associates to each $m \in M$ its class $[m]_\theta$ is a morphism from $M$ onto the *quotient monoid* $M/\theta$. Conversely, if $\alpha : M \to M'$ is a morphism, then the relation $\theta$ defined by

$$m \sim m' \ (\text{mod } \theta) \quad \text{if and only if} \quad \alpha(m) = \alpha(m')$$

is a congruence. The number of equivalence classes of an equivalence relation $\theta$ is the *index* of $\theta$. The index is a positive integer or infinite.

Given a relation $\theta$ over a monoid $M$, the congruence $\hat{\theta}$ *generated* by $\theta$ is the least congruence containing $\theta$. The congruence $\hat{\theta}$ can be constructed as follows: Define a relation $\theta_1$ on $M$ by:

$$\begin{aligned} m \sim m' \ (\text{mod } \theta_1) \ \ &\text{if and only if} \ \ m = uxv, m' = uyv \\ &\text{and } (x \sim y \ (\text{mod } \theta) \text{ or } y \sim x \ (\text{mod } \theta))\,. \end{aligned}$$

Next define a relation $\theta_1^*$ by $m \equiv m'$ (mod $\theta_1^*$) if and only if there exist $k \geq 0$ and $m_0, \ldots, m_k \in M$ such that $m = m_0$, $m' = m_k$ and $m_i \sim m_{i+1}$ (mod $\theta_1$) for $i = 0, \ldots, k-1$. Then it is easily shown that $\theta_1^* = \hat{\theta}$.

**Example 3.1** Let $A$ be an alphabet, and define a relation over $A^*$ by

$$ab \sim ba \quad \text{for } a, b \in A, \ a \neq b\,.$$

Let $\hat{\theta}$ be the congruence generated by this relation. Then $u \equiv v$ (mod $\hat{\theta}$) if and only if $|u|_a = |v|_a$ for all $a \in A$. The quotient monoid $A^*/\hat{\theta}$ is denoted by $A^\oplus$ and is called the *free commutative monoid* generated by $A$.

## Exercises

**3.1** Let $M$ be a group, $M'$ be a monoid, and let $\alpha : M \to M'$ be a monoid morphism. Show that $\alpha(M)$ is a group and that $\alpha$ is a group morphism ($\alpha(m^{-1}) = (\alpha(m)^{-1}$ for $m \in M$).

**3.2** Give examples of morphisms $\alpha : A^* \to B^*$ such that $\alpha^{-1}(XY) \supsetneq \alpha^{-1}(X)\alpha^{-1}(Y)$ and $\alpha^{-1}(X^*) \supsetneq (\alpha^{-1}(X))^*$.

**3.3** Let $A, B$ be alphabets and let $\alpha : A^* \to B^*$ be a morphism. Show that there are an alphabet $C$, an injective morphism $\beta : A^* \to C^*$ and a projection $\gamma : C^* \to B^*$ such that $\alpha = \gamma \circ \beta$.

**3.4** Let $A$ be an alphabet. Given $X \subset A^*$, the *norm* of $X$ is the number

$$\|X\| = 2^{-\omega(A)}, \quad \text{where } \omega(X) = \min\{|u| \mid u \in X\}, \quad \omega(\emptyset) = \infty\,.$$

If $Y \subset A^*$, the *distance* $d(X,Y)$ is the number

$$d(X,Y) = \|X \setminus Y \cup Y \setminus X\|\,.$$

a) Show that $\|\ \|$ and $d$ are a norm and a distance in the usual topological sense, and that $d$ satisfies the ultrametric inequality: $d(X,Y) \le \max\{d(X,Z), d(Z,Y)\}$.
b) Let $\alpha : A^* \to B^*$ be a morphism. Show that the mapping from $\mathfrak{P}(A^*)$ into $\mathfrak{P}(B^*)$ defined by $\alpha$ is continuous for this topology if an only if $\alpha(A) \subset B^+$. (This is the reason why an $\varepsilon$-free morphism is called continuous.)

**3.5** Let $A$ be an alphabet, and let $L \subset A^*$. The *syntactic congruence* $\theta_L$ of $L$ is the coarsest (greatest) congruence over $A^*$ which saturates $L$, that is such that $u \in L$, $u \equiv v \pmod{\theta_L}$ implies $v \in L$. Show that

$$u \equiv v \pmod{\theta_L} \text{ if and only if for all } x, y \in A^* : xuy \in L \iff xvy \in L\,.$$

The quotient monoid $\mathrm{Synt}(L) = A^*/\theta_L$ is called the *syntactic monoid* of $L$. Show that $\mathrm{Synt}(L) = \mathrm{Synt}(A^* \setminus L)$.

**3.6** Let $M, N$ be monoids, $\alpha : M \to N$ a morphism. Let $X \subset M$, $Q \subset N$, and set $Y = \alpha(X)$, $P = \alpha^{-1}(Q)$. Show that $X^{-1}P = \alpha^{-1}(Y^{-1}Q)$.

# 4 Finite Automata, Regular Languages

In this section, we review some basic facts concerning finite automata, mainly in order to fix notation and to allow references in later chapters. When the proofs are omitted, they can be found in any of the books listed in the bibliography.

**Definition** A finite (deterministic) automaton $\mathcal{A} = \langle A, Q, q_-, Q_+, \delta\rangle$ consists of an *alphabet* $A$, a *finite* set $Q$ of *states*, an *initial state* $q_- \in Q$, a set of *final states* $Q_+ \subset Q$, and a *next state function* $\delta : A \times Q \to Q$.

If no confusion can arise, we denote $\delta$ by a dot, and we write

$$\mathcal{A} = \langle A, Q, q_-, Q_+\rangle$$

instead of the above notation. The next state function is extended to $Q \times A^*$ by setting

$$q \cdot 1 = q \tag{4.1}$$
$$q \cdot ua = (q \cdot u) \cdot a \quad u \in A^*, a \in A\,. \tag{4.2}$$

Then the formula

$$q \cdot uv = (q \cdot u) \cdot v \quad u, v \in A^* \tag{4.3}$$

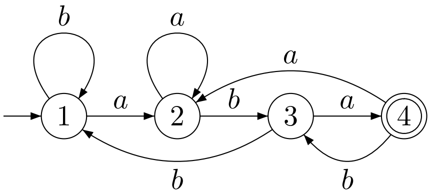

Figure I.1

is easily verified. A word $u \in A^*$ is *recognized* or *accepted* by $\mathcal{A}$ if and only if $q_- \cdot u \in Q_+$. The *language recognized* by $\mathcal{A}$ is

$$|\mathcal{A}| = \{u \in A^* \mid q_- \cdot u \in Q_+\}\,. \tag{4.4}$$

A language $L \subset A^*$ is *recognizable* or *regular* if and only if $L = |\mathcal{A}|$ for some finite automaton $\mathcal{A}$.

Finite automata can be represented by a graph in the following way. Each state $q$ is represented by a vertex, and an edge labeled $a$ is drawn from $q$ to $q'$ if and only if $q \cdot a = q'$. The initial state has an arrow entering in it. Final states are circled twice.

**Example 4.1** Let $\mathcal{A}$ be defined by $A = \{a, b\}$, $Q = \{1, 2, 3, 4\}$, $q_- = 1$, $Q_+ = \{4\}$, and the next state function given by

| | $a$ | $b$ |
|---|---|---|
| 1 | 2 | 1 |
| 2 | 2 | 3 |
| 3 | 4 | 1 |
| 4 | 2 | 3 |

Then $\mathcal{A}$ is represented in Figure I.1. A word is recognized by $\mathcal{A}$ if and only if it has $aba$ as a suffix. Thus $|\mathcal{A}| = A^*aba$.

The following result is known as Kleene's Theorem.

**Theorem 4.1** (Kleene 1956) *The family of regular languages over $A$ is equal to the least family of languages over $A$ containing the empty set and the singletons, and closed under union, product and the star operation.*

We shall see another formulation of this theorem in Section 2. Following closure properties can be proved for regular languages.

**Proposition 4.2** *Regular languages are closed under union, product, the star and the plus operation, intersection, complementation, reversal, morphism, inverse morphism, regular substitution.*

A substitution $\sigma : A^* \to B^*$ is called *regular* if and only if $\sigma(a)$ is a regular language for all $a \in A$.

There are several variations for the definition of finite automata. Thus in a *nondeterministic* finite automaton, the next state function is a function from

$Q \times A$ into the subsets of $Q$. Thus $q \cdot a \subset Q$ for $q \in Q, a \in A$. This notation is extended by defining first

$$Q' \cdot a = \bigcup_{q \in Q'} q \cdot a \quad \text{for } Q' \subset Q\,. \tag{4.5}$$

Then the next state function can be defined on $Q \times A^*$ by (4.1) and (4.2), and (4.3) is easily seen to hold. The language recognized by $\mathcal{A}$ is then

$$|\mathcal{A}| = \{u \in A^* \mid q_- \cdot u \cap Q_+ \neq \emptyset\}\,.$$

Note that this definition agrees with (4.4) in the case where $\mathcal{A}$ is deterministic. Note next that (4.5) can also be considered as the definition of the next state function of a deterministic finite automaton $\mathcal{B} = \langle A, P, p_-, P_+\rangle$, where $P = \mathfrak{P}(Q)$. With $p_- = \{q_-\}$ and $P_+ = \{Q' \subset Q \mid Q' \cap Q_+ \neq \emptyset\}$, it is easily seen that $|\mathcal{B}| = |\mathcal{A}|$. Thus a language is regular if and only if it is recognized by some nondeterministic finite automaton. Nondeterministic automata are represented pictorially like deterministic automata, by drawing an edge labeled $a$ from $q$ to $q'$ whenever $q' \in q \cdot a$.

**Example 4.2** Figure I.2 represents a nondeterministic finite automaton $\mathcal{A}$, with alphabet $A = \{a, b\}$. It is easily verified that $|\mathcal{A}| = A^*aba$.

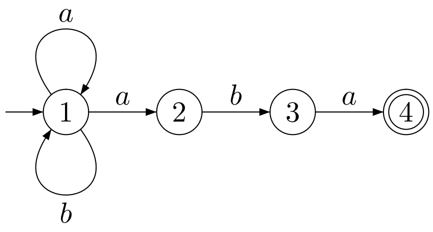

Figure I.2

Let $\mathcal{A} = \langle A, Q, q_-, Q_+\rangle$ be a finite (deterministic) automaton. A state $q$ is called *accessible* if $q_- \cdot u = q$ for at least one $u \in A^*$. $\mathcal{A}$ is accessible if all its states are accessible. If $\mathcal{A}$ is not accessible, let $P \subset Q$ be the set of accessible states of $\mathcal{A}$. Then $q_- \in P$. Define $\mathcal{B} = \langle A, P, q_-, P_+\rangle$ by $P_+ = P \cap Q_+$, and by taking as next state function the restriction to $P$ of the next state function of $\mathcal{A}$. Then $|\mathcal{B}| = |\mathcal{A}|$. $\mathcal{B}$ is called the *accessible part* of $\mathcal{A}$.

Given a finite automaton $\mathcal{A} = \langle A, Q, q_-, Q_+\rangle$ , an equivalence relation called the *Nerode equivalence*, noted $\equiv$, is defined by

$$q \equiv q' \quad \text{if and only if} \quad \text{for all } u \in A^*,\ q \cdot u \in Q_+ \iff q' \cdot u \in Q_+\,.$$

This equivalence relation is easily shown to be right regular, that is to verify $q \equiv q', w \in A^* \implies q \cdot w \equiv q' \cdot w$. Hence a next state function can be defined on the quotient set $Q/\!\equiv$ by $[q] \cdot a = [q \cdot a]$ ($[q]$ is the class of $q$ in the equivalence). Let $L = |\mathcal{A}|$, and

$$\mathcal{A}/\!\equiv\, = \langle A, Q/\!\equiv, [q_-], \{[q] \mid q \in Q_+\}\rangle$$

be the *quotient automaton* with the next state function defined above. Then it can be shown that $|\mathcal{A}/{\equiv}| = |\mathcal{A}|$, and that the accessible part of $\mathcal{A}/{\equiv}$ is the unique automaton (up to a renaming of states) recognizing $L$ having a minimal number of states among all finite automata recognizing $L$. Therefore this automaton is called the *minimal automaton* of the language $L$.

Another useful concept is the notion of semiautomaton. A *semiautomaton* $\mathcal{S} = \langle A, Q, q_- \rangle$ is defined as a finite automaton, but without specifying the set of final states. There is a language recognized by $\mathcal{S}$ for any subset $Q' \subset Q$, defined by $|\mathcal{S}(Q')| = \{u \in A^* \mid q_- \cdot u \in Q'\}$. Semiautomata are used to recognize "simultaneously" several regular languages: Consider two (more generally any finite number of) regular languages $X, Y \subset A^*$, and let $\mathcal{A} = \langle A, Q, q_-, Q_+ \rangle$, $\mathcal{B} = \langle A, P, p_-, P_+ \rangle$ be finite automata with $|\mathcal{A}| = X$, $|\mathcal{B}| = Y$. Define a semiautomaton $\mathcal{S} = \langle A, Q \times P, (q_-, p_-) \rangle$ by

$$(q, p) \cdot a = (q \cdot a, p \cdot a) \qquad a \in A, \quad (q, p) \in Q \times P\,.$$

Then $X = |\mathcal{S}(Q_+ \times P)|$ and $Y = |\mathcal{S}(Q \times P_+)|$. Usually only the accessible part of $\mathcal{S}$ is conserved in this construction.

There exist several characterizations of regular languages. The first uses local regular languages.

**Definition** A language $K \subset A^*$ is a *local regular language* if and only if there are subsets $U, V$ of $A$ and $W$ of $A^2$ such that

$$K = (UA^* \cap A^*V) \setminus A^*WA^* \text{ or } K = 1 \cup (UA^* \cap A^*V) \setminus A^*WA^*$$

Clearly such a language is regular.

The terminology is justified by the following observation: In order to check that a word $w$ is in $K$, it suffices to verify that the first letter of $w$ is in $U$, the last letter of $w$ is in $V$, and that no couple of consecutive letters of $w$ is in $W$. These verifications are all of local nature. The set $W$ is called the set of *forbidden transitions*, and $A^2 \setminus W$ is called the set of *authorized transitions*.

**Proposition 4.3** *A language $L \subset A^*$ is regular if and only if there are an alphabet $C$, a local regular language $K \subset C^*$, and a strictly alphabetic morphism $\alpha : C^* \rightarrow A^*$ such that $\alpha(K) = L$.*

*Proof.* By Proposition 4.2, $\alpha(K)$ is regular for a regular language $K$. Conversely, let $\mathcal{A} = \langle A, Q, q_-, Q_+ \rangle$ be a finite automaton such that $L = |\mathcal{A}|$. Define $C$ by

$$C = \{(q, a, q \cdot a) \mid q \in Q,\ a \in A\}$$

and define a morphism $\alpha : C^* \rightarrow A^*$ by $\alpha((q, a, q \cdot a)) = a$. Then $\alpha$ is strictly alphabetic. Next, let

$$U = \{(q, a, q \cdot a) \mid q = q_-\}\,, \quad V = \{(q, a, q \cdot a) \mid q \cdot a \in Q_+\}\,,$$
$$W = \{(q_1, a_1, q_1 \cdot a_1)(q_2, a_2, q_2 \cdot a_2) \mid q_1 \cdot a_1 \neq q_2\}$$

and set $K = (UC^* \cap C^*V) \setminus C^*WC^*$. Then for $n \geq 1$

$$c = (q_1, a_1, q_1 \cdot a_1)(q_2, a_2, q_2 \cdot a_2) \cdots (q_n, a_n, q_n \cdot a_n) \in K \qquad (4.6)$$

if and only if

$$q_1 = q_-, \quad q_{i+1} = q_i \cdot a_i \quad i = 1, \ldots, n-1, \quad q_n \cdot a_n \in Q_+ \,. \tag{4.7}$$

Consequently, $\alpha(c) = a_1 a_2 \cdots a_n \in L$. Conversely, if $u = a_1 a_2 \cdots a_n \in L$, $(n \geq 1, a_i \in A)$, then there are states $q_1, \ldots q_n$ such that (4.7) holds, and in view of (4.6), $u \in \alpha(K)$. Thus $L = \alpha(K)$ if $1 \notin L$. If $L \in L$, the same equality holds if the empty word is added to $K$. ∎

Another important characterization of regular languages is the following.

**Proposition 4.4** *A language $L \subset A^*$ is regular if and only if there exist a finite monoid $M$, a morphism $\alpha : A^* \to M$, and a subset $R \subset M$ such that $L = \alpha^{-1}(R)$.*

*Proof.* We first show that the condition is necessary. Consider a finite automaton $\mathcal{A} = \langle A, Q, q_-, Q_+ \rangle$ such that $L = |\mathcal{A}|$. For each word $w$ define a mapping $\bar{w} : Q \to Q$ which associates to $q \in Q$ the state $q \cdot w$. For convenience, we write the function symbol on the right of the argument. Thus $(q)\bar{w} = q \cdot w$. Then

$$(q)\overline{ww'} = q \cdot ww' = (q \cdot w) \cdot w' = (q\bar{w})\bar{w}' \tag{4.8}$$

$$(q)\bar{1} = q \cdot 1 = q \,. \tag{4.9}$$

Let $\alpha$ be the function from $A^*$ into the (finite!) monoid $Q^Q$ of all functions from $Q$ into $Q$ defined by $\alpha(w) = \bar{w}$. Then $\alpha$ is a morphism in view of (4.8) and (4.9). Next, define $R \subset Q^Q$ by $R = \{m \in Q^Q \mid (q_-)m \in Q_+\}$. Then $w \in L$ if and only if $q_- \cdot w \in Q_+$, thus if and only if $\alpha(w) \in R$. Consequently, $L = \alpha^{-1}(R)$.

Conversely, define a finite automaton $\mathcal{A} = \langle A, M, 1_M, R \rangle$ by setting

$$m \cdot a = m\alpha(a) \quad m \in M, \; a \in A \,.$$

Since $\alpha$ is a morphism, $m \cdot w = m\alpha(w)$ for all $w \in A^*$. Consequently $w \in |\mathcal{A}|$ if and only if $1_M\alpha(w) = \alpha(w) \in R$, thus if and only if $w \in \alpha^{-1}(R)$. ∎

There exist several versions of the Iteration Lemma or Pumping Lemma for regular languages. The most general formulation is perhaps the analogue of an Iteration Lemma for context-free languages prove by Ogden (Lemma II.2.3). Let $A$ be an alphabet, and consider a word

$$w = a_1 a_2 \cdots a_n \quad (a_i \in A) \,.$$

Then a *position* in $w$ is any integer $i \in \{1, \ldots, n\}$. Given a subset $I$ of $\{1, \ldots, n\}$, a position $i$ is called *marked* with respect to $I$ if and only if $i \in I$.

**Lemma 4.5** (Ogden's Iteration Lemma for Regular Languages) *Let $L \subset A^*$ be a regular language. Then there exists an integer $N \geq 1$ such that, for any word $w \in L$, and for any choice of at least $N$ marked positions in $w$, $w$ admits a factorization $w = xuy$, $(x, u, y \in A^*)$ such that*

(i) *$u$ contains at least one and at most $N$ marked positions;*
(ii) *$xu^*y \subset L$ .*

*Proof.* Let $\mathcal{A} = \langle A, Q, q_-, Q_+\rangle$ be a finite automaton recognizing $L$, and set $N = \mathrm{Card}(Q)$. Let $w = a_1a_2\cdots a_n$, $(a_i \in A)$ be a word in $L$, and consider a choice $I \subset \{1,\ldots,n\}$ of at least $N$ marked positions in $w$. Since $\mathrm{Card}(I) \geq N$, we have $n \geq N$. Let $1 \leq i_1 < i_2 < \cdots < i_N \leq n$ be the $N$ smallest elements of $I$, and define a factorization

$$w = z_0z_1\cdots z_Nz_{N+1}$$

by

$$z_0 = a_1\cdots a_{i_1-1}, \quad z_1 = a_{i_1}, \quad z_k = a_{i_{k-1}+1}\cdots a_{i_k} \quad (k = 2,\ldots,N),$$
$$z_{N+1} = a_{i_N+1}\cdots a_n\,.$$

Then each $z_k$ $(1 \leq k \leq N)$ contains exactly one marked position. Set

$$q_0 = q_- \cdot z_0, \quad q_k = q_{k-1}\cdot z_k \quad (k = 1,\ldots,N), \quad q_+ = q_N \cdot z_{N+1}\,.$$

By assumption $q_+ \in Q_+$. Next two among the $N+1$ states $q_0,\ldots,q_N$ are equal. Thus there exist $i, j$, with $0 \leq i < j \leq N$ such that $q_i = q_j$ Define

$$x = z_0z_1\cdots z_i, \quad u = z_{i+1}\cdots z_j, \quad y = z_{j+1}\cdots z_{N+1}\,.$$

Then $q_- \cdot x = q_- \cdot xu = q_- \cdot xu^m = q_j$ for all $m \geq 1$, whence $q_- \cdot xu^my = q_+$ for all $m \geq 0$ and $xu^*y \subset L$. Next $x$ contains exactly $j - i$ marked positions. Since $0 < j - i \leq N$, this proves the lemma. ∎

If the marked positions in $w$ are chosen to be consecutive, the same proof gives the following

**Corollary 4.6** *Let $L \subset A^*$ be a regular language. Then there exists an integer $N \geq 1$ such that for any word $w \in L$, and for any factorization $w = zvz'$ with $|v| \geq N$, $v$ admits a factorization $v = xuy$ such that*
(i) $0 < |u| \leq N$*;*
(ii) $zxu^*yz' \subset L$*.*

If $B$ is a subset of $A$, and if the marked positions are chosen to be occurrences of letters in $B$, we obtain

**Corollary 4.7** *Let $L \subset A^*$ be a regular language, and let $B \subset A$. Then there is an integer $N \geq 1$ such that for any $w \in L$, and for any factorization $w = zvz'$ with $|v|_B \geq N$, $v$ admits a factorization $v = xuy$ such that*
(i) $0 < |u|_B \leq N$*;*
(ii) $zxu^*yz' \subset L$*.*

## Exercises

**4.1** Let $K$ be a local regular language, and let $x, u, y$ be words. Show that if $xuy, xu^2y \in K$, then $xu^+y \subset K$.

**4.2** Let $K \subset A^*$ be a regular language. Show that there are two integers $N, M$ such that if $xu^ky \in K$ and $k \geq N$, then $xu^k(u^M)^*y \subset K$.

**4.3** (continuation of Exercise 3.5). Let $L \subset A^*$, and assume that $L = \alpha^{-1}(P)$ where $\alpha$ is a morphism from $A^*$ onto a monoid $M$ and $P \subset M$. Show that there is a morphism $\beta : M \to \mathrm{Synt}(L)$, and $R \subset \mathrm{Synt}(L)$, such that $P = \beta^{-1}(R)$. Show that $L$ is regular if and only if $\mathrm{Synt}(L)$ is finite. (Since $\mathrm{Synt}(L) = \mathrm{Synt}(A^* \setminus L)$, such a characterization cannot exist for context-free languages. See Perrot and Sakarovitch 1977.)

# Chapter II

# Context-Free Languages

The first section of this chapter contains the definitions of context-free or algebraic languages by means of context-free grammars and of systems of algebraic equations. In the second section, we recall without proof several constructions and closure properties of context-free languages. This section contains also the iteration lemmas for context-free languages. The third section gives a description of various families of Dyck languages. They have two definitions, as classes of certain congruences, and as languages generated by some context-free grammars. The section ends with a proof of the Chomsky-Schützenberger Theorem. Two other languages, the Lukasiewicz language and the language of completely parenthesized arithmetic expressions, are studied in the last section.

## 1 Grammars, Languages, Equations

In this section, we define context-free grammars and context-free languages. We show how a system of equations can be associated to each context-free grammar in such a way that the languages generated by the grammar are precisely the minimal solution of the system of equations. For this reason, context-free languages and more generally context-free grammars are also called algebraic grammars and algebraic languages.

**Definition** A *context-free* or *algebraic grammar* $G = \langle V, A, \mathcal{P} \rangle$ consists of an alphabet $V$ of *variables* or *nonterminals*, of an alphabet $A$, disjoint from $V$, of *terminal letters*, and of a *finite* set $\mathcal{P} \subset V \times (V \cup A)^*$ of *productions*.

A production $(\xi, \alpha) \in \mathcal{P}$ is usually written in the form

$$\xi \to \alpha\,.$$

If $\xi \to \alpha_1, \xi \to \alpha_2, \ldots, \xi \to \alpha_n$ are the productions of $G$ having the same left side $\xi$, they are grouped together by using one of the following notations

$$\xi \to \alpha_1 \mid \alpha_2 \mid \cdots \mid \alpha_n \quad \xi \to \alpha_1 + \alpha_2 + \cdots + \alpha_n \quad \xi \to \{\alpha_1, \alpha_2, \ldots, \alpha_n\}\,.$$

Clearly, the above definition is equivalent to another notation consisting of a triple $T, A, \mathcal{P}$, where $T$ is the total alphabet and $A$ is a subset of $T$. Then $V = T \setminus A$.

**Example 1.1** Let $V = \{\xi\}$, $A = \{a,b\}$, $\mathcal{P} = \{\xi \to \xi\xi, \xi \to a\}$. Then the productions can be written as $\xi \to \xi\xi + a$.

**Example 1.2** Let $V = \{\xi, \xi_a, \xi_b\}$, $A = \{a,b\}$, and let $\mathcal{P}$ be the set given by:

$$\xi \to 1 + a\xi_a b\xi + b\xi_b a\xi; \quad \xi_a \to 1 + a\xi_a b\xi_a;$$
$$\xi_b \to 1 + b\xi_b a\xi_b\,.$$

Let $G = \langle V, A, \mathcal{P}\rangle$ be a context-free grammar, and let $x, y$ be in $(V \cup A)^*$. Then we define

$$x \underset{G}{\to} y \tag{1.1}$$

if and only if there are factorizations $x = u\xi v$, $y = u\alpha v$, with $\xi \in V$, $u, \alpha, v \in (V \cup A)^*$ and $\xi \to \alpha \in \mathcal{P}$. If no confusion can arise, we write $x \to y$ instead of (1.1). For any $p \geq 0$, define

$$x \overset{p}{\underset{G}{\to}} y$$

if and only if there exist $x_0, x_1, \ldots, x_p \in (V \cup A)^*$ such that

$$x = x_0,\ y = x_p,\ \text{and } x_{i-1} \underset{G}{\to} x_i \text{ for } i = 1, \ldots, p\,.$$

(In particular $x \overset{0}{\underset{G}{\to}} x$ for any $x \in (V \cup A)^*$.) The sequence

$$(x_0, x_1, \ldots, x_n)$$

is a *derivation* from $x$ into $y$, and $p$ is the *length* of the derivation. Finally, we define

$$x \overset{*}{\underset{G}{\to}} y \quad \text{if and only if} \quad x \overset{p}{\underset{G}{\to}} y \text{ for some } p \geq 0\,;$$
$$x \overset{+}{\underset{G}{\to}} y \quad \text{if and only if} \quad x \overset{p}{\underset{G}{\to}} y \text{ for some } p > 0\,.$$

In the first case, we say that $x$ *derives* $y$ in $G$, in the second case that $x$ properly derives $y$ in $G$. If no confusion can arise, the index $G$ is dropped. For any variable $\xi \in V$, the *language generated by* $\xi$ in $G$ is

$$L_G(\xi) = \{w \in A^* \mid \xi \overset{*}{\to} w\}\,.$$

More generally, the *language generated by* $x \in (V \cup A)^*$ in $G$ is

$$L_G(x) = \{w \in A^* \mid x \overset{*}{\to} w\}\,.$$

Clearly, $L_G(x) = \{x\}$ for $x \in A^*$. The *language of sentential forms generated by* $x \in (V \cup A)^*$ in $G$ is

$$\hat{L}_G(x) = \{w \in (V \cup A)^* \mid x \overset{*}{\to} w\}\,.$$

Of course

$$L_G(x) = \hat{L}_G(x) \cap A^*\,.$$

As noted by Schützenberger (1961a), there is a close relation between the derivations in a context-free grammar and derivations in an algebra. Recall that a derivation in an algebra $M$ is a linear function $\partial$ satisfying

$$\partial(xy) = \partial(x) \cdot y + x \cdot \partial(y) \quad x, y \in M\,.$$

Given a grammar $G = \langle V, A, \mathcal{P} \rangle$, define $\partial : (V \cup A)^* \to \mathfrak{P}((V \cup A)^*)$ by

$$y \in \partial(x) \quad \text{if and only if} \quad x \underset{G}{\to} y\,.$$

and for $X \subset (V \cup A)^*$, $\partial(X) = \cup_{x \in X} \partial(x)$. Then (see Lemma 1.1 below) we have

$$\partial(XY) = \partial(X) \cdot Y \cup X \cdot \partial(Y)\,.$$

Further

$$\hat{L}_G(X) = \partial^*(X)\,,$$

where $\partial^*(X) = \cup_{n \geq 0} \partial^n(X)$. Thus $L_G(x) = \partial^*(x) \cap A^*$.

A context-free grammar $G = \langle V, A, \mathcal{P} \rangle$ *generates* a language $L \subset A^*$ if and only if $L = L_G(\xi)$ for some $\xi \in V$. Thus a grammar $G$ generates $\mathrm{Card}(V)$ languages, not necessarily distinct.

**Definition** A language $L$ is *context-free* or *algebraic* if there is some grammar $G$ that generates $L$. The set of all context-free languages of $A^*$ is denoted by $\mathrm{Alg}(A^*)$.

**Example 1.1** (*continued*) The language generated by $\xi$ is $L_G(\xi) = a^+$; further $\hat{L}_G(\xi) = \{a, \xi\}^+$.

**Example 1.2** (*continued*) The language generated by $\xi_a$ is the so-called restricted Dyck language $D_1'^*$ over $A$, with opening parenthesis $a$, and closing parenthesis $b$ (see also Section 3); $L_G(\xi_b)$ is obtained from $L_G(\xi_a)$ by exchanging $a$ and $b$. Finally, $L_G(\xi)$ is the Dyck set over $A$, consisting in all words $w$ such that $|w|_a = |w|_b$.

Let $G = \langle V, A, \mathcal{P} \rangle$ be a context free grammar. The following lemma is very useful.

**Lemma 1.1** *Let $x_1, x_2, y \in (V \cup A)^*$, and let $p \geq 0$ be an integer. Then*

$$x_1 x_2 \overset{p}{\to} y$$

*if and only if there are $y_1, y_2 \in (V \cup A)^*$, $p_1, p_2 \geq 0$ such that*

$$x_1 \overset{p_1}{\to} y_1, \quad x_2 \overset{p_2}{\to} y_2, \quad y = y_1 y_2, \quad p = p_1 + p_2\,.$$

*Proof.* If $x_1 \overset{p_1}{\to} y_1$ and $x_2 \overset{p_2}{\to} y_2$, then

$$x_1 x_2 \overset{p_1}{\to} y_1 x_2 \overset{p_2}{\to} y_1 y_2,$$

and thus $x_1 x_2 \overset{p}{\to} y$.

Assume conversely that $x_1 x_2 \overset{p}{\to} y$. If $p = 0$, there is nothing to prove. Arguing by induction on $p$, suppose $p > 0$. Then

$$x_1 x_2 \xrightarrow{p-1} z \to y$$

for some $z \in (V \cup A)^*$, and by induction there is a factorization

$$z = z_1 z_2 \quad \text{with } x_1 \overset{q_1}{\longrightarrow} z_1,\ x_2 \overset{q_2}{\longrightarrow} z_2,\ q_1 + q_2 = p - 1\,.$$

Since $z \to y$, there are $\xi \to \alpha \in \mathcal{P}$ and words $u, v$ with

$$z = u\xi v,\ y = u\alpha v\,.$$

If $|u\xi| \le |z_1|$, then $z_1 = u\xi\bar{u}$ for some word $\bar{u}$. Thus setting

$$y_1 = u\alpha\bar{u},\ y_2 = z_2\,,$$

we obtain

$$y = y_1 y_2,\ x_1 \xrightarrow{1+q_1} y_1,\ x_2 \overset{q_2}{\longrightarrow} y_2\,.$$

Otherwise, $|\xi v| \le |z_2|$, and a symmetric argument completes the proof. ■

**Corollary 1.2** *For any $x_1, x_2 \in (V \cup A)^*$, $L_G(x_1x_2) = L_G(x_1)L_G(x_2)$.*

*Proof.* By the preceding lemma, $w \in L_G(x_1x_2)$ if and only if there is a factorization $w = w_1w_2$ such that $w_1 \in L_G(x_1)$, $w_2 \in L_G(x_2)$. ■

Since $L_G(1) = \{1\}$, the mapping $x \mapsto L_G(x)$ is a *substitution* from $(V \cup A)^*$ into itself. We denote it by $L_G$. The same is true for $\hat{L}_G$ (Exercise 1.2).

**Lemma 1.3** *Let $G = \langle V, A, \mathcal{P}\rangle$ be a context-free grammar, $\xi \in V$. Then*

$$L_G(\xi) = \bigcup_{\xi \to \alpha \in \mathcal{P}} L_G(\alpha) = L_G\big(\{\alpha \mid \xi \to \alpha \in \mathcal{P}\}\big)\,.$$

*Proof.* For $\xi \to \alpha \in \mathcal{P}$, clearly $L_G(\alpha) \subset L_G(\xi)$. Conversely, let $w \in L_G(\xi)$. Since $w \in A^*$, we have $\xi \overset{+}{\longrightarrow} w$. Thus there is a production $\xi \to \alpha \in \mathcal{P}$ such that $\xi \to \alpha \overset{*}{\longrightarrow} w$. Thus $w \in L_G(\alpha)$. ■

Now we associate to each context-free grammar a system of equations. We shall see that the minimal solution of the system of equations is formed of the languages generated by the grammar. In certain special cases, the system has a unique solution. This gives a characterization of context-free languages by systems of equations.

**Definition** Let $V = \{\xi_1, \ldots, \xi_N\}$ and $A$ be two disjoint alphabets. A *system of algebraic equations* is a set

$$\xi_i = P_i \quad i = 1, \ldots, N \tag{1.2}$$

of equations, where $P_1, \ldots, P_N$ are finite subsets of $(V \cup A)^*$. The letters $\xi_i$ are called the *variables* of the system.

The terminology comes from the analogy with systems of algebraic equations over, say the field of real numbers. Such a system is given by a set of polynomial equations $Q_i(y_1, \ldots, y_N) = 0$, $(i = 1, \ldots, N)$. In the case where, in each $Q_i$, there is a monomial $y_i$, the system can be written in the form $y_i = Q'_i(y_1, \ldots, y_N)$, with each $Q'_i$ a polynomial. In the same manner, the sets $P_i$ of (1.2) can be considered as "polynomials" by writing

$$P_i = \sum_{\alpha \in P_i} \alpha$$

with coefficients in the Boolean semiring. The theory of systems of algebraic equations over arbitrary semirings allows in particular to take into account the ambiguity of a grammar. This is beyond the scope of the book. See Salomaa and Soittola (1978), Eilenberg (1978).

The correspondence between systems of algebraic equations and context-free grammars is established as follows. Given a context-free grammar $G = \langle V, A, \mathcal{P} \rangle$, number the nonterminals such that $V = \{\xi_1, \ldots, \xi_N\}$ with $N = \mathrm{Card}(V)$ and define

$$P_i = \{\alpha \mid \xi_i \in \mathcal{P}\} \quad i = 1, \ldots, N\,.$$

Then (1.2) is the system of equations *associated* to $G$.

Conversely, the context-free grammar associated to (1.2) has as set of productions

$$\mathcal{P} = \{\xi_i \to \alpha \mid \alpha \in P_i, 1 \le i \le N\}\,.$$

We now define a solution of (1.2) as a vector $X = (X_1, \ldots, X_N)$ of languages such that the substitution in $P_i$ of the languages $X_j$ to each occurrence of $\xi_j$ yields precisely the language $X_i$.

Formally, given (1.2), let $X = (X_1, \ldots, X_N)$ with $X_i \subset (V \cup A)^*$ for $i = 1, \ldots, N$. Define a substitution $\underline{X}$ from $(V \cup A)^*$ into itself by

$$\underline{X}(a) = \{a\} \quad a \in A\,;$$
$$\underline{X}(\xi_i) = X_i \quad i = 1, \ldots, N\,.$$

**Definition** A vector $X = (X_1, \ldots, X_N)$ is a *solution* of the system of equations (1.2) if and only if

$$\underline{X}(P_i) = X_i \quad i = 1, \ldots, N\,. \tag{1.3}$$

**Example 1.1** (*continued*) The equation $\xi = \xi\xi + a$ has the solution $a^+$ since $a^+ = a^+a^+ \cup a$ and also the solutions $A^*$ and $(V \cup A)^*$, since $A^* = A^*A^* \cup a$ and similarly for the second set.

**Example 1.2** (*continued*) As will be shown below, the vector $(L_G(\xi), L_G(\xi_a), L_G(\xi_b))$ is the unique solution of the system

$$\xi = 1 + a\xi_a b\xi + b\xi_b a\xi\,, \quad \xi_a = 1 + a\xi_a b\xi_a\,, \quad \xi_b = 1 + b\xi_b a\xi_b\,.$$

A system of equations (1.2) may have several, and even an infinity of solutions. We order the solutions by setting, for $X = (X_1, \ldots, X_N)$, $Y = (Y_1, \ldots, Y_N)$, $X \subset Y$ if and only if $X_i \subset Y_i$ for $i = 1, \ldots, N$.

**Theorem 1.4** *Let $G$ be a context-free grammar, and let* (1.2) *be the system of algebraic equations associated to $G$. The vector $L_G = (L_G(\xi_1), \ldots, L_G(\xi_N))$ is the minimal solution of* (1.2).

The result contains a converse statement: given a system of algebraic equations, the components of the minimal solution are context-free languages. For this reason, context-free languages are called algebraic languages. Note that only the components of the minimal solution are claimed to be context-free. There are solutions of systems which are not context-free (Exercise 1.4).

*Proof.* By definition, we have $\underline{L_G}(x) = L_G(x)$ for all $x \in (V \cup A)^*$. We shall verify that the substitution $L_G$ satisfies (1.3). Indeed, in view of Lemma 1.3,

$$L_G(P_i) = \bigcup_{\alpha \in P_i} L_G(\alpha) = L_G(\xi_i) \quad i = 1, \ldots N\,.$$

This shows that $L_G = (L_G(\xi_1), \ldots, L_G(\xi_N))$ is a solution of (1.2). Next, let $X = (X_1, \ldots, X_N)$ be another solution of (1.2). We show that

$$L_G(x) \subset \underline{X}(x) \quad x \in (V \cup A)^* \tag{1.4}$$

by induction on the length of the derivation of the words of $L_G(x)$. Let $w \in L_G(x)$. If $x \xrightarrow{0} w$, then $x = w \in A^*$ and $w \in \underline{X}(x)$. Assume now $x \xrightarrow{p} w$ and $p > 0$. There exist a word $y$ such that

$$x \longrightarrow y \xrightarrow{p-1} w\,,$$

and factorizations $x = u\xi_i v$, $y = u\alpha v$ such that $\xi_i \to \alpha \in \mathcal{P}$. Since $w \in \underline{X}(y)$ by induction, it follows that

$$w \in \underline{X}(g) = \underline{X}(u)\underline{X}(\alpha)\underline{X}(v) \subset \underline{X}(u)\underline{X}(P_i)\underline{X}(v)\,.$$

Since $\underline{X}(P_i) = X_i = \underline{X}(\xi_i)$, we have

$$\underline{X}(u)\underline{X}(P_i)\underline{X}(v) = \underline{X}(u\xi_i v) = \underline{X}(x)\,.$$

Thus $w \in \underline{X}(x)$. From (1.4), we obtain

$$L_G(\xi_i) \subset \underline{X}(\xi_i) = X_i \quad i = 1, \ldots, N\,.$$ ■

We now show that in some cases a system of algebraic equations has a unique solution.

**Definition** An algebraic grammar $G = \langle V, A, \mathcal{P}\rangle$ is *strict* if and only if for each production $\xi \to \alpha \in \mathcal{P}$, either $\alpha = 1$ or $\alpha$ contains at least one terminal letter, thus if and only if

$$\alpha \in 1 \cup (V \cup A)^* A (V \cup A)^*\,.$$

A system of equations is strict if the associated grammar is strict.

By Greibach's Normal Form Theorem, a strict grammar can be supplied for any context-free language (see the books listed in the bibliography).

**Theorem 1.5** *Let $G = \langle V, A, \mathcal{P}\rangle$ be a context-free grammar. If $G$ is strict, then $L_G = (L_G(\xi_1), \dots, L_G(\xi_N))$ is the unique solution of the system of equations associated to $G$.*

*Proof.* Let (1.2) be the system of equations associated with $G$, and let $X = (X_1, \dots, X_N)$, $Y = (Y_1, \dots, Y_N)$ be two solutions of this system. We prove:

$$\text{for } i = 1, \dots, N,\ w \in X_i,\ |w| \le n \text{ implies } w \in Y_i \tag{1.5}$$

by induction on $n$. This shows that $X \subset Y$, and $X = Y$ by symmetry.

If $1 \in X_i = \underline{X}(P_i)$, then $1 \in \underline{X}(\alpha)$ for some $\alpha \in P_i$ and since $G$ is strict, this implies $\alpha = 1$. Thus $1 \in P_i$ and $1 \in \underline{Y}(P_i) = Y_i$. Assume $w \in X_i$ and $|w| = n > 0$. As before, $w \in \underline{X}(\alpha)$ for some $\alpha \in P_i$. If $\alpha \in A^*$, then $\alpha = w \in P_i$ and $w \in Y_i$. Thus suppose the contrary. Then

$$\alpha = u_0 \xi_{i_1} u_1 \cdots u_{r-1} \xi_{i_r} u_r$$

with $r \ge 1$, $u_0, \dots, u_r \in A^*$, $\xi_{i_1}, \dots, \xi_{i_r} \in V$. Therefore

$$w = u_0 v_1 u_1 \cdots u_{r-1} v_r u_r$$

with $v_k \in \underline{X}(\xi_{i_k}) = X_{i_k}$ for $k = 1, \dots, r$. Now $u_0 u_1 \cdots u_r \ne 1$ since $G$ is strict. Since $r \ge 1$, $|v_k| < n$ for all $k = 1, \dots, r$ and by the induction hypothesis, $v_k \in Y_{i_k} = \underline{Y}(\xi_{i_k})$ for $k = 1, \dots, r$. Thus

$$w \in u_0 \underline{Y}(\xi_{i_1}) u_1 \cdots u_{r-1} \underline{Y}(\xi_{i_r}) u_r = \underline{Y}(\alpha) \subset Y_i\,. \qquad \blacksquare$$

Note that the finiteness of the sets $P_i$ was used in the proofs of neither Theorem 1.4 nor 1.5. Thus these remain true if the sets $P_i$ are infinite, provided grammars with infinite sets of productions are allowed or alternatively, if the connections with grammars are dropped in the statements. Thus especially Theorem 1.5 can be used to prove uniqueness of the solution of equations (Exercise 1.5).

We conclude this section with a result that permits transformations of systems of equations without changing the set of solutions. This is used later to show that systems of equations which are not strict have a unique solution by transforming them into strict systems.

**Definition** Two systems of equations

$$\xi_i = P_i \ \ (1 \le i \le N) \quad \text{and} \quad \xi_i = Q_i \ \ (1 \le i \le N)$$

with the same set of variables are *equivalent* if they have the same set of solutions.

**Proposition 1.6** (Substitution Lemma) *Let*

$$\xi_i = P_i \quad i = 1, \dots, N \tag{1.6}$$

*be a system of equations. Assume that $\alpha = u\xi_j v \in P_k$ for some $j, k \in \{1, \dots, N\}$ and some words $u, v$. Define $Q_i = P_i$ for $i \ne k$ and $Q_k = (P_k \setminus \alpha) \cup uP_j v$. Then* (1.6) *is equivalent to*

$$\xi_i = Q_i \quad i = 1, \dots, N\,. \tag{1.7}$$

**Example 1.1** (*continued*) Starting with $\xi = P$ where $P = a + \xi\xi$, we single out $\alpha = \xi\xi$ and form $Q = P \setminus \alpha \cup \xi P = a + \xi\xi\xi + \xi a$ The substitution lemma claims that the equation $\xi = a + \xi\xi\xi + \xi a$ is equivalent to the initial one.

**Example 1.3** Let $A = \{a, b\}$, and consider the system

$$\xi = 1 + \eta\xi\,; \quad \eta = a\xi b\,.$$

Taking $\alpha = \eta\xi$, and replacing $\eta$ by $a\xi b$, yields the strict system

$$\xi = 1 + a\xi b\xi\,; \quad \eta = a\xi b\,.$$

By the substitution lemma, the first system has a unique solution.

For the proof of Proposition 1.6, we need a technical lemma.

**Lemma 1.7** *Let $B$ be an alphabet, and let $X, Y, Z, L$ and $M$ be subsets of $B^*$. If*

$$L = X \cup YMZ \quad \textit{and} \quad M = X \cup YLZ$$

*then $L = M$.*

*Proof* If $Y = \emptyset$ or $Z = \emptyset$, then $L = M = X$. Next, if $1 \in Y$ and $1 \in Z$, then by the first equation $M \subset YMZ \subset L$, and similarly $L \subset M$, hence $L = M$. Thus we may assume that $1 \notin YZ$. Then $1 \in L$ if and only if $1 \in X$, hence if and only if $1 \in M$. Arguing by induction on the length of words, consider $w \in B^*$, $|w| = p > 0$, and assume $w \notin X$. Then $W \in L$ if and only if $w \in YMZ$, hence if and only if $w = yw'z$ with $y \in Y$, $z \in Z$, $w' \in M$ and $|w'| < p$. Thus $w' \in L$ and $w \in YLZ \subset M$. Similarly $w \in M$ implies $w \in L$. This proves the lemma. ■

*Proof* of Proposition 1.6. Let $X = (X_1, \ldots, X_N)$ be a solution of (1.6). By definition, $\underline{X}(P_i) = X_i$ for $i = 1, \ldots, N$. Thus

$$\underline{X}(Q_i) = X_i \quad i = 1, \ldots, N,\ i \neq k\,,$$
$$\underline{X}(Q_k) = \underline{X}(P_k \setminus \alpha) \cup \underline{X}(u)\underline{X}(P_j)\underline{X}(v) = \underline{X}(P_k \setminus \alpha) \cup \underline{X}(\alpha) = X_k\,,$$

showing that $X$ is a solution of (1.7).

Conversely, let $Y = (Y_1, \ldots, Y_N)$ be a solution of (1.7). Then

$$\begin{aligned} \underline{Y}(P_i) &= Y_i \quad i = 1, \ldots, N,\ i \neq k\,, \\ \underline{Y}(P_k) &= \underline{Y}(P_k \setminus \alpha) \cup \underline{Y}(\alpha) = \underline{Y}(P_k \setminus \alpha) \cup \underline{Y}(u)\underline{Y}(\xi_j)\underline{Y}(v) \\ &= \underline{Y}(P_k \setminus \alpha) \cup Y(u)\underline{Y}(Q_j)\underline{Y}(v) \end{aligned} \tag{1.8}$$

If $j \neq k$, then $Q_j = P_j$. Thus

$$\underline{Y}(P_k) = \underline{Y}(P_k \setminus \alpha \cup uP_jv) = \underline{Y}(Q_j) = Y_k$$

and $Y$ is a solution of (1.6). If $j = k$, then by (1.8)

$$\underline{Y}(P_k) = \underline{Y}(P_k \setminus \alpha) \cup \underline{Y}(u)\underline{Y}(Q_k)\underline{Y}(v)\,;$$
$$\underline{Y}(Q_k) = \underline{Y}(P_k \setminus \alpha) \cup \underline{Y}(u)\underline{Y}(P_k)\underline{Y}(v)$$

by definition. In view of Lemma 1.7, we have

$$\underline{Y}(P_k) = \underline{Y}(Q_k) = Y_k\,;$$

thus $Y$ is a solution of (1.6). ■

## Exercises

**1.1** A context-free grammar $G = \langle V, A, \mathcal{P} \rangle$ is called *proper* if each production $\xi \to \alpha \in \mathcal{P}$ verifies $\alpha \notin 1 \cup V$. A vector $X = (X_1, \ldots, X_N)$ of languages is called proper if $1 \notin X_i$ for $i = 1, \ldots, N$. Prove that the system of equations associated to a proper grammar has a unique proper solution.

**1.2** Show that Corollary 1.2 remains true if $L_G$ is replaced by $\hat{L}_G$, and that Lemma 1.3 becomes false.

**1.3** Show that the languages of sentential forms of a context-free grammar are context-free.

**1.4** Show that there are non context-free languages among the solutions of the equation of Example 1.1.

**1.5** Use Theorem 1.5 to show that the equation $\xi = X \cup \xi Y$ has the unique solution $XY^*$ provided $1 \notin Y$.

# 2 Closure Properties, Iteration

We recall here some closure properties of the family of context-free languages, and also some iteration lemmas for these languages. We give no proof: we just recall some constructions that will be used later. Proofs of the results stated here can be found in standard books on formal languages (see Bibliography).

**Theorem 2.1** *Context-free languages are closed under union, product, star operation, reversal, morphism, inverse morphism, intersection with regular sets, context-free substitution.*

A *context-free substitution* is a substitution $\theta : A^* \to B^*$ such that $\theta(a)$ is a context-free language for each $a \in A$.

We now recall the usual constructions employed to prove closure under morphism, inverse morphism, intersection with regular sets and substitution. Let $L \subset A^*$ be an algebraic language, let $G = \langle V, A, \mathcal{P} \rangle$ be an algebraic grammar and let $\sigma \in V$ be such that $L = L_G(\sigma)$.

**a) Morphism** Let $\psi : A^* \to B^*$ be a morphism. Extend $\psi$ to a morphism from $(V \cup A)^*$ into $(V \cup B)^*$ by setting $\psi(\xi) = \xi$ for $\xi \in V$. Define a grammar

$$\psi G = \langle V, B, \psi \mathcal{P} \rangle$$

by

$$\psi \mathcal{P} = \{\xi \to \psi(\alpha) \mid \xi \to \alpha \in \mathcal{P}\}.$$

Then is is readily shown that

$$\psi L_G(\xi) = L_{\psi G}(\xi) \quad \xi \in V.$$

Thus $\psi L = L_{\psi G}(\sigma)$ is a context-free language.

**b) Inverse alphabetic morphism** Let $\phi : B^* \to A^*$ be an alphabetic morphism. As above, extend $\phi$ to $(V \cup B)^*$ by setting $\phi(\xi) = \xi$ for $\xi \in V$. Define $C = \{b \in B \mid \phi(b) = 1\}$ and $T = B \setminus C$. Finally, let $\omega$ be a new letter $(\omega \notin V \cup A \cup B)$. Define a grammar

$$\phi^{-1}G = \langle \omega \cup V, B, \mathcal{P}' \rangle$$

where

$$\mathcal{P}' = \mathcal{P}'' \cup \Big\{\omega \to 1 + \sum_{c \in C} \omega c\Big\}$$

and where $\mathcal{P}''$ is defined as follows: For $\xi \in V$, $k \geq 0$, $b_1, b_2, \ldots, b_k \in V \cup T$

$$\xi \to \omega b_1 \omega b_2 \omega \cdots \omega b_k \omega \in \mathcal{P}'' \iff \xi \to \phi(b_1 b_2 \cdots b_k) \in \mathcal{P} .$$

Since the restriction of $\phi$ to $(V \cup T)^*$ is strictly alphabetic, $\mathcal{P}''$ is finite. Next, it is easy to prove that

$$\phi^{-1} L_G(\xi) = L_{\phi^{-1}(G)}(\xi) \quad \xi \in V ,$$

and $L_{\phi^{-1}(G)}(\omega) = C^*$. Thus $\phi^{-1}(L)$ is a context-free language. Any inverse morphism can be factorized into an inverse alphabetic morphism, followed by the intersection with a regular language, followed by a morphism. Thus closure under arbitrary inverse morphism can be deduced from above and from the following construction.

**c) Intersection with a regular language** Let $K \subset A^*$ be a regular language, and $\mathcal{A} = \langle A, Q, q_-, Q_+ \rangle$ be a finite automaton such that $K = |\mathcal{A}|$. Let $\hat{\sigma}$ be a new symbol, and define a grammar

$$G_K = \langle \hat{\sigma} \cup (Q \times V \times Q), A, \mathcal{P}_K \rangle$$

where $\mathcal{P}_K = \mathcal{P}' \cup \mathcal{P}''$, with

$$\mathcal{P}'' = \{\hat{\sigma} \to (q_-, \sigma, q_+) \mid q_+ \in Q_+\} ,$$

and $\mathcal{P}''$ composed of the following productions: For $k \geq 0$, $\xi, \eta_1, \ldots, \eta_k \in V$, $u_0, \ldots, u_k \in A^*$, $q, q', q_1, \ldots, q_k, q'_1, \ldots, q'_k \in Q$

$$(q, \xi, q') \to u_0 (q_1, \eta_1, q'_1) u_1 (q_2, \eta_2, q'_2) \cdots (q_k, \eta_k, q'_k) u_k \in \mathcal{P}'$$

if and only if

$$\xi \to u_0 \eta_1 u_1 \eta_2 \cdots \eta_k u_k \in \mathcal{P} \text{ and}$$
$$q \cdot u_0 = q_1,\ q'_i \cdot u_i = q_{i+1}\ (i = 1, \ldots, k-1),\ q'_k \cdot u_k = q' .$$

It is not difficult to show that

$$L_{G_K}(q, \xi, q') = L_G(\xi) \cap K_{q,q'} \quad (q, q' \in Q, \xi \in V)$$

where

$$K_{q,q'} = \{x \in A^* \mid q \cdot x = q'\} .$$

Thus $L \cap K = L_{G_K}(\hat{\sigma})$.

**d) Context-free substitution** Let $\theta : A^* \to B^*$ be a context-free substitution. For each $a \in A$, let

$$G_a = \langle V_a, B, \mathcal{P}_a \rangle$$

be a context-free grammar such that $\theta(a) = L_{G_a}(\sigma_a)$ for some $\sigma_a \in V_a$. Clearly the alphabets $V_a$ may be assumed pairwise disjoint and disjoint from $V$. Define a copy morphism $\gamma : (V \cup A)^* \to (V \cup \{\sigma_a : a \in A\})^*$ by $\gamma(\xi) = \xi$ for $\xi \in V$, $\gamma(a) = \sigma_a$ for $a \in A$, and let $\gamma G = \langle V, \{\sigma_a : a \in A\}, \gamma\mathcal{P} \rangle$ be defined as in a). Let

$$H = \langle W, B, \mathcal{Q} \rangle$$

be the grammar with $W = V \cup \bigcup_{a \in A} V_a$, $\mathcal{Q} = \gamma P \cup \bigcup_{a \in A} \mathcal{P}_a$. Then it can be shown that

$$L_H(\xi) = \theta(L_G(\xi)) \quad \xi \in V\,.$$

Consequently $\theta(L) = L_H(\sigma)$.

The iteration lemmas for context-free languages are not as accurate as the corresponding lemmas for regular sets. It can be shown (Exercise 2.1) that a strict analog of the iteration lemmas for regular languages does not exist. The most frequently used iteration lemma is due to Bar-Hillel, Perles and Shamir.

**Lemma 2.2** (Iteration Lemma for Algebraic Languages) *Let $L \subset A^*$ be an algebraic language. There exists an integer $N \geq 1$ such that any word $w \in L$ with $|w| \geq N$ admits a factorization $w = xuyvz$ $(x, u, y, v, z \in A^*)$ satisfying*

(i) $xu^nyv^nz \in L$ *for all* $n \geq 0$ *;*

(ii) $0 < |uv| \leq N$ .

There is some difficulty in the use of this lemma arising from the fact that the position of the segments $u$ and $v$ in $W$ cannot be predicted. The following refinement of the above lemma states that at least the position of one of the two segments can be located with some precision. The notion of marked position is the same as in Section 4.

**Lemma 2.3** (Ogden's Iteration Lemma for Algebraic Languages) *Let $L \subset A^*$ be an algebraic language. There exists an integer $N \geq 1$ such that any word $w \in L$, and for any choice of at least $N$ marked positions in $w$, $w$ admits a factorization $w = xuyvz$ $(x, u, y, v, z \in A^*)$ satisfying*

(i) $xu^nyv^nz \in L$ *for all* $n \geq 0$ *;*

(ii) *(each of $x$ and $u$ and $y$) or (each of $y$ and $v$ and $z$) contains at least one marked position ;*

(iii) *$uv$ contains at most $N$ marked positions .*

If all positions in $w$ are marked, we obtain Lemma 2.2. Assume that $N$ consecutive positions are marked, hence that a segment $s$ of $w$ has been distinguished. Then (ii) implies that either $u$ or $v$ is a segment of $s$. Thus we have

**Corollary 2.4** *Let $L \subset A^*$ be an algebraic language. There exists an integer $N$ such that any word $w \in L$ and for any factorization $w = tst'$ $(t, s, t' \in A^*)$ with $|s| \geq N$, $w$ admits a factorization $w = xuyvz$ $(x, u, y, v, z \in A^*)$ satisfying*

(i) $xu^nyv^nz \in L$ *for all* $n \geq 0$ *;*
(ii) *either* $u$ *is a segment of* $s$ *and* $|u| > 0$ *or* $v$ *is a segment of* $s$ *and* $|v| > 0$ *.*

We do not prove these lemmas (see (Ogden 1968, Aho and Ullman 1972, Autebert and Cousineau 1976)). The proof is on derivation trees and the lemmas are in fact results on derivations in algebraic grammars. We give this version of the lemma for later use.

**Lemma 2.5** (Ogden's Iteration Lemma for Algebraic Grammars) *Let* $G = \langle V, A, \mathcal{P}\rangle$ *be an algebraic grammar. There exists an integer* $N$ *such that, for any derivation* $\xi \xrightarrow{*} w$ *with* $\xi \in V$*,* $w \in (V \cup A)^*$*, and for any choice of* $N$ *marked positions in* $w$*, there is a factorization* $w = xuyvz$ *(*$x, u, y, v, z \in A^*$*) and* $\eta \in V$ *such that*
(i) $\xi \xrightarrow{*} x\eta z$, $\eta \xrightarrow{*} u\eta v$, $\eta \xrightarrow{*} y$ *;*
(ii) *(*$x$ *and* $u$ *and* $y$*) or (*$y$ *and* $v$ *and* $z$*) contain at least one marked position;*
(iii) $uv$ *contains at most* $N$ *marked positions.*

Note that the integer $N$ is independent of the nonterminal $\xi$. Note also that the lemma is true for sentential forms as well as for words in $A^*$.

A context-free grammar $G = \langle V, A, \mathcal{P}\rangle$ can be "reduced" in several ways. Let $\sigma \in V$. Then $G$ is:

*reduced* in $\sigma$ if for each $\xi \in V$, $L_G(\xi) \neq \emptyset$ and $\sigma \xrightarrow{*} u\xi v$ for some words $u, v \in A^*$,

*strictly reduced* in $\sigma$ if $G$ is reduced in $\sigma$ and if further $L_G(\xi)$ is infinite for each $\xi \in V$.

**Lemma 2.6** *Let* $L \subset A^*$ *be a context-free language. If* $L$ *is nonempty, then* $L = L_G(\sigma)$ *for some context-free grammar* $G = \langle V, A, \mathcal{P}\rangle$ *which is reduced in* $\sigma$*. If* $L$ *is infinite, then* $G$ *can be assumed to be strictly reduced in* $\sigma$*.*

We only give the construction. Let $L = L_G(\sigma)$ for some context-free grammar $G = \langle V, A, \mathcal{P}\rangle$, and let $V'$ be the set of $\xi \in V$ such that $L_G(\xi) \neq \emptyset$ and $\sigma \xrightarrow{*} u\xi v$ for some $u, v \in A^*$. If $L \neq \emptyset$, then $\sigma \in V'$. Let $G' = \langle V', A, \mathcal{P}'\rangle$, where $\mathcal{P}' = \{\xi \to \alpha \in \mathcal{P} \mid \xi \in V', \alpha \in (V' \cup A)^*\}$. Then $G'$ is reduced in $\sigma$, and $L_G(\xi) = L_{G'}(\xi)$ for each $\xi \in V'$.

Next, let $V'' = \{\xi \in V' \mid L_{G'}(\xi) \text{ is infinite}\}$, and define a grammar $G'' = \langle V'', A, \mathcal{P}''\rangle$ as follows. Let $\theta : (V' \cup A)^* \to (V'' \cup A)^*$ be the substitution given by

$$\theta(a) = a \ (a \in A), \quad \theta(\xi) = \xi \ (\xi \in V''), \quad \theta(\xi) = L_{G'}(\xi) \ (\xi \in V' \setminus V''),$$

and set

$$\mathcal{P}'' = \{\xi \to \beta \mid \xi \to \alpha \in \mathcal{P}', \beta \in \theta(\alpha)\}.$$

If $L$ is infinite, then $\sigma \in V''$, $G''$ is strictly reduced in $\sigma$, and $L_{G''}(\xi) = L_{G'}(\xi)$ for each $\xi \in V''$.

## Exercise

**2.1** Show that Corollary 2.4 cannot be strengthened to assert the existence, for each factorization $w = tst's't''$ of $w \in L$ of a factorization $w = xuyvz$ satisfying (i) and such that both $u$ is a segment of $s$ and $v$ is a segment of $s'$.

# 3 Dyck Languages

The Dyck sets are among the most frequently cited context-free languages. In view of the Chomsky-Schützenberger Theorem proved below, they are also the most "typical" context-free languages. In Chapter VII, we shall see another formulation of this fact: The Dyck languages are, up to four exceptions, generators of the cone of context-free languages.

A Dyck language consists of "well-formed" words over a finite number of pairs of parentheses. There are two (and in fact even four) families of Dyck languages defined by different constraints on the use of parentheses. The *restricted Dyck languages* $D_n'^*$, $(n \geq 1)$ are formed of the words over $n$ pairs of parentheses which are "correct" in the usual sense. Thus

$$(\,[\,(\,)\,(\,)\,]\,\{\,\}\,[\,]\,)\,(\,)$$

is a word of $D_3'^*$. For the *Dyck languages* $D_n^*$, the interpretation of the parentheses is different. Two parentheses of the same type are rather considered as formal inverses for each other. A word is considered as "correct" if and only if successive deletion of factors of associated parentheses (say of the form $a\bar{a}$ and $\bar{a}a$) yields the empty word. Thus

$$\bar{a}a\bar{a}a\bar{b}b\bar{a}a$$

is a word of $D_2^*$. This interpretation is used for the construction of free groups. Finally, $D_n$ and $D_n'$ are the sets of *Dyck-primes* and *restricted Dyck-primes*, that is the words of $D_n^*$ (resp. $D_n'^*$) which are not product of two nonempty words of $D_n^*$ (resp. $D_n'^*$).

The appropriate framework to formalize the definitions of $D_n'^*$ and $D_n^*$ are congruences. We first give this definition, and prove then that the four families consist of context-free languages. The section ends with a proof of the Chomsky-Schützenberger Theorem.

Let $n \geq 1$ be an integer, and let $A_n = \{a_1, \ldots, a_n\}$, $\bar{A}_n = \{\bar{a}_1, \ldots, \bar{a}_n\}$ be two alphabets of $n$ letters. Each couple $a_k, \bar{a}_k$ can be considered as a pair of parentheses of the same type. Define $C_n = A_n \cup \bar{A}_n$. We introduce the following useful notation. For $c \in C_n$, let

$$\bar{c} = \begin{cases} \bar{a}_k & \text{if } c = a_k\,; \\ a_k & \text{if } c = \bar{a}_k\,. \end{cases}$$

Thus $\bar{\bar{c}} = c$.

**Definition** The *restricted Dyck congruence* $\delta_n'$ is the congruence of $C_n^*$ generated by

$$a_k\bar{a}_k \sim 1 \quad k = 1, \ldots, n\,. \tag{3.1}$$

The Dyck congruence $\delta_n$ is the congruence generated by (3.1) and by

$$\bar{a}_k a_k \sim 1 \quad k = 1, \ldots, n\,. \tag{3.2}$$

Thus two words $w$ and $w'$ are congruent modulo $\delta'_n$ or modulo $\delta_n$, and we write

$$w \equiv w' \pmod{\delta'_n} \qquad \text{or} \qquad w \equiv w' \pmod{\delta_n}$$

if and only if $w'$ can be obtained from $w$ by a finite number of insertions or deletions of factors of the form $a_k\bar{a}_k$ (resp. $a_k\bar{a}_k$ or $\bar{a}_k a_k$).

**Definition** The *restricted Dyck language* $D'^*_n$ is the class of 1 in the congruence $\delta'_n$: $D'^*_n = [1]_{\delta'_n}$. The *Dyck language* $D^*_n$ is the class of 1 in the congruence $\delta_n$: $D^*_n = [1]_{\delta_n}$.

Clearly by definition both $D'^*_n$ and $D^*_n$ are submonoids of $C^*_n$.

**Definition** The set $D'_n$ of *restricted Dyck primes* is

$$D'_n = (D'^*_n \setminus 1) \setminus (D'^*_n \setminus 1)^2 .$$

The set of *Dyck primes* is $D_n = (D^*_n \setminus 1) \setminus (D^*_n \setminus 1)^2$.

The notation is consistent since $D'_n$ and $D_n$ indeed generate the submonoids $D'^*_n$ and $D^*_n$ (see Section I.2). In fact, we shall see that $D'_n$ and $D_n$ are bifix codes, thus $D'^*_n$ and $D^*_n$ are free submonoids of $C^*_n$. In order to give a unified treatment, we follow an idea of M.-P. Schützenberger and introduce a more general family of congruences and languages. It will appear that the restricted and the general Dyck languages are just extremal cases in the new formalism.

**Definition** Let $I$ be a subset of $\{1, \ldots, n\}$. The congruence $\delta_I$ is the congruence generated by

$$a_k\bar{a}_k \sim 1 \ (k = 1, \ldots, n) \quad \text{and} \quad \bar{a}_i a_i \sim 1 \ (i \in I) .$$

The language $D^*_I$ is the class of the empty word in the congruence $\delta_I$.

Clearly $D^*_I$ is a submonoid of $C^*_n$, justifying thus the notation. Anyone of the $2^n$ subsets of $\{1, \ldots, n\}$ defines a "Dyck-like" language. If $I = \emptyset$, then $\delta_I = \delta'_n$ and $D^*_I = D'^*_n$; if $I = \{1, \ldots, n\}$, then $\delta_I = \delta_n$ and $D^*_I = D^*_n$.

Our aim is to prove that $D^*_I$ and $D_I = (D^*_I \setminus 1) \setminus (D^*_I \setminus 1)^2$ are context-free languages for any $I \subset \{1, \ldots, n\}$. For this, we first introduce a new relation. Let $u, v \in C^*_n$, and set $u \underset{I}{\longmapsto} v$ if and only if there are $x, y \in C^*_n$ such that $u = x\alpha y$, $v = xy$, and either $\alpha = a_k\bar{a}_k$ for some $k \in \{1, \ldots, n\}$ or $\alpha = \bar{a}_i a_i$ for some $i \in I$. The reflexive and transitive closure $\overset{*}{\underset{I}{\longmapsto}}$ of $\underset{I}{\longmapsto}$ is called the *Dyck reduction*. Clearly, if $u \overset{*}{\underset{I}{\longmapsto}} v$, then $|u| \geq |v|$, and $|u| = |v|$ implies $u = v$. The congruence $\delta_I$ and the reduction $\overset{*}{\underset{I}{\longmapsto}}$ are linked by

$$u \equiv v \pmod{\delta_I}$$

if and only if there are $k \geq 0$, $u_0, \ldots, u_k \in C^*_n$ such that

$$u_0 = u, \ u_k = v,$$

and

$$(u_p \underset{I}{\longmapsto} u_{p+1} \text{ or } u_{p+1} \underset{I}{\longmapsto} u_p) \ p = 0, \ldots, k-1 .$$

Thus $u \underset{I}{\overset{*}{\longmapsto}} v$ implies $u \equiv v \pmod{\delta_I}$, but the converse is false.

A word is *reduced* mod $\delta_I$ if and only if it contains no factor of the form $a_k\bar{a}_k$ or $\bar{a}_i a_i$ $(i \in I)$. Thus $u$ is reduced if and only if $\{v \mid u \underset{I}{\longmapsto} v\} = \emptyset$. For any word $w \in C_n^*$ there is at least one reduced word $u$ congruent to $w$ (mod $\delta_I$). Usually, there are several ways to compute a reduced word. We shall prove that all computations lead to the same reduced word which is unique. We follow Autebert and Cousineau (1976) rather than the standard exposition as treated in Magnus et al. (1966). Indeed, the presentation below is closer to the extensions to more general congruences over free monoids as considered by Cochet and Nivat (1971), Benois and Nivat (1972).

**Example 3.1** For $n = 2$, $I = \{1, 2\}$, consider the word $\bar{a}a\bar{a}a\bar{b}b\bar{a}a$. It can be reduced to the empty word in at least the two following manners:

$$\begin{aligned}
w &= \underline{\bar{a}a}\bar{a}a\bar{b}b\bar{a}a & \qquad w &= \bar{a}\underline{a\bar{a}}a\bar{b}b\bar{a}a \\
w_1 &= \underline{\bar{a}a}\bar{b}b\bar{a}a & w_1' &= \bar{a}a\underline{\bar{b}b}\bar{a}a \\
w_2 &= \underline{\bar{b}b}\bar{a}a & w_2' &= \bar{a}\underline{a\bar{a}}a \\
w_3 &= \underline{\bar{a}a} & w_3' &= \underline{\bar{a}a} \\
w_4 &= 1 & w_4' &= 1
\end{aligned}$$

From now on, we write $\longmapsto$ and $\overset{*}{\longmapsto}$ instead of $\underset{I}{\longmapsto}$ and $\underset{I}{\overset{*}{\longmapsto}}$.

**Lemma 3.1** (Confluence Lemma) *If $w \overset{*}{\longmapsto} u_1$ and $w \overset{*}{\longmapsto} u_2$, then there exists a word $v$ such that $u_1 \overset{*}{\longmapsto} v$ and $u_2 \overset{*}{\longmapsto} v$.*

Thus the lemma asserts the existence of a word $v$ such that the following diagram holds (Figure II.1). We first prove the lemma in a special case.

$$\begin{tikzcd}
 & w \arrow[dl, mapsto, "*"] \arrow[dr, mapsto, "*"] & \\
u_1 \arrow[dr, mapsto, "*"'] & & u_2 \arrow[dl, mapsto, "*"] \\
 & v &
\end{tikzcd}$$

Figure II.1

**Lemma 3.2** *If $w \longmapsto u_1$ and $w \longmapsto u_2$, then there exists a word $v$ such that $u_1 \overset{*}{\longmapsto} v$ and $u_2 \overset{*}{\longmapsto} v$.*

*Proof.* There are words $x_1, y_1, x_2, y_2 \in C_n^*$ and $z_1, z_2 \in C_n^2$ such that

$$w = x_1 z_1 y_1 = x_2 z_2 y_2, \ u_1 = x_1 y_1, \ u_2 = x_2 y_2 \,.$$

If $|u_1| = |u_2|$, then $u_1 = u_2$ and there is nothing to prove. Assume for instance $|u_1| < |u_2|$. We distinguish two cases.

a) $|u_1| + 2 \leq |u_2|$. Then $u_2 = u_1 z_1 t$ for some word $t$, thus $w = z_1 z_1 t z_2 y_2$, and $v = z_1 t z_2$ satisfies $u_1 \longmapsto v$, $u_2 \longmapsto v$.

b) $|u_1| + 1 = |u_2|$. The $u_2 = u_1 c$ for some letter $c$, hence $z_1 = c\bar{c}$ and $z_2 = \bar{c}c$. (This implies that $c = a_i$ or $c = \bar{a}_i$ with $i \in I$.) Thus $w = x_1 c\bar{c} c y_2$, and $u_1 = x_1 c y_2 = u_2$. Hence $v = u_1$ satisfies the conditions. ■

*Proof* of Lemma 3.1 By induction on $|w|$. If $|w| = 0$, then $u_1 = w = u_2 = 1$, and $v = w$ satisfies the lemma. Assume $|w| = p > 0$. If $|u_1| = |w|$, then $u_1 = w$ and the lemma holds for $v = u_2$. Thus we may suppose $|u_1| < p$ and similarly $|u_2| < p$. There exist two words $v_1, v_2$ with $|v_1| = |v_2| = p - 2$ such that

$$w \longmapsto v_1 \overset{*}{\longmapsto} u_1, \; w \longmapsto v_2 \overset{*}{\longmapsto} u_2 \, .$$

Thus, in view of Lemma 3.2, there is a word $t$ such that

$$v_1 \overset{*}{\longmapsto} t, \; v_2 \overset{*}{\longmapsto} t \, .$$

Since $v_1 \overset{*}{\longmapsto} u_1$, $v_1 \overset{*}{\longmapsto} t$ and $|v_1| < p$, by induction there is a word $w_1$ such that

$$u_1 \overset{*}{\longmapsto} w_1, \; t \overset{*}{\longmapsto} w_1 \, .$$

Since $v_2 \overset{*}{\longmapsto} u_2$, $v_2 \overset{*}{\longmapsto} t \overset{*}{\longmapsto} w_1$ and $|v_2| < p$, by induction there is a word $v$ such that

$$u_2 \overset{*}{\longmapsto} v, \; w_1 \overset{*}{\longmapsto} v \, .$$

This show that $u_1 \overset{*}{\longmapsto} w_1 \overset{*}{\longmapsto} v$ and $u_2 \overset{*}{\longmapsto} v$. ■

The construction of the proof is reflected in Figure II.2.

$$\begin{tikzcd}
 & & w \arrow[dl, mapsto] \arrow[dr, mapsto] & & \\
 & v_1 \arrow[dl, mapsto, "*"'] \arrow[dr, mapsto, "*"] & & v_2 \arrow[dl, mapsto, "*"'] \arrow[dr, mapsto, "*"] & \\
u_1 \arrow[dr, mapsto, "*"'] & & t \arrow[dl, mapsto, "*"'] & & u_2 \arrow[ddll, mapsto, "*"] \\
 & w_1 \arrow[dr, mapsto, "*"'] & & & \\
 & & v & &
\end{tikzcd}$$

Figure II.2

**Corollary 3.3** *Let $u, v \in C_n^*$; then $u \equiv v \pmod{\delta_I}$ if and only if there exists a word $w$ such that $u \overset{*}{\longmapsto} w$ and $v \overset{*}{\longmapsto} w$.*

*Proof* Assume $u \equiv v$ (mod $\delta_I$). Then there are $k \geq 0$, $u_0, \ldots, u_k \in C_n^*$ such that $u_0 = u$, $u_k = v$ and

$$u_p \longmapsto u_{p+1} \text{ or } u_{p+1} \longmapsto u_p \quad \text{for } p = 0, \ldots, k-1 \, .$$

If $k = 0$, then $u = v$ and there is nothing to prove. Arguing by induction on $k$, there is a word $w_1$ such that

$$u_1 \overset{*}{\longmapsto} w_1 \text{ and } v \overset{*}{\longmapsto} w_1 \,.$$

If $u_0 \longmapsto u_1$, then $u_0 \overset{*}{\longmapsto} w_1$ and the corollary is true with $w = w_1$. If $u_1 \longmapsto u_0$, there exists, by the Confluence Lemma, a word $w_2$ such that $u_0 \overset{*}{\longmapsto} w_2$ and $w_1 \overset{*}{\longmapsto} w_2$, whence $v \overset{*}{\longmapsto} w_2$. The converse is obvious. ∎

**Remark** The Confluence Lemma can be considered as a property of some binary relations: Let $\overset{*}{\longmapsfrom}$ be the relation opposed to $\overset{*}{\longmapsto}$. Then the congruence $\delta_I$ is the least congruence containing $\overset{*}{\longmapsfrom}$ and $\overset{*}{\longmapsto}$. Corollary 3.3 states that $\delta_I$ is the *product* (of relations) of $\overset{*}{\longmapsto}$ and $\overset{*}{\longmapsfrom}$; the Confluence Lemma asserts the existence of a weak commutativity property: the product of $\overset{*}{\longmapsfrom}$ by $\overset{*}{\longmapsto}$ is contained in the product of $\overset{*}{\longmapsto}$ by $\overset{*}{\longmapsfrom}$.

We list two other corollaries

**Corollary 3.4** *If $v$ is reduced and $u \equiv v$ $(mod\ \delta_I)$, then $u \overset{*}{\longmapsto} v$.*

*Proof.* By Corollary 3.3, there is a word $w$ such that $u \overset{*}{\longmapsto} w$ and $v \overset{*}{\longmapsto} w$. Since $v$ is reduced, $v = w$. ∎

**Corollary 3.5** *Any class of the congruence $\delta_I$ contains exactly one reduced word.*

*Proof.* It is clear that any class contains at least one reduced word. Assume $u, v$ are reduced and $u \equiv v \pmod{\delta_I}$. Then by Corollary 3.4 $u \overset{*}{\longmapsto} v$ and $v \overset{*}{\longmapsto} u$, thus $u = v$. ∎

We denote by $\rho_I(w)$ the unique reduced word congruent to $w$ mod $\delta_I$. If $I = \emptyset$, we write $\rho'$ and if $I = \{1, \ldots, n\}$, we write $\rho$ instead of $\rho_I$. The language $\rho_I(C_n^*)$ of reduced words is a local regular set, since

$$\rho_I(C_n^*) = C_n^* \setminus C_n^* V_I C_n^* \,,$$

with

$$V_I = \{a_k \bar{a}_k \mid k = 1, \ldots, n\} \cup \{\bar{a}_i a_i \mid i \in I\} \,.$$

The next lemma describes the words which reduce to a given word. It is the key lemma for the proof that the languages $D_I^*$ are context-free.

**Lemma 3.6** *Let $x, w \in C_n^*$, $w = c_1 c_2 \cdots c_m, (c_p \in C_n^*)$. Then*

$$x \overset{*}{\longmapsto} w$$

*if and only if there exist $y_0, y_1, \ldots, y_m \in C_n^*$ such that*

$$x = y_0 c_1 y_1 c_2 \cdots y_{m-1} c_m y_m$$

*and*

$$y_0 \overset{*}{\longmapsto} 1, y_1 \overset{*}{\longmapsto} 1, \ldots, y_m \overset{*}{\longmapsto} 1 \,.$$

*Proof.* The conditions are clearly sufficient. The proof of the converse is by induction on $|x| - |w|$. If $|x| = |w|$, then $x = w$; if $|x| > |w|$, then there exists $x'$ such that $|x'| = |x| - 2$ and $x \longmapsto x' \overset{*}{\longmapsto} w$. By induction,

$$x' = y_0 c_1 y_1 c_2 \cdots y_{m-1} c_m y_m$$

for some words $y_r$ with $y_r \overset{*}{\longmapsto} 1$, $(r = 0, \ldots, m)$. Next, there is a factorization

$$x = uzv, \text{ with } x' = uv\,,$$

and $z = a_k \bar{a}_k$ for some $k \in \{1, \ldots, n\}$ or $z = \bar{a}_i a_i$ for some $i \in I$. Hence there is an integer $j$, $(0 \le j \le m)$ and a factorization $y_j = y'y''$, $(y', y'' \in C_n^*)$ such that

$$u = y_0 c_1 \cdots c_j y',\ v = y'' c_{j+1} \cdots c_m y_m\,.$$

Set $t_j = y'zy''$. Then $t_j \longmapsto y_j \overset{*}{\longmapsto} 1$ and

$$x = y_0 c_1 \cdots c_j t_j c_{j+1} \cdots c_m y_m\,. \qquad \blacksquare$$

**Theorem 3.7** *The languageD$_I^*$ is context-free. More precisely, $D_I^*$ is the language generated by the grammar $G_I$ with productions:*

$$\xi \to 1 + \sum_{k=1}^{n} a_k \xi \bar{a}_k \xi + \sum_{i \in I} \bar{a}_i \xi a_i \xi\,. \tag{3.3}$$

First, we introduce the notation

$$B_I = A_n \cup \{\bar{a}_i \mid i \in I\}\,.$$

Thus $B_I = A_n$ if $I = \emptyset$, and $B_I = C_n$ if $I = \{1, \ldots, n\}$.

*Proof* The grammar $G_I$ is strict. Thus it suffices to show that $D_I^*$ is a solution of the equation associated to (3.3). Assume $w = cw'\bar{c}w''$ with $w' \equiv w'' \equiv 1 \pmod{\delta_I}$ and $c \in B_I$. Then $w \equiv c\bar{c} \equiv 1 \pmod{\delta_I}$ and $w \in D_I^*$. This shows the inclusion

$$D_I^* \supset 1 \cup \bigcup_{1 \le k \le n} a_k D_I^* \bar{a}_k D_I^* \cup \bigcup_{i \in I} \bar{a}_i D_I^* a_i D_I^*\,.$$

Conversely, let $w \in D_I^*$, $w \ne 1$. Since 1 is reduced, $w \overset{*}{\longmapsto} 1$ by Corollary 3.4. Since $w \ne 1$ there is a letter $c \in B_I$ such that $w \overset{*}{\longmapsto} c\bar{c}$. By Lemma 3.6, $w$ factorizes in

$$w = y_0 c y_1 \bar{c} y_2$$

with $y_0, y_1, y_2 \in D_I^*$. If $y_0 = 1$, then $w \in cD_I^*\bar{c}D_I^*$. If $y_0 \ne 1$, then $|y_0| < |w|$ and, arguing by induction, $y_0 \in bD_I^*\bar{b}D_I^*$ for some $b \in B_I$. Thus $w \in bD_I^*\bar{b}D_I^*cD_I^*\bar{c}D_I^* \subset bD_I^*\bar{b}D_I^*$. This completes the proof. $\blacksquare$

We now investigate the language

$$D_I = (D_I^* \setminus 1) \setminus (D_I^* \setminus 1)^2\,.$$

For $c \in C_n$, define

$$D_{I,c} = D_I \cap cC_n^*\,.$$

**Proposition 3.8** (i) *The language $D_I$ is bifix;*
(ii) *$D_{I,c} \neq \emptyset$ if and only if $c \in B_I$;*
(iii) *if $D_{I,c} \neq \emptyset$, then any $w \in D_{I,c}$ admits a unique factorization*

$$w = cu_1u_2 \cdots u_m\bar{c} \quad \textit{with} \quad m \geq 0,\ u_1, \ldots, u_m \in D_I \setminus D_{I,\bar{c}}\,.$$

*Proof* (i) Let $w \in D_I$, and assume $w = uv$ with $u \in D_I, v \in C_n^*$. Then $1 \equiv uv \equiv v \pmod{\delta_I}$, thus $v \in D_I^*$. Thus $v = 1$ by the definition of $D_I$. This shows that $D_I$ is prefix. A symmetric argument shows that $D_I$ is suffix.

(ii) Let $w \in D_{I,c}$. Then $w = cu$ for some word $u$. Since $w \overset{*}{\longmapsto} 1$, there is a letter $b \in B_I$ such that $w \overset{*}{\longmapsto} b\bar{b}$. In view of Lemma 3.6, $w$ factorizes in $w = y_0by_1\bar{b}y_2$, with $y_0, y_1, y_2 \in D_I^*$. Since $w \in D_I$, $y_0 = y_2 = 1$ and $b = c$. This proves the assertion, since clearly $D_{I,c} \neq \emptyset$ if $c \in B_I$.

(iii) We just have seen that a word $w \in D_{I,c}$ factorizes in $w = cy_1\bar{c}$ with $y_1 \in D_I^*$. Thus either $y_1 = 1$ or $y_1 = u_1u_2 \cdots u_m$ with $u_1, \ldots, u_m \in D_I$. Assume that $u_p \in D_{I,c}$ for some $p$. Then $u_p = \bar{c}yc$ for some $y \in D_I^*$, and

$$w = (cu_1 \cdots u_{p-1}\bar{c})y(cu_{p+1} \cdots u_m\bar{c}) \in (D_I^* \setminus 1)^2\,,$$

contrary to the definition of $D_I$. The uniqueness is immediate since $D_I$ is a code.

■

By Proposition 3.8,

$$D_I = \bigcup_{c \in B_I} D_{I,c} \tag{3.4}$$

$$D_{I,c} = c\Delta_{I,c}\bar{c} \quad (c \in B_I) \tag{3.5}$$

where $\Delta_{I,c}$ is the submonoid of $C_n^*$ generated by $D_I \setminus D_{I,\bar{c}}$:

$$\Delta_{I,c} = \Big(\bigcup_{b \in B_I \setminus \bar{c}} D_{I,b}\Big)^*\,. \tag{3.6}$$

Finally, since $D_I$ generates $D_I^*$, we have

$$D_I^* = 1 \cup D_ID_I^*\,. \tag{3.7}$$

From Equations (3.4)–(3.7), we deduce the following grammar $H_I = \langle V_I, C_n, \mathcal{P}_I\rangle$. Set

$$V_I = \{\xi, \eta\} \cup \{\xi_c, \eta_c \mid c \in B_I\}\,,$$

and let $\mathcal{P}_I$ contain the productions:

$$\xi \to 1 + \eta\xi\,; \quad \eta = \sum_{c \in B_I} \eta_c\,; \quad \eta_c = c\xi_c\bar{c}\,;$$

$$\xi_c = 1 + \Big(\sum_{b \in B_I \setminus \bar{c}} \eta_b\Big)\xi_c \quad (c \in B_I)\,.$$

By the Substitution Lemma, the system of equations associated to $H_I$ is equivalent to

$$\xi = 1 + \sum_{c \in B_I} c\xi_c\bar{c}\xi\,; \quad \xi_c = 1 + \sum_{b \in B_I \setminus \bar{c}} b\xi_b\bar{b}\xi_c \quad (c \in B_I) \tag{3.8}$$
$$\eta = \sum_{c \in B_I} \eta_c\,; \quad \eta_c = c\xi_c\bar{c}\,; \quad (c \in B_I)\,.$$

The equations (3.8) are strict, thus the system associated to $H_I$ has a unique solution, and Equations (3.4)-(3.7) show that $H_I$ generates the various languages related to the Dyck sets:

$$D_I^* = L_{H_I}(\xi), \quad D_I = L_{H_I}(\eta), \quad D_{I,c} = L_{H_I}(\eta_c), \quad \Delta_{I,c} = L_{H_I}(\xi_c)\,.$$

**Corollary 3.9** *The languages $D_I$ are context-free.* ■

If $I = \emptyset$, the grammar $H_I$ reduces, after short-cutting the $\eta_z$, to the grammar with productions

$$\xi \to 1 + \eta\xi\,; \quad \eta \to \sum_{k=1}^{n} a_k\xi\bar{a}_k\,.$$

Thus we have, for $D_n'^*$, $D_n'$, $D_n^*$, $D_n$ the following formulas:

$$\begin{aligned} &D_n'^* = 1 \cup D_n' D_n'^*\,; && D_n' = \bigcup_{1 \le k \le n} a_k D_n'^* \bar{a}_k\,; \\ &D_n^* = 1 \cup D_n D_n^*\,; && D_n = \bigcup_{c \in C_n} D_{n,c}\,; \\ &D_{n,c} = c\Delta_{n,c}\bar{c} \ \ (c \in C_n)\,; && \Delta_{n,c} = \Big(\bigcup_{b \in C_n \setminus \bar{c}} D_{n,b}\Big)^* \quad (c \in C_n)\,. \end{aligned}$$

It can be shown (Exercise 3.1) that $D_n'^*$ is also generated by the grammar with productions

$$\xi \to \xi\xi + \sum_{k=1}^{n} a_k\xi\bar{a}_k + 1\,,$$

and that $D_n^*$ is generated by the grammar with productions

$$\xi \to \xi\xi + \sum_{k=1}^{n} a_k\xi\bar{a}_k + \sum_{k=1}^{n} \bar{a}_k\xi a_k + 1\,.$$

Let $A_n^{(*)} = C_n^*/\delta_n$ be the quotient monoid; we denote by $\delta_n$ the canonical morphism from $C_n^*$ onto $A_n^{(*)}$ defined by $\delta_n(w) = [w]_{\delta_n}$. For $w = c_1c_2\cdots c_m \in C_n^*$, $(c_i \in C_n)$, define $\bar{w} = \bar{c}_m\bar{c}_{m-1}\cdots\bar{c}_1$. Since

$$w\bar{w} \equiv \bar{w}w \equiv 1 \pmod{\delta_n}\,,$$

$A_n^{(*)}$ is a group, and $\delta_n(\bar{w}) = (\delta_n(w))^{-1}$. In particular, $\delta_n(\bar{c}) = (\delta_n(c))^{-1}$ for $c \in C_n$. It can even be shown that $A_n^{(*)}$ is a free group (see Magnus et al. 1966). $A_n^{(*)}$ is called the *free group generated* by $A_n$. Since each class $[w]_{\delta_n}$ contains exactly one reduced word $\rho(w)$, there is a bijection from $A_n^{(*)}$ onto $\rho(C_n^*)$ which associates to any $u \in A_n^{(*)}$ the unique reduced word $w$ such that $u = \delta_n(w)$. If no confusion can arise, the index $n$ will be omitted in the above notations.

Note that any word in $A_n^*$ is already reduced. Thus $A_n^* \subset \rho(C_n^*)$. It is sometimes convenient to identify $A_n^*$ with its image in $A_n^{(*)}$. This identification allows use of inverses and may simplify considerably certain formulations. However, it is important not to confuse the product $x^{-1}y$ in $A_n^{(*)}$, where $x, y \in A_n^*$, with the left quotient operation defined in Section I.2: Viewed as an operation in $A_n^{(*)}$, $x^{-1}y$ is always a well-defined element of $A_n^{(*)}$ and $x^{-1}y = z \in A_n^*$ if and only if $xz = y$. Viewed as an operation in $A_n^*$, $x^{-1}y$ is either the empty set or a word in $A_n^*$, according to $x$ is not, or is a prefix of $y$. The embedding of $A_n^*$ into $A_n^{(*)}$ will be used only in Sections IV.2 and IV.6. In all other circumstances, $x^{-1}y$ should be interpreted as the left quotient defined in Section I.2.

The Dyck languages are known by the Chomsky-Schützenberger Theorem. We prove the following

**Theorem 3.10** (Chomsky-Schützenberger Theorem) *Let $L \subset B^*$ be an algebraic language. Then there are an integer $n \geq 1$, an alphabetic morphism $\phi : C_n^* \to B^*$, and a local regular language $K$ such that*

$$L = \phi(D_n^* \cap K) = \phi(D_n'^* \cap K) = \phi(D_n \cap K) = \phi(D_n' \cap K)\,.$$

*Proof.* Assume the theorem proved in the case where $1 \notin L$. Then $1 \notin K$. Thus setting $K' = K \cup 1$, $K'$ is still a local language and the theorem holds for $L \cup 1$. Thus we may assume $1 \notin L$.

The idea of the proof is simple: each production in a grammar generating $L$ is bracketed by a distinct pair of parentheses, and new letters are added to make the new grammar generate a subset of $D_n^*$, and in fact of $D_n'$. Thus it has only to be shown that none of the generated words is in $D_n^* \setminus D_n'$.

We assume that $L$ is generated by a grammar $G = \langle V, B, \mathcal{P}\rangle$ in quadratic form, that is such that each production $\xi \to \alpha \in \mathcal{P}$ satisfies $\alpha \in B \cup V^2$. Such a grammar can always be obtained (see e.g. the books listed in the bibliography). We set

$$V = \{\xi_1, \ldots, \xi_N\}, \quad B = \{b_1, \ldots, b_q\}\,,$$

and define

$$\begin{aligned} A_n = B \,\cup\, &\{a_{i,j,k}, b_{i,j,k} \mid i,j,k = 1, \ldots, N\} \\ \cup\, &\{d_{i,s} \mid i = 1, \ldots, N,\ s = 1, \ldots, q\}\,, \end{aligned}$$

where the $a_{i,j,k}, b_{i,j,k}, d_{i,s}$ are new letters. Thus $n = 2N^3 + Nq + q$. Set $\bar{A}_n = \{\bar{a} \mid a \in A_n\}$ and $C_n = A_n \cup \bar{A}_n$. Let $H = \langle V, C_n, \mathcal{Q}\rangle$ be the grammar with the following productions:

For $i, j, k \in \{1, \ldots, N\}$,

$$\xi_i \to a_{i,j,k} b_{i,j,k} \xi_j \bar{b}_{i,j,k} \xi_k \bar{a}_{i,j,k} \in \mathcal{Q} \tag{3.9}$$

if and only if

$$\xi_i \to \xi_j \xi_k \in \mathcal{P}\,.$$

Further, for $i \in \{1, \ldots, N\}$, $s = 1, \ldots q$,

$$\xi_i \to d_{i,s} b_s \bar{b}_s \bar{d}_{i,s} \in \mathcal{Q} \tag{3.10}$$

if and only if

$$\xi_i \to b_s \in \mathcal{P}\,.$$

For $i = 1, \ldots, N$, set $M_i = L_H(\xi_i)$, and let $\phi : C_n^* \to B^*$ be the projection. Then clearly

$$\phi(M_i) = L_G(\xi_i)\,.$$

We shall prove that

$$M_i = D_n^* \cap K_i = D_n'^* \cap K_i = D_n \cap K_i = D_n' \cap K_i \quad i = 1, \ldots, N \tag{3.11}$$

where

$$K_i = (X_i C_n^* \cap C_n^* \bar{X}_i) \setminus C_n^* Y C_n^*$$

is the local regular set defined by:

$$\begin{aligned} X_i &= \{a_{i,j,k} \mid j,k = 1, \ldots, N\} \cup \{d_{i,s} \mid s = 1, \ldots, q\}\,, \\ \bar{X}_i &= \{\bar{x} \mid x \in X_i\}\,, \quad C_n^2 \setminus Y = W_1 \cup W_2 \cup W_3\,, \end{aligned}$$

with

$$W_1 = \{a_{i,j,k} b_{i,j,k} \mid i,j,k = 1, \ldots, N\}\,; \tag{3.12}$$

$$W_2 = \{d_{i,s} b_s, \bar{b}_s \bar{d}_{i,s} \mid i = 1, \ldots, N,\ s = 1, \ldots, q\} \cup \{b_s \bar{b}_s \mid s = 1, \ldots, q\} \tag{3.13}$$

$$W_3 = \bigcup_{i,j,k} b_{i,j,k} X_j \cup \bar{b}_{i,j,k} X_k \cup \bar{X}_j \bar{b}_{i,j,k} \cup \bar{X}_k \bar{a}_{i,j,k}\,. \tag{3.14}$$

a) $M_i \subset D_n^* \cap K_i$, $(i = 1, \ldots, N)$. Let indeed $w \in M_i$. Then either, by (3.10),

$$w = d_{i,s} b_s \bar{b}_s \bar{d}_{i,s}$$

for some $s \in \{1, \ldots, q\}$, and clearly $w \in D_n^* \cap K_i$, or by (3.9)

$$w = a_{i,j,k} b_{i,j,k} u \bar{b}_{i,j,k} v \bar{a}_{i,j,k}$$

for some $j, k \in \{1, \ldots, n\}$ and $u \in M_j$, $v \in M_k$. Arguing by induction, $u \in D_n^* \cap K_j$, $v \in D_n^* \cap K_k$, thus $w \in D_n^*$ and, in view of (3.12) and (3.14), $w \in K_i$.

b) $D_n^* \cap K_i \subset D_n'^* \cap K_i$, $(i = 1, \ldots, N)$. First, we verify

$$D_{n,\bar{a}} \cap C_n^* \setminus C_n^* Y C_n^* = \emptyset \quad \text{for } \bar{a} \in \bar{A}_n\,. \tag{3.15}$$

Assume the contrary, and let $w \in D_{n,\bar{a}} \cap C_n^* \setminus C_n^* Y C_n^*$ be of minimal length. Then $|w| > 2$ since $\bar{a}a \in Y$. In view of Proposition 3.8(iii), $w = \bar{a}u_1 \cdots u_m a$, with $u_p \in D_n \cap A_n C_n^* \bar{A}_n$, $(p = 1, \ldots, m)$ by the minimality of $w$. Since the first letter of $u_1$ is not barred, $\bar{a} = \bar{b}_{i,j,k}$ for some indices $i, j, k$ by (3.14). Thus, by (3.12), the last letter of $u_m$ is $a_{i,j,k}$ and $u_m \notin D_n \cap A_n C_n^* \bar{A}_n$. This proves (3.15).

Now let $w \in D_n^* \cap K_i$, $w = w_1 w_2 \cdots w_r$ with $w_p \in D_n \cap A_n C_n^* \bar{A}_n$ for $p = 1, \ldots r$ by (3.15). Then $w_1 \in X_i C_n^* \bar{X}_i$ for some $i$, thus if $r > 1$, the first letter of $w_2$ would be barred by (3.14). Thus $r = 1$ and $w \in D_n$. Next, if $w$ begins with a letter $d_{i,s}$, then $w = d_{i,s} b_s \bar{b}_s \bar{d}_{i,s}$ by (3.13) and $w \in D'_n$. Finally, if $w$ begins with the letter $a_{i,j,k}$, then $w = a_{i,j,k} u \bar{a}_{i,j,k}$ for some $u \in D_n^*$ and in view of (3.12), $u = b_{i,j,k} v_1 \bar{b}_{i,j,k} v_2$ for some $v_1, v_2 \in D_n^*$. In view of (3.14), $v_1 \in K_i$, $v_2 \in K_k$, and arguing by induction, $v_1 \in D'_n \cap K_j$, $v_2 \in D'_n \cap K_k$. Thus $w \in D'_n$.

c) $D'_n \cap K_i \subset M_i$, $(i = 1, \ldots, N)$. Let $w \in D'_n \cap K_i$. If $w$ begins with a letter $d_{i,s}$, then by (3.13) $w = d_{i,s} b_s \bar{b}_s \bar{d}_{i,s}$ and $w \in M_i$ by (3.10). Otherwise, $w = a_{i,j,k} u \bar{a}_{i,j,k}$ for some indices $j, k$ and $u \in D_n'^*$. By (3.12), $u = b_{i,j,k} v_1 \bar{b}_{i,j,k} v_2$ for some $v_1, v_2 \in D_n'^*$. Moreover, $v_1 \in K_j$ and $v_2 \in K_k$. Thus $v_1 \in D_n'^* \cap K_j \subset D'_n \cap K_j$ and similarly $v_2 \in D'_n \cap K_k$, by part b) of the proof. Therefore by induction $v_1 \in M_j, v_2 \in M_k$ and $w \in M_i$ by (3.9).

Thus we proved

$$M_i \subset D_n^* \cap K_i \subset D'_n \cap K_i \subset M_i \quad i = 1, \ldots, N\,,$$

and (3.11) follows. ■

## Exercises

**3.1** Show that for any $I \subset \{1, \ldots, n\}$, $D_I^*$ is the language generated by the grammar with productions

$$\xi \to \xi\xi + \sum_{k=1}^{n} a_k \xi \bar{a}_k + \sum_{i \in I} \bar{a}_i \xi a_i + 1\,.$$

**3.2** Same question as in Exercise 3.1, for the grammar

$$\xi \to \xi\xi + \sum_{k=1}^{n} a_k \xi\xi \bar{a}_k + \sum_{i \in I} \bar{a}_i \xi\xi a_i + 1\,.$$

**3.3** (Magnus et al. (1966)) Define a function $\theta_I : C_n^* \to C_n^*$ inductively as follows: $\theta_I(1) = 1$, $\theta_I(c) = c$ for $c \in C_n$, and if $\theta_I(w) = c_1 c_2 \cdots c_m$ $(c_i \in C_n)$, then

$$\theta_I(wc) = \begin{cases} c_1 c_2 \cdots c_{m-1} & \text{if } c_m \in B_I \text{ and } c_m = \bar{c}, \\ c_1 c_2 \cdots c_m c & \text{otherwise.} \end{cases}$$

Show that $\theta_I = \rho_I$.

**3.4** Show that $ww' \in D_n^* \implies w'w \in D_n^*$.

**3.5** Show that for each $w \in C_n^*$, the class $[w]_{\delta_I}$ is a context-free language.

**3.6** For $w \in C_n^*$, define

$$\|w\| = |w|_{A_n} - |w|_{\bar{A}_n} = \sum_{k=1}^{n} |w|_{a_k} - |w|_{\bar{a}_k}$$

Show the following assertions:

a) $w \in D_n^* \implies \|w\| = 0$.

b) $w \in D_n'^* \implies \|w'\| \geq 0$ for each prefix $w'$ of $w$.

c) $w \in D_n' \implies \|w'\| > 0$ for each proper nonempty prefix $w'$ of $w$.

d) $w \in D_1^* \iff \|w\| = 0$.

**3.7** (Requires knowledge in ambiguity.) Show that the grammars $H_I$ are unambiguous.

**3.8** Assume that the grammar $G = \langle V, B, \mathcal{P} \rangle$ for $L$ in the proof of the Chomsky-Schützenberger Theorem is in Greibach Normal Form, that is $\xi \to \alpha$ implies $\alpha \in B \cup BV \cup BVV$.

a) Show that $G$ can be transformed in such a way that for any two productions $\xi \to b\beta$, $\xi \to b'\beta'$ $(b, b' \in B)$, if $b \neq b'$, then $\beta \neq \beta'$.

b) Replace the productions of the form

$$\begin{array}{lll} \xi_i \to b\xi_j\xi_k & \text{by} & \xi_i \to a_{i,j,k}\xi_j\bar{a}_{i,j,k}\xi_k \\ \xi_i \to b\xi_j & \text{by} & \xi_i \to b_{i,j}\bar{b}_{i,j}\xi_j \\ \xi_i \to b & \text{by} & \xi_i \to d_i\bar{d}_i \end{array}$$

and prove that $L = \phi(D_n'^* \cap K)$ where $K$ is a local regular set and where $\phi$ erases barred letters, and replaces unbarred letters according to the above rules.

c) Show that each word in $D_n'^* \cap K$ ends by exactly one barred letter, and that no word in $D_n'^* \cap K$ contains a factor of more than two barred letters.

d) Show that any context-free language $L$ can be represented in the form $L = \phi(D_n'^* \cap R)$ with $R$ local and $\phi$ $\varepsilon$-limited on $R$ (that is $k \cdot |\phi(w)| \geq |w|$ for all $w$ in $R$ and for some $k > 0$).

## 4 Two Special Languages

We present some properties of the Lukasiewicz language, and of the language of completely parenthesized arithmetic expressions.

**a) The Lukasiewicz language** Ł over $A = \{a, b\}$ is the language generated by the grammar with productions

$$\xi \to a\xi\xi + b\,.$$

Thus Ł is the unique language satisfying

$$Ł = aŁŁ \cup b\,. \tag{4.1}$$

The first words of Ł are

$$b, abb, aabbb, ababb, aaabbbb, aababbb, \ldots$$

The language of Lukasiewicz is the simplest of a family of languages constructed in order to write arithmetic expressions without parentheses (prefix or "polish" notation). The letter $a$ represents a binary operations, say +, and $b$ represents the operand. Thus the word $abb$ represents the expression $b+b$, and $aababbb$ represents the expression $((b + (b + b)) + b)$.

For $w \in A^*$, define

$$\|w\| = |w|_a - |w|_b\,.$$

Clearly $\|ww'\| = \|w\| + \|w'\|$.

**Proposition 4.1** *Let $w \in A^*$. Then $w \in Ł$ if and only if $w$ satisfies the two following conditions:*
(i) $\|w\| = -1$;
(ii) $\|w'\| \geq 0$ *for each proper prefix $w'$ of $w$.*

Clearly, Proposition 4.1 implies that Ł is prefix.

*Proof.* Let $w \in Ł$. If $w = b$, then (i) and (ii) are satisfied. Assume $|w| > 1$. Then by (4.1), $w = auv$ with $u, v \in Ł$. Thus $\|w\| = 1 + \|u\| + \|v\| = -1$. Next, let $w'$ be a proper prefix of $w$. If $w' = a$, or if $w'$ is a proper prefix of $au$, then clearly $\|w'\| \geq 0$. If $w' = auv'$ and $v'$ is a proper prefix of $v$, then $\|w'\| = \|v'\| \geq 0$.

Conversely, let $w$ be a word satisfying (i) and (ii). If $|w| = 1$, then $w = b \in Ł$. Arguing by induction on $|w|$, assume $|w| > 1$. First note that by (ii) $w$ begins with the letter $a$. Thus $w = aw'$ for some $w'$. Next, since $\|w\| = -1$, there exists a shortest nonempty prefix $u$ of $w'$ such that $\|au\| = 0$. Set $w = auv$. Then $\|u\| = -1$, and for any nonempty proper prefix $u'$ of $u$, $\|u'\| \geq 0$ by the minimality assumption on $u$. Thus $u \in Ł$. Next $\|v\| = \|w\| = -1$, and $\|v\|' = \|auv'\| \geq 0$ for any proper prefix $v'$ of $v$ since $w$ satisfies (ii). Thus $v \in Ł$ and $w \in Ł$ by (4.1). ■

Proposition 4.1 can be used to draw a pictorial representation of a word $w$ in Ł. This is given by the graph of the function $w' \mapsto \|w'\|$, where $w'$ ranges over the prefixes of $w$. Thus, for $w = aabaabbabbabaaabbbb$, we obtain Figure II.3. Next, consider the restricted Dyck language $D_1'^*$ over $A$, that is with $a_1 = a, \bar{a}_1 = b$. Then $D_1'^*$ is defined by

$$D_1'^* = 1 \cup aD_1'^*bD_1'^*\,.$$

Multiply this equation by $b$ on the right. This gives

$$D_1'^*b = b \cup aD_1'^*bD_1'^*b\,.$$

Thus $D_1'^*b$ is a solution of (4.1), and therefore $D_1'^*b = Ł$.

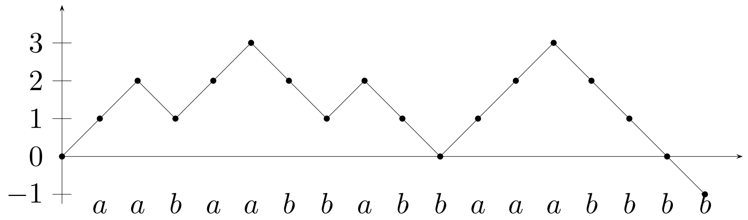

Figure II.3

**Corollary 4.2** *Let $w \in A^*$. Then $w \in D_1'^*$ if and only if $w$ satisfies:*

(i) $\|w\| = 0\,;$
(ii) $\|w'\| \geq 0$ *for each proper prefix $w'$ of $w$.* ∎

Recall that $u$ and $v$ are *conjugate* if and only if $u = xy$ and $v = yx$ for some words $x, y$.

**Proposition 4.3** *Let $u \in A^*$ with $\|u\| = -1$. Then there exists one and only one word $v$ conjugate to $u$ such that $v \in Ł$.*

*Proof.* We show first the uniqueness. Assume $u = xy, v = yx \in Ł$, $v \neq 1$. Then by Proposition 4.1, $\|x\| \geq 0$, thus $\|u\| = -1 = \|x\| + \|v\| \geq \|v\|$, and $v$ cannot be a proper prefix of $v$. Thus $x = 1$ and $u = v$.

Next, let $p = \min\{\|u'\| \mid u' \text{ proper prefix of } u\}$. If $p \geq 0$, then $u \in Ł$. Assume $p < 0$, and let $x$ be the shortest prefix of $u$ such that $\|x\| = p$. Write $u = xy$. Then

$$\|x'\| \geq p + 1 \quad \text{for any proper prefix } x' \text{ of } x \tag{4.2}$$

by the minimality of $x$. Next

$$\|y'\| \geq 0 \quad \text{for any proper prefix } y' \text{ of } y \tag{4.3}$$

since $p \leq \|xy'\| = p + \|y'\|$ by definition of $p$ and

$$\|y\| = -1 - p \geq 0\,. \tag{4.4}$$

Let $v = yx$. Then $\|v\| = \|u\| = -1$. Let $v'$ be a proper prefix of $v$. If $v'$ is a prefix of $y$, then $\|v'\| \geq 0$ by (4.3) and (4.4). Otherwise, $v' = yx'$, where $x'$ is a proper prefix of $x$, and $\|v'\| = -1 - p + \|x'\| \geq 0$ by (4.2). In view of Proposition 4.1, $v \in Ł$. ∎

**b) The language of completely parenthesized arithmetic expressions** $E$ over $A = \{a, b, c, d\}$ is the language generated by the grammar with productions

$$\xi \to a\xi b\xi c + d\,.$$

Thus $E$ is the unique language satisfying

$$E = aEbEc \cup d\,. \tag{4.5}$$

The first words of $E$ are

$$d, adbdc, aadbdcbdc, adbadbdcc, aadbdcbadbdcc, \ldots$$

The terminology is from Nivat (1967). Write indeed "(" for "$a$", ")" for "$c$", "+" for "$b$" and "$i$" for "$d$". The words listed above become

$$i, (i+i), ((i+i)+i), (i+(i+i)), ((i+i)+(i+i)), \ldots$$

Consider the morphism that erases $c$ and $d$. Then by (4.5) the image of $E$ is the language $D_1'^*$ over $\{a, b\}$. If $b$ and $c$ are erased, then the image of $E$ is the language Ł over $\{c, d\}$. Thus $E$ is closely related to these languages. In fact, we shall prove later (Chapter VII) that the language $E$ is a generator of the cone of context-free languages.

**Lemma 4.4** *Let $w \in E$. Then*

(i) $|w|_a = |w|_b = |w|_c = |w|_d - 1$ *;*

(ii) *If $w'$ is a proper nonempty prefix (resp. suffix) of $w$, then $|w'|_a > |w'|_c$ (resp. $|w'|_a < |w'|_c$).*

The easy proof is left to the reader. Note that (ii) implies that the language $E$ is bifix.

Let $\eta$ be the congruence over $A^*$ generated by the relation

$$adbdc \sim d\,.$$

**Theorem 4.5** *The language $E$ is equal to the class of $d$ in the congruence $\eta$: $E = [d]_\eta$.*

*Proof.* Clearly $d \in [d]_\eta$. Let $w \in E$, $w \neq d$. Then $w = aubvc$ for some $u, v \in E$ by (4.5). Arguing by induction, $u \equiv v \equiv d \pmod{\eta}$, thus $w \equiv adbdc \equiv d \pmod{\eta}$. This shows the inclusion $E \subset [d]_\eta$.

To show the converse inclusion, it suffices to prove that for any two words $w = udv$ and $w' = uadbdcv$,

$$w \in E \iff w' \in E\,. \tag{4.6}$$

We verify (4.6) by induction on $|w| = |w'| - 4$. If $u = 1$, then $w \in E$ if and only if $w = d$, and $w' = adbdc$, since $E$ is prefix. Thus we may assume $u \neq 1$. Suppose $w \in E$. Then $w = aw_1bw_2c$ for some $w_1, w_2 \in E$. Then either $|ud| \leq |aw_1|$ or $|dv| \leq |w_2c|$. In the first case, $w_1 = u_1dv_1$ for $u_1$ and $v_1$ defined by $au_1 = u$, $v = v_1bw_2c$. By induction, $w_1' = u_1adbdcv_1$ belongs to $E$. Thus $aw_1'bw_2c = w' \in E$ by (4.5). The second case is handled in the same way. Conversely, suppose $w' \in E$. Then

$$w' = uadbdcv = aw_1'bw_2'c$$

for $w'_1, w'_2 \in E$. If $|aw'_1| = |uad|$, then $w'_1 = d$ since $E$ is suffix, hence $u = 1$ contrary to the assumption. Thus either $|uad| < |aw'_1|$ or $|dvc| < |w'_2c|$. It suffices to consider the first case. Clearly, it implies that $|uadbdc| \le |aw'_1|$, thus $w'_1 = u'_1adbdcv'_1$ with $au'_1 = u$ and $v = v'_1bw'_2c$. By induction, $w_1 = u'_1dv'_1 \in E$, hence

$$aw_1bw'_2c = w \in E\,. \qquad \blacksquare$$

Theorem 4.5 admits the following

**Corollary 4.6** *Let $u, u' \in E$. Then $xuy \in E$ if and only if $xu'y \in E$.*

*Proof.* $xuy \equiv xu'y \pmod{\eta}$. Thus $xuy \equiv d \pmod{\eta}$ if and only if $xu'y \equiv d \pmod{\eta}$. ■

## Exercises

**4.1** Show that Ł $= [b]_\lambda$, where $\lambda$ is the congruence over $\{a, b\}^*$ generated by the relation $abb \sim b$.

**4.2** Let $p_n = \mathrm{Card}(A^{2n+1} \cap$ Ł$)$. Show that $p_n = \dfrac{1}{n+1}\dbinom{2n}{n}$. Show that $p_n = q_n$, where $q_n = \mathrm{Card}(A^{4n+1} \cap E)$.

# Chapter III

# Rational Transductions

Rational transductions are defined by rational relations, that is rational subsets of the product of two free monoids. The chapter therefore begins with two sections concerned with recognizable and rational subsets of an arbitrary monoid. The next two sections contain the definition and basic properties of rational relations and rational transductions. Examples of rational transductions are given in Section 5. Then the machines realizing rational transductions are introduced. Matrix representations of rational transductions are investigated in Section 7. In the last section we show that most of the usual decision problems are unsolvable for rational transductions.

## 1 Recognizable Sets

Kleene's Theorem gives a characterization of the regular languages of a finitely generated free monoid, but the theorem cannot be extended to arbitrary monoids. Therefore we can investigate the class of monoids where Kleene's theorem remains true. An example of such a monoid was given by Amar and Putzolu (1965). A wider family of semigroups where Kleene's Theorem is partially true is formed by the equidivisible semigroups of McKnight and Storey (1969). S. Eilenberg had the idea, formulated for instance in (Eilenberg 1967), to distinguish in each monoid two families of subsets, called the recognizable and the rational subsets. These two families are of distinct nature and Kleene's Theorem precisely asserts that they coincide in finitely generated free monoids. Properties of regular languages like closure properties can be proved some for recognizable subsets, others for the rational subsets of a monoid. This gives also insight in the structure of regular languages by showing from which of their two aspects originate their properties.

This section deals with recognizable, the next section with rational subsets of a monoid. We are mainly interested in properties which are of later use for rational transductions, but we also touch slightly on properties of rational subsets of groups.

We want recognizable sets to be, in free monoids, exactly the languages recognized by finite automata. Instead of a generalization of finite automata, we prefer to use as definition a characterization via morphism into a finite monoid. This simplifies the exposition.

**Definition** Let $M$ be a monoid. A subset $X$ of $M$ is *recognizable* if there exist a finite monoid $N$, a morphism $\alpha$ from $M$ into $N$ and a subset $P$ of $N$ such that $X = \alpha^{-1}(P)$.

If this holds, then $\alpha(X) = P \cap \alpha(M)$, and consequently $X = \alpha^{-1}(\alpha(X))$. Next, $\alpha$ considered as a morphism onto $\alpha(M)$ is surjective, and $X = \alpha^{-1}(Q)$ with $Q = P \cap \alpha(M)$. Thus we may assume that $\alpha$ is surjective in the above definition. An equivalent condition for $X \subset M$ to be recognizable is the existence of a congruence relation $\theta$ on $M$ of *finite* index such that $X$ is *saturated* for $\theta$, that is $X$ is a union of equivalence classes of $\theta$.

The set of all recognizable subsets of $M$ is denoted by $\mathrm{Rec}(M)$.

**Example 1.1** Let $M$ be any monoid, and let $N = \{1\}$ be the monoid consisting of a single element. Let $\alpha$ be the unique morphism from $M$ onto $N$. Then $\emptyset = \alpha^{-1}(\emptyset)$ and $M = \alpha^{-1}(N)$. Thus $M, \emptyset \in \mathrm{Rec}(M)$ for any monoid $M$.

**Example 1.2** If $M$ is a finite monoid, then any subset of $M$ is recognizable.

**Example 1.3** If $M = A^*$ and $A$ is an alphabet, then $X \in \mathrm{Rec}(A^*)$ if and only if $X$ is recognized by a finite automaton (Proposition I.4.4).

**Example 1.4** Consider the additive group $\mathbb{Z}$ of integers. Let $\alpha$ be a morphism from $\mathbb{Z}$ onto a finite monoid $N$. Then $\alpha$ is a group morphism and $N = \alpha(\mathbb{Z})$ is a finite group, thus $N = \mathbb{Z}/n\mathbb{Z}$ for some integer $n \geq 1$ (Exercise I.3.1). Consequently $N$ can be identified with the set $\{0, 1, \ldots, n-1\}$, and for $p \in N$, $\alpha^{-1}(p) = p + n\mathbb{Z}$. Thus for $P \subset N$, $\alpha^{-1}(P) = \bigcup_{p \in P} p + n\mathbb{Z}$. Conversely, any subset of $\mathbb{Z}$ of this form is recognizable. It follows that $X \in \mathrm{Rec}(\mathbb{Z})$ if and only if $X$ is a finite union of arithmetic progressions. In particular, any nonempty recognizable subset of $\mathbb{Z}$ is infinite.

**Proposition 1.1** *Let $M$ be a monoid. Then* $\mathrm{Rec}(M)$ *is closed under union, intersection and complementation.*

Since $\emptyset, M \in \mathrm{Rec}(M)$, it follows that $\mathrm{Rec}(M)$ is a boolean algebra.

*Proof.* Let $X \in \mathrm{Rec}(M)$, let $N$ be a finite monoid, let $\alpha : M \to N$ be a surjective morphism and let $P$ be a subset of $N$ such that $X = \alpha^{-1}(P)$. Then $M \setminus X = \alpha^{-1}(N \setminus P)$. Thus $M \setminus X \in \mathrm{Rec}(M)$. This proves the closure under complementation.

Next, let $Y \in \mathrm{Rec}(M)$, $Y = \beta^{-1}(Q)$, where $\beta$ is a surjective morphism from $M$ onto some finite monoid $N'$ and $Q \subset N'$. Let $N'' = N \times N'$ be the product monoid and define $\gamma : M \to N''$ by $\gamma(m) = (\alpha(m), \beta(m))$, $m \in M$. Then $\gamma$ is a morphism. Further $\gamma(m) \in P \times Q$ if and only if $\alpha(m) \in P$ and $\beta(m) \in Q$, thus if and only if $m \in \alpha^{-1}(P) \cap \beta^{-1}(Q)$. Consequently $X \cap Y = \gamma^{-1}(P \times Q)$, and since $N''$ is finite, $X \cap Y \in \mathrm{Rec}(M)$. Thus $\mathrm{Rec}(M)$ is closed under intersection. Closure under union follows from de Morgan's rule. ■

**Corollary 1.2** *If $X, Y \in \mathrm{Rec}(M)$, then $X \setminus Y \in \mathrm{Rec}(M)$.* ■

An important property of recognizable sets is the closure under inverse morphisms.

**Proposition 1.3** *Let $M$ and $M'$ be monoids, and let $\gamma : M \to M'$ be a morphism. If $X' \in \mathrm{Rec}(M')$, then $\gamma^{-1}(X') \in \mathrm{Rec}(M)$.*

*Proof.* Let $\alpha : M' \to N$ be a surjective morphism onto a finite monoid $N$, and let $P \subset N$ be such that $X' = \alpha^{-1}(P)$. Then $\gamma^{-1}(X') = \beta^{-1}(P)$, with $\beta = \alpha \circ \gamma$. Thus $\gamma^{-1}(X') \in \mathrm{Rec}(M)$. ■

If the monoid $M'$ in Proposition 1.3 is finitely generated, then $M$ can be chosen to be the free monoid generated by an alphabet. It follows that $\gamma^{-1}(X')$ is a regular language.

**Corollary 1.4** *Let $\gamma$ be an isomorphism from $M$ onto $M'$. Then $X \in \mathrm{Rec}(M)$ if and only if $\gamma(M) \in \mathrm{Rec}(M')$.* ■

The following example shows that the homomorphic image of a recognizable set is not recognizable in general.

**Example 1.5** Let $A = \{a, b\}$, and let $\gamma : A^* \to \mathbb{Z}$ be the morphism defined by $\gamma(w) = |w|_a - |w|_b$ ($w \in A^*$). Then $\{1\} \in \mathrm{Rec}(A^*)$, and $\gamma(\{1\}) = \{0\}$. In view of Example 1.4, $\{0\} \notin \mathrm{Rec}(\mathbb{Z})$. This can also be seen by applying Proposition 1.3. Assume indeed $\{0\} \in \mathrm{Rec}(\mathbb{Z})$. Then $\gamma^{-1}(0)$ is a recognizable subset of $A^*$, that is a regular language. Since $\gamma^{-1}(0) = D_1^*$, the Dyck language over $A$ (Exercise II.3.6), this yields a contradiction.

In general, the family $\mathrm{Rec}(M)$ is closed neither under product nor under star operation. This is shown by the following example which is credited to S. Winograd by Eilenberg (1974).

**Example 1.6** Consider the additive group $\mathbb{Z}$, and add to $\mathbb{Z}$ two new elements $\varepsilon$ and $a$. The set $M = \mathbb{Z} \cup \{\varepsilon, a\}$ is a commutative monoid with addition extended as follows:

$$\varepsilon + m = m \ \ (m \in M), \quad a + a = 0, \ a + x = x \ (x \in \mathbb{Z}) .$$

Thus $\varepsilon$ is the neutral element of $M$. We first show that $\{\varepsilon\}, \{a\} \in \mathrm{Rec}(M)$. Consider indeed the commutative monoid $N = \{\bar\varepsilon, \bar a, \bar 0\}$ with neutral element $\bar\varepsilon$, and with addition defined by $\bar 0 + \bar 0 = \bar 0 + \bar a = \bar a + \bar a = \bar 0$. Then $\alpha : M \to N$ given by $\alpha(\varepsilon) = \bar\varepsilon$, $\alpha(a) = \bar a$, $\alpha(x) = \bar 0$, ($x \in \mathbb{Z}$) is a morphism, and $\{\varepsilon\} = \alpha^{-1}(\bar\varepsilon)$, $\{a\} = \alpha^{-1}(\bar a)$. Next if $X \in \mathrm{Rec}(M)$, then $X \cap \mathbb{Z} \in \mathrm{Rec}(\mathbb{Z})$. Let indeed $\beta$ be a morphism from $M$ onto a finite monoid $N'$, let $\beta_1$ be the restriction of $\beta$ on $\mathbb{Z}$, and set $N_1 = \beta_1(\mathbb{Z})$. If $X = \beta^{-1}(P)$ for $P \subset N'$, then

$$\beta_1^{-1}(P \cap N_1) = \beta^{-1}(P \cap N_1) \cap \mathbb{Z} = \beta^{-1}(P) \cap \mathbb{Z} = X \cap \mathbb{Z} .$$

Consequently, $X \cap \mathbb{Z} \in \mathrm{Rec}(\mathbb{Z})$. Define now $X = \{a\}$. Then $X \in \mathrm{Rec}(M)$, and $X + X = \{0\}$, $X^+ = \{0, a\}$, $X^* = \{0, \varepsilon, a\}$. None of these subsets is in $\mathrm{Rec}(M)$, since otherwise their intersection with $\mathbb{Z}$, that is $\{0\}$ would be a recognizable subset of $\mathbb{Z}$ in contradiction with Example 1.4.

The following theorem gives a description of the recognizable subsets of the product of two monoids. Eilenberg (1974) attributes it to Mezei.

**Theorem 1.5** (Mezei) *Let $M_1, M_2$ be monoids and $M = M_1 \times M_2$. Then $Y \in \mathrm{Rec}(M)$ if and only if $Y$ is a finite union of sets of the form $X_1 \times X_2$, with $X_1 \in \mathrm{Rec}(M_1)$ and $X_2 \in \mathrm{Rec}(M_2)$.*

*Proof.* The condition is sufficient. Let indeed $\pi_i : M \to M_i$, $(i = 1, 2)$ be the canonical projections. If $X_1 \subset M_1$, $X_2 \subset M_2$, then

$$X_1 \times X_2 = (X_1 \times M_2) \cap (M_1 \times X_2) = \pi_1^{-1}(X_1) \cap \pi_2^{-1}(X_2)\,.$$

Thus, if $X_1 \in \mathrm{Rec}(M_1)$, $X_2 \in \mathrm{Rec}(M_2)$, then $X_1 \times X_2 \in \mathrm{Rec}(M)$ in view of Propositions 1.3 and 1.1. Since $\mathrm{Rec}(M)$ is closed under union, $Y \in \mathrm{Rec}(M)$.

Conversely, assume $Y \in \mathrm{Rec}(M)$. Then there exists a finite monoid $N$, a morphism $\beta : M \to N$, and a subset $P$ of $N$ such that $Y = \beta^{-1}(P)$. Consider the morphisms $\alpha_i : M_i \to P$ defined by

$$\alpha_1(m_1) = \beta(m_1, 1), \quad \alpha_2(m_2) = \beta(1, m_2)$$

and let $\gamma : M \to N \times N$ be the morphism defined by

$$\gamma(m_1, m_2) = (\alpha_1(m_1), \alpha_2(m_2))\,.$$

In $N \times N$ consider the set

$$Q = \{(n_1, n_2) \mid n_1 n_2 \in P\}\,.$$

Then $\gamma(m_1, m_2) \in Q$ if and only if $\alpha_1(m_1)\alpha_2(m_2) \in P$. Since

$$\alpha_1(m_1)\alpha_2(m_2) = \beta(m_1, m_2)\,,$$

and since $(m_1, m_2) \in Y$ if and only if $\beta(m_1, m_2) \in P$, it follows that $Y = \gamma^{-1}(Q)$. Next $\gamma^{-1}(n_1, n_2) = \alpha_1^{-1}(n_1) \times \alpha_2^{-1}(n_2)$, whence

$$Y = \bigcup_{(n_1,n_2)\in Q} \gamma^{-1}(n_1, n_2) = \bigcup_{(n_1,n_2)\in Q} \alpha_1^{-1}(n_1) \times \alpha_2^{-1}(n_2)\,.$$

Since the sets $\alpha_i^{-1}(n_i)$ are recognizable subsets of $M_i$, $(i = 1, 2)$, the required decomposition of $Y$ is obtained. ∎

## Exercises

**1.1** Let $M'$ be a monoid, $M$ a submonoid of $M'$. Show that if $X' \in \mathrm{Rec}(M')$, then $X' \cap M \in \mathrm{Rec}(M)$. Give an example showing that $\mathrm{Rec}(M)$ is in general not contained in $\mathrm{Rec}(M')$, even if $M \in \mathrm{Rec}(M')$. (Hint (Perrin): Consider $M = (ab^+)^* \in \mathrm{Rec}(\{a, b\}^*)$.)

**1.2** Let $M$ be a monoid. Define a *finite automaton $\mathcal{A}$ over $M$* by a finite set of states $Q$, an initial state $q_-$, a set of final states $Q_+$ and a next state function $Q \times M \to Q$ satisfying the following conditions

$$\begin{aligned} &q \cdot 1 = q && (q \in Q) \\ &q \cdot mm' = (q \cdot m) \cdot m' && (q \in Q,\ m, m' \in M)\,. \end{aligned}$$

The subset of $M$ recognized by $\mathcal{A}$ is by definition $|\mathcal{A}| = \{m \in M \mid q_- \cdot m \in Q_+\}$. Show that $X \in \mathrm{Rec}(M)$ if and only if $X$ is recognized by a finite automaton over $M$. (For further discussion on these lines, see Walljasper (1970) and Vogel (1972).)

**1.3** Let $G$ be a group. Show that $X \in \mathrm{Rec}(G)$ if and only if there exists an invariant subgroup $H$ of $G$ of finite index (that is $G/H$ is finite) such that $X$ is a union of cosets of $H$. Show that a subgroup of $G$ is recognizable if and only if it is of finite index.

**1.4** Let $M$ be a monoid, $X \in \mathrm{Rec}(M)$. Show that for any $Y \subset M$, $Y^{-1}X = \{m \mid Ym \cap X \neq \emptyset\}$ is a recognizable subset of $M$. (Hint: use Exercise I.3.6.)

# 2 Rational Sets

In this section, we study the rational subsets of a monoid and their relation to recognizable subsets.

**Definition** Let $M$ be a monoid. The family $\mathrm{Rat}(M)$ of *rational subsets* of $M$ is the least family $\mathcal{R}$ of subsets of $M$ satisfying the following conditions:

$$\text{(i)} \qquad \emptyset \in \mathcal{R}\,,\ \{m\} \in \mathcal{R} \text{ for all } m \in M\,; \tag{2.1}$$

$$\text{(ii)} \qquad \text{if } X, Y \in \mathcal{R}, \text{ then } X \cup Y, XY \in \mathcal{R}\,; \tag{2.2}$$

$$\text{(iii)} \qquad \text{if } X \in \mathcal{R}, \text{ then } X^+ = \cup_{n \geq 1} X^n \in \mathcal{R}\,. \tag{2.3}$$

In presence of (i) and (ii), the condition (iii) is equivalent to

$$\text{(iii}'\text{)} \qquad X \in \mathcal{R} \implies X^* \in \mathcal{R}\,.$$

Assume indeed $X^+ \in \mathcal{R}$. Since $\{1\} \in \mathcal{R}$ by (i), it follows by (ii) that $X^* = \{1\} \cup X^+ \in \mathcal{R}$. Conversely, if $X, X^* \in \mathcal{R}$, then by (ii) $X^+ = XX^* \in \mathcal{R}$.

Any subset $X$ of $M$ obtained from the singletons by a finite number of unions, products and plus or star operations is in $\mathrm{Rat}(M)$. Moreover, the family of subsets of $M$ obtained in that way, together with the empty set satisfies conditions (i)–(iii), and therefore is the family $\mathrm{Rat}(M)$. Thus a rational subset of $M$ is either empty or can be expressed, starting with singletons by a finite number of unions, products, and plus or stars. Such an expression is called a *rational expression*. It is the simplest way to show that a given set is rational.

**Example 2.1** Any subset of a finite monoid is rational.

**Example 2.2** Let $A$ be an alphabet, and let $A^\oplus$ be the free commutative monoid generated by $A$. We claim that $X$ is a rational subset of $A^\oplus$ if and only if $X$ is a finite union of sets of the form

$$xy_1^* y_2^* \cdots y_n^* \quad (n \geq 0,\ x, y_1, \ldots, y_n \in A^\oplus)\,. \tag{2.4}$$

Unions of sets (2.4) are also called *semilinear*. Clearly, any set of the form (2.4) is rational, thus any semilinear set is rational. Next, if $X, Y \subset A^\oplus$, then $(X \cup Y)^* = X^*Y^*$, and $(xy_1^*y_2^* \cdots y_n^*)^* = x^*y_1^*y_2^* \cdots y_n^*$. This shows that semilinear sets are closed under the star operation. The empty set and the singletons are semilinear, further semilinear sets are obviously closed under union and product. Thus any rational set is semilinear. This proves that the semilinear sets are exactly the rational subsets of $A^\oplus$.

**Example 2.3** If $A$ is an alphabet, then the rational subsets are, according to Kleene's Theorem, exactly the languages recognized by finite automata.

Thus Kleene's Theorem can be formulated as follows:

**Theorem 2.1** (Kleene) *Let $A$ be a (finite) alphabet. Then* $\mathrm{Rat}(A^*) = \mathrm{Rec}(A^*)$.

In view of this theorem, we also call regular languages indistinctly rational or recognizable languages.

We now prove that rational sets are closed under morphism.

**Proposition 2.2** *Let $M, M'$ be monoids, and let $\alpha : M \to M'$ be a morphism. If $X \in \mathrm{Rat}(M)$, then $\alpha(X) \in \mathrm{Rat}(M')$. Further if $\alpha$ is surjective, then for any $X' \in \mathrm{Rat}(M')$, there is a set $X \in \mathrm{Rat}(M)$ such that $\alpha(X) = X'$.*

*Proof.* Let $\mathcal{R}$ be the family of subsets $X$ of $M$ such that $\alpha(X) \in \mathrm{Rat}(M')$. Then $\emptyset \in \mathcal{R}$ and $\{m\} \in \mathcal{R}$ for $m \in M$. Next

$$\alpha(X \cup Y) = \alpha(X) \cup \alpha(Y),\ \alpha(XY) = \alpha(X)\alpha(Y),\ \alpha(X^+) = (\alpha(X))^+ \quad (2.5)$$

for any subsets $X, Y$ of $M$. Thus $X, Y \in \mathcal{R}$ implies that $X \cup Y, XY, X^+ \in \mathcal{R}$. Thus $\mathcal{R}$ satisfies conditions (2.1), (2.2), (2.3). Consequently $\mathcal{R} \supset \mathrm{Rat}(M)$ and the first statement is proved.

Consider now the family $\mathcal{S}$ of subsets $X'$ of $M'$ such that $X' = \alpha(X)$ for some $X \in \mathrm{Rat}(M)$. Since $\alpha$ is surjective, $\{m'\} \in \mathcal{S}$ for all $m' \in M'$. Obviously $\emptyset \in \mathcal{S}$. In view of (2.5), $\mathcal{S}$ is closed under union, product and the plus operation. Thus $\mathcal{S} \supset \mathrm{Rat}(M')$. ∎

**Corollary 2.3** *Let $\alpha$ be an isomorphism from $M$ onto $M'$. Then $X \in \mathrm{Rat}(M)$ if and only if $\alpha(X) \in \mathrm{Rat}(M')$.* ∎

Note that the second part of Proposition 2.2 only claims the existence of a rational set $X$ such that $\alpha(X) = X' \in \mathrm{Rat}(M')$. Obviously this does not imply that any subset $X$ of $M$ with $\alpha(X) \in \mathrm{Rat}(M')$ is rational. In particular, the inverse image $\alpha^{-1}(X')$ is generally not rational for rational subsets $X'$ of $M'$.

**Example 2.4** Consider, as in Example 1.5 the alphabet $A = \{a, b\}$ and the morphism $\gamma : A^* \to \mathbb{Z}$ defined by $\gamma(w) = |w|_a - |w|_b$ ($w \in A^*$). Then $\{0\} \in \mathrm{Rat}(\mathbb{Z})$, and $\gamma^{-1}(0) = \{w \in A^* \mid |w|_a = |w|_b\} = D_1^* \notin \mathrm{Rat}(A^*)$.

Although Kleene's Theorem is not true in arbitrary monoids, there is a weakened version for finitely generated monoids.

**Proposition 2.4** (McKnight 1964) *Let $M$ be a finitely generated monoid. Then* $\mathrm{Rec}(M) \subset \mathrm{Rat}(M)$.

*Proof.* Since $M$ is finitely generated, there exist an alphabet $A$ and a surjective morphism $\alpha : A^* \to M$. Let $X \in \mathrm{Rec}(M)$. Then $\alpha^{-1}(X) \in \mathrm{Rec}(A^*)$ by Proposition 1.3. By Kleene's Theorem, $\alpha^{-1}(X) \in \mathrm{Rat}(A^*)$. In view of Proposition 2.2, $\alpha(\alpha^{-1}(X)) = X \in \mathrm{Rat}(M)$. ∎

Proposition (2.4) is not true in monoids which are not finitely generated. Consider indeed such a monoid $M$. Then $M \in \mathrm{Rec}(M)$, but $M \notin \mathrm{Rat}(M)$ in view of the following lemma.

**Lemma 2.5** *Let $M$ be a monoid. For any $X \in \mathrm{Rat}(M)$, there exists a finitely generated submonoid $M_1$ of $M$ such that $X \subset M_1$.*

*Proof.* Let $\mathcal{R}$ be the family of subsets $X$ of $M$ contained in some finitely generated submonoid of $M$. Obviously $\emptyset \in \mathcal{R}$ and $\{m\} \in \mathcal{R}$ for $m \in M$. Next let $X, Y \in \mathcal{R}$, and let $R, S$ be finite subsets of $M$ such that $X \subset R^*$, $Y \subset S^*$. Then $X \cup Y, XY \subset (R \cup S)^*$ and $X^* \subset R^*$. Consequently $X \cup Y, XY, X^* \in \mathcal{R}$ and $\mathcal{R} \supset \mathrm{Rat}(M)$.

**Proposition 2.6** *Let $M$ be a monoid. If $X \in \mathrm{Rat}(M)$ and $Y \in \mathrm{Rec}(M)$, then $X \cap Y \in \mathrm{Rat}(M)$.*

*Proof.* Let $X$ be a rational subset of $M$. Then there exists a finitely generated submonoid $M_1$ of $M$ such that $X \subset M_1$, and consequently $X \in \mathrm{Rat}(M_1)$. Next, there is an alphabet $A$ and a morphism $\alpha : A^* \to M$ that maps $A^*$ onto $M_1$. Thus by the second part of Proposition 2.2, there is a rational language $X' \subset A^*$ such that $\alpha(X') = X$. Let $Y$ be a recognizable subset of $M$. Then $Y' = \alpha^{-1}(Y)$ is a recognizable subset of $A^*$ by Proposition 1.3. In view of Kleene's Theorem, $Z' = X' \cap Y'$ is a regular, thus a rational language, and $\alpha(Z') \in \mathrm{Rat}(M)$ by Proposition 2.2. Since

$$\alpha(Z') = \alpha(X' \cap \alpha^{-1}(Y)) = \alpha(X') \cap Y = X \cap Y\,,$$

it follows that $X \cap Y \in \mathrm{Rat}(M)$. ■

The following example shows that the intersection of two rational sets is not necessarily rational.

**Example 2.5** Let $M = \{a\}^* \times \{b,c\}^*$, and consider the sets

$$X = (a,b)^*(1,c)^* = \{(a^n, b^n c^k) \mid n, k \geq 0\}\,,$$
$$Y = (1,b)^*(a,c)^* = \{(a^n, b^k c^n) \mid n, k \geq 0\}\,.$$

Clearly, $X, Y \in \mathrm{Rat}(M)$. Suppose that

$$Z = X \cap Y = \{(a^n, b^n c^n) \mid n \geq 0\}$$

is rational, and define a morphism $\pi : M \to \{b,c\}^*$ by $\pi(a,1) = 1, \pi(1,b) = b, \pi(1,c) = c$. Then $\pi(Z) = \{b^n c^n \mid n \geq 0\}$ would be a rational subset of $\{b,c\}^*$ by Proposition 2.2. Thus $Z$ is not rational.

Sometimes the notion of starheight of a rational set is useful. Let $M$ be a monoid, and define inductively sets $\mathrm{Rat}_0(M) \subset \mathrm{Rat}_1(M) \subset \cdots$ by:

$$\begin{array}{ll} X \in \mathrm{Rat}_0(M) & \text{if and only if } X \text{ is a finite subset of } M\,; \\ X \in \mathrm{Rat}_{h+1}(M) & \text{if and only if } X \text{ is a finite union of sets} \\ & \text{of the form } Y_1Y_2\cdots Y_n\,, \end{array}$$

where either $Y_i$ is a singleton or $Y_i = Z_i^*$ for some $Z_i \in \mathrm{Rat}_h(M)$. It is readily shown (Exercise 2.1) that

$$Rat(M) = \bigcup_{h \geq 0} Rat_h(M)\,.$$

The sets in $\mathrm{Rat}_h \setminus \mathrm{Rat}_{h-1}$ are said to have *starheight* $h$.

We use starheight in the proof of the following result which gives an interpretation of rational sets in groups.

**Theorem 2.7** (Anissimow and Seifert (1975)) *Let $G$ be a group, and let $H$ be a subgroup of $G$. Then $H$ is finitely generated if and only if $H$ is a rational subset of $G$.*

*Proof.* For any subset $X$ of $G$, let $\langle X \rangle$ denote the subgroup generated by $X$, and let $X^{-1} = \{x^{-1} \mid x \in X\}$. Then $\langle X \rangle = (X \cup X^{-1})^*$. This shows that a finitely generated subgroup is rational.

In order to prove the converse, we first consider the following situation. Let $X$ be a subset of $G$ such that

$$X = z_1 T_1^* z_2 T_2^* \cdots z_n T_n^* z_{n+1} \tag{2.6}$$

with $z_1, \ldots, z_{n+1} \in G$, $T_1, \ldots, T_n \subset G$, and define

$$y_i = z_1 z_2 \cdots z_i \quad i = 1, \ldots, n+1 \tag{2.7}$$

$$S_i = y_i T_i y_i^{-1} \quad i = 1, \ldots, n$$

$$X' = y_{n+1} \cup S_1 \cup \cdots \cup S_n\,. \tag{2.8}$$

Then we claim:

$$\langle X \rangle = \langle X' \rangle\,. \tag{2.9}$$

Indeed, observe that by (2.6), $y_{n+1}, y_{n+1}^{-1} \in \langle X \rangle$. Further

$$S_i = (z_1 \cdots z_i T_i z_{i+1} \cdots z_{n+1}) y_{n+1}^{-1}\,.$$

Thus $S_i \subset \langle X \rangle$, whence $X' \subset \langle X \rangle$ and $\langle X' \rangle \subset \langle X \rangle$. Next

$$S_i^* (y_i T_i y_i^{-1})^* = y_i T_i^* y_i^{-1}\,.$$

Since $z_1 = y_1$ and $z_i = y_{i-1}^{-1} y_i$ $(2 \le i \le n+1)$,

$$X = y_1 T_1^* y_1^{-1} y_2 T_2^* y_2^{-1} \cdots y_n T_n^* y_n^{-1} y_{n+1} = S_1^* S_2^* \cdots S_n^* y_{n+1}\,.$$

Thus $X \subset \langle X' \rangle$, whence $\langle X \rangle \subset \langle X' \rangle$. This proves (2.9).

Consider now a subgroup $H$ of $G$ such that $H \in \mathrm{Rat}(G)$. Since $H = \langle H \rangle$, $H$ has a rational set of generators. We have to show that $H$ has a set of generators of starheight 0. Let $R$ be the rational set of generators of minimal starheight $h$, and assume $h > 0$. Then

$$R = X_1 \cup X_2 \cup \cdots \cup X_r\,,$$

where each $X_k$, $(1 \le k \le r)$ has the form (2.6), and at least one $X_k$ has starheight $h$. Set

$$R' = X_1' \cup X_2' \cup \cdots \cup X_r'\,,$$

where each $X'_k$ is deduced from $X_k$ by (2.7) and (2.8). Then clearly $R'$ has starheight $h-1$. By (2.9), each $X_k$ is contained in $\langle R' \rangle$, and conversely each $X'_k$ is contained in $R$. Thus $\langle R \rangle = \langle R' \rangle = H$, and $R'$ is a set of generators of $H$ of starheight $h-1$, in contradiction with the minimality of $h$. Thus $h=0$ and the theorem is proved. ∎

In the case of free groups, a more precise description of rational sets can be given. Consider an alphabet $A = \{a_1, \dots, a_n\}$, let $\bar{A} = \{\bar{a} \mid a \in A\}$, and set $C = A \cup \bar{A}$. Let $A^{(*)}$ be the free group generated by $A$ (see Section II.3), and let $\delta : C^* \to A^{(*)}$ be the canonical morphism. As already mentioned, there exists an injection $\iota : A^{(*)} \to C^*$ which associates, to each element $u \in A^{(*)}$, the unique reduced word $\iota(u) = w \in \rho(C^*)$ such that $\delta(w) = u$. The following result describes a property of the mapping $\rho$.

**Proposition 2.8** (Benois (1969)) *Let $K \subset C^*$ be a regular language. Then the language $\rho(K)$ is also regular.*

This theorem yields the following characterization of rational subsets of $A^{(*)}$.

**Theorem 2.9** (Benois (1969)) *Let $K \subset A^{(*)}$. Then $K \in \mathrm{Rat}(A^{(*)})$ if and only if $\iota(K)$ is a regular language.*

*Proof.* Let $K \in \mathrm{Rat}(A^{(*)})$. In view of Proposition 2.2, there exists a regular language $K' \subset C^*$ such that $\delta(K') = K$. Thus $K'' = \rho(K')$ is regular by Proposition 2.8. Now $\rho = \iota \circ \delta$, whence $K'' = \iota(K)$. Thus $\iota(K)$ is regular. Conversely, assume $\iota(K) \in \mathrm{Rat}(C^*)$. Then the homomorphic image $\delta(\iota(K)) = K$ is in $\mathrm{Rat}(A^{(*)})$ by Proposition 2.2. ∎

The following corollary is interesting.

**Corollary 2.10** (Fliess (1971)) $\mathrm{Rat}(A^{(*)})$ *is closed under intersection and complementation.*

*Proof.* It suffices to show closure under complementation. Let $K \in \mathrm{Rat}(A^{(*)})$. Then $\iota(K) \in \mathrm{Rat}(C^*)$ by Theorem 2.9. Next $\rho(C^*)$ is regular, thus $\rho(C^*) \setminus \iota(K)$ is regular. Since $\iota(K) \subset \rho(C^*)$, it follows that $\delta(\rho(C^*) \setminus \iota(K)) = A^{(*)} \setminus K \in \mathrm{Rat}(A^{(*)})$ by Proposition 2.2. ∎

It remains to prove Proposition 2.8. For this, we first establish a lemma derived from (Fliess 1971). Consider an alphabet $B$, and let $X \subset B^*$ be an arbitrary language. Define a function $\lambda_X$ from $B^*$ into the subsets of $B^*$ as follows. For $w, w' \in B^*$, $w' \in \lambda_X(w)$ if and only if there exists a factorization

$$w = x_0 b_1 x_1 b_2 \cdots x_{r-1} b_r x_r$$

with $r \geq 0$, $x_0, x_1, \dots, x_r \in X$, $b_1, \dots, b_r \in B$ such that

$$w' = b_1 b_2 \cdots b_r\,.$$

Thus $\lambda_X(w)$ consists of all subwords of $w$ obtained by deleting, in $w$, factors in $X$ which are separated by letters.

**Lemma 2.11** *For any $X \subset B^*$, and for any regular language $K \subset B^*$, $\lambda_X(K)$ is a regular language.*

*Proof.* Let $\mathcal{A} = \langle B, Q, q_-, Q_+ \rangle$ be a finite automaton recognizing $K$. Set $K_{p,q} = \{w \in B^* \mid p \cdot w = q\}$ for $p, q \in Q$. Let $s \notin Q$, and let $\mathcal{B} = \langle B, Q \cup s, s, Q' \rangle$ be the nondeterministic finite automaton with next state function define by

$$\begin{aligned} q \in p \cdot b &\iff bX \cap K_{p,q} \neq \emptyset \qquad b \in B\,,\ p, q \in Q\,; \\ q \in s \cdot b &\iff XbX \cap K_{q_-,q} \neq \emptyset \qquad b \in B\,,\ q \in Q\,. \end{aligned}$$

Next, let

$$Q' = \begin{cases} Q_+ & \text{if } X \cap K = \emptyset\,; \\ s \cup Q_+ & \text{if } X \cap K \neq \emptyset\,. \end{cases}$$

Then clearly

$$\lambda_X(K) = |\mathcal{B}| = \{w \in B^* \mid s \cdot w \cap Q' \neq \emptyset\}\,.$$ ■

*Proof* of Proposition 2.8. Choose in Lemma 2.11 $X = D_n^* = \rho^{-1}(1)$, and $B = C$. Then for $w \in C^*$,

$$\rho(w) = \lambda_{D_n^*}(w) \cap \rho(C^*)\,.$$

Consequently, for $K \in \mathrm{Rat}(C^*)$, $\rho(K) = \lambda_{D_n^*}(K) \cap \rho(C^*)$. Since $\rho(C^*)$ is regular, $\rho(K)$ is a regular language. ■

## Exercises

**2.1** Show that $\mathrm{Rat}(M) = \bigcup_{h \geq 0} \mathrm{Rat}_h(M)$. Compute $\mathrm{Rat}_h(A^\oplus)$ for $h \geq 0$.

**2.2** Let $G$ be a group. Show that $K \in \mathrm{Rat}(G)$ implies $K^{-1} \in \mathrm{Rat}(G)$.

**2.3** Prove the following group theoretic result: let $G$ be a finitely generated group, and let $H$ be a subgroup of $G$. If $H$ is of finite index, then $H$ is finitely generated (Hint. Use Exercise 1.3.)

**2.4** (Anissimow and Seifert (1975)) Prove the following theorem of Howson: The intersection of two finitely generated subgroups of a free group is again a finitely generated subgroup.

**2.5** Show that for any rational subset $K$ of $A^{(*)}$, $\delta^{-1}(K)$ is a context-free language. (Hint (Sakarovitch 1977). Write $K = (K^{-1})^{-1} \cdot 1$ and use Exercise I.3.6.)

**2.6** Show that in Proposition 2.8 and in the following statements, $\rho$ can be replaced by $\rho'$ and in fact by $\rho_I$ as defined in Section II.3.

# 3 Rational Relations

A relation can be considered as a subset of the Cartesian product of two sets, or as a mapping from the first set into the set of subsets of the second. For the exposition of rational transductions we use in this section the first, "static" aspect, and in the next section the second, more "dynamic" point of view. Rational transductions (more precisely rational relations) are defined as rational subsets of the product of two monoids. Several characterizations are given. The examples are grouped in Section 5.

**Definition** Let $A$ and $B$ be alphabets. A *rational* (resp. *recognizable*) *relation over $A$ and $B$* is a rational (resp. recognizable) subset of the monoid $A^* \times B^*$.

The family $\mathrm{Rec}(A^* \times B^*)$ of recognizable relations is described by Mezei's Theorem 1.5. More precisely, we have

**Proposition 3.1**
(i) $\mathrm{Rec}(A^* \times B^*) \subsetneq \mathrm{Rat}(A^* \times B^*)$ *;*
(ii) *if* $X, Y \in \mathrm{Rec}(A^* \times B^*)$*, then* $XY \in \mathrm{Rec}(A^* \times B^*)$*.*

Thus, recognizable relations are closed under product. It follows from the proof below that they are not closed under the star operation.

*Proof.* (i) Since $A^* \times B^*$ is a finitely generated monoid, then inclusion $\mathrm{Rec}(A^* \times B^*) \subset \mathrm{Rat}(A^* \times B^*)$ follows from Proposition 2.4. To show that the inclusion is proper, let $a \in A$, $b \in B$ and consider $X = (a,b)^* = \{(a^n, b^n) \mid n \geq 0\}$. Clearly $X$ is a rational relation. Assume $X$ is recognizable, let $C = \{\bar{a}, \bar{b}\}$, and consider the morphism $\gamma : C^* \to A^* \times B^*$ defined by $\gamma(\bar{a}) = (a, 1)$, $\gamma(\bar{b}) = (1, b)$. Then $\gamma^{-1}(X) = \{w \in C^* \mid |w|_{\bar{a}} = |w|_{\bar{b}}\}$ is recognizable, thus a regular language. This yields the contradiction.

(ii). In view of Mezei's Theorem,

$$X = \bigcup_{i=1}^{n} R_i \times S_i \,, \quad Y = \bigcup_{j=1}^{m} R'_j \times S'_j \,,$$

with $R_i, R'_j \in \mathrm{Rat}(A^*)$, $S_i, S'_j \in \mathrm{Rat}(B^*)$. Consequently

$$XY = \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} R_i R'_j \times S_i S'_j \,,$$

and $R_i R'_j \in \mathrm{Rat}(A^*)$, $S_i S'_j \in \mathrm{Rat}(B^*)$. By Mezei's Theorem, $XY \in \mathrm{Rec}(A^* \times B^*)$. ∎

We extend the notion of *copy* defined in Section I.3 as follows: $A^* \times B^*$ is a copy of $A'^* \times B'^*$ if $A^*$ is a copy of $A'^*$ and $B^*$ is a copy of $B'^*$. Then $A^* \times B^*$ and $A'^* \times B'^*$ are isomorphic, and recognizable and rational relations are preserved through isomorphism by Corollaries 1.4 and 2.3.

The following characterizations of rational relations are fundamental.

They allow to express rational relations by means of regular languages and morphisms of free monoids, and thus rely the algebraic definition to more combinatorial notions. Further, we shall see later that in view of the theorem, a family of languages is closed under rational transduction if and only if it is closed under morphism, inverse morphism and intersection with regular sets.

**Theorem 3.2** (Nivat (1968)) *Let $A$ and $B$ be alphabets. The following conditions are equivalent:*
(i) $X \in \mathrm{Rat}(A^* \times B^*)$ *;*
(ii) *There exist an alphabet $C$, two morphisms $\phi : C^* \to A^*$, $\psi : C^* \to B^*$ and a regular language $K \subset C^*$ such that*

$$X = \{(\phi z, \psi z) \mid z \in K\} ;$$

(iii) *There exist an alphabet $C$, two alphabetic morphisms $\alpha : C^* \to A^*$, $\beta : C^* \to B^*$ and a regular language $K \subset C^*$ such that*

$$X = \{(\alpha z, \beta z) \mid z \in K\} ;$$

(iv) *There exist an alphabet $C$, two alphabetic morphisms $\alpha : C^* \to A^*$, $\beta : C^* \to B^*$ and a local regular language $K \subset C^*$ such that*

$$X = \{(\alpha z, \beta z) \mid z \in K\} ;$$

*If $A \cap B = \emptyset$, then* (i) *is equivalent to*
(v) *There exist a regular language $K \subset (A \cup B)^*$ such that*

$$X = \{(\pi_A z, \pi_B z) \mid z \in K\} ,$$

*where $\pi_A$ and $\pi_B$ are the projections of $(A \cup B)^*$ onto $A^*$ and $B^*$ respectively.*

A couple $(\phi, \psi)$ of morphisms $\phi : C^* \to B^*$ and $\psi : C^* \to A^*$ is called a *bimorphism.*

*Proof.* The implications (iv)⇒(iii)⇒(ii) are obvious. We prove (ii)⇒(i). Define $\gamma : C^* \to A^* \times B^*$ by $\gamma z = (\phi z, \psi z)$ $(z \in C^*)$. Then $\gamma$ is a morphism and $\gamma(K) = X$. Since $K \in \mathrm{Rat}(C^*)$, $X \in \mathrm{Rat}(A^* \times B^*)$ by Proposition 2.2.

Next, we prove (iii)⇒(iv). There exist an alphabet $C'$, an alphabetic morphism $\gamma : C'^* \to C^*$ and a local regular language $K' \subset C'^*$ such that $\gamma(K') = K$ (see for instance Section I.4). Thus $X = \{(\alpha(\gamma z'), \beta(\gamma z')) \mid z' \in K'\}$ and the morphisms $\alpha \circ \gamma$, $\beta \circ \gamma$ are alphabetic.

Assume now $A \cap B = \emptyset$, and define $\pi : (A \cup B)^* \to A^* \times B^*$ by $\pi z = (\pi_A z, \pi_B z)$. Obviously $\pi$ is a surjective morphism. Thus, if $X \in \mathrm{Rat}(A^* \times B^*)$, there exists, by the second part of Proposition 2.2, a regular language $K \subset (A \cup B)^*$ such that $\pi(K) = X$. This proves (i)⇒(v).

Conversely, if (v) holds, then $\pi(K) = X \in \mathrm{Rat}(A^* \times B^*)$ by the first part of Proposition 2.2.

Finally, we prove (i)⇒(iii). Assume $X \in \mathrm{Rat}(A^* \times B^*)$. If $A \cap B = \emptyset$, then (iii) follows from (v). Otherwise, let $A'^* \times B'^*$ be a copy of $A^* \times B^*$ with $A' \cap B' = \emptyset$, let $\omega_A : A^* \to A'^*$, $\omega_B : B^* \to B'^*$ be the copy isomorphisms and set $X' = \{(\omega_A x, \omega_B y) \mid (x, y) \in X\}$. Then $X'$ is a rational relation, and in view of (v), $X' = \{(\pi_{A'} z, \pi_{B'} z) \mid z \in K\}$ for some regular language $K \subset (A' \cup B')^*$. Consequently $X = \{((\omega_A^{-1} \circ \pi_{A'})z, (\omega_B^{-1} \circ \pi_{B'})z) \mid z \in K\}$. ■

Theorem 3.3 can be used to derive an iteration lemma for rational relations.

**Lemma 3.3** (Iteration Lemma for Rational Relations) *Let $X \subset A^* \times B^*$ be a rational relation. There exists an integer $N \geq 1$ such that any $(w, w') \in X$ with $|w| + |w'| \geq N$ admits a factorization*

$$(w, w') = (x, x')(u, u')(y, y') \qquad x, u, y \in A^* \,,\ x', u', y' \in B^*$$

*such that*
(i) $0 < |u| + |u'| \leq N$ *;*
(ii) $(x, x')(u, u')^*(y, y') \subset X$ *.*

*Proof.* After a copy, we may assume $A \cap B = \emptyset$, and by Theorem 3.2(v), $X = \{(\pi_A z, \pi_B z) \mid z \in K\}$ for some regular language $K$. Since $|z| = |\pi_A z| + |\pi_B z|$, then lemma follows directly from the iteration lemmas for regular languages (see Section I.4) applied to $K$. ■

**Remark** Several versions of the iteration lemma for regular languages can be transposed to rational relations. Thus we may assume that in addition to (i) and (ii), the following condition holds:

$$|x| + |x'| + |u| + |u'| \leq N \,.$$

The definition of rational relations holds also for arbitrary monoids.

**Definition** Let $M$ and $M'$ be monoids. A *rational relation* over $M$ and $M'$ is a rational subset of $M \times M'$.

We shall see in the next section how this definition can be used to define interesting rational transductions. Here we just note the following:

**Proposition 3.4** *Let $M, M'$ be monoids. Then $X$ is a rational relation over $M$ and $M'$ if and only if there exists an alphabet $C$, two morphisms $\alpha : C^* \to M$, $\beta : C^* \to M'$ and a regular language $K \subset C^*$ such that $X = \{(\alpha z, \beta z) \mid z \in K\}$.*

*Proof.* Let $X \in \mathrm{Rat}(M \times M')$. Then $X \subset N$, in view of Lemma 2.5, where $N$ is a finitely generated submonoid of $M \times M'$. Thus there exist an alphabet $C$, and a morphism $\gamma : C^* \to M \times M'$ such that $\gamma(C^*) = N$. Since $X \in \mathrm{Rat}(N)$, $X = \gamma(K)$ for some regular language $K \subset C^*$. Next define $\alpha : C^* \to M$, $\beta : C^* \to M'$ by $\gamma z = (\alpha z, \beta z)$, $(z \in C^*)$. This yields the desired representation. The converse is clear. ■

## Exercises

**3.1** Let $M$ be a finitely generated, infinite monoid. Show that $X = \{(m, m) \mid m \in M\}$ is a rational and not a recognizable subset of $M \times M$.

**3.2** Let $A$ be an alphabet with at least two letters. Show that the relation $R = \{(w, \tilde{w}) \mid w \in A^*\}$ is not rational.

**3.3** Give a counter example to the following version of the Iteration Lemma: For $X \in \mathrm{Rat}(A^* \times B^*)$ there is an integer $N \geq 1$ such that for any $(s, s') \in X$ and for any factorization

$$(s, s') = (z_1, z_1')(w, w')(z_2, z_2') \quad \text{with } |w| + |w'| \geq N \,,$$

$(w, w')$ admits a factorization $(w, w') = (x, x')(u, u')(y, y')$ such that $0 < |u| + |u'| \leq N$ and

$$(z_1, z_1')(x, x')(u, u')^*(y, y')(z_2, z_2') \subset X \,.$$

**3.4** A *right linear system of equations over* $A^* \times B^*$ is a system of equations of the form

$$\xi_i = \sum_{j=1}^{N} C_{i,j}\xi_j + D_i \quad i = 1, \ldots, N \,,$$

where $C_{i,j}, D_i \subset A^* \times B^*$. The system is *strict* if and only if $(1, 1) \notin C_{i,j}$ for $i, j = 1, \ldots, N$. A vector $X = (X_1, \ldots, X_N)$ of subsets of $A^* \times B^*$ is a *solution* of the system if and only if

$$X_i = \bigcup_{j=1}^{N} C_{i,j}X_j \cup D_i \quad i = 1, \ldots, N \,,$$

a) Show that a strict right linear system has a unique solution.
b) Show that $R \subset A^* \times B^*$ is a rational relation if and only if $R$ is a component of the solution of a strict right linear system of equations with $C_{i,j}, D_i$ finite. (Hint. Use the fact that a) and b) hold in free monoids and apply Nivat's Theorem.)

# 4 Rational Transductions

The "static" notion of rational relation is now transformed into the "dynamic" notion of rational transduction.

A *transduction* $\tau$ from $A^*$ to $B^*$ is a function from $A^*$ into the set $\mathfrak{P}(B^*)$ of subsets of $B^*$. For commodity, we write $\tau : A^* \to B^*$. The *domain* $\mathrm{dom}(\tau)$ and the *image* $\mathrm{im}(\tau)$ are defined by

$$\mathrm{dom}(\tau) = \{x \in A^* \mid \tau(x) \neq \emptyset\} \,;$$
$$\mathrm{im}(\tau) = \{y \in B^* \mid \exists x \in A^* : y \in \tau(x)\} \,.$$

The transduction $\tau$ is extended to a mapping from $\mathfrak{P}(A^*)$ into $\mathfrak{P}(B^*)$ by setting

$$\tau(X) = \bigcup_{x \in X} \tau(x) \quad X \subset A^* \,.$$

The *graph* of $\tau$ is the relation $R$ defined by

$$R = \{(x, y) \in A^* \times B^* \mid y \in \tau(x)\} \,.$$

Conversely, for any relation $R \subset A^* \times B^*$, the transduction $\tau : A^* \to B^*$ *defined* by $R$ is given by

$$\tau(x) = \{y \in B^* \mid (x, y) \in R\} \,.$$

**Definition** A transduction $\tau : A^* \to B^*$ is *rational* if and only if its graph $R$ is a rational relation over $A$ and $B$.

Let $\tau : A^* \to B^*$ be a rational transduction, and let $R \subset A^* \times B^*$ be the graph of $\tau$. The monoids $A^* \times B^*$ and $B^* \times A^*$ are isomorphic. Thus the relation

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}$$

is rational, and the transduction $\tau^{-1} : B^* \to A^*$ defined by $R^{-1}$ is rational. $\tau^{-1}$ is the *inverse* transduction of $\tau$. Clearly

$$\tau^{-1}(Y) = \{x \in A^* \mid \tau(x) \cap Y \neq \emptyset\} \qquad Y \subset B^* .$$

In general, $\tau(\tau^{-1}(Y)) \neq Y$, and $\tau^{-1}(\tau(X)) \neq X$, $(X \subset A^*)$. The domain $\mathrm{dom}(\tau)$ and the image $\mathrm{im}(\tau)$ are homomorphic images of the rational relation $R$, and consequently are regular languages.

Let $\tau_1, \tau_2 : A^* \to B^*$ be rational transductions, and let $R_1, R_2$ be the graphs of $\tau_1$ and $\tau_2$. We denote by $\tau_1 \cup \tau_2$, $\tau_1\tau_2$ and $\tau_1^+$ the transductions with graphs $R_1 \cup R_2, R_1R_2, R_1^+$. Obviously these transductions are rational. They verify:

$$(\tau_1 \cup \tau_2)(x) = \tau_1(x) \cup \tau_2(x)\,; \quad (\tau_1\tau_2)(x) = \bigcup_{x_1x_2=x} \tau_1(x_1)\tau_2(x_2)\,;$$

$$\tau_1^+(x) = \bigcup\{\tau_1(x_1) \cdots \tau_n(x_n) \mid n \geq 1,\ x_1 \cdots x_n = x\}\,.$$

If $\mathrm{dom}(\tau_1) \cap \mathrm{dom}(\tau_2) = \emptyset$, we also write $\tau_1 + \tau_2$ instead of $\tau_1 \cup \tau_2$. Finally, we associate to $\tau : A^* \to B^*$ a transduction $\tilde{\tau} : A^* \to B^*$ by setting $\tilde{\tau}(x) = (\tau(\tilde{x}))\tilde{}$. Let $R$ be the graph of $\tau$, and let $\tilde{R}$ be the graph of $\tilde{\tau}$. Then $\tilde{R} = \{(\tilde{x}, \tilde{y}) \mid (x, y) \in R\}$. The formulas

$$(X \cup Y)\tilde{} = \tilde{X} \cup \tilde{Y}\,; \quad (XY)\tilde{} = \tilde{Y}\tilde{X}\,; \quad (X^+)\tilde{} = (\tilde{X})^+ \quad (X, Y \subset A^* \times B^*)$$

show that $\tilde{R}$ is rational if and only if $R$ is rational. Thus the transduction $\tilde{\tau}$, the *reversal* of $\tau$ is rational if and only if $\tau$ is rational.

Nivat's Theorem proved in the preceding section can be formulated as follows for rational transductions.

**Theorem 4.1** (Nivat (1968)) *Let $A$ and $B$ be alphabets. The following conditions are equivalent:*

(i) *$\tau : A^* \to B^*$ is a rational transduction;*

(ii) *There exist an alphabet $C$, two morphisms $\phi : C^* \to A^*$, $\psi : C^* \to B^*$ and a regular language $K \subset C^*$ such that*

$$\tau(x) = \psi(\phi^{-1}(x) \cap K) \quad x \in A^*\,; \tag{4.1}$$

(iii) *There exist an alphabet $C$, two alphabetic morphisms $\alpha : C^* \to A^*$, $\beta : C^* \to B^*$ and a regular language $K \subset C^*$ such that*

$$\tau(x) = \beta(\alpha^{-1}(x) \cap K) \quad x \in A^*\,;$$

(iv) *There exist an alphabet $C$, two alphabetic morphisms $\alpha : C^* \to A^*$, $\beta : C^* \to B^*$ and a local regular language $K \subset C^*$ such that*

$$\tau(x) = \beta(\alpha^{-1}(x) \cap K) \quad x \in A^*\,;$$

*Further, if $A \cap B = \emptyset$, then* (i) *is equivalent to*
(v) *There exist a regular language $K \subset (A \cup B)^*$ such that*

$$\tau(x) = \pi_B(\pi_A^{-1}(x) \cap K) \quad x \in A^* ;$$

*where $\pi_A$ and $\pi_B$ are the projections of $(A \cup B)^*$ onto $A^*$ and $B^*$ respectively.* ∎

From (4.1), we deduce immediately that

$$\tau^{-1}(y) = \phi(\psi^{-1}(y) \cap K) \quad y \in B^* .$$

It follows also from (4.1) that

$$\tau(X) = \psi(\phi^{-1}(X) \cap K) \quad X \subset A^* .$$

Thus:

**Corollary 4.2** *Each rational transduction preserves rational and algebraic languages. That is, for each rational transduction $\tau$, $\tau(X)$ is rational if $X$ is rational, and $\tau(X)$ is algebraic if $X$ is algebraic.* ∎

**Example 4.1** Let $A = \{a, b\}, B = \{c, d\}$, and consider the transduction $\tau : A^* \to B^*$ defined by

$$\tau(x) = \begin{cases} \emptyset & \text{if } x \notin a^+b^* ; \\ (c^+d)^n c^{2m} d & \text{if } x = a^n b^m, \ n \geq 1, \ m \geq 0 . \end{cases}$$

Obviously, $\operatorname{dom}(\tau) = a^+b^*$, $\operatorname{im}(\tau) = (c^+d)^+(c^2)^*d$. We claim that the transductions $\tau$ is rational. This can be shown in several ways. First, let $R$ be the graph of $\tau$. Then

$$R = (\{a\} \times c^+d)^+(b, c^2)^*(1, d) \in \operatorname{Rat}(A^* \times B^*) .$$

Next, let $C = \{r, s, t, u\}$ and define $\phi : C^* \to A^*$, $\psi : C^* \to B^*$ by

$$\phi(r){=}a , \ \ \phi(s) = 1 , \ \ \phi(t){=}b , \ \ \phi(u) = 1 ;$$
$$\psi(r){=}d , \ \ \psi(s) = c , \ \ \psi(t){=}c^2 , \ \psi(u) = d .$$

Let $K = (s^+r)^+t^*u$. Then $\phi K = a^+b^*, \psi K = (c^+d)^+(c^2)^*d$. Further

$$\phi^{-1}(a^n b^m) \cap K = (s^+r)^n t^m u \quad n \geq 1, \ m \geq 0 ,$$

thus $\tau(x) = \psi(\phi^{-1}(x) \cap K)$ for all $x \in A^*$.

Finally, since $A \cap B = \emptyset$, we can represent $\tau$ by projections. Consider indeed the regular language

$$K' = ac\{c, dac\}^*d(bc^2)^*d \subset (A \cup B)^* .$$

Then $\pi_A(K') = aa^*b^*$. Next, if $x = a^n b^m$, $(n \geq 1, m \geq 0)$, then

$$\pi_A^{-1}(x) \cap K' = ac(c^*dac)^{n-1}c^*d(bc^2)^m d ,$$
$$\pi_B(\pi_A^{-1}(x) \cap K') = c(c^*dc)^{n-1}c^*dc^{2m}d = (c^+d)^n c^{2m} d .$$

As for rational relations, the definition of rational transductions can be extended to arbitrary monoids.

**Definition** Let $M, M'$ be monoids. A *rational transduction* $\tau : M \to M'$ is a function from $M$ into $\mathfrak{P}(M')$ such that the graph $R = \{(m, m') \mid m' \in \tau(m)\}$ of $\tau$ is a rational subset of $M \times M'$.

From Proposition 3.4, we immediately obtain:

**Proposition 4.3** *Let $M, M'$ be monoids. A transduction $\tau : M \to M'$ is rational if and only if there exist an alphabet $C$, two morphisms $\alpha : C^* \to M$, $\beta : C^* \to M'$ and a rational language $K \subset C^*$ such that*

$$\tau(m) = \beta(\alpha^{-1}(m) \cap K) \qquad m \in M\,. \qquad \blacksquare$$

If $X \subset M$, then

$$\tau(X) = \beta(\alpha^{-1}(X) \cap K)\,. \tag{4.2}$$

Thus, if $X$ is a recognizable subset of $M$, then $\alpha^{-1}(X)$ is recognizable, hence regular, $\alpha^{-1}(X) \cap K$ is regular, hence rational, and finally $\tau(X)$ is a rational subset of $M'$. Note that $\tau(X)$ is not necessarily recognizable, and that $\tau(X)$ is not necessarily rational if $X$ is rational. This follows from Examples 1.5 and 2.4 since morphisms and inverse morphisms are particular rational transductions.

We now consider composition of rational transductions. If $\tau : M \to M'$ and $\tau' : M' \to M''$ are transductions, then the composition $\tau' \circ \tau : M \to M''$ is defined by

$$(\tau' \circ \tau)(m) = \tau'(\tau(m)) = \bigcup_{m' \in \tau(m)} \tau'(m')\,.$$

First we settle the case of free monoids.

**Theorem 4.4** (Elgot and Mezei (1965)) *Let $A, B, C$ be alphabets, and let $\tau : A^* \to B^*$ and $\tau' : B^* \to C^*$ be rational transductions. Then the transduction $\tau' \circ \tau : A^* \to C^*$ is rational.*

We first prove the theorem in a special case. The general case follows then from the special case.

**Lemma 4.5** *Let $A, B, C$ be three pairwise disjoint alphabets. Set $A' = A \cup B$, $C' = B \cup C$, $D = A \cup B \cup C$, and let*

$$\alpha : A'^* \to B^*\,, \quad \beta : C'^* \to B^*\,, \quad \alpha' : D^* \to A'^*\,, \quad \beta' : D^* \to C'^*$$

*be the projections. Then $\beta^{-1} \circ \alpha = \beta' \circ \alpha'^{-1}$.*

Lemma 4.5 is represented in Figure III.1.

*Proof.* The mappings $\beta^{-1} \circ \alpha$ and $\beta' \circ \alpha'^{-1}$ are morphisms of the semigroup $A'^*$ into the (multiplicative) semigroup $\mathfrak{P}(C'^*)$. Thus it suffices to prove that they are equal on $A' \cup 1$. First

$$\beta^{-1} \circ \alpha(1) = \beta^{-1}(1) = C^*\,, \; \beta' \circ \alpha'^{-1}(1) = \beta'(C^*) = C^*\,.$$

$$\begin{tikzcd}
 & (A \cup B \cup C)^* \arrow[dl, "\alpha'"'] \arrow[dr, "\beta'"] & \\
(A \cup B)^* \arrow[rr, dashed, "\beta^{-1} \circ \alpha = \beta' \circ \alpha'^{-1}"] \arrow[dr, "\alpha"'] & & (B \cup C)^* \arrow[dl, "\beta"] \\
 & B^* &
\end{tikzcd}$$

Figure III.1

Then, for $a \in A$, $\beta^{-1} \circ \alpha(a) = \beta^{-1}(1) = C^*$ and $\beta' \circ \alpha'^{-1}(a) = \beta'(C^* a C^*) = C^*$. Finally, if $b \in B$, then $\beta^{-1} \circ \alpha(b) = \beta^{-1}(b) = C^* b C^*$ and $\beta' \circ \alpha'^{-1}(b) = \beta'(C^* b C^*) = C^* b C^*$. This proves the lemma. ∎

*Proof* of Theorem 4.4. After a copy if necessary, we may assume that the alphabet $A, B, C$ are pairwise disjoint. Set $A' = A \cup B$, $C' = B \cup C$. In view of Nivat's Theorem, there exists a regular language $K \subset A'^*$ such that

$$\tau(x) = \alpha(\pi^{-1}(x) \cap K) \qquad x \in A^* , \tag{4.3}$$

where $\pi : A'^* \to A^*$ and $\alpha : A'^* \to B^*$ are the projections. Next, there is a regular language $M \subset C'^*$ such that

$$\tau'(y) = \omega(\beta^{-1}(y) \cap M) \qquad y \in B^* , \tag{4.4}$$

where $\beta : C'^* \to B^*$ and $\omega : C'^* \to C^*$ are the projections. Thus we have Figure III.2.

$$\begin{tikzcd}
 & A'^* \arrow[r, "\cap K"] \arrow[dl, "\pi"'] & A'^* \arrow[dr, "\alpha"] & & C'^* \arrow[r, "\cap M"] \arrow[dl, "\beta"'] & C'^* \arrow[dr, "\omega"] & \\
A^* \arrow[rrr, "\tau"'] & & & B^* \arrow[rrr, "\tau'"'] & & & C^*
\end{tikzcd}$$

Figure III.2

According to Lemma 4.5, $\beta^{-1} \circ \alpha = \beta' \circ \alpha'^{-1}$ where $D = A \cup B \cup C$, and $\beta', \alpha'$ are the projections of $D^*$ onto $C'^*$ and $A'^*$ respectively. Thus the above diagram can be completed to Figure III.3.

Next, setting $\tau'' = \tau' \circ \tau$, we have by (4.3), (4.4), for $x \in A^*$,

$$\tau''(x) = \omega\big[(\beta^{-1} \circ \alpha)(\pi^{-1}(x) \cap K) \cap M\big] .$$

Since $\beta^{-1} \circ \alpha = \beta' \circ \alpha'^{-1}$,

$$\begin{aligned} \tau''(x) &= \omega\big[(\beta' \circ \alpha'^{-1})(\pi^{-1}(x) \cap K) \, \cap M\big] \\ &= \omega\big[\beta'\big((\pi \circ \alpha')^{-1}(x) \cap \alpha'^{-1}(K)\big) \, \cap M\big] . \end{aligned} \tag{4.5}$$

$$\begin{tikzcd}
 & & & D^* \arrow[dl, "\alpha'"'] \arrow[dr, "\beta'"] & & & \\
 & A'^* \arrow[r, "\cap K"] \arrow[dl, "\pi"'] & A'^* \arrow[dr, "\alpha"] & & C'^* \arrow[r, "\cap M"] \arrow[dl, "\beta"'] & C'^* \arrow[dr, "\omega"] & \\
A^* \arrow[rrr, "\tau"'] & & & B^* \arrow[rrr, "\tau'"'] & & & C^*
\end{tikzcd}$$

Figure III.3

Define $\psi : \omega \circ \beta' : D^* \to C^*$, $\phi : \pi \circ \alpha' : D^* \to A^*$, and set $K' = \alpha'^{-1}(K)$, $M' = \beta'^{-1}(M)$, $N = K' \cap M'$. Then (4.5) implies

$$\begin{aligned} \tau''(x) &= \omega\bigl[\beta'(\phi^{-1}(x) \cap K') \cap M\bigr] = \omega\bigl[\beta'(\phi^{-1}(x) \cap K' \cap M')\bigr] \\ &= \psi(\phi^{-1}(x) \cap N)\,. \end{aligned} \tag{4.6}$$

Since $N \subset T^*$ is a regular language, the transduction $\tau''$ is rational by (4.6). ∎

If $M, M', M''$ are arbitrary monoids, then the composition of two rational transductions $\tau : M \to M'$ and $\tau' : M' \to M''$ is not necessarily rational.

**Example 4.2** Let $a, b, c$ be letters, $M = a^*$, $M' = b^* \times c^*$, $M'' = \{b, c\}^*$. Define $\tau : M \to M'$ and $\tau' : M' \to M''$ by

$$\tau(a^n) = (b^n, c^n)\,, \quad \tau'(b^n, c^k) = b^n c^k \quad (n, k \geq 0)\,.$$

The graphs $R$ and $R'$ of $\tau$ and $\tau'$ are:

$$R = (a, (b, c))^*\,, \quad R' = ((b, 1), b)^*((1, c), c)^*\,,$$

thus $\tau$ and $\tau'$ are rational. Next

$$(\tau' \circ \tau)(a^n) = b^n c^n \quad n \geq 0\,.$$

Since the image $\mathrm{im}(\tau' \circ \tau) = \{b^n c^n \mid n \geq 0\}$ is not a regular language, $\tau' \circ \tau$ is not rational.

Despite this example, we have

**Proposition 4.6** *Let $M, M'$ be monoids, and let $B$ be an alphabet. If $\tau : M \to B^*$ and $\tau' : B^* \to M'$ are rational transductions, then $\tau' \circ \tau$ is rational.*

*Proof.* In view of Proposition 4.3,

$$\begin{aligned} &\tau(m) = \beta(\alpha^{-1}(m) \cap K) \quad m \in M \\ &\tau'(y) = \delta(\gamma^{-1}(y) \cap L) \quad y \in B^* \end{aligned}$$

where $A, C$ are alphabets, $K \in \mathrm{Rat}(A^*)$, $L \in \mathrm{Rat}(Z^*)$, and

$$\alpha : A^* \to M, \quad \beta : A^* \to B^*, \quad \gamma : C^* \to B^*, \quad \delta : C^* \to M'$$

are morphisms. It follows that

$$(\tau' \circ \tau)(m) = \delta[(\gamma^{-1} \circ \beta)(\alpha^{-1}(m) \cap K) \cap L] \quad m \in M \, .$$

Since $\gamma^{-1} \circ \beta : A^* \to C^*$ is the composition of two rational transductions, it is a rational transduction by Elgot and Mezei's Theorem. Thus

$$(\gamma^{-1} \circ \beta)(x) = \psi(\phi^{-1}(x) \cap N) \quad x \in A^*$$

for some alphabet $D$, morphisms $\psi : D^* \to A^*$, $\phi : D^* \to B^*$ and some $N \in \mathrm{Rat}(D^*)$. Thus as in the proof of Theorem 4.4,

$$(\tau' \circ \tau)(m) = (\delta \circ \psi)[(\alpha \circ \phi)^{-1}(m) \cap (\phi^{-1}(K) \cap N \cap \psi^{-1}(L))] \quad m \in M \, ,$$

showing that $\tau' \circ \tau$ is rational. ■

It is natural to look for a generalization of rational transductions involving context-free languages. This can be done by developing a theory of algebraic sets in arbitrary monoids analogue to the theory of rational sets (see Eilenberg (1978), also Exercises 4.5, 4.6). This yields an analogue of Nivat's Theorem. We prefer in this context to take that analogue as a definition.

**Definition** A transduction $\tau : A^* \to B^*$ is *algebraic* if there exist an alphabet $C^*$, two morphisms $\alpha : C^* \to A^*$, $\beta : C^* \to B^*$ and a context-free language $X \subset C^*$ such that

$$\tau(x) = \beta(\alpha^{-1}(x) \cap X) \quad x \in A^* \, .$$

It follows immediately that $\tau(L)$ is context-free if $L \subset A^*$ is regular, and it is easy to see that $\tau(L)$ is not necessarily context-free if $L$ is context-free. The following result is proved in the same way as Theorem 4.4.

**Proposition 4.7** *Let $\tau : A^* \to B^*$ and $\tau' : B^* \to C^*$ be transductions. If one of them is rational and the other is algebraic, then $\tau' \circ \tau$ is algebraic.* ■

If both transductions are algebraic, then $\tau' \circ \tau$ is not necessarily algebraic.

## Exercises

**4.1** Give an example of a transduction $\tau : A^* \to B^*$, and of subsets $X \subset A^*$, $Y \subset B^*$ such that $\tau^{-1}(\tau(X)) \neq X$ and $\tau(\tau^{-1}(Y)) \neq Y$.

**4.2** Prove Proposition 4.7.

**4.3** Give an example of two algebraic transductions $\tau, \tau'$ such that the composition $\tau' \circ \tau$ is not algebraic.

**4.4** Consider the Dyck reduction $\rho : C_n^* \to C_n^*$. Show that $\rho$ is an algebraic transduction. Show that $\rho$ is not a rational transduction.

**4.5** (Eilenberg (1978)) Let $M$ be a monoid and let $V$ be an alphabet disjoint from $M$. The set $M[V]$ of words

$$w = m_0\xi_1 m_1 \cdots m_{k-1}\xi_k m_k$$

with $k \geq 0$, $m_0, \dots, m_k \in M$, $\xi_1, \dots, \xi_k \in V$ is a monoid when multiplication of $w$ with $w' = n_0\zeta_1 \cdots \zeta_\ell n_\ell$ is defined by

$$ww' = m_0\xi_1 \cdots \xi_k(m_k n_0)\zeta_1 \cdots \zeta_\ell n_\ell\,.$$

An *algebraic grammar* $G = \langle V, M, \mathcal{P}\rangle$ over $M$ is given by a finite subset $\mathcal{P}$ of $V \times M[V]$. Derivations are defined as in free monoids. The language $L_G(\xi)$ generated by $\xi$ is the set of all $m \in M$ derived from $\xi$. Languages generated by algebraic grammars over $M$ are called *algebraic subsets* of $M$.
a) Show that for any algebraic grammar $G = \langle V, M, \mathcal{P}\rangle$, there exists an algebraic grammar $G_1 = \langle V, M_1, \mathcal{P}\rangle$, where $M_1$ is a finitely generated submonoid of $M$, such that $L_G(\xi) = L_{G_1}(\xi)$ for all $\xi \in V$.
b) Show that $X$ is an algebraic subset of $M$ if and only if there exists an alphabet $A$, a morphism $\phi : A^* \to M$ and a context-free language $L \subset A^*$ such that $\phi(L) = X$.
c) Show that any rational subset of $M$ is algebraic.
d) Show that a transduction $\tau : A^* \to B^*$ is algebraic in the sense given in the text if and only if its graph is an algebraic subset of $A^* \times B^*$.

**4.6** (continuation of 4.5) Show that in a free commutative monoid $A^\oplus$, any algebraic subset is rational. (This is Parikh's Theorem. For a proof, see Conway (1971), Ginsburg (1966).) Show that the same result holds in any commutative monoid.

**4.7** Nivat's Theorem implies that morphisms and inverse morphisms can be represented by means of projections, inverse projections, and intersection with regular sets. Give such representations explicitly.

**4.8** (Elgot and Mezei (1965)) Let $\tau : A^* \to B^*$ be a rational transduction. Then $\tau = \tau_0 + \tau_\infty$, where

$$\begin{aligned} \tau_0(x) = \tau(x) \quad \tau_\infty(x) = \emptyset \quad &\text{if } \mathrm{Card}(\tau x) < \infty\,;\\ \tau_0(x) = \emptyset \quad \tau_\infty(x) = \tau(x) \quad &\text{if } \mathrm{Card}(\tau x) = \infty\,. \end{aligned}$$

Show that $\tau_0, \tau_\infty$ are rational transductions.

**4.9** Let $M, M', M''$ be finitely generated monoids, and let $\tau : M \to M'$, $\tau' : M' \to M''$ be transductions. Show that if one of them is recognizable (that is its graph is recognizable) and the other is rational, then $\tau' \circ \tau : M \to M''$ is rational, and even recognizable, provided $M, M', M''$ are free monoids. Show that if $\tau$ and $\tau'$ are recognizable, then $\tau' \circ \tau$ is always recognizable.

# 5 Examples

The explicit description of a rational transduction is a simple method to prove that certain transformations preserve regular and context-free languages. Rational transductions can also be used to prove that a given language is context-free, by representing it as the image of a language "known" to be context-free. One of the most important applications of rational transductions will be shown in later chapters: They are used as a tool of comparison of subfamilies of the family of context-free languages. The proof of the rationality of a given transduction is frequently realized through one of the versions of Nivat's Theorem, or else through a rational expression for the graph of the transduction.

**5.1** The *identity mapping* $x \mapsto x$ from $A^*$ into itself is a rational transduction. This is straightforward by Nivat's Theorem. The graph of this mapping is

$$\Delta = \{(x,x) \mid x \in A^*\} = \Big(\bigcup_{a\in A}(a,a)\Big)^* .$$

**5.2** The *rational constants* $\tau_K : A^* \to B^*$ defined for a fixed regular language $K \subset B^*$ by $\tau_K(x) = K$ are rational. The graph of $\tau_K$ is $A^* \times K$.

**5.3** Any *morphism*, any *inverse morphism* is a rational transduction.

**5.4** A *rational substitution* is a substitution $\sigma : A^* \to B^*$ such that $\sigma(a) \in \mathrm{Rat}(B^*)$ for $a \in A$. The graph of $\sigma$ is

$$\Big(\bigcup_{a\in A}\{a\} \times \sigma(a)\Big)^* ;$$

thus $\sigma$ is a rational transduction.

**5.5** The *union* (and of course the *intersection*) with a regular language is performed by a rational transduction. Let $K \subset A^*$ be a regular language, and consider the transduction $w \mapsto w \cup K$ from $A^*$ into $A^*$. Then its graph is $\Delta \cup (A^* \times K)$.

**5.6** The *product* with a rational language: let $K \in \mathrm{Rat}(A^*)$ and consider the transduction $w \mapsto Kw$ for $w \in A^*$. Its graph is $(\{1\} \times K)\Delta$.

**5.7** The (left or right) *quotient* by a rational language. Let $K \subset A^*$ be a rational language. The transduction $A^* \to A^*$ defined by

$$w \mapsto K^{-1}w = \{z \in A^* \mid \exists u \in K : uz = w\}$$

is the inverse of the transduction of Example 5.6, and consequently is rational. (This proves that $K^{-1}L$ is context-free if $L$ is a context-free language.)

**5.8** The transduction $\tau : A^* \to A^*$ with $\tau(x) = x^{-1}K = \{y \in A^* \mid xy \in K\}$ is rational if $K \subset A^*$ is a regular language. Consider indeed its graph

$$R = \{(x,y) \mid xy \in K\} .$$

Let $\bar{A} = \{\bar{a} \mid a \in A\}$ be a copy of $A$, disjoint from $A$, set $C = A \cup \bar{A}$, and define morphisms $\alpha, \beta, \gamma : C^* \to A^*$ by

$$\begin{array}{llll} \alpha(a) = a\,, & \beta(a) = 1\,, & \gamma(a) = a & \quad a \in A\,; \\ \alpha(\bar{a}) = 1\,, & \beta(\bar{a}) = a\,, & \gamma(\bar{a}) = a & \quad \bar{a} \in \bar{A}\,. \end{array}$$

Consider the regular language $K' = \gamma^{-1}(K) \cap A^*\bar{A}^* \subset C^*$. Any word $z \in K'$ factorizes in a unique way into $z = xy$, $(x \in A^*, y \in \bar{A}^*)$. It follows that

$$R = \{(\alpha z, \beta z) \mid z \in K'\} .$$

**5.9** The transduction $A^* \to A^*$ which associates to any word $x \in A^*$ the set of its subwords (resp. factors, prefixes, suffixes) is rational. Let indeed $\bar{A}, C, \alpha, \gamma$ be as above. Then the set of subwords of $x$ is $\alpha(\gamma^{-1}(x))$, the set of factors of $x$ is $\alpha(\gamma^{-1}(x) \cap \bar{A}^* A^* \bar{A}^*)$, etc. (Note that the set of prefixes of $x$ is $x(A^*)^{-1}$. Thus the rationality of this transduction follows from Example 5.7.)

**5.10** Let $\tau : A^* \to A^*$ be defined for $x = a_1 a_2 \cdots a_n$, $(n \geq 1, a_i \in A)$ by $\tau(x) = a_1 a_3 a_5 \cdots$, and $\tau(1) = 1$. With the notations of Example 5.8,

$$\tau(x) = \alpha(\gamma^{-1}(x) \cap [(A\bar{A})^* \cup (A\bar{A})^* A]) .$$

**5.11** The transduction $\tau : a^* \to \{b, c\}^*$ defined by

$$\tau(a^n) = \begin{cases} b^n & n \text{ even} , \\ c^n & n \text{ odd} , \end{cases}$$

is rational. Indeed, its graph is $(a^2, b^2)^* \cup (a, c)(a^2, c^2)^*$.

**5.12** According to Greibach (1973), the "hardest" context-free language is the language $L_0 \subset A^*$, with $A = \{a_1, a_2, \bar{a}_1, \bar{a}_2, \cent, |, \#\}$ defined in the following way. Set $B = A \setminus \#$. Then $x \in L_0$ if and only if either $x = 1$ or

$$x = u_1 | v_1 | w_1 \# u_2 | v_2 | w_2 \# \cdots \# u_n | v_n | w_n ,$$

with $u_1, w_1, \ldots, u_n, w_n \in B^*$, $v_1, \ldots, v_n \in \{a_1, a_2, \bar{a}_1, \bar{a}_2\}^*$ and $v_1 v_2 \cdots v_n \in \cent D_2'^*$. In order to show that $L_0$ is indeed context-free, consider two transductions $\tau, \tau_1 : A^* \to A^*$:

$$\tau(z) = \# B^* | z | B^* \quad \tau_1(z) = B^* | \cent z | B^* \quad (z \in A^*) .$$

In view of Example 5.6, these transductions are rational. Consequently, the transduction $\tau' = \tau_1 \tau^*$ is rational. Since $L_0 = 1 \cup \tau'(D_2'^*)$, $L_0$ is context-free.

**5.13** The transduction $A^* \to A^*$ which associates to any $x \in A^*$ its reversal $\tilde{x}$ is not rational if $\mathrm{Card}(X) \geq 2$ since its graph $\{(x, \tilde{x}) \mid x \in A^*\}$ is not a rational relation (Exercise 3.2). (This is an example of an irrational relation that preserves regular and context-free languages.)

All the transductions given above are unary operations. Some of the examples, like product, union, etc. are binary operations. Thus we consider them now as binary transductions.

**5.14** The transduction $(x, y) \mapsto xy$ from $A^* \times A^*$ into $A^*$ is rational. Its graph is indeed

$$X = \{(a, 1, a) \mid a \in A\}^* \{(1, a, a) \mid a \in A\}^* .$$

**5.15** The *shuffle* $x \sqcup\!\sqcup\, y$ of two words $x, y \in A^*$ is defined as

$$\begin{aligned} x \sqcup\!\sqcup\, y = &\{x_1 y_1 \cdots x_n y_n \mid x_1, \ldots, x_n , y_1, \ldots, y_n \in A^*, \\ &\quad x_1 \cdots x_n = x , \ y_1 \cdots y_n = y\} . \end{aligned}$$

The transduction $(x, y) \mapsto x \sqcup\!\sqcup\, y$ is rational, since its graph is $X^*$, with $X$ given as in Example 5.14.

**5.16** Finally, we show that *addition* of nonnegative integers in some fixed base $k \geq 2$ can be performed by a rational transduction. (For $k = 1$, this is done by Example 5.14.)

Let $k \geq 2$, and let $\Bbbk = \{0, 1, \ldots, k-1\}$. The empty word of $\Bbbk^*$ is denoted by $\varepsilon$. For each $x = a_0 a_1 \cdots a_n$, $(a_i \in \Bbbk)$, let

$$\langle x \rangle = \sum_{i=0}^{n} a_i k^{n-i}$$

be the integer represented by $x$ in base $k$. Then $\langle \varepsilon \rangle = 0$, and for any $m \in \mathbb{N}$, there is a unique $x \in \Bbbk^* \setminus 0\Bbbk^*$ such that $\langle x \rangle = m$. The transduction

$$\bigoplus : \Bbbk^* \times \Bbbk^* \to \Bbbk^*$$

which associates to any $(x, y) \in \Bbbk^* \times \Bbbk^*$ the unique word $z \in \Bbbk^* \setminus 0\Bbbk^*$ such that $\langle z \rangle = \langle x \rangle + \langle y \rangle is rational.$ The construction is in three steps. The first step just adds leading zeros in order to make the two arguments of the same length.

Consider a transduction

$$\tau_1 : \Bbbk^* \times \Bbbk^* \to (\Bbbk \times \Bbbk)^* .$$

In order to avoid confusion, elements of $\Bbbk \times \Bbbk$ are noted $[a, b]$. If $x = a_1 a_2 \cdots a_n$, $y = b_1 b_2 \cdots b_m$, $(a_i, b_i \in \Bbbk)$, $\tau_1(x, y)$ is defined to be equal either to

$$[0,0]^+ [a_1, 0] \cdots [a_{n-m}, 0][a_{n-m+1}, b_1] \cdots [a_n, b_m]$$

or to

$$[0,0]^+ [0, b_1] \cdots [0, b_{m-n}][a_1, b_{m-n+1}] \cdots [a_n, b_m]$$

according to $n \geq m$ or $m \geq n$. Define $R, S, T \subset \Bbbk^* \times \Bbbk^* \times (\Bbbk \times \Bbbk)^*$ by

$$\begin{aligned} S &= \{(\varepsilon, b, [0, b]) \mid b \in \Bbbk\}^* \cup \{(a, \varepsilon, [a, 0]) \mid a \in \Bbbk\}^* , \\ T &= \{(a, b, [a, b] \mid a, b \in \Bbbk\}^* , \quad R = (\varepsilon, \varepsilon, [0, 0])^+ ST . \end{aligned}$$

Then $R$ is rational and is the graph of $\tau_1$. Next, we define

$$\tau_2 : (\Bbbk \times \Bbbk)^* \to \Bbbk^*$$

to perform the addition step: For

$$w = [a_0, b_0] \cdots [a_n, b_n] , \quad a_0 = b_0 = 0 , \ x = a_0 \cdots a_n , \ y = b_0 \cdots b_n , \qquad (5.1)$$

$\tau_2(w)$ will be the word $z = c_0 \cdots c_n$ such that $\langle z \rangle = \langle x \rangle + \langle y \rangle$. For this, we introduce an auxiliary alphabet $B = \{0, 1\} \times \Bbbk \times \Bbbk \times \Bbbk$ composed of quadruples $[r, c, a, b]$. During the computation, $c + r \cdot k$ represents the number $a+b+1$ or $a+b+0$, according to the existence or not of a "carry" from a previous computation. Formally, we define morphisms

$$\phi : B^* \to (\Bbbk \times \Bbbk)^*, \quad \psi : B^* \to \Bbbk^*$$

by

$$\phi[r,c,a,b] = [a,b] \quad \psi[r,c,a,b] = c \qquad [r,c,a,b] \in B\,.$$

Next, we define a local regular language

$$\begin{aligned}
&K = (UB^* \cap B^*V) \setminus B^*WB^* \\
&U = \{[0,1,0,0],[0,0,0,0]\}\,, \quad V = \{[r,c,a,b] \mid c + rk = a + b\}\,, \\
&B^2 \setminus W = \{[r,c,a,b][r',c',a',b'] \mid c + rk = a + b + r'\}\,.
\end{aligned}$$

Then, for $w$ given by (5.1),

$$\phi^{-1}(w) \cap K = [r_0, c_0, a_0, b_0] \cdots [r_n, c_n, a_n, b_n]$$

with $a_n + b_n = c_n + kr_n$, $a_i + b_i + r_{i+1} = c_i + kr_i$ $(i = n-1, \ldots, 0,\ r_0 = 0)$. Hence $\psi(\phi^{-1}(w) \cap K) = \tau_2(w)$ and $\tau_2$ is rational. The final step just deletes initial zeros from the result. It is performed by the transduction

$$\tau_3 : \mathbb{k}^* \to \mathbb{k}^*\,, \quad \tau_3(z) = (0^*)^{-1}z \cap \mathbb{k}^* \setminus 0\mathbb{k}^*$$

which is clearly rational. Thus, by Proposition 4.6, the transduction $\bigoplus = \tau_3 \circ \tau_2 \circ \tau_1$ is rational.

(For further properties of arithmetic operations considered as rational transductions, see Eilenberg (1974) and Exercises 5.3, 5.4.)

## Exercises

**5.1** Let $A = \{a_1, a_2, \ldots, a_k\}$. Define an order on $A^*$ by

$$x \underset{\ell}{<} y \iff \begin{cases} y = xu \text{ for some } u \in A^+ \text{ or} \\ x = ua_iv,\ y = ua_jv' \text{ and } i < j\,; \end{cases}$$

this is the lexicographic order. The "radix" order is defined by

$$x \underset{r}{<} y \iff \begin{cases} |x| < |y| \\ |x| = |y| \text{ and } x \underset{\ell}{<} y\,. \end{cases}$$

Show that the four transductions from $A^*$ into itself which associate to $x$ the sets

$$\{y \mid y > x\} \quad (\text{resp. } \{y \mid y < x\})$$

are rational for both orders.

**5.2** Show that a transduction $\tau : A^* \times B^* \to C^*$ is rational if and only if there are an alphabet $D$, three morphisms

$$\alpha_1 : D^* \to A^*\,, \quad \alpha_2 : D^* \to B^*\,, \quad \beta : D^* \to C^*$$

and a regular language $K \subset D^*$ such that

$$\tau(x,y) = \beta(\alpha_1^{-1}(x) \cap \alpha_2^{-1}(y) \cap K) \quad (x,y) \in A^* \times B^*\,.$$

Show that for $R \subset A^*$, the transduction $\tau' : B^* \to C^*$ given by $\tau'(y) = \tau(R \times \{y\})$, $(y \in B^*)$ is rational if $R$ is regular, and is algebraic if $R$ is context-free. Use this to deduce Example 5.5 from Example 5.14.

**5.3** Show that multiplication $\bigotimes$ from $\mathbb{k}^* \times \mathbb{k}^*$ into $\mathbb{k}^*$ is not a rational transduction. (Hint (Messerschmidt). Compute for $k = 2$ the language $\otimes(10^*1 \times 1^*)$.)

**5.4** Show that for a fixed $q \geq 1$, the multiplication by $q{:}\mathbb{k}^* \to \mathbb{k}^*$ which associates to $x \in \mathbb{k}^*$ the word $x' \in \mathbb{k}^* \setminus 0\mathbb{k}^*$ such that $\langle x' \rangle = q \cdot \langle x \rangle$ is rational.

**5.5** Let $A = \{a, b\}$, and let $\sigma$ be the congruence generated by $baa \sim abb$. Show that the transduction $\tau : A^* \to A^*$ which associates to $x$ the class $[x]_\sigma = \{y \mid y \equiv x \pmod{\sigma}\}$ is rational. (Note that this is not true for all congruences: thus the result does not hold for the Lukasiewicz congruence $\lambda$ of Section II.4.)

# 6 Transducers

The machines realizing rational transductions are called transducers. As for transductions, transducers can be regarded either in a static or in a dynamic way. In the first case, a transducer is a finite nondeterministic acceptor reading on two tapes. It then recognizes the pairs of words of a rational relation. In the second case, the automaton reads input words on one tape, and prints output words on a second tape. The automaton thus realizes a rational transduction. Both aspects clearly are equivalent. In the following presentation, we adopt the second point of view which corresponds to the use of transductions as a tool for transformation of languages.

**Definition** A i*transducer* $\mathcal{T} = \langle A, B, Q, q_-, Q_+, E \rangle$ is composed of an *input alphabet* $A$, an *output alphabet* $B$, a finite set of *states* $Q$, an *initial state* $q_-$, a set of *final states* $Q_+$, and a *finite* set of *transitions* or *edges* $E$ satisfying

$$E \subset Q \times A^* \times B^* \times Q\,. \tag{6.1}$$

The terminology stems from Elgot and Mezei (1965) and Eilenberg (1974). Ginsburg (1975) uses the term "*a*-transducer", the letter "*a*" emphasizing the presence of accepting states. Transductions are defined by means of transducers in the paper of Elgot and Mezei (1965). They prove then that a transduction is realized by a transducer if and only if its graph is a rational relation.

Transducers have a graphical representation very similar to the usual representation of finite automata. Each state $q$ is represented by a circle, labeled $q$ an to each transition $e = (q, u, v, q')$ is associated an arrow directed from $q$ to $q'$ and labeled $u/v$. The initial state has an arrow entering in it, and final states are doubly circled.

**Example 6.1** Consider the transducer given by $A = B = \{a, b\}$, $Q = \{s, t\}$, $q_- = s$, $Q_+ = \{t\}$, $E = \{(s, a^2b, 1, s), (s, 1, 1, t), (t, a, a, t), (t, b, b, t)\}$. Its representation is shown in Figure III.4.

We now introduce some additional definitions. Consider the free monoid $E^*$ generated by the set $E$ of transitions. The empty word of $E^*$ is denoted by $\varepsilon$. Given a word

$$e = (p_1, u_1, v_1, q_1) \cdots (p_n, u_n, v_n, q_n)\,, \tag{6.2}$$

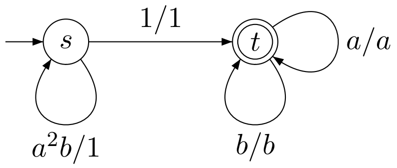

Figure III.4

the *label* of $e$ is the pair of words $|e| = (x, y)$ defined by $x = u_1 \cdots u_n$, $y = v_1 \cdots v_n$. By convention, $|\varepsilon| = (1, 1)$. Clearly the function $e \mapsto |e|$ is a morphism from $E^*$ into $A^* \times B^*$ which can be decomposed into two morphisms $\alpha : E^* \to A^*$, $\beta : E^* \to B^*$ defined by $|e| = (\alpha e, \beta e)$. $\alpha e$ and $\beta e$ are the *input label* and the *output label* of $e$. The word $e$ given by (6.2) is a *path* or a *computation* in $\mathcal{T}$ from $p_1$ to $q_n$ if and only if $q_i = p_{i+1}$, $(i = 1, \ldots, n-1)$. For $p, q \in Q$, $\Lambda(p, q)$ is the set of all paths from $p$ to $q$. By convention, $\varepsilon \in \Lambda(p, p)$ for all $p \in Q$. We extend the notation by setting

$$\Lambda(p, Q') = \bigcup_{q \in Q'} \Lambda(p, q) \qquad Q' \subset Q\,.$$

Finally, define

$$T(p, q) = \{|e| \,:\, e \in \Lambda(p, q)\}, \quad T(p, Q') = \{|e| \,:\, e \in \Lambda(p, Q')\}\,.$$

A path $e$ from $p$ to $q$ is *successful* if $p = q_-$ and $q \in Q_+$. Thus the set of all successful paths is $\Lambda(q_-, Q_+)$.

**Definition** The transduction $|\mathcal{T}| : A^* \to B^*$ realized by $\mathcal{T}$ is defined by

$$|\mathcal{T}|(x) = \{y \in B^* \mid (x, y) \in T(q_-, Q_+)\}\,. \tag{6.3}$$

Thus $y \in |\mathcal{T}|(x)$ if and only if there exists a successful path in $\mathcal{T}$ with label $(x, y)$. With the morphisms $\alpha$ and $\beta$, (6.3) can be reformulated as

$$|\mathcal{T}|(x) = \beta(\alpha^{-1}(x) \cap \Lambda(q_-, Q_+))\,. \tag{6.4}$$

**Example 6.1** (*continued*) The set of successful paths is

$$\Lambda(s, t) = (s, a^2b, 1, s)^*(s, 1, 1, t)\{(t, a, a, t), (t, b, b, t)\}^*\,.$$

The set of labels of successful paths is

$$T(s, t) = (a^2b, 1)^*\{(a, a), (b, b)\}^*$$

The transduction $\tau$ realized by the transducer is

$$\tau(x) = K^{-1}x \quad \text{with } K = (a^2b)^*\,.$$

**Theorem 6.1** *A transduction $\tau : A^* \to B^*$ is rational if and only if $\tau$ is realized by a transducer.*

*Proof.* Let $\mathcal{T} = \langle A, B, Q, q_-, Q_+, E\rangle$ be a transducer. The rationality of $|\mathcal{T}|$ follows immediately from (6.4), provided $\Lambda(q_-, Q_+)$ is a regular language. To show this, it suffices to show that the set $\Lambda(p, q)$ of all paths from $p$ to $q$ is regular. This follows from the fact that

$$\Lambda(p,q) = \Omega \cup (U_p E^* \cap E^* V_q) \setminus E^* W E^* \,,$$

where

$$\begin{aligned} &U_p = \{(q_1,u,v,q_2) \in E \mid q_1 = p\}\,, \quad V_q = \{(q_1,u,v,q_2) \in E \mid q_2 = q\}\,, \\ &W = \{(q_1,u_1,v_1,q_1')(q_2,u_2,v_2,q_2') \in E^2 \mid q_1' \neq q_2'\}\,, \quad \Omega = \Lambda(p,q) \cap \{\varepsilon\}\,. \end{aligned}$$

Conversely, let $\tau : A^* \to B^*$ be rational transduction. After a copy, we may assume $A \cap B = \emptyset$. Thus

$$\tau(x) = \pi_B(\pi_A^{-1}(x) \cap K) \qquad x \in A^*\,,$$

with $K \subset (A \cup B)^*$ a regular language and $\pi_A$, $\pi_B$ the projections of $(A\cup B)^*$ onto $A^*$ and $B^*$. Let $\mathcal{A} = \langle A \cup B, Q, q_-, Q_+\rangle$ be the finite automaton recognizing $K$, and define a transducer

$$\begin{aligned} &\mathcal{T} = \langle A, B, Q, q_-, Q_+, E\rangle \\ &E = \{(q, \pi_A(c), \pi_B(c), q\cdot c) \mid q \in Q, c \in A \cup B\}\,. \end{aligned} \tag{6.5}$$

Then $\mathcal{T}$ realizes $\tau$. ■

We easily obtain the following corollary

**Corollary 6.2** *Any rational transduction $\tau : A^* \to B^*$ can be realized by a transducer $\mathcal{T} = \langle A, B, Q, q_-, Q_+, E\rangle$ such that*

$$E \subset Q \times (A \cup \{1\}) \times (B \cup \{1\}) \times Q \tag{6.6}$$

*and further $Q_+$ consists of a single state $q_+ \neq q_-$, and $(p,u,v,q) \in E$ implies $p \neq q_+$ and $q \neq q_-$.*

*Proof.* The condition (6.6) is fulfilled with $E$ satisfying (6.5). Next, add to $Q$ two new states $q^0$ and $q^1$, and to $\mathcal{T}$the new transitions

$$\begin{aligned} &\{(q^0,u,v,q') \mid (q_-,u,v,q') \in E\} \\ &\{(q,u,v,q^1) \mid (q,u,v,q') \in E \text{ and } q' \in Q_+\} \end{aligned}$$

and

$$(q^0, 1, 1, q^1) \text{ if } q_- \in Q_+\,.$$

Let $\mathcal{T}'$ be the transducer obtained in this way with initial state $q^0$ and unique final state $q^1$. Then obviously $\tau = |\mathcal{T}'|$. ■

**Remark** If $\tau(1) = \emptyset$, then (6.6) can be replaced by

$$E \subset (Q \times A \times \{1\} \times Q) \cup (Q \times \{1\} \times B \times Q)\,.$$

Note that the proof of Theorem 6.1, and equation (6.4) give an effective procedure to construct a transducer from a bimorphism and conversely. For the construction of the bimorphism, it is frequently easier to take as alphabet the set of labels of transitions instead of the set of transitions itself.

**Example 6.1** (*continued*) Consider the alphabet $C$ composed of the three "letters" $a^2b/1$, $a/a$, $b/b$. Define morphisms $\phi$, $\psi$ from $C^*$ into $A^*$ by $\phi(u/v) = u$, $\psi(u/v) = v$. Then

$$T(s,t) = \{(\phi z, \psi z) \mid z \in R\} \qquad \text{with} \quad R = (a^2b/1)^*\{a/a, b/b\}^*\,.$$

**Example 6.2** Consider the transduction $\tau : A^* \to B^*$ with $A = \{a, b\}$, $B = \{c, d\}$ of Example 4.1 defined by

$$\tau(x) = \begin{cases} \emptyset & \text{if } x \notin a^+b^*\,; \\ (c^+d)^n c^{2m} d & \text{if } x = a^n b^m,\ n \geq 1,\ m \geq 0\,. \end{cases}$$

With the notations of this example, a finite nondeterministic automaton for $K = (s^+r)^+t^*u$ is given in Figure III.5. Thus we obtain the following transducer realizing $\tau$ (Figure III.6).

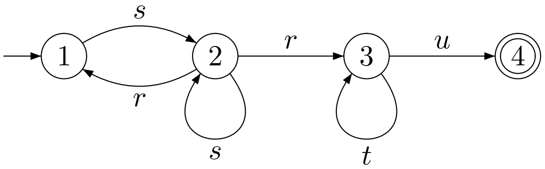

Figure III.5

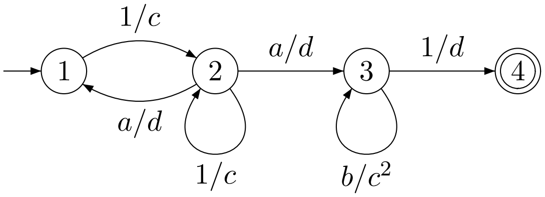

Figure III.6

## Exercise

**6.1** Let $\mathcal{T}$ be a transducer realizing a transduction $\tau$. Show how finite automata recognizing $\mathrm{dom}(\tau)$ and $\mathrm{im}(\tau)$ can be obtained from $\mathcal{T}$.

# 7 Matrix Representations

Matrix representations are another equivalent definition of rational transductions. They constitute a compact formulation of transducers, obtained by grouping in one matrix all output words corresponding to a fixed input word by considering all pairs of states. The multiplication of matrices corresponds then to the concatenation of paths in the transducer, and to the union of sets of output words of these paths.

Let $S$ be a semiring, and let $Q$ be a finite set. Then the set $S^{Q\times Q}$ of all $Q\times Q$-matrices with entries in $S$ is again a semiring for addition and multiplication of matrices induces by the operations in $S$ (see Section I.2). The identity matrix is denoted by $I$.

Let $A$ be an alphabet. A *morphism* $\mu : A^* \to S^{Q\times Q}$ is a monoid morphism from $A^*$ into the multiplicative monoid $S^{Q\times Q}$. Thus

$$\mu(xy) = \mu(x)\mu(y) \qquad x, y \in A^* \tag{7.1}$$

$$\mu(1) = I\,. \tag{7.2}$$

If only (7.1) is verified, then $\mu$ is a *semigroup morphism*. In this case, $\mu(A^*) = \{\mu(x) \mid x \in A^*\}$ is a monoid of $Q\times Q$-matrices with neutral element $\mu 1$, and $\mu 1$ is idempotent ($\mu 1 \cdot \mu 1 = \mu 1$) by (7.1). We are interested here in matrices whose entries are regular languages over the alphabet $B$. Thus the semiring $S$ is $\mathrm{Rat}(B^*)$. Consequently, the identity matrix $I$ is given by

$$I_{p,q} = \begin{cases} 1 & \text{if } p = q\,; \\ \emptyset & \text{otherwise.} \end{cases}$$

For simplicity, we frequently write 0 instead of $\emptyset$.

**Definition** A *matrix representation* $\mathcal{M} = \langle \mu, Q, q_-, Q_+\rangle$ from $A^*$ into $B^*$ is composed of a finite set of *states* $Q$, an *initial state* $q_-$, a set of *final states* $Q_+$, and a *semigroup morphism* $\mu : A^* \to \mathrm{Rat}(B^*)^{Q\times Q}$. The transduction $|\mathcal{M}| : A^* \to B^*$ *realized* by $\mathcal{M}$ is defined by

$$|\mathcal{M}|(x) = \bigcup_{q\in Q_+} \mu_x q_-, q\,. \tag{7.3}$$

For $p, q \in Q$, note $\mu_{p,q}$ the transduction $w \to \mu_w p, q$. Then (7.3) can be written as

$$|\mathcal{M}| = \bigcup_{q\in Q_+} \mu_{q_-,q}\,.$$

**Example 7.1** Let $A$ be an alphabet and $a_0 \in A$. Set $Q = \{1, 2\}$, and define a monoid morphism $\mu : A^* \to \mathrm{Rat}(A^*)^{2\times 2}$ by

$$\mu a = \begin{bmatrix} 0 & 0 \\ 0 & a \end{bmatrix} \quad a \in A \setminus a_0, \qquad \mu a_0 = \begin{bmatrix} 0 & 1 \\ 0 & a_0 \end{bmatrix}\,.$$

Then

$$\mu x = \begin{bmatrix} 0 & 0 \\ 0 & x \end{bmatrix} \quad \text{if } x \notin a_0 A^*,\ x \neq 1\,,$$

and

$$\mu x = \begin{bmatrix} 0 & y \\ 0 & x \end{bmatrix} \quad \text{if } x = a_0 y\,.$$

Thus for $\mathcal{M} = \langle \mu, Q, 1, \{2\} \rangle$, $|\mathcal{M}|(x) = \mu_x 1, 2 = a_0^{-1} x$, $(x \in A^*)$.

**Theorem 7.1** *A transduction $\tau : A^* \to B^*$ is rational if and only if there exists a matrix representation $\mathcal{M} = \langle \mu, Q, q_-, Q_+ \rangle$ realizing $\tau$. Then the following hold:*

(i) *if $\tau(1) = 0$ or $\tau(1) = 1$, then $\mu$ can be chosen to be a monoid morphism;*

(ii) *$Q_+$ can be assumed to consist of a single state $q_+ \neq q_-$, and $\mu_x q, q_- = \mu_x q_+, q = 0$ for all $x \in A^+$, $q \in Q$.*

(iii) *if $\tau(1) = 0$, both* (i) *and* (ii) *can be satisfied simultaneously.*

Note that $\mu$ cannot always be chosen to be a monoid morphism. Indeed in this case $\tau(1) = \bigcup_{q \in Q_+} \mu 1_{q_-, q}$ is equal to 1 or 0 according to $q_- \in Q_+$ or $q_- \notin Q_+$. The fact that semigroup morphisms are necessary is equivalent to the possibility for transducers to have transitions with the empty word as input label. This complicates the proof of the theorem.

*Proof.* We first prove the existence of a matrix representation. Let $\mathcal{T} = \langle A, B, Q, q_-, Q_+, E \rangle$ be a transducer realizing $\tau$. In view of Corollary 6.2, we may suppose that $Q_+ = \{q_+\}$, $q_+ \neq q_-$,

$$E \subset Q \times (A \cup \{1\}) \times B^* \times Q\,,$$

and moreover $(q, u, v, q') \in E$ implies $q' \neq q_-, q \neq q_+$. Let $\alpha : E^* \to A^*$ and $\beta : E^* \to B^*$ be the input and output morphism as defined in the preceding section. Then

$$\tau(x) = \beta(\alpha^{-1}(x) \cap \Lambda(q_-, q_+))\,. \tag{7.4}$$

Next note that for $p, q \in Q$,

$$\Lambda(p, q) = \bigcup_{r \in Q} \Lambda(p, r) \Lambda(r, q)\,.$$

Since $\alpha$ is an alphabetic morphism by the assumption on $E$, we have $\alpha^{-1}(xy) = \alpha^{-1}(x)\alpha^{-1}(y)$ for $x, y \in A^*$. Consequently

$$\alpha^{-1}(xy) \cap \Lambda(p, q) = \bigcup_{r \in Q} (\alpha^{-1}(x) \cap \Lambda(p, r))(\alpha^{-1}(y) \cap \Lambda(r, q))\,; \tag{7.5}$$

Define a mapping $\mu : A^* \to \mathfrak{P}(B^*)^{Q \times Q}$ by

$$\mu x_{p,q} = \beta(\alpha^{-1}(x) \cap \Lambda(p, q)) \quad p, q \in Q,\ x \in A^*\,. \tag{7.6}$$

In view of (7.5), $\mu$ is a semigroup morphism, and by (7.6), $\mu x_{p,q}$ is a regular language. Let $\mathcal{M} = \langle \mu, Q, q_-, q_+ \rangle$. Then by (7.4)

$$|\mathcal{M}|(x) = \mu x_{q_-, q_+} = \tau(x)\,.$$

This proves the existence of a matrix representation. Further, since $\Lambda(q,q_-)\cap E^+ = \Lambda(q_+,q)\cap E^+ = \emptyset$ for $q \in Q$ by the assumptions on $\mathcal{T}$, condition (ii) holds. Next, define the (monoid) morphism $\bar\mu$ by

$$\bar\mu x = \mu x \quad (x \in A^+)\,, \quad \bar\mu 1 = I\,.$$

and $\bar{\mathcal{M}} = \langle \bar\mu, Q, q_-, q_+\rangle$. Since $q_- \neq q_+$, $|\bar{\mathcal{M}}| = \tau$ in the case where $\tau(1) = 0$. This proves (i) in that case and proves also (iii). It remains to prove (i) in the case where $\tau(1) = 1$. For this, consider $\mu$ given by (7.6), let $q_0 \notin Q$, set $P = q_0 \cup Q$ and define

$$\mu' : A^* \to \mathrm{Rat}(B^*)^{P\times P}$$

by $\mu' 1 = I$ and

$$\mu' x_{p,q} = \begin{cases} \mu x_{p,q} & \text{if } p,q \in Q\,; \\ \mu x_{q_-,q} & \text{if } p = q_0, q \in Q\,; \\ 0 & \text{otherwise}\,. \end{cases} \qquad (x \in A^+)$$

Then $\mu'$ is easily seen to be a morphism, and

$$\tau(x) = \mu' x_{q_0,q_+} \cup \mu' x_{q_0,q_0} \quad (x \in A^*)\,.$$

Thus $\tau$ is realized by the matrix representation $\langle \mu', P, q_0, \{q_0, q_+\}\rangle$.

Conversely, let $\tau : A^* \to B^*$ be the transduction realized by a matrix representation $\mathcal{M} = \langle \mu, Q, q_-, Q_+\rangle$. In order to prove the rationality of $\tau$, we proceed in several steps.

First, we show that $Q_+$ can be assumed to consist of a single state $q_+ \neq q_-$. Let indeed $s \notin Q$, set $P = s \cup Q$ and define a semigroup morphism $\nu : A^* \to \mathrm{Rat}(B^*)^{P\times P}$ for $u \in 1 \cup A$ by

$$\begin{aligned} \nu u_{p,q} &= \mu u_{p,q} && (p,q \in Q) \\ \nu u_{s,q} &= \mu u_{s,s} = 0 && (q \in Q) \\ \nu u_{q,s} &= \cup_{p\in Q_+} \mu u_{q,p} && (q \in Q)\,. \end{aligned}$$

Then these formulas hold for any word $x \in A^*$. This is obvious for the two first formulas; the third follows by induction from:

$$\nu(xy)_{q,s} = \bigcup_{r\in Q} \mu x_{q,r} \nu y_{r,s} = \bigcup_{p\in Q_+} \bigcup_{r\in Q} \mu x_{q,r} \mu y_{r,p} = \bigcup_{p\in Q_+} \mu(xy)_{q,p}\,.$$

Thus

$$\tau(x) = \bigcup_{p\in Q_+} \mu x_{q_-,p} = \nu x_{q_-,s}\,.$$

Consequently, we may assume $Q_+ = \{q_+\}$ and $q_+ \neq q_-$. Next, define the monoid morphism $\bar\mu : A^* \to \mathrm{Rat}(B^*)^{Q\times Q}$ by $\bar\mu a = \mu a$ $(a \in A)$. Then $\bar\mu x_{q_-,q_+} = \mu x_{q_-,q_+} = \tau(x)$ for $x \in A^+$, and $\bar\mu 1_{q_-,q_+} = \emptyset$. Thus

$$\tau = \tau_1 \cup \bar\tau\,,$$

where $\bar{\tau}$ is the transduction realized by $\langle \bar{\mu}, Q, q_-, q_+ \rangle$, and where $\tau_1 : A^* \to B^*$ is defined by $\tau_1(1) = \mu 1_{q_-,q_+} \in \mathrm{Rat}(B^*)$ and $\tau_1(x) = \emptyset$ for $x \in A^+$. Since $\tau_1$ is obviously a rational transduction, it suffices to show that $\bar{\tau}$ is rational.

Thus we may assume that $\mu$ is a monoid morphism and $\tau(1) = 0$. Let $C = Q \times A \times Q$ and define a strictly alphabetic morphism $\phi : C^* \to A^*$ by

$$\phi((p, a, q)) = a\,.$$

Let

$$K = \big[(q_- \times A \times Q)C^* \cap C^*(Q \times A \times q_+)\big] \setminus C^*WC^*$$

with

$$W = \{(q, a, q')(p, b, p') \in C^2 \mid q' \neq p\}\,.$$

Then $K$ is a local regular language, $\phi^{-1}(1) \cap K = \emptyset$, and for $x = a_1a_2\cdots a_n$, $(a_i \in A)$,

$$\phi^{-1}(x) \cap K = \{(q_-, a_1, q_1)(q_1, a_2, q_2)\cdots(q_{n-1}, a_n, q_+) \mid q_1, \ldots, q_{n-1} \in Q\}\,. \tag{7.7}$$

Define a rational substitution $\sigma : C^* \to A^*$ by

$$\sigma((p, a, q)) = \mu a_{p,q}\,.$$

Then

$$\sigma(\phi^{-1}(1) \cap K) = \emptyset = \tau(1) \tag{7.8}$$

and, in view of (7.7),

$$\sigma(\phi^{-1}(x) \cap K) = \mu x_{q_-,q_+} = \tau(x) \qquad (x \in A^+) \tag{7.9}$$

Consequently, $\tau$ is a composition of rational transductions and therefore is rational.

■

The proof of Theorem 7.1 yields the following corollary which is another variation of Nivat's Theorem.

**Corollary 7.2** *Let $\tau : A^* \to B^*$ be a transduction with $\tau(1) = 0$ or $\tau(1) = 1$. Then $\tau$ is rational if and only if there exist an alphabet $C$, a strictly alphabetic morphism $\phi : C^* \to A^*$, a rational substitution $\sigma : C^* \to B^*$ and a local regular language $K \subset C^*$ such that*

$$\tau(x) = \sigma(\phi^{-1}(x) \cap K) \qquad (x \in A^*)\,. \tag{7.10}$$

*Proof.* Let $\tau$ be given by (7.10). Then $\tau$ is rational. Conversely, the conclusion holds if $\tau(1) = 0$ in view of (7.8) and (7.9). If $\tau(1) = 1$, then it suffices to replace the language $K$ of the preceding proof by $K \cup 1$. ■

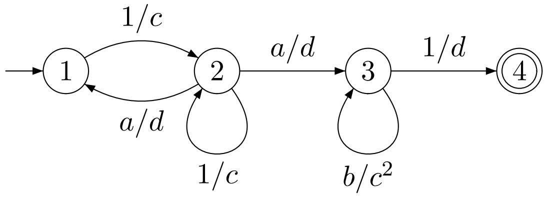

Figure III.7

**Example 7.2** Consider for $A = \{a, b\}$, $B = \{c, d\}$, the transducer of Example 6.2 (Figure III.7). Formula 7.6 gives the following semigroup morphism $\mu$:

$$\mu 1 = \begin{bmatrix} 1 & c^+ & 0 & 0 \\ 0 & c^* & 0 & 0 \\ 0 & 0 & 1 & d \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad \mu a = \begin{bmatrix} c^+d & c^+dc^+ & 0 & 0 \\ c^*d & c^*dc^+ & c^*d & c^*d^2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad \mu b = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & c^2 & c^2d \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Theorem 7.1 shows a relationship between rational transductions and formal power series. In the terminology of Eilenberg (1974) or Salomaa and Soittola (1978), a transduction $\tau : A^* \to B^*$ is rational if and only if the formal power series $\sum_{x \in A^*} \tau(x) \cdot x$ with coefficients in the semiring $\mathrm{Rat}(B^*)$ is recognizable. The following theorem is the analogue to a well-known characterization of recognizable formal power series.

**Proposition 7.3** *A transduction $\tau : A^* \to B^*$ is rational if and only if there exist a finite set $Q$, a monoid morphism $\mu : A^* \to \mathrm{Rat}(B^*)^{Q \times Q}$, a row $Q$-vector $\lambda$, a column $Q$-vector $\rho$ with entries in $\mathrm{Rat}(B^*)$ such that*

$$\tau(x) = \lambda \mu x \rho \qquad (x \in A^*)\,. \tag{7.11}$$

*Proof.* Let $\tau$ be given by (7.11). Then

$$\tau(x) = \bigcup_{p,q \in Q} \lambda_p \mu x_{p,q} \rho_q\,.$$

By Theorem 7.1, the transductions $\mu_{p,q} : x \mapsto \mu x_{p,q}$ are rational. Since $\lambda_p$, $\rho_q$ are regular languages, the transductions $\mu_{p,q} : x \mapsto \lambda_p \mu x_{p,q} \rho_q$ are rational. Thus $\tau$ is rational.

Conversely, let $\tau$ be realized by the matrix representation $\mathcal{M} = \langle \nu, P, q_-, \{q_+\} \rangle$ with $q_- \neq q_+$. Let $s \notin P$, set $Q = s \cup P$ and define a monoid morphism $\mu : A^* \to \mathrm{Rat}(B^*)^{Q \times Q}$ by

$$\begin{array}{lll} \mu a_{p,q} = \nu a_{p,q} & p, q \in P & \\ \mu a_{p,q} = \emptyset & p = s \text{ or } q = s & \end{array} \qquad (a \in A)$$

Then clearly

$$\mu x_{p,q} = \begin{cases} \nu x_{p,q} & p, q \in P \\ \emptyset & p = s \text{ or } q = s \end{cases} \qquad (x \in A^+)\,.$$

Next, define the $Q$-vectors $\lambda$ and $\rho$ by

$$\begin{array}{l} \lambda_s = (\nu 1)_{q_-, q_+}\,; \quad \rho_s = \{1\}\,, \quad \lambda_{q_-} = \{1\}\,, \quad \rho_{q_+} = \{1\}\,, \\ \lambda_q = \rho_q = \emptyset \quad \text{otherwise}\,. \end{array}$$

Then

$$\lambda\mu 1\rho = \lambda\rho = \lambda_s\rho_s = \tau(1)\,, \quad \lambda\mu x\rho = \lambda_{q_-}\mu x_{q_-,q_+}\rho_{q_+} = \tau(x)\,, \quad x \in A^+\,. \quad \blacksquare$$

**Example 7.3** Let $A = \{a\}$, $B = \{b, c\}$, $Q = \{1, 2, 3, 4\}$, and let $\mu$ be the monoid morphism defined by

$$\mu a = \begin{bmatrix} 0 & b & 0 & 0 \\ b & 0 & 0 & 0 \\ 0 & 0 & 0 & c \\ 0 & 0 & c & 0 \end{bmatrix} \qquad \lambda = [1,\, 0,\, 1,\, 0] \quad \rho = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

A simple computation shows that

$$\lambda\mu a^n = \begin{cases} [b^n,\, 0,\, c^n,\, 0] & \text{if } n \text{ is even;} \\ [0,\, b^n,\, 0,\, c^n] & \text{if } n \text{ is odd.} \end{cases}$$

Thus

$$\lambda\mu a^n\rho = \begin{cases} b^n & n \text{ even;} \\ c^n & n \text{ odd.} \end{cases}$$

We conclude this section by considering a useful technical notion.

**Definition** Let $\mathcal{M} = \langle \mu, Q, q_-, Q_+ \rangle$ be a matrix representation from $A^*$ into $B^*$. Then $\mathcal{M}$ is *trim* if the following condition is satisfied. For any $q \in Q$, there exist $x, y \in A^*$, $q_+ \in Q_+$ such that

$$\mu x_{q_-,q} \neq \emptyset \quad \text{and} \quad \mu y_{q,q_+} \neq \emptyset\,. \tag{7.12}$$

**Proposition 7.4** *Let* $\tau : A^* \to B^*$ *be a transduction with* $\mathrm{dom}(\tau) \neq \emptyset$*, and let* $\mathcal{M} = \langle \mu, Q, q_-, Q_+ \rangle$ *with* $\mu$ *a monoid morphism be a matrix representation realizing* $\tau$*. Then there exists a trim matrix representation* $\mathcal{M}' = \langle \nu, P, q_-, P_+ \rangle$ *realizing* $\tau$ *with* $P \subset Q$ *and* $P_+ = Q_+ \cap P$*.*

*Proof.* Let $P \subset Q$ be the set of states such that (7.12) holds. Since $\mathrm{dom}(\tau) \neq \emptyset$ and $\mu$ is a monoid morphism, we have $q_- \in P$ and $P_+ = Q_+ \cap P \neq \emptyset$. Moreover, for any $q \in Q_+$, $q \in P_+$ if and only if $\mu z_{q_-,q} \neq \emptyset$ for at least one word $z \in A^*$. Consequently

$$|\mathcal{M}| = \bigcup_{q \in Q_+} \mu_{q_-,q} = \bigcup_{q \in P_+} \mu_{q_-,q}\,. \tag{7.13}$$

Define a monoid morphism $\nu : A^* \to \mathrm{Rat}(B^*)^{P \times P}$ by

$$\nu a_{p,q} = \mu a_{p,q} \quad p, q \in P,\ a \in A\,.$$

In order to prove the desired result, it suffices to show that

$$\nu x_{p,q} = \mu x_{p,q} \quad p, q \in P,\ x \in A^*\,. \tag{7.14}$$

since then, in view of (7.13)

$$|\mathcal{M}'| = \bigcup_{q \in P_+} \nu_{q_-,q} = \bigcup_{q \in P_+} \mu_{q_-,q} = |\mathcal{M}| \,.$$

To show (7.14), we first verify that for $p, q \in P$, $r \in Q \setminus P$,

$$\mu x_{p,r} = \emptyset \quad \text{or} \quad \mu y_{r,q} = \emptyset \tag{7.15}$$

for any pair of words $x, y$. Assume the contrary. Then there exist words $x, y$ such that both $\mu x_{p,r} \neq \emptyset$ and $\mu y_{r,q} \neq \emptyset$. Since $p \in P$, there is a word $x'$ such that $\mu x'_{q_-,p} \neq \emptyset$, and similarly $\mu y'_{q,q_+} \neq \emptyset$ for some word $y'$ and some $q_+ \in Q_+$. But then $\emptyset \neq \mu x'_{q_-,p} \mu x_{p,r} \subset \mu x' x_{q_-,r}$ and $\emptyset \neq \mu y_{r,q} \mu y'_{q,q_+} \subset \mu y y'_{r,q_+}$, and by (7.12), $r \in P$ contrary to the assumption. This proves (7.15).

Now (7.14) is true if $|x| \leq 1$. Arguing by induction, let $x \in A^*, a \in A$. Then for $p, q \in P$,

$$(\mu x a)_{p,q} = \bigcup_{r \in Q} \mu x_{p,r} \mu a_{r,q} = \bigcup_{r \in P} \mu x_{p,r} \mu a_{r,q}$$

by (7.15). Consequently

$$(\mu x a)_{p,q} = \bigcup_{r \in P} \nu x_{p,r} \nu a_{r,q} = (\nu x a)_{p,q} \,. \qquad \blacksquare$$

## Exercises

**7.1** Show that $\mathcal{M} = \langle \mu, Q, q_-, Q_+ \rangle$ is trim if and only if for any $q \in Q$, there exist $q_+ \in Q_+$ and $x, y \in A^*$ with $|x|, |y| \leq \operatorname{Card} Q$ such that $\mu x_{q_-,q} \neq \emptyset$ and $\mu y_{q,q_+} \neq \emptyset$.

**7.2** A transduction $\tau : A^* \to B^*$ is *faithful* if $\tau^{-1}(y)$ is finite for all $y \in B^*$, and is *continuous* if $\tau(x) \subset B^+$ for $x \in A^+$. Show that a rational transduction $\tau : A^* \to B^*$ is faithful and continuous if and only if

$$\tau(x) = \psi(\phi^{-1}(x) \cap K) \quad x \in A^*$$

for some alphabet $C$, $K \in \operatorname{Rat}(C^*)$, $\phi : C^* \to A^*$ a morphism and $\psi : C^* \to B^*$ a strictly alphabetic morphism. (Hint: Apply Corollary 7.2 to $\tau^{-1}$.) Show that the composition of two faithful (continuous) transductions is still faithful (continuous).

**7.3** Let $\mathcal{R}$ be the least family of subsets of $A^* \times B^*$ closed under union, product and the plus operation, and containing $\emptyset$, $\{(1,1)\}$ and the relations $\{(u,b)\}$ for $u \in 1 \cup A, b \in B$.
a) Show that $RS, SR \in \mathcal{R}$ for all $R \in \mathcal{R}$ such that $(1,1) \notin R$ and $S \in \operatorname{Rat}(A^* \times B^*)$.
b) Show that $R \in \mathcal{R}$ if and only if the transduction with graph $R$ is rational, faithful and continuous.

# 8 Decision Problems

We show in this section that most of the usual questions are undecidable for rational transductions. We shall see in the next chapter that some of these questions become decidable for rational functions. The results of this section are mainly from Fischer and Rosenberg (1968).

The proof of undecidability are "relative" in the following sense: We give (without proof) a particular undecidable problem (Post's Correspondence Problem) and we prove that some property is undecidable by showing that the existence of a decision problem for this property would imply a decision procedure for the Correspondence Problem.

**Post's Correspondence Problem** *Given an alphabet $A$ with at least two letters, and given two sequences*

$$x_1, x_2, \ldots, x_p\,, \text{ and } y_1, u_2, \ldots, y_p \tag{8.1}$$

*of words of $A^*$, decide whether there exists indices $i_1, i_2, \ldots, i_k$, ($k > 0$) such that*

$$x_{i_1} x_{i_2} \cdots x_{i_k} = y_{i_1} y_{i_2} \cdots y_{i_k}\,. \tag{8.2}$$

**Theorem 8.1** Post's Correspondence Theorem. *Post's Correspondence Problem is undecidable.*

For a proof, see for instance Davis (1958) or Schnorr (1974). The theorem means that there exists no algorithm that has as input two sequences (8.1), and yields as output "yes" or "no" according to the existence or the non-existence of a sequence $i_1, i_2, \ldots, i_k$ such that (8.2) holds.

First we give two decidable properties. As usual for decision problems, the word "given" in the statement should be interpreted to mean that an explicit description of the object, here of the rational relation $R$ is provided. This can be done in the present context by a rational expression, by a matrix representation, by a transducer or by a bimorphism. From the constructions of the previous sections, it should be clear that any of the above descriptions of a rational relation can be obtained effectively from another one.

**Proposition 8.2** *Given a rational relation $R \subset A^* \times B^*$, it is decidable whether $R$ is empty and whether $R$ is finite.*

*Proof.* $R$ is empty if and only if one of the two projections $\pi_A(R)$ and $\pi_Y(R)$ on $A^*$ and $Y^*$ is empty, and $R$ is finite if and only if both are finite. Each projection is a regular language, and an explicit description of these languages is readily obtained from an effective description of $R$. Since emptiness and finiteness are decidable for regular languages, the conclusion follows. ■

We now prove a lemma which will be of use later. Let $A = \{a, b\}$, let $B$ be an alphabet, and let $u_1, \ldots, u_p \in B^*$. Define

$$U = \{(ab, u_1), (ab^2, u_2), \ldots, (ab^p, u_p)\}\,.$$

Clearly $U$, hence $U^*$ is a rational relation over $A$ and $B$.

**Lemma 8.3** *The relation $(A^* \times B^*) \setminus U^+$ is rational.*

Usually, $\mathrm{Rat}(A^* \times B^*)$ is not closed under complementation, thus Lemma 8.3 has to be proved.

*Proof.* We show that $W = (A^* \times B^*) \setminus U^+$ is rational by writing $W$ as a union of four rational relations. First the relation $H$ composed of all $(x, y) \in A^* \times B^*$ such that

$$x \notin \{ab, ab^2, \ldots, ab^p\}^+$$

is rational and even recognizable since

$$H = (A^* \setminus \{ab, ab^2, \ldots, ab^p\}^+) \times Y^* .$$

Next

$$(x, y) \in W \quad \text{and} \quad (x, y) \notin H$$

if and only if

$$x = ab^{i_1} ab^{i_2} \cdots ab^{i_r} \quad \text{for some } r > 0,\ 1 \le i_1, \ldots, i_r \le p \tag{8.3}$$

and

$$y \neq u_{i_1} u_{i_2} \cdots u_{i_r} . \tag{8.4}$$

Now (8.4) holds if and only if one of the three following conditions hold

$$|y| < |u_{i_1} u_{i_2} \cdots u_{i_r}| \tag{8.5}$$
$$|y| > |u_{i_1} u_{i_2} \cdots u_{i_r}| \tag{8.6}$$
$$|y| = |u_{i_1} u_{i_2} \cdots u_{i_r}|, \tag{8.7}$$

and there is a factorization $y = y'zy''$ and $k \in \{1, \ldots, p\}$ with

$$|y'| = |u_{i_1} \cdots u_{i_{k-1}}|,\ |z| = |u_{i_k}|,\ h \neq u_{i_k},\ |y''| = |u_{i_{k+1}} \cdots u_{i_r}| .$$

Define the following relations which are clearly rational:

$$F = \bigcup_{i=1}^{p} ab^i \times B^{|u_i|} ; \quad G = \bigcup_{i=1}^{p} ab^i \times (B^{|u_i|} \setminus u_i) = F \setminus U ;$$
$$D = \bigcup_{i=1}^{p} ab^i \times B^{|u_i|} B^+ = F \cdot (1 \times B^+) ; \quad C = \bigcup_{i=1}^{p} ab^i \times B_i ,$$

with

$$B_i = \{u \in B^* \mid |u| < |u_i|\} .$$

Then $CF = FC$, $DF = FD$, and

$$\{(x, y) \mid (x, y) \text{ verifies (8.3) and (8.5)}\} = C^+ F^* ;$$
$$\{(x, y) \mid (x, y) \text{ verifies (8.3) and (8.6)}\} = D^+ F^* ;$$
$$\{(x, y) \mid (x, y) \text{ verifies (8.3) and (8.7)}\} = F^* G F^* .$$

Thus

$$W = H \cup C^+ F^* \cup D^+ F^* \cup F^* G F^* \in \mathrm{Rat}(A^* \times B^*) . \qquad \blacksquare$$

**Theorem 8.4** *Let $A, B$ be alphabets with at least two letters. Given rational relations $X, Y \subset A^* \times B^*$, it is undecidable to determine whether*

(i) $X \cap Y = \emptyset$;
(ii) $X \subset Y$;
(iii) $X = Y$;
(iv) $X = A^* \times B^*$;
(v) $(A^* \times B^*) \setminus X$ *is finite;*
(vi) $X$ *is recognizable.*

*Proof.* We assume that $A$ contains exactly two letters, and set $A = \{a, b\}$. Consider two sequences

$$u_1, u_2, \ldots, u_p \quad \text{and} \quad v_1, v_2, \ldots, v_p \tag{8.8}$$

of words of $B^*$ and define

$$U = \{(ab, u_1), \ldots, (ab^p, u_p)\}, \quad V = \{(ab, v_1), \ldots, (ab^p, v_p)\}.$$

Then $U^+$, $V^+$ are rational relations, and by the preceding lemma, $\bar{U} = (A^* \times B^*) \setminus U^+$ and $\bar{V} = (A^* \times B^*) \setminus V^+$ are rational relations.

(i) Let $X = U^+$, $Y = V^+$. Then $X \cap Y \neq \emptyset$ if and only if there exist integers $i_1, \ldots, i_k$ such that $u_{i_1} \cdots u_{i_k} = v_{i_1} \cdots v_{i_k}$, thus if and only if the Correspondence Problem 8.1 has a solution. Thus if the emptiness $X \cap Y = \emptyset$ would be decidable, Post's Correspondence Problem would be decidable. This proves (i).

(ii) Let $X = U^+$, $Y = \bar{V}$. Then $X \subset Y$ if and only if $U^+ \cap V^+ = \emptyset$. Thus (ii) follows from (i).

(iii) is a consequence of (iv) since $A^* \times B^*$ is rational.

(iv) Let $X = \bar{U} \cup \bar{V}$. Then $X = A^* \times B^*$ if and only if $A^* \times B^* \setminus X = U^+ \cap V^+ = \emptyset$. Thus (iv) is undecidable by (i).

(v) Let again $X = \bar{U} \cup \bar{V}$. Then $(m, u) \in A^* \times B^* \setminus X$ if and only if there exist $i_1, \ldots, i_r$ such that $m = ab^{i_1} \cdots ab^{i_r}$ and $u = u_{i_1} \cdots u_{i_r} = v_{i_1} \cdots v_{i_r}$. Thus $(m, u) \in A^* \times B^* \setminus X$ implies $(m^k, u^k) \in A^* \times B^* \setminus X$ for any $k \geq 1$. Consequently, $A^* \times B^* \setminus X$ is finite if and only if $A^* \times B^* \setminus X$ is empty, and the last property is undecidable.

(vi) Let again $X = \bar{U} \cup \bar{V}$. Then $X$ is recognizable if and only if $A^* \times B^* \setminus X = U^+ \cap V^+$ is recognizable since $\mathrm{Rec}(A^* \times B^*)$ is closed under complementation. We shall see that $U^+ \cap V^+$ is recognizable if and only if $U^+ \cap V^+ = \emptyset$. Assume $U^+ \cap V^+$ recognizable. Then by Mezei's Theorem

$$U^+ \cap V^+ = P_1 \times Q_1 \cup \cdots \cup P_\ell \times Q_\ell$$

for $P_1, \ldots, P_\ell \in \mathrm{Rat}(A^*)$, $Q_1, \ldots, Q_\ell \in \mathrm{Rat}(B^*)$. Next assume $(m, u) \in U^+ \cap V^+$. Then $(m^k, u^k) \in U^+ \cap V^+$ for $k \geq 1$, thus there exist integers $r, s$, $(r > s \geq 1)$ such that

$$(m^r, u^r), (m^s, u^s) \in P_j \times Q_j$$

for some $j$, $(1 \leq j \leq \ell)$. Then $(m^s, u^r) \in P_j \times Q_j$, but $(m^s, u^r) \notin U^+ \cap V^+$ since $s \neq r$. Thus $U^+ \cap V^+ = \emptyset$, and (vi) follows from (i). ■

## Exercises

**8.1** Show that all properties of Theorem 8.4 are decidable for recognizable relations.

**8.2** Let $\mathcal{M} = \langle \mu, Q, q_-, Q_+ \rangle : A^* \to B^*$ be a matrix representation. Show that a trim matrix representation realizing $|\mathcal{M}|$ can effectively be constructed.

**8.3** (continuation of Exercise 4.8) Assume that a rational transduction $\tau : A^* \to B^*$ is effectively given. Show that the rational transductions $\tau_0$ and $\tau_\infty$ can be computed effectively.

# Chapter IV

# Rational Functions

The present chapter deals with rational functions, that is rational transductions which are partial functions. Rational functions have remarkable properties. First, several decision problems become solvable. This is shown in Section 1. Then there exist special representations, called unambiguous representations for rational functions. They are defined by the property that there exist at most one successful path for each input word. Two different methods for constructing unambiguous representations are given in Sections 3 and 4, the first by means of a cross-section theorem due to Eilenberg, the second through so-called semimonomial representations and due to Schützenberger. Section 2 is concerned with sequential functions which are a particular case of rational functions. In Section 5, bimachines are defined as composition of a left sequential followed by a right sequential function. In Section 6, we prove that it is decidable whether a rational function is sequential.

## 1 Rational Functions

In this section, rational functions are defined and some examples are given. Further a decidability result is proved. A more detailed description of rational functions will be given in Sections 4 and 5.

**Definition** A *rational function* $\alpha : A^* \to B^*$ is a rational transduction which is a partial function, that is such that $\mathrm{Card}(\alpha w) \leq 1$ for all $w \in A^*$.

In order to simplify statements and proofs, we first make a general observation. Given a transduction

$$\tau : A^* \to B^*$$

define two transductions $\tau_1, \tau_+ : A^* \to B^*$ by

$$\tau_1(1) = \tau(1)\,; \quad \tau_+(1) = \emptyset\,;$$
$$\tau_1(w) = \emptyset\,; \quad \tau_+(w) = \tau(w) \quad w \in A^+\,.$$

Then $\tau = \tau_1 \cup \tau_+$ (and even $\tau = \tau_1 + \tau_+$), and $\tau$ is rational if and only if $\tau_1$ and $\tau_+$ are rational. Further, any transduction $\tau' : A^* \to B^*$ with $\tau'_+ = \tau_+$ is rational if and only if $\tau$ is rational and $\tau'(1)$ is a rational language. Thus, rational transductions can always be considered "up to the value $\tau(1)$". Therefore we stipulate that in this chapter, $\tau(1)$ is always equal to $\emptyset$ or $\{1\}$. Then, according to Theorem III.7.1, the morphism of a matrix representation $\mathcal{M} = \langle \mu, Q, q_-, Q_+ \rangle$ realizing $\tau$ can always be chosen to be a monoid morphism.

Further, we recall that if $\tau(1) = 0$, then we may assume that $Q_+ = \{q_+\}$ and $q_+ \neq q_-$, and that $\mu w_{q,q_-} = \mu_w q_+, q = 0$ for $w \in A^*, q \in Q$. As a result of the above discussion we thus may assume that this relation also holds if $\tau(1) = 1$, and that $Q_+ = \{q_-, q_+\}$. Then indeed $\tau(1) = \mu 1_{q_-,q_-} = 1$, and $\tau(w) = \mu w_{q_-,q_+}$ if $w \in A^+$.

A matrix representation which satisfies the above conditions and which is trim is called *normalized*. Normalization clearly is effective.

**Proposition 1.1** *Let $\tau : A^* \to B^*$ be the transduction realized by a normalized matrix representation $\mathcal{M} = \langle \mu, Q, q_-, Q_+ \rangle$. Then $\tau$ is a partial function if and only if* $\mathrm{Card}(\mu w_{p,q}) \leq 1$ *for any $w \in A^*$, $(p, q \in Q)$.*

*Proof.* If the conclusion holds, then $\mathrm{Card}(\mu w_{q_-,q_+}) \leq 1$ for any $w \in A^+$, thus $\mathrm{Card}(\tau(w)) \leq 1$ for any $w \in A^*$. Conversely, assume that $\mathrm{Card}(\mu w_{p,q}) \geq 2$ for some $w \in A^*$, $(p, q \in Q)$. Then $w \in A^+$ since $\mu 1$ is the identity matrix. Since $\mathcal{M}$ is trim, $\mu z_{q_-,p} \neq \emptyset$ and $\mu z'_{q,q_+} \neq \emptyset$ for some $z, z' \in A^*$. Then

$$\tau(zwz') = \mu(zwz')_{q_-,q_+} \supset \mu z_{q_-,p} \mu w_{p,q} \mu z'_{q,q_+} ,$$

and $\mathrm{Card}\, \tau(zwz') \geq 2$. ■

Let $\alpha : A^* \to B^*$ be a rational function realized by a normalized matrix representation $\mathcal{M} = \langle \mu, Q, q_-, Q_+ \rangle$. Then we associate to $\mathcal{M}$ the transducer $\mathcal{T} = \langle A, B, Q, q_-, Q_+, E \rangle$ with

$$E = \{(p, a, \mu a_{p,q}, q) \mid p, q \in Q,\ a \in A,\ \mu a_{p,q} \neq 0\} .$$

Thus $E \subset Q \times A \times B^* \times Q$, and for any $(p, a, q) \in Q \times A \times Q$, there is at most one $z \in B^*$ such that $(p, a, z, q) \in E$. Conversely, if $E$ satisfies these conditions then the formula

$$\mu a_{p,q} = \begin{cases} z & \text{if } (p, a, z, q) \in E\,; \\ 0 & \text{otherwise} \end{cases}$$

defines a matrix representation $\mathcal{M} = \langle \mu, Q, q_-, Q_+ \rangle$. The transducer $\mathcal{T}$ and the matrix representation $\mathcal{M}$ are called *associated*, and we sometimes identify them. Thus we speak about a normalized transducer, of a path in a matrix representation and so on.

**Example 1.1** Let $\alpha : a^* \to \{b, c\}^*$ be given by

$$\alpha(a^n) = \begin{cases} b^n & n \text{ even;} \\ c^n & n \text{ odd.} \end{cases}$$

Then $\alpha$ is a rational transduction (Example III.7.3), hence a rational function.

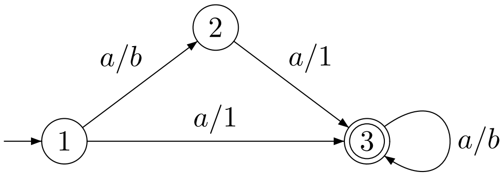

Figure IV.1

**Example 1.2** Let $A = \{a\}$, $B = \{b\}$, and consider the transducer in Figure IV.1 corresponding to the matrix

$$\mu a = \begin{bmatrix} 0 & b & 1 \\ 0 & 0 & 1 \\ 0 & 0 & b \end{bmatrix}$$

The transduction $\alpha$ realized by this transducer is given by $\alpha(1) = 0$ and $\alpha(a^n) = b^{n-1}$, $(n \geq 1)$; hence $\alpha$ is a rational function.

**Example 1.3** (Choffrut) Let again $A = \{a\}$, $B = \{b\}$, and consider the transducer in Figure IV.2. Let $\alpha$ be the transduction realized. It is easy to see that there are 3 nonempty paths from state 1 to itself without internal node 1. They are of length 3 and 4 and have labels $(a^3, b^6)$ and $(a^4, b^8)$. Thus, if $\alpha(a^n) \neq \emptyset$, then $\alpha(a^n) = b^{2n}$, and thus $\alpha$ is a partial function. Further $\text{dom}(\alpha) = 1 \cup a^3 \cup a^4 \cup a^6 a^*$.

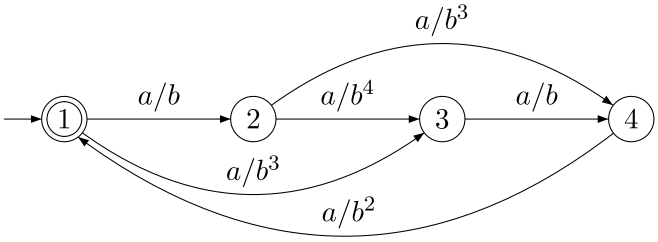

Figure IV.2

The above example shows that it is not always easy to determine whether the transduction realized by a transducer is a (partial) function. However, this property has been shown to be decidable by Schützenberger (1975) (see also Blattner and Head (1977)):

**Theorem 1.2** *Let $\tau : A^* \to B^*$ be a transduction realized by a normalized matrix representation $\mathcal{M} = \langle \mu, Q, q_-, q_+ \rangle$, and let $m = \text{Card}(Q)$. Then $\tau$ is a rational function if and only if $\text{Card}(\mu w_{p,q}) \leq 1$ for all $p, q \in Q$ and all $w \in A^*$ with $|w| \leq 1 + 2m(m-1)$.*

*Proof.* By Proposition 1.1 the condition is necessary. Assume the converse is false. Then, still by Proposition 1.1, $\text{Card}(\mu w_{p,q}) \geq 2$ for some $w \in A^+$ and $p, q \in Q$. Choose a word $w$ of minimal length such that $\text{Card}(\mu w_{p,q}) \geq 2$ for some $p, q \in Q$. Then $|w| > 1 + 2m(m-1)$. Set $w = a_1 \cdots a_n$ with $a_1, \ldots, a_n \in A$. There is a sequence of $n+1$ pairs of states $(q_j, q'_j)$,$(j=0,\ldots,n)$ such that $q_0 = q'_0 = p$, $q_n = q'_n = q$, and such that with

$$u_j = (\mu a_j)_{q_{j-1},q_j}\,, \quad v_j = (\mu a_j)_{q'_{j-1},q'_j}\,,$$

the words $u = u_1 \cdots u_n$ and $v = v_1 \cdots v_n$ are two distinct elements of $\mu w_{p,q}$. Since $w$ has been chosen of minimal length, $q_j \neq q'_j$ for $j = 1,\ldots,,n-1$. Indeed, assume $q_j = q'_j$ for some $j$. Then either $u_1 \cdots u_j \neq v_1 \cdots v_j$ or $u_{j+1} \cdots u_n \neq v_{j+1} \cdots v_n$. Next, since $n-1 > 2m(m-1)$, there are three indices $1 \le i < j < k \le n-1$ such that

$$(q_i, q'_i) = (q_j, q'_j) = (q_k, q'_k)\,. \tag{1.1}$$

Define

$$\begin{aligned}
&w_1 = a_1 \cdots a_i\,, \quad w_2 = a_{i+1} \cdots a_j\,, \quad w_3 = a_{j+1} \cdots a_k\,, \quad w_4 = a_{k+1} \cdots a_n\,;\\
&x_1 = u_1 \cdots u_i\,, \quad x_2 = u_{i+1} \cdots u_j\,, \quad x_3 = u_{j+1} \cdots u_k\,, \quad x_4 = u_{k+1} \cdots u_n\,;\\
&y_1 = v_1 \cdots v_i\,, \quad y_2 = v_{i+1} \cdots v_j\,, \quad y_3 = v_{j+1} \cdots v_k\,, \quad y_4 = v_{k+1} \cdots v_n\,.
\end{aligned}$$

Then by (1.1)

$$\begin{aligned}
&x_1x_4, y_1y_4 \in \mu(w_1w_4)_{p,q}\,; \quad x_1x_2x_4, y_1y_2y_4 \in \mu(w_1w_2w_4)_{p,q}\,;\\
&x_1x_3x_4, y_1y_3y_4 \in \mu(w_1w_3w_4)_{p,q}\,.
\end{aligned}$$

By the minimality of $w$, we have

$$x_1x_4 = y_1y_4\,, \quad x_1x_2x_4 = y_1y_2y_4\,, \quad x_1x_3x_4 = y_1y_3y_4\,. \tag{1.2}$$

We shall deduce from (1.2) that $u = v$, in contradiction with the assumption. By symmetry, we may suppose $|x_1| \le |y_1|$, hence $y_1 = x_1z$ for some $z \in B^*$. Then the first of the equations (1.2) implies $x_4 = zy_4$. Reporting this in the two other equations (1.2) yields $x_2z = zy_2$ and $x_3z = zy_3$. It follows that

$$u = x_1x_2x_3x_4 = x_1x_2x_3zy_4 = x_1x_2zy_3y_4 = x_1zy_2y_3y_4 = v\,. \qquad \blacksquare$$

Given two rational functions $\alpha, \beta : A^* \to B^*$, we write $\alpha \subset \beta$ if $\alpha(w) \neq 0 \implies \alpha(w) = \beta(w)$, $(w \in A^*)$.

**Corollary 1.3** *Given two rational functions $\alpha, \beta : A^* \to B^*$, it is decidable whether $\alpha \subset \beta$, and whether $\alpha = \beta$.*

*Proof.* Clearly $\alpha \subset \beta$ if and only if the two following conditions hold:

(i) $\mathrm{dom}(\alpha) \subset \mathrm{dom}(\beta)$;
(ii) $\alpha \cup \beta$ is a rational function.

Condition (i) is decidable since $\mathrm{dom}(\alpha)$ and $\mathrm{dom}(\beta)$ are regular languages. Condition (ii) is decidable by the previous theorem. Next $\alpha = \beta$ if and only if $\alpha \subset \beta$ and $\beta \subset \alpha$, thus equality of functions is decidable. $\blacksquare$

## Exercises

**1.1** Show that it is decidable whether a rational function $\alpha$ is recognizable (that is its graph is a recognizable relation).

**1.2** Show that it is decidable, for rational functions $\alpha, \beta : A^* \to B^*$, whether there exists a word $w \in A^*$ such that $\alpha(w) = \beta(w)$.

# 2 Sequential Transductions

For practical purposes, a rational transduction is required not only to be a partial function, but also to be computable in some sequential way. Such a model is provided by sequential transductions. In fact, transducers which are used for instance in compilation are more general, since there is usually an output after the lecture of the last letter of the input word. In order to fit into the model of sequential transducers, the input word is frequently considered to be followed by some "end marker". Another way to describe this situation is to add a supplementary output function to a sequential transducer. This is the definition of the subsequential transducers.

In this section, we define sequential and subsequential transductions, and give a "machine independent"characterization of these particular rational functions. Sequential transductions are among the oldest concepts in formal language theory. For a complete exposition, see Eilenberg (1974). Subsequential transductions are defined in Schützenberger (1977). A systematic exposition can be found in Choffrut (1978).

**Definition** A *left sequential transducer* (or *sequential transducer* for short) $\mathcal{L}$ consists of an *input alphabet* $A$, an *output alphabet* $B$, a finite set of *states* $Q$, an initial state $q_- \in Q$, and of two partial functions

$$\delta : Q \times A \to Q\,, \quad \lambda : Q \times A \to B^*$$

having the same domain and called the *next state function* and the *output function* respectively.

We usually denote $\delta$ by a dot, and $\lambda$ by a star. Thus we write $q \cdot a$ for $\delta(q, a)$ and $q * a$ for $\lambda(q, a)$. Then $\mathcal{L}$ is specified by

$$\mathcal{L} = \langle A, B, Q, q_- \rangle\,.$$

With the conventions of Section I.1, $Q$ can be considered as a subset of $\mathfrak{P}(Q)$, and $q \cdot a$ is undefined if and only if $q \cdot a = \emptyset$ (or $q \cdot a = 0$ by writing 0 for $\emptyset$). Further $0 \cdot a = 0$ for all $a \in A$. Thus, the next state function can also be viewed as a total function from $Q \cup \{0\} \times A$ into $Q \cup \{0\}$, and 0 can be considered as a new, "sink" state.

A sequential transducer is called a *generalized sequential machine* (gsm) by Eilenberg (1974) and Ginsburg (1966).

The next state function and the output function are extended to $Q \times A^*$ by setting, for $w \in A^*$, $a \in A$

$$\begin{aligned} &q \cdot 1 = q\,; \quad q \cdot (wa) = (q \cdot w) \cdot a\,; \\ &q * 1 = 1\,; \quad q * (wa) = (q * w)((q \cdot w) * a)\,. \end{aligned} \tag{2.1}$$

The parentheses in (2.1) can be omitted without ambiguity. We agree that concatenation has higher priority than the dot, and that the dot has higher priority than the star. For $x, y \in A^*$, $(q \in Q)$, the following formulas hold

$$q \cdot xy = (q \cdot x) \cdot y\,; \tag{2.2}$$

$$q * xy = (q * x)(q \cdot x * y)\,. \tag{2.3}$$

Indeed (2.2) is clear, and (2.3) is proved by induction on $|y|$: the formula is obvious for $|y| = 0$. If $y = za$ with $z \in A^*, a \in A$, then

$$\begin{aligned} q * xy = q * xza &= (q * xz)(q \cdot xz * a) \\ &= (q * x)(q \cdot x * z)((q \cdot x) \cdot z * a) = (q * x)(q \cdot x * za) \\ &= (q * x)(q \cdot x * y)\,. \end{aligned}$$

The partial function $|\mathcal{L}| : A^* \to B^*$ realized by $\mathcal{L}$ is defined by

$$|\mathcal{L}|(w) = q_- * w \quad (w \in A^*)\,.$$

**Definition** A partial function $\alpha : A^* \to B^*$ is a (left) *sequential transduction* or (left) *sequential function* if $\alpha = |\mathcal{L}|$ for some sequential transducer $\mathcal{L}$.

If $\alpha = |\mathcal{L}|$ with $\mathcal{L}$ as above, then

$$\alpha(1) = 1 \tag{2.4}$$

$$\alpha(xy) = \alpha(x)(q_- \cdot x * y)\,. \tag{2.5}$$

By (2.4), dom$(\alpha)$ is nonempty. Say that a partial function $\alpha : A^* \to B^*$ *preserves prefixes* if (2.4) holds and if further

$$\alpha(xy) \neq 0 \implies \alpha(xy) \in \alpha(x)B^*\,.$$

Then by (2.5) a sequential function preserves prefixes. Not that this is a rather strong constraint. In particular, the domain of such a function is prefix-closed, that is it contains the prefixes of its elements. Of course, this is due to the lack of final states.

To each sequential transducer $\mathcal{L} = \langle A, B, Q, q_- \rangle$ we associate a transducer $\mathcal{T} = \langle A, B, Q, q_-, Q_+, E \rangle$ by setting $Q_+ = Q$ and

$$E = \{(q, a, q * a, q \cdot a) \mid q \in Q, a \in A, q \cdot a \neq 0\}\,.$$

Then clearly $|\mathcal{L}| = |\mathcal{T}|$. Thus

**Proposition 2.1** *Any sequential function is rational.* ∎

**Example 2.1** Any morphism is a sequential function.

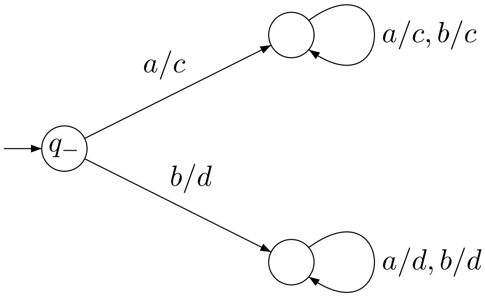

Figure IV.3

**Example 2.2** Let $A = \{a, b\}, B = \{c, d\}$, and define $\alpha : A^* \to B^*$ by

$$\alpha(x) = \begin{cases} c^{|x|} & \text{if } x \in aA^*\,, \\ d^{|x|} & \text{otherwise.} \end{cases}$$

Then $\alpha$ is a sequential function realized by the following transducer (Figure IV.3).

**Example 2.3** The function $\tau : a^* \to \{b, c\}^*$ defined by

$$\tau(a^n) = \begin{cases} b^n & n \text{ even;} \\ c^n & n \text{ odd.} \end{cases}$$

is rational, but not sequential, since it does not preserve prefixes.

Sometimes, it is useful to have some “reversal” of a left sequential transducer.

**Definition** A *right sequential transducer* $\mathcal{R} = \langle A, B, Q, q_- \rangle$ is given by the objects $A, B, Q, q_-$ which have the same meaning as for left sequential transducers, and by two partial functions

$$A \times Q \to Q\,; \quad A \times Q \to B^*$$

which have same domain, called next state and output function and denoted by a dot and by a star respectively.

As above, these functions are extended to $A^* \times Q$ by setting

$$\begin{aligned} &1 \cdot q = q\,; \quad aw \cdot q = a \cdot (w \cdot q)\,; \\ &1 * q = 1\,; \quad aw * q = (a * w \cdot q)(w * q)\,. \end{aligned}$$

Then the “reversal” of formulas (2.3) and (2.4) hold:

$$xy \cdot q = x \cdot (y \cdot q)\,; \quad xy * q = (x * y \cdot q)(y * q)\,. \quad (x, y \in A^*)$$

The partial function $|\mathcal{R}|$ realized by $\mathcal{R}$ is defined by

$$|\mathcal{R}|(x) = x * q_- \quad (x \in A^*)\,;$$

and a partial function realized by a right sequential transducer is called a *right sequential transduction* or a *right sequential function*.

**Proposition 2.2** *Let $\alpha : A^* \to B^*$ be a partial function, and define $\beta : A^* \to B^*$ by $\beta(w) = [\alpha(\tilde{w})]^\sim, (w \in A^*)$. Then $\alpha$ is left sequential if and only if $\beta$ is right sequential.*

*Proof.* Note first that $\alpha(w) = [\beta(\tilde{w})]^\sim$, $(w \in A^*)$. Thus it suffices to show that if $\alpha$ is right or left sequential, then $\beta$ is left or right sequential. Assume that $\alpha$ is realized by some right sequential transducer $\mathcal{R} = \langle A, B, Q, q_- \rangle$, and define a left sequential transducer $\mathcal{L} = \langle A, B, Q, q_- \rangle$ by setting

$$q \cdot a = a \cdot q\,; \quad q * a = (a * q)^\sim .$$

Then

$$q \cdot w = \tilde{w} \cdot q \text{ and } q * w = (\tilde{w} * q)^\sim .$$

since by induction, for $z \in A^*, a \in A$,

$$\begin{aligned} q \cdot za &= (q \cdot z) \cdot a = a \cdot (\tilde{z} \cdot q) = (za)^\sim \cdot q\,, \\ q * za &= (q * z)(q \cdot z * a) = (\tilde{z} * q)^\sim (a * \tilde{z} \cdot q)^\sim \\ &= [(a * \tilde{z} \cdot q)[\tilde{z} * q)]^\sim = [(za)^\sim * q]^\sim . \end{aligned}$$

Thus $|\mathcal{L}|(w) = \big[|\mathcal{R}|(\tilde{w})\big]^\sim$ for all $w \in A^*$, and $\beta = |\mathcal{L}|$. ∎

**Corollary 2.3** *A right sequential function is rational.*

*Proof.* Let $\alpha : A^* \to B^*$ be a right sequential function, and let $\beta$ be defined by $\beta(w) = [\alpha(\tilde{w})]^\sim$. Then $\beta$ is sequential, hence rational, and its graph $S$ is a rational relation. Let $R$ be the graph of $\alpha$. Then $R = \{(\tilde{x}, \tilde{y}) \mid (x, y) \in S\}$, and $R$ is rational (see Section III.4). ∎

**Example 2.2** (*continued*) The function $\alpha$ is not right sequential since it does not preserve suffixes.

**Example 2.3** (*continued*) For the same reason, the function $\tau$ is not right sequential.

**Example 2.4** The basic step for addition in some base $k$ is realized (see Example III.5.16) by a function $\alpha$ which associates, to two words $u, v \in \Bbbk^*$ of the same length, the shortest word $w$ such that $\langle u \rangle + \langle v \rangle = \langle w \rangle$. The number $\langle u \rangle$ can be defined, for $u = a_0 a_1 \cdots a_n$, $(a_i \in \Bbbk)$ either as in Example III.5.16, or by

$$\langle u \rangle = a_0 + a_1 k + \cdots + a_n k^n .$$

This is the "reversal interpretation" which is more convenient when the input is read from left to right, as will be done here. Since $u$ and $v$ have the same length, $\alpha$ can be considered as a function $\alpha : \Bbbk^* \times \Bbbk^* \to \Bbbk^*$. If $v = b_0 b_1 \cdots b_n$, then the argument of $\alpha$ is $x = (a_0, b_0)(a_1, b_1) \cdots (a_n, b_n)$. For simplicity, we write indistinctly $\alpha(u, v)$ or $\alpha(x)$. By Example III.5.16, $\alpha$ is known to be rational, but $\alpha$ is neither left nor right sequential. Consider for instance $k = 2$. Then

$$\alpha(11, 10) = w_1 = 001 \quad \alpha(11111, 10010) = w_2 = 000101 .$$

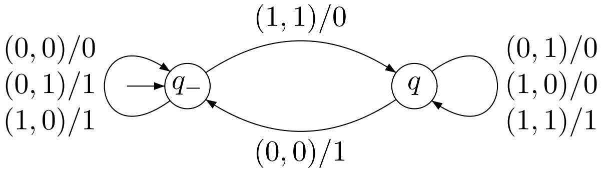

Figure IV.4

The word $x_1 = (1,1)(1,0)$ is both a prefix and a suffix of $x_2 = (1,1)(1,0)(1,0)(1,1)(1,0)$, but $w_1$ is neither a prefix nor a suffix of $w_2$. Now consider the following (left) sequential transducer (Figure IV.4) and let $\beta$ be the sequential function realized. Then

$$\alpha(x) = \begin{cases} \beta(x) & \text{if } q_- \cdot x = q_-; \\ \beta(x)1 & \text{if } q_- \cdot x = q. \end{cases}$$

Thus $\alpha$ is "almost" a sequential function. This leads to the following definition.

**Definition** A (left) *subsequential transducer* $\mathcal{S} = \langle A, B, Q, q_-, \rho \rangle$ is composed of a sequential transducer $\langle A, B, Q, q_- \rangle$ and of a partial function $\rho : Q \to B^*$. The partial function $|\mathcal{S}| : A^* \to B^*$ *realized* by $\mathcal{S}$ is defined by

$$|\mathcal{S}|(x) = (q_- * x)\rho(q_- \cdot x)\,. \tag{2.6}$$

A *subsequential function* is a partial function realized by some subsequential transducer.

According to the discussion at the beginning of this section, $\rho(q_- \cdot x)$ has the value 0 in (2.6) whenever $q_- \cdot x = 0$.

**Example 2.4** (*continued*) The function $\alpha$ is subsequential with $\rho(q_-) = \varepsilon$, $\rho(q) = 1$.

**Example 2.5** Any sequential function is subsequential: it suffices to define $\rho(q)$ to be the empty word for all $q \in Q$.

**Example 2.6** Any partial function with finite domain is subsequential (this is not true for sequential functions). Consider indeed $\alpha : A^* \to B^*$ and suppose $\text{dom}(\alpha)$ is finite. We define a subsequential transducer $\mathcal{S} = \langle A, B, Q, q_-, \rho \rangle$ as follows: $Q = \text{dom}(\alpha)(A^*)^{-1}$ is the set of prefixes of words in $\text{dom}(\alpha)$; $q_- = 1$. The next state and the output functions are defined for $u \in Q, a \in A$ by

$$u \cdot a = \begin{cases} ua & \text{if } ua \in Q; \\ 0 & \text{otherwise} \end{cases} \qquad u * a = \begin{cases} 1 & \text{if } ua \in Q; \\ 0 & \text{otherwise} \end{cases}$$

Finally

$$\rho(u) = \begin{cases} \alpha(u) & \text{if } u \in \text{dom}(\alpha); \\ 0 & \text{otherwise} \end{cases} \qquad u \in Q\,.$$

Then clearly $\alpha = |\mathcal{S}|$.

**Example 2.7** The function $\tau$ of Example 2.3 is not subsequential. Assume indeed that $\tau = |\mathcal{S}|$ for $\mathcal{S}$ as in the definition and set $K = \max\{|\rho(q)| : \rho(q) \neq 0, q \in Q\}$. Let $n$ be even. Then

$$\begin{aligned}
|\mathcal{S}|(a^n) &= (q_- * a^n)\rho(q_- \cdot a^n) = b^n \\
|\mathcal{S}|(a^{n+1}) &= (q_- * a^n)(q_- \cdot a^n * a)\rho(q_- \cdot a^{n+1}) = c^{n+1}
\end{aligned}$$

If $n > K$, then $w = q_- * a^n$ is not the empty word, and $w \in b^+ \cap c^+$, which is impossible.

**Proposition 2.4** *A subsequential function is rational.*

*Proof.* Consider a subsequential transducer $\mathcal{S} = \langle A, B, Q, q_-, \rho\rangle$ and define a morphism $\mu : A^* \to \mathrm{Rat}(B^*)^{Q\times Q}$ by

$$\mu a_{p,q} = \begin{cases} p * a & \text{if } p \cdot a = q; \\ 0 & \text{otherwise.} \end{cases} \qquad (a \in A) \tag{2.7}$$

Then an obvious induction shows that (2.7) still holds when $a$ is replaced by a word $w \in A^*$. Next consider $\rho$ as a column $Q$-vector, and define a row vector $\lambda$ by

$$\lambda_q = \begin{cases} 1 & \text{if } q = q_-; \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\lambda\mu w\rho = \bigcup_{q\in Q} \mu w_{q_-,q}\rho(q) = (q_- * w)\rho(q_- \cdot w) = |\mathcal{S}|(w)\,.$$

Thus $|\mathcal{S}|$ is rational by Proposition III.7.3. ■

Note that the matrices $\mu w$ of the preceding proof are *row monomial*, that is for each $p \in Q$, there is at most one $q \in Q$ such that $\mu w_{p,q} \neq 0$. Thus the transductions $w \mapsto \mu w_{q_-,q}$ for $q \in Q$ have disjoint domains, and the same holds for the transductions $w \mapsto \mu w_{q_-,q}\rho(q)$.

**Proposition 2.5** *Let $\alpha : A^* \to B^*$ and $\beta : B^* \to C^*$ be subsequential functions. Then $\beta \circ \alpha : A^* \to C^*$ is subsequential. If further $\alpha$ and $\beta$ are sequential (right sequential), then $\beta \circ \alpha$ is sequential (right sequential).*

*Proof.* Consider two subsequential transducers

$$\mathcal{S} = \langle A, B, Q, q_-, \rho\rangle, \quad \mathcal{T} = \langle B, C, P, p_-, \sigma\rangle$$

realizing $\alpha$ and $\beta$ respectively. Elements of the product $P \times Q$ are noted $[p, q]$ for easier checking. Define

$$\mathcal{T} \circ \mathcal{S} = \langle A, C, P \times Q, [p_-, q_-], \omega\rangle$$

$$[p, q] \cdot a = [p \cdot (q * a), q \cdot a] \tag{2.8}$$

$$[p, q] * a = p * (q * a) \qquad p \in P, q \in Q, a \in A \tag{2.9}$$

$$\omega([p, q]) = (p * \rho(q))\sigma(p \cdot \rho(q))\,. \tag{2.10}$$

We prove that (2.8) and (2.9) remain true if $a$ is replaced by a word $w \in A^*$. This is clear for $x = 1$. Arguing by induction, consider $x = za$, with $z \in A^*$, $a \in A$, and set

$$w = q * z\,, \quad w' = q \cdot z * a\,.$$

Then $ww' = q * za = q * x$ by (2.3). Next

$$\begin{aligned}
[p, q] \cdot x &= [p \cdot (q * z), q \cdot z] \cdot a = [p \cdot w, q \cdot z] \cdot a \\
&= [p \cdot w \cdot (q \cdot z * a), q \cdot z \cdot a] \\
&= (p \cdot ww', q \cdot za] = [p \cdot (q * x), q \cdot x]\,. \\
[p, q] * x &= ([p, q] * z)([p, q] \cdot z * a) = (p * (q * z))([p \cdot (q * z), q \cdot z] * a) \\
&= (p * w)([p \cdot w, q \cdot z] * a) \\
&= (p * w)(p \cdot w * (q \cdot z * a)) = (p * w)(p \cdot w * w') = p * ww' \\
&= p * (q * x)\,.
\end{aligned}$$

Finally

$$\begin{aligned}
\omega([p_-, q_-] \cdot x) = \omega(&[p_- \cdot (q_- * x), q_- \cdot x]) \\
&= (p_- \cdot (q_- * x) * \rho(q_- \cdot x))\sigma(p_- \cdot (q_- * x) \cdot \rho(q_- \cdot x)) \\
&= (p_- \cdot (q_- * x) * \rho(q_- \cdot x))\sigma(p_- \cdot \alpha(x))\,.
\end{aligned}$$

Consequently

$$\begin{aligned}
|\mathcal{T} \circ \mathcal{S}|(x) &= ([p_-, q_-] * x)\omega([p_-, q_-] \cdot x) \\
&= (p_- * (q_- * x))(p_- \cdot (q_- * x) * \rho(q_- \cdot x))\sigma(p_- \cdot \alpha(x)) \\
&= (p_- * (q_- * x)\rho(q_- \cdot x))\sigma(p_- \cdot \alpha(x)) \\
&= (p_- * \alpha(x)\sigma(p_- \cdot \alpha(x)) = \beta(\alpha(x))\,.
\end{aligned}$$

Thus $|\mathcal{T} \circ \mathcal{S}| = \beta \circ \alpha$. If both $\alpha$ and $\beta$ are sequential, then $\rho$ and $\sigma$ can be assumed to have always the value 1. Then by (2.10), $\omega([p, q]) = (p*1)\sigma(p \cdot 1) = 1$ and $\beta \circ \alpha$ is sequential. For right sequential functions, the result follows from Proposition 2.2. ■

If one of the two partial functions $\alpha$ and $\beta$ is left sequential and the other is right sequential, then $\beta \circ \alpha$ is a rational function. It is quite remarkable that conversely any rational function can be factorized as a composition of a left and a right sequential function. This will be proved in Section 5.

A sequential function preserves prefixes. We show now that a subsequential function which preserves prefixes is sequential.

**Proposition 2.6** *Let $\alpha : A^* \to B^*$ be a partial function. Then $\alpha$ is sequential if and only if the following conditions hold:*

(i) *$\alpha$ is subsequential;*
(ii) *$\alpha$ preserves prefixes.*

*Proof.* Clearly, the conditions are necessary. Conversely, assume that $\alpha$ satisfies (i) and (ii), and consider a subsequential transducer $\mathcal{S} = \langle A, B, Q, q_-, \rho \rangle$ realizing

$\alpha$. We first put $\mathcal{S}$ into some standard form. Consider a state $q \in Q$. If $q$ is not accessible, that is if there is no word $u$ such that $q_- \cdot u = q$, then the state $q$ can clearly be deleted. Thus we may assume that all states are accessible. Next, if $\rho(q) = 0$, then $\alpha(u) = 0$ for all $u \in A^*$ such that $q_- \cdot u = q$, and further $\alpha(uv) = 0$ for all $v \in A^*$ since $\alpha$ preserves prefixes. Consequently, if the next state function and the output function are modified be setting $q' \cdot a = 0$, $q' * a = 0$ for all $(q', a)$ such that $q' \cdot a = q$, then the new subsequential transducer realizes the same function. Thus $q$ can be deleted (since it is no longer accessible), and consequently we can assume that $\rho(q) \neq 0$ for all $q \in Q$.

Next, we claim that for all $q \in Q$, $a \in A$, there exists $\lambda(q, a) \in B^* \cup \{\emptyset\}$ such that

$$\rho(q)\lambda(q, a) = (q * a)\rho(q \cdot a) \tag{2.11}$$
$$\lambda(q, a) \neq 0 \iff q * a \neq 0\,. \tag{2.12}$$

Indeed, (2.12) follows from (2.11) since $\rho(q) \neq 0$ for all $q \in Q$. Next, in order to prove (2.11), let $u$ be a word such that $q_- \cdot u = q$. If $q * a \neq 0$ then

$$\alpha(ua) = (q_- * u)(q * a)\rho(q \cdot a) \neq 0\,,$$

and since $\alpha$ preserves prefixes,

$$\alpha(ua) = \alpha(u)y = (q_- * u)\rho(q)y$$

for some word $y \in B^*$. Thus

$$\rho(q)y = (q * a)\rho(q \cdot a)$$

showing that $y$ is independent of $u$. We define

$$\lambda(q, a) = \begin{cases} y & \text{if } q * a \neq 0; \\ 0 & \text{otherwise.} \end{cases}$$

Then $\lambda$ has the same domain as the output function of $\mathcal{S}$.

Consider now the sequential transducer $\mathcal{L} = \langle A, B, Q, q_- \rangle$ with the same next state function as $\mathcal{S}$, and with output function $\lambda$. We claim that $\alpha = |\mathcal{L}|$, that is that $\alpha(x) = \lambda(q_-, x)$ for $x \in A^*$. By $(ii)$, this holds for $x = 1$. If $x = za$ with $z \in A^*$, $a \in A$, then

$$\begin{aligned} \lambda(q_-, x) &= \lambda(q_-, z)\lambda(q_- \cdot z, a) = \alpha(z)\lambda(q_- \cdot z, a) \\ &= (q_- * z)\rho(q_- \cdot z)\lambda(q_- \cdot z, a) \\ &= (q_- * z)(q_- \cdot z * a)\rho(q_- \cdot za) = \alpha(za)\,. \end{aligned}$$

■

Subsequential functions preserve prefixes only if they are sequential. However, they satisfy a property which is closely related to the preservation of prefixes. Consider indeed a subsequential transducer $\mathcal{S} = \langle A, B, Q, q_-, \rho \rangle$, and let $\alpha = |\mathcal{S}|$. If $u_1, u_2 \in \mathrm{dom}(\alpha)$ are "near" in the sense that $u_1 = uv_1$, $u_2 = uv_2$ and $|v_1| + |v_2|$ is "small", then $\alpha(u_1)$ and $\alpha(u_2)$ are also near, since

$$\alpha(uv_i) = (q_- * u)(q_- \cdot u * v_i)\rho(q_- \cdot uv_i) \quad i = 1, 2\,,$$

and the length of the words $(q_- \cdot u * v_i)\rho(q_- \cdot uv_i)$ are bounded by some function of $|v_1|$ and $|v_2|$. This observation expresses some topological property. In order to explain it, we introduce some definitions.

For words $u, v \in A^*$, we define

$$u \wedge v = \text{the greatest common prefix of } u \text{ and } v\,.$$

More generally, if $X$ is a nonempty language, define

$$\bigwedge X = \text{the longest word which is a prefix of all words in } X\,.$$

The notation is justified by the following remark: Define a relation $\preceq$ by: $u \preceq v$ if and only if $u$ is a prefix of $v$. Then $\preceq$ is a partial order, sometimes called the "prefix order". Since $u \preceq v$ if and only if $u \wedge v = u$, $A^*$ is a semi-lattice, and $u \wedge v$ is the greatest lower bound of $u$ and $v$.

**Definition** The (left) *distance* of $u$ and $v$ is the number

$$\|u, v\| = |u| + |v| - 2|u \wedge v|\,.$$

Thus, $\|u, v\|$ is the sum of the length of those words which remain when the greatest common prefix of $u$ and $v$ is erased. In order to verify that we get a distance, we first observe that $\|u, v\| = 0$ if and only if $|u|+|v| = 2|u \wedge v|$. Since $|u \wedge v| \leq |u|, |v|$, this is equivalent to $|u \wedge v| = |u| = |v|$, that is to $u = v$. Next, we verify that

$$\|u, v\| \leq \|u, w\| + \|w, v\| \quad u, v, w \in A^*\,.$$

A straightforward computation shows that this inequality is equivalent to

$$|u \wedge w| + |w \wedge v| \leq |w| + |u \wedge v|\,.$$

Since $u \wedge w$ and $v \wedge w$ are prefixes of $w$, either $u \wedge w$ is a prefix of $v \wedge w$, thus of $u$ and of $v$, and $|u \wedge w| \leq |u \wedge v|$ or $v \wedge w$ is a prefix of $u$ and of $v$, and $|v \wedge w| \leq |u \wedge v|$. Both cases give the desired inequality.

From $|u \wedge v| \leq |u|, |v|$, we obtain immediately

$$\big||u| - |v|\big| \leq \|u, v\| \quad u, v \in A^*\,. \tag{2.13}$$

Another useful inequality is the following: if $X \subset A^*$, $X \neq \emptyset$, and $w = \bigwedge X$, then

$$\|w, u\| \leq \max_{x,y \in X} \|x, y\| \quad u \in X\,. \tag{2.14}$$

Indeed, for any $u \in X$, there is some $v \in X$ such that $u \wedge v = w$ (since otherwise $w$ would be a proper prefix of all $u' \wedge v$, $(v \in X)$ for some $u' \in X$, thus of all $v \in X$). Consequently $\|w, u\| = \|u \wedge v, u\| \leq \|v, u\| \leq \max_{x,y \in X} \|x, y\|$.

**Definition** A partial function $\alpha : A^* \to B^*$ has *bounded variation* if and only if for all $k \geq 0$, there exists $K \geq 0$ such that

$$u, v \in \operatorname{dom}(\alpha), \|u, v\| \leq k \implies \|\alpha(u), \alpha(v)\| \leq K\,.$$

**Example 2.8** A subsequential function has bounded variation. Let indeed $\alpha = |\mathcal{S}|$ with $\mathcal{S} = \langle A, B, Q, q_-, \rho \rangle$, and set

$$M = \max\{|q * a| : q \in Q, a \in A, q * a \neq 0\}\,,$$
$$N = \max\{|\rho(q)| : q \in Q, \rho(q) \neq 0\}\,.$$

If $uv \in \mathrm{dom}(\alpha)$, then $\alpha(uv) = (q_- * u)(q_- \cdot u * v)\rho(q_- \cdot uv)$. Thus $|\alpha(uv)| \leq |q_- * u| + |v| \cdot M + N$. Let $k \geq 0$, and define $K = k \cdot M + 2N$. If $u_1, u_2 \in \mathrm{dom}(\alpha)$ and $\|u_1, u_2\| \leq k$, then $u_1 = uv_1$, $u_2 = uv_2$, with $|v_1| + |v_2| \leq k$. Consequently $\alpha(uv_1) = (q_- * u)w_1$, $\alpha(uv_2) = (q_- * u)w_2$ and

$$\|\alpha(uv_1), \alpha(uv_2)\| \leq |w_1| + |w_2| \leq (|v_1| + |v_2|)M + 2N \leq K\,.$$

Note that for $M' = \max(M, 2N)$, we have a stronger inequality:

$$\|\alpha(u_1), \alpha(u_2)\| \leq M'(1 + \|u_1, u2\|)\,.$$

The following result gives a characterization of subsequential functions.

**Theorem 2.7** (Choffrut (1978)) *Let $\alpha : A^* \to B^*$ be a partial function. Then $\alpha$ is subsequential if and only if*

(i) *$\alpha$ has bounded variation;*
(ii) *for all $L \in \mathrm{Rat}(B^*)$, $\alpha^{-1}(L) \in \mathrm{Rat}(A^*)$.*

This theorem is an extension of a characterization of sequential functions:

**Theorem 2.8** (Ginsburg and Rose (1966)) *Let $\alpha : A^* \to B^*$ be a partial function. Then $\alpha$ is sequential if and only if*

(i) *$\alpha$ preserves prefixes;*
(ii) *there exists an integer $M$ such that, for all $u \in A^*$, $a \in A$:*

$$ua \in \mathrm{dom}(\alpha),\ \alpha(ua) = \alpha(u)y \quad \textit{imply} \quad |y| \leq M\,;$$

(iii) *for all rational languages $L \subset B^*$, $\alpha^{-1}(L)$ is a rational language.*

*Proof.* In order to deduce Theorem 2.8 from Theorem 2.7, it suffices to show that $\alpha$ has bounded variation. The desired conclusion then follows by Proposition 2.6. Let $k \geq 0$, and let $uv_1, uv_2 \in \mathrm{dom}(\alpha)$ be such that $v_1 \wedge v_2 = 1$, and $\|uv_1, uv_2\| = |v_1| + |v_2| \leq k$. Then $\alpha(uv_1) = \alpha(u)y_1$, $\alpha(uv_2) = \alpha(u)y_2$ and, by (ii), $|y_1| < |v_1|M$, $|y_2| < |v_2|M$. Consequently $\|\alpha(uv_1), \alpha(uv_2)\| \leq |y_1| + |y_2| \leq kM$. ■

*Proof* of Theorem 2.7. This proof is an adaptation of the proof of the Ginsburg-Rose Theorem, as given for instance in Ginsburg (1966) or in Eilenberg (1974). Since a subsequential function verifies (i) and (ii), we have to prove that these conditions are sufficient.

The proof is in four parts. We first associate to $\alpha$ a finite set $R$ of partial functions from $A^*$ into $B^*$. We then prove that a certain family $X_r$, $(r \in R)$ of subset of $A^*$ is composed of regular languages. This enables us to construct a machine realizing $\alpha$, which works like a subsequential transducer excepted that the output function has its values in the free group $B^{(*)}$ generated by $B$. The last

step consists in replacing this transducer by a sequential transducer satisfying our definition. We use the following abbreviation:
If $C$ is an alphabet and $n \geq 0$ is an integer, then

$$C^{(n)} = 1 \cup C \cup \cdots \cup C^n = C^* \setminus C^n C^+ .$$

Let $\alpha : A^* \to B^*$ satisfy (i) and (ii). Then $\mathrm{dom}(\alpha) = \alpha^{-1}(B^*)$ is a regular language by (ii). Let $N$ be the number of states of a finite automaton recognizing $\mathrm{dom}(\alpha)$. Then we note, for later reference, that

$$uA^* \cap \mathrm{dom}(\alpha) \neq \emptyset \quad \text{if and only if} \quad uA^{(N-1)} \cap \mathrm{dom}(\alpha) \neq \emptyset . \tag{2.15}$$

Indeed, if $uv \in \mathrm{dom}(\alpha)$ and $|v| \geq N$, then there exists, by the Iteration Lemma for Regular Languages, a word $v'$ such that $|v'| < |v|$ and $uv' \in \mathrm{dom}(\alpha)$.

For $u \in A^*$, define

$$J(u) = \{v \in A^{(N)} \mid \alpha(uv) \neq \emptyset\}$$

and define a partial function $\beta : A^* \to B^*$ by

$$\beta(u) = \begin{cases} 0 & \text{if } J(u) = \emptyset; \\ \bigwedge\{\alpha(uv) \mid v \in J(u)\} & \text{otherwise.} \end{cases}$$

Thus $\beta(u) \neq 0$ if and only if $J(u) \neq \emptyset$ if and only if $uA^{(N)} \cap \mathrm{dom}(\alpha) \neq \emptyset$. In this case there exists, for $v \in J(u)$, a word $r_u(v) \in B^*$ such that

$$\alpha(uv) = \beta(u) r_u(v) \tag{2.16}$$

and further there are words $v_1, v_2 \in J(u)$ such that

$$r_u(v_1) \wedge r_u(v_2) = 1 . \tag{2.17}$$

(Note that (2.17) holds even if $J(u)$ is a singleton $v$ since then $r_u(v) = 1$.) We complete the definition by setting $r_u(v) = 0$ for $v \in A^{(N)} \setminus J(u)$. Thus, for any $u \in A^*$, there is a partial function $r_u$ from $A^{(N)}$ into $B^*$ satisfying (2.16), with $\mathrm{dom}(r_u) = J(u)$. Further $\alpha(u) \neq 0$ if and only if $1 \in J(u)$ if and only if $r_u(1) \neq 0$.

a) We prove that there exists an integer $M$ such that $\max\{|r_u(v)| : v \in \mathrm{dom}(r_u)\} \leq M$ for all $u \in A^*$. For this, consider $v_1, v_2 \in J(u)$. Then $\|uv_1, uv_2\| \leq |v_1 + |v_2| \leq 2N$. In view of condition (i), there exists an integer $M$ such that

$$\|\alpha(uv_1), \alpha(uv_2)\| \leq M \quad v_1, v_2 \in J(u) .$$

Consequently, by (2.14),

$$|r_u(v) = \|\beta(u), \alpha(uv)\| \leq \max_{v_1, v_2 \in J(u)} \|\alpha(uv_1), \alpha(uv_2)\| \leq M$$

for all $v \in J(u)$. Thus each $r_u$ is a partial function $A^{(N)} \to B^{(M)}$ and the set

$$R_u = \{r_u \mid u \in A^*\}$$

as a subset of the finite set of all partial function from $A^{(N)}$ into $B^{(M)}$ is itself finite. We note $\mathbf{0}$ the partial function $A^{(N)} \to B^{(M)}$ with empty domain.

b) For $r \in R$, define $X_r = \{u \in A^* \mid r_u = r\}$. We claim: the languages $X_r$ are rational. To prove this, define for $i = 0, \ldots, 2M$ and $z \in B^M$:

$$D_{i,z} = \{y \in B^* : |y| \equiv i \pmod{2M+1} \text{ and } (y \in B^*z \text{ or } z \in B^y)\}\,.$$

(Note that there is at most one $y \in D_{i,z}$ such that $z \in B^*y$.) Clearly the language $D_{i,z}$ is rational. Consider a fixed $r \in R$ and define

$$\begin{aligned} L_{v,i,z} &= [\alpha^{-1}(D_{i,z}r(v))]v^{-1} \quad \text{for } \ v \in \operatorname{dom}(r) \\ K_v &= [A^* \setminus \operatorname{dom}(\alpha)]v^{-1} \quad \text{for } \ v \in A^{(N)} \setminus \operatorname{dom}(r)\,. \end{aligned}$$

By (ii), these languages are rational. Set

$$K = \bigcap_{v \in A^{(N)} \setminus \operatorname{dom}(r)} K_v\,; \quad L_{i,z} \bigcap_{v \in \operatorname{dom}(r)} L_{v,i,z}\,; \quad Y_r = K \cap \Big(\bigcup_{i=0}^{2M} \bigcup_{z \in B^M} L_{i,z}\Big)\,.$$

Then $Y_r$ is a rational language. We show that $Y_r = X_r$, which proves the claim.

Consider first $u \in Y_r$. We must show that $r_u = r$. There exist $i \in \{0, \ldots, 2M\}$, $z \in B^M$ such that $u \in K \cap L_{i,z}$. Thus if $v \in \operatorname{dom}(r)$, $\alpha(uv) \in D_{i,z}r(v)$, and if $v \in A^{(N)} \setminus \operatorname{dom}(r)$, then $\alpha(uv) = 0$. Thus $\operatorname{dom}(r) = \operatorname{dom}(r_u)$. If $r = \mathbf{0}$, then $r = r_u$. Next if $\operatorname{dom}(r)$ is a singleton $v$, then since $r = r_{u'}$ for some $u' \in A^*$, $r(v) = 1$ by the remark following (2.17), and $r = r_u$. Thus assume $\operatorname{Card}(\operatorname{dom}(r)) \geq 2$. Then for each $v \in \operatorname{dom}(r)$, there is a word $y_v \in D_{i,z}$ such that

$$\alpha(uv) = \beta(u)r_u(v) = y_v r(v)\,, \tag{2.18}$$

and it suffices to show that $y_v = \beta(u)$ for $v \in \operatorname{dom}(r)$. Let $v, v' \in \operatorname{dom}(r)$. By (2.13), we have

$$\begin{aligned} |y_v| - |y_{v'}| &= |\alpha(uv)| - |\alpha(uv')| + |r(v')| - |r(v)| \\ &\leq \|\alpha(uv), \alpha(uv')\| + M \leq 2M\,, \end{aligned}$$

thus $\big||y_v| - |y_{v'}|\big| \leq 2M$. Since further $|y_v| \equiv |y_{v'}| \pmod{2M+1}$, it follows that $|y_v| = |y_{v'}|$ for all $v, v' \in \operatorname{dom}(r)$. Let $n$ be the common length of the words $y_v$ $(v \in \operatorname{dom}(r))$.

Since $r = r_{u'}$ for some $u' \in A^*$, there exist, by (2.17), words $v_1, v_2 \in \operatorname{dom}(r)$ such that $r(v_1) \wedge r(v_2) = 1$. Consider (2.18) for these words. This shows that $|\beta(u)| \leq n$. Next, let $v_1, v_2$ be two words in $\operatorname{dom}(r)$ such that $r_u(v_1) \wedge r_u(v_2) = 1$. By (2.18) there are words $y_1, y_2$ of the same length such that

$$r_u(v_1) = y_1 r(v_1)\,, \quad r_u(v_2) = y_2 r(v_2)\,.$$

Therefore $|y_1| = |y_2| \leq M$ and $y_1, y_2$ are both suffixes of $z$. Thus $y_1 = y_2$. Since $r_u(v_1) \wedge r_u(v_2) = 1$, $y_1 = y_2 = 1$ and $|\beta(u)| = n$. Thus $u \in X_r$.

Conversely, let $u \in X_r$. If $r = r_u = \mathbf{0}$, then $L_{i,z} = A^*$ for all $i$ and all $z$, and clearly $u \in K$. Thus $u \in Y_r$ in this case. Thus assume $\operatorname{dom}(r) \neq \emptyset$, and let $i$ be the integer such that $0 \leq i \leq 2M$ and $|\beta(u)| \equiv i \pmod{2M+1}$. Next let $z$ be either the unique suffix of length $M$ of $\beta(u)$ if $|\beta(u)| \geq M$, or any word in $B^M \cap B^*\beta(u)$ otherwise. Then $\alpha(uv) \in D_{i,z}r(v)$ for any $v \in \operatorname{dom}(r)$, and consequently $u \in L_{i,z}$. Since clearly $u \in K$, we have $u \in Y_r$.

c) Let $\mathcal{S}' = \langle A, Q', q_- \rangle$ be an accessible semiautomaton recognizing simultaneously all $X_r$ for $r \in R$ (for the construction, see Section I.4). Then for each $r \in R$, there is a subset $Q_r$ of $Q'$ such that

$$X_r = |\mathcal{S}'(Q_r)| = \{u \in A^* \mid q_- \cdot u \in Q_r\}\,.$$

Clearly the $Q_r$ are pairwise disjoint and $Q' = \cup_{r \in R} Q_r$. Next set

$$R_+ = \{r \in R \mid r(1) \neq 0\} \quad Q_+ = \cup_{r \in R_+} Q_r\,.$$

Then $\mathbf{0} \notin R_+$ and $\operatorname{dom}(\alpha) = |\mathcal{S}'(Q_+)|$. Observe that

$$u \in X_{\mathbf{0}} \iff q_- \cdot u \in Q_{\mathbf{0}} \iff \beta(u) = 0 \tag{2.19}$$

and that further, in view of (2.15),

$$u \in X_{\mathbf{0}} \iff uA^* \cap \operatorname{dom}(\alpha) = \emptyset \iff uA^{(N-1)} \cap \operatorname{dom}(\alpha) = \emptyset\,. \tag{2.20}$$

Thus $u \in X_{\mathbf{0}}$ implies $uA^* \subset X_{\mathbf{0}}$ (in other terms, $X_{\mathbf{0}}$ is a right ideal). Thus $q \in Q_{\mathbf{0}}$ implies $q \cdot x \in Q_{\mathbf{0}}$ for all $x \in A^*$, and further $q_- \notin Q_{\mathbf{0}}$ since otherwise $\alpha = 0$ and there is nothing to prove.

Define $\mathcal{S} = \langle A, Q, q_- \rangle$ by setting $Q = Q' \setminus Q_{\mathbf{0}}$, and by defining the next state function of $\mathcal{S}$ to be the partial function obtained by restriction of the next state function of $\mathcal{S}'$ to $Q$. Thus $q \cdot a = 0$ in $\mathcal{S}$ if and only if $q \cdot a \in Q_{\mathbf{0}}$ in $\mathcal{S}'$. Then for $q \in Q_r \subset Q$, $a \in A$:

$$q \cdot a = 0 \quad \text{if and only if} \quad \operatorname{dom}(\alpha) \cap aA^{(N-1)} = \emptyset\,. \tag{2.21}$$

Indeed, let $u \in A^*$ be such that $q_- \cdot u = q$. Then by (2.20), $q \cdot a = 0$ if and only if $uaA^{(N-1)} \cap \operatorname{dom}(\alpha) = \emptyset$, and this holds if and only if $\operatorname{dom}(r) \cap aA^{(N-1)} = \emptyset$.

After these preliminaries, we now construct a subsequential transducer realizing $\alpha$, but with output function into the free group $B^{(*)}$ generated by $B$. (Since each word in $B^*$ is reduced, $B^*$ can be identified with its image in $B^{(*)}$, and hence $B^*$ can be viewed as a submonoid of $B^{(*)}$. In particular, if $u, v \in B^*$ then $u^{-1}v$ is always a well defined element of $B^{(*)}$, and $u^{-1}v$ is in $B^*$ if and only if $u$ is a prefix of $v$. See also II.3.) Consider a new state $q_0$, and extend the next state function of $\mathcal{S}$ be setting

$$q_0 \cdot a = q_- \cdot a \quad (a \in A)\,.$$

Next define

$$q_0 * a = \beta(a) \quad (a \in A)\,,$$

and for $q \in Q_r$, $a \in A$,

$$q * a = \begin{cases} 0 & \text{if } q \cdot a = 0; \\ r(av)r'(v)^{-1} & \text{if } q \cdot a \in Q_{r'},\ v \in \operatorname{dom}(r) \cap aA^{(N-1)}\,. \end{cases}$$

First we verify that the definition is correct. If $q \cdot a = q' \in Q_{r'}$, then $\operatorname{dom}(r) \cap aA^{(N-1)} \neq \emptyset$ by (2.20). Thus if $u \in A^*$ is such that $q_- \cdot u = q$, then for $v \in \operatorname{dom}(r) \cap aA^{(N-1)}$,

$$0 \neq \alpha(uav) = \beta(u)r(av) = \beta(ua)r'(v)\,, \tag{2.22}$$

showing first that $r'(v) \neq 0$, and next that $r(av)r'(v)^{-1} = \beta(u)^{-1}\beta(ua)$ is an element of $B^{(*)}$ which is independent of the choice of $v$ in $\mathrm{dom}(r) \cap aA^{(N-1)}$. Thus the next state function and the output function have the same domain. We claim:

$$q_0 * u = \beta(u) \quad u \in A^+ . \tag{2.23}$$

This holds for $|u| = 1$. Arguing by induction, consider $u \in A^+, a \in A$. If $\beta(u) = 0$, then $u \in X_{\mathbf{0}}$, and $ua \in X_{\mathbf{0}}$. Consequently $q_0 * ua = 0 = \beta(ua)$ by (2.19). If $\beta(u) \neq 0$, then $q_0 \cdot u = q$ for some $q \in Q_r$, $(r \in R \setminus \mathbf{0})$. Then by (2.22),

$$q_0 * ua = \beta(u)(q * a) = \begin{cases} 0 & \text{if } q \cdot a = 0 \\ \beta(u)\beta(u)^{-1}\beta(ua) & \text{otherwise.} \end{cases}$$

Since by (2.19) $q \cdot a = 0$ if and only if $\beta(ua) = 0$, (2.23) is proved. Finally define $\rho : q_0 \cup Q \rightarrow B^*$ by $\rho(q_0) = \alpha(1)$ and

$$\rho(q) = \begin{cases} 0 & \text{if } q \notin Q_+ \\ r(1) & \text{if } q \in Q_r \text{ and } r \in R_+ . \end{cases} \qquad q \in Q$$

Then $(q_0 * u)\rho(q_0 \cdot u) = \alpha(u)$ for all $u \in A^*$.

d) It remains to transform the above transducer into a subsequential transducer which agrees with our definition. For $q \in Q \cup q_0$, set

$$U_q = \{u \in A^* \mid q_0 \cdot u = q\}$$
$$\sigma(q) = \text{the longest suffix common to the words } q_0 * u \ (u \in U_q).$$

Then for all $u \in U_q$, there is a word $\theta(u)$ such that $\beta(u) = q_0 * u = \theta(u)\sigma(q)$. Extend the definition by setting $\theta(u) = 0$ whenever $q_0 \cdot u = 0$. Then $\theta : A^* \rightarrow B^*$ is a partial function with the same domain as $\beta$. Let $q \in Q \cup q_0$, and let $u \in U_q$, and suppose that there is a letter $a$ such that $q \cdot a \neq 0$. Then

$$q_0 * ua = \theta(u)\sigma(q)(q * a) = \theta(ua)\sigma(q \cdot a) .$$

Since $q_0 * u$, $q_0 * ua \in B^*$, and $q * a \in B^{(*)}$, there are words $x, y, z \in B^*$ such that $\theta(u)\sigma(q) = xz$, $z^{-1}y = q{*}a$. The last relation shows that $z, y$ are independent of the choice of $u$ in $U_q$. Thus $z$ is a common suffix to all $q_0 * u$ for $u \in U_q$. Consequently $\sigma(q) = tz$ for some $t \in B^*$, and $\sigma(q)(q * a) = w \in A^*$ with $w = tzz^{-1}y = ty$. Thus

$$\theta(u)w = \theta(ua)\sigma(q \cdot a) \quad u \in U_q .$$

Assume $|w| < |\sigma(q \cdot a)|$. Then the words $\theta(u)$ have a nonempty common suffix, in contradiction with the definition of $\sigma(q)$. Thus $|w| \geq |\sigma(q \cdot a)|$, and there is a word $\lambda(q, a) \in B^*$ such that

$$\theta(u)\lambda(q, a) = \theta(ua) \quad (u \in U_q) . \tag{2.24}$$

Define $\lambda(q, a) = 0$ whenever $q \cdot a = 0$, and consider $\mathcal{S}$ equipped with the output function $\lambda$. $\lambda$ and the next state function have the same domain, further $\lambda(q_0, 1) =$

1 and by (2.24) $\theta(u) = \lambda(q_0, u)$ for all $u \in A^*$. Define $\tau : Q \cup q_0 \rightarrow B^*$ by $\tau(q) = \sigma(q)\rho(q)$. Then

$$\alpha(u) = \beta(u)\rho(q_0 \cdot u) = \lambda(q_0, u)\tau(q_0 \cdot u) \quad u \in A^* ,$$

and $\alpha$ is realized by the sequential transducer $\mathcal{S} = \langle A, Q \cup q_0, q_0, \tau \rangle$ with output function $\lambda$. ■

**Remark** Consider a partial function $\alpha : A^* \rightarrow B^*$ realized by a "generalized" sequential transducer defined as a sequential transducer, but with an output function from $A^*$ into the free group $B^{(*)}$. Such a transducer can erase suffixes of an already computed output word, and can replace it by another word. The last part of the preceding proof shows that such a transducer can be simulated by a subsequential transducer working without erasing, that is $\alpha$ is subsequential.

## Exercises

**2.1** Let $\alpha : A^* \rightarrow B^*$ be a partial function, and let # be a new symbol. Show that $\alpha$ is subsequential if and only if there exists a sequential function $\beta : (A \cup \#)^* \rightarrow B^*$ such that $\alpha(u) = \beta(u\#)$ for all $u \in A^*$.

**2.2** Let $\alpha_1, \alpha_2 : A^* \rightarrow B^*$ be sequential functions. Show that if $\alpha_1 \cup \alpha_2$ is a partial function, then $\alpha_1 \cup \alpha_2$ is sequential. Show that $\alpha_1 \cup \alpha_2$ is not necessarily subsequential if $\alpha_1, \alpha_2$ are subsequential.

**2.3** Let $\alpha : A^* \rightarrow B^*$ be a subsequential function, and let $R \subset A^*$ be a rational language. Show that the restriction $\alpha|_R$ is subsequential.

# 3 The Cross-Section Theorem

The following theorem is due to Eilenberg (1974). It will be used in the next section in order to construct special representations for rational functions.

**Theorem 3.1** (Cross-Section Theorem) *Let $\alpha : A^* \rightarrow B^*$ be a morphism. For any rational language $X \subset A^*$, there exists a rational language $Y \subset X$ such that $\alpha$ maps $Y$ bijectively onto $\alpha(X)$.*

Set $Z = \alpha(X)$. The theorem asserts that in each class $X \cap \alpha^{-1}(z)$, $(z \in Z)$ a unique word $u_z$ can be chosen in such a way that the language $Y = \{u_z \mid z \in Z\}$ is rational. The language $Y$ is called a *cross-section* of $\alpha$ on $X$. We shall see that the proof is effective. Thus given $\alpha$ and $X$, a cross-section of $\alpha$ on $X$ can be constructed effectively.

*Proof.* We shall factorize $\alpha$ in morphisms of special form. Therefore we first verify that if $\beta : B^* \rightarrow C^*$ is a second morphism, and if the conclusion holds for $\alpha$ and $\beta$, it also holds for $\beta \circ \alpha : A^* \rightarrow C^*$. Indeed, let $X \subset A^*$ be rational, and let $Y$ be a rational cross-section of $\alpha$ on $X$. Set $Z = \alpha(X) = \alpha(Y)$, and let $T \subset B^*$ be a rational cross-section of $\beta$ on $Z$. Define $U = Y \cap \alpha^{-1}(T)$. Then $U$ is rational, $\alpha$ is injective on $U$, and $\alpha(U) = T$. Since $\beta$ is injective on $T$, it follows that $\beta \circ \alpha$

is injective on $U$. Further $\beta \circ \alpha(U) = \beta(T) = \beta(Z) = \beta \circ \alpha(X)$. Thus $U$ is a cross-section of $\beta \circ \alpha$ on $X$.

Next note that if $\alpha$ is injective, the conclusion holds trivially by taking $Y = X$. Since any morphism $\alpha : A^* \to B^*$ can be factorized into $\alpha = \beta \circ \gamma$, where $\gamma : A^* \to C^*$ is injective and $\beta : C^* \to B^*$ is alphabetic, it suffices to consider the case where $\alpha$ is alphabetic. Further, any alphabetic morphism factorizes into projections and strictly alphabetic morphisms. Thus it suffices to consider the following two cases:

$$\begin{aligned}
&A = \{a_1, \ldots, a_n\}\,, \quad B = \{a_1, \ldots, a_{n-1}\} \quad (n \geq 2)\\
&\alpha(a_i) = a_i\,, \quad i = 1, \ldots, n-1\\
&\alpha(a_n) = a_{n-1} \quad \text{or} \quad \alpha(a_n) = 1\,.
\end{aligned}$$

Define the lexicographical order on $A^*$ by setting $u < v$ if either one of the following cases holds

$$v = uw\,, \text{with } w \neq 1 \qquad \text{or} \qquad u = xa_iy\,,\ v = xa_jy'\,,\ \text{with } i < j.$$

Next define a transduction $\tau : A^* \to A^*$ by setting

$$\tau(u) = \{v \mid v > u \text{ and } \alpha(v) = \alpha(u)\}\,,$$

and set

$$Y = X \setminus \tau(X)\,.$$

Thus for each $u \in X$, the smallest element of $\alpha^{-1}\alpha(u) \cap A$ is selected, and $Y$ is the set of all elements so selected, thus $Y$ is a cross-section of $\alpha$ on $X$.

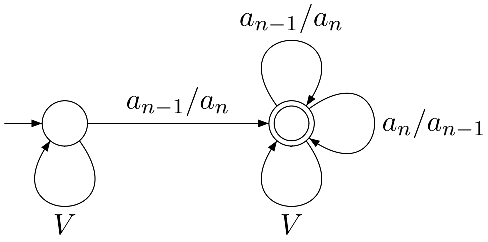

Figure IV.5

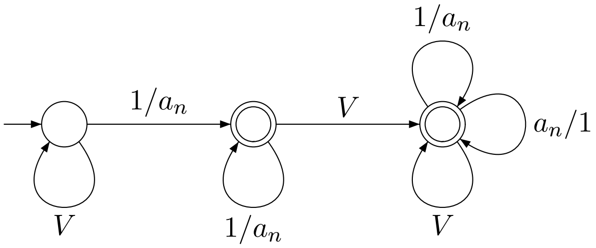

Figure IV.6

To prove that $Y$ is rational, it suffices to show that the transduction $\tau$ is rational. This will be done by constructing transducers realizing $\tau$. If $\alpha(a_n) = a_{n-1}$, we define a transducer by Figure IV.5 with $V = \{a_i/a_i \mid i = 1, \ldots, n\}$. If $\alpha(a_n) = 1$, then we consider the transducer in Figure IV.6. Then it is easily seen that these transducers realize $\tau$. ■

Note that any morphism can be factorized into an injective morphism followed by a projection (Exercise I.3.3). Thus in the above proof, the case $\alpha(a_n) = a_{n-1}$ can be skipped. We conserved it since in the construction of unambiguous representations for rational functions, precisely this case appears, and it is easier to handle directly than through an additional decomposition.

We emphasize the fact that the cross-section $Y$ can be obtained effectively from $X$. Assume $\alpha(a_n) = a_{n-1}$. Then we can proceed as follows. Let $b$ and $c$ be new letters, define $C = A \cup \{b, c\}$, and let $\phi, \psi : C^* \to A^*$ be the morphisms

$$\begin{aligned} &\phi(a_i) = \psi(a_i) = a_i\,, && i = 1, \ldots, n \\ &\phi(b) = \psi(c) = a_{n-1}\,, && \phi(c) = \psi(b) = a_n\,. \end{aligned} \tag{3.1}$$

Then for $X \subset A^*$,

$$\tau(X) = \psi(\phi^{-1}(X) \cap K)$$

where $K$ is the rational language over $C$ recognized by the automaton in Figure IV.7. Thus, if $X$ is given by a finite automaton, finite automata recognizing $\phi^{-1}(X)$, $\phi^{-1}(X) \cap K$, $\tau(X)$ and $X \setminus \tau(X)$ can be effectively constructed.

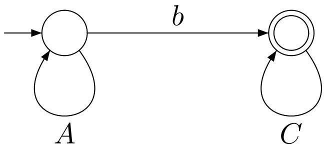

Figure IV.7

**Example 3.1** Let $A = \{a, b\}$ and let $\alpha : A^* \to a^*$ be the morphism given by $\alpha(a) = \alpha(b) = a$. Further, let $X \subset A^*$ be given by Figure IV.8. The lexicographical order is given here by $a < b$. Then

$$\tau(X) = bA^+$$

and the desired cross-section is

$$Y = X \setminus \tau(X) = aba^* \cup b\,.$$

**Example 3.2** Let $A = \{a, b, c, d\}$, and let $\alpha : A^* \to a^*$ be the morphism given by $\alpha(A) = a$, and let $X \subset A^*$ be recognized by Figure IV.9. Thus

$$X = \left[(bdb \cup bc \cup cb)a\right]^*.$$

Define a factorization $\alpha = \alpha_3 \circ \alpha_2 \circ \alpha_1$:

$$A^* \xrightarrow{\alpha_1} \{a, b, c\}^* \xrightarrow{\alpha_2} \{a, b\}^* \xrightarrow{\alpha_3} a^*$$

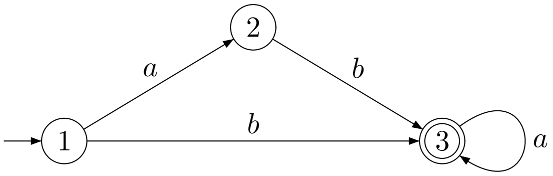

Figure IV.8

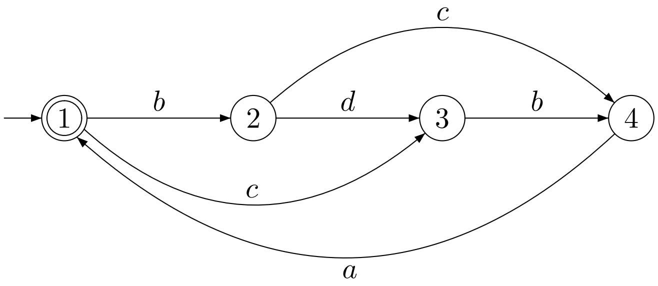

Figure IV.9

by $\alpha_1(d) = c$, $\alpha_2(c) = b$, $\alpha_3(b) = a$, the other letters being unchanged. We compute a cross-section of $\alpha$ on $X$.

First

$$X_1 = \alpha(X) = \left[(bcb \cup bc \cup cb)a\right]^*,$$

and $\alpha_1$ is injective on $X$. Next

$$X_2 = \alpha_2(X_1) = \left[(b^3 \cup b^2)a\right]^*.$$

We have $b < c$, and

$$X_1' = \left[(bcb \cup bc)a\right]^* \subset X_1$$

is a rational cross-section of $\alpha_2$ on $X_1$. Then

$$X_3 = \alpha_2(X_2) = \left[a^4 \cup a^3\right]^*.$$

Since $a < b$, the construction of the proof yields

$$X_2' = (b^2a)^*(1 \cup b^3a \cup (b^3a)^2)$$

as a rational cross-section of $\alpha_3$ on $X_2$. By backward computation

$$X_1'' = X_1' \cap \alpha_2^{-1}(X_2') = (bca)^*(1 \cup bcba \cup (bcba)^2)$$

is a rational cross-section of $\alpha_3 \circ \alpha_2$ on $X_1$, and

$$Y = X \cap \alpha_1^{-1}(A_1'') = (bca)^*(1 \cup bdba \cup (bdba)^2)$$

is a rational cross-section of $\alpha$ on $X$.

## Exercise

**3.1** Replace $\alpha$ in Example 3.1 by $\alpha(a) = \alpha(b) = b$, and compute a cross-section of $\alpha$ on $X$.

# 4 Unambiguous Transducers

We use the Cross-Section Theorem to construct particular representations for rational functions. An alternative construction is also presented which allows a direct computation of these representations.

In this section, a transducer

$$\mathcal{T} = \langle A, B, Q, q_-, Q_+, E \rangle$$

is assumed to satisfy the two conditions

$$E \subset Q \times A \times B^* \times Q\,, \tag{4.1}$$
$$(p, a, z, q), (p, a, z', q) \in E \implies z = z'\,. \tag{4.2}$$

**Definition** The transducer $\mathcal{T}$ is called *unambiguous* if any word $x \in A^*$ is the input label of at most one successful path $e$ in $\mathcal{T}$.

Let $\tau$ be the transduction realized by $\mathcal{T}$. If $\mathcal{T}$ is unambiguous and if $x \in \mathrm{dom}(\tau)$, then there exists a successful path $e$ in $\mathcal{T}$ with input label $x$. Let $y$ be the output label of $e$. Then $\tau(x) = y$. Thus

**Proposition 4.1** *The transduction realized by an unambiguous transducer is a partial function.* ■

Conversely, we have

**Theorem 4.2** (Eilenberg (1974)) *Let $\tau : A^* \to B^*$ be a rational function (with $\tau(1) = 0$ or $\tau(1) = 1$). Then there exists an unambiguous transducer realizing $\tau$.*

*Proof.* By Corollary III.7.2, there are an alphabet $C$, a strictly alphabetic morphism $\alpha : C^* \to A^*$, a rational substitution $\sigma : C^* \to B^*$ and a regular language $K \subset C^*$ such that

$$\tau(x) = \sigma(\alpha^{-1}(x) \cap K) \quad x \in A^*\,.$$

Clearly we may assume $C$ minimal, that is each letter $c \in C$ has at least one occurrence in a word in $\alpha^{-1}(A^*) \cap K$. Then $\sigma$ is a morphism, since $\tau$ is a partial function.

Since $\mathrm{dom}(\tau) = \alpha(K)$, there exists, by the Cross-Section Theorem, a rational language $R \subset K$ that maps bijectively onto $\mathrm{dom}(\tau)$. Let

$$A = \langle C, Q, q_-, Q_+ \rangle$$

be a finite automaton recognizing $R$, and define

$$\begin{aligned} \mathcal{T} &= \langle A, B, Q, q_-, Q_+, E\rangle \\ E &= \{(q, \alpha c, \sigma c, q \cdot c) \mid q \in Q, c \in C\}\,. \end{aligned}$$

Note that $\mathcal{T}$ satisfies (4.1) and (4.2). Indeed, since $\alpha$ is strictly alphabetic, $\alpha c \in A$ for $c \in C$. Next consider two paths

$$\begin{aligned} e &= (q_-, u_1, v_1, q_1) \cdots (q_{n-1}, u_n, v_n, q) \\ e' &= (q_-, u'_1, v'_1, q'_1) \cdots (q_{m-1}, u'_m, v'_m, q') \end{aligned}$$

and let $c_i, c'_j \in C$ be such that $\alpha c_i = u_i$, $(1 \le i \le n)$, $\alpha c'_j = u'_j$, $(1 \le j \le m)$. Assume that $e$ and $e'$ have the same input label $x = \alpha z = \alpha z'$ with $z = c_1 \cdots c_n$, $z' = c'_1 \cdots c'_m$. Since $z, z' \in R$ and $\alpha$ is injective on $R$, it follows that $z = z'$ and $e = e'$. This shows that $\mathcal{T}$ is unambiguous. ■

**Corollary 4.3** *Let $\tau : A^* \to B^*$ be a rational function. Then there exists a normalized unambiguous transducer realizing $\tau$.*

*Proof.* Let $\mathcal{T} = \langle A, B, Q, q_-, Q_+, E\rangle$ be an unambiguous transducer realizing $\tau$. Add two new states $q_0, q_1$ to $Q$, and the transitions

$$\{(q_0, a, z, q) \mid (q_-, a, z, q) \in E\} \cup \{(q, a, z, q_1) \mid (q, a, z, q_+) \in E, q_+ \in Q_+\}$$

to $E$. Take $q_0$ as a new initial state and $\{q_1\}$ or $\{q_0, q_1\}$ as final states, according to $\tau(1) = 0$ or $= 1$. Next the resulting transducer can be made trim by deleting unnecessary states. Clearly it is unambiguous. ■

**Example 4.1** Consider a left sequential transducer. Any path starting at the initial state is successful, and two distinct successful paths have distinct input labels. Thus any left sequential transducer is unambiguous.

**Example 4.2** Let $A = \{a\}$, $B = \{b, c\}$, and consider the transducer in Figure IV.10 realizing the function

$$\tau(a^n) = \begin{cases} b^n & n \text{ even;} \\ c^n & n \text{ odd} \end{cases}$$

The transducer is unambiguous since if $n$ is even the only sucessful path leads to state 3, and if $n$ is odd the only successful path leads to state 2.

**Example 4.3** Consider the transducer of Example 1.2 (Figure IV.11). This transducer is ambiguous. Take as alphabet $C$ the labels of the transitions: $C = \{(a/b), (a/1)\}$, and consider the morphism $\alpha : C^* \to a^*$ defined by $\alpha((a/b)) = \alpha((a/1)) = a$. Then up to a renaming, we are in the situation of Example 3.1. Thus $Y = (a/b)(a/1)(a/b)^* \cup (a/1)$ is a suitable cross-section, giving the unambiguous transducer in Fig IV.12.

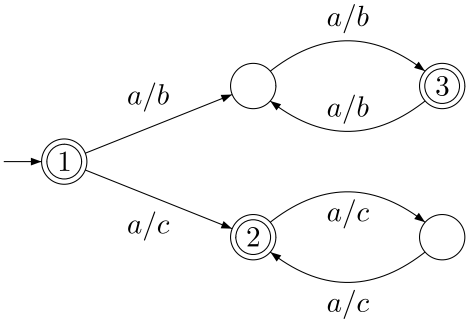

Figure IV.10

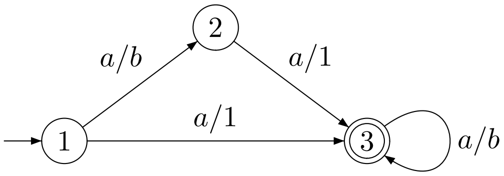

Figure IV.11

**Example 4.4** Consider the ambiguous transducer of Example 1.3 (Figure IV.13). Take again the alphabet $C = \{(a/b), (a/b^2), (a/b^3), (a/b^4)\}$ and the morphism $\alpha$ mapping all letters onto $a$. Then, after a renaming, we are in the situation of Example 3.2. Thus the language

$$\begin{aligned} Y = {} & \big[(a/b)(a/b^3)(a/b^2)\big]^* \cup \big(1 \cup (a/b)(a/b^4)(a/b)(a/b^2) \\ & \cup \big[(a/b)(a/b^4)(a/b)(a/b^2)\big]^2\big) \end{aligned}$$

is a suitable cross-section. This gives the unambiguous transducer in Figure IV.14. The simpler transducer in Figure IV.15 cannot be obtained in that way.

Let $\mathcal{T} = \langle A, B, Q, q_-, Q_+, E\rangle$ be a transducer satisfying (4.1) and (4.2). Define a matrix representation $\mathcal{M} = \langle \mu, Q, q_-, Q_+\rangle$ by

$$\mu a_{p,q} = \begin{cases} z & \text{if } (p,a,z,q) \in E; \\ 0 & \text{otherwise.} \end{cases}$$

**Proposition 4.4** *Assume $\mathcal{T}$ trim. Then $\mathcal{T}$ is unambiguous if and only if $\mathcal{M}$ satisfies the two conditions*

(i) *For $p, q \in Q$, $x, x' \in A^*$, there is at most one $r \in Q$ such that $\mu x_{p,r} \neq 0$ and $\mu x'_{r,q} \neq 0$.*

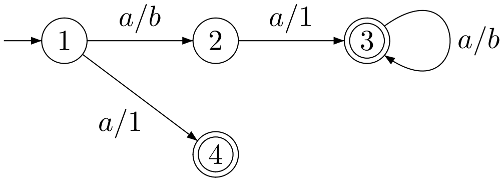

Figure IV.12

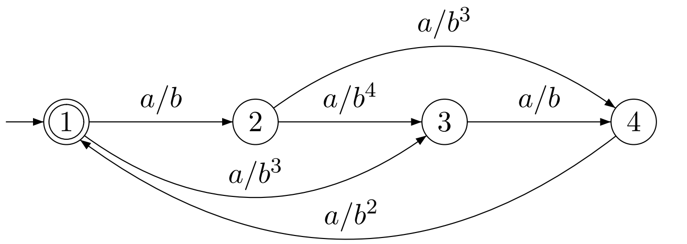

Figure IV.13

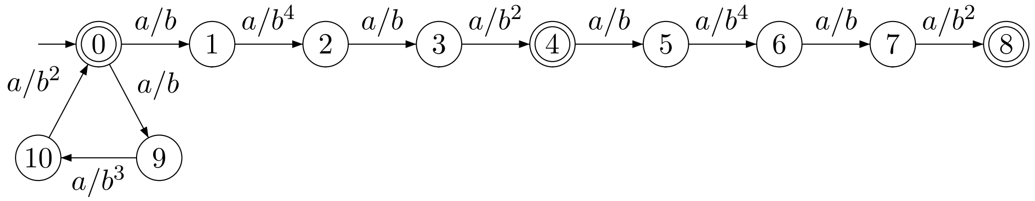

Figure IV.14

(ii) $\mathrm{dom}(\mu_{q_-,q_1}) \cap \mathrm{dom}(\mu_{q_-,q_2}) = \emptyset$ *for* $q_1, q_2 \in Q_+$, $q_1 \neq q_2$.

*Proof.* If $\mathcal{T}$ is unambiguous, then (ii) is clearly satisfies. Next, since $\mathcal{T}$ is trim, for any $p, q \in Q$, there are $z, z' \in A^*$ such that $\mu z_{q_-,p} \neq 0$, $\mu h'_{q,q_+} \neq 0$ for some $q_+ \in Q_+$. Thus if (i) fails for some $p, q \in Q$, $x, x' \in A^*$, then $zxx'z'$ is the input label of at least two successful paths.

Conversely, consider two paths $e_1$ and $e_2$ from $q_-$ to some final states $q_1$ and $q_2$, and assume they have the same input label $x$. Then $q_1 = q_2$ by (ii), and $e_1 = e_2$ by (i). ■

If $\mathcal{M}$ is normalized, then (ii) is satisfied by definition. Thus the unambiguity of $\mathcal{T}$ is equivalent to condition (i).

**Definition** A morphism $\mu$ satisfying condition (i) of Proposition 4.4 is called *unambiguous*.

**Example 4.5** If the matrices $\mu_x$, $(x \in A^*)$ are row monomial, then $\mu$ is unambiguous. Similarly, if the matrices $\mu_x$, $(x \in A^*)$ are column monomial, then $\mu$ is unambiguous.

An unambiguous morphism $\mu : A^* \to \mathrm{Rat}(B^*)^{Q\times Q}$ is called a $(0,1)$-morphism (Schützenberger (1976), Nivat (1968)) for the following reason. Associate to each matrix

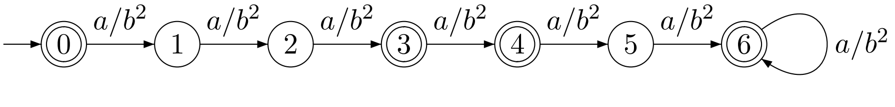

Figure IV.15

$\mu_x$, $(x \in A^*)$ a $Q \times Q$-matrix $\theta\mu x$ with integral entries by

$$\theta\mu x_{p,q} = \begin{cases} 1 & \text{if } \mu x_{p,q} \neq 0; \\ 0 & \text{otherwise.} \end{cases}$$

Then $\theta$ is a morphism if and only if $\mu$ is unambiguous. Thus the product of two such matrices, computed in $\mathbb{N}^{Q\times Q}$, is still a matrix with entries 0 or 1.

Row monomial and column monomial matrix morphisms are special cases of a more general construction.

**Definition** Let $\mu : A^* \to \mathfrak{P}(B^*)^{Q\times Q}$ be a morphism. Then $\mu$ is called *semimonomial* if the set $Q$ is of the form $Q = V \times P$, and if, for any $a \in A$, the following hold:

(i) For any $v \in V$, there is at most one $v' \in V$ such that the submatrix

$$(\mu a)_{v\times P, v'\times P} = (\mu a_{(v,p),(v',p')})_{p,p'\in P}$$

is nonzero.

(ii) any submatrix $(\mu a)_{v\times P, v'\times P}$ is column monomial.

Thus the matrix $\mu a$, considered as a $V \times V$ matrix, whose entries are $P \times P$-matrices is a row monomial matrix, and each of the $P \times P$-block is column monomial. Clearly, the product of two semimonomial matrices with the same index set $V \times P$ is also semimonomial.

**Example 4.6** For $V = \{1, 2, 3\}$ and $P = \{1, 2, 3\}$, the following matrix is semimonomial.

$$\left[\begin{array}{c|c|c} 0 & \begin{matrix} 0 & b & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{matrix} & 0 \\ \hline 0 & 0 & \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{matrix} \\ \hline 0 & 0 & \begin{matrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & b \end{matrix} \end{array}\right]$$

Any semimonomial morphism $\mu$ is unambiguous. Consider indeed two words $x, x'$ and assume

$$\mu x_{(v,p)(v',p')} \neq 0 \quad \text{and} \quad \mu'_{(v',p')(v'',p'')} \neq 0\,.$$

Then $v'$ is uniquely determined by $v$ in view of condition (i), and $p'$ is uniquely determined by $p''$ in view of (ii).

The following theorem asserts the existence of a semimonomial representation for any rational function.

**Theorem 4.5** (Schützenberger (1976)) *Let $\tau : A^* \to B^*$ be a rational function. Then there exists a matrix representation $\mathcal{M} = \langle \mu, Q, q_-, Q_+ \rangle$ realizing $\tau$ such that $\mu$ is semimonomial and*

$$\tau = \sum_{q_+ \in Q_+} \mu_{q_-, q_+}\,.$$

Recall that we use the symbol $\sum$ when the domains $\mathrm{dom}(\mu_{q_-,q_+})$ are disjoint.

*Proof.* Let $\mathcal{M} = \langle \mu, Q, q_-, Q_+\rangle$ be a normalized matrix representation realizing $\tau$. The proof is in two steps. First, the usual power set algorithm for the determinization of an automaton is employed to obtain the set $V$. Then, “unnecessary” entries in the matrices $\mu a$, $(a \in A)$ are deleted to get the row monomial part.

Let $V$ be the family of subsets of $Q$ defined by

$$v \in V \iff \exists x \in A^* : v = \{q \in Q \mid \mu x_{q_-,q} \neq 0\}\,.$$

Thus $v \in V$ if and only if $v$ is the set of states accessible in $\mathcal{M}$ by paths starting in $q_-$ and with input label $x$. A “next state” function $V \times A \to V$ is defined by

$$v \cdot a = \{q' \in Q \mid \exists q \in v, \mu a_{q,q'} \neq 0\}\,.$$

This function is extended to $V \times A^*$ by setting, as usual, $v \cdot 1 = v$, $v \cdot ax = (v \cdot x) \cdot a$,$(x \in A^*, a \in A)$. Then clearly

$$v \cdot xy = (v \cdot x) \cdot y \quad x, y, \in A^*\,.$$

For each $v \in V$, $a \in A$, define a $Q \times Q$-matrix $\bar{\mu}_v a$ in the following way. Set $v' = v \cdot a$, and for each $q' \in v'$, let $p(q')$ be an arbitrary element of $v$ such that $\mu a_{p(q'),q'} \neq 0$. Then

$$(\bar{\mu}_v a)_{q,q'} = 0 \quad q \in Q,\ q' \notin v'\,; \tag{4.3}$$

$$(\bar{\mu}_v a)_{q,q'} = \begin{cases} \mu a_{p(q'),q'} & \text{if } q = p(q'); \\ 0 & \text{if } q \neq p(q'). \end{cases} \quad q' \in v'\,. \tag{4.4}$$

By definition $\bar{\mu}_v a$ is column monomial. It is obtained from $\mu a$ by deleting all but one nonempty element in each column $q' \in v'$, and by setting equal to zero the other columns.

Next, let $S = V \times Q$, and define the morphism

$$\lambda : A^* \to \mathrm{Rat}(B^*)^{S\times S}$$

by blocks for $v, v' \in V$, $a \in A$:

$$(\lambda a)_{v\times Q, v'\times Q} = \begin{cases} 0 & \text{if } v' \neq v \cdot a; \\ \bar{\mu}_v a & \text{if } v' = v \cdot a. \end{cases}$$

Then the matrices $\lambda a$ are semimonomial. Further if $x = a_1 a_2 \cdots a_r$, $(r \geq 1, a_i \in A)$, then clearly

$$(\lambda x)_{v\times Q, v'\times Q} = \begin{cases} 0 & \text{if } v' \neq v \cdot x; \\ \bar{\mu}_v a_1 \bar{\mu}_{v_2} a_2 \cdots \bar{\mu}_{v_r} a_r & \text{if } v' = v \cdot x. \end{cases} \tag{4.5}$$

where $v_2 = v \cdot a_1, \ldots, v_r = v_{r-1} \cdot a_{r-1}$ and $v' = v_r \cdot a_r$.

Next, we prove that for $v_- = \{q_-\}$, $x \in A^+$, $v = v_- \cdot x$,

$$\lambda x_{(v_-,q_-),(v,q)} = \mu x_{q_-,q} \quad q \in Q\,. \tag{4.6}$$

For $|x| = 1$, (4.6) results from (4.4). Arguing by induction, let $x = ya$ with $y \in A^+$, $a \in A$, and let $v' = v_- \cdot y$. Then $v = v' \cdot a$, and

$$(\lambda ya)_{(v_-,q_-),(v,q)} = \bigcup_{r \in v'} \mu y_{q_-,r} (\lambda a)_{(v',r),(v,q)}$$

since $(\lambda y)_{(v_-,q_-),(v',r)} = \mu y_{q_-,r} = 0$ for $r \notin v'$. Next if $q \notin v$, then $(\bar{\mu}_{v'} a)_{r,q} = \mu a_{r,q} = 0$ for $r \in v'$ and $\mu x_{q_-,q} = 0$. Thus (4.6) holds if $q \notin v$. If $q \in v$, then there is a unique $p \in v'$ such that $(\bar{\mu}_{v'} a)_{p,q} = \mu a_{p,q} \neq 0$. Thus

$$(\lambda x)_{(v_-,q_-),(v,q)} = \mu y_{q_-,p}\, \mu a_{p,q} = \mu x_{q_-,q}\,.$$

This proves (4.6). Finally, set $V_+ = \{v \in V \mid q_+ \in v\}$ and let

$$S_+ = \begin{cases} V_+ \times \{q_+\} & \text{if } Q_+ = \{q_+\}; \\ (V_+ \times \{q_+\}) \cup (v_-, q_-) & \text{if } Q_+ = \{q_-, q_+\}. \end{cases}$$

Then $(\lambda 1)_{(v_-,q_-),S_+} = 0$ or $1$ according to $(v_-, q_-) \notin S_+$ or $(v_-, q_-) \in S_+$, and for $x \in A^+$:

$$(\lambda x)_{(v_-,q_-),S_+} = \bigcup_{v \in V_+} \lambda x_{(v_-,q_-),(v,q_+)} = \mu x_{q_-,q_+}\,. \tag{4.7}$$

Indeed, (4.7) holds if $v_- \cdot x \in V_+$ (by (4.6)). If $v_- \cdot x \notin V_+$, that is if $q_+ \notin v_- \cdot x$, then $\mu x_{q_-,q_+} = 0$ and $(\lambda x)_{(v_-,q_-),S_+} = 0$ by (4.5). Since there is at most one $v \in V_+$ such that $v = v_- \cdot x$ for any $x \in A^+$, the functions $\lambda_{(v_-,q_-),(v,q_+)}$ have disjoint domains. This completes the proof. ■

**Example 4.7** Consider the rational function $\alpha : a^* \to b^*$ of Example 4.3, with matrix

$$\mu a = \begin{bmatrix} 0 & b & 1 \\ 0 & 0 & 1 \\ 0 & 0 & b \end{bmatrix}$$

We first compute $V$: $v_1 = v_- = \{1\}$, $v_2 = v_1 \cdot a = \{2, 3\}$, $v_3 = v_2 \cdot a = \{3\} = v_3 \cdot a$. The matrices $\bar{\mu}_i$ (we write $\bar{\mu}_i$ instead of $\bar{\mu}_{v_i}$) are:

$$\bar{\mu}_1 a = \begin{bmatrix} 0 & b & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \quad \bar{\mu}_2 a = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \quad \text{or} \quad \bar{\mu}_2 a = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & b \end{bmatrix} \quad \bar{\mu}_3 a = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & b \end{bmatrix}$$

Thus, there are two possible choices for $\bar{\mu}_2$: each choice yields another matrix $\lambda a$:

$$\lambda a = \begin{bmatrix} 0 & \bar{\mu}_1 a & 0 \\ 0 & 0 & \bar{\mu}_2 a \\ 0 & 0 & \bar{\mu}_3 a \end{bmatrix}$$

With the first matrix $\bar{\mu}_2 a$, the matrix $\alpha a$ is the matrix of Example 4.6. Next, $V_+ = \{v_2, v_3\}$. Thus $S_+ = \{(v_2, 3), (v_3, 3)\}$. In the usual notation, these are the columns 6 and 9. For both morphisms $\lambda$, the row with index $(v_-, 1)$ of $\lambda a^n$ is:

$$(0, 0, 0; 0, b, 1; 0, 0, 0) \quad n = 1\,;$$
$$(0, 0, 0; 0, 0, 0; 0, 0, b^{n-1}) \quad n \geq 2\,.$$

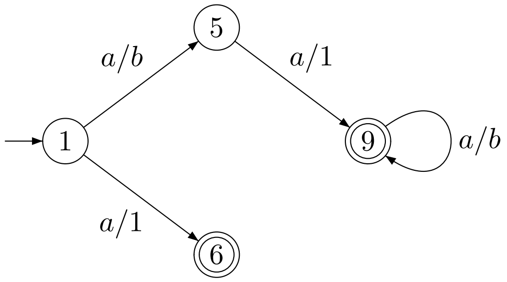

Figure IV.16

Note that $\lambda$ is not trim. The trim transducer associated to $\lambda$ for the first choice of $\bar{\mu}_2 a$ is given in Figure IV.16. Thus we get the same transducer as in Example 4.3.

Semimonomial morphisms are particular unambiguous morphisms. Clearly, an unambiguous morphism is not necessarily semimonomial. There is nevertheless an interesting relation between unambiguous and semimonomial morphisms: any unambiguous morphism can be obtained from some semimonomial morphism by choosing in that morphism some fixed rows and by collapsing columns. This yields some procedure for constructing unambiguous morphisms.

**Definition** Let $\mu : A^* \to \mathrm{Rat}(B^*)^{Q\times Q}$ and $\lambda : A^* \to \mathrm{Rat}(B^*)^{S\times S}$ be two morphisms. Then $\mu$ is *summed up* from $\lambda$ if there exist two functions $\ell : Q \to S$ and $c : Q \to 2^S$ such that

$$\mu x_{p,q} = \lambda x_{\ell(p),c(q)} \Big( \bigcup_{r\in c(q)} \lambda x_{\ell(p),r} \Big) \quad (p, q \in Q,\ x \in A^+)\,.$$

Thus $\mu$ is obtained from $\lambda$ by conserving just one row of $\lambda$ for each $p \in Q$, and by summing up elements of that row according to some rule which is independent from $p$.

**Proposition 4.6** *Let $\mathcal{M} = \langle \mu, Q, q_-, Q_+\rangle$ be a trim matrix representation from $A^*$ into $B^*$. If $\mu$ is unambiguous, then $\mu$ is summed up from some semimonomial morphism.*

*Proof.* Assume $\mu$ is unambiguous. We shall verify that $\mu$ can be extracted from the semimonomial morphism $\lambda$ constructed in the proof of Theorem 4.5. We keep the notations of that proof. First, we claim that for the matrix $\bar{\mu}_v a$ defined by (4.3) and (4.4), we have

$$(\bar{\mu} a)_{q,q'} = \begin{cases} \mu a_{q,q'} & \text{if } q \in v, q' \in Q; \\ 0 & \text{if } q \notin v, q' \in Q. \end{cases} \tag{4.8}$$

Thus $\bar{\mu}_v a$ and $\mu a$ have the same rows with index $q \in v$. Indeed, $(\bar{\mu}_v a)_{q,q'} = 0$ for $q \notin v$ by (4.4), and $(\bar{\mu}_v a)_{q,q'} = \mu a_{q,q'} = 0$ for $q \in v$, $q' \in Q \setminus v'$ by definition of $v' = v \cdot a$. Next, for any $q' \in v'$, there exists a unique $p \in v$ such that $\mu a_{p,q'} \neq 0$, since for any $x$ such that $v_- \cdot x = v$, one has $\mu x_{q,p} \neq 0$ and $\mu a_{p,q'} \neq 0$, and thus $p$ is unique by Proposition 4.4(i). Therefore $(\bar{\mu}_v a)_{p,q'} = \mu a_{p,q'}$ for that $p$, and $(\bar{\mu}_v a)_{q,q'} = \mu a_{q,q'} = 0$ for all $q \in v \setminus p$. Thus (4.8) is proved.

Next, we prove that for $x \in A^+$, $v \in V$, $v' = v \cdot x$,

$$(\lambda x)_{(v,p),(v',q)} = \begin{cases} \mu x_{p,q} & \text{if } p \in v, q \in Q; \\ 0 & \text{i } p \notin v, q \in Q. \end{cases} \tag{4.9}$$

For $|x| = 1$, (4.9) holds by (4.8) in view of the definition of $\lambda$. Arguing by induction, let $x = ya$ with $y \in A^+, a \in A$, $v'' = v \cdot y$, thus $v' = v'' \cdot a$. Then clearly

$$(\lambda x)_{(v,p),(v',q)} = 0 \quad \text{if } p \notin v, q \in Q\,.$$

Thus assume $p \in v$. Then

$$(\lambda x)_{(v,p),(v',q)} = \bigcup_{r \in Q} (\lambda y)_{(v,p),(v'',r)} (\lambda a)_{(v'',r),(v',q)}\,,$$

and since $(\lambda a)_{(v'',r),(v',q)} = 0$ if $r \notin v''$, it follows from (4.8) that

$$(\lambda x)_{(v,p),(v',q)} = \bigcup_{r \in v''} \mu y_{p,r} \mu a_{r,q} = \mu x_{p,q}\,.$$

Note that in view of (4.5)

$$\lambda x_{(v,p)(v',q)} = 0 \quad \text{if } v' \neq v \cdot x \qquad (p, q \in Q)\,.$$

Thus it follows from (4.9) that

$$\mu x_{p,q} = \bigcup_{v' \in V} \lambda x_{(v,p)(v',q)} \quad (p \in v)\,. \tag{4.10}$$

Now define a function $\ell : Q \to S$ as follows. For any $p \in Q$, choose a $v \in V$ such that $p \in v$ and set $\ell(p) = (v, p)$. Such a $v$ exists since $\mu$ is trim. Next, define $c$ by

$$c(q) = \{(v', q) \mid v' \in V\}\,.$$

Then by (4.10)

$$\mu x_{p,q} = \lambda x_{\ell(p),c(q)}\,. \qquad \blacksquare$$

For a more exhaustive treatment of related questions, especially in connection with codes, see Boë (1976), Césari (1974), Perrin and Schützenberger (1977).

## Exercises

**4.1** Compute the trim transducer associated to the second of the two semimonomial morphisms $\lambda$ of Example 4.7.

**4.2** Use Exercise 3.1 to give a second unambiguous transducer for the transduction of Example 4.3, and compare with the transducer of Exercise 4.1.

**4.3** A partial function $\beta : A^* \to C^*$ is *length preserving* if $\beta x \neq 0$ implies $|x| = |\beta x|$. Show that any rational function $\alpha : A^* \to B^*$ can be written in the form $\alpha = \gamma \circ \beta$, where $\beta : A^* \to C^*$ is a length preserving rational function and $\gamma : C^* \to B^*$ is a morphism.

**4.4** Let $M$ be a monoid. The family of *unambiguous* rational subsets of $M$ is the least family of subsets of $M$ containing $\emptyset$ and the singletons $\{m\}$, $(m \in M)$ and closed under the following operations: unambiguous union, unambiguous product, unambiguous star. (A union $X \cup Y$ is unambiguous if $X \cap Y = \emptyset$. A product $XY$ is unambiguous if $x, x' \in X$, $y, y' \in Y$, $xy = x'y'$ imply $x = x'$ and $y = y'$. A star $X^*$ is unambiguous if $X^*$ a free submonoid freely generated by $X$.)
Show that if $\alpha : A^* \to B^*$ is a rational function, then the graph of $\alpha$ is an unambiguous rational subset of $A^* \times B^*$.

**4.5** (Choffrut) Show that for any rational function $\alpha : A^* \to B^*$, there is a rational subset $X$ of $\mathrm{dom}(\alpha)$ such that $\alpha$ maps bijectively $X$ onto $\alpha(A^*) = \mathrm{im}(\alpha)$. (This is an extension of the Cross-Section Theorem to rational functions.)

**4.6** (Choffrut) Show that for any rational function $\alpha : A^* \to B^*$, there exists a rational function $\beta : B \to A^*$ such that $\alpha \circ \beta : \alpha(A^*) \to \alpha(A^*)$ is the identity function (Hint: Use Exercise 4.5).

**4.7** (Choffrut) Use the previous exercise to show that if $\alpha : A^* \to B^*$ and $\beta : B^* \to C^*$ are partial functions, and if $\alpha$ and $\beta \circ \alpha$ and $\beta$ are rational, then the restriction $\beta|_{\alpha(A^*)}$ is rational. Show that if $\beta \circ \alpha$ and $\beta$ are rational, then $\alpha$ needs not to be rational.

# 5 Bimachines

Bimachines are, in some sense, simultaneously left sequential and right sequential transducers. We show that a partial function is rational if and only if it is realized by a bimachine, and use this fact to prove that any rational function can be obtained as the composition of a left sequential function followed by a right sequential function.

**Definition** A *bimachine* $\mathcal{B} = \langle Q, q_-, P, p_-, \gamma \rangle$ over $A$ and $B$ is composed of two finite sets of *states* $Q, P$, two *initial states* $q_- \in Q$, $p_- \in P$, of two partial next state functions $Q \times A \to Q$ and $A \times P \to P$ denoted by dots, and a partial output function $\gamma : Q \times A \times P \to B^*$.

The next state functions are extended to $Q \times A^*$ and $A^* \times P$ in the usual way by setting

$$\begin{aligned} q \cdot 1 &= 1, & 1 \cdot p &= p \\ q \cdot (xa) &= (q \cdot x) \cdot a & (ax) \cdot p &= a \cdot (x \cdot p) \end{aligned}$$

for $q \in Q$, $p \in P$, $x \in A^*$, $a \in A$. Next the output function $\gamma$ is extended to $Q \times A^* \times P$ by

$$\begin{aligned} &\gamma(q, 1, p) = 1\,; \\ &\gamma(q, xa, p) = \gamma(q, x, a \cdot p)\gamma(q \cdot x, a, p) \end{aligned}$$

for $x \in A^*$, $a \in A$, $q \in Q$, $p \in P$. Then it is easily verified that

$$\gamma(q, xy, p) = \gamma(q, x, y \cdot p)\gamma(q \cdot x, y, p) \quad (x, y \in A^*).$$

and if $x = a_1 a_2 \cdots a_n$, $(a_i \in A)$, then

$$\gamma(q, x, p) = \gamma(q, a_1, a_2 \ldots a_n \cdot p)\gamma(q \cdot a_1, a_2, a_3 \ldots a_n \cdot p)$$
$$\cdots \gamma(q \cdot a_1 \ldots a_{n-1}, a_n, p)\,.$$

The partial function $A^* \to B^*$ realized by $\mathcal{B}$ is defined by

$$|\mathcal{B}|(x) = \gamma(q_-, x, p_-)\,.$$

If $P = \{p_-\}$, then $\mathcal{B}$ is, up to considerations concerning the domains, a left sequential transducer. Similarly, if $Q = \{q_-\}$, then $\mathcal{B}$ is a right sequential transducer.

Bimachines were introduced by Schützenberger (1961b). See also Nivat (1968).

**Example 5.1** Let $\alpha : a^* \to \{b, c\}^*$ be given by

$$\alpha(a^n) = \begin{cases} b^n & \text{if } n \text{ is even;} \\ c^n & \text{if } n \text{ is odd.} \end{cases}$$

Consider $P = \{p_-, p_1\}, Q = \{q_-, q_1\}$ and define the next state functions by $a \cdot p_- = p_1$, $a \cdot p_1 = p_-$, and $q_- \cdot a = q_1$, $q_1 \cdot a = q_-$. Further, let $\gamma$ be givens by the table

| | $p_-$ | $p_1$ |
|---|---|---|
| $q_-$ | $c$ | $b$ |
| $q_1$ | $b$ | $c$ |

Then a simple calculation shows that $\alpha(a^n) = \gamma(q_-, a^n, p_-)$ for $n \geq 0$.

Note that in the above definition, no assumption was made about the domains of the next state functions and $\gamma$. Call a bimachine *state complete* if both next state functions $Q \times A \to Q$ and $A \times P \to P$ are total functions.

**Theorem 5.1** (Eilenberg (1974)) *Let $\alpha : A^* \to B^*$ be a partial function with $\alpha(1) = 1$. Then $\alpha$ is rational if and only if it is realized by some bimachine over $A$ and $B$.*

We shall see that a rational function can always be realized by a state complete bimachine.

*Proof.* Let $\mathcal{B} = \langle Q, q_-, P, p_-, \gamma \rangle$ be a bimachine over $A$ and $B$, define $S = Q \times P$ and consider the transducer $\mathcal{T}$ with set of states $S$, and set of transitions $E \subset S \times A \times B^* \times S$ given by:

$$((q, p), a, z, (q', p')) \in E$$

if and only if $q \cdot a = q'$, $p = a \cdot p'$, and $z = \gamma(q, a, p') \neq 0$. Consider any path

$$((q_1, p_1), a_1, z_1, (q_1', p_1')) \cdots ((q_n, p_n), a_n, z_n, (q_n', p_n'))$$

in $\mathcal{T}$, with $x = a_1 a_2 \cdots a_n$, $y = z_1 z_2 \cdots z_n$. Then clearly $q_1 \cdot x = q_n'$, $p_1 = x \cdot p_n'$, and $y = \gamma(q_1, x, p_n')$. For any $q \in Q$, $p \in P$, define the rational transduction $\tau_{q,p} : A^* \to B^*$ by

$$\tau_{q,p}(x) = y$$

if and only if there is a path from $(q_-, p)$ to $(q, p_-)$ with input label $x$ and output label $y$, and set $\tau_{q,p}(x) = 0$ otherwise. Then $\tau_{q,p}(x) = y \neq 0$ if and only if $y = \gamma(q_-, x, p_-)$, and

$$\alpha = \sum_{(q,p)\in S} \tau_{q,p} \,.$$

Thus $\alpha$ is a rational function.

Conversely, let $\alpha$ be realized by an unambiguous normalized matrix representation $\mathcal{M} = \langle \mu, Q, q_-, \{q_-, q_+\}\rangle$. Define two families $V, W$ of subsets of $Q$ as follows:

$$\begin{aligned} v \in V &\iff \exists x \in A^* : v = \{q \in Q \mid \mu x_{q_-,q} \neq 0\}\,; \\ w \in W &\iff \exists x \in A^* : w = \{q \in Q \mid \mu x_{q,q_+} \neq 0\}\,. \end{aligned}$$

Then define functions $V \times A \to V$, $A \times W \to W$ as follows:

$$\begin{aligned} v \cdot a &= \{q' \in Q \mid \exists q \in v : \mu a_{q,q'} \neq 0\} \quad v \in V\,; \\ a \cdot w &= \{q' \in Q \mid \exists q \in w : \mu a_{q',q} \neq 0\} \quad w \in W\,. \end{aligned}$$

Extend them to words in the usual way by setting:

$$\begin{aligned} v \cdot 1 &= v\,, \quad v \cdot (xa) = (v \cdot x) \cdot a\,; \\ 1 \cdot w &= w\,, \quad (ax) \cdot w = a \cdot (x \cdot w) \end{aligned}$$

for $x \in A^*$, $a \in A$. Then clearly for $x \in A^*$

$$\begin{aligned} v \cdot x &= \{q' \in Q \mid \exists q \in v : \mu x_{q,q'} \neq 0\} \qquad v \in V\,; \\ x \cdot w &= \{q' \in Q \mid \exists q \in w : \mu x_{q',q} \neq 0\} \qquad w \in W\,. \end{aligned} \tag{5.1}$$

Next, we prove

$$\operatorname{Card}(v \cap w) \leq 1 \quad \text{for } v \in V,\ w \in W\,. \tag{5.2}$$

Assume indeed that $r, r' \in v \cap w$. By definition, there exists a word $x$ such that $\mu x_{q_-,r} \neq 0$, $\mu x_{q_-,r'} \neq 0$, and similarly there exists $y \in A^*$ such that $\mu y_{r,q_+} \neq 0$, $\mu y_{r',q_+} \neq 0$. Then $r = r'$ by Proposition 4.4.

Define a partial function

$$\gamma : V \times A^* \times W \to B^*$$

by

$$\gamma(v, 1, w) = 1$$

and for $x \in A^*$,

$$\gamma(v, x, w) = \begin{cases} 0 & \text{if } v \cap x \cdot w = \emptyset \text{ or } v \cdot x \cap w = \emptyset; \\ \mu x_{p,q} & \text{if } v \cap x \cdot w = p \text{ and } v \cdot x \cap w = q. \end{cases} \tag{5.3}$$

We claim

$$\gamma(v, zz', w) = \gamma(v, z, z' \cdot w)\gamma(v \cdot z, z', w) \quad z, z' \in A^*\,. \tag{5.4}$$

Clearly, (5.4) holds if $z = 1$ or $z' = 1$. Thus we may assume $z, z' \in A^+$. Next, if $v \cap zz' \cdot w = \emptyset$ or $v \cdot zz' \cap w = \emptyset$, then both sides of (5.4) are empty. If $p = v \cap zz' \cdot w$ and $q = v \cdot zz' \cap w$, then by definition $\gamma(v, zz', w) = \mu zz'_{p,q} \neq 0$. Since $\mu$ is unambiguous, there is exactly one $r \in Q$ such that

$$\mu zz'_{p,q} = \mu z_{p,r} \mu z'_{r,q} \,. \tag{5.5}$$

Thus, by (5.1) $r \in v \cdot z$ and $r \in z' \cdot w$. Consequently $r = v \cdot z \cap z' \cdot w$ by (5.2), and therefore $g(v, z, z' \cdot w) = \mu z_{p,r}$ and $\gamma(v \cdot z, z', w) = \mu z'_{r,q}$. Thus (5.4) follows from (5.5).

Define $v_- = \{q_-\}$, $w_+ = \{q_+\}$. Then in view of (5.4),

$$\mathcal{B} = \langle V, v_-, W, w_+, \gamma \rangle$$

is a bimachine over $A$ and $B$, and by construction $\mathcal{B}$ is state complete. Next let $x \in A^+$. Then by (5.1)

$$q_+ \in v_- \cdot x \iff \mu x_{q_-, q_+} \neq 0 \iff q_- \in x \cdot w_+ \iff x \in \mathrm{dom}(\alpha)\,.$$

Thus (5.3) implies

$$\gamma(v_-, x, w_+) = \mu x_{q_-, q_+} \quad (x \in A^+)\,.$$

Since

$$\gamma(v_-, 1, w_+) = 1\,,$$

it follows that $\alpha = |\mathcal{B}|$. ∎

We conclude this section by the following nice "decomposition theorem".

**Theorem 5.2** (Elgot and Mezei (1965)) *Let $\alpha : A^* \to B^*$ be a partial function with $\alpha(1) = 1$. The $\alpha$ is rational if and only if there are a left sequential function $\lambda : A^* \to C^*$ and a right sequential function $\rho : C^* \to B^*$ such that $\alpha = \rho \circ \lambda$. Moreover $\lambda$ can be chosen to be total and length preserving (that is $|\lambda(x)| = |x|$ for all $x \in A^*$).*

Thus in order to compute $\alpha(x)$ for some $x \in A^*$, one first reads $x$ sequentially from left to right and transforms it into a word $y$ by some left sequential transducer; then the resulting word $y$ is read from right to left and transformed into $\alpha(x)$ by a right sequential transducer.

*Proof.* If $\alpha = \rho \circ \lambda$, then $\alpha$ is a partial function and $\alpha$ is rational since the composition of two rational transductions is a rational transduction.

Conversely, consider a bimachine $\mathcal{B} = \langle Q, q_-, P, p_-, \gamma \rangle$ over $A$ and $B$ realizing $\alpha$. We may assume that $\mathcal{B}$ is state complete, that is the next state functions $Q \times A \to Q$ and $A \times P \to P$ are total. Set $C = Q \times A$, and define a left sequential transducer

$$\mathcal{L} = \langle A, C, Q, q_- \rangle$$

as follows. The next state function of $\mathcal{L}$ is the next state function $Q \times A \to Q$ of $\mathcal{B}$, and for $q \in Q, a \in A$,

$$q * a = (q, a) .$$

Define $\lambda = |\mathcal{L}|$. Then $\lambda$ is length preserving. Next define a right sequential transducer

$$\mathcal{R} = \langle C, B, P, p_- \rangle$$

by

$$\begin{aligned}
&(q, a) * p = \gamma(q, a, p) \\
&(q, a) \cdot p = \begin{cases} 0 & \text{if } \gamma(q, a, p) = 0; \\ a \cdot p & \text{otherwise,} \end{cases}
\end{aligned}$$

where $a \cdot p$ is the next state of $p$ in $\mathcal{B}$. Thus the next state function and the output function of $\mathcal{R}$ have the same domain. Set $\rho = |\mathcal{R}|$.

Let $x = a_1 a_2 \cdots a_n$, $(n \geq 1, a_i \in A)$. Then

$$\begin{aligned}
\lambda(x) &= (q_- * a_1)(q_- \cdot a_1 * a_2) \cdots (q_- \cdot a_1 a_2 \cdots a_{n-1} * a_n) \\
&= (q_-, a_1)(q_1, a_2) \cdots (q_{n-1}, a_n) ,
\end{aligned}$$

where $q_i = q_- \cdot a_1 a_2 \cdots a_i$ for $i = 1, \ldots, n-1$. Consequently,

$$\begin{aligned}
\rho(\lambda(x)) = \lambda(x) * p_- = ((q_-, a_1) &* p_{n-1})((q_1, a_2) * p_{n-2}) \\
&\cdots ((q_{n-2}, a_{n-1}) * p_1)((q_{n-1}, a_n) * p_-)
\end{aligned}$$

where $p_i = (q_{n-i}, a_{n-i+1}) \cdots (q_{n-1}, a_n) \cdot p_-$ for $i = 1, \ldots, n-1$. Thus

$$\rho(\lambda(x)) = \gamma(q_-, a_1, p_{n-1}) \cdots \gamma(q_{n-1}, a_n, p_-) = \alpha(x) .$$

(This computation holds also if $\alpha(x) = 0$ with the usual convention that $a \cdot 0 = 0$.) Thus $\alpha = \rho \circ \lambda$, and the theorem is proved. ■

## Exercises

**5.1** Prove that a partial function $\alpha : A^* \to B$ is rational if and only if $\alpha = \lambda \circ \rho$, where $\rho : A^* \to C^*$ is a right sequential function and $\lambda : C^* \to B^*$ is left sequential.

**5.2** Let $a, b$ be letters. A partial function $\alpha : a^* \to b^*$ can be viewed as a partial function $\alpha : \mathbb{N} \to \mathbb{N}$ by identifying a word with its length. Show that $\alpha : \mathbb{N} \to \mathbb{N}$ is rational if and only if $\alpha = \alpha_1 + \cdots + \alpha_n$, where each $\alpha_i$ is a partial function with domain $r_i\mathbb{N} + s_i$, $(r_i, s_i \in \mathbb{N})$ given by $\alpha_i(r_i n + s_i) = r_i' n + s_i'$ $(n \in \mathbb{N})$ for some $r_i', s_i' \in \mathbb{N}$.

# 6 A Decidable Property

In this section, we continue the investigation of sequential and subsequential functions started in Section 2.

**Theorem 6.1** (Choffrut (1977)) *Given a matrix representation $\mathcal{M}$ from $A^*$ into $B^*$, it is decidable whether $|\mathcal{M}|$ is subsequential, and whether $|\mathcal{M}|$ is sequential.*

According to Proposition III.7.4 (and Exercise III.8.3), $\mathcal{M}$ can be supposed to be trim. In view of Theorem 1.2, it is decidable whether $|\mathcal{M}|$ is a rational function. Further, the results of Section 4 show that then an unambiguous representation realizing $|\mathcal{M}|$ can effectively be constructed. Thus we may assume that the representation $\mathcal{M}$ in Theorem 6.1 is unambiguous and normalized.

We use the notations and definitions of Section 2. We consider $B^*$ as a submonoid of the free group $B^{(*)}$, according to the discussion of Section II.3. Let $\mathcal{M} = \langle \mu, Q, q_-, Q_+ \rangle$ be an unambiguous normalized matrix representation from $A^*$ into $B^*$, and set $\alpha = |\mathcal{M}|$. Then in particular $Q_+ = \{q_-, q_+\}$ or $Q_+ = \{q_+\}$, according to $1 \in \mathrm{dom}(\alpha)$ or $1 \notin \mathrm{dom}(\alpha)$. First, we define a property on $\mathcal{M}$ which will appear to express that $\alpha$ has bounded variation.

**Definition** Two states $q_1, q_2 \in Q$ are *twinned* if and only if for all $x, u \in A^*$ the following condition holds

$$\left.\begin{array}{ll} 0 \neq y_1 = \mu x_{q_-,q_1}\,, & 0 \neq z_1 = \mu u_{q_1,q_1} \\ 0 \neq y_2 = \mu x_{q_-,q_2}\,, & 0 \neq z_2 = \mu u_{q_2,q_2} \end{array}\right\} \implies y_1 z_1 y_1^{-1} = y_2 z_2 y_2^{-1} \tag{6.1}$$

$\mathcal{M}$ has the *twinning property* if any two states are twinned.

A pair $x, u \in A^*$ which satisfies the hypotheses of (6.1) is called *admissible* for $q_1, q_2$. The conclusion of (6.1) can be formulated as follows without use of inverses.

**Proposition 6.2** *Let $y_1, y_2, z_1, z_2 \in B^*$. Then*

$$y_1 z_1 y_1^{-1} = y_2 z_2 y_2^{-1} \tag{6.2}$$

*if and only if one of the following conditions is verified:*

(i) $z_1 = z_2 = 1$*;*

(ii) $z_1 \neq 1 \neq z_2$ *and there exists* $t \in B^*$ *such that either*

  (ii.1) $y_2 = y_1 t$ *and* $t z_2 = z_1 t$*; or*

  (ii.2) $y_1 = y_2 t$ *and* $t z_1 = z_2 t$*.*

*Proof* Assume (i) holds. Then (6.2) is obvious. Next, suppose for instance (ii.1). Then $y_2 z_2 y_2^{-1} = y_1 t z_2 t^{-1} y_1^{-1} = y_1 z_1 t t^{-1} y_1^{-1} = y_1 z_1 y_1^{-1}$.

Conversely, suppose that (6.2) holds. Then $z_1 = 1$ if and only if $z_2 = 1$. Thus assume $z_1 \neq 1, z_2 \neq 1$, and let $y$ be the longest common prefix of $y_1$ and $y_2$. Set $y_1 = y s_1$, $y_2 = y s_2$. Then (6.2) becomes $s_1 z_1 s_1^{-1} = s_2 z_2 s_2^{-1}$. If $s_1 = 1$, then (ii.1) holds with $t = s_2$; if $s_2 = 1$, then (ii.2) holds with $t = s_1$. If both $s_1, s_2 \neq 1$, then they differ by their initial letter by definition of $y$. Thus the equation $s_1 z_1 s_1^{-1} = s_2 z_2 s_2^{-1}$ implies $z_1 = z_2 = 1$, contrary to the assumption. ■

**Example 6.1** Consider the following unambiguous normalized transducer (Figure IV.17). The function $\alpha : a^* \to \{b,c,d\}^*$ realized by this transducer is given by

$$\alpha(1) = 1\,;\ \alpha(a^{2n}) = d(cb)^n\,,\ n \geq 1\,;\ \alpha(a^{2n+1}) = d(cb)^{n+1}\,,\ n \geq 0\,.$$

In order to verify that the matrix representation $\mathcal{M}$ associated to the transducer has the twinning property, it suffices to show that the states 2 and 3 are twinned. For this, let $x = a^{2n+1}, u = a^{2m}$ be an admissible pair for $2,3$. Then $y_1 = \mu x_{1,2} = d(cb)^n$, $z_1 = \mu u_{2,2} = (cb)^m$, and $y_2 = \mu x_{1,3} = dc(bc)^n = d(cb)^n c = y_1 t$ with $t = c$, and $z_2 = \mu u_{3,3} = (bc)^m$, whence $tz_2 = z_1 t$. Thus $y_1 z_1 y_1^{-1} = y_2 z_2 y_2^{-1}$ by Proposition 6.2, and $2,3$ are twinned.

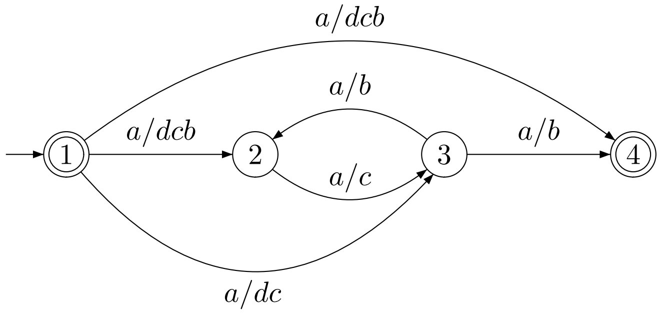

Figure IV.17

We note the following corollary.

**Corollary 6.3** *Let $y_1, y_2, z_1, z_2 \in B^*$. If $y_1 z_1^k y_1^{-1} = y_2 z_2^k y_2^{-1}$ for some $k > 0$, then $y_1 z_1 y_1^{-1} = y_2 z_2 y_2^{-1}$.*

*Proof.* We may assume $z_1, z_2 \neq 1$ and for instance $|y_2| \geq |y_1|$. Then there exists, in view of Proposition 6.2, a word $t \in B^*$ such that $y_2 = y_1 t$ and $tz_2^k = z_1^k t$. We prove that this implies $tz_2 = z_1 t$ by induction on $|t|$, the case $|t| = 0$ being immediate. If $|t| \leq |z_1|$, then $z_1 = ts$ for some word $s$, hence $tz_2^k = (ts)^k t = t(st)^k$. Therefore $z_2 = st$ and $tz_2 = tst = z_1 t$. If $|t| > |z_1|$, then $t = z_1 t'$ for some $t'$. Next $tz_2^k = z_1 t' z_2^k = z_1^k z_1 t'$, thus $t' z_2^k = z_1^k t'$ and $t' z_2 = z_1 t'$ by induction. Thus $tz_2 = z_1 t$. ■

We note also that if $y_1 z_1 y_1^{-1} = y_2 z_2 y_2^{-1}$, then for all $r_1, r_2$

$$\|y_1 z_1 r_1, y_2 z_2 r_2\| \leq \|y_1 r_1, y_2 r_2\| \tag{6.3}$$

Indeed, (6.3) is obvious if $z_1 = z_2 = 1$. Otherwise, we may assume by Proposition 6.2 that for instance $y_2 = y_1 t$, and $tz_2 = z_1 t$ for some word $t$. Then $y_2 z_2 = y_1 z_1 t$, and consequently $|y_1 z_1 r_1 \wedge y_2 z_2 r_2| \geq |y_1 z_1|$. This proves (6.3).

**Proposition 6.4** *The following two conditions are equivalent:*

(i) *$\mathcal{M}$ has the twinning property;*
(ii) *$\alpha$ has bounded variation.*

*Proof.* Assume that $\mathcal{M}$ has the twinning property. Let $n$ be the number of states of $Q$. Consider an integer $k \geq 0$, and define

$$K = \max\{\|\alpha(x_1), \alpha(x_2)\| : x_1, x_2 \in \mathrm{dom}(\alpha), \|x_1, x_2\| \leq k, |x_1 \wedge x_2| \leq n^2\}\,.$$

Note that $\|x_1, x_2\| \leq k$ and $|x_1 \wedge x_2| \leq n^2$ imply $|x_1| + |x_2| \leq k + 2n^2$. Thus $K$ is finite. We prove that $\|x_1, x_2\| \leq k$ and $x_1, x_2 \in \mathrm{dom}(\alpha)$ imply: $\|\alpha(x_1), \alpha(x_2)\| \leq K$. This holds by definition if $|x_1 \wedge x_2| \leq n^2$. Arguing by induction on $|x_1 \wedge x_2|$, we assume $|x_1 \wedge x_2| > n^2$. Then there exist words $s, v_1, v_2$ with $s = x_1 \wedge x_2$, $x_i = sv_i$, $i = 1, 2$, $|s| > n^2$. Consider the successful paths in $\mathcal{M}$ with input labels $x_1$ and $x_2$. Since $|s| > n^2$, there exists a factorization $s = wuv$, $|u| > 0$, and two states $q_1, q_2$ such that $\alpha(x_i) = y_i z_i r_i$, where $y_i = \mu w_{q_-, q_i}$, $z_i = \mu u_{q_i, q_i}$, $r_i = \mu(vv_i)_{q_i, q_+}$, $(i = 1, 2)$.

Since $q_1$ and $q_2$ are twinned, we have by (6.3)

$$\|\alpha(x_1), \alpha(x_2)\| \leq \|y_1 r_1, y_2 r_2\| = \|\alpha(x_1'), \alpha(x_2')\|$$

where $x_1' = wvv_1, x_2' = wvv_2 \in \mathrm{dom}(\alpha)$. Further $x_1' \wedge x_2' = wv$ is strictly shorter than $s$. Consequently $\|\alpha(x_1), \alpha(x_2)\| \leq K$ and $\alpha$ has bounded variation.

Conversely, let $q_1, q_2$ be two states in $\mathcal{M}$, and consider a pair $x, u$ of words which is admissible for $q_1, q_2$, that is satisfying the hypotheses of (6.1). Since $\mathcal{M}$ is trim, there are words $v_1, v_2 \in A^*$ such that $r_i = (\mu v_i)_{q_i, q_+} \neq 0$ for $i = 1, 2$. Consequently $xu^m v_i \in \mathrm{dom}(\alpha)$ for $m \geq 0, i = 1, 2$. Next $\|xu^m v_1, xu^m v_2\| = \|v_1, v_2\|$, and since $\alpha$ has bounded variation, there exists an integer $K$ such that

$$\|y_1 z_1^m r_1, y_2 z_2^m r_2\| \leq K \qquad m \geq 0\,.$$

Consequently, there exist words $s_1, s_2$, with $|s_1| + |s_2| \leq K$ such that $s_i$ is a suffix of $y_i z_i^m r_i$ $(i = 1, 2)$ for an infinity of exponents $m$. In particular, there are integers $p \geq 0$, $k > 0$ such that

$$y_1 z_1^p r_1 s_1^{-1} = y_2 z_2^p r_2 s_2^{-1}\,; \tag{6.4}$$

$$y_1 z_1^{k+p} r_1 s_1^{-1} = y_2 z_2^{k+p} r_2 s_2^{-1}\,. \tag{6.5}$$

(6.5) can be written as:

$$y_1 z_1^k y_1^{-1} y_1 z_1^p r_1 s_1^{-1} = y_2 z_2^k y_2^{-1} y_2 z_2^p r_2 s_2^{-1}\,.$$

In view of (6.4), this implies:

$$y_1 z_1^k y_1^{-1} = y_2 z_2^k y_2^{-1}\,,$$

and by Corollary 6.3, $y_1 z_1 y_1^{-1} = y_2 z_2 y_2^{-1}$. Thus $q_1$ and $q_2$ are twinned. This completes the proof.

The following proposition provides the main argument for the proof of Theorem 6.1.

**Proposition 6.5** *Let $n = \mathrm{Card}(Q)$. Then $\mathcal{M}$ has the twinning property if and only if for all $q_1, q_2 \in Q$, (6.1) holds for all pairs $x, u \in A^*$ with $|xu| \leq 2n^2$.*

*Proof.* We argue by induction on $|xu|$, that is we assume that (6.1) holds for all $q_1, q_2 \in Q$, and for all pairs $x', u'$ of words admissible for $q_1, q_2$ such that $|x'u'| < |xu|$. Consider $q_1, q_2 \in Q$, and consider a pair $x, u$ of words such that the hypotheses of (6.1) hold. Clearly we may assume $|xu| > 2n^2$ and $|u| > 0$. Thus either $|x| > n^2$ or $|u| > n^2$. If $|x| \geq n^2 + 1$, then there exist a factorization $x = x_1 v x_2$, with $v \neq 1$, and $p_1, p_2 \in Q$, $r_1, s_1, t_1, r_2, s_2, t_2 \in B^*$ such that $y_1 = r_1 s_1 t_1$, $y_2 = r_2 s_2 t_2$ and

$$\begin{aligned} r_1 &= \mu(x_1)_{q_-,p_1}\,,\ s_1 = \mu v_{p_1,p_1}\,,\ t_1 = \mu(x_2)_{p_1,q_1}\,,\\ r_2 &= \mu(x_1)_{q_-,p_2}\,,\ s_2 = \mu v_{p_2,p_2}\,,\ t_2 = \mu(x_2)_{p_2,q_2}\,. \end{aligned}$$

Thus $x_1, v$ is an admissible pair for $p_1, p_2$ and $x_1 x_2, u$ is an admissible pair for $q_1, q_2$. Consequently by induction

$$r_1 s_1 r_1^{-1} = r_2 s_2 r_2^{-1} \quad \text{and} \quad r_1 t_1 z_1 t_1^{-1} r_1^{-1} = r_2 t_2 z_2 t_2^{-1} r_2^{-1}$$

Hence

$$\begin{aligned} y_1 z_1 y_1^{-1} &= (r_1 s_1 r_1^{-1})(r_1 t_1 z_1 t_1^{-1} r_1^{-1})(r_1 s_1^{-1} r_1^{-1})\\ &= r_2 s_2 t_2 z_2 t_2^{-1} s_2^{-1} r_2^{-1} = y_2 z_2 y_2^{-1}\,. \end{aligned}$$

Next assume $|u| \geq n^2 + 1$. Then similarly there exist a factorization $u = u_1 v u_2$ with $v \neq 1$, and $p_1, p_2 \in Q$, $r_1, s_1, t_1, r_2, s_2, t_2 \in B^*$ such that $z_1 = r_1 s_1 t_1$, $z_2 = r_2 s_2 t_2$ and

$$\begin{aligned} r_1 &= \mu(u_1)_{q_1,p_1}\,,\ s_1 = \mu v_{p_1,p_1}\,,\ t_1 = \mu(u_2)_{p_1,q_1}\,,\\ r_2 &= \mu(u_1)_{q_1,p_2}\,,\ s_2 = \mu v_{p_2,p_2}\,,\ t_2 = \mu(u_2)_{p_2,q_2}\,. \end{aligned}$$

If $u_2 = 1$, then $p_1 = q_1$, $p_2 = q_2$, $t_1 = t_2 = 1$. Thus $(x, u_1)$ and $(x, v)$ are admissible pairs for $q_1, q_2$, and by induction

$$y_1 r_1 y_1^{-1} = y_2 r_2 y_2^{-1} \quad \text{and} \quad y_1 s_1 y_1^{-1} = y_2 s_2 y_2^{-1}\,.$$

Then

$$\begin{aligned} y_1 z_1 y_1^{-1} &= y_1 r_1 s_1 y_1^{-1} = (y_1 r_1 y_1^{-1})(y_1 s_1 y_1^{-1})\\ &= (y_2 r_2 y_2^{-1})(y_2 s_2 y_2^{-1}) = y_2 z_2 y_2^{-1}\,. \end{aligned}$$

Finally, if $u_2 \neq 1$, then $x, u_1 u_2$ is an admissible pair for $q_1, q_2$ and $x u_1, v$ is an admissible pair for $p_1, p_2$. By induction

$$y_1 r_1 t_1 y_1^{-1} = y_2 r_2 t_2 y_2^{-1} \quad \text{and} \quad y_1 r_1 s_1 r_1^{-1} y_1^{-1} = y_2 r_2 s_2 r_2^{-1} y_2^{-1}\,.$$

It follows that

$$\begin{aligned} y_1 z_1 y_1^{-1} &= y_1 r_1 s_1 t_1 y_1^{-1} = (y_1 r_1 s_1 r_1^{-1} y_1^{-1})(y_1 r_1 t_1 y_1^{-1})\\ &= (y_2 r_2 s_2 r_2^{-1} y_2^{-1})(y_2 r_2 t_2 y_2^{-1}) = y_2 r_2 s_2 t_2 y_2^{-1} = y_2 z_2 y_2^{-1}\,. \quad \blacksquare \end{aligned}$$

**Proposition 6.6** *If $\mathcal{M}$ has $n$ states and has the twinning property, then $\alpha$ preserves prefixes if and only if $\alpha(1) = 1$ and for any $x \in A^*$ with $|x| \leq n^2$, and for any $a \in A$, $\alpha(xa) \neq 0$ implies $\alpha(xa) \in \alpha(x)B^*$.*

*Proof.* The conditions are obviously necessary. Conversely, let $x \in A^*$, $a \in A$ such that $xa \in \mathrm{dom}(\alpha)$. Arguing by induction, we may assume $|x| > n^2$. There exists a factorization $x = x_1vx_2$ with $v \neq 1$, and $q_1, q_2 \in Q$, $y_1, z_1, r_1, y_2, z_2, r_2 \in B^*$ such that

$$\begin{aligned} &\alpha(x) = y_1z_1r_1\,, \quad \alpha(xa) = y_2z_2r_2\,,\\ &y_1 = \mu(x_1)_{q-,q_1}\,, \quad z_1 = \mu v_{q_1,q_1}\,, \quad r_1 = \mu(x_2)_{q_1,q+}\,,\\ &y_2 = \mu(x_1)_{q-,q_2}\,, \quad z_2 = \mu v_{q_2,q_2}\,, \quad r_2 = \mu(x_2a)_{q_2,q+}\,, \end{aligned}$$

It follows that $\alpha(x_1x_2) = y_1r_1$, $\alpha(x_1x_2a) = y_2r_2$. Since $\mathcal{M}$ has the twinning property, and since $x_1, v$ is an admissible pair for $q_1, q_2$,

$$y_1z_1y_1^{-1} = y_2z_2y_2^{-1}\,. \tag{6.6}$$

Next, since $|x_1x_2| < |x|$, there is a word $u \in B^*$ such that

$$y_2r_2 = \alpha(x_1x_2a) = \alpha(x_1x_2)u = y_1r_1u\,. \tag{6.7}$$

Combining (6.6) and (6.7), we obtain

$$\alpha(xa) = y_2z_2r_2 = y_2z_2y_2^{-1}y_2r_2 = y_1z_1y_1^{-1}y_1r_1u = y_1z_1r_1u = \alpha(x)u\,. \qquad \blacksquare$$

*Proof* of Theorem 6.1. Since $\alpha$ is realized by $\mathcal{M}$, $\alpha$ is rational. Consequently $\alpha^{-1} : A^* \to B^*$ is a rational transduction and by Corollary III.4.2, $\alpha^{-1}$ preserves rational languages. Thus in view of Theorem 2.7, $\alpha$ is subsequential if and only if $\alpha$ has bounded variation, and by Proposition 6.4 this holds if and only if $\mathcal{M}$ has the twinning property which is decidable by Proposition 6.5. Thus it is decidable whether $\alpha$ is subsequential. Further, $\alpha$ is sequential if and only if $\mathcal{M}$ has the twinning property and $\alpha$ preserves prefixes. By Proposition 6.6, this is decidable. Thus the proof is complete. $\blacksquare$

# Bibliography

Expository texts on formal languages include Autebert and Cousineau (1976), Ginsburg (1966), Becker and Walter (1977), Eilenberg (1974), Ginsburg (1966), Hopcroft and Ullman (1969), Hotz (1968, 1969), Hotz and Claus (1972), Maurer (1977), Salomaa (1969, 1973). Salomaa (1973) contains a list of books on formal languages and automata theory up to March 1972. Ginsburg (1975) is a tratise on AFL theory. For rational tranductions and rational functions, see Eilenberg (1974).

Aho A. V and Ullman J. D . *The theory of parsing, translation, and compiling. Vol. I: Parsing.* Prentice-Hall Inc., Englewood Cliffs, N. J., 1972. Prentice-Hall Series in Automatic Computation. 2

Amar V and Putzolu G . Generalizations of regular events. *Information and Control*, 8:56–63, 1965. ISSN 0890-5401. 1

Anissimow A. W and Seifert F. D . Zur algebraischen Charakteristik der durch kontext-freie Sprachen definierten Gruppen. *Elektron. Informationsverarbeit. Kybernetik*, 11(10–12):695–702, 1975. ISSN 0013-5712. 2.7, 2.4

Autebert J.-M and Cousineau G . *Théorie des automates et des langages formels: I. Les languages algébriques.* Institut de Programmation, Université de Paris, 1976. 2, 3, 6

Becker H and Walter H . *Formale Sprachen.* Vieweg, Braunschweig, 1977. Eine Einführung, Skriptum für Hörer aller Fachrichtungen ab 3. Semester, Uni-Text. (document), 6

Benois M . Parties rationnelles du groupe libre. *C. R. Acad. Sci. Paris Sér. A-B*, 269:A1188–A1190, 1969. 2.8, 2.9

Benois M and Nivat M . Congruences parfaites et quasi-parfaites. In *Séminaire Dubreil, 25e année 1971-72.* Inst. H. Poincaré, Université de Paris, 1972. 3

Blattner M and Head T . Single-valued *a*-transducers. *J. Comput. System Sci.*, 156(3):310–327, 1977. ISSN 0022-0000. 1

Boë J.-M . *Représentations des monoïdes. Applications à la théorie des codes.* Thèse de 3e cycle, Université de Montpellier, 1976. 4

Césari Y . Sur l'application du théorème de Suschkewitsch à l'étude des codes rationnels complets. In *Automata, languages and programming (Second Colloq., Univ. Saarbrücken, Saarbrücken, 1974)*, pages 342–350. Lecture Notes in Comput. Sci., Vol. 14. Springer-Verlag, Berlin, 1974. 4

Choffrut C . Une caractérisation des fonctions séquentielles et des fonctions sous-séquentielles en tant que relations rationnelles. *Theoret. Comput. Sci.*, 5(3): 325–337, 1977. ISSN 0304-3975. 6.1

Choffrut C . *Contribution à l'étude de quelques familles remarquables de fonctions rationnelles.* Thèse d'état, niversité Paris VII, Paris, 1978. 2, 2.7

Cochet Y and Nivat M . Une généralisation des ensembles de Dyck. *Israel J. Math.*, 9:389–395, 1971. ISSN 0021-2172. 3

Conway J. H . *Regular Algebra and Finite Machines.* Chapman and Hall, 1971. 4.6

Davis M . *Computability and unsolvability.* McGraw-Hill Series in Information Processing and Computers. McGraw-Hill Book Co., Inc., New York, 1958. 8

Eilenberg S . *Algèbre catégorique et théorie des automates.* Institut Henri Point-caré, Université de Paris, 1967. 1

Eilenberg S . *Automata, Languages, and Machines. Vol. A.* Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York, 1974. Pure and Applied Mathematics, Vol. 58. 1, 1, 5.16, 6, 7, 2, 2, 2, 3, 4.2, 5.1, 6

Eilenberg S . Automata, Languages, and Machines. Vol. C, 1978. in preparation. 1, 4, 4.5

Elgot C. C and Mezei J. E . On relations defined by generalized finite automata. *IBM J. Res. Develop*, 9:47–68, 1965. ISSN 0018-8646. 4.4, 4.8, 6, 5.2

Fischer P. C and Rosenberg A. L . Multitape one-way nonwriting automata. *J. Comput. System Sci.*, 2:88–101, 1968. ISSN 0022-0000. 8

Fliess M . Deux applications de la représentation matricielle d'une série rationnelle non commutative. *J. Algebra*, 19:344–353, 1971. ISSN 0021-8693. 2.10, 2

Ginsburg S . *The Mathematical Theory of Context-Free Languages.* McGraw-Hill Book Co., New York, 1966. (document), 4.6, 2, 2, 6

Ginsburg S . *Algebraic and Automata-Theoretic Properties of Formal Languages.* North-Holland Publishing Co., Amsterdam, 1975. Fundamental Studies in Computer Science, Vol. 2. 6, 6

Ginsburg S and Rose G. F . A characterization of machine mappings. *Canad. J. Math.*, 18:381–388, 1966. ISSN 0008-414X. 2.8

Greibach S. A . The hardest context-free language. *SIAM J. Comput.*, 2:304–310, 1973. ISSN 1095-7111. 5.12

Hopcroft J. E and Ullman J. D . *Formal languages and their relation to automata.* Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. (document), 6

Hotz G . *Automatentheorie und formale Sprachen. Band I. Turingmaschinen und rekursive Funktionen.* B. I.-Hochschulskripten, Band 821 821a. Bibliographisches Institut, Mannheim, 1968. Ausgearbeitet von Hermann Walter. 6

Hotz G . *Automatentheorie und formale Sprachen. Band II: Endliche Automaten.* B. I.-Hochschulskripten, Band 822/822a. Bibliographisches Institut, Mannheim, 1969. Ausgearbeitet von Hermann Walter. 6

Hotz G and Claus V . *Automatentheorie und formale Sprachen. Band III. Formale Sprachen.* B.I.-Hochschulskripten, No. 823a. Bibliographisches Institut, Mannheim, 1972. 6

Kleene S. C . Representation of events in nerve nets and finite automata. In *Automata studies*, Annals of mathematics studies, no. 34, pages 3–41. Princeton University Press, Princeton, N. J., 1956. 4.1

Magnus W , Karrass A , and Solitar D . *Combinatorial Group Theory: Presentations of groups in terms of generators and relations.* Interscience Publishers [John Wiley & Sons, Inc.], New York-London-Sydney, 1966. 3, 3, 3.3

Maurer H . *Theoretische Grundlagen der Programmiersprachen. Theorie der Syntax.* B.I.-Hochschultaschenbücher, Band 404. Bibliographisches Institut, Mannheim, 1977. 6

McKnight, Jr. J. D . Kleene quotient theorems. *Pacific J. Math.*, 14:1343–1352, 1964. ISSN 0030-8730. 2.4

McKnight, Jr. J. D and Storey A. J . Equidivisible semigroups. *J. Algebra*, 12: 24–48, 1969. ISSN 0021-8693. 1

Nivat M . *Transductions des langages de Chomsky.* Thèse d'état, Université de Paris, 1967. 4

Nivat M . Transductions des langages de Chomsky. *Ann. Inst. Fourier (Grenoble)*, 18(fasc. 1):339–455, 1968. ISSN 0373-0956. 3.2, 4.1, 4, 5

Ogden W . A helpful result for proving inherent ambiguity. *Math. Systems Theory*, 2:191–194, 1968. ISSN 0025-5661. 2

Perrin D and Schützenberger M.-P . Codes et sous-monoïdes possédant des mots neutres. In *Theoretical computer science (Third GI Conf., Darmstadt, 1977)*, volume 48 of *Lecture Notes in Comput. Sci.*, pages 270–281. Springer-Verlag, Berlin, 1977. 4

Perrot J.-F and Sakarovitch J . A theory of syntactic monoids for context-free languages. In *Information processing 77 (Proc. IFIP Congr., Toronto, Ont., 1977)*, pages 68–72. IFIP Congr. Ser., Vol. 7. North-Holland, Amsterdam, 1977. 4.3

Sakarovitch J . Sur les groupes infinis, considérés comme monoïdes syntaxiques de langages formels. In *Séminaire d'Algèbre Paul Dubreil, 29ème année (Paris, 1975–1976)*, pages 168–179. Lecture Notes in Math., 586. Springer, Berlin, 1977. 2.5

Salomaa A . *Theory of automata.* International Series of Monographs in Pure and Applied Mathematics, Vol. 100. Pergamon Press, Oxford, 1969. 6

Salomaa A . *Formal languages.* Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1973. ACM Monograph Series. (document), 6

Salomaa A  and Soittola M . *Automata-theoretic aspects of formal power series.* Springer-Verlag, New York, 1978. ISBN 0-387-90282-1. Texts and Monographs in Computer Science. 1, 7

Schnorr C.-P . *Rekursive Funktionen und ihre Komplexität.* B. G. Teubner, Stuttgart, 1974. Teubner Studienbücher: Informatik, Leitfäden der angewandten Mathematik und Mechanik LAMM, Band 24. 8

Schützenberger M.-P . Some remarks on Chomsky's context-free languages. *Quarterly Progress Report of the Research Lab. of Electronics, MIT*, 68:155–170, 1961a. 1

Schützenberger M.-P . A remark on finite transducers. *Information and Control*, 4:185–196, 1961b. ISSN 0890-5401. 5

Schützenberger M.-P . Sur les relations rationnelles. In *Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975)*, volume 33 of *Lecture Notes in Comput. Sci.*, pages 209–213. Springer-Verlag, Berlin, 1975. 1

Schützenberger M.-P . Sur les relations rationnelles entre monoïdes libres. *Theoret. Comput. Sci.*, 3(2):243–259, 1976. ISSN 0304-3975. 4, 4.5

Schützenberger M.-P . Sur une variante des fonctions séquentielles. *Theoret. Comput. Sci.*, 4(1):47–57, 1977. ISSN 0304-3975. 2

Vogel H . Zur Theorie des rationalen und deterministischen Mengen. Technical Report 18, Gesellschaft Math. Datenverarb., 1972. 1.2

Walljasper S. J . Nondeterministic automata and effective languages. Ph. d., University of Iowa, 1970. 1.2

# Index